THE EFFECTS OF BLACK HOLE ATTACKS ON THE PERFORMANCE OF AODV, DSR AND OLSR IN MOBILE AD-HOC NETWORKS

by

SHANE KALICHURN

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 ELISHA O. OCHOLA

December 2021

Declaration

I declare that

THE EFFECTS OF BLACK HOLE ATTACKS ON THE PERFORMANCE OF AODV, DSR AND OLSR IN MOBILE AD-HOC NETWORKS

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.

I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

SKalichurn

Signature

29 May 2022

Date

Acknowledgements

To my family and friends, thank you for your unceasing support and encouragement. To my parents, Shirley Kalichurn and Suren Kalichurn (late), I would like to thank you for always loving me and giving me the best, especially for guiding me and praying for God's best over my life. I would like to give special thanks to my wife and best friend, Jezelle Genevee Kondiah, for motivating me and encouraging me to be the best I can be. I love you all very much.

A special thank you to my supervisor, Mr Elisha Ochola, for assisting me with this study. I am also thankful to the University of South Africa for allowing me the opportunity to learn and for providing me with the necessary resources to complete this study. I would also like to extend a huge and heartfelt thank you to Lianne Hugo, who through the process of review and assisting me with the language editing has become a dear friend, thank you once again for going beyond the call of duty and giving me a helping hand when I needed it the most.

Most importantly and above all else, I would like to thank my Lord and Saviour, Jesus Christ, for guiding me and providing me with the wisdom, knowledge and understanding to complete this study. For through Him, I can do all things.

Conference Publications

The following peer-reviewed conference paper was published as a contribution of this study:

Shane Kalichurn and Elisha Oketch Ochola, “Comparison of AODV, DSR and OLSR Performance Under Black Hole Attack in Mobile Ad-Hoc Network”, Proceedings of the *18th JOHANNESBURG International Conference on Science, Engineering, Technology & Waste Management (SETWM-20)*, Johannesburg, South Africa, 16-17 November 2020.

Acronyms and Abbreviations

Abbreviation	Phrase or word
ACK	Acknowledgement Packet
AODV	Ad-hoc On-Demand Distance Vector
AODVR	Ad-hoc On-Demand Distance Vector Robust
BC-AODV	Blockchain Ad-hoc On-Demand Distance Vector
CACK	Credit Acknowledgement
CAODV	Credit-based Ad--hoc On-Demand Distance Vector
DoS	Denial of Service
DRI	Data Routing Information
DSDV	Destination-Sequenced Distance-Vector
DSR	Dynamic Source Routing
EVM	Encrypted Verification Method
FREP	Further Reply
FREQ	Further Request
GWMM	Gauss-Markov Mobility Model
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
MANET	Mobile Ad-hoc Network
MAOMDV	Modified Ad-hoc On-Demand Multipath Distance Vector
MPR	Multi-point Relays
NAM	Network Animator
NHN	Next Hop Node
NS2	Network Simulator 2
OLSR	Optimised Link State Routing
OMD	Overhearing based Misbehaviour Detection
PDR	Packet Delivery Ratio
RDMM	Random Direction Mobility Model
RERR	Route Error
RPGMM	Reference Point Group Mobility Model
RREP	Route Reply
RREQ	Route Request
RWMM	Random Walk Mobility Model
RWPMM	Random Waypoint Mobility Model

SAODV	Secure Ad-hoc On-Demand Distance Vector
SYN	Synchronization
TC	Topology Control
TCP	Transmission Control Protocol
TVP	Threat Value Parameter
UDP	User Diagram Protocol
VANET	Vehicular Mobile Ad-hoc Network
WSN	Wireless Sensor Networks
ZRP	Zone Routing Protocol

Abstract

Black Hole attacks manipulate Mobile Ad-hoc Network (MANET) routing protocols by deceiving nodes sending data into believing that the malicious Black Hole node has the optimal route available for data transmission to the intended recipient node. The ability to implement the appropriate routing protocol is essential in minimising the impact Black Hole attacks have on MANETs. In this study, the Ad-hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Optimised Link State Routing (OLSR) protocols were simulated under no-attack as well as under Black Hole attack scenarios to determine which of these protocols performed best. The results were analysed using the performance metrics of throughput, end-to-end delay, and packet delivery ratio (PDR). The results of the simulations showed that AODV was more vulnerable to Black Hole attacks than DSR or OLSR. Furthermore, the results showed that the adverse effects of a Black Hole attack on throughput, end-to-end delay, and PDR were more significant in AODV as opposed to DSR, which had the best overall performance.

Keywords: AODV Protocol, Black Hole Attack, DSR Protocol, Mobile Ad-Hoc Networks, OLSR Protocol, MANET Routing Protocol Comparison, Mobility Model Comparison, MANET Security Issues, Random Waypoint Model, NS2 Simulation

Table of Contents

Chapter 6 – Simulation Implementation and Simulation Environment

Chapter 7 – Simulation Results and Analysis

Chapter 8 – Conclusion and Future Work

List of Figures

List of Tables

Chapter 1 – Introduction

1.1 Background

The increasing demand for lightweight, low-cost, portable mobile devices has resulted in Mobile Ad-hoc Networks (MANETs) becoming very popular as they provide a means for effective and efficient communications amongst these devices. A MANET is formed when a group of wireless mobile devices dynamically establish a temporary network to share resources without using any fixed network infrastructure or centralised management (Raza *et al*., 2016). MANETs are suitable for providing communications in cases where it is impossible to set up traditional wired networks (Aluvala, Sekhar & Vodnala, 2016).

In a MANET, nodes within transmission range communicate by forwarding messages directly to each other, whereas nodes not within data transmission range depend on intermediary nodes to facilitate communication. Routing protocols facilitate data communications and establish an optimal path, i.e., one with the least hops, from the source node to the destination node. In ad-hoc networks, nodes new to a network need to detect and discover the network topology and layout before any form of data transmission, both sending and receiving, between other nodes in the network can occur, which is done via the Route Discovery process. A new node announces its presence in the topology and then listens for announcements broadcast from its neighbour nodes (Boulaiche, 2020). Each node learns about the other nodes nearby and the routes needed to reach them. Data packets need to be delivered timeously. Therefore, minimum overhead and bandwidth are crucial to the success of a routing protocol (Raza *et al*., 2016). MANET routing protocols need to function in different networking contexts, ranging from small ad-hoc groups to more extensive and complex mobile multi-hop networks. MANET routing protocols are classified based on how nodes build and maintain communication routes within the MANET.

Reactive routing protocols, such as Ad-hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), establish routes to destination nodes only when the source node does not have a valid (active) route available for data transmission to occur, via the Route Discovery process. Reactive routing protocols have a much lower control overhead as routes are only created when required; however, route discovery can cause the MANET to suffer long delays (Boulaiche, 2020).

Proactive routing protocols, such as Optimised Link State Routing Protocol (OLSR), function by ensuring updated records of network routes are stored. All nodes in the

network have a local routing table to determine how to establish a connection with other nodes in the network. Nodes exchange topology information to maintain a consistent network view in their local routing tables. This exchange of information among nodes results in a high control overhead (Ballav, 2016).

Hybrid routing protocols, such as Zone Routing protocol (ZRP), use proactive routing protocols to obtain the initial network topology and other unknown routing information. Once the initial network topology is obtained, the hybrid protocol uses the reactive routing protocols' mechanisms to maintain the routing information when any changes occur in the network topology (Walikar & Biradar, 2017).

MANETs are more susceptible to malicious attacks than traditional wired networks due to the need for portability, open communication and the lack of physical infrastructure connecting devices in the network. The physical boundaries of MANETs cannot be defined precisely, allowing an adversary to gain access quickly and easily to the network if they are within the transmission range of a node within the MANET (Thangaraj, Rengarajan & Selvanayaki, 2019). The low bandwidth capacity within MANETs makes them more susceptible to attenuation, interference, and signal noise (Bhalia, 2015). Most MANET routing protocols assume all nodes are non-malicious and cooperative. Therefore, if an adversary joins the MANET, it can quickly become an essential routing agent and disrupt the network operations within the MANET (Thangaraj *et al.*, 2019).

The exploitation of any of these vulnerabilities would result in the compromised performance of the MANET. It is important to understand how MANETs are attacked and the underlying causes of these attacks, all of which primarily occur in the routing protocols. Most routing protocols used by MANETs were designed under the assumption that all nodes in the network could be trusted and are fully cooperative. However, should one of these nodes be compromised, the entire MANET is vulnerable to various attacks, including the Black Hole attack.

1.2 Motivation

Secure and protected communication is fundamentally important to all wired and wireless networks. The ultimate success of MANETs will not only be determined by how efficient and effective communication is but also by how much confidence users have in how secure communication amongst nodes within the MANET is. Therefore, the security aspects of MANETs need to be analysed to identify potential threats and vulnerabilities. This study is focused on the most common and dangerous security attack occurring in MANETs, the Black Hole attack. The primary aim of a Black Hole attack is confusion and disruption to the routing process. The effect that Black Hole attacks have on the

performance of MANETs is often tested under Reactive Routing Protocols as they are more susceptible to this attack since they establish routes on demand. The performance of a MANET is severely hampered when Black Hole nodes exist, as inefficient and malicious paths are used for data transmission instead of the shortest path between the sender and destination nodes.

1.3 Problem Statement

One of the most used MANET routing protocols is the Ad-hoc On-demand Distance Vector (AODV) routing protocol. The impact, in terms of performance and functionality, Black Hole attacks have on MANETs using the AODV routing protocol has been studied extensively, resulting in the proposal of several detection schemes and mitigation solutions. However, the advancement in research of the AODV routing protocol has been done at the expense of other routing protocols. Therefore, this study is aimed at analysing and recognising the impact Black Hole attacks have on MANETs implementing other routing protocols as compared to the impact that Black Hole attacks have on MANETs implementing the AODV routing protocol.

1.4 Research Objectives

The following objectives have been identified for this research:

1. To analyse the impact Black Hole attacks have on the performance of a MANET.
2. To compare the performance of AODV, DSR and OLSR protocols under Black Hole attack.
3. To identify possible solutions to the vulnerabilities in Routing Protocol used by MANETs.
4. To determine which Mobility Model is most suitable for MANET simulation scenarios.

1.5 Research Questions

1. What impact does a Black Hole attack have on the performance of MANETs using the different types of routing protocols?
2. Which (reactive or proactive) routing protocol is more vulnerable to attacks in MANETs?
3. What are the existing and proposed solutions to Black Hole attacks in MANETs?
4. Which Mobility Model best simulates the movement patterns of nodes in a MANET?

1.6 Research Methodology

The main aim of this study is to fulfil the research objectives and answer the research questions that have been presented. In this instance, the proposed research questions need both qualitative and quantitative approaches to be answered adequately. The qualitative approach is used to gain insight from previously completed research work to understand any research shortcomings. In contrast, the quantitative approach is used in studies that require experiments or simulations to be conducted, and the results analysed to draw a conclusion (Newman & Benz, 1998).

This study required analysis to be conducted using a theoretical and a simulation model. The theoretical modelling was derived based on review and study of existing related literature. Simulation models were created using simulation software to test different scenarios to gather results and findings. Once the simulation data had been collected, it was analysed to find the necessary conclusions.

1.6.1 Research Strategy

A research strategy defines how a study should be carried out, how the research activities should be set out, and how they should be completed. According to Saunders, Lewis, and Thornhill (2012), a research strategy is a systematic plan that a researcher uses to answer their research questions, to solve the research problem. For a research strategy to be effective, it should contain clear objectives, appropriate research questions as well as accurate and effective data collection methods. An effective research strategy assists a researcher by providing specific data collection methods that can support foundational arguments (Saunders *et al.*, 2012). A research method is a tool used to explore an area of study, collect relevant data for analysis, and draw conclusions based on the analysis (Walliman, 2017).

Literature review, modelling and simulation experiments are the main research methods used for this study. The literature review provides answers to the research questions regarding the strengths and weaknesses of the existing countermeasures to Black Hole attacks as well as which routing protocols are more vulnerable to attacks in MANETs. Simulations were used to model MANETs, using different routing protocols, under Black Hole attacks to determine the effect these attacks have on the performance of MANETs. It should be noted that the non-standardised nature of simulations can make it difficult to determine what should and what should not be part of the simulation. This limitation can be overcome by looking at each scenario of events independently to better simulate it. Another limitation to bear in mind is that the simulated model might not provide adequate information regarding multiple variables; this is because the simulation might not allow

for multiple phenomena to manifest at the same time. To overcome this limitation, multiple simulations were designed and combined to form a joint simulation.

Once the literature reviews and simulations were completed, the set of findings were collated, analysed and a conclusion was drawn based on the results obtained from the simulation of how MANETs perform under Black Hole attacks, using the different routing protocols. Observations relating to the strengths and weaknesses of the current, existing solutions to Black Hole attacks in MANETs required non-empirical research methods to be used and analysed using a qualitative approach.

1.6.2 Research Process

The research was conducted as per the following protocol:

i. **Identification of research problem**

   Identifying a research problem is the most critical step in the research process and should be done first. The research area found to be of most interest relates to MANETs. After reviewing literature related to MANETs, it was decided that analysis into the performance issues facing MANETs needed to be researched further, focusing on MANETs under Black Hole attack.

ii. **Reviewing of existing related literature (theoretical modelling)**

   Once a research problem has been identified, it is important to review related literature to develop a sound background understanding of the research area. Literature based on Black Hole attacks in MANETs has been reviewed for this study, including existing proposed solutions to Black Hole attacks.

iii. **Simulation Parameter Set-up**

   Simulations were developed based on the research problem's requirements and the key findings obtained from the literature review as well as environmental factors.

iv. **Results analysis and Conclusions**

   The results obtained from the simulation need to be analysed to draw accurate conclusions and to report key findings for future work.

Figure 1.1 illustrates the research flow that was followed for this study.

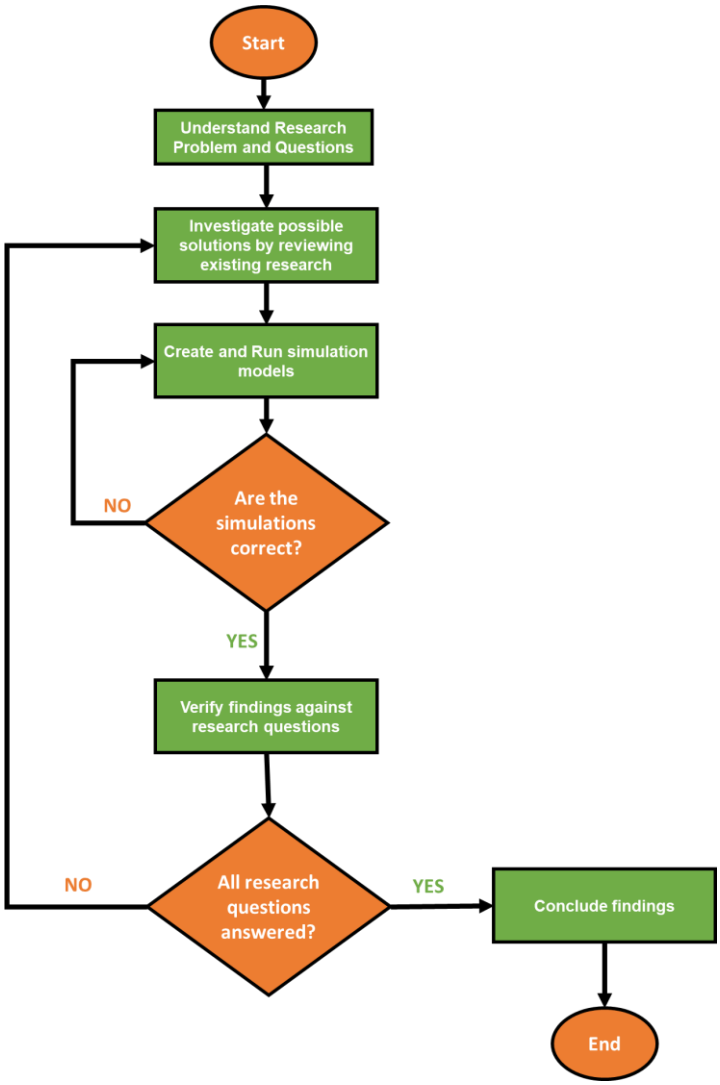

Figure 1.1 – Research Process Flow

1.7 Research Contribution

The following contributions have been identified for this research:

1. The performance of MANETs under Black Hole attack using various routing protocols was investigated using simulations with packet delivery ratio, throughput, and average end-to-end delay as performance metrics. The results of this investigation determined which MANET routing protocol was most vulnerable to Black Hole attacks, thereby creating an opportunity for future researchers to investigate potential solutions to make the vulnerable protocol secure.
2. The research conducted demonstrated the severity of the impact that Black Hole attacks have on MANETs.
3. The review of the proposed solutions provides a high-level understanding of the current approaches available to combat Black Hole attacks.

4. The simulation results provided critical insights into the effects Black Hole attacks have on the performance of a MANET.
5. The simulation results provided key insights around which Mobility Model best simulates the movement patterns of nodes in a MANET.

1.8 Research Scope, Assumptions and Limitations

The impact and effects Black Hole attacks have on MANETs were studied and analysed using two Reactive Routing Protocols (AODV and DSR) as well as a Proactive Routing Protocol (OLSR). These three protocols were chosen arbitrarily due to their popularity.

Simulations were conducted using NS-2.35 (Network Simulator). The different routing protocols were simulated under regular operations to establish a performance benchmark. The Black Hole attack scenarios were then simulated and compared against these benchmarks. A consistent set of simulation parameters was used and tested across the different routing protocol simulations. The simulations were used to obtain data related to packet delivery ratio, throughput, and average end-to-end delay.

- **Throughput** – is the amount of data successfully transferred or received per second over a communication channel. It is the ratio of data received from the source to the total time spent sending the entire message to the receiver. The data traffic is represented in bits per second (Chauhan, 2015). Throughput can suffer due to low bandwidth, limited energy, change in topology and untrusted communication (Rohal, Dahiya and Dahiya, 2013).
- **Average End-to-End Delay** – is the average time it takes for a packet to travel from the source node to the destination node. Delays can occur throughout the transmission process from the source node to intermediate nodes to the destination node. The average end-to-end delay can be calculated by summing the times taken by all received packets divided by their total numbers (Chauhan, 2015).
- **Packet Delivery Ratio** – is the ratio of the successful data packets received at the destination node over the number of data packets generated from the source node. It measures the protocol's reliability in action (Rohal *et al.*, 2013).

This study assumed that Black Hole nodes act independently without coordinating with other nodes to execute an attack. Therefore, only a single malicious node Black Hole attack were considered, with multiple Black Hole attacks falling out of scope. Hybrid routing protocols also fall outside the scope of this study. However, a high-level understanding is provided to enhance the body of knowledge related to MANETs.

1.9 Organisation of the Dissertation

Chapter 2 provides the background research of Mobile Ad-hoc Networks (MANETs). A literature review highlighting what MANETs are, the key features of MANETs, the real-world application of MANETs, and the classifications of the different MANET routing protocols is provided.

Chapter 3 discusses the various vulnerabilities in MANETs, security parameters, and the security services available to protect MANETs against exploitation of these vulnerabilities. Finally, the classification of various security attacks occurring in MANETs is provided and briefly discussed, along with relevant examples.

Chapter 4 presents an analysis of Black Hole attacks in MANETs. This chapter describes the different Black Hole attacks in networks using AODV, DSR, or OLSR protocols. This chapter explains what Black Hole attacks are and how they compromise the security and functions of MANETs. Finally, the chapter looks at solutions and techniques previously proposed to reduce the impact of Black Hole attacks.

Chapter 5 summarises the related works to identify any shortcomings or research gaps that this study will potentially address.

Chapter 6 discusses how the simulations were conducted and an analysis of the results obtained from the simulations. Details of the modifications made to include Black Hole nodes and the modifications applied to implement OLSR in NS2 have also been provided. A review of existing mobility models is provided in this chapter to determine which mobility model is best suited for MANET type simulations. The tools used to conduct the network simulations and the performance metrics used in evaluating the simulation results were highlighted in this chapter. Finally, a demonstration of what happens within NS2 while a simulation is being conducted is shown.

Chapter 7 provides an overview of the performance metrics used to evaluate the routing protocols and describes how the results were retrieved from the NS2 trace files. Those results are then analysed using the chosen performance metrics and presented using graphs.

Chapter 8 concludes the study with the final results of the simulations presented along with observations and conclusions based on the results given. Recommendations for future work relating to this study are also provided.

1.10 Summary

This chapter presented the need and motivation to conduct this study. The problem statement was explained to provide the scope of this study. The research questions that need to be answered for this study to be successful were also presented along with the research objectives. The next chapter provides background information on MANETs.

Chapter 2 – Mobile Ad-hoc Networks

2.1 Introduction

This chapter provides information and literature focused on MANETs. An overview is provided highlighting what MANETs are, the key features of MANETs, the real-world application of MANETs, and the classifications of the different MANET routing protocols.

2.2 Related Background

Raza *et al.* (2016) describes a MANET as a temporary, dynamic wireless network formed by a group of self-organising mobile devices, such as laptops, cell phones and tablets, without the need for any centralised network management or fixed network communication infrastructure. Nodes in a MANET need to cooperate and communicate to compensate for the lack of a centralised network management authority and to implement standard networking functionality (Aluvala *et al.*, 2016). Nodes within transmission range communicate by forwarding messages directly to each other. In contrast, nodes not within transmission range depend on intermediary nodes to facilitate communication using either Proactive, Reactive or Hybrid routing protocols. All nodes participating in the communication automatically create a wireless network known as a MANET (directly or via intermediary nodes), as illustrated in Figure 2.1.

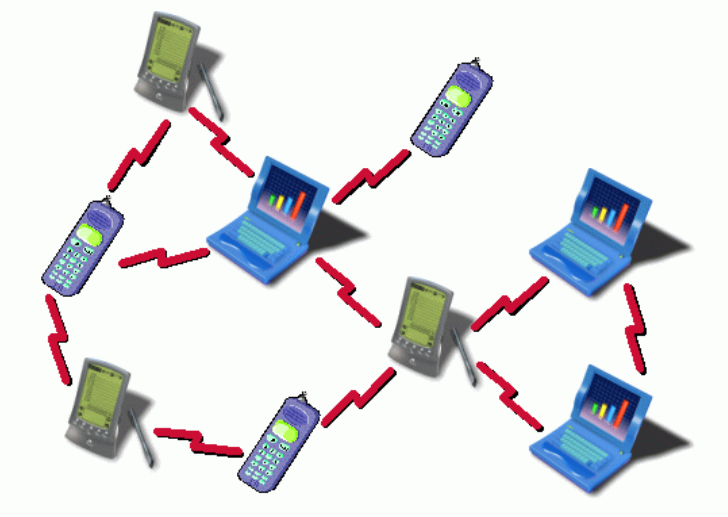

Figure 2.1 – Mobile Ad-hoc Network (Kaushik & Dureja, 2013)

A node that is new to the network topology is required to first discover the MANET before any form of communication between itself and other nodes in the network can occur. Route discovery occurs when a node joins the MANET, announces its presence to the rest of the network, and waits for broadcast announcements from its neighbouring nodes (Boulaiche, 2020). By doing this, each node learns about the other nodes in its vicinity

and the routes needed to reach them. MANETs reconstruct their network topology and routing table information each time a node joins or leaves the network (Raza *et al*., 2016). Routing protocols decide which route to use when packets are sent between source and destination nodes during data transmission.

2.3 Features of Mobile Ad-hoc Networks

Typical Mobile Ad-hoc Networks have the following features:

2.3.1 Energy and Power Supply Constraints

All nodes in a MANET rely on a battery or some limited external energy source to keep operational. As such, these nodes have a limited amount of energy available at any given time, resulting in a node becoming unavailable for communication once its power is depleted (Bhalia, 2015). Nodes need to ensure their energy reserves are shared optimally between the various node networking processes, including data transmission, processing, and routing packets to their destination. When an intermediary node receives a data packet and then loses power before it can relay that data to the next node, the likelihood of packet delivery delays and data loss increases, causing the MANET to become unstable (Thangaraj *et al.*, 2019).

2.3.2 Limited Physical Security

Nodes in a MANET are often small hand-held mobile devices that can easily be lost or stolen which is of significant concern in sensitive type networks, as compromised nodes can be used to perform attacks from “within” the MANET. MANETS are more prone to physical security threats than a fixed infrastructure network. For an adversary node to attack a traditional wired network, it needs to find a way to enter the network before physically performing any malicious activities. In a MANET, an adversary node can communicate with nodes belonging to the MANET within its transmission range and become part of the network without direct physical access to the actual network. Furthermore, MANETs do not have any shared defence mechanisms; therefore, each node must be equipped to defend itself against threats or attacks (Laxman, 2014).

2.3.3 Lack of Centralised Network Management Authority

There is no mechanism to centralise network operations control, as such control is distributed amongst all nodes in a MANET. The lack of a central network management authority, such as a server, monitoring the network's operations makes it difficult to detect any attacks or malicious behaviour that might occur. Without a central management authority governing the network's operations, nodes need to work together and communicate to implement standard networking functions, such as security and routing protocols (Aarti & Tyagi, 2013). Network security relies on all nodes adopting a

cooperative security policy. The lack of a central network management authority makes it difficult to establish trust amongst nodes, as decision-making is often decentralised and might result in conflicting views (Laxman, 2014).

2.3.4 Dynamic Topology

Nodes in a MANET are mobile and constantly moving from one position to another. Each time a node moves in or out of transmission range from other nodes, the routing information changes and must be updated. As a result, tracking a specific node in a large-scale MANET is a complicated undertaking, as each node can be a fast-moving target (Raza *et al*., 2016). The dynamic nature of MANETs will result in multi-hop communication, randomly changing topologies, and the creation of unpredictable bidirectional transmission links (Thangaraj *et al.*, 2019).

2.3.5 Fixed Infrastructure Not Necessary

MANETs form spontaneously without prior knowledge of the physical location and networking environment. The lack of infrastructure makes it suitable for a variety of applications where traditional networks may fall short. In this kind of network, all nodes or devices are mobile, and all networking functionality, including routing, security, and network management, are performed by the nodes (Laxman, 2014).

2.3.6 Multi-hop Environment

MANETs contain nodes that can act as hosts and routers, allowing each node to transfer data packets through multi-hop routes to get the data to its destination (Raza *et al*., 2016). The exploitation of the inherent trust in MANET routing protocols often starts with multi-hop data transmissions being compromised as the only way to disseminate data in a MANET is to use other nodes in the MANET to act as a data transmission medium. Therefore, securing the multi-hop data transmission process is critical to ensure the success of a MANET routing protocol.

2.3.7 Bandwidth Optimisation

MANETs have a fixed range of bandwidth that can be utilised by all the nodes accessing the network; as such, nodes are limited and restricted by the bandwidth they are allowed to use. The available bandwidth of a MANET is much lower than a traditional wired network. Congestion problems arise when network applications require more available bandwidth or when new nodes join the network. Nodes need to use the same network links for control messages and data transmission, resulting in contention for the use of available links (Bhalia, 2015). Routing protocols need to ensure efficient management and allocation of bandwidth for all routing related tasks, including route discovery, routing updating, and the actual routing of data packets between nodes in a MANET.

2.3.8 Shared Physical Medium

Wireless communications are accessible to anyone with the appropriate equipment and adequate resources, making it difficult to restrict access to a specific channel. An adversary can easily eavesdrop on data transmissions and manipulate what is being sent without any hassle. The balance between securing communication and allowing the MANET to be easily accessible is an essential but difficult task (Aarti & Tyagi, 2013).

2.3.9 Scalability

Unlike traditional wired networks, which are built with predefined scales and cater for scalability as needed, the size and scale of a MANET are often unknown and ever-changing due to its dynamic nature. Being able to predict the number of nodes that will be part of a MANET in the future is an impossible and challenging task; as a result, routing protocols and all other network-related services need to be scalable, allowing the MANET to grow or shrink as needed (Thangaraj *et al.*, 2019).

2.3.10 Heterogeneity in Node Capabilities

MANETs can be formed by various types of nodes that are heterogeneous. A MANET can contain various device combinations, including laptops, tablets, smartphones, smart wireless sensors, and other mobile devices with wireless networking capabilities as nodes. Each node in a MANET can have one or more radio interfaces with varying transmitting and receiving capabilities, operating on different frequency bands. This variation can result in asymmetric links being created. Each node may also have different processing capabilities causing speed variations when data is processed or transmitted (Ahmed & Khalifa, 2017).

MANETs are more susceptible to malicious attacks than traditional wired networks due to their features (Raza *et al*., 2016). MANETs are far more vulnerable than traditional wired networks as it is far more difficult to enforce security in MANETs. These vulnerabilities can be exploited and cause severe damage if an attacker succeeds in executing the malicious attack (Boulaiche, 2020). Therefore, careful attention needs to be given to these issues to prevent them from occurring or dealing with them should they occur. Security and vulnerability issues in MANETs will be further explained in Chapter 3.

2.4 Real-World Applications of Mobile Ad-hoc Networks

MANETs can be used in just about any networking scenario. Improvements in wireless communication technology and the increase in popularity of mobile devices have resulted in MANETs becoming a popular deployment in areas where temporary network connectivity is required and in areas where fixed network infrastructure cannot be easily implemented (Raza *et al*., 2016).

2.4.1 Tactical and Military Networks

The use of MANETs in a tactical environment is particularly appealing due to its infrastructure-less and self-organising nature. MANETs can be used to create autonomous battlefields devoid of human personnel in the frontline and allow for intelligence gathering and warfare to be done more effectively and efficiently without risking any lives (Raza *et al*., 2016). Furthermore, MANETs allow for information to be shared amongst soldiers, military vehicles, trusted personnel, and tactical team information headquarters, as depicted in Figure 2.2, over secure, reliable communication networks and channels (Ramamoorthy & Devi, 2013). In contrast, traditional networks in a tactical environment can cause delays in setup and be a point of vulnerability should the physical medium be attacked.

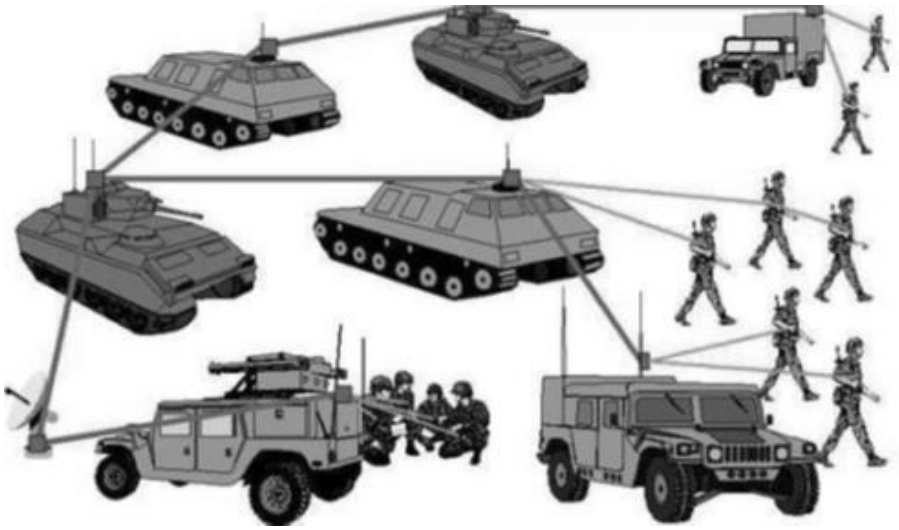

Figure 2.2 – MANETs on the Battlefield (Ramamoorthy & Devi, 2013)

2.4.2 Vehicular Networks (VANETs)

Modern-day vehicles are fitted with short-range wireless interfaces, which enable them to communicate with other vehicles to obtain information for coordination and to interact with fixed roadside infrastructure to obtain information about road conditions, traffic congestion or accident warnings (Ahmed & Khalifa, 2017). Figure 2.3 depicts the relay of information from various vehicles in a VANET to alert emergency services and each other of any incidents on the road and traffic conditions.

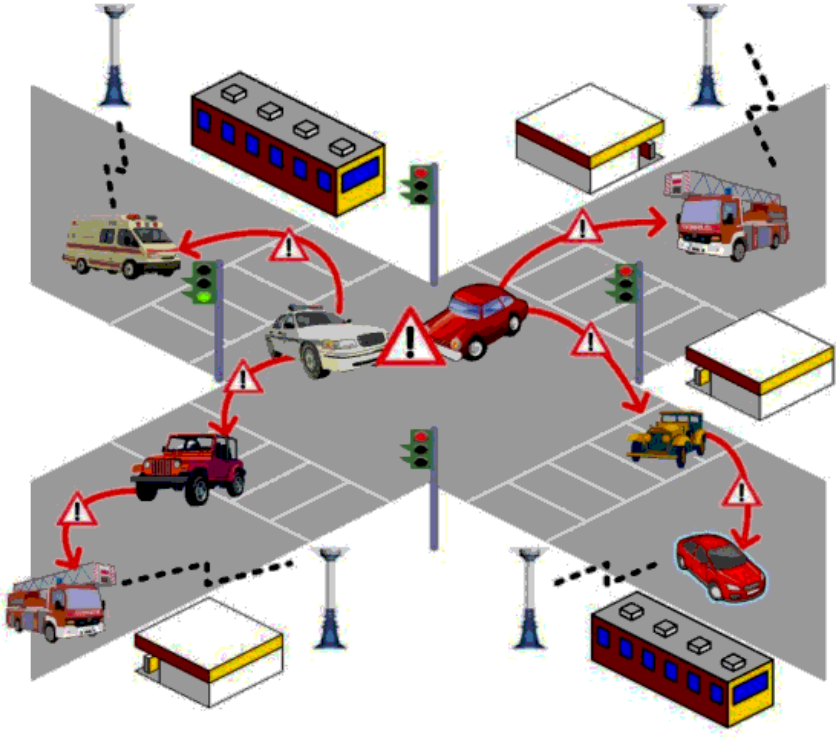

Figure 2.3 – Example of a VANET (Defrawy, 2010)

2.4.3 Wireless Sensor Networks (WSN)

Advances in hardware and wireless network technologies allow for the creation of low-cost, low-power, multifunctional miniature sensor devices that can collaborate among themselves wirelessly, thereby establishing a sensory network. These sensor nodes are usually embedded in buildings, bridges, streets, animals, or mountains to monitor events and changes in the sensory environment. Sensor Networks can collect real-time data to automate everyday functions, monitor and measure variables, such as a change in pressure or temperature, and track the positions and movement of objects and animals (Kanakaris, Ndzi & Ovaliadis, 2012).

2.4.4 Commercial-Civilian Environments

The need for communication networks between individuals and business or government organisations is constantly growing and can be seen almost everywhere we go. MANETs can facilitate community networks in areas were setting up fixed infrastructure is not viable due to financial and geographical considerations at a fraction of the cost of a traditional wireless network. MANET implementations have also made e-commerce widely available, allowing electronic payments to be made anywhere and anytime, with minimal equipment (Ahmed & Khalifa, 2017).

2.4.5 Mobile and Video Conferencing

Mobile devices, such as laptops, tablets, and cellular phones, have become essential for people in meetings, conferences, classrooms, and everyday life. A MANET can assist in

establishing a temporary network allowing and enabling users to collaborate, share documents, or exchange ideas in environments where no network infrastructure is available (Raza *et al*., 2016).

2.4.6 Emergency Services and Disaster Relief

MANETs can be quickly deployed in emergencies where there is a need for a short-term network and in cases where network infrastructure has been severely damaged or destroyed (Raza *et al*., 2016). This could be due to any natural disaster, terrorist attack, rioting, or unforeseen circumstances that damage communication channels.

2.4.7 Internet of Things (IoT)

Everyday life objects fitted with micro-controllers and transceivers can connect to a MANET via appropriate communication protocols, enabling communication with other devices and users over the internet (Ahmed & Khalifa, 2017).

2.5 Mobile Ad-hoc Networks Routing Protocols

Routing allows data to be forwarded correctly from one node in a network to another node that is not within its transmission range. Routing comprises three distinct phases, route discovery, data forwarding, and route maintenance (Boulaiche, 2020).

The route discovery phase aims for all nodes in a network to discover their neighbouring nodes and construct the necessary routing tables. These routing tables can be constructed based on key metrics, such as minimum hop, minimum transmission cost, energy consumption, overhead generated, and end-to-end transmission delay. Routing tables allow nodes access to a suitable, maintained path for efficient data packet forwarding. Should any routing failures occur, the node detecting the failure will propagate an update packet through the network to notify other nodes of the failure. Consequently, each node receiving the failure notification updates its routing table (Boulaiche, 2020).

MANET routing protocols establish an optimal path, one with the least hops, from the source node to the destination node. Packets need to be delivered timeously; therefore, minimum overhead and minimum bandwidth are crucial to the success of a routing protocol (Raza *et al*., 2016). MANET routing protocols are designed to function over a wide range as nodes exist across different locations, often far apart from each other, and in different networking contexts, ranging from small ad-hoc groups to more extensive, more complex mobile multi-hop networks. MANETs routing protocols can be categorised into Reactive, Proactive and Hybrid protocols. Their differences are based on how nodes

create and sustain communication paths within the MANET. Figure 2.4 illustrates the different types of MANET Routing Protocols.

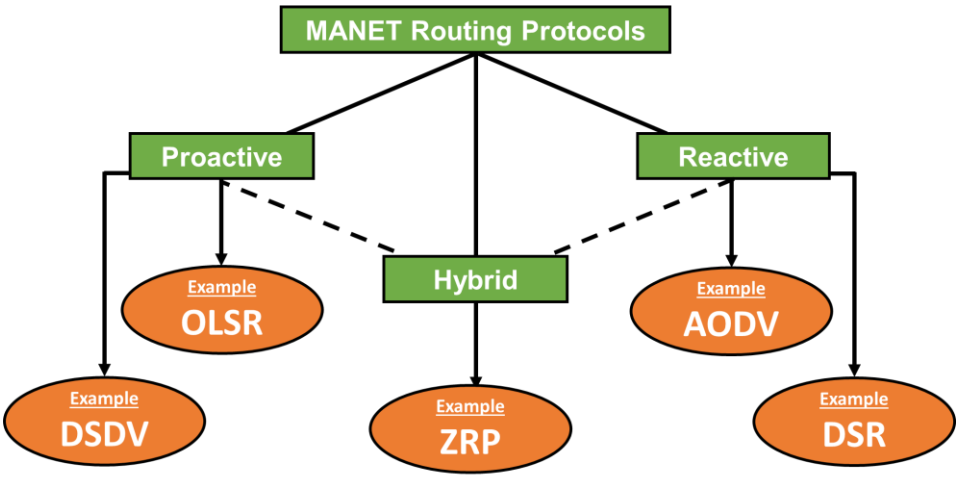

Figure 2.4 – MANET Routing Protocols

2.5.1 Reactive Protocols

Reactive routing protocols, such as Ad-hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), establish routes to destination nodes only when the source node does not have a valid (active) route available for data transmission to occur via the Route Discovery process (Shivahare & Shivahare, 2012). This means that the sender node will only search for routing paths when needed; the route discovery process must be initiated when a sender node wishes to communicate with a receiver node. Reactive routing protocols have a much lower control overhead as routes are only created when required; however, route discovery can cause the MANET to suffer long delays (Boulaiche, 2020).

2.5.2 Proactive Protocols

Proactive routing protocols, such as Destination-Sequenced Distance-Vector Routing Protocol (DSDV) and Optimised Link State Routing Protocol (OLSR), function by ensuring updated records of network routes are stored. Each node in the network has a local routing table to determine how to establish a connection with other nodes in the network (Kaur & Kumar, 2012). Nodes exchange topology information to maintain a consistent network view in their local routing tables. Whenever a node wishes to send a message, it can search its local routing table for a path to the destination node without having to wait for route discovery, thereby reducing delays. This exchange of information among nodes results in a high control overhead (Ballav, 2016).

2.5.3 Hybrid Protocols

Hybrid routing protocols, such as Zone Routing Protocol (ZRP), use proactive routing protocols to obtain the initial network topology and other unknown routing information.

Once the initial network topology is obtained, the hybrid protocol uses the reactive routing protocols mechanisms to maintain the routing information when any changes occur in the network topology (Walikar & Biradar, 2017). Most of the current hybrid routing protocols are designed or structured by means of a hierarchical or layered network model.

2.6 Popular Mobile Ad-hoc Network Routing Protocols

This section describes the operations and mechanisms of popular examples of MANET routing protocols. AODV, DSR and OLSR will be discussed in Section 2.6.1, 2.6.2 and 2.6.3, respectively, as the research is focused on the performance of these protocols. Other popular routing protocol examples will be described briefly in Section 2.6.4 and 2.6.5, respectively.

2.6.1 Ad-hoc On-demand Distance Vector (AODV)

The Ad-hoc On-demand Distance Vector (AODV) is a reactive routing protocol that uses traditional routing tables containing one entry per destination node and the most recently used sequence number. Sequence numbers are used to determine how recent a route is in relation to other routes. A key feature of AODV is that when a routing entry has not been used recently, that entry expires (Gurjar & Dande, 2013). The use of routing tables ensures the routing information is up to date, preventing routing loops. Nodes that are not part of a selected route path do not maintain routing information. This is because routing messages sent to intermediary nodes do not contain information about the whole route path but instead contain information about the source and destination concerning itself. Routing messages do not increase in size (Dwivedi & Gupta, 2016).

AODV routes are built using a Route Request (RREQ) (Arya, Chaurasia & Gupta, 2015). When a source node needs to communicate packets to a destination node for which no route exists or no recent or fresh route exists, the source node broadcasts an RREQ to its neighbouring nodes across the MANET. The RREQ contains information on the source node's Internet Protocol (IP) address, current sequence number, the Broadcast ID, and the latest sequence number that the source node is aware of (Arya *et al.*, 2015). Each node that receives the broadcast updates its information about the source node and then sets up a route back towards the source node; this will only be done if a recent route does not exist. All nodes that receive this request will only send a Route Reply (RREP) message if it is either the intended destination node or has a route to the destination with a sequence number greater than or equal to the sequence number contained in the RREQ. If an RREP needs to be sent, it is unicast back to the source node, the node from which the RREQ originated (Gurjar & Dande, 2013). All nodes keep

a record of the broadcast IDs and source node IP addresses that it has processed. If a node receives an RREQ that has been processed, the RREQ will not be further processed, and the RREQ will be discarded at that node. As the RREP is broadcasted to the source node, intermediary nodes create forward routes to the destination. The source node can forward data packets to the respective destination nodes when the RREP is received (Dwivedi & Gupta, 2016). If a source node receives an RREP containing a route with a greater sequence number or an RREP with the same sequence number, but with a smaller hop count, the routing information may be updated for that destination node and the optimised route will be used. A route will be maintained for as long as it remains active. If a break in the network occurs at any point, a Route Error message (RERR) is sent to notify the other nodes of the breakage, and if an active route is broken while in use, the node upstream of the break will notify the source node of the breakage (Arya *et al.*, 2015). If the source node wishes to continue with the communication, a route discovery must be initiated to find an alternative route to the destination node (Dwivedi & Gupta, 2016).

In Figure 2.5, node *R* wishes to establish communication with node *W*, for which there exists no direct route. An RREQ is broadcast to all of *R*'s neighbouring nodes across the MANET. Once *W* receives the request, it sends a reply (RREP) message to *R* using its neighbouring nodes *T* and *U*. Then the reply is propagated using neighbouring nodes of *T* and *U* until it finally goes back to *R*. Once node *R* receives the first RREP, in this case *via W-T-R*, communication between *R* and *W* can begin.

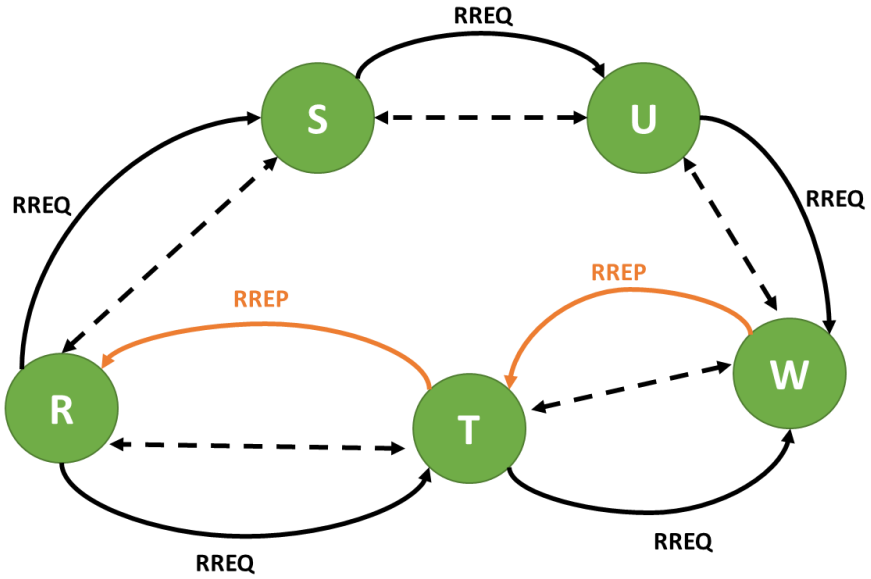

Figure 2.5 – AODV Route Establishment

2.6.2 Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a simple and efficient reactive routing protocol designed specifically for multi-hop MANETs. DSR allows the network to be wholly self-organised and self-configured, without the need for any existing network infrastructure or administration (Liu & Shang, 2015). DSR comprises a route discovery and route maintenance mechanism that allow nodes to discover and maintain routes in the MANET (Kumar, 2012). Whenever a node needs to transmit data packets, it checks the route cache for an available route to the destination. If an active route does not exist, the route discovery process will be launched by broadcasting the RREQ packet, which contains the address of the destination node, the address of the source node and a unique identification number.

When an intermediate node receives the RREQ message with no path to the destination, it alters the route record by adding its address and then rebroadcasts the packet to its neighbouring nodes. A receiving node only processes the RREQ if it has never seen the request before, which helps to reduce the number of RREQs processed and reduce delays (Kumar, 2012). An RREP packet is formed and transmitted to the source node when the RREQ message reaches either the destination node or an intermediate node with a new path to the destination node. After receiving the RREP packet, the source node instantly begins broadcasting packets to the destination node (Mayank & Gupta, 2015).

In Figure 2.6, node *1* wishes to establish communication with node *8*, for which there exists no direct route. A route request (RREQ) is broadcast to node *1*'s neighbouring nodes across the MANET.

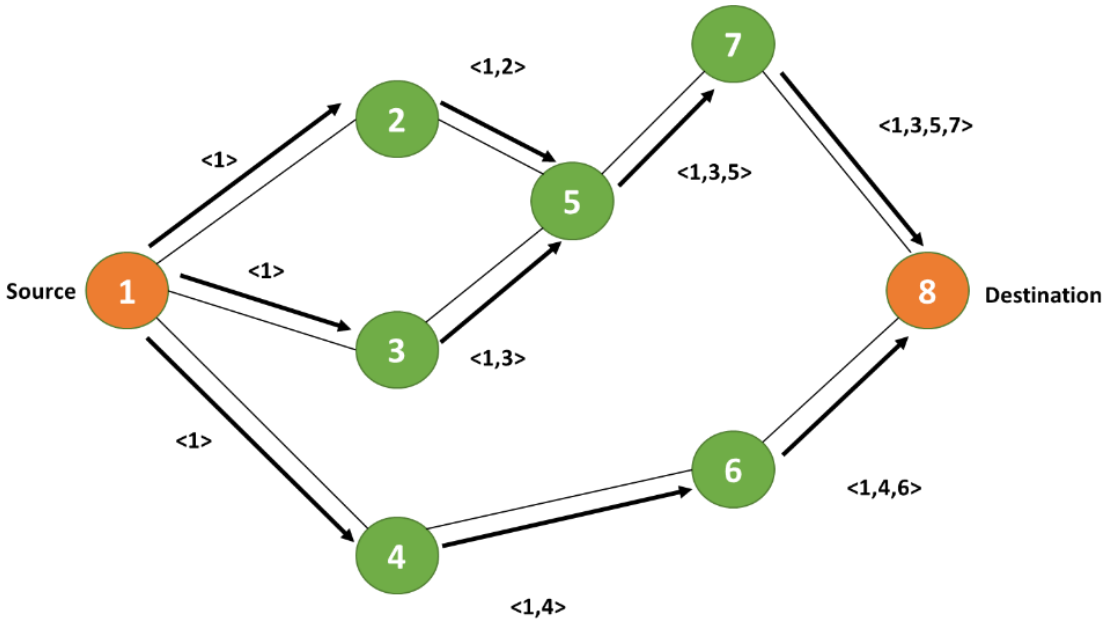

Figure 2.6 – DSR Route Discovery

Once node *8* receives the request, it sends a reply (RREP) message to node *1* using the shortest path (made up of nodes *8-6-4-1*). The reply is then propagated using this path (nodes *8-6-4-1*) until it finally returns to node *1,* shown in Figure 2.7. Once node *1* receives the RREP packet, transmission can begin between nodes *1* and *8*.

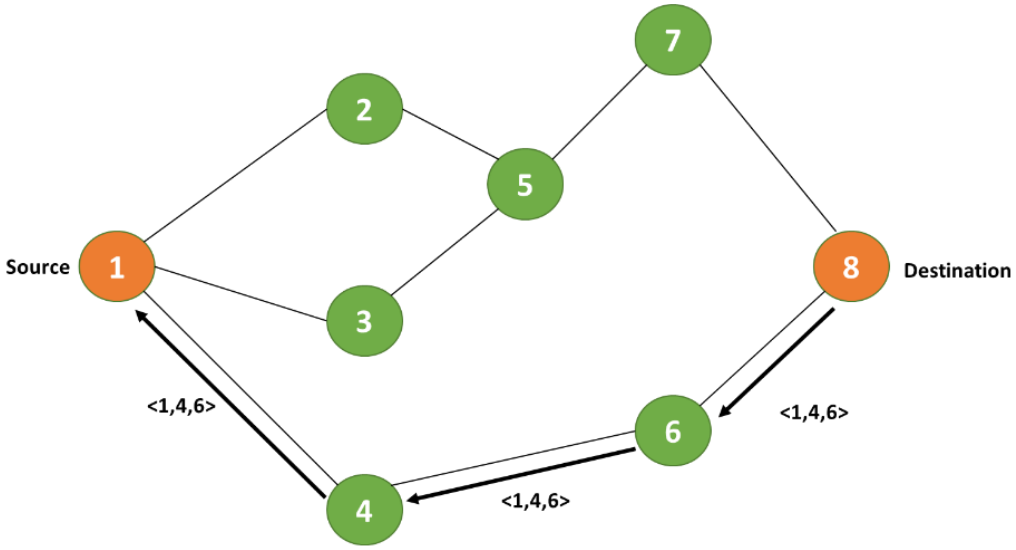

Figure 2.7 – DSR Route Reply Propagation

This protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets. All aspects of this protocol operate entirely on-demand, thereby allowing the routing packet overhead of DSR to scale automatically to only what is needed to react to changes in the routes currently in use. The DSR protocol is designed mainly for MANETs containing approximately two hundred nodes and works well even with very high mobility rates (Kaur & Kumar, 2012).

2.6.3 Optimised Link State Routing (OLSR)

The Optimised Link State Routing (OLSR) protocol is a proactive routing protocol based on the link-state algorithm, implemented by a table-driven approach (Kaur & Kumar, 2012). The key benefit of using this protocol is that a route is immediately accessible from the standard routing table, eliminating delays caused by route discovery. Each node always maintains possible routes to all other nodes within the MANET (Kaur, Bala & Sahni, 2015). OLSR minimises control traffic overheads by using select neighbouring nodes to retransmit control messages, called Multi-Point Relays (MPR). The nodes not in the MPR still receive and process broadcast packets but do not retransmit them. This technique significantly reduces the number of retransmissions required to send messages to all nodes in the network (Salehi & Samavati, 2012).

In Figure 2.8, node *A* is the source node. Node A has five neighbouring nodes, nodes *B, C, D, E,* and *F*. However, only two nodes have been selected as multipoint relays, nodes *C* and *E*; as such, only these nodes can retransmit control messages.

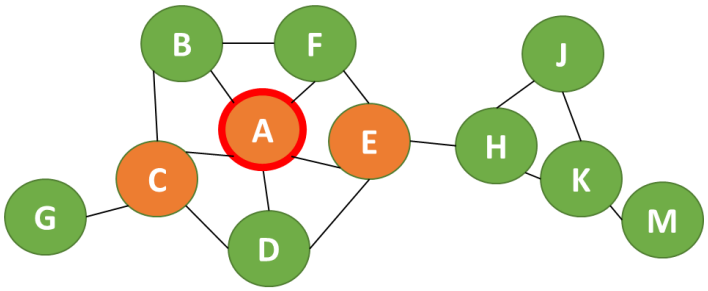

Figure 2.8 – OLSR Multi-Point Relays

OLSR control messages can be categorised into two types, i.e., HELLO and Topology Control (TC) messages. HELLO messages are sent by all nodes to their neighbours to get to know them and find out their link statuses through the responses received. TC messages are broadcast packets that contain information about the one-hop neighbours of nodes (Kaur *et al.*, 2015).

2.6.4 Destination-Sequenced Distance-Vector Routing (DSDV)

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven proactive routing protocol for MANETs, based on the improved version of the classical Bellman-Ford routing algorithm to calculate the shortest route between nodes (Naaz, 2014).

In DSDV, nodes maintain their own routing tables containing all possible destinations within the MANET, the number of hops required to get to each destination and a sequence number. DSDV uses periodic as well as triggered updates to maintain routing table consistency (Ballav, 2016). The periodic information sent by a node contains the sequence number, the destination address, and the number of hops to the destination node. When a node detects a network topology change, an update packet is sent to its neighbouring nodes, alerting them of the change. Consequently, the neighbouring nodes will update their routing tables; if the new address has a higher sequence number, the node takes the higher sequence number route and discards the old one. If the incoming sequence number matches that of an existing route, the route with the lowest cost is selected. This process is repeated until all nodes have been updated (Naaz, 2014).

As the total number of nodes increases, the packet overhead of DSDV also increases. Therefore, DSDV is suitable for small networks as larger networks will increase packet overheads, making the network unstable to the point that update packets might not reach nodes on time.

In Figure 2.9, the routing table for node *B* is shown. Node *B* has neighbour nodes *A, C, D* and *H*. The dashed lines show no communication links exist between the corresponding node pair; as such, node *B* does not have any information about node *H*.

Nodes in DSDV only store one route per source-destination pair in their routing tables as DSDV does not support multi-path routing.

Routing Table for Node B			
Destination	Next Hop	Metrics (No. of hops)	Destination Sequence No.
A	A	1	123
B	0	0	516
C	C	1	212
D	D	1	168
E	D	2	372
H	A	INFINITY	432

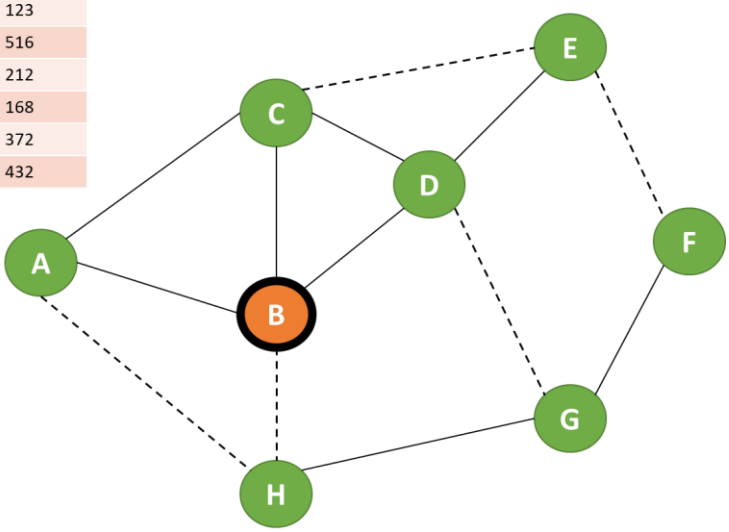

Figure 2.9 – DSDV Routing Table

2.6.5 Zone Routing Protocol (ZRP)

Zone Routing Protocol (ZRP) is a hybrid routing protocol that combines the benefits of both the reactive and proactive routing protocols into a joint protocol to overcome their disadvantages (Kumar, 2012). ZRP combines the benefits of proactive route discovery within a node's local neighbourhood and uses a reactive protocol for communication between those neighbourhoods. In a MANET, the assumption can be made that the majority of communication occurs between nodes near to each other. ZRP is a framework for other protocols rather than a separate routing protocol. Detaching a node's local neighbourhood from the entire network's topology enables different methodologies to be applied, which takes advantage of the properties of each approach for a given situation. These local neighbourhoods are referred to as Zones, and each node may be contained within numerous overlapping zones, each of which may be of varying size. A zone's size is not calculated by physical dimension but is determined by a radius of length or number of hops to the outer limits of the zone. The MANET is divided into overlapping variably sized zones, thereby creating several components in the ZRP. When these components are combined, ZRP provides the full routing benefit (Jamwal, Sharma & Chauhan, 2014).

As shown in Figure 2.10, the ZPR uses the proactive routing protocols to transmit packets within a zone (Intra-zone routing) and reactive protocols to transmit packets from one zone to another (Inter-zone routing).

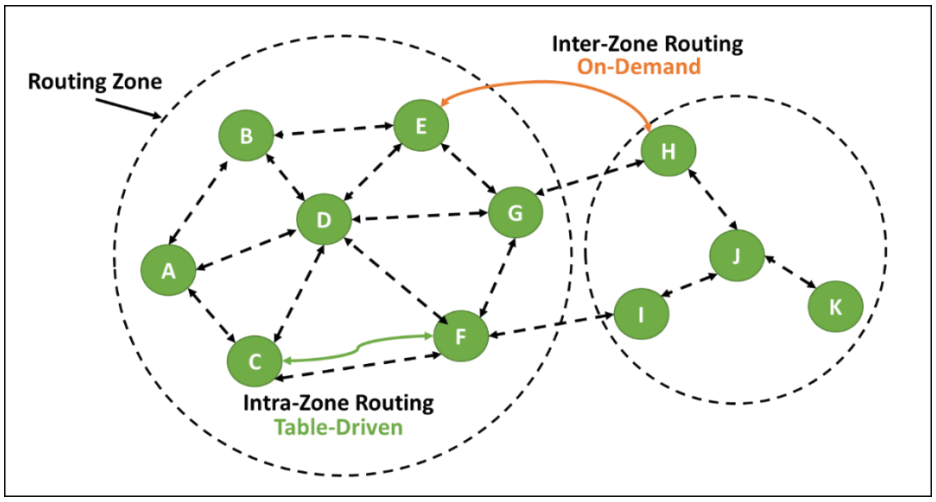

Figure 2.10 – ZPR Intra-zone and Inter-zone

2.7 Summary

This chapter discussed literature based on MANETs, thereby describing what they are and how they work. This chapter provided an overview of the routing protocols used in MANETs by outlining their classifications based on how nodes establish and maintain paths when using the protocol. This chapter also explained the features of a MANET and potential vulnerabilities in this type of network. The next chapter discusses security issues and vulnerabilities in MANETs.

Chapter 3 – Security and Vulnerability issues in MANETs

3.1 Introduction

MANETs are more susceptible to malicious attacks than traditional wired networks due to their inherent features. MANETs are more likely to experience security attacks due to their innate characteristics and vulnerabilities (Sarika *et al.,* 2016). It is vitally important to understand the different attacks that can occur against MANETs, how to prevent them from occurring, and how to deal with them should they occur.

This chapter discusses the various vulnerabilities in MANETs, security parameters, and the security services available to protect MANETs against exploitation of these vulnerabilities. Finally, the classification of various security attacks occurring in MANETs is provided and briefly discussed, along with relevant examples.

3.2 Vulnerabilities in MANETs

MANETs are more susceptible to malicious attacks than the traditional wired network due to their characteristics (Panda, Patra & Hota, 2020). MANET vulnerabilities can be exploited and cause severe damage if an attacker succeeds in executing the malicious attack. Most commonly, these attacks include data tampering, message replay and contamination, DoS attacks and leakage of information, to name just a few. These attacks can make it hard for nodes in the network to resist the attack as the nodes being attacked do not recognise it as an attack (Mohebi & Scott, 2013). Some of these vulnerabilities are discussed in the following subsections.

3.2.1 Lack of Secure Boundaries

In traditional wired networks, it is easy to implement security mechanisms to create a clear line of defence to protect all nodes within the network. Firewalls and gateways in a traditional wired network make it difficult for a malicious adversary to launch any attacks against the network. The adversary must physically bypass all the security mechanisms to gain access to the network.

Nodes in a MANET can move freely within the network and are free to leave and re-join the network at any time. In a MANET, the malicious adversary can communicate with nodes within its transmission range and become part of the network without direct physical access. As such, the physical boundaries of MANETs cannot be defined

precisely, making it easy for an adversary to gain access to the network provided they are within the transmission range of a node within the MANET (Sarika *et al.,* 2016).

3.2.2 Compromised Nodes in the MANET

Nodes in a MANET act and exist independently of each other, allowing them to freely participate in various activities within the network and leave the network without any consequence. This open policy makes it difficult to create strategies that effectively prevent and track all malicious behaviour from occurring. It becomes challenging to trace all the malicious behaviour carried out by a compromised node, as they can change their attack targets frequently and relatively quickly due to the mobility characteristics of nodes (Panda *et al.*, 2020). The risk of attack from inside the MANET is greater than the risk of attack from outside as the compromised nodes are considered legitimate nodes before they are compromised (Mohebi & Scott, 2013).

Figure 3.1 is a basic example of how an insider attack occurs. Sender node *S* transmits data to the intended destination node *R* via an intermediary node *I*. Node *C* joins the network by initially establishing itself as a trusted node. Once node *C* is a trusted part of the network it is now able to overhear the data being sent from node *S* to node *I*. Node *C* can then start interfering with the data packets being sent to node *I*, resulting in compromised and potentially malicious data being transmitted to node *R*.

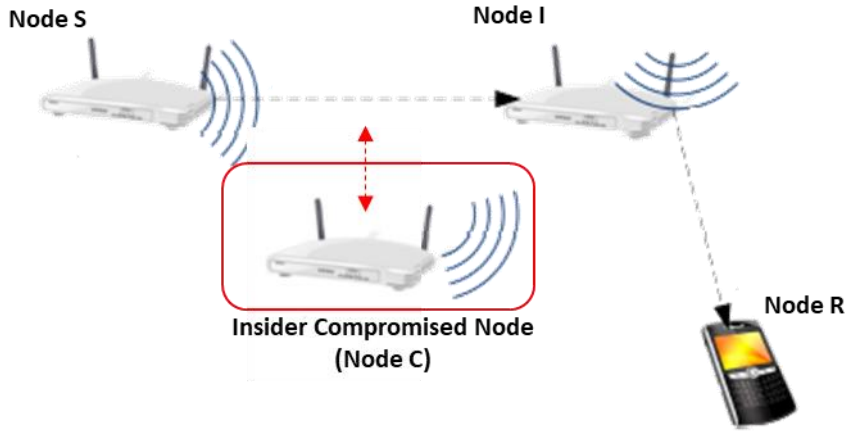

Figure 3.1 – Insider Attack (Lazos & Krunz, 2011)

3.2.3 Decentralised Network Management

Traditional wired networks have unique access control mechanisms to monitor and measure what is happening across the different nodes in the network. These control mechanisms restrict what nodes can and cannot do and which nodes can access the network. The lack of a centralised network management facility in MANETs, such as servers to monitor and control access, may increase the likelihood of attack and exploit vulnerabilities as there is no central control mechanism to ensure all parties abide by security protocols (Aluvala *et al.*, 2016). Without a central management authority

governing the operations of a MANET, nodes need to work together and communicate among themselves to implement standard networking functions, such as security and routing protocols. (Aarti & Tyagi, 2013). This makes it difficult to establish trust amongst nodes as decision-making is often decentralised and might result in a conflicting view; therefore, network security relies on all nodes adopting a cooperative security policy (Laxman, 2014). Detecting attacks in a MANET without a central control mechanism is very difficult since the network traffic is dynamic and ever-changing.

3.2.4 Resource Constraints

The low bandwidth capacity within MANETs makes them more susceptible to attenuation, interference, and signal noise (Aluvala *et al.*, 2016). MANETs have a fixed range of bandwidth that can be utilised by all the nodes accessing the network; as such, nodes are limited and restricted by the bandwidth they are allowed to use. Nodes need to use the same network links for control messages and data transmission, resulting in contention to use the available links (Bhalia, 2015).

MANETs get their energy supply from battery power and other rechargeable means, resulting in them becoming unavailable once a node's energy supply is depleted. As such, an adversary can use malicious means to target specific nodes attempting to deplete its power (Sarika *et al.,* 2016). Nodes need to ensure their energy reserves are shared optimally between the various node networking processes, including data transmission, data processing, and routing packets to their destination. When an intermediary node receives a data packet and then loses power before it can relay that data to the next node, the likelihood of packet delivery delays and data loss increases, causing the MANET to become unstable (Thangaraj *et al.*, 2019).

3.2.5 Cooperativeness

Most MANET routing protocols assume all nodes are non-malicious and cooperative. MANET routing protocols and other ad-hoc networking algorithms rely heavily on the cooperation of all nodes within the MANET. Therefore, if an adversary joins the MANET, it can quickly become an essential routing agent and disrupt the network operations within the MANET (Sarika *et al*., 2016). A malicious node can easily use this vulnerability and perform targeted attacks to break these cooperative algorithms and gain control of the network (Panda *et al.*, 2020).

MANETs are far more vulnerable than traditional wired networks due to difficulties in being able to enforce security. These vulnerabilities can be exploited and cause severe damage if an attacker succeeds in executing them.

3.3 MANET Security Services

In their research, Dorri, Kamel and Kheyrkhah (2015) discuss the importance of implementing security services that protect a network before an attack can occur, making it difficult for malicious nodes to cause harm to the network. Although challenging, when creating a secure MANET environment, the following security services should be implemented.

3.3.1 Availability

The availability service ensures that all authorised nodes have access to data and services within the network (Pooja *et al*., 2018). This service's success relies on the correct data redundancies, physical protection, and backups being used. The dynamic topology and open boundary nature of MANETs can create availability challenges by causing delays. When implementing security and authentication levels, the time needed to process these requests should be as efficient and quick as possible while still providing maximum security and protection. The time to access network services or data is essential, as processing time is one of the security parameters considered when implementing security services (Dorri *et al.*, 2015). Any nodes suspected of malicious behaviour need to be identified quickly and isolated from the network to guarantee the availability and ensure the MANET's survivability (Kauser & Kumar, 2016). A Denial of Service (DoS) attack is an example of an attack on the availability of a MANET. During a DoS attack, a malicious node will send an excessive number of messages to congest the network in the hopes of bringing it down, resulting in network resources being unavailable to other nodes (Kumari & Chugh, 2018).

3.3.2 Access Control or Authorisation

Ensuring only authorised participants are issued credentials that specify an entity's privileges and permissions is a critical security mechanism in a MANET. The access control service also ensures that the correct information is accessed and used correctly by authorised nodes with the corresponding permissions for the accessed data. The access control service uses verified credentials and permissions to ensure access to information is controlled, and nodes are only allowed to access the information they are privileged to (Sarika *et al*., 2016).

3.3.3 Authentication

The purpose of authentication is to ensure that all nodes participating in a MANET are genuine and not impersonators. The authentication service aims to provide reliable communications between nodes using a specific set of qualification criteria, i.e., user credentials, to verify the identity of a node or user (Ahuja & Sugandha, 2017). In wired

networks, a central authority, such as a router, facilitates the verification process. However, there is no central management authority in MANETs, making it challenging to perform authentication at a centralised place. MANETs can overcome this shortcoming by implementing authentication as part of the chosen routing protocol or using built-in access control mechanisms that form part of a node (Pooja *et al*., 2018).

3.3.4 Data Confidentiality

Data confidentiality ensures that private data is only accessible by entities with the authority and permission to access it. Sensitive information must be kept unreadable to unauthorised users or nodes during communication. This can be a considerable challenge as MANET's use an open communication medium, and all nodes within the transmission range can access the data being transmitted (Pooja *et al*., 2018). Eavesdropping is a typical attack against data confidentiality. Eavesdropping occurs when a passive, but malicious node listens in on network traffic and network communication. While this attack does occur in wired networks, it is even easier to execute in a wireless network as the malicious node does not have to physically connect to the network as it only needs to be within transmission range of the network to be able to listen in on the network traffic and network communications. Data confidentiality can be guaranteed by using encryption mechanisms to prevent attacks, like eavesdropping and others of a similar nature, from occurring in a MANET (Kauser & Kumar, 2016).

3.3.5 Integrity

An integrity security service ensures that security-related data cannot be modified whilst being transmitted or stored, and only authorised nodes can create, edit, or delete data packets. This ensures that data will not be altered during transmission, and if the data is altered, then the integrity detection mechanism can address the issue as needed. It is common practice for the integrity service to be implicitly provided by the authentication service (Liu, Yan & Pedrycz, 2018). The purpose of an integrity service is to ensure all messages received at a destination are identical to the message sent from the source. This can be a challenge in MANETs as messages are passed from source to destination using various intermediary nodes. Nodes in a MANET are prone to failure, and messages are transmitted over unstable communication channels.

3.3.6 Non-Repudiation

Non-repudiation ensures that the node sending a message cannot deny sending it. This accountability service assists in determining if a node is misbehaving or not. As such, any node that receives messages containing errors from a malfunctioning node can use that message as proof to alert other nodes about the malicious node, and the malicious nodes cannot deny sending the harmful message. (Sarika *et al*., 2016). This service also

ensures that source and destination nodes can prove the transmission or reception of information (Dorri *et al.*, 2015). In a MANET, non-repudiation can be implemented using digital signatures. A digital signature is created and attached to each message being transmitted, allowing for ownership of the message to be established. The sender node will sign a message using its private key, and all other nodes can identify the message's legitimacy using the sender's public key. This process prevents a sender node from denying that its signature is attached to the message (Chahal & Kharb, 2017). Security services provide a layer of protection against attacks. It is also important to implement additional security mechanisms to detect and eliminate nodes that enter a MANET with malicious intent (Dorri *et al.*, 2015).

3.4 MANET Security Attack Classification

Many characteristics can be used to classify attacks in MANETs. MANET attacks are commonly classified based on the behaviour of the attack (Passive vs Active attacks), the source of the attack (Internal vs External attacks), the number of attackers (Single vs Multiple), and on which layer of the network protocol stack the attack occurs (Sarika *et al*., 2016).

3.4.1 Behaviour of the attack

Passive attacks aim to steal and discard valuable information from a targeted network without causing any physical disruption to the network's operations. Passive attacks are relatively difficult to detect as the attacker does not send any data but rather eavesdrops on the data being sent on the network (Lui *et al*., 2018). Examples of passive attacks are Eavesdropping and Snooping. Whereas active attacks intentionally obstruct the regular operation of a targeted network by destroying or modifying data transmitted within the network (Sarika *et al*., 2016). Examples of active attacks are Denial of Service attacks, Wormhole attacks, and Black Hole attacks.

3.4.2 Source of the attack

External attacks originate from malicious nodes that do not have the authority to participate in any network operations and reside outside the network topology (Sarika *et al*., 2016). These attacks usually cause network congestion, deny access to specific network functions, or disrupt the whole network operations (Gandhewar & Patel, 2012). Examples of external attacks are Denial of Service attacks and Impersonation attacks. Internal attacks are initiated by compromised or misbehaving nodes within a network. External nodes use these nodes to infiltrate a network for malicious purposes. Internal attacks are difficult to detect and cause the most damage (Sarika *et al*., 2016). Examples of internal attacks are Routing attacks, Wormhole attacks, and Eavesdropping.

3.4.3 Number of attackers

Attacks can be launched against a network by a single adversary or multiple adversaries colluding together. Single adversary attacks, such as a Sinkhole attack, can generate a moderate traffic load and have similar abilities and limitations as other nodes in the network. As such, resource constraints make these forms of attacks relatively weak. Once the malicious node's power source is depleted, the attack cannot continue, and the network will return to regular operation. However, if multiple attackers collude to launch attacks, defending the network against them becomes much more challenging (Gandhewar & Patel, 2012). An example of a multi-adversary attack is a Distributed Denial of Service attack.

3.4.4 Attack on Protocol Stack Layer

Attacks can occur across the different layers of the network protocol stack. Each attack aims to take advantage of the constraints, limitations, and features of the layer in which the attack occurs (Lui *et al*., 2018). As such, the attack can be classified based on which layer of the protocol stack it occurs.

Network layer attacks aim to disrupt the routing process and target routing protocols to do this (Dorri *et al.*, 2015). Examples of network layer attacks are Black Hole attacks, Wormhole attacks, and Byzantine attacks.

Transport layer attacks target shortcomings in the communication services used by applications in a network (Dorri *et al.*, 2015). Attacks exploit either connection-oriented transmissions, which is managed by the Transmission Control Protocol (TCP) or message forwarding, which is managed by the User Datagram Protocol (UDP) (Lui *et al*., 2018). Examples of transport layer attacks are Session Hijacking and Flooding attacks.

Application layer attacks target the services that make applications available for users (Dorri *et al.*, 2015). Examples of application-layer attacks are Malicious Code and Repudiation.

The data layer is responsible for the efficient communication of data between machines connected to the network; as such, data layer attacks occur due to the exploitation of vulnerabilities within this communication (Singh, 2018). Examples of data link layer attacks are Traffic Analysis and Selfish Node attacks.

The physical layer is responsible for the transmission and reception of all data in a network; therefore, attacks on the physical layer aim to paralyse a node or the entire network by flooding the network with an excessive amount of traffic to consume the

critical resources of the network (Singh, 2018). Examples of physical layer attacks are Eavesdropping and Denial of Service (DoS) attacks.

3.5 MANET Security Attack Examples

Security can be compromised when the network and its nodes do not have strong countermeasures to deal with attacks. Malicious nodes attempt to expose and exploit the inherent vulnerabilities of a MANET to conduct various attacks to compromise and cripple the network. To better understand these attacks and how they are conducted, some of the common security attacks that occur in MANETs will be described in this section. Figure 3.2 shows a categorised view of the different types of MANET security attacks along with examples.

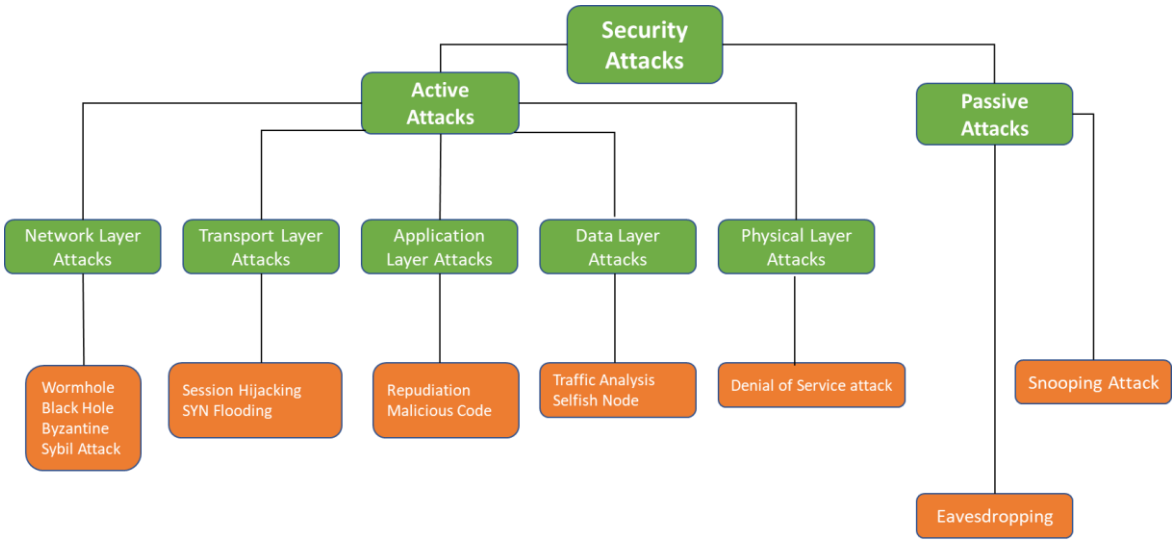

Figure 3.2 – MANET Security Attacks

3.5.1 Black Hole Attack

A Black Hole attack occurs when a malicious node sends a reply message to a source node to fictitiously advertise itself as having the shortest path to the destination node (Gurjar & Dande, 2013). Once the node has placed itself between the communicating nodes, it can do anything with the packets passing through it, resulting in data packet manipulation or data packet loss (Kauser & Kumar, 2016). This attack will be discussed in detail in Chapter 4.

3.5.2 Gray Hole Attack

Gray Hole attacks are performed similarly to Black Hole attacks. However, unlike a Black Hole attack in which the malicious nodes drop all data packets, the malicious nodes in a Gray Hole attack drop data packets selectively and with different probabilities. During the route discovery process, the malicious Gray Hole node will remain trustworthy. Once

trusted routes are established, the Gray Hole node will drop data packets selectively (Saranya & Rajesh, 2018). This attack is more difficult to detect than a Black Hole attack.

A Gray Hole attack can occur in three different ways:

- it may drop data packets coming from a specific node while continuing to forward the data packets from other nodes;
- it may behave maliciously for a set time and then switch to normal behaviour later; or
- as a combination of the above.

In Figure 3.3, malicious node *G* acts as a Gray Hole node. Node *G* drops all data packets that it receives destined for node *4* but still allows data packets to be forwarded to node *2* and node *3*. All other nodes are unaware of this malfunction and continue sending data packets to node *G* with the expectation that node *G* will forward those data packets to node *4*. This results in the creation of a Gray Hole attack.

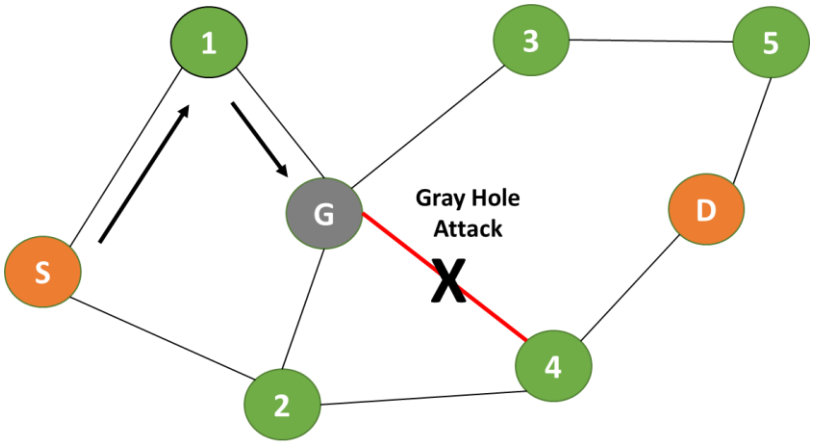

Figure 3.3 – Gray Hole Attack

3.5.3 Byzantine Attack

A Byzantine attack occurs within a MANET by a group of compromised intermediate nodes collaborating to launch their attacks. These attacks can cause the disruption of routing services and degrade the network. Successfully detecting this attack is not easy as the network will appear to be fully functional and operate as expected by other network users (Manohar & Kumar, 2019).

Some Features of Byzantine attack are as follows:

- nodes create loops to send data amongst themselves (within the loop) with no definite end;
- sending data packets through non-optimal routes; and/or
- The specific dropping of packets

Figure 3.4 shows an example of how a Byzantine attack can occur. Source node *S* wants to send data to destination node *D*. The shortest path from node *S* to node *D* is via path *S-2-3-D*. However, nodes *3* and *7* are malicious. Instead of node *3* sending the data packets it receives directly to the destination node *D*, node *3* sends the data packets it receives to node *8*. Node *8,* being non-malicious, then send the data packets to its closest neighbour, node *7*. Malicious node *7* will ignore the optimal route to node *D* via node *5* and instead send the data packets it receives to node *4*. Node *4* will then send the data packets it receives back to node *S*, unintentionally creating a data transmission routing loop. The data packets will continually follow this path (via *S-2-3-8-7-4*), resulting in a Byzantine attack.

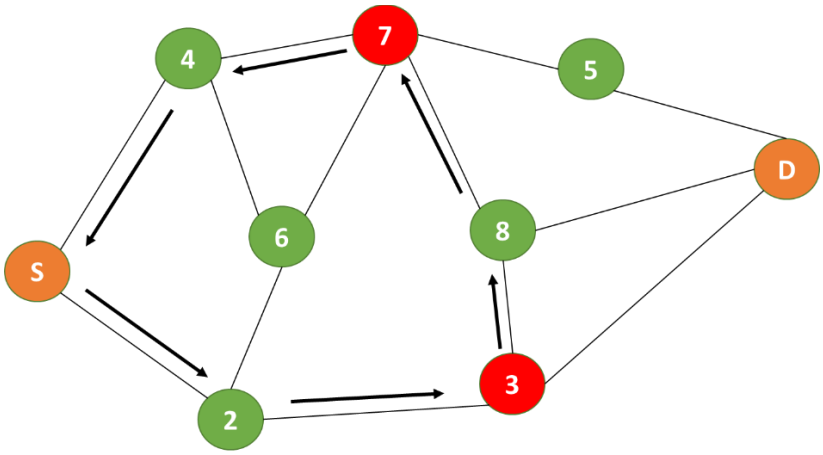

Figure 3.4 – Byzantine Attack

3.5.4 Denial of Service

A Denial of Service (DoS) attack aims to prevent other authorized nodes from accessing network data or services, thereby deteriorating the network's performance and preventing it from delivering expected functions. A malicious node will send an excessive number of messages to congest the network in the hopes of bringing it down, resulting in network resources being unavailable to the other nodes, leading to the creation of a DoS attack (Kumari & Chugh, 2018). A specific node or service may be rendered unreachable as a result of this attack, and network resources, such as bandwidth, will be squandered, increasing packet delay and network congestion (Kauser & Kumar, 2016).

A Jamming attack is a type of DoS attack in which the goal of the jammer is to disrupt legitimate wireless communications. A jammer can accomplish this by either blocking valid traffic sources from transmitting data packets or by preventing legitimate packets from being received (Singh & Gupta, 2017).

Figure 3.5 shows an example of how a jamming device adds dummy packets to legitimate data transmission between a sender and receiver. The receiver will receive a

compromised message consisting of the legitimate message and the dummy data added on to the data transmission by the jamming device.

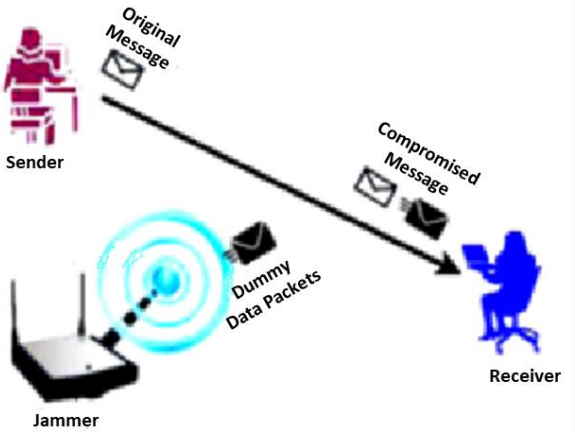

Figure 3.5 – Jamming Attack (Singh & Gupta, 2017)

3.5.5 Impersonation Attack

An impersonation attack occurs when a malicious node joins a network by pretending to be a trustworthy node. Once trust is established, the malicious node sends false and misleading routing information to other nodes in the network (Panda *et al.*, 2020). Sybil attacks are a type of impersonation attack that occurs in MANETs.

A Sybil attack occurs when a malicious node attempts to generate multiple virtual nodes, using the identities of valid nodes to create these fake identities. This confuses the routing process and disrupts the entire network, preventing legitimate communications from taking place.

Figure 3.6 shows multiple Sybil nodes surrounding a valid node to prevent that node from connecting to the legitimate nodes in the MANET. This prevents the sending or receiving of valid information in the network (Aggarwal & Kumar, 2021).

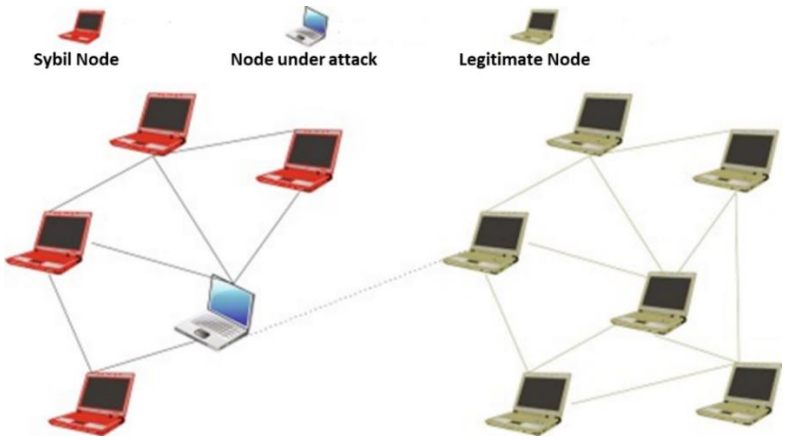

Figure 3.6 – Sybil Attack (Aggarwal & Kumar, 2021)

3.5.6 Wormhole Attack

In a Wormhole attack, a pair of malicious nodes work together to transfer data packets received at one network location over to a different network location using low latency tunnels. To do this, one of the malicious nodes captures the routing packets at a specific location within the MANET and then tunnels those packets to a second malicious node at another location in the MANET, bypassing any intermediate nodes. The tunnel created shares a private fast transmission link between the malicious nodes allowing them to appear as if they are next to each other (or one hop away) in the MANET, thereby making the wormhole invisible. This attack can have severe consequences by disrupting communication services that ensure authenticity and confidentiality (Verma, Sharma & Singh, 2017).

Figure 3.7 depicts a Wormhole created by nodes *1* and *4* using a highspeed private communication tunnel between these nodes, which bypasses the normal routing processes should either node be part of a data transmission route. The other nodes are unaware of this route which might result in routing delays in some routing scenarios.

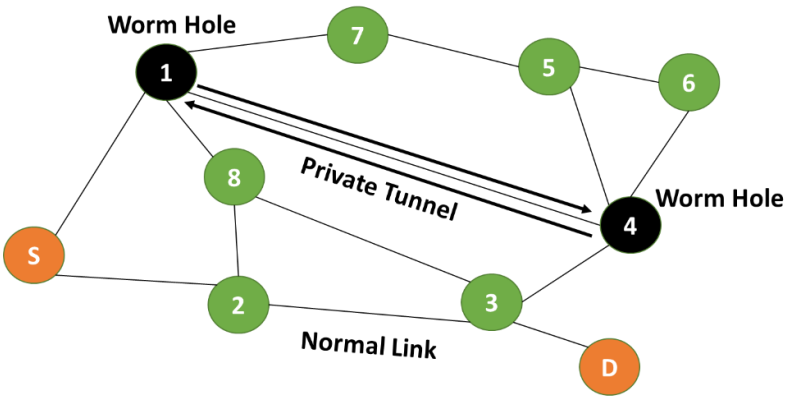

Figure 3.7 – Wormhole Attack

3.5.7 Session Hijacking

During a Session Hijacking attack, a malicious attacker exploits an unprotected session after it is initial setup by spoofing the IP address of a victim node then finding the sequence number expected by the target to launch an array of DoS attacks. The malicious node aims to collect secure data and other sensitive information from the victim nodes (Shabbir *et al.,* 2015).

Figure 3.8 shows a common form of Session Hijacking called a TCP-ACK storm. Malicious node *M* sends acknowledgement and session data to node *A*. Node *A* sends an acknowledgement packet (ACK) to node *B* containing a sequence number that node *B* will not accept. To rectify this, node *B* tries to synchronise the TCP session with node *A* which fails due to the change in session data made by node *M*. Node *B* will continue to attempt resynchronisation with node *A* and fail, causing a TCP-ACK loop to be

established. This ultimately results in creating a TCP- ACK storm causing the system to become unavailable to other nodes.

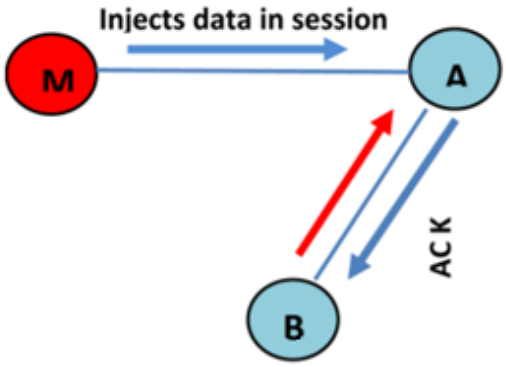

Figure 3.8 – Session Hijacking Attack (Shabbir *et al.,* 2015)

3.5.8 Rushing attacks

During a Rushing attack, the route discovery process is compromised. A rushing attack occurs when a legitimate node broadcasts an RREQ message, and as soon as a malicious node receives this request, it quickly floods a malicious RREQ message throughout the network before the legitimate nodes request can be received, causing the legitimate RREQ message to be discarded. This results in the malicious node being perceived as an intermediate node in all routes discovered by the legitimate requesting node (Panda *et al.*, 2020).

Figure 3.9 shows how a Rushing Attack occurs when source node *S* initiates a route discovery request and malicious node *M* acts quickly to send an RREQ to all the neighbouring nodes of destination node *D* before the arrival of legitimate RREQ from node *S*. Nodes *X* and *Y* receive the compromised RREQ from node *M* faster than the RREQs from nodes *B* and *E* resulting in the legitimate RREQs (from nodes *B* and *E*) being discarded by nodes *X* and *Y*. As such node *S* will only receive unsafe routes that involve malicious node *M* as part of the routing.

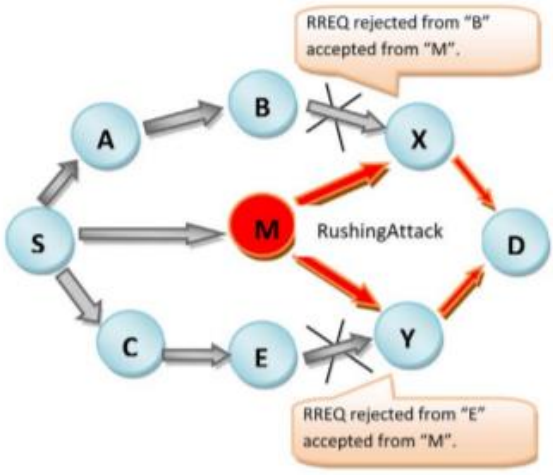

Figure 3.9 – Rushing Attack (Shabbir *et al.,* 2015)

3.5.9 Repudiation Attacks

Attacks against repudiation result in the denial of active participation in all or part of the network communication making it difficult to determine the origin of any malicious activity as no one will accept the responsibility for what is happening. Application layer firewalls and protection mechanisms need to provide security against this type of attack. Spyware detection software is an excellent example of a mechanism that will protect against repudiation attacks (Shabbir *et al.,* 2015).

3.5.10 Traffic Monitoring and Analysis Attacks

Traffic monitoring and analysis attacks are passive attacks in which a malicious node monitors and listens to the communication between nodes within the MANET to perform analysis on the network to determine the location of key nodes and the routing structures. In this type of attack, the malicious node does not compromise the actual data (Shabbir *et al.,* 2015).

3.5.11 Malicious Code Attack

Various types of malicious code attacks, such as viruses, worms, spy-wares, and trojan horse attacks, can be deployed against operating systems and user applications in a MANET, causing the network to slow down or become unavailable. An adversary can use this type of malware to get the information and data they so desire (Archana & Gracy, 2015).

3.5.12 SYN Flooding Attack

To start any TCP communication between a client and a server, a client will send a SYN (synchronisation) request to the server. The server will then acknowledge the client by sending a SYN-ACK, creating a half-open connection. Once the client node receives the SYN-ACK, an acknowledgement (ACK) is sent back to the server from the client, thereby establishing a full TCP connection. This is called a three-way handshake of TCP. A SYN flooding attack is performed when a malicious node exploits the TCP three-way handshake and creates multiple half-opened TCP connections with the victim node. These half-opened connections are never completed and remain open while consuming resources causing memory buffers to become full. When this happens, the server will not accommodate any new requests causing legitimate requests to be denied (Shabbir *et al.,* 2015). SYN flooding is a type of Denial of Service (DoS) attack.

3.5.13 Fabrication Attack

Fabrication attacks occur when a malicious node manipulates the routing table of other nodes by inserting fake route error messages and routing updates. This falsified information is used to establish what is assumed to be valid paths between nodes,

resulting in network resources being wasted, decreasing packet delivery rates, and increasing packet loss (Panda *et al.*, 2020).

3.6 MANET Security Approach Parameters

A security approach should be implemented to eliminate and reduce the likelihood of an attack in a MANET. When determining the viability and applicability of a security approach, the unique nature and characteristics of MANETs require the consideration of key benchmarking metrics, called Security Parameters. Each security approach and all security mechanisms proposed must be aware of these security parameters and should not disregard them; else, the security approach may be deemed inadequate for use in a MANET (Dorri *et al.*, 2015). The security parameters in MANET are as follows:

3.6.1 Network Overhead

The shared wireless media nature of MANETs can result in additional control packets being created, leading to network congestion and packet collisions occurring. The high packet overhead increases the likelihood of packet loss and the need for packets to be retransmitted, which then wastes nodes' energy and network resources (Dorri *et al.*, 2015). Some security approaches modify packet headers to sign and encrypt the data packets being transmitted digitally. If these data packet header modifications are not managed correctly or optimised, then there is the opportunity for data transmission overheads to increase rapidly. As such, the network overhead parameter is used to monitor and measure the number of control packets generated by a security approach and can be used to benchmark the efficiency of a security approach (Kauser & Kumar, 2016).

3.6.2 Computational Resources

All wireless nodes in MANETs have a limited set of computational resources to be shared amongst all data communication and processing (Polverini *et al*., 2018). A security approach needs to process data and determine the nature of the communications as efficiently and effectively as possible using the available resources optimally and as needed. This will ensure the operational overheads of the security approach is kept low and will not result in any prolonged transmission delays.

3.6.3 Processing Time

All security approaches need the ability to detect if nodes are misbehaving and have mechanisms in place to eliminate any malicious nodes. The dynamic topology nature of MANETs makes it highly likely for routes between two different nodes to break due to node mobility (Dorri *et al.*, 2015). Real-time, rapid, predictive analysis of data transmissions will allow a security approach to process the data it receives in a very short

time and determine if the data being transmitted are valid, non-malicious and complete. This will allow the network to function optimally and as efficiently as possible, with only the necessary data transmission being in-flight at any given time with all unnecessary and invalid communications being terminated. A security approach must aim to have a very short processing time to increase MANET flexibility and avoid the need for packet rerouting (Patel & Kamboj, 2017).

3.6.4 Energy Consumption

All wireless nodes in MANETs have limited energy supplies. Managing energy usage efficiently is challenging in MANETs; as such, any energy-intensive activity performed by the network, or nodes in the network, will reduce the life span of the network and the nodes in the network (Kauser & Kumar, 2016). Therefore, all security approaches need to be optimised to ensure that they are as energy efficient as possible.

Security approaches must consider these security parameters in their entirety. However, in some situations, trade-offs between these parameters ensure a certain level of satisfaction for all parties involved, thereby allowing the maximum benefit to be achieved. Security protocols that disregard these security parameters become obsolete and inefficient, resulting in wasted network resources (Dorri *et al.*, 2015).

3.7 Summary

The need for security-related data to be collected and analysed in MANETs becomes crucial in evaluating and measuring MANET's real-time security and giving the network the suitable mechanisms to react accordingly (Liu *et al.*, 2018).

This chapter reviewed the security and vulnerability aspects of MANETs. It firstly addressed and discussed the vulnerability issues and challenges experienced by MANETs, highlighting that MANETs are far more vulnerable than traditional wired networks due to difficulties in enforcing security. These vulnerabilities can be exploited and cause severe damage if an attacker succeeds in executing them. The chapter also explained the security services or goals that the network must satisfy to be deemed secure. Next, the different attack classifications were explained, along with examples of the various attacks initiated against a MANET. Finally, the security parameters that should be considered when determining the viability and effectiveness of a security approach were discussed. Security attacks in a MANET aim to exploit the inherent vulnerabilities and any shortcomings in security services. One such attack is the Black Hole attack. The next chapter will describe what Black Hole attacks are and the effects they have on a MANET.

Chapter 4 – Black Hole attacks in MANETs

4.1 Introduction

This chapter provides a detailed explanation of Black Hole attacks in MANETs and defines the different Black Hole attacks in networks using AODV, DSR, or OLSR routing protocols. Finally, the chapter looks at solutions and techniques previously proposed to reduce the impact of Black Hole attacks.

4.2 Overview of Black Hole attacks

A Black Hole attack occurs when a malicious node sends a reply message to a source node to fictitiously advertise itself as having the shortest and optimal path to the destination node. The Black Hole node does this by sending false route replies to ensure that data packets will be routed through it. However, instead of forwarding the data packets to the destination node, the Black Hole node simply discards it (Khan & Jamil, 2017). Once the node has placed itself between the source and destination nodes, it can do anything with the packets passing through it. The malicious node intends to hinder the path-finding process and intercept packets sent to the destination node (Gurjar & Dande, 2013).

For example, a malicious Black Hole node may trick a requesting source node by sending a fake reply message (RREP) that contains the desired parameters for successful route establishment when a request message is received. Once the route is established, the malicious node can drop all the network traffic it receives from the source nodes. This deliberate dropping of packets by a malicious node is known as a Black Hole attack (Khan & Jamil, 2017).

In Figure 4.1, malicious node *4* has entered the network by compromising the link between node *S* and node *7*. When source node *S* wants to transmit data to destination node *D*, it initiates a route discovery process. Malicious node *4* receives this route request and immediately sends a response to the source node *S*, identifying it as having the shortest path to the destination node *D*. If the reply from malicious node *4* reaches the source node *S* before the correct reply (path *S-2-3-D*), *S* will ignore all other reply messages and begin sending packets via the malicious node *4* route. As a result, all data packets are consumed or lost at the malicious node.

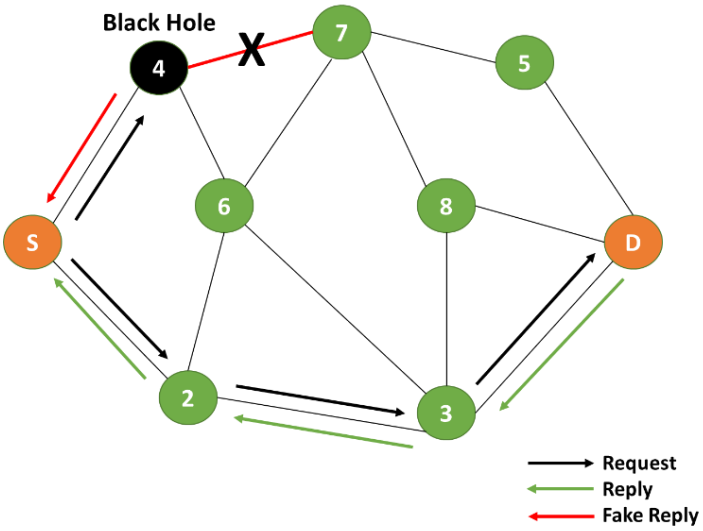

Figure 4.1 – Black Hole Attack

Black Hole attacks are incredibly harmful to MANETs as the data discarded is randomly selected and may include critical network data. According to Ahmed and Ko (2016), the presence of a Black Hole attack increases network overheads that deplete the nodes' energy in the network, thereby reducing the network's lifespan and ultimately destroying the network.

Black Hole nodes have two distinct properties (Hamamreh, 2018):

- These nodes seek to exploit the ad-hoc routing protocol by advertising themselves as having a fresh valid route to a destination node. These routes are fake and are intent on intercepting data packets.
- The packets that are intercepted are consumed and discarded.

Many solutions to Black Hole attacks assume that there might only ever exist one Black Hole node in the network; this is not true as Black Hole attacks can be executed by multiple nodes working together (Bala, 2016). When multiple Black Hole nodes exist in one MANET, it can become complicated and challenging to detect.

4.3 Classification and types of Black Hole attacks

According to Gurjar and Dande (2013), understanding the different classifications and types of Black Hole attacks will allow for the creation and implementation of better-suited solutions.

There are two classifications of Black Hole attacks in MANETS:

1) Internal Black Hole attacks

These attacks occur when the malicious node fits between the source and destination node. The malicious node is an active data route element in the MANET, enabling it to

conduct an attack at the start of the data transmission, making this type of attack more severe (Ahuja & Sugandha, 2017).

In Figure 4.2, source node *S* wishes to transmit data to the destination node *D*, initiating the route discovery process. The malicious Black Hole node *B* exists within the network and is fully aware of the RREQ, allowing it to respond with an RREP containing the shortest route to node *D*. As such, node *B* is assumed to be a trusted intermediary node, as it sits within the network, and is part of the transmission route between source node *S* and the destination node *D*. Malicious node *B* is now able to disrupt the transmission of data from within the MANET creating an internal Black Hole attack.

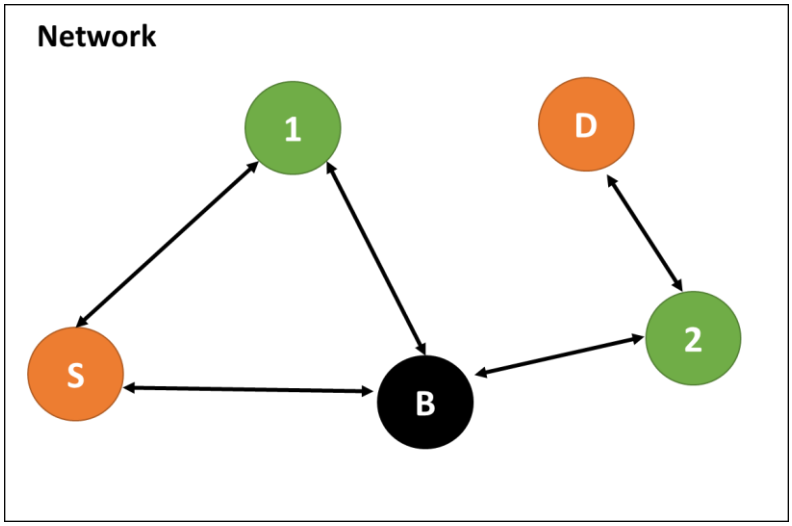

Figure 4.2 – Internal Black Hole Attack

2) External Black Hole attacks

External Black Hole attacks are launched from outside the MANET with the sole purpose of denying other nodes access to the network by creating network congestion or by disrupting all communications within the network (Bala, 2016). External Black Hole attacks occur when an external malicious node takes control of an internal node, turning it malicious. The external attacker then uses the newly attained malicious internal node to attack other nodes in the MANET by controlling the internal node. External Black Hole attacks function similarly to internal Black Hole attacks, except that the internal malicious node is controlled by an external attacker (Gurjar & Dande, 2013).

In Figure 4.3, the malicious Black Hole node *B* exists outside the MANET. Node *B* plans on creating congestion in the MANET by sending false traffic to the network. To do this, node *B* needs to gain access to the MANET by attacking a node within the network. Once node *B* successfully attacks an internal node, gaining access to the network via the compromised node, node B can begin transmitting fake data via the compromised node

without ever revealing the true source of the malicious data. This is an example of an external Black Hole attack.

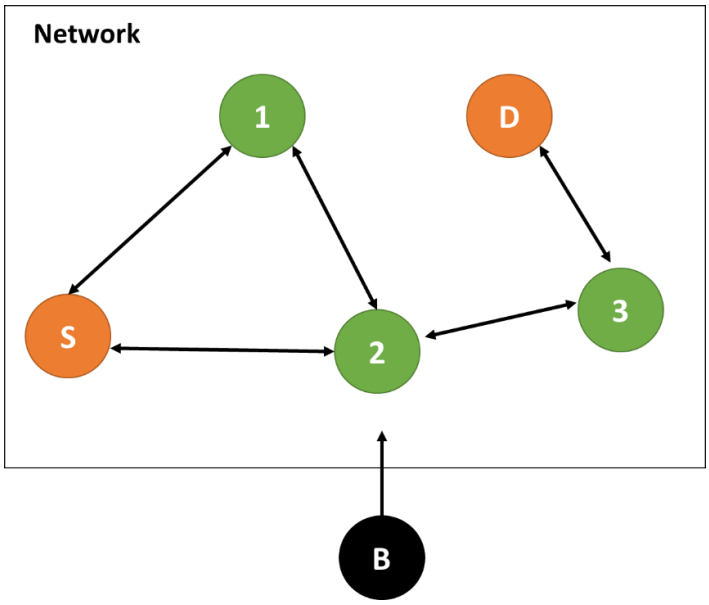

Figure 4.3 – External Black Hole Attack

There are two types of Black Hole attacks that can occur:

1) Single Black Hole attack

This is when a single malicious node acts alone to carry out a Black Hole attack. To do this, the malicious node violates the routing protocol by advertising itself as having the shortest, valid route to a destination node (Basulaim & Aman, 2017). Once communication is established, the malicious node drops intercepted packets rather than transmitting them, creating a Black Hole.

In Figure 4.4, source node *S* wants to send data to destination node *D*. The route discovery process is initiated from node *S* to node *D* using nodes *1, 2, 3* and *B* as intermediate nodes. Node *B* is a malicious Black Hole node that claims to have an active route to the destination *D*. Upon receiving the RREQ packets, malicious node *B* immediately responds by sending an RREP to *S* before any of the other legitimate nodes, thereby tricking node *S* into believing that node *B* is a legitimate node and can be a trusted part of the active data transmission route. Node *S* will then discard all the RREPs it received from legitimate nodes, causing the route discovery process to end. The malicious node *B* can now do as it wishes with the data packets it receives from node *S*, which may lead to packets being dropped or fabricated, resulting in the creation of a Black Hole attack.

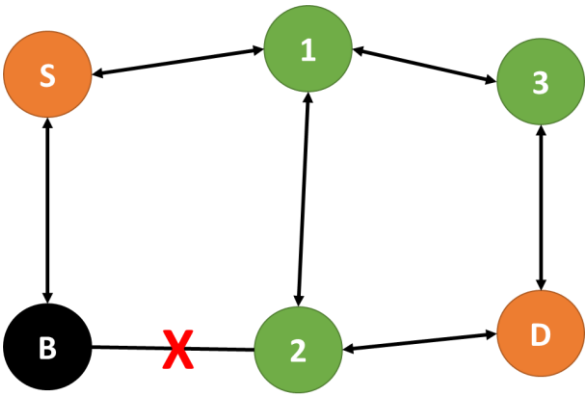

Figure 4.4 – Single Black Hole Attack

2) Collaborative Black Hole attack

In collaborative or cooperative Black Hole attacks, more than one malicious node works together to violate the routing protocol and bypass the implemented security mechanisms (Bala, 2016).

In Figure 4.5, *S* is the source node, and *D* is the destination node, with *1, 2, 3, 4, B1* and *B2* acting as the intermediate nodes. Nodes *B1* and *B2* act as cooperative Black Hole nodes. Node *S* wants to send data packets to node *D*; the route discovery process is initiated, and RREQ packets are sent to all the neighbouring nodes. The malicious nodes being part of the network also accept the RREQ and immediately send an RREP to node *S*. The RREP from *B1* reaches node *S* before any legitimate RREPs from the other nodes. Node *S* then starts sending data packets to *B1,* assuming it to be a legitimate node. Instead of forwarding the data packets, the malicious node *B1* can drop or transmit them to the other malicious node, *B2*. Node *B2* can then drop all the data packets it receives instead of forwarding them to the destination node *D*.

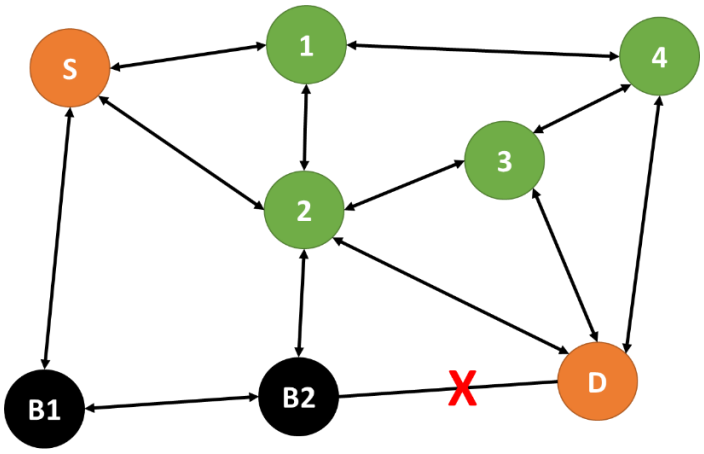

Figure 4.5 – Cooperative Black Hole Attack

4.4 Black Hole attacks in Reactive Routing Protocols

When the AODV routing protocol is under a Black Hole attack, the Black Hole node will first seek the active route between the source and destination node. The malicious node sends an RREP containing the spoofed destination address, including a very small hop count and high sequence number, to an intermediary node just before the source node. This intermediary node then forwards this RREP to the source node. This route will now be used for data transfer between the source node and the "destination" node, impersonated by the malicious node. This way, the data will arrive at the malicious node (Praveen, Gururaj & Ramesh, 2016). The malicious node can now drop these data packets. The normal communication between the source and intended destination will no longer exist, thus creating a Black Hole. The source node may never realise that the Black Hole exists as it believes that it is transmitting data to the correct destination (Sharma & Sharma, 2012). A malicious node inside the MANET basically forges an RREP message to appear as if it has a fresh route to the destination node when it receives the RREQ from the source node.

The malicious node creates an RREP with an increased sequence number to suppress any legitimate RREP messages that the source node may receive. This type of malicious node is a Black Hole node (Gurjar & Dande, 2013). Black Hole nodes reply to RREQ almost immediately with an RREP containing spoofed information, and this is done without executing the standard AODV operations. These RREPs are sent with high sequence numbers as higher sequence numbers are perceived to come from fresher routes. Black Hole attacks uncontrollably increase the network overhead and the network's energy consumption, which will finally lead to the network's demise. The type of data packets dropped are not checked or verified in any way. This makes the attack very dangerous as critical data could be lost forever (Praveen *et al.*, 2016).

Black Hole attacks in MANETs using the DSR protocol occur either as an RREP attack or an RREQ attack. RREP Black Hole attacks occur when a source node commences the route discovery process by broadcasting a route request (RREQ), and a malicious node responds to the RREQ, pretending to have the freshest and shortest route to the destination node (Mejaele & Ochola, 2015). The malicious node deceives the other nodes by sending forged RREP messages that always return valid RREP even when the malicious node does not have a valid route to the destination. The data packets transmitted to the destination will always pass through the malicious node allowing the malicious node to absorb or discard messages silently (Panda & Pattanayak, 2018). RREQ Black Hole attacks occur when a malicious node sends out forged RREQ messages pretending as if the forged RREQ is a rebroadcast RREQ packet originating

from the node it is targeting in the network. The malicious node adds itself as the next hop in the route record, so the entire messages destined for the target node will pass through the malicious node, silently absorbing or discarding the messages (Mejaele & Ochola, 2015).

4.5 Black Hole attacks in Proactive Routing Protocols

In the OLSR routing protocol, valid routes transmit HELLO and Topology Control (TC) messages. If an attacker can modify the HELLO messages, TC messages or both messages simultaneously to be false, then a successful attack can be executed (Kaur *et al.*, 2015).

When a MANET using the OLSR protocol is under a Black Hole attack, the malicious node uses false HELLO or TC messages to manipulate its way into earning a privileged position within the network to become an MPR. The malicious node will receive all routing messages from its neighbouring nodes and then drop them, resulting in a Black Hole attack (Nabou, Laanaoui & Ouzzif, 2019). There are three cases in which Black Hole attacks can be implemented in OLSR. They are TC-Black-Hole, HELLO-Black-Hole and TC-HELLO-Black-Hole attacks (Salehi, Samavati & Dehghan, 2011).

4.5.1 TC-Black-Hole attack

In this attack, depicted in Figure 4.6, malicious nodes try to advertise a false route by modifying the TC messages, claiming that all other nodes have selected it as their MPR. This means the malicious node sends the address of all the nodes within the network in its TC messages. All the nodes on the network update their routing tables with this false information, thus creating and storing these new routes. At data transmission, the source node may send its data packets through these newly established routes. Once the malicious Black Hole node receives the data packets, it may choose to drop or modify them (Salehi & Samavati, 2013).

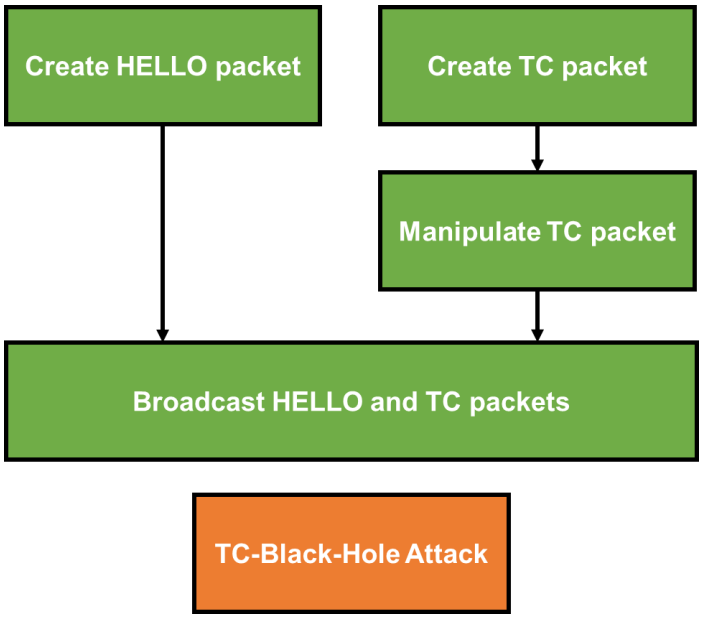

Figure 4.6 – TC-Black-Hole Attack

4.5.2 HELLO-Black-Hole

In this attack, depicted in Figure 4.7, HELLO messages are manipulated at the time of transmission. The malicious node embeds the address of all the network nodes into the HELLO message and then broadcasts that message. This means the malicious node claims to be the neighbour of all nodes in the network and has a full-duplex transmission link to all of them. This will result in the malicious node being selected as the MPR node by its neighbour nodes. All the nodes on the network update their routing tables with this false information and then create and store these new routes. Therefore, these malicious Black Hole nodes will receive the data packets and then drop them preventing them from reaching their destination (Salehi & Samavati, 2013).

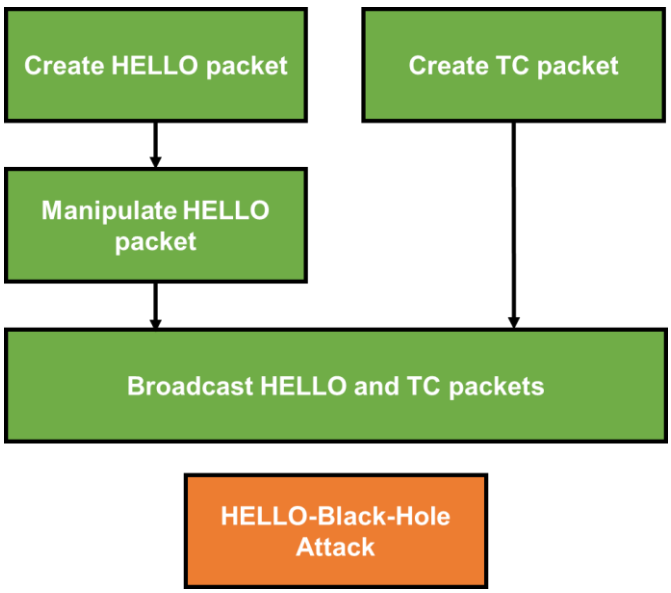

Figure 4.7 – HELLO-Black-Hole Attack

4.5.3 TC-HELLO-Black-Hole attack

This type of attack combines the TC-Black-Hole and HELLO-Black-Hole attacks, depicted in Figure 4.8. The malicious Black Hole node modifies the HELLO message and the TC message. The malicious node will be selected as the MPR and facilitate the creation of false links using fake TC messages. This will allow Black Hole nodes to advertise fake routes more quickly and direct more data transmissions towards themselves, resulting in more packets being dropped and leading to the network's demise (Salehi & Samavati, 2013).

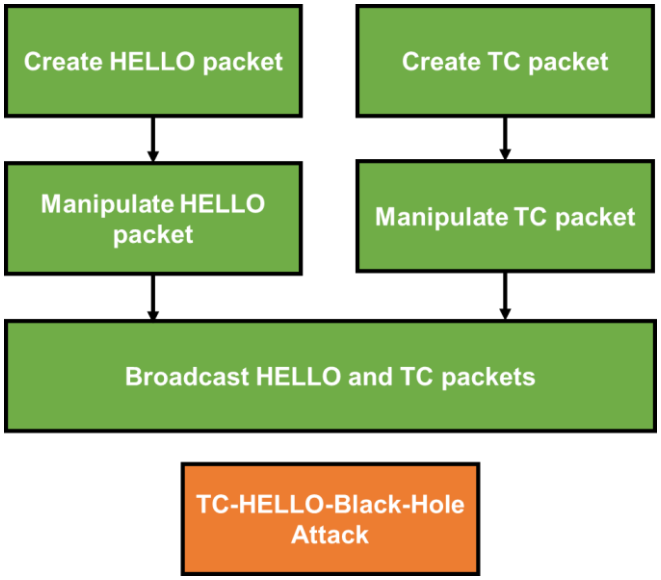

Figure 4.8 – TC-HELLO-Black-Hole Attack

4.6 Black Hole attack Detection Techniques

Many researchers have proposed different techniques to detect Black Hole attacks in MANETs. However, Gurung and Chauhan (2017) propose these techniques be classed based on broader categories:

1) Cryptography and Encryption based schemes

Cryptography studies mathematical techniques to create a layer of protection for information using encryption methods to prevent unauthorised access to unencrypted data (Mohan & Nirmal, 2013). Cryptography is often used to enforce the following security mechanisms: availability, authenticity, data confidentiality, data integrity, and non-repudiation. Cryptography based schemes can also be used to provide secure routing in MANETs. These schemes use encryption and cryptography technologies, such as symmetric-key cryptography, hashing, and digital signatures, to secure the MANET from possible attacks (Gurung & Chauhan, 2017).

Mohammad, Mahmood and Vemuru (2018) compared the performance of cryptographic solutions based on the Chaotic maps and RSA to protect MANETs from being attacked. The results obtained from their research show that RSA provides excellent security but has a much higher time complexity, which negatively impacts the network's performance in terms of end-to-end delay. Their research findings conclude that Chaotic map-based techniques are the better alternative to the RSA techniques as Chaotic maps provide adequate security and protection with far less time and resource overheads.

Ahmed and Oh (2013) proposed an encryption-based Black Hole detection mechanism for MANETs. This encryption verification method effectively minimised multiple Black Hole nodes by employing an encryption mechanism in the form of an Encrypted Verification Method (EVM). Their EVM approach makes use of two steps. Firstly, every node examines its neighbouring nodes by inspecting their data transmission behaviour, and secondly, a detection node monitors for suspicious RREPs. Should a suspicious RREP be detected, the detection node sends an encrypted verification message directly to the destination node along with the suspicious RREP for verification.

An investigation to discover and mitigate the effect single and cooperative Black Hole attacks have on AODV in terms of end-to-end delay, network load and throughput was conducted by Basulaim and Aman (2017). Their proposed solution was based on a one-way hash chain to deal with single and cooperative Black Hole attacks. The results based on their simulations showed substantial improvements across end-to-end delay, network load and throughput when using their proposed approach.

Selvavinayaki and Karthikeyan (2012) proposed a solution modelled around a Modified Ad-hoc On-Demand Multipath Distance Vector Routing (MAOMDV) with an additional secret sharing scheme. To conserve bandwidth, the protocol employs Shamir's secret sharing technique. When a source node wants to interact with another node, it must first decide on a secret sharing strategy that will be used to split the message into smaller blocks. Once this is done, the source node must forward these blocks to the destination through selected paths. Once the destination node receives a predefined number of correct blocks, it can recover the original message by reconstructing the blocks. This method can be used to detect whether multiple Black Hole nodes exist along a transmission path.

Umaparvathi and Varughese (2012) created a Two-Tier Secure Ad-hoc On-Demand Routing Protocol that can be used to combat Black Hole attacks. The protocol employs a symmetric key system and verification messages to find safe pathways. The proposed solution can be utilised to identify both single and cooperative Black Hole attacks by merely confirming the authenticity of the RREP message. The basic assumption is that

there is a strong symmetric key distribution system in the MANET. As such, each node pair within the network shares a unique secret key. The proposed protocol uses two security levels during the route discovery process and the data transfer process. This means that if the detection of a Black Hole attack fails at the route discovery process, the next level will identify it.

2) Overhearing based scheme

This is based on nodes in a MANET being able to overhear its neighbouring nodes' transmission, and should it find a neighbouring node to be doing something unexpected, it considers it as malicious and notifies the network of its findings (Gurung & Chauhan, 2017).

Agarwal and Rout (2015) proposed a solution called Overhearing based Misbehaviour Detection (OMD), which uses overhearing and independent agents in the MANET to detect any nodes misbehaving. In OMD, each node overhears the broadcasts of its neighbours and computes its own packet forwarding ratio as well as its neighbours. The source node uses this information to categorise whether a node is a misbehaving node or not.

Sharma and Gupta (2012) proposed a scheme to detect Black Hole nodes by using the promiscuous mode of the node. This promiscuous mode allows node A to overhear communication to and from B if it is within the range of node B, even if those communications do not directly involve node A.

3) Sequence number and Threshold-based scheme (Dynamic learning)

A source node calculates a threshold value using the destination sequence number parameter of reply packets. If a reply packet contains a sequence number greater than the threshold, the reply packet is dropped (Gurung & Chauhan, 2017).

Sreedhar, Verma and Kasiviswanath (2012) proposed a solution that implements a secure communication channel between nodes in MANETs. During routing, a Threat Value Parameter (TVP) is calculated for each node and compared against a threshold value. If a node has a TVP higher than the threshold value, that node should be marked as a node at risk of attack and is not suitable for further routing. An alternate path should then be selected for routing. The routing path is selected using nodes with the lowest TVP values.

Mistry, Jinwala and Zaveri (2010) developed an approach that enhances the actual source code of the AODV protocol. As part of the enhancements, a new table (CMG_RREP_TAB), a timer (MOS_WAIT_TIME) and a variable (MALI_NODE) were added to the original AODV protocol source code. With this approach, once the initial

RREP message is received, the source node waits for MOS_WAIT_TIME to complete and then saves all other RREP messages received to the CMG_RREP_TAB table. The source node then analyses the RREPs stored in the CMG_RREP_TAB table and discards any RREP that has a suspiciously high destination sequence number. The node from which the RREP with a high sequence number was received is treated as a malicious node. The identity of the malicious node is stored as MALI_NODE, and all future control messages coming from that node are discarded. Once the malicious node has been identified, the RREP with the next highest destination sequence number is chosen from the CMG_RREP_TAB table. The CMG_RREP_TAB is flushed once an RREP is chosen from it. This solution fails to detect cooperative Black Hole attacks.

Raj and Swadas (2009) proposed a solution that uses dynamic learning systems to detect Black Hole nodes in a MANET and then notify the other nodes in the network of the Black Hole node. During communication, a node receives the RREP packet. The node then checks the first value of the sequence number in its routing table. This threshold value is the average difference of the sequence numbers between the routing table and the RREP packet; this value is updated dynamically. If the sequence number is set higher than the predefined threshold value, this node will be considered a malicious node. The dynamic learning system has decreased average end-to-end delays and has assisted in reducing routing overheads. If a multi-node Black Hole attack occurs in the MANET, the process to detect them will be too complex, and this solution will not work in combating the attack.

Khan *et al.* (2018) suggested implementing a signature-based Black Hole detection algorithm that uses assigned sequence numbers to identify Black Hole nodes. For nodes to be considered malicious, the sequence number of the malicious node should not exist between a specified minimum and maximum sequence number. Their approach also detected collaborative Black Hole attacks by restricting all nodes with sequence numbers higher than the specified maximum sequence number and lower than the specified minimum sequence number from being included in any routing protocols.

Kurosawa *et al.* (2007) suggested a dynamic learning approach to find a Black Hole attack in a MANET. This method was intended to observe the characteristic change of a node over a specific period of time. If the features of a node vary over time, it will be identified as a Black Hole node. The characteristics observed are the number of sent RREQs, the number of received RREPs and the mean destination sequence numbers of RREQs and RREPs. The limitation of this approach is that it cannot isolate the Black Hole nodes due to the absence of a detection mode.

4) Acknowledgement and Trust-based scheme

The use of an acknowledgement packet is sent by the destination node to confirm it has received the transmission (Gurung & Chauhan, 2017).

Deng, Li and Agrawal (2002) proposed a solution using On-Demand Distance Vector (ODV) for Black Hole attacks. In this solution, when an intermediate node replies to an RREQ, the RREP packet should include information about its next-hop node. The source node transmits a Further Request (FREQ) to the next-hop node to enquire about the intermediary node and its route to the destination. This approach may help identify the intermediary node's reliability if the next-hop node is trusted. However, one of the drawbacks of this solution is related to collaborative Black Hole attacks on MANETs. This approach could be used for individual attacks but cannot prevent collaborative attacks.

Saetang and Charoenpanyasak (2012) put forward a solution to detect and eliminate the Black Hole attack using a Credit-based Ad-hoc On-Demand Distance Vector (CAODV) routing protocol. This method makes use of a credit mechanism to check the next-hop node in order to determine whether it can be trusted or not. The first step is for a source node to send an RREQ to all other nodes in the network. The receiving nodes assign a credit score to the next-hop node based on how the next-hop node responds and acts. For example, when a node part of the route path sends a packet, one credit is deducted from the next-hop node. Once the destination node receives the data packets, it sends a Credit Acknowledge (CACK) back to the source node. Each node on the way back to the source node that was a part of the chosen transmission route will increase the credit of the next-hop by 2 to indicate a higher trust level. On the other hand, credit will be decreased if a node does not receive the CACK. When a node’s credit reaches zero, this node will not be trusted and will be blacklisted.

Tamilselvan and Sankaranarayanan (2007) developed a solution using a modified version of the AODV protocol. The solution used a Fidelity table in which every node is given a fidelity level relating to its reliability. A node with a fidelity value of zero is eliminated from the network as it is considered a malicious node. Fidelity levels of nodes are updated based on their trusted interactions among nodes within the network. Once a destination node receives the data packets sent from the source node, an acknowledgement is sent to the source to confirm receipt. This then allows the intermediate node’s fidelity levels to be incremented. If an acknowledgement is not received, the intermediate node’s fidelity level will be decremented as the node is considered suspicious. The processing delay is the main drawback of this solution.

5) Cross-layer Collaboration based scheme

These solutions rely on more than two network layers to cooperate to detect any malicious activity in the MANET (Gurung & Chauhan, 2017).

Weerasinghe (2011) created a methodology that could detect multiple Black Hole nodes working together to execute a cooperative Black Hole attack. The solution proposed uses the Data Routing Information (DRI) table by cross-checking routes, using Further Requests (FREQ) and Further Reply's (FREP). This produces a modified version of the AODV protocol. This solution proved to be much better in solving the issue of cooperative Black Hole attacks when compared to previously available solutions. However, it still does not solve cooperative attacks completely.

Tamilselvan and Sankaranarayanan (2007) created a solution based on AODV, in which the source node waits for all route replies even after receiving an initial reply. The RREPs are collected and stored. The collected information is then analysed, and if a repeated next-hop node is present among the collected routes, then it is assumed that those paths do not contain malicious nodes and are safe for use. This solution has time delay overheads because source nodes must wait for all route replies before choosing a route to send packets. This method cannot be used to detect cooperative Black Hole attacks.

Deng, Li and Agrawal (2002) proposed another solution that uses an additional route between the source node and the intermediate node to check the route's viability. If it is viable and exists, then the intermediate node can be trusted, and the data packets can be sent. If not, the reply message from the intermediate node is discarded, and an alarm message is sent out to the network.

6) IDS based scheme

IDS based schemes are similar to Overhearing based schemes, with the exception being the use of special Intrusion Detection System (IDS) nodes. IDS nodes detect the malicious activities in a MANET and then notify the network to isolate the malicious node (Gurung & Chauhan, 2017).

Abu *et al.* (2011) proposed a solution called Ad-hoc On-Demand Distance Vector Robust (AODVR). The AODVR algorithm contains RREQ, RERR and HELLO packets similar to the packet types in AODV. The significant difference between AODV and AODVR is that AODVR modifies the content and format of the RREP and contains a new ALARM packet type. This modified AODV protocol makes use of a Packet Classifier. As packets arrive in the network, the Packet Classifier can determine if a packet is an RREQ, RERR, RREP secure, HELLO or ALARM packet. A new Extractor module is used to extract the contents required from the various packets, except the HELLO packet. Once a node is

identified as a malicious Black Hole node, the ALARM Broadcaster sends alerts to neighbouring nodes to let them know about the Black Hole node identified. Once a node receives an ALARM packet, it immediately sends a message to other nodes in its vicinity to inform them of the breach. This is done until the entire network is aware of the breach.

While other schemes exist, these solution scheme categories form the majority of those commonly used to propose solutions to Black Hole attacks. Other schemes include isolating malicious nodes, reducing the reliance on using the shortest path, and other modified methods (Gurung & Chauhan, 2017).

In their research, Jain and Tokekar (2015) present an approach using a Route Reply caching mechanism to overcome Black Hole attacks in AODV, called Secure AODV (SAODV). Their approach eliminates routing through the Black Hole node. Their simulation results show that the proposed SAODV protocol works very well under all circumstances irrespective of the number of Black Hole nodes in the MANET.

A solution has been proposed by Careem and Dutta (2020), based on the reputation information spread via a blockchain, using the shortest, most reputed path routing scheme called BC-AODV. The proposed approach uses the blockchain to establish creditability and reputation amongst nodes. The cost metric of AODV is modified to reflect a node's reputation and helps improve the reliability of the route selection. The simulation results show an improvement in the overall packet delivery in the presence of routing attacks.

Suryawanshi and Tamhankar (2012) proposed a solution that decreases the impact of a Black Hole attack. The routing process of AODV has been altered by the addition of a mechanism that ignores the route that is established first. The premise is that the network under attack receives numerous RREP packets from different pathways, with the first RREP packet originating from a rogue node. Before transmitting an RREP packet, a Black Hole node does not consult its routing table. As a result, the initial RREP is ignored to prevent updating the routing table with the malicious route entry. Although this strategy enhances packet delivery, it does have certain drawbacks. This method will not detect an attack if the first RREP originates from a legitimate intermediate node with a valid path to the destination node or if the RREP message from a malicious node arrives after the first RREP.

Gupta, Kar and Dharmaraja (2011) developed a protocol called the Black Hole attack avoidance protocol (or BAAP), which is based on the Ad-hoc On-Demand Multipath Distance Vector (AOMDV). Every node in BAAP keeps track of the legitimacy table and uses it to select the most valid node when delivering RREP back to the source node.

This method can be used to prevent the appearance of multiple Black Hole nodes. The only drawback is that this method uses an additional table to restrict malicious Black Hole nodes from compromising the route between a source node and a destination node.

Jhaveri, Patel and Jinwala (2012) presented a theoretical solution against Black Hole attacks, which finds an effective short and secure route to the destination node. Their approach increased the packet delivery ratio (PDR) with a negligible difference due to the routing overhead. In their approach, the source node broadcasts a list of the known malicious nodes when sending out the RREQ. Nodes that receive the RREP confirm the truthfulness of the routing information. Nodes update their route tables when they receive any information of malicious nodes from routing packets. The malicious nodes are isolated and are not allowed to participate in transmission, which helps improve the PDR. The authors of this approach believe that this solution could be used in any protocol as it finds malicious nodes and helps eliminate them during the route discovery phase.

Sen, Koilakonda and Ukil (2011) proposed the creation of a mechanism, which modifies the AODV protocol so that it can be used to defend or fight against cooperative Black Hole attacks. For this mechanism to work, each node needs to keep a Data Routing Information (DRI) table. The sender node transmits an RREQ message to find a safe route to the intended destination node. In the suggested mechanism, the nodes that respond to the RREQ message during the route discovery process needs to transmit two additional bits of information. Each intermediate node replies with a next-hop node (NHN) and its DRI to the sender node. Once the sender node receives these replies from the intermediate node, the sender node then checks its own DRI table to establish the reliability of the intermediate node. If the sender node has used the intermediate node for routing data packets on prior occasions, the sender node can start sending the data packets through the intermediate node. If this is an unknown intermediary node, the sender node will send a FREQ to the NHN to establish the reliability of the intermediary node. This technique can be used to detect the existence of multiple cooperative Black Hole nodes. However, a key weakness of this technique is that nodes need to keep an additional database of previous routing experiences over and above the normal routing information.

Singh (2011) created a feedback-based solution to detect Black Hole nodes. In this approach, the number of sent packets need to be examined at each node. It is safe to assume that a Black Hole node will almost always have zero sent packets. Once a Black Hole node has been found, a feedback method is adopted to stop packets from being sent to the malicious Black Hole nodes. Packets that arrive at the node closest to the

Black Hole node are returned to the sender. The sender then takes a more secure path to the recipient. This solution is unable to discover cooperative Black Hole nodes.

Dorri (2016) proposed a table-based approach to detect and eliminate cooperative malicious Black Hole nodes in MANETs using the AODV routing protocol. The proposed approach uses data control packets to ensure the authenticity of all the nodes in the selected path. The concept of an extended Data Routing Information (DRI) table was used to detect and eliminate all malicious nodes from the MANET. The results of the OPNET14 simulations show a decrease in packet overheads and an increase in network throughput, with the added benefit of no false positive detection.

Table 4.1 presents a summary of the different approaches in terms of detection techniques, how they respond to attacks and the research contribution of the approach.

Table 4.1 – Summary of Existing Black Hole Detection and Mitigation Approaches

Author	**Approach or Detection Technique**	**Response to Attack**	**Contribution**
Mohammad, Mahmood and Vemuru (2018)	Cryptography	Proactively protects MANET from being attacked.	Chaotic map-based techniques are the better alternative to the RSA techniques as Chaotic maps provide adequate security and protection with far less time and resource overheads.
Ahmed and Oh (2013)	Encryption	Every node examines its neighbouring nodes by inspecting their data transmission behaviour, and a detection node monitors for suspicious RREPs.	Encryption messages are used to verify a route.
Basulaim and Aman (2017)	Cryptography	Prevent unintentional manipulation of data.	A one-way hash function is used to encode the identity of a node and can only be decrypted by a valid destination node.
Selvavinayaki and Karthikeyan (2012)	Encryption	-	Based on encryption techniques to transmit and receive data in blocks across multiple paths to detect the existence of Black Hole nodes.
Umaparvathi and Varughese (2012)	Encryption	-	Two-tier security to detect and identify potential Black

			Hole nodes using symmetric keys.
Agarwal and Rout (2015)	Overhearing	-	Listens to transmission using overhearing and independent agents to detect malicious behaviour.
Sharma and Gupta (2012)	Network Traffic Monitoring	Promiscuous monitoring of nodes	Nodes are aware of the other nodes in their vicinity.
Sreedhar, Verma and Kasiviswanath (2012)	Verification	Nodes are marked as at risk of attack and are not suitable for further routing. An alternate path is then selected for routing.	Threat Value Parameters (TVP) are used to determine if a route is prone to attack or if it can be used for communication.
Mistry, Jinwala and Zaveri (2010)	Trust	Discard the use of potentially malicious nodes.	Checks all RREP sequence numbers to discard any extreme outliers.
Raj and Swadas (2009)	Dynamic Learning	-	Verify sequence numbers against thresholds to detect malicious nodes.
Khan *et al.* (2018)	Threshold Sequence Number	Restrict all nodes with sequence numbers higher than the specified maximum sequence number and lower than the specified minimum sequence number from being included in any routing protocols.	Signature-based Black Hole detection algorithm that uses assigned sequence numbers to identify Black Hole nodes.
Kurosawa *et al.* (2007)	Dynamic Learning	Observe changes to nodes to identify any potential risks.	Monitor the behaviour of nodes in a MANET to identify any changes that may point to malicious intent.
Tamilselvan and Sankaranarayanan (2007)	Trust	-	Fidelity tables are used to establish the reliability of a node. These values are changed based on the nodes' responses to requests.
Deng, Li and Agrawal (2002)	Trust	Limits the use of a node if untrusted.	Ensures secure packet delivery.
Saetang and Charoenpanyasak (2012)	Trust	Blacklists untrusted nodes.	Checks if a node can be trusted or if it needs to be blacklisted.
Tamilselvan and Sankaranarayanan (2007)	Verification	-	Sender nodes wait for all route replies and then verify a route by checking for

			repeated next-hops amongst the collected data.
Weerasinghe (2011)	Verification	-	Able to detect multiple Black Hole nodes by the cross-checking of routes.
Deng, Li and Agrawal (2002)	Verification	Establishes the viability of the route.	Uses additional routes to establish the viability of a primary route.
Abu *et al.* (2011)	Intrusion Detection	Sends alert to nodes.	Ensures all nodes are working under normal operation.
Jain and Tokekar (2015)	Caching Mechanism	Eliminates routing through the Black Hole node.	Uses a Route Reply caching mechanism to overcome Black Hole attacks in AODV.
Careem and Dutta (2020)	Reputation Establishment	Reputable routes are favoured.	Approach uses the blockchain to establish creditability and reputation amongst nodes.
Suryawanshi and Tamhankar (2012)	Safest Route Detection	The first RREP route is discarded.	The first route reply received is discarded as it is assumed to originate from a malicious node.
Gupta, Kar and Dharmaraja (2011)	Reservation of Data Flow	Restricts the use of nodes to be avoided.	Implements avoidance techniques in MANETS.
Jhaveri, Patel and Jinwala (2012)	Shortest Path Detection	Publishes a list of known malicious nodes to all other nodes in MANET.	Isolates malicious nodes.
Sen, Koilakonda and Ukil (2011)	Trust	-	Checks if a route has been used previously to determine the reliability of the route.
Singh (2011)	Verification	If feedback is not received from a route, then packets are not sent via that path.	Feedback based solution to determine if packets that are sent via a route reach their destination.
Dorri (2016)	Data Routing Information Table	Extended Data Routing Information is used to detect and eliminate all malicious nodes from a MANET.	Data control packets to ensure the authenticity of all the nodes in the selected path.

4.7 Summary

This chapter provided a detailed discussion around Black Hole attacks in MANETs. It provided a general overview of what Black Hole attacks are and how they affect the integrity of MANETs. The different classifications of Black Hole attacks and their effects on the operation of a MANET were presented. Black Hole nodes can restrict traffic in a network and disrupt communication amongst nodes. This chapter also illustrated how Black Hole attacks could occur in the AODV, DSR and OLSR routing protocols. The chapter closed with a discussion of some of the solutions and techniques proposed to detect, mitigate, and prevent Black Hole attacks from occurring. The next chapter provides a review of related works to identify any shortcomings or research gaps that this study will potentially address.

Chapter 5 – AODV, DSR and OLSR routing protocols under Black Hole Attack

5.1 Introduction

This chapter provides a review of related works to identify any shortcomings or research gaps that this study will potentially address.

5.2 Related Works

This section provides an overview of previous research conducted on AODV, DSR and OLSR while under regular operation and Black Hole attack.

The behaviour of OLSR and DSR was examined under the influence of selfish node attacks and various types of Black Hole attacks in a study by Salehi and Samavti (2012). The simulations findings reveal that the PDR and end-to-end delay for DSR is higher than OLSR while under the various attacks and the number of routing packets imposed on the network by OLSR was more than what was imposed by DSR.

Das (2014) conducted performance studies for MANET routing protocols AODV and DSR by varying network load, mobility, and network size. The packet delivery ratio (PDR) was observed, and it was found that DSR performed better than AODV in smaller sized networks with lower load and lower mobility. In contrast, in larger sized networks with more load and higher mobility, AODV performed better than DSR. Overall, the routing load generated by DSR is less than AODV. This study only considered PDR as a performance metric and omitted OLSR in its comparisons.

Neeraj and Barwar (2014) evaluated the performance of AODV, OLSR and ZRP under Black Hole attack in NS2 using PDR, average throughput, and average end-to-end delay as performance metrics. Their findings noted that the performance of AODV was affected more harshly and adversely when under Black Hole attack compared to other protocols across the different scenarios.

Praveen, Gururaj and Ramesh (2016) analysed and compared the AODV and OLSR protocols using packet delivery ratio (PDR) and throughput as performance metrics. Their simulation results showed that AODV generally outperforms OLSR under regular operation and Black Hole attacks. Both AODV and OLSR showed decreased values in PDR and throughput when compared under regular operation and Black Hole attack.

However, their study failed to compare DSR with AODV and OLSR to analyse the joint performance of the three protocols.

Adel and Melad (2016) used the OPNET network simulator to evaluate the performance of the AODV, DSR, OLSR and GRP MANET routing protocols based on performance metrics, delay and throughput. The simulation results indicate that OLSR performed better than ADOV, GRP and DSR concerning delay and throughput under heavy FTP traffic. The authors did not analyse the performance using PDR as a metric.

Shankar and Chelle (2016) evaluated the performance of AODV, DSDV, DSR and OLSR based on PDR, throughput, and end-to-end delay. The results from their simulations show that OLSR and DSDV perform best in densely populated networks with a low node mobility rate. Whereas AODV was better suited for networks with more nodes, DSR performed well in low-density networks with a low node mobility rate. The effects of a Black Hole attack were not considered as part of this study.

In a study by Singh and Choundary (2017), AODV and OLSR routing protocols were evaluated and analysed under Black Hole attack, using the performance metrics PDR, end-to-end delay, network load and average throughput. Their results show that a larger number of nodes and increased route requests have a more significant effect on the performance of the MANET. Also, their results show that AODV is more vulnerable than OLSR under Black Hole attacks. The authors did not consider DSR in their comparisons.

Singh and Khurana (2017) evaluated the performance of DSR, OLSR and ZRP in terms of performance metrics throughput in Mbps and delay in milliseconds using NETSIM. Their simulations were created using 5 and 10 nodes in a 500m x 500m network area (a low-density network). Their simulations proved that ZRP is a more reliable protocol in terms of delay and throughput than OLSR and DSR. This study did not consider AODV and does not depict a modern-day real-world network scenario truly in terms of network density.

Khurana, Kumar and Sharma (2017) analysed routing protocols AODV, DSR and ZRP to determine how they handle congestion, as congestion is considered a limiting factor that deteriorates the performance of a network. This study evaluated the performance of AODV, DSR and ZRP with the number of packets transmitted, packets errored, packets collided and throughput as performance evaluation criteria. These simulations were done using the NETSIM simulator. The simulation results found that the AODV protocol performed better and more effectively controlled congestion in MANETs. This study did not consider the effects of a Black Hole attack and did not include simulations for the OLSR routing protocol.

Nurcahyani and Hartadi (2018) analysed AODV and DSR during single Black Hole and collaborative Black Hole attacks in MANET, using average throughput, delay, and packet loss as Quality of Service (QoS) parameters, to determine which routing protocol performed better. Their simulations showed that AODV had a lower decrease in throughput than DSR when exposed to both single and collaborative Black Hole attacks. DSR also experienced a more considerable packet loss under collaborative Black Hole attacks. This study did not consider OLSR in the comparisons.

Jubair *et al*. (2018) evaluated the performance of AODV and OLSR routing protocols in a MANET environment with throughput, packet delivery ratio (PDR), and end-to-end delay as performance metrics using NS2.33 to conduct their simulations. Their study used simulations to examine the performance of the routing protocols based on the number of nodes in the network and the size of the network terrain. The results of their simulations show that the AODV outperforms the OLSR in most scenarios and that the number of nodes and network terrain size has a significant impact on the performance of both routing protocols. This study did not consider DSR in the comparisons, nor did it simulate Black Hole attack scenarios for the protocols under consideration.

Kuyoro *et al*. (2018) simulated two network scenarios, with Black Hole and without Black Hole attacks, using Network Simulator (NS-2.35) with performance metrics throughput, PDR, and end-to-end delay. These simulations were conducted on four routing protocols, reactive routing protocols, AODV & TORA, and proactive routing protocols, OLSR & DSDV. The susceptibility of these protocols was analysed. Based on the analysis of simulated results, it was concluded that the Black Hole attack's impact is more severe on AODV and OLSR in the reactive and proactive protocols, respectively. This study did not consider DSR in the comparisons.

Nabou, Laanaoui and Ouzzif (2018) analysed the performance of AODV and OLSR, using throughput, PDR, end-to-end delay, and packet lost to determine which protocol is more exposed to Black Hole attacks. All measurements were conducted using Network Simulation 3 (NS3). The evaluation of these routing protocols under Black Hole Attack was carried out by changing two crucial parameters in the mobility environment, namely, the number of nodes and the pause time. In the Random Way Point Mobility Model, the pause time is the amount of time each node waits before altering its direction or speed. The results of several diverse measurements show that AODV is more vulnerable to the Black Hole in both scenarios. Furthermore, the Black Hole attack adversely affects both protocols when the number of nodes is limited and the mobility is slow.

Panda and Pattanayak (2018) studied and analysed the behaviour of MANET routing protocols AODV and DSR under Black Hole attack. In their study both AODV and DSR

were analysed in the presence of a Black Hole attack with performance parameters end-to-end delay, PDR, and throughput. The results of their study show that in terms of end-to-end delay and throughput, DSR performed better than AODV under Black Hole attack. Whereas in terms of PDR, AODV performed better than DSR under Black Hole attack. As a result, they concluded that AODV is more vulnerable to Black Hole attacks than DSR. This study did not consider OLSR in the protocol comparisons.

Chandan and Mishra (2019) researched the effects of a Black Hole attack on the AODV routing protocol by comparing the network performance of a standard implementation of AODV against AODV under a Black Hole attack. Their study showed that PDR and Average throughput decreased while end-to-end delay (EED) increased under Black Hole attacks. This study did not compare the effects of a Black Hole attack on DSR and OLSR.

Kalakar, Ali and Chack (2020) analysed the effect Black Hole attacks had on AODV and OLSR using end-to-end delay, throughput, and network load as performance metrics. Their simulations showed that the Black Hole attack had a marginally greater effect on the end-to-end delay of AODV compared to OLSR and the throughput of AODV decreased by almost two times more than the throughput of OLSR. However, the effect of the Black Hole attack on the network load of AODV was less than that of OLSR; as such, their research and analysis of their simulation results concluded that AODV is more vulnerable to Black Hole attack than OLSR.

Employing the OPNET Modeler 14.5 simulator, Khan, Akre, and Saeed (2021) investigated the efficiency of the OLSR and DSR protocols in the presence and absence of a Black Hole attack in terms of throughput, end-to-end delay, PDR, and network load in various situations. The results of this study revealed that the Black Hole attack drastically reduced DSR and OLSR performance. However, the performance degradation of DSR was more severe than the performance of OLSR in the presence of a Black Hole attack.

Table 5.1 summarises the related works reviewed, highlighting their findings and shortcomings that provide insight into the need for the research conducted by this study.

Table 5.1 – Summary of Related Works

Author	Protocol(s)	Results or Outcome	Shortcomings or Research Gaps
Salehi and Samavti (2012)	DSR, OLSR	The PDR and end-to-end delay for DSR is higher than OLSR, while under the various attacks, the number of routing packets imposed on the network by OLSR was more than what was imposed by DSR.	AODV was not considered for comparison. Average throughput was not analysed as a performance metric.
Das (2014)	AODV, DSR	It was found that DSR performed better than AODV in smaller sized networks with lower load and lower mobility, whereas in larger sized networks with more load and higher mobility, AODV performed better than DSR.	OSLR was not considered for comparison. Only PDR was analysed as a performance metric.
Neeraj and Barwar (2014)	AODV, OLSR, ZRP	Using PDR, average throughput, and average end-to-end delay as performance metrics, their findings noted that the performance of AODV was affected more harshly and adversely under Black Hole attack when compared to other protocols across the different scenarios.	DSR was not considered for comparison.
Praveen, Gururaj and Ramesh (2016)	AODV, OLSR	Using packet delivery ratio (PDR) and throughput as performance metrics, their simulation results showed AODV generally outperforms OLSR while under regular operation and Black Hole attack. Both AODV and OLSR showed decreased values in PDR and throughput when compared under regular operation and Black Hole attack.	DSR was not considered for comparison.
Adel and Melad (2016)	AODV, DSR, OLSR, GRP	The simulation results indicate that OLSR performed better than ADOV, GRP, and DSR concerning delay and throughput under heavy FTP traffic.	Simulations were conducted using OPNET. PDR was not analysed as a performance metric.
Shankar and Chelle (2016)	AODV, DSDV, DSR, OLSR	Their simulations show that OLSR and DSDV perform best in densely populated networks with a low node mobility rate. Whereas AODV was better suited for networks with a larger number of nodes and DSR performed well in low-density networks with a low node mobility rate.	The protocols under review were not simulated under Black Hole attack to understand its effects on network performance.
Singh and Choundary (2017)	AODV, OLSR	Their results show that a larger number of nodes and increased route requests have a more significant effect on the performance of the MANET.	DSR was not considered for comparison.

Singh and Khurana (2017)	DSR, OLSR, ZRP	The results of their simulations proved that ZRP is a more reliable protocol in terms of delay and throughput than OLSR and DSR.	AODV was not considered for comparison. The network density used is not indicative of modern-day real-world networks.
Khurana, Kumar and Sharma (2017)	AODV, DSR, ZRP	Their study evaluated the performance of AODV, DSR and ZRP, with the number of packets transmitted, packets errored, packets collided and throughput as performance evaluation criteria, to determine how they handle congestion, as congestion is considered a limiting factor that deteriorates the performance of a network. The simulation results found that the AODV protocol performed better and is more effective in controlling congestion in MANETs.	OLSR was not considered for comparison. The protocols under review were not simulated under Black Hole attack to understand its effects on network performance.
Nurcahyani and Hartadi (2018)	AODV, DSR	Their simulations show that AODV had a lower decrease in throughput than DSR when exposed to both single and collaborative Black Hole attacks. DSR also experienced a more considerable packet loss under collaborative Black Hole attack.	OLSR was not considered for comparison.
Nabou, Laanaoui and Ouzzif (2018)	AODV, OLSR	The evaluation of these routing protocols under Black Hole Attack was carried out by varying two important parameters in the mobility environment, namely, the number of nodes and the pause time. The results of different metrics show that AODV is more vulnerable to the Black Hole in both scenarios.	DSR was not considered for comparison. Node mobility speed was not considered as a variation parameter.
Panda and Pattanayak (2018)	AODV, DSR	Black Hole attack with performance parameters end-to-end delay, PDR, and throughput. The results of their study showed that in terms of end-to-end delay and throughput, DSR performed better than AODV under Black Hole attack. Whereas in terms of PDR, AODV performed better than DSR under Black Hole attack.	OLSR was not considered for comparison.

Kuyoro *et al.* (2018)	AODV, DSDV, OLSR, TORA	The susceptibility of these protocols was analysed and based on the analysis of simulated results it was concluded that the impact of Black Hole attack is more severe on AODV and OLSR in the reactive and proactive protocols, respectively.	DSR was not considered for comparison.
Jubair *et al*. (2018)	AODV, OLSR	Their study uses simulations to examine the performance of the routing protocols based on the number of nodes in the network and the size of the network terrain. The results of their simulations show that the AODV outperforms the OLSR in most scenarios and further show that the number of nodes and network terrain size has a great impact on the performance of both routing protocols.	DSR was not considered for comparison. The protocols under review were not simulated under Black Hole attack to understand its effects on network performance.
Chandan and Mishra (2019)	AODV	The result of their study shows that PDR and average throughput decreased while end-to-end delay (EED) increased under Black Hole attacks.	DSR and OLSR were not considered for comparison.
Kalakar, Ali and Chack (2020)	AODV, OLSR	Their simulations showed that the Black Hole attack had a marginally greater effect on the end-to-end delay of AODV compared to OLSR and the throughput of AODV decreased by almost two times more than the throughput of OLSR. However, the effect of the Black Hole attack on the network load of AODV was less than that of OLSR.	DSR was not considered for comparison.
Khan, Akre and Saeed (2021)	OLSR, DSR	The results obtained from the OPNET Modeler 14.5 simulations show that Black Hole attacks significantly degraded the performance of both DSR and OLSR. However, the performance degradation of DSR was more severe than the performance of OLSR in the presence of a Black Hole attack.	AODV was not considered for comparison.

5.3 Summary

This chapter provided a summary of the work previously conducted related to AODV, DSR and OLSR, while under regular operation and Black Hole attack to identify any shortcomings or research gaps. The next chapter provides an overview of the simulation environment detailing the simulation controls and parameters used and the modifications made to the NS2 source code.

Chapter 6 – Simulation Implementation and Simulation Environment

6.1 Introduction

The purpose of this study is to analyse the performance of the AODV, DSR and OLSR routing protocols under Black Hole attack to determine which protocol is most effective in reducing and withstanding the impact of the attack. It is essential to see the effect a malicious node has on the network to understand how the malicious node disrupts the regular operation of the network.

The purpose of using simulations to gather data is to ensure that results are consistent and reproducible. Setting up physical networking environments consisting of multiple computers and routers to carry out networking research can be a costly undertaking. Using simulators to generate these networking environments can save money and time while accomplishing the research goals. Simulations are relatively easy to configure and execute. The disadvantage of using a simulation tool is that some parameters will need to be assumed. It is difficult and costly to accurately replicate the real world in a computer model (Khandelwal, 2018). However, if all factors are kept consistent and as close to reality as possible, then the routing protocol being investigated should not be adversely affected by any unintentional external forces or factors. For these reasons, a simulator-based approach has been chosen for this study.

The Network Simulator (NS2) was selected to simulate and conduct all the experiments for this study, specifically version NS2.35. NS2 is an event-driven network simulator developed at the University of California Berkley, which is used extensively in network research (Mohanapriya & Krishnamurthi, 2014). NS2 is an open-source environment that allows the creation of new routing protocols and modification of existing ones. Each NS2 simulation requires a scenario file and a connection file. The scenario file contains detailed information about each node's movement, packet creation, and the time when each change in movement or packet creation is to occur. The connection file describes how the nodes will communicate and how the network traffic will be routed (Khandelwal, 2018).

After each simulation was run, a detailed trace file containing all events happening during the simulation, such as the number of packets delivered successfully, routes taken by packets, and other detail relating to the internal operations of the simulation network,

was produced. Once the trace files were created, the data was analysed using an AWK script, a programming language designed to process text files, and Microsoft Excel to produce the necessary visual aids.

There is a need for a deeper understanding of mobility models and their impact on the performance of a routing protocol. Random Mobility Models are often used in various network simulation scenarios; however, these mobility models are not suitable for all simulation scenarios. To address the shortcomings of Random Mobility Models, researchers have proposed ways to model the movement of the nodes based on the specific needs of a simulation scenario.

This chapter provides an overview of the simulation environment detailing the simulation controls and parameters used along with the modifications applied to implement OLSR and Black Hole attacks in NS2. A review of existing mobility models is provided in this chapter to assist in determining which mobility model is best suited for MANET type simulations. Finally, a demonstration of what happens within NS2 during a simulation is shown.

6.2 NS2 code Modifications and Implementation

AODV, DSR and OLSR were simulated under regular operation and in the presence of Black Hole using the NS-2.35 network simulator. AODV and DSR are already implemented as part of the standard NS2 distribution. It should be noted that the OLSR protocol is not implemented as part of the standard NS2 distribution. However, open-source modification patches are available, allowing OLSR to be compiled into any existing implementation of NS2. Black Hole attacks can also be implemented by modifying the source code of the various routing protocols as these attacks are not part of the standard NS2 distribution.

6.2.1 Black Hole attack implementation in AODV

In the aodv.h file, the Black Hole node variable is declared.

```
//Blackhole node
  bool blackhole;
```

In the constructor of the aodv.cc file, the new variable is initialised as false to ensure all nodes defined are not initialised as Black Hole nodes by default.

```
//Blackhole node
  blackhole = false;
```

In the aodv.cc file, the code below was added to the AODV::command function to detect if a node is a Black Hole node.

```
//Blackhole node
  if(strncasecmp(argv[1], "blackhole",9) == 0) {
     blackhole = true;
     return TCL_OK;
  }
```

In the aodv.cc file, the code below was added to the AODV::rt_resolve function to drop packets received by a node if the node is a Black Hole node.

```
//Blackhole node
 if (blackhole == true) {
   if (ch->ptype() == PT_CBR) {
      drop(p, DROP_RTR_ROUTE_LOOP);
      return;
   }
 }
```

In the aodv.cc file, the code below was added to the AODV::recvRequest function to advertise the Black Hole node as having the shortest path when it receives a request.

```
//Blackhole node
 else if(blackhole == true)
 {
   seqno = max(seqno, rq->rq_dst_seqno)+1;
   if (seqno%2) seqno++;
       sendReply(rq->rq_src,
                 1,
                 rq->rq_dst,
                 seqno,
                 MY_ROUTE_TIMEOUT,
                 rq->rq_timestamp);
                 //rt->pc_insert(rt0->rt_nexthop);

  Packet::free(p);
 }
```

6.2.2 Black Hole attack implementation in DSR

In the DSRagent.h file, the Black Hole node variable is declared.

```
//Blackhole node
  bool blackhole;
```

In the constructor of the DSRagent.cc file, the new variable is initialised as false to ensure all nodes defined are not initialised as Black Hole nodes by default.

```
//Blackhole node
  blackhole = false;
```

In the DSRagent.cc file, the code below was added to the DSRAgent::command function to detect if a node is a Black Hole node.

```
//Blackhole node
  if(strncasecmp(argv[1], "blackhole",9) == 0) {
     blackhole = true;
     return TCL_OK;
  }
```

In the DSRagent.cc file, this code was added to the DSRAgent::handleForwarding function to drop packets received by a node if the node is a Black Hole node.

```
//Blackhole node
  if (blackhole == true) {
    if (ch->ptype() == PT_CBR) {
       drop(p.pkt, DROP_RTR_ROUTE_LOOP);
       return;
    }
  }
```

6.2.3 Black Hole attack implementation in OLSR

In the OLSR.h file, the Black Hole node is declared.

```
//Blackhole node
  bool blackhole;
```

In the constructor of the OLSR.cc file, the new variable is initialised as false to ensure all nodes defined are not initialised as Black Hole nodes by default.

```
//Blackhole node
  blackhole = false;
```

In the OLSR.cc file, the code below was added to the OLSR::command function to detect if a node is a Black Hole node.

```
//Blackhole node
  if(strcasecmp(argv[1], "blackhole") == 0) {
     blackhole = true;
     return TCL_OK;
  }
```

In the OLSR.cc file, this code was added to the OLSR:: recv function to drop packets received by a node if the node is a Black Hole node.

```
//Blackhole node
  if(blackhole==true) {
    drop(p,DROP_RTR_ROUTE_LOOP);
  }
```

After modifying the existing NS2 source code to incorporate the Black Hole nodes and the OLSR routing protocol, it was recompiled using the "make clean" and "make" command in the ns-2.35 home directory.

6.3 Mobility Models

The purpose of a mobility model is to describe the movement pattern of nodes in a network concerning how their location, velocity, and acceleration change over time. Mobility models aim to emulate the movement pattern of a targeted real-life application. Therefore, mobility models need to provide accurate and reliable position information as close as possible to the real-world scenario being simulated and researched. When assessing MANET routing protocols, the appropriate underlying mobility model must be

selected based on the type of research being conducted (Bai & Helmy, 2004). If the incorrect mobility model is selected, the observations and conclusions drawn from the simulation studies may be misleading.

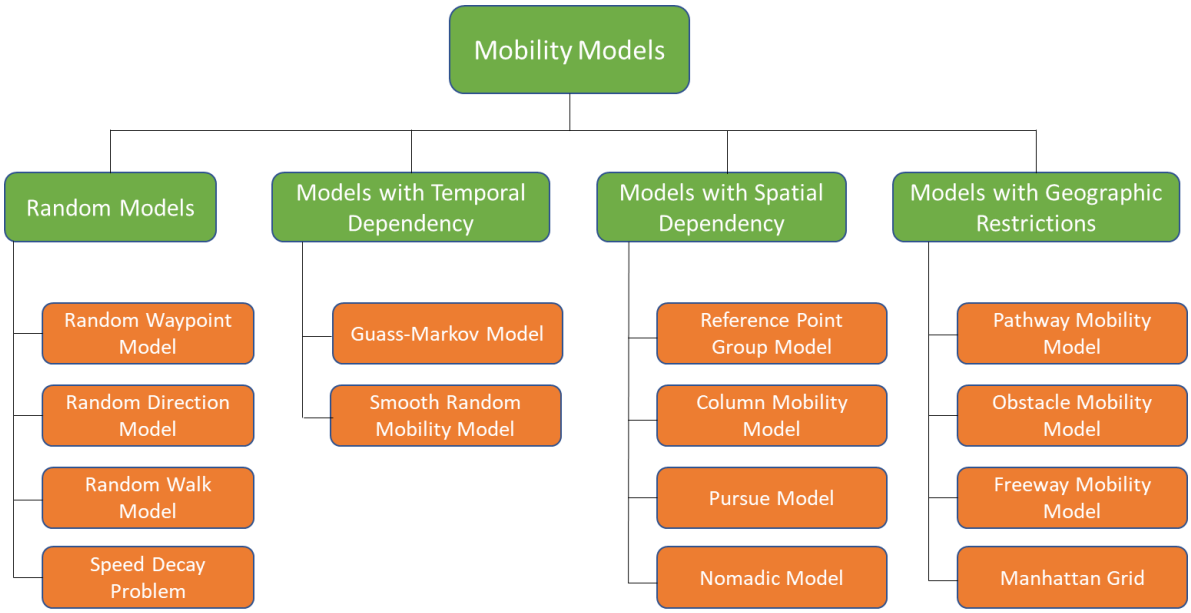

Figure 6.1 – Classification of Mobility Models in MANETs

Figure 6.1 shows the classifications of the different mobility models. In this section, we will briefly explain the operations of these models.

6.3.1 Random Models

Random Mobility Models allow nodes to move randomly and freely, without any restriction, which means that the direction, velocity, and destination is chosen randomly and independently of any other node. Random Models are sometimes called entity models because nodes are considered entities that move and act independently (Vinayagam, 2014). The Random Waypoint, Random Walk, and Random Direction models are considered among the more popular random mobility models.

Random Waypoint Model

The Random Waypoint Mobility Model (RWPMM) allows nodes to emulate natural movement in scenarios requiring extreme and unpredictable direction and speed changes. A mobile node will begin by waiting in one location for a certain period and then move to another location by choosing a random destination and a uniformly distributed speed between the defined minimum and maximum speeds. The RWPMM has three parameters, namely pause time, movement speed, and node position allocation. The RWPMM nodes randomly select a direction and speed to reach its destination (or waypoint). Upon arrival at the destination, the mobile node pauses for a specified period,

allowing it to change its direction and speed before starting the process again (Manoharan & Ilavarasan, 2010).

The RWPMM was first proposed by Johnson and Maltz (1996). The RWPMM is simple to use and widely available in most network simulation software, making it one of the most popular mobility models used to evaluate MANET routing protocols. The shortfall of the RWPMM is that it does not cater for regular movement patterns, nor does it contain a mechanism that keeps track of historic movement behaviours (Gupta, Sadawarti & Verma, 2013).

Figure 6.2 shows the movement trace of how a node, denoted by the orange dot, in the RWPMM moves within the simulation area, with random speed to the different waypoints until reaching its destination, denoted by the green dot.

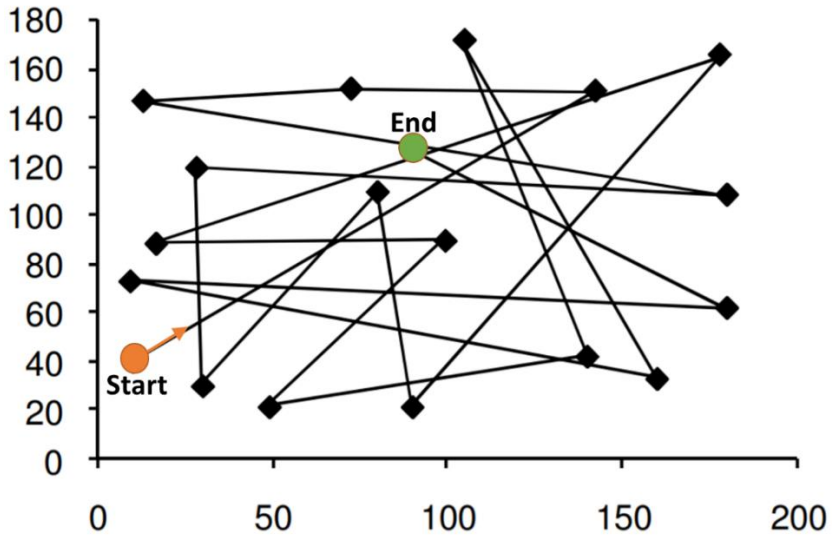

Figure 6.2 – Movement Pattern of the Random Waypoint Mobility Model

Random Walk Model

In the Random Walk Mobility Model (RWMM), a mobile node randomly and uniformly chooses a direction and speed at which to move. RWMM has seven parameters, namely pause time, movement speed, time, distance, mode (either based on time or distance), movement direction, and area bounds. Based on the defined mode parameter, either after a fixed time has passed or a certain distance has been travelled, a new direction and speed are calculated and assigned to the node for it to follow. If the node reaches the border of the network area, it is bounced back into the network area at the same speed it arrived and continues moving until new instructions are issued; this effect is called the Border Effect. The RWMM is a memoryless mobility process that does not retain any information about a node's previous state when moving to the next destination (Nisar, Mehmood & Nadeem, 2013).

The RWMM was initially proposed and mathematically described by Albert Einstein to emulate the unpredictable movement of particles in physics (Bai & Helmy, 2004). The RWMM has similarities with the RWPMM model as the node movement has strong randomness in both models. RWMM can also be considered an RWPMM with zero pause time. The RWMM is the simplest mobility model to implement. It generates unpredictable movements, allowing long-running simulations to consider all locations and all types of node interactions. However, the RWMM can create unrealistic movement patterns with sharp and sudden turns. RWMM is also referred to as the Brownian Motion Mobility Model or Brownian Walk (Gupta *et al.*, 2013).

Figure 6.3 shows the movement trace of how a node, denoted by the orange dot, in the RWMM moves within the simulation area, with random speed and direction, until reaching its destination, denoted by the green dot.

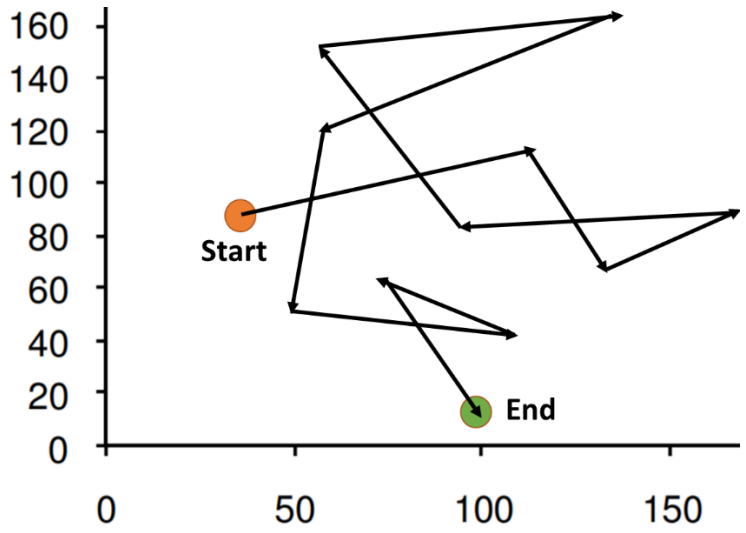

Figure 6.3 – Movement Pattern of the Random Walk Mobility Model

Random Direction Model

In the Random Direction Mobility Model (RDMM), a node chooses a random direction and speed, then moves in the chosen direction until it arrives at the border of the network area. The node then halts for a specified pause time and will select a new direction to move in and continue doing this until the end of the simulation (Vinayagam, 2014). RDMM has three parameters, namely pause time, movement speed, and area bounds. Due to the mobile nodes travelling to the border of the network area and then pausing for some time, the average hop count for packets is much higher than other mobility models (Nisar *et al.*, 2013).

The RDMM was created to overcome a flaw discovered in the RWPMM. In the RDMM, a mobile node will choose a random direction instead of a random destination. However, the RDMM generates unrealistic movement patterns resulting in the average distances

between mobile nodes being much higher than in other mobility models, leading to incorrect results during routing protocol evaluation (Gupta *et al.*, 2013).

Figure 6.4 shows the movement trace of how a node, denoted by the orange dot in the RDMM moves within the simulation area, with random speed and direction, to its end location, denoted by the green dot.

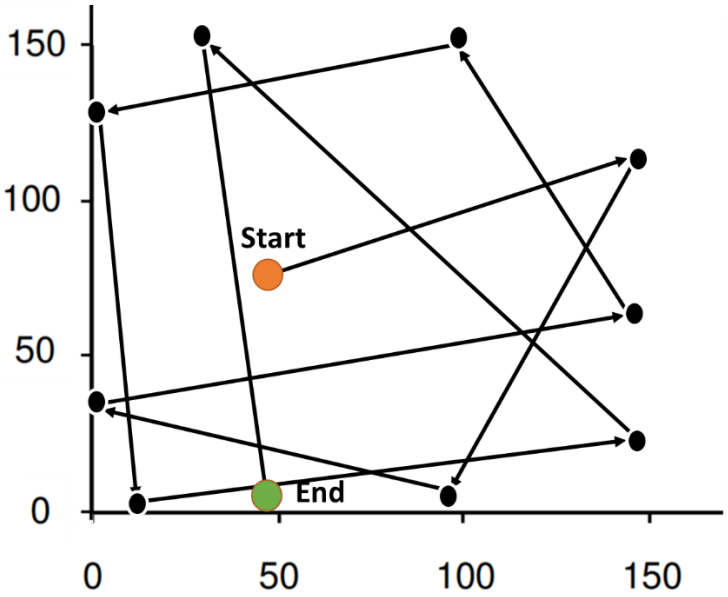

Figure 6.4 – Movement Pattern of the Random Direction Mobility Model

6.3.2 Models with Temporal Dependency

In Random Mobility Models, the velocity of a node is a memoryless random process, which means that a node's current speed is independent of its historic speed (Nisar *et al.*, 2013). The use of Random Mobility Models results in extreme and erratic mobility behaviour, such as sudden stops, sudden acceleration, and sharp turns, being generated by Random Mobility Models. In real-world scenarios, such as the speed of vehicles and pedestrians, nodes will accelerate incrementally and change directions smoothly and seamlessly (Bai & Helmy, 2004). For this reason, and in specific scenarios, the speed of a node at different time intervals is interrelated and should be aware of the speed at previous time intervals. This mobility characteristic of nodes is known as Temporal Dependency. The Gauss-Markov Mobility Model and Smooth Random Mobility Model are considered among the more popular mobility models with Temporal Dependency.

Gauss-Markov Mobility Model

Mobile nodes are allocated in random locations within the wireless network (Gupta *et al.*, 2013). However, the movement of each node is still independent of any other node within the same network. The Gauss-Markov Mobility Model (GWMM) aims to improve the shortcomings of the Random models by using temporal dependency as a factor, i.e., the

speed and direction of a mobile node are updated according to its past values at earlier periods.

Figure 6.5 depicts a node's movement trace in GWMM. The GWMM avoids the RWMM's abrupt stops and quick turns by enabling previous speed and direction to influence current and future speed and direction.

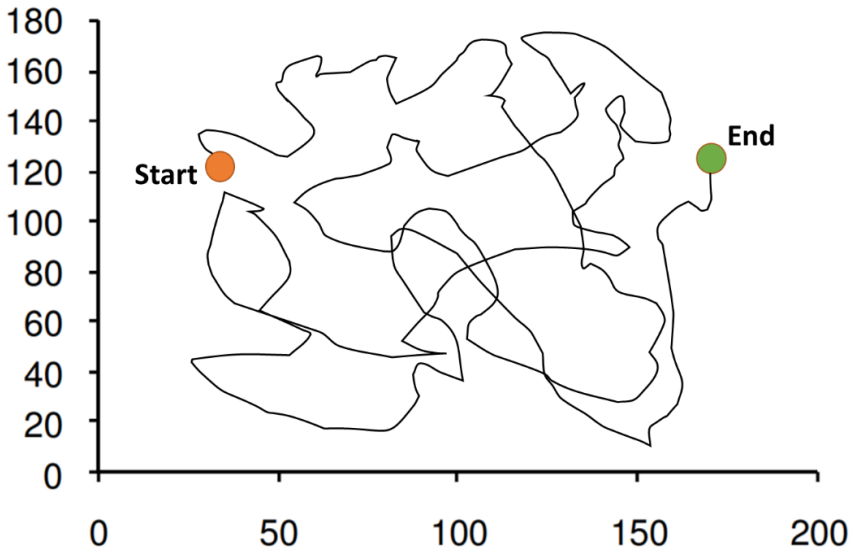

Figure 6.5 – Movement pattern of the Gauss-Markov Mobility Model

6.3.3 Models with Spatial Dependency

As mentioned in Random Mobility Models, every node is regarded as an entity. Each node is different from every other node in terms of speed, direction, and movement pattern. This renders Random Mobility Models inadequate and unsuitable for use in cases where nodes need to work in a group or when the movement of a member node is influenced by a leader node, for example, in disaster relief scenarios. Simulation scenarios that require nodes to work together should use Spatial Dependent mobility models (Vinayagam, 2014). Nodes with Spatial Dependent mobility are correlated and can function with a leader (Nisar *et al.*, 2013). The Reference Point Group Model and Pursue Model are considered among the more popular mobility models with Spatial Dependency.

Reference Point Group Mobility Model

The Reference Point Group Mobility Model (RPGMM) is a group mobility model representing the random motion of a group of mobile nodes and the random motion of each node within a group (Bai & Helmy, 2004). In the RPGMM, each group has a logical centre or a group leader node. Each group is composed of one leader and multiple member nodes. The group leader's movement completely defines the movement of its related group member nodes, including their direction and speed. As such, the

movement of the group leader determines the mobility behaviour of the entire group via a group motion vector. RPGMM is prevalent in many scenarios that demand group communications. (Manoharan & Ilavarasan, 2010).

Figure 6.6 depicts the RPGMM with the group leader represented in green and the members represented in red and yellow, respectively. V_{group} is the group leader's motion vector, and this motion vector is also assigned to the members of the group.

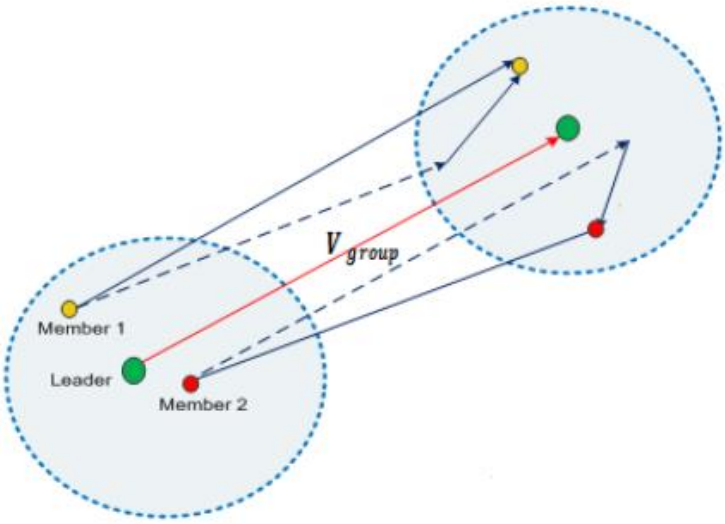

Figure 6.6 – RPGMM Group leader and Group interactions (Husieen & Rasheed, 2015)

6.3.4 Models with Geographic Restrictions

In Random Mobility Models, nodes move freely within the simulation field without restrictions (Nisar *et al.*, 2013). However, in many real-world scenarios, the movement of a node might be restricted by obstacles, buildings, streets, or freeways. For this reason, researchers have proposed mobility models that allow for Geographic Restrictions (Bai & Helmy, 2004). The Manhattan Grid and Freeway Mobility Model are considered among the more popular mobility models with Geographic Restrictions.

Manhattan Grid

In the Manhattan Grid Model, the mobile nodes emulate the movement patterns like that of streets on a map. Manhattan Grid models use a grid road topology composed of several horizontal and vertical streets to define movement patterns (Manoharan & Ilavarasan, 2010).

The node's speed is dynamic but dependent on the previous speed of the node. The Manhattan Grid model is designed to maintain a certain distance between nodes travelling in the same direction. Nodes are allowed to move along the grid of horizontal and vertical streets on the map. Each street has two lanes, one for each direction. At an intersection of a horizontal and a vertical street, nodes can turn left, turn right, or move

straight through. The probability of a node moving straight is 0.5. The probability of a node changing its direction either vertically or horizontally is 0.25 (Rangaraj & Anitha, 2017).

Figure 6.7 shows the movement pathways of nodes in a typical Manhattan Grid Mobility Model.

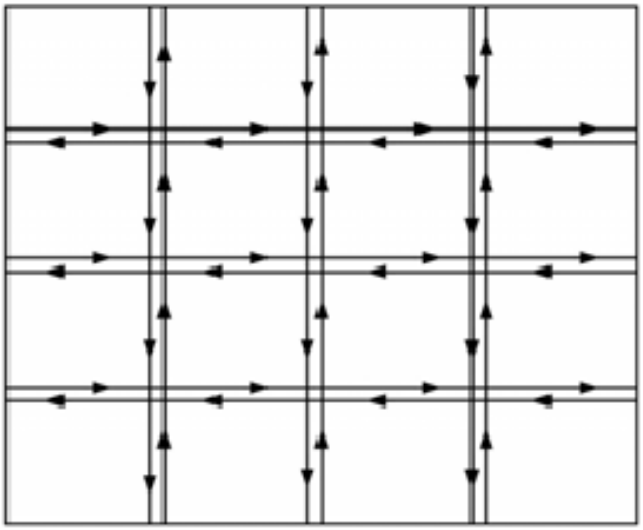

Figure 6.7 – Manhattan Grid Model (Gueraa, Rachid & Aboutajdine, 2015)

6.4 Simulation Environment and Simulation Parameters

The simulations for this study were done on a square area of 750m X 750m. The number of nodes per simulation ranges from 20 to 60, and the nodes move at maximum speeds ranging from 20m/s to 100m/s. The packets are broadcast at the rate of 4 packets/sec, generated at a constant bit rate (CBR) with a data packet size of 512 bytes.

The User Datagram Protocol (UDP) was chosen as the transport layer protocol. UDP allows for connectionless communication and is primarily used to establish low-latency and loss tolerating connections between nodes. UDP enables data transfer to start before an acknowledgement is received; this is beneficial for the simulation of Black Hole attacks as data transmission will continue even when a malicious node discards the data being transmitted. If the Transmission Control Protocol (TCP) were used, the source node would stop transmitting data packets if the recipient's acknowledgement packet was not received.

The Random Waypoint model was chosen as the mobility model to create the simulations in this research as it provides an adequate representation of real-world mobile node movements. The Random Waypoint model allows nodes to be placed at random, different locations in a network and then uses the specified speed and pause

time parameters to generate the necessary node movements. Nodes travel within the specified speed ranges towards a randomly selected destination node. Once it reaches that destination, the node pauses for a specific time before selecting another destination node, repeating this process until the end of the simulation.

AODV, DSR and OLSR were implemented as the network layer routing protocols. Each simulation ran for 500 seconds.

Table 6.1 depicts the parameters used during the various simulations.

Table 6.1 – Simulation Parameters

Protocols	AODV, DSR and OLSR
Simulation Time	500 seconds
Terrain	750m x 750m
Number of Nodes	20, 30, 40, 50, 60
Connections	1, 2, 3, 4, 5
Mobility (m/s)	20, 40, 60, 80, 100
Mobility Model	Random Waypoint Model
Traffic Type	CBR

The main goal of this study was to determine which protocol amongst AODV, DSR and OLSR performed better under the Black Hole attack. The same mobility model and connection patterns were utilised throughout the simulations for consistency. It should be noted that only one parameter changed per simulation to ensure the quality of data and to ensure only one factor influenced the results obtained.

6.5 Simulation Illustration

Figure 6.8 and Figure 6.9 illustrates, with the use of a NAM visual simulation, how a network performs while under regular operation and while under Black Hole attack. *Node 1,* denoted in blue, is the source node, *node 5,* denoted in green, is the destination node, and *node 6,* denoted in red, is a malicious Black Hole node.

Figure 6.8 illustrates a simulation in a network under regular operation with no attack; as such, the destination node, *node 5*, receives data packets sent by the source node, *node 1*.

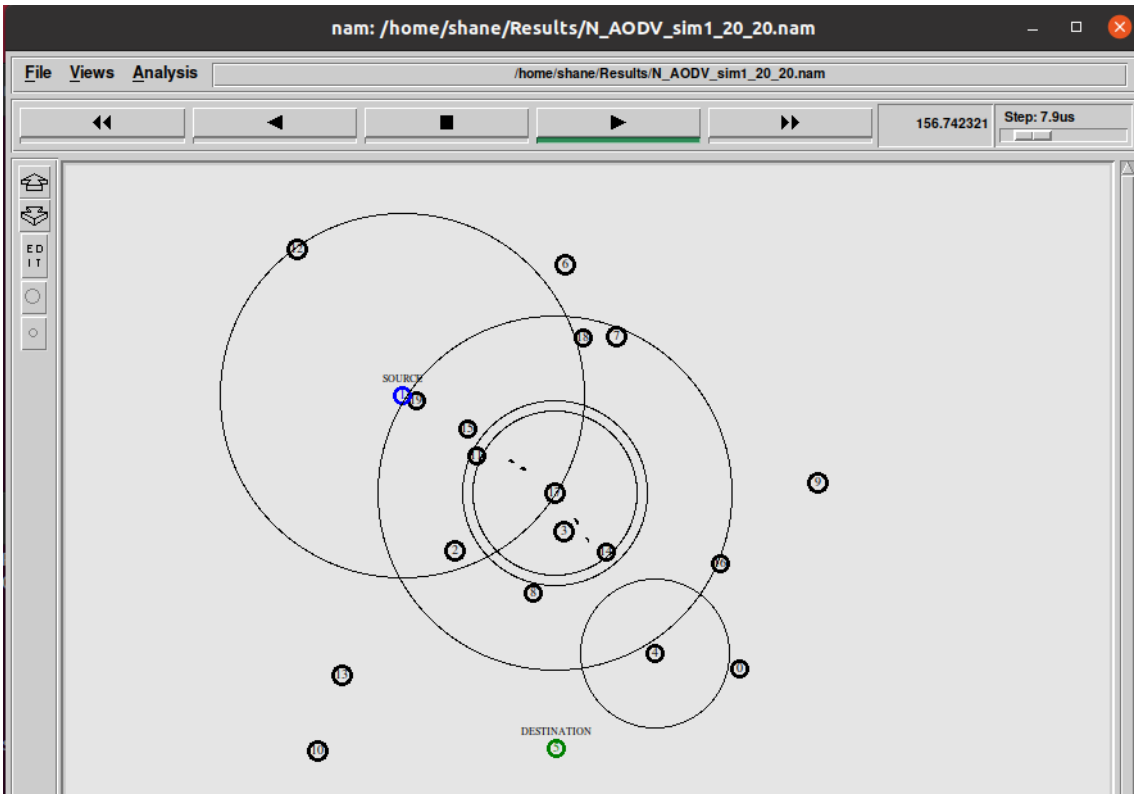

Figure 6.8 – NAM Simulation: MANET under Regular Operation

Figure 6.9 illustrates a network under Black Hole attack, with a Black Hole node (*node 6*) absorbing data packets from the source node (*node 1*) instead of sending them to the destination node (*node 5*).

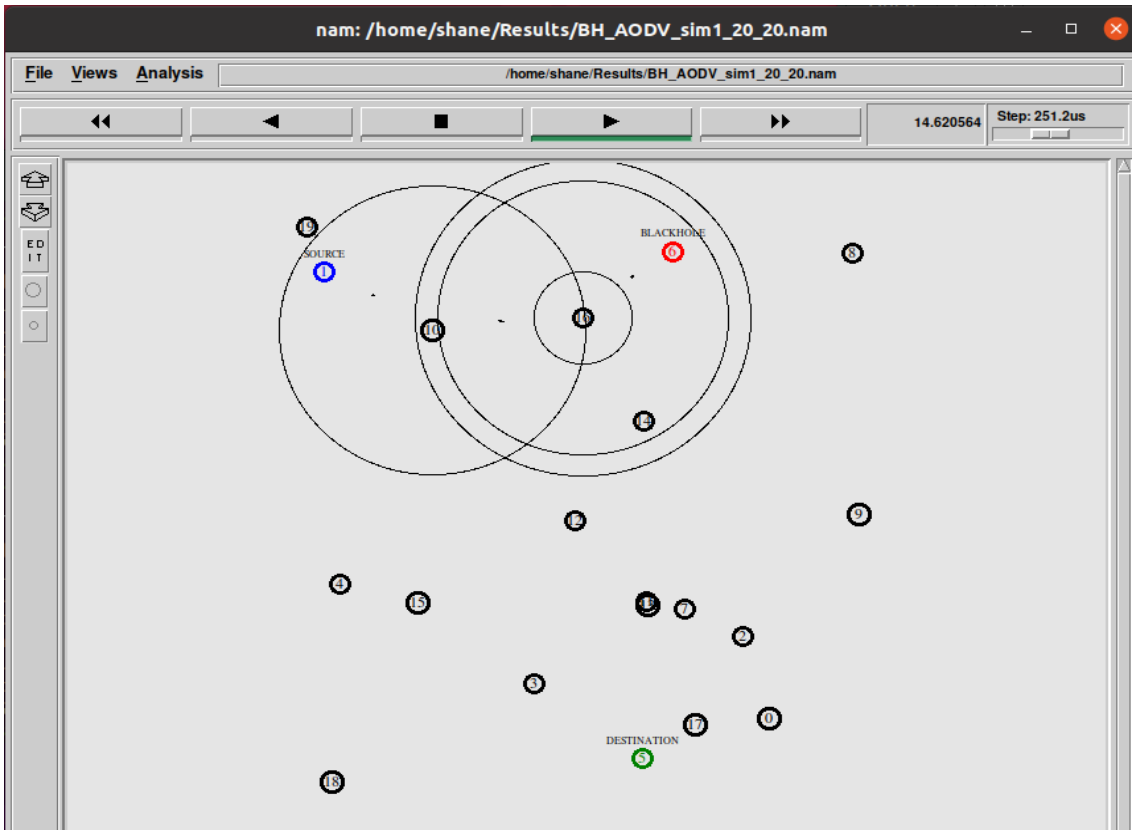

Figure 6.9 – NAM Simulation: MANET under Black Hole Attack

6.6 Summary

This chapter presented the description of the simulation environment detailing the simulation controls and parameters used. NS2 was also chosen as the simulation tool used in this study based on its capability and adaptability. Next, the modifications made to the NS2 source code to implement OLSR and Black Hole attacks in AODV, DSR and OLSR were explained. The Random Waypoint model was chosen as the mobility model to create the mobility scenarios for the simulations in this research as it provided an adequate representation of real-world mobile node movements. However, based on the nature of this study, it is essential to understand the effects that different mobility models have on the performance of a MANET under regular operation and under Black Hole attack to ascertain the viability of the different mobility models should a particular simulation scenario require it. As such, the mobility models classified as part of the Random Model category will also be simulated to analyse the performance of the different mobility models.

The next chapter presents the results and performance information obtained from the NS2 simulations.

Chapter 7 – Simulation Results and Analysis

7.1 Introduction

This chapter provides an overview of the performance metrics used to evaluate the routing protocols and describes how the results were retrieved from the NS2 trace files. Those results were analysed using the chosen performance metrics and presented using graphs.

7.2 Performance Metrics

Many different performance evaluation metrics can be used to evaluate routing protocols. The following quantitative metrics were chosen to evaluate the performance of the AODV, DSR and OLSR routing protocols:

7.2.1 Throughput (TH)

TH is the amount of data transferred or received per second successfully over a communication channel. It is the ratio of data received from the sender to the total time consumed in transmitting the entire message to the destination. The data traffic is represented in bits per second. Throughput can suffer due to low bandwidth, limited energy, change in topology and untrusted communication.

$$TH = \frac{\sum data_{bits\ received}}{Simulation\ time}$$

The higher the throughput, the better the performance.

7.2.2 End-to-End Delay (EED)

EED is the average time a packet takes to reach the destination node from the source node. Delays can occur throughout the transmission process from the source node to intermediate nodes right towards the destination node. It includes transmission delay, propagation delay, processing delay and queuing delay. The average end-to-end delay can be calculated by summing the times taken by all received packets divided by the total number of packets received. It is expressed in milliseconds (ms).

$$EED = \frac{\sum(Time_{Received} - Time_{Sent})}{\sum Time_{Received}}$$

The lower the EED value, the better the protocol's performance.

7.2.3 Packet Delivery Ratio (PDR)

PDR is the ratio of the successful data packets received at the destination node over the number generated from the source node. It measures the protocol's reliability in action and is expressed as a percentage.

$$PDR = \frac{\sum data\ packets_{Successfully\ Received}}{\sum data\ packets_{\ Sent}} \times 100$$

The higher the PDR percentage, the better the performance of the network.

7.3 Simulation Results – Routing Protocols

The results of the Black Hole attack simulations are shown by the graphs created using the data extracted by the AWK scripts. The simulation scenarios aim to show the effect on the performance of AODV, DSR, and OLSR when there is no attack and in the presence of a Black Hole attack while varying the number of mobile nodes, speeds, and traffic loads within the simulation network.

For each scenario, two simulations were conducted 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. As mentioned, the performance metrics of throughput (TH), end-to-end delay (EED), and packet delivery ratio (PDR) were used to analyse the performance of the network. The following parameters were changed during the simulations to determine the effect each parameter had on the simulation performance:

a. **Network Density**: By varying the number of mobile nodes in the network.
b. **Network Mobility Speed**: By changing the speed of node movements in the network.
c. **Network Traffic Load**: By changing the number of connections between nodes in the network to increase or decrease the network traffic.

The average results of six simulation runs were analysed and compared to determine which protocol performs better while under Black Hole attack. Additionally, multiple simulations assist in determining the average effect of the attack over multiple positions, as the position of the malicious Black Hole node can affect the network in several ways. For example, if a Black Hole node is positioned closer to the source node, it can cause more damage than if the Black Hole node is further away. Only one parameter was modified per simulation to ensure differences in results were attributed to the correct parameter modification.

7.3.1 Network Density

In this scenario, the number of nodes in the network changed per simulation, starting with 20 nodes and increasing by ten nodes for each subsequent simulation, until the network contained a maximum of 60 nodes, with the node mobility speed set at 20 m/s and only one active data transmission connection. All three protocols, AODV, DSR and OLSR, were simulated to evaluate the performance of the MANET under regular operation as well as under Black Hole attack, using the performance metrics of throughput (TH), end-to-end delay (EED) and packet delivery ratio (PDR) as shown by the graphs in this section.

Table 7.1 shows the summarised results of the simulations conducted while varying the number of nodes in the MANET.

Table 7.1 – Summary of Network Density Simulation Results

Protocol	Density	Speed (m/s)	Connections	Blackholes	TH (Kbps)	EED (ms)	PDR (%)
AODV	20	20	1	0	16.27	214.18	95.33
DSR	20	20	1	0	15.99	270.91	97.17
OLSR	20	20	1	0	12.74	15.21	74.67
AODV	20	20	1	1	7.87	38.74	45.83
DSR	20	20	1	1	11.66	179.22	70.83
OLSR	20	20	1	1	12.71	40.42	78.00
AODV	30	20	1	0	16.74	76.50	98.50
DSR	30	20	1	0	15.81	88.59	96.83
OLSR	30	20	1	0	13.61	30.64	79.67
AODV	30	20	1	1	11.27	33.52	65.67
DSR	30	20	1	1	13.74	71.68	84.17
OLSR	30	20	1	1	13.60	10.04	80.33
AODV	40	20	1	0	16.67	40.68	98.00
DSR	40	20	1	0	15.66	124.02	95.33
OLSR	40	20	1	0	12.82	11.85	75.17
AODV	40	20	1	1	9.69	33.42	53.33
DSR	40	20	1	1	13.68	66.93	83.17
OLSR	40	20	1	1	12.80	90.55	75.50
AODV	50	20	1	0	16.90	33.88	99.17
DSR	50	20	1	0	16.21	82.79	98.33
OLSR	50	20	1	0	14.49	9.38	85.00
AODV	50	20	1	1	11.94	10.39	66.17
DSR	50	20	1	1	16.03	48.53	93.50
OLSR	50	20	1	1	14.49	10.58	85.00
AODV	60	20	1	0	16.78	38.24	98.67
DSR	60	20	1	0	15.63	148.93	95.50
OLSR	60	20	1	0	13.54	38.07	79.33
AODV	60	20	1	1	9.31	21.45	45.83
DSR	60	20	1	1	14.40	111.23	87.33
OLSR	60	20	1	1	13.27	143.61	78.00

Figure 7.1 shows the throughput results of AODV, DSR and OLSR simulations under regular operation, without any attacks, and under Black Hole attack, while varying node density in the network.

Under regular operation, throughput marginally increased as the number of nodes increased. AODV had a higher average throughput at 16.67kbps, while DSR (15.86kbps) and OLSR (13.44kbps) had a lower average throughput. Under Black Hole attack, the average throughput of AODV decreased by 39.94% to 10.01kbps, DSR decreased by 12.35% to 13.9kbps, and OLSR decreased by 0.5% to 13.37kbps. As the MANET node density increased, throughput remained relatively consistent across the simulated scenarios.

The average throughput decreased across all protocols while under Black Hole attack due to some of the data packets being absorbed or discarded by the malicious Black Hole node, reducing the total number of data packets received by the destination node. AODV's throughput drops significantly under Black Hole compared to DSR's and OLSR's under the same Black Hole attack. DSR performs better than AODV and OLSR under Black Hole attacks due to the source routing nature of DSR, which is not dependant upon the routing table of intermediary nodes during the route discovery process.

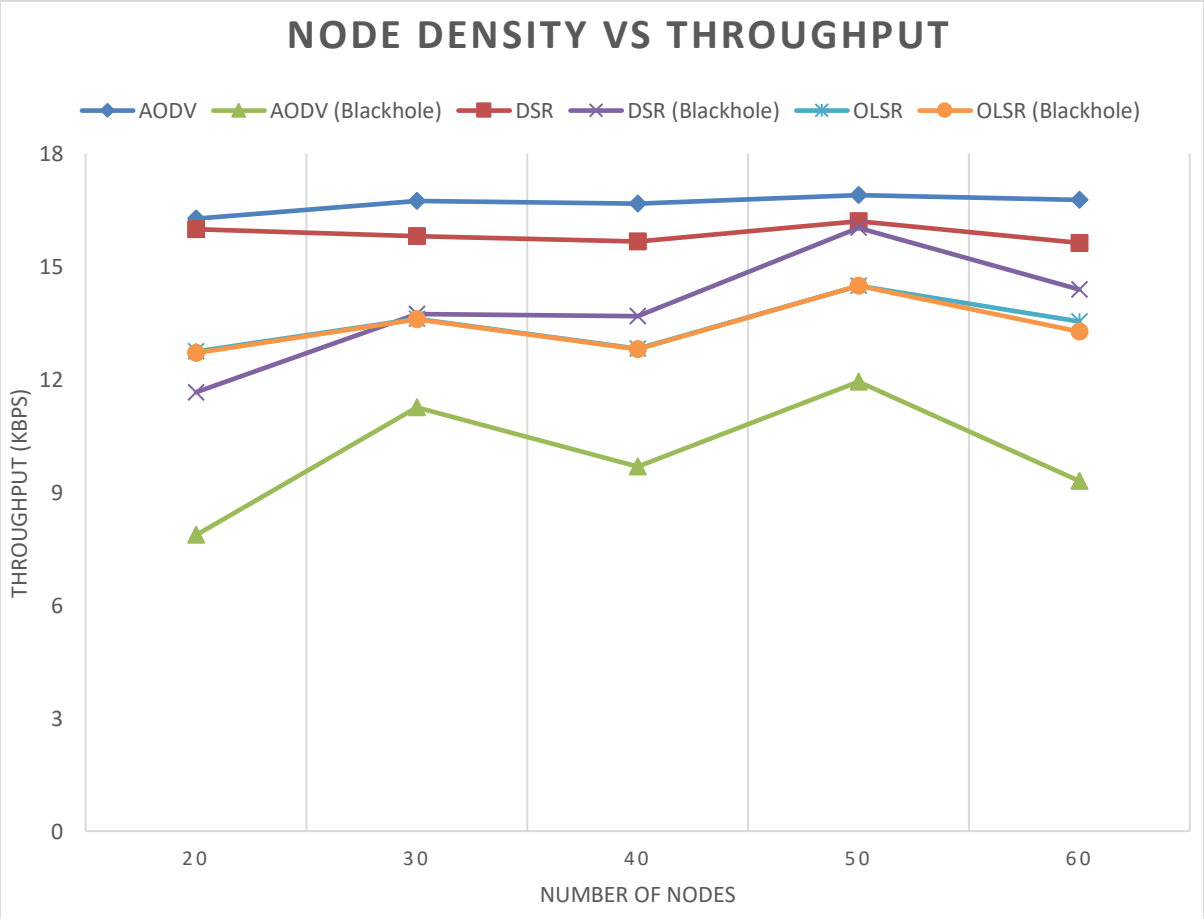

Figure 7.1 – Node Density vs Throughput

Figure 7.2 shows the end-to-end delay of AODV, DSR and OLSR simulations under regular operation, without any attacks, and under Black Hole attack, while varying node density in the network.

Under regular operation, the average end-to-end delay of OLSR (21.03ms) is significantly lower than AODV (80.7ms) and DSR (143.05ms) due to OLSR being a proactive routing protocol, with route calculations and establishment done in advance, for all potential destinations. The end-to-end delay for AODV and DSR under Black Hole attack is reduced, as the Black Hole node responds to the route request immediately without checking the routing table, resulting in a shorter route discovery process time. It can also be observed that there is a higher end-to-end delay in DSR, compared to AODV, due to the significant overhead in keeping complete records of routes from the source node to the destination node, including the intermediate nodes. End-to-end delay is relatively lower when the MANET is under Black Hole attack for AODV and DSR, as the Black Hole node does not have to search for the route in the routing table. Finally, the end-to-end delay of OLSR under Black Hole attack increases slightly. This slight increase in end-to-end delay can be attributed to the malicious Black Hole node pretending to have a valid route between the source and destination node even when the malicious Black Hole node is far away from the source and destination node, resulting in transmission delays.

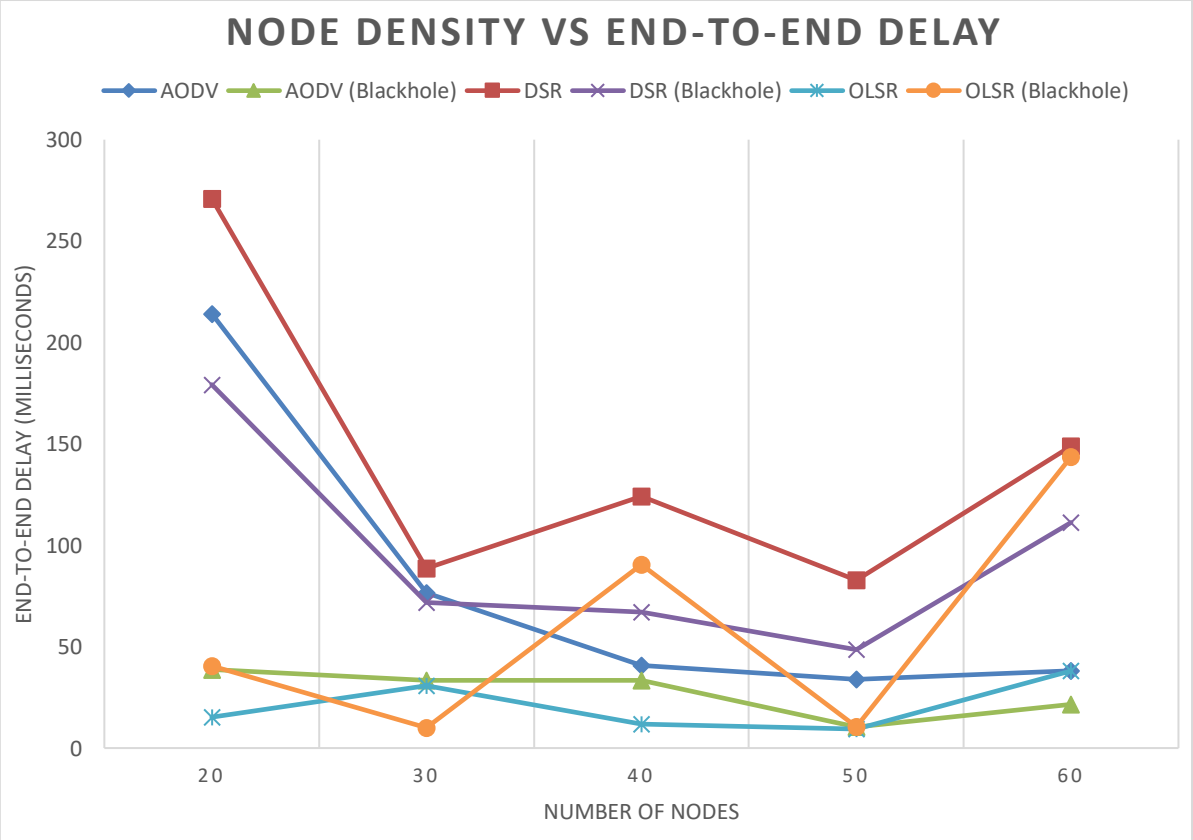

Figure 7.2 – Node Density vs End-to-End Delay

Figure 7.3 shows the packet delivery ratio of AODV, DSR and OLSR under regular operation, without any attacks, as well as under Black Hole attack, with a varying number of nodes.

Under regular operation, as the number of nodes in the MANET increased, the packet delivery ratio remained relatively consistent. The PDR for AODV under regular operation averaged at 97.93%, with DSR and OLSR averaging 96.63% and 78.77%, respectively. Under Black Hole attack, the PDR of AODV decreased on average by 43.46%, which was significantly more than the average decrease in the PDR of DSR and OLSR, at 13.28% and 0.13%, respectively. Despite the lower decrease in the average PDR for OLSR under Black Hole attack, DSR still performed the best under Black Hole attack, upholding an average PDR of 83.8%.

The simulation results show that with an increasing number of nodes in a MANET, there is no significant change to the packet delivery ratio for AODV, DSR and OLSR under regular operation. It can be observed that when the Black Hole attack is introduced into the MANET, the packet delivery ratio is negatively impacted as the Black Hole node discards some packets. A further observation is that when under Black Hole attack, DSR performs better than AODV and OLSR. The PDR of AODV drops significantly during the Black Hole attack.

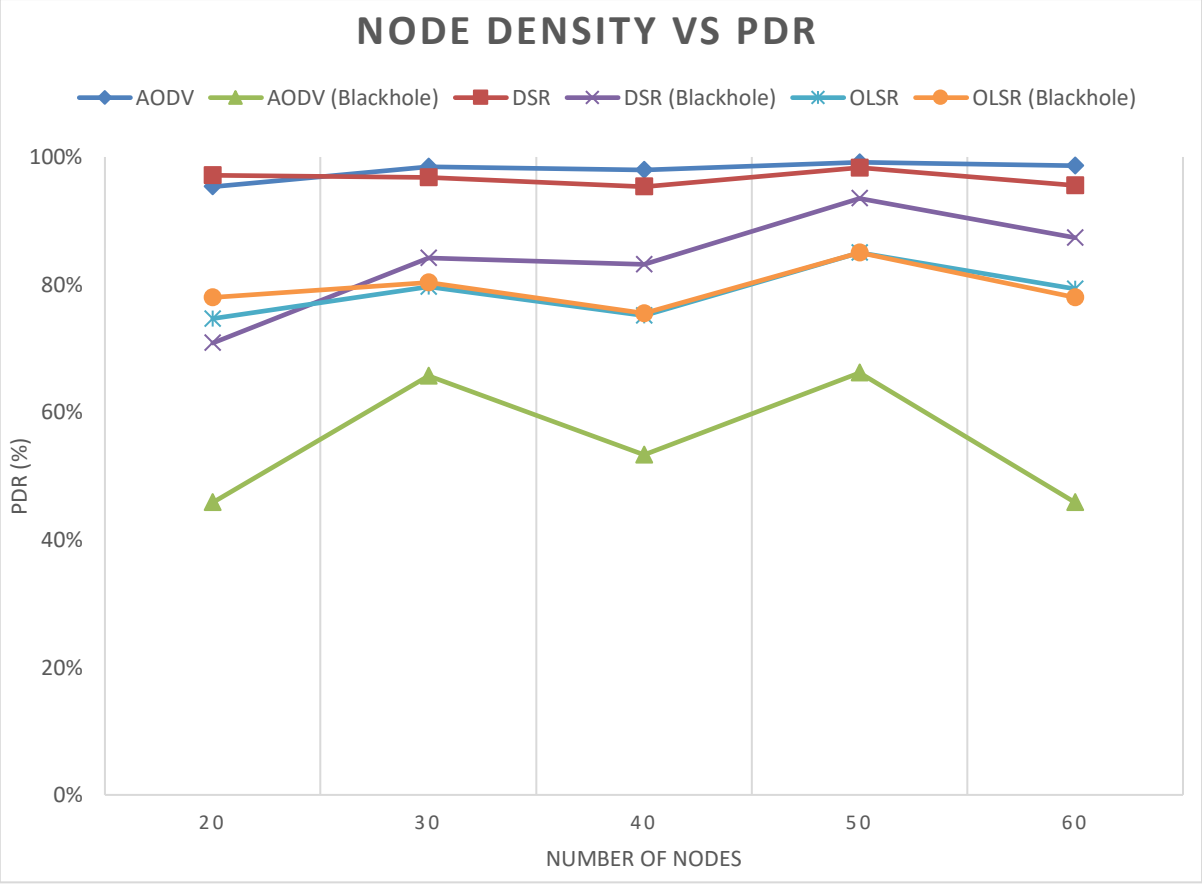

Figure 7.3 – Node Density vs PDR

7.3.2 Network Mobility Speed

In this scenario, the node mobility speed of the nodes in the MANET was changed per simulation, starting at 20m/s and increasing by 20m/s for each subsequent simulation, until the node mobility speed peaked at 100m/s, with the node density set at 20 nodes and only one active data transmission connection. The simulations were conducted across all three protocols, AODV, DSR, and OLSR, to evaluate the performance of the MANET under regular operation as well as under Black Hole attack, using the performance metrics of throughput (TH), end-to-end delay (EED) and packet delivery ratio (PDR) as shown by the graphs in this section.

Table 7.2 shows the summarised results of the simulations conducted while changing the mobility speed of the nodes in the MANET.

Table 7.2 – Summary of Node Mobility Speed Simulation Results

Protocol	Density	Speed (m/s)	Connections	Blackholes	TH (Kbps)	EED (ms)	PDR (%)
AODV	20	20	1	0	16.27	214.18	95.33
DSR	20	20	1	0	15.99	270.91	97.17
OLSR	20	20	1	0	12.74	15.21	74.67
AODV	20	20	1	1	7.87	38.74	45.83
DSR	20	20	1	1	11.66	179.22	70.83
OLSR	20	20	1	1	12.71	40.42	58.00
AODV	20	40	1	0	16.54	86.56	97.00
DSR	20	40	1	0	15.92	236.07	96.67
OLSR	20	40	1	0	10.32	19.49	60.33
AODV	20	40	1	1	8.77	19.86	45.33
DSR	20	40	1	1	12.59	136.65	72.67
OLSR	20	40	1	1	10.21	10.38	59.33
AODV	20	60	1	0	16.19	229.14	94.00
DSR	20	60	1	0	15.80	597.45	96.00
OLSR	20	60	1	0	9.38	60.90	54.67
AODV	20	60	1	1	8.05	49.89	41.83
DSR	20	60	1	1	11.27	172.62	68.33
OLSR	20	60	1	1	9.38	58.23	54.83
AODV	20	80	1	0	15.63	250.62	92.00
DSR	20	80	1	0	15.67	536.99	95.50
OLSR	20	80	1	0	8.40	143.70	49.00
AODV	20	80	1	1	8.39	91.58	47.17
DSR	20	80	1	1	11.09	211.41	67.50
OLSR	20	80	1	1	8.45	68.03	48.67
AODV	20	100	1	0	16.07	201.63	94.83
DSR	20	100	1	0	15.80	306.47	96.33
OLSR	20	100	1	0	10.13	72.03	58.50
AODV	20	100	1	1	8.79	72.56	49.83
DSR	20	100	1	1	12.24	227.17	74.83
OLSR	20	100	1	1	10.04	8.10	58.00

Figure 7.4 shows the throughput results of AODV, DSR, and OLSR under regular operation, without any attacks, and under Black Hole attacks while varying the mobility speed of the nodes in the network.

Under Black Hole attack, throughput decreases due to the malicious Black Hole node discarding data packets being transmitted. AODV's average throughput drops drastically by 48.13%, from 16.14kbps to 8.37kbps, compared to DSR's average throughput, which drops by 25.68%, from 15.84kbps to 11.77kbps and OLSR's average throughput, which drops by 0.38%, from 10.19kbps to 10.16kbps.

Raising the mobility speed of nodes in the MANET did not bring a notable change in throughput across all scenarios under regular operation or Black Hole attack. Throughput for AODV, DSR, and OLSR was marginally higher at lower mobility speeds. The decrease in throughput can be attributed to the rapid changes in the location of nodes, which may cause changes in the route to the destination. At the same time, some packets have already been sent from the source node using an outdated route, resulting in the loss of data packets. While under Black Hole attack, average throughput of AODV, DSR and OLSR decreased due to packets being discarded by the Black Hole node. The drastic decrease in the average throughput of AODV while under Black Hole attack can be attributed to AODV's need for constant route establishment to ensure all routes are updated. A further observation is that DSR performs better in average throughput than AODV and OLSR when under Black Hole attack upholding an average throughput of 11.77kbps.

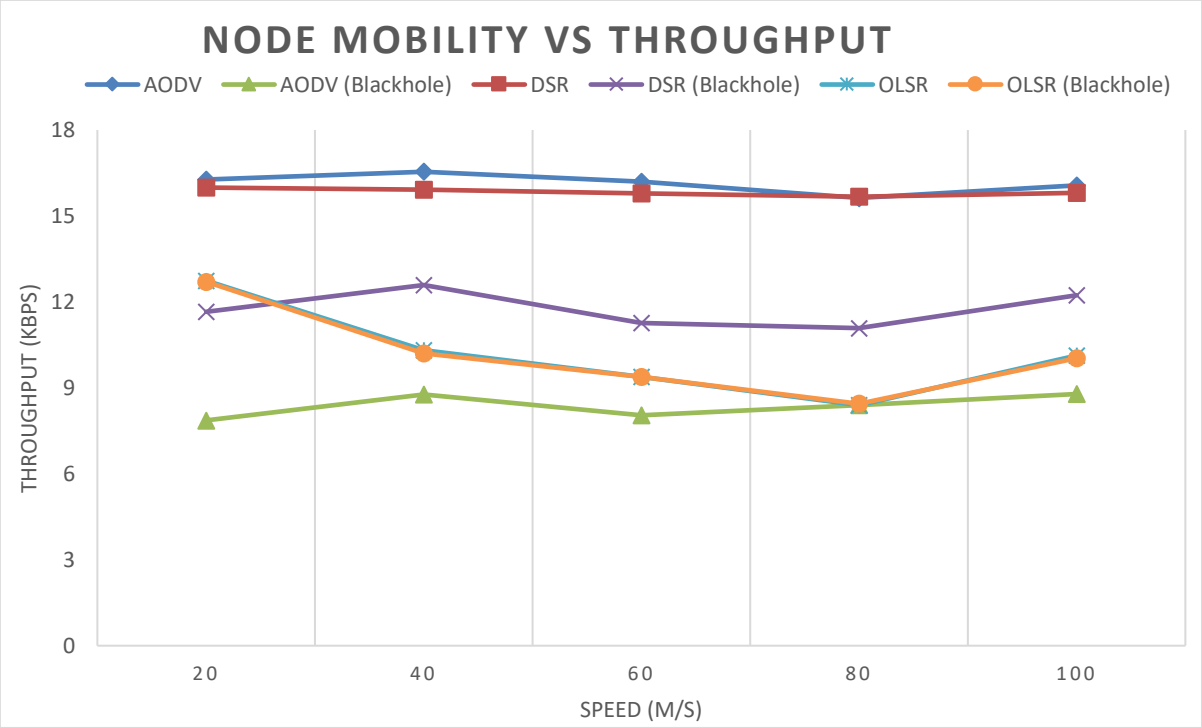

Figure 7.4 – Node Mobility vs Throughput

Figure 7.5 shows the end-to-end delay of AODV, DSR, and OLSR under regular operation, without any attacks, and under Black Hole attacks while varying the mobility speed of the nodes in the network.

Under regular operation, the average end-to-end delay in OLSR (62.27ms) is significantly lower than AODV (196.43ms) and DSR (389.58ms). The end-to-end delay in OLSR remained relatively consistent as the node mobility speed increased due to OLSR being a proactive routing protocol, with route calculations and establishment done in advance for all potential destinations, regardless of node mobility speed. The end-to-end delay for AODV and DSR under no attack increases as the node mobility speed increases due to the rapid node location changes occurring. The end-to-end delay for AODV and DSR under Black Hole attack is reduced, as the Black Hole node responds to the route request immediately without querying the routing table, resulting in a shorter route discovery process time.

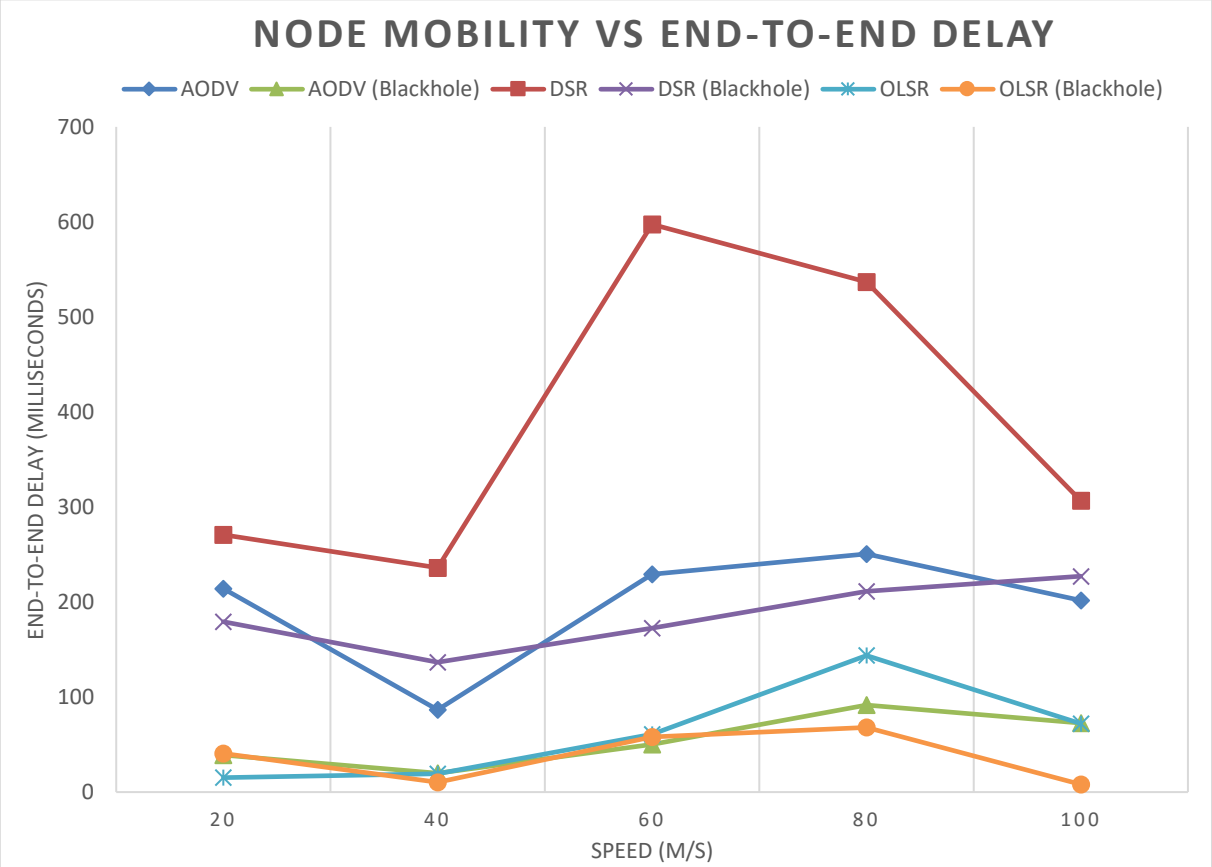

Figure 7.5 – Node Mobility vs End-to-End Delay

Figure 7.6 shows the packet delivery ratio of AODV, DSR, and OLSR under regular operation, without any attacks, and under Black Hole attacks while varying the mobility speed of the nodes in the network.

Under regular operation, as the node mobility speed increased, the packet delivery ratio gradually decreased in AODV and DSR, and there was a more significant decrease in the PDR of OLSR at higher mobility speed. The PDR for AODV under regular operation averaged at 94.63%, with DSR and OLSR averaging 96.33% and 59.43%, respectively. Under Black Hole attack, the PDR of AODV decreased on average by 51.39%, which was significantly more than the average decrease in the PDR of DSR and OLSR, at 26.47% and 0.62%, respectively. DSR performed the best under the Black Hole attacks, upholding an average PDR of 70.83%.

The simulation results show that AODV and DSR perform similarly under regular operation. It can be observed that when the Black Hole attack is introduced into the MANET, the packet delivery ratio is negatively impacted due to the quick changes in the network topology. A further observation is that when under Black Hole attack, the PDR in AODV is much lower than the PDR of DSR or OLSR.

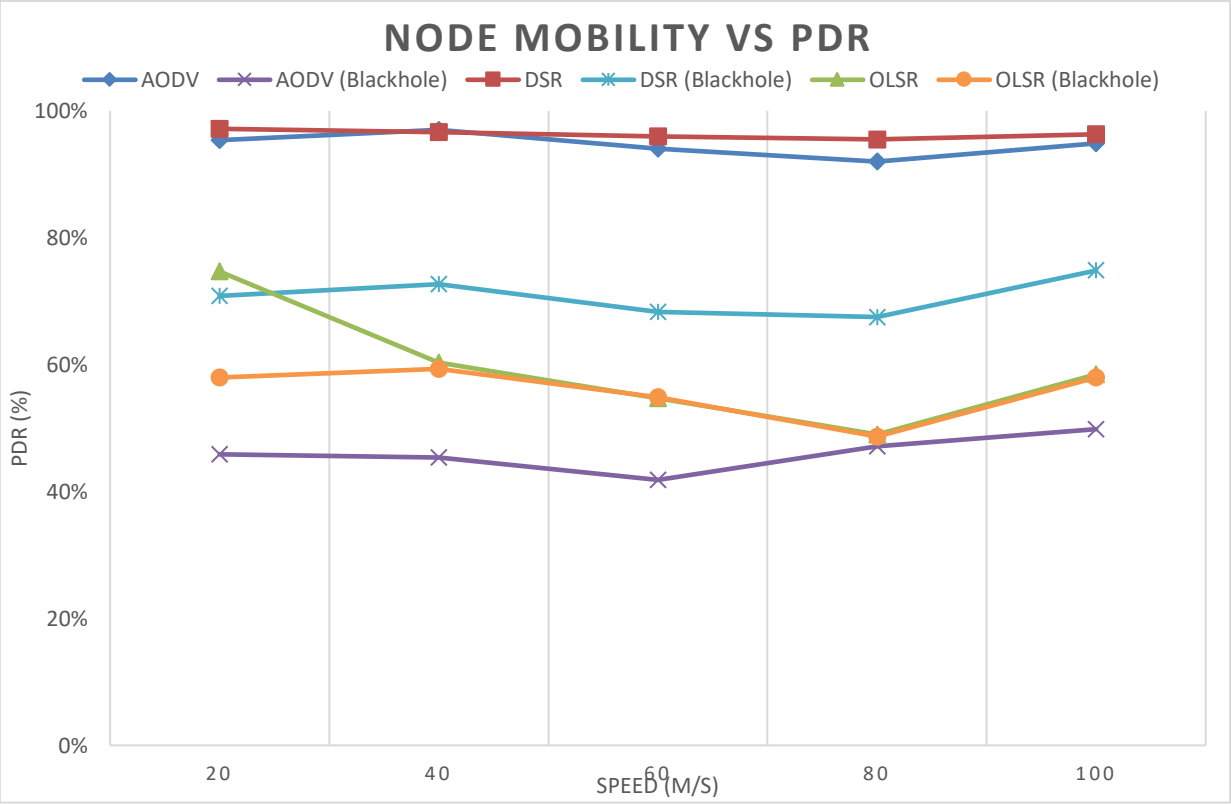

Figure 7.6 – Node Mobility vs PDR

7.3.3 Network Traffic Load

In this scenario, the number of active data connections in the MANET was changed per simulation, starting with one connection and increasing by one for each subsequent simulation, until the active connections peaked at five, with the node density set at 20 nodes and node mobility speed set at 20m/s. The simulations were conducted across all three protocols, AODV, DSR, and OLSR, to evaluate the performance of the MANET under regular operation as well as under Black Hole attack, using the performance metrics of throughput (TH), end-to-end delay (EED), and packet delivery ratio (PDR) as shown by the graphs in this section.

Table 7.3 shows the summarised results of the simulations conducted while varying the number of concurrent active connections in the MANET.

Table 7.3 – Summary of Network Load Simulation Results

Protocol	Density	Speed (m/s)	Connections	Blackholes	TH (Kbps)	EED (ms)	PDR (%)
AODV	20	20	1	0	16.27	856.73	95.33
DSR	20	20	1	0	15.99	1083.65	97.17
OLSR	20	20	1	0	12.74	60.85	74.67
AODV	20	20	1	1	7.87	38.74	45.83
DSR	20	20	1	1	11.66	179.22	70.83
OLSR	20	20	1	1	12.71	40.42	46.67
AODV	20	20	2	0	30.75	665.38	95.83
DSR	20	20	2	0	30.41	1293.77	98.00
OLSR	20	20	2	0	23.66	298.28	73.33
AODV	20	20	2	1	12.26	117.12	37.83
DSR	20	20	2	1	23.88	168.38	77.00
OLSR	20	20	2	1	23.50	39.13	73.00
AODV	20	20	3	0	42.70	576.61	96.50
DSR	20	20	3	0	41.84	1185.28	98.33
OLSR	20	20	3	0	32.25	211.31	72.83
AODV	20	20	3	1	29.49	155.89	66.50
DSR	20	20	3	1	35.78	186.10	84.00
OLSR	20	20	3	1	23.46	70.18	53.17
AODV	20	20	4	0	57.50	597.90	96.83
DSR	20	20	4	0	56.26	924.18	98.17
OLSR	20	20	4	0	43.52	245.13	73.00
AODV	20	20	4	1	37.71	130.76	63.33
DSR	20	20	4	1	49.94	148.99	87.67
OLSR	20	20	4	1	23.47	60.73	39.33
AODV	20	20	5	0	73.05	467.61	96.50
DSR	20	20	5	0	71.42	855.03	98.00
OLSR	20	20	5	0	55.50	77.31	73.50
AODV	20	20	5	1	43.35	91.64	57.33
DSR	20	20	5	1	61.60	106.98	84.67
OLSR	20	20	5	1	35.20	36.24	46.67

Figure 7.7 shows the throughput results of AODV, DSR, and OLSR under regular operation, without any attacks, and Black Hole attack while varying the number of active data connections in the network.

Increasing the number of active data connections resulted in an almost linear increase in throughput across all scenarios, under regular operation and Black Hole attack. The average throughput increased with more connections as more network traffic was transmitted between the source and destination nodes. AODV and DSR were almost identical under regular operation, with an average throughput of 44.05kbps and 43.18kbps, respectively. Under regular operation, the throughput for AODV and DSR increased as the traffic load increased due to the route establishment process used by on-demand protocols. The average throughput of OLSR under regular operation was 33.53kbps. The throughput of OLSR did not increase at the same rate as that of AODV and DSR under regular operation; this can be attributed to the need for an available MPR node to transmit data.

The throughput decreases under Black Hole attack, as the malicious Black Hole node discards some packets being transmitted. AODV's average throughput drops drastically by 40.67%, from 44.05kbps to 26.14kbps, compared to DSR's average throughput, which drops by 15.32%, from 43.18kbps to 36.57kbps, and OLSR's average throughput, which drops by 29.42%, from 33.53kbps to 23.67kbps. While under Black Hole attack, the average throughput of AODV, DSR, and OLSR decreased due to packets being discarded by the Black Hole node. A further observation is that DSR performs better in average throughput than AODV and OLSR when under Black Hole attack, upholding an average throughput of 36.57kbps.

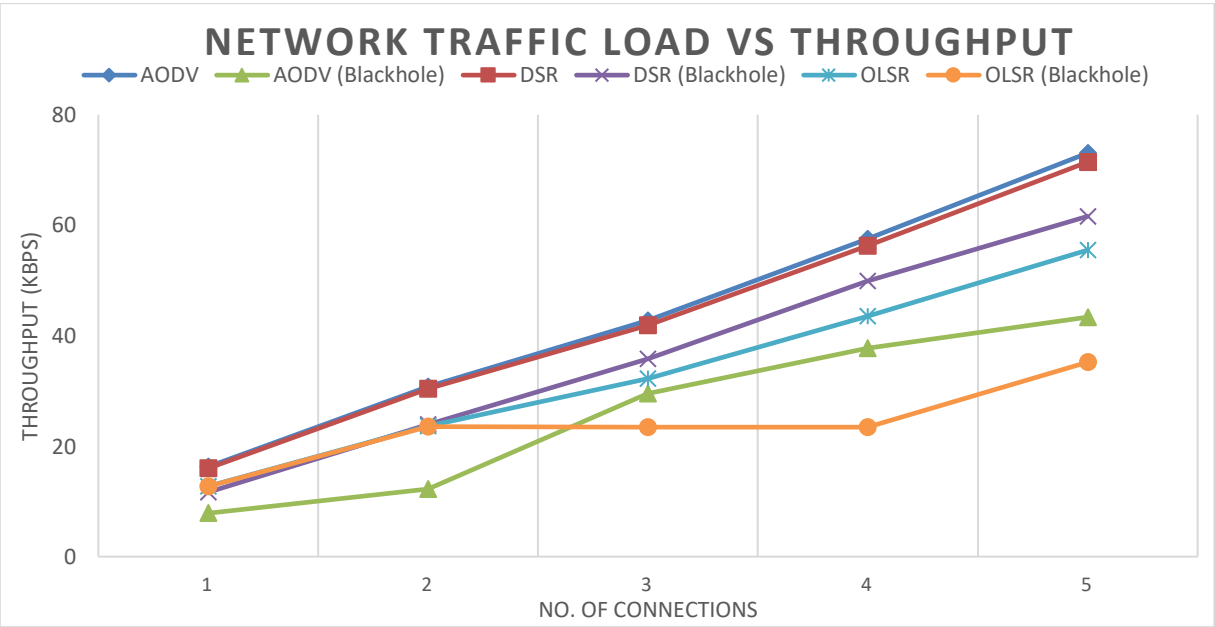

Figure 7.7 – Network Traffic Load vs Throughput

Figure 7.8 shows the end-to-end delay of AODV, DSR, and OLSR simulations under regular operation, without any attacks, as well as under Black Hole attack while varying the number of active data connections in the network.

Under regular operation, the average end-to-end delay of OLSR (178.58ms) is significantly lower than AODV (632.84ms) and DSR (1068.38ms), due to OLSR being a proactive routing protocol, with route calculations and establishment done in advance regardless of the number of connections, for all potential destinations. The end-to-end delay for AODV and DSR under Black Hole attack is reduced, as the Black Hole node responds to the route request immediately without checking the routing table, resulting in a shorter route discovery process time. It can also be observed that there is a higher end-to-end delay in DSR (compared to AODV) due to the significant overhead in keeping complete records of routes from the source node to the destination node, including the intermediate nodes. End-to-end delay is relatively lower when the MANET is under Black Hole attack for AODV and DSR, as the Black Hole node does not have to search for the route in the routing table.

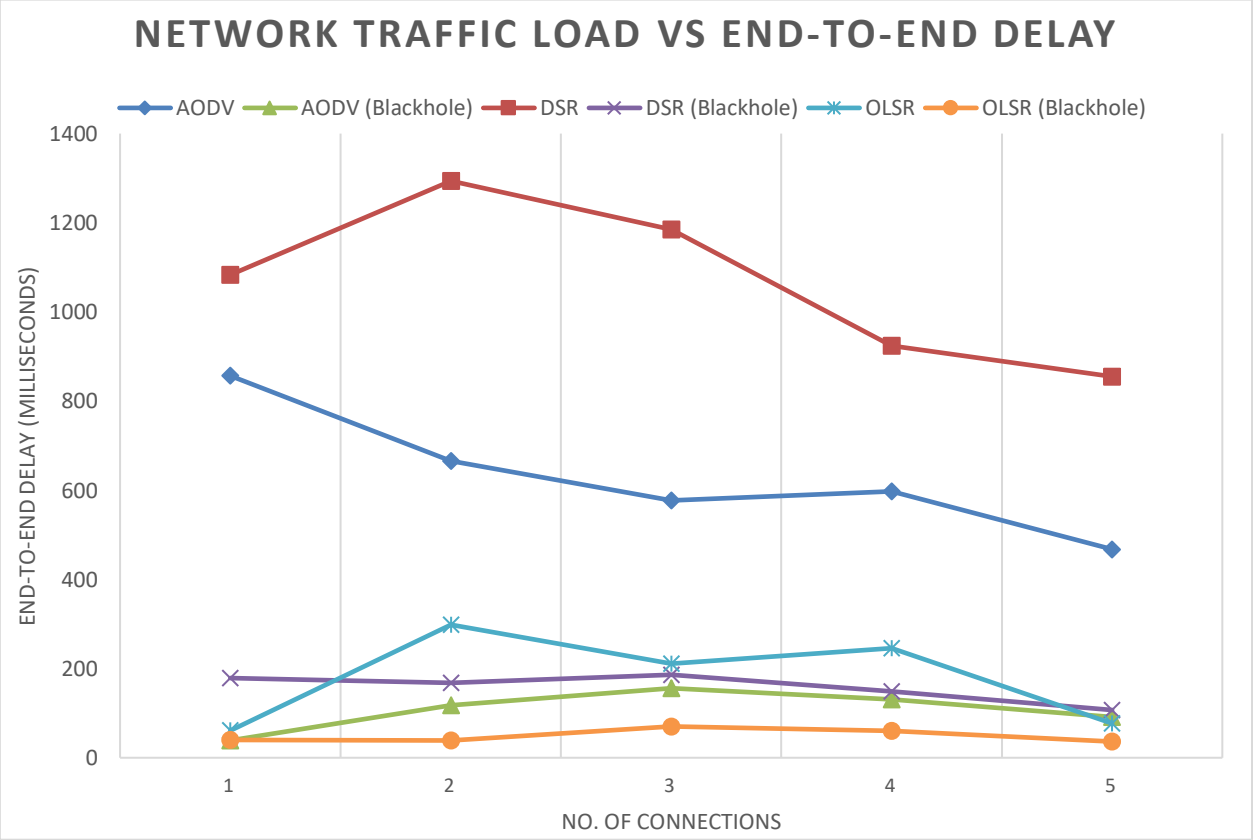

Figure 7.8 – Network Traffic Load vs End-to-End Delay

Figure 7.9 shows the packet delivery ratio of AODV, DSR, and OLSR under regular operation without any attacks and under Black Hole attack while varying the number of active data connections in the network.

Under regular operation, the packet delivery ratio gradually increased in AODV and DSR but decreased in OLSR when more data connections were active. The PDR for AODV under regular operation averaged at 96.2%, with DSR and OLSR averaging 97.93% and 73.47%, respectively. Under Black Hole attack, the PDR of AODV decreased on average by 43.69%, which was significantly more than the average decrease in the PDR of DSR and OLSR, at 17.46% and 21.96%, respectively. DSR performed the best under the Black Hole attack, upholding an average PDR of 80.83%.

The simulation results show that with an increase in the number of connections between nodes in a MANET, there is no significant change in the packet delivery ratio (PDR) for AODV, DSR, and OLSR while under regular operation. It can be observed that when the Black Hole attack is introduced into the MANET, the packet delivery ratio is negatively impacted as packets are discarded by the Black Hole node, which results in a decrease in the PDR. The PDR of AODV and OLSR under Black Hole attack is far less than the PDR of DSR under Black Hole attack.

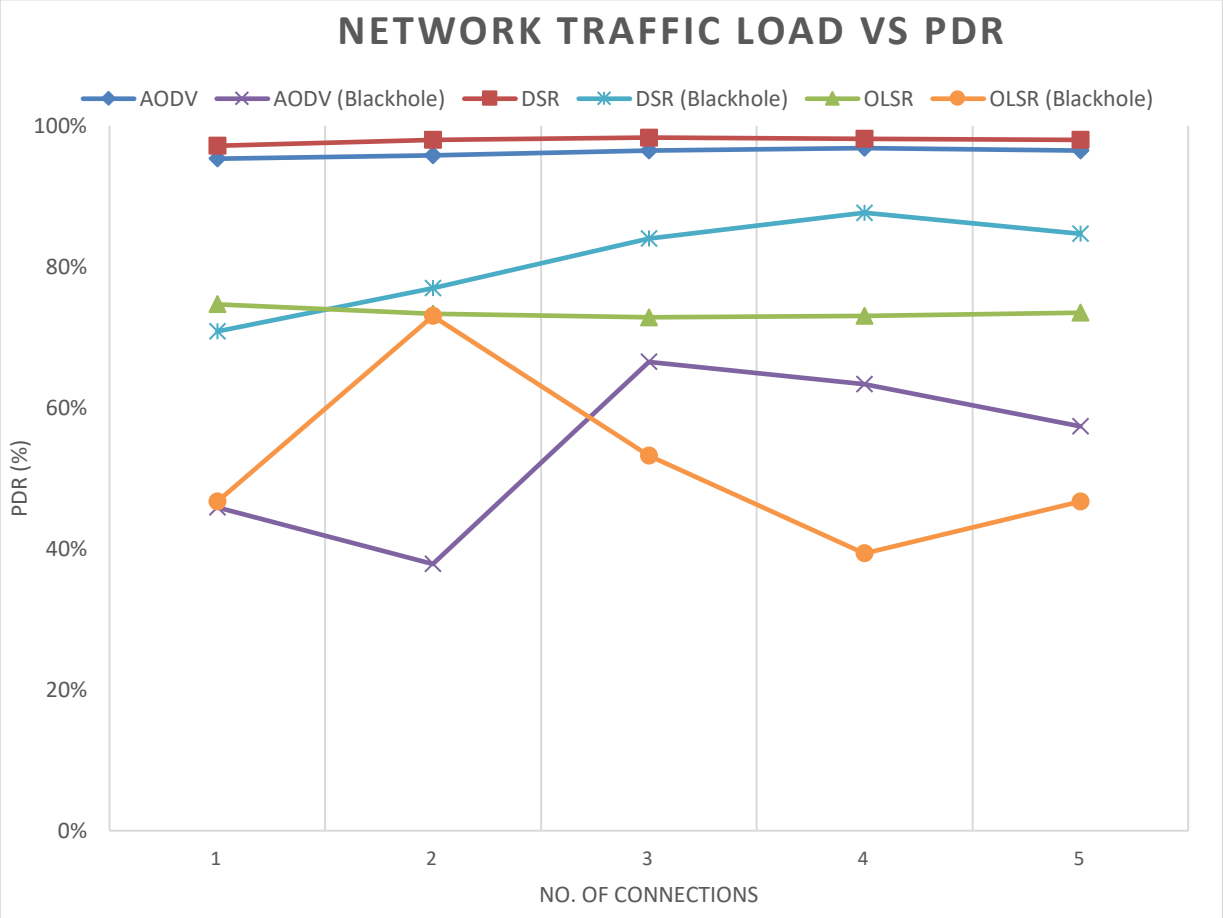

Figure 7.9 – Network Traffic Load vs PDR

7.4 Simulations Results – Mobility Model

The effect that different mobility models have on the performance of a MANET under regular operation and Black Hole attack is essential in determining the viability of using different mobility models based on the requirements of a particular simulation scenario.

The simulation scenarios aim to show the effect on the performance of the Random Waypoint, Random Walk, and Random Direction mobility models under regular operation and in the presence of a Black Hole attack, using routing protocols AODV, DSR, and OLSR. Two simulation scenarios were modelled for each protocol and mobility model pairing. A Black Hole node was not included in the first scenario, but it was incorporated in the second scenario. For all simulation scenarios, the node density was set at 20 nodes, with the node mobility speed set at 20m/s and only one active data transmission connection. As mentioned, the performance metrics of throughput (TH), end-to-end delay (EED), and packet delivery ratio (PDR) were used to analyse the performance of the network. The average results of six simulation runs were analysed and compared to determine how each mobility model performs based on the simulated scenario.

Table 7.4 shows the summarised results of the mobility model simulations while under regular operation and in the presence of a Black Hole attack, using routing protocols AODV, DSR, and OLSR.

Table 7.4 – Summary of Mobility Model Simulation Results

Mobility Model	Protocol	Blackholes	TH (Kbs)	EED (ms)	PDR (%)
Random Direction	**AODV**	0	15.52	45.07	89.50%
	AODV	1	8.62	12.10	50.17%
	DSR	0	15.77	246.22	95.33%
	DSR	1	14.76	244.93	89.17%
	OLSR	0	15.08	16.77	87.33%
	OLSR	1	15.05	16.88	87.33%
Random Walk	**AODV**	0	10.73	401.10	59.50%
	AODV	1	10.05	417.31	53.67%
	DSR	0	10.59	550.12	60.33%
	DSR	1	10.59	550.12	60.33%
	OLSR	0	9.02	18.33	51.83%
	OLSR	1	9.15	18.48	52.17%
Random Waypoint	**AODV**	0	16.94	33.40	99.67%
	AODV	1	14.85	9.49	65.00%
	DSR	0	16.33	11.02	100.00%
	DSR	1	14.76	10.41	90.33%
	OLSR	0	16.59	10.31	97.50%
	OLSR	1	16.55	10.29	97.33%

Figure 7.10 shows the throughput results of the Random Waypoint (RWP), Random Walk (RW), and Random Direction (RD) mobility models, using routing protocols AODV, DSR, and OLSR while under regular operation and under Black Hole attack (BH).

Under regular operation, the Random Waypoint mobility model simulations maintained the highest average throughput of 16.62kbps across all three protocols. The average throughput of the Random Walk mobility model under regular operation averaged at 10.12kbps, with the Random Direction mobility model maintaining an average throughput of 15.46kbps under regular operation. While under Black Hole attack, average throughput decreased due to packets being discarded by the Black Hole node. The average throughput of the Random Direction mobility model decreased by 17.12% to 12.81kbps, and the average throughput of the Random Walk mobility model decreased by 1.83% to 9.93kbps. The average throughput of the Random Waypoint mobility model simulations under Black Hole attack decreased by 7.42% to 15.39kbps.

The Black Hole attack had a minor effect on the Random Walk mobility model regarding percentage change in average throughput. However, compared to the other mobility models, the average throughput of the Random Walk simulations is the lowest. This can be attributed to the unpredictable movements of the nodes in terms of speed and direction, resulting in nodes moving inconsistently. Interestingly, the Random Waypoint mobility model under Black Hole attack performed better than the average throughput of the Random Walk mobility model under regular operation (10.12kbps) and only marginally lower than the average throughput of the Random Direction mobility model under regular operation (15.46kbps). The Random Waypoint simulations performed the best and maintained the best average throughputs across all scenarios.

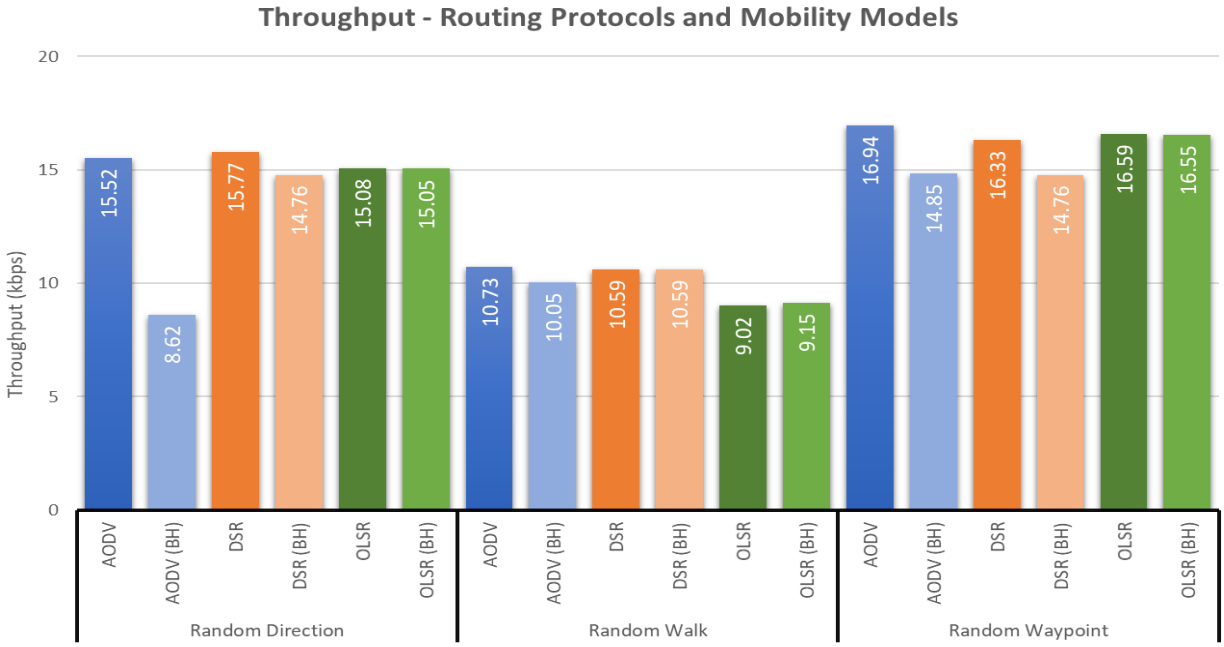

Figure 7.10 – Throughput (Routing Protocols and Mobility Models)

Figure 7.11 shows the end-to-end delays experienced by the Random Waypoint (RWP), Random Walk (RW), and Random Direction (RD) mobility models, using routing protocols AODV, DSR, and OLSR while under regular operation and under Black Hole attack (BH).

Under regular operation, the Random Waypoint mobility model simulations maintained the lowest average end-to-end delay of 18.24ms across all three protocols. The average end-to-end delay of the Random Walk mobility model under regular operation averaged at 323.18ms, with the Random Direction mobility model maintaining an average end-to-end delay of 102.68ms under regular operation. The higher end-to-end delay of the Random Walk and Random Direction mobility model simulations can be attributed to the inconsistent node movements resulting in longer delays in data transmissions.

Under Black Hole attack, the average end-to-end delay of the Random Waypoint mobility model decreased by 44.82% to 10.06ms, with the average end-to-end delay of the Random Direction mobility model decreasing by 11.08% to 91.31ms. The average end-to-end delay of the Random Walk mobility model simulations under Black Hole attack marginally increased by 1.69% to 328.63ms.

The end-to-end delay of AODV and DSR in the Random Walk model is significantly higher than the end-to-end delay of OLSR in the same mobility model, as OLSR is a proactive routing protocol, with route calculations and establishment done in advance for all potential destinations, regardless of the node mobility model used.

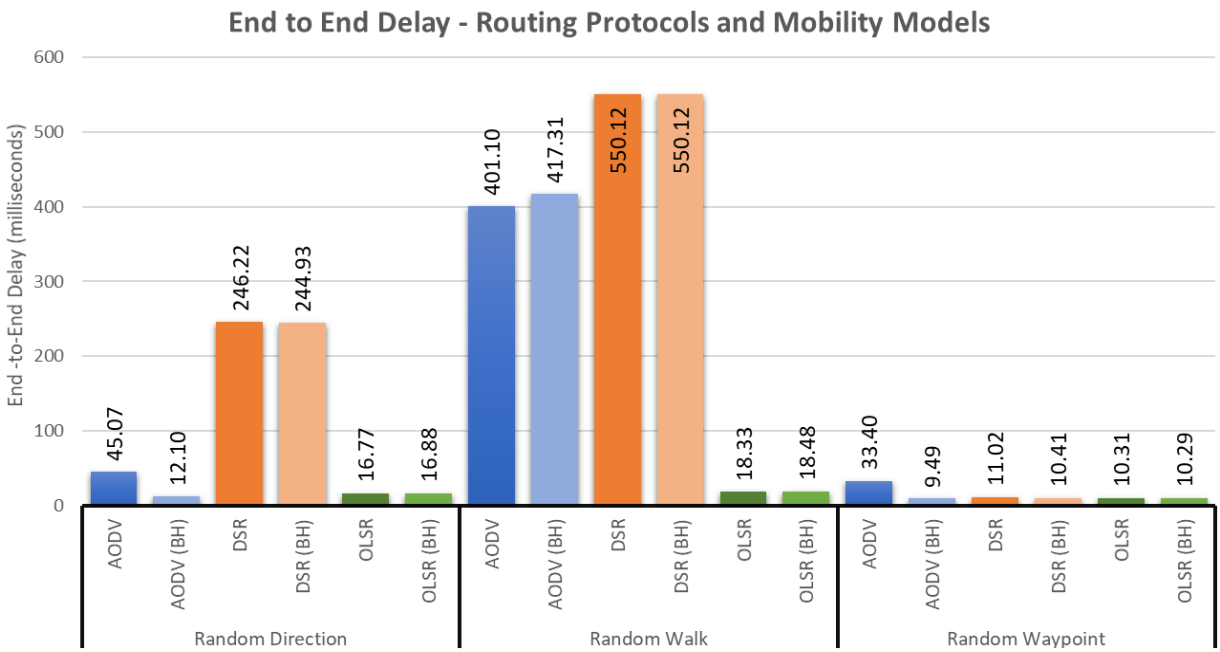

Figure 7.11 – End-to-End Delay (Routing Protocols and Mobility Models)

Figure 7.12 shows the packet delivery ratio of the Random Waypoint (RWP), Random Walk (RW), and Random Direction (RD) mobility models, using routing protocols AODV, DSR, and OLSR while under regular operation and under Black Hole attack (BH).

Under regular operation, the Random Waypoint mobility model simulations maintained the highest average PDR of 99.06% across all three protocols. The average PDR of the Random Walk mobility model under regular operation averaged at 57.22%, with the Random Direction mobility model maintaining an average PDR of 90.72% under regular operation.

The average PDR of the Random Direction mobility model decreased on average by 16.72% to 75.56%, with the average PDR of the Random Walk mobility model decreasing by 3.2% to 55.39%. The average PDR of the Random Waypoint mobility model simulations under Black Hole attack decreased by 14.97% to 84.22%.

The Random Waypoint mobility model performed the best in terms of PDR under regular operation and Black Hole attack.

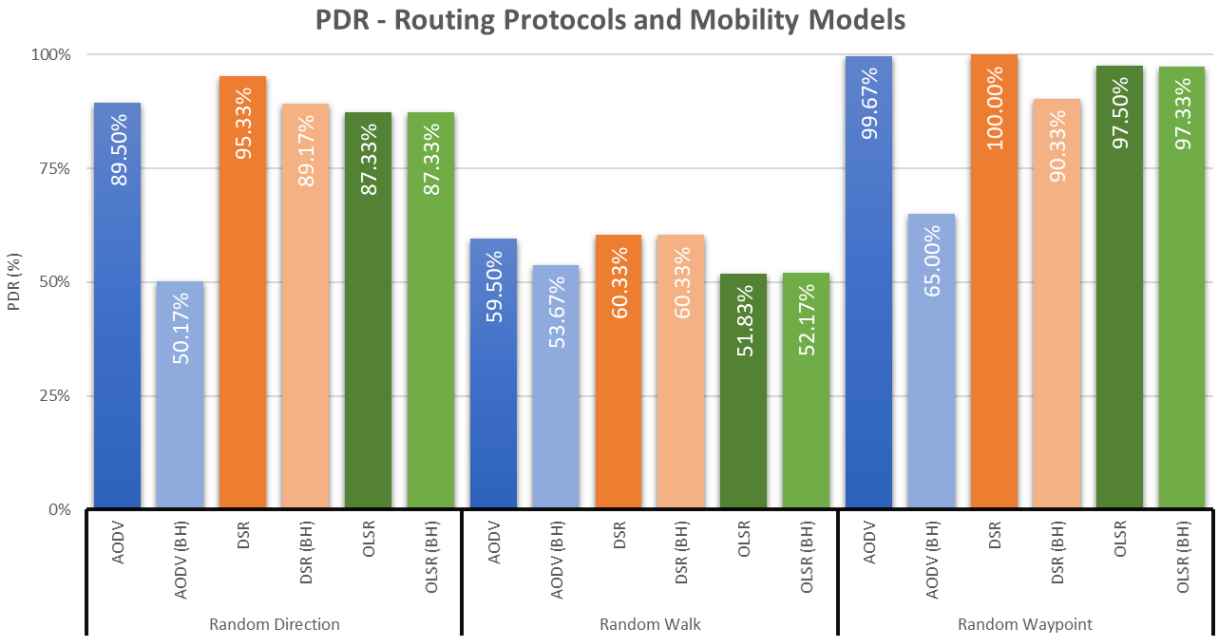

Figure 7.12 – PDR (Routing Protocols and Mobility Models)

7.5 Summary

This chapter evaluated the performance of three routing protocols, namely AODV, DSR, and OLSR, while under regular operation and Black Hole attack scenarios using NS2.

The performance metrics, average throughput, packet delivery ratio, and end-to-end delay, were used to analyse the effects that Black Hole attacks have on the performance of networks with Network Density, Network Traffic Load, and Node Mobility Speed as simulation scenarios. From the results using the abovementioned performance metrics, it has been observed that Black Hole attacks cause deterioration in the performance of MANETs. The adverse effects that Black Hole attacks have on the overall performance of MANETs were more significant in AODV than in DSR or OLSR. This result proved that AODV is more vulnerable to Black Hole attack than DSR or OLSR and the effects of a Black Hole attack are greater in AODV.

Additionally, the performance of the Random Waypoint, Random Walk, and Random Direction was also evaluated to determine which mobility model is the most suitable for MANET simulations and which performed best. The Random Waypoint mobility model performed the best under regular operation, demonstrated in its high average throughput with minimal end-to-end delay and a strong PDR across all protocols and scenarios.

The next chapter presents the concluding remarks of this study and provides recommendations for future research on Black Hole attacks in MANETs.

Chapter 8 – Conclusion and Future Work

8.1 Conclusion

Mobile Ad-hoc Networks are temporary network topologies formed when a wireless mobile node system establishes a dynamic network on the fly without relying on any pre-existing communication infrastructure. MANETs are made up of several cooperative mobile nodes, making them more susceptible to security attacks, such as Black Hole attacks. These attacks work to manipulate the cooperative nature of MANETs.

AODV, DSR, and OLSR are among the most popular protocols for MANETs. This study evaluated these three protocols under regular operation and Black Hole attack scenarios using the NS2 simulator. The results of the simulations prove that the existence of Black Hole nodes in a MANET severely impacts the overall performance of the network system in terms of packet delivery ratio, end-to-end delay, and throughput.

The following observations were made based on the results of the simulations:

- A MANET under regular operation outperforms a MANET under Black Hole attack in terms of average throughput and PDR in AODV, DSR and OLSR. This occurs due to the Black Hole node claiming to have the shortest route to the destination node by responding with a quick RREP to the source node.
- In terms of end-to-end delay in both AODV and DSR, the results show that a MANET under Black Hole attack has a reduced end-to-end delay. This reduction in end-to-end delay is not seen as a positive sign as the Black Hole node compromises the network communication to achieve this reduction. At the same time, end-to-end delay in OLSR remained relatively unchanged under Black Hole attack.
- The adverse effects that Black Hole attacks have on the overall performance of MANETs were more significant in AODV than in DSR or OLSR.
- The Random Waypoint mobility model performed the best under regular operation, demonstrated in its high average throughput with minimal end-to-end delay and a strong PDR across all protocols and scenarios.
- The performance of the Random Walk and Random Direction mobility models is fair. These mobility models can be considered for use in scenarios that require more randomness and flexibility in node movement parameters.

To conclude, the adverse effects that Black Hole attacks have on the overall performance of MANETs were more significant in AODV than in DSR or OLSR. This result proved that

AODV is more vulnerable to Black Hole attacks than DSR or OLSR and the effects of a Black Hole attack are greater in AODV. Based on the observed simulation results, DSR performs best under Black Hole attack based on the simulation parameters used. The Random Waypoint mobility model is the best mobility model to use in MANET simulation scenarios as it allows for the implementation of a malicious node and allows for accurate simulation of a Black Hole attack.

8.2 Future Work

This study focused on the effects that Black Hole attacks have on the performance of Mobile Ad-hoc Networks using Reactive and Proactive Routing Protocols, with specific emphasis on AODV, DSR, and OLSR. Therefore, analysis needs to be conducted on other Reactive and Proactive Routing protocols to determine which protocol can best mitigate the effects of Black Hole attacks.

Research needs to be conducted on the other types of MANET security attacks mentioned in Chapter 3 to assist in attack classification based on the impact each attack has on the performance of a MANET.

Future work to analyse the effects that Black Hole attacks have on the performance of Mobile Ad-hoc Networks in terms of mean delay time, packet overhead, and memory usage will further assist in determining which protocol performs best. The effects multiple Black Hole attacks have on the performance of Mobile Ad-hoc Networks is also important to determine which protocol best withstands the effects of a cooperative Black Hole attack.

8.3 Summary

This chapter brings this study to a conclusion by providing an overview of the work conducted during the study. The results and findings of the simulations are also presented with observations and conclusions based on the results given. Finally, recommendations for future work related to this study are provided.

References

AARTI, M. & TYAGI, S. 2013. Study of MANET: Characteristics, Challenges, Application and Security Attacks*. International Journal of Advanced Research in Computer Science and Software Engineering*, 3(5), pp. 252-257.

ABU, M., AHMED, S., ABU, M. & KUMAR, T. 2011. AODV Robust (AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes. *International Journal of Advanced Computer Science and Applications*, 2(8).

ADEL, A. & MELAD, M. 2016. Performance Evaluation of AODV, DSR, OLSR, and GRP MANET Routing Protocols Using OPNET. *International Journal of Future Computer and Communication*, 5, pp. 57-60.

AGARWAL, D. & ROUT, R. 2015. Detection of Node-misbehaviour Using Overhearing and Autonomous Agents in Wireless Ad-Hoc Networks. In-*applications and Innovations in Mobile Computing*, pp. 152-157.

AGGARWAL, S. & KUMAR, N. 2021. Attacks on Blockchain. *Advances in Computers*, pp. 399-410.

AHMED, D. & KHALIFA, O. 2017. An Overview of MANETs: Applications, Characteristics, Challenges and Recent Issues. *International Journal of Engineering and Advanced Technology*, 6(4), pp. 128-133.

AHMED, F. & KO, Y. 2016. Mitigation Of Black Hole Attacks in Routing Protocol for Low Power and Lossy Networks. *Security and Communication Networks*, 9(18), pp. 5143-5154.

AHMED, F. & OH, H. 2013. An Encryption Based Black Hole Detection Mechanism in Mobile Ad-hoc Networks. *IJSIA*, 7(6), pp. 1-10.

AHUJA, G. & SUGANDHA 2017. A Review on Black Hole Attack in MANET. *Institution of Electronics and Telecommunication Engineers*, pp. 645-649.

ALUVALA, S., SEKHAR, K.R, & VODNALA, D. 2016. An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks. *2nd International Conference on Intelligent Computing, Communication*.

ARCHANA, R. & GRACY, T. 2015. Survey on Attacks in MANET. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(9), pp. 125 - 131.

ARYA, A., CHAURASIA, B.P & GUPTA, S.K. 2015. Performance Analysis of Optimize AODV and AODV Routing Protocol. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(9), pp. 456-460.

BAI, F. & HELMY, G. 2004. A survey of mobility models. *Wireless Ad-hoc Networks*, 206, pp. 147.

BALA, K. 2016. A Survey of Black Hole Detection Policies in Mobile AD HOC Networks. *International Journal of Future Generation Communication and Networking*, 9(12), pp. 295-304.

BALLAV, B. 2016. Performance Comparison of Multi-hop Wireless Ad Hoc Network Routing Protocols using NS2. *Journal of Mobile Computing, Communications & Mobile Networks*, 3(1), pp. 1-10.

BASULAIM, K.O. & AMAN, S.A. 2017. Solution for Black Hole and Cooperative Black Hole Attacks in Mobile Ad Hoc Networks. *Egyptian Computer Science Journal*, 41(1), pp. 66-81.

BHALIA, M. 2015. Analysis of MANET Characteristics, Applications and its routing challenges. *International Journal of Engineering Research and General Science*, 3(4), pp. 139-143.

BOULAICHE, M. 2020. Survey of Secure Routing Protocols for Wireless Ad Hoc Networks. *Wireless Personal Communications*, 114(1), pp. 483-517.

CAREEM, M. & DUTTA, A. 2020. Reputation Based Routing in MANET Using Blockchain. *2020 International Conference on Communication Systems & NETworkS (COMSNETS)*.

CHAHAL, D. & KHARB, L. 2017. Security Concepts Underlying MANET. *IJETER*, 5(3), pp. 94-98.

CHANDAN, R. & MISHRA, P. 2019. Performance Analysis of AODV under Black Hole Attack. *ICACSE*.

CHAUHAN, S. 2015. Performance Evaluation of Routing Protocols for MANET Using NS2. *International Journal of Computer Science and Mobile Computing*, 4(9), pp. 242-249.

DAS, S. 2014. Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks. Personal Communications, *IEEE*, pp. 1-11.

DEFRAWY, K. 2010. Security and Privacy in Location-based Mobile Ad-Hoc Networks, PhD. Dissertation, Bren School of Information and Computer Science, University of California Irvine.

DENG, H., LI, W. & AGRAWAL, D. 2002. Routing security in wireless ad-hoc networks. *IEEE*, 40(10), pp. 70-75.

DORRI, A. (2016). An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. *Wireless Networks*, 23(6), pp. 1767-1778.

DORRI, A., KAMEL, S. & KHEYRKHAH, E. 2015. Security Challenges in Mobile Ad Hoc Networks: A Survey. *International Journal of Computer Science AND Engineering Survey*, 6(1), pp. 15-29.

DWIVEDI, P. & GUPTA, S. 2016. A Survey on Route Maintenance and Attacks in AODV Routing Protocol. *International Journal of Computer Applications*, 133(9), pp. 23-26.

GANDHEWAR, N. & PATEL, R. 2012. Review on Sinkhole Detection Techniques in Mobile Ad-hoc Network. *Advances in Intelligent and Soft Computing*, pp. 535-548.

GUERAA, A., RACHID, S. & ABOUTAJDINE, D. 2015. Impact of mobility model on packet transmission in vehicular ad hoc network based on IR-UWB. *IEEE*, pp. 1-5.

GUPTA, A., SADAWARTI, H. & VERMA, A. 2013. Performance Analysis of MANET Routing Protocols in Different Mobility Models. *International Journal of Information Technology and Computer Science*, 5(6), pp. 73-82.

GUPTA, S., KAR, S. & DHARMARAJA, S. 2011. BAAP: Black Hole attack avoidance protocol for wireless network. *2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011)*.

GURJAR, A. & DANDE, A. 2013. Black Hole Attack in MANETs: A Review Study. *International Journal of IT, Engineering and Applied Sciences Research*, 23, pp. 12-14.

GURUNG, S. & CHAUHAN, S. 2017. Review of Black-Hole Attack Mitigation Techniques and its Drawbacks in Mobile Ad-hoc Network. *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 2379-2385.

HAMAMREH, R. 2018. Protocol for Multiple Black Hole Attack Avoidance in Mobile Ad Hoc Networks. *Recent Advances in Cryptography and Network Security*.

HUSIEEN, N. & RASHEED, M. 2015. Analysing Optimal Setting of Reference Point Group Mobility Model Using DSR Protocol In MANETS. *ICIT 2015 The 7th International Conference on Information Technology*, pp. 213 – 222.

JAIN, A. & TOKEKAR, V. 2015. Mitigating the effects of Black Hole attacks on AODV routing protocol in mobile ad hoc networks. *2015 International Conference on Pervasive Computing (ICPC)*, pp. 1-6.

JAMWAL, D., SHARMA, K. & CHAUHAN, S. 2014. Zone Routing Protocol. *International Journal of Recent Research Aspects*, pp. 16 - 20.

JHAVERI, R., PATEL, S. & JINWALA, D. 2012. DoS Attacks in Mobile Ad-hoc Networks: A Survey. *2012 Second International Conference on Advanced Computing AND Communication Technologies*.

JOHNSON, D. & MALTZ, D. 1996. Dynamic source routing in ad hoc wireless networks. *Mobile Computing*, pp. 153- 181.

JUBAIR, M., KHALEEFAH, S., BUDIYONO, A., MOSTAFA, S. & MUSTAPHA, A. 2018. Performance Evaluation of AODV and OLSR Routing Protocols in MANET Environment. *IJASEIT*, 8(4), pp. 1277-1283.

KALAKAR, V., ALI, S. & CHACK, H. 2020. Performance Analysis of Black Hole Attack in MANET using OPNET. *IJIRT*, 6(10), pp. 299-307.

KANAKARIS, V., NDZI, D. & OVALIADIS, K. 2012. Applications of MANET Routing Protocols in Sensor Network. *International Journal of Research and Reviews in Ad hoc Networks*, 1, pp. 2046-5106.

KAUR, D. & KUMAR, N. 2012. Comparative Analysis of AODV, OLSR, TORA, DSR and DSDV Routing Protocols in Mobile Ad-Hoc Networks. *International Journal of Computer Network and Information Security*, 5(3), pp. 39-46.

KAUR, H., BALA, M. & SAHNI, V. 2015. Study of Black Hole Attack Using Different Routing Protocols in MANET. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 2(7), pp. 3031-3039.

KAUSER, S. & KUMAR, P. 2016. MANET: Services, Parameters, Applications, Attacks & Challenges. *IJSRSET*, 2(2), pp. 4-9.

KAUSHIK, N. & DUREJA, A. 2013. Performance Evaluation of Modified AODV Against Black Hole Attack in MANET. *European Scientific Journal*, 9(18), pp. 182-193.

KHAN, D. & JAMIL, M. 2017. Study Of Detecting and Overcoming Black Hole Attacks in MANET: A Review. *2017 International Symposium on Wireless Systems and Networks (ISWSN)*, pp. 1-4.

KHAN, S., USMAN, F., MATIULLAH & KHAN, F. 2018. Enhanced Detection and Elimination Mechanism from Cooperative Black Hole Threats in MANETs. *International Journal of Advanced Computer Science and Applications*, 9(3).

KHAN, W., AKRE, V. & SAEED, K. 2021. Impact of black hole attack on the performance of dynamic source routing and optimized link state routing protocols in MANETs. *JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES*, 16(3), pp. 13-30.

KHANDELWAL, A. 2018. A Study on Network Simulator 2. *International Journal of Current Research in Life Sciences*, 7(2), pp. 1036-1039.

KHURANA, S., KUMAR, S. & SHARMA, D. 2017. Performance Evaluation of Congestion Control in MANETs using AODV, DSR and ZRP Protocols. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(6), pp. 398-403.

KUMAR, S. 2012. Simulation-Based Comparative Performance Study of AODV, DSR and ZRP in Mobile Ad-hoc Networks (MANETs) Using Qualnet 5.0.2. *IOSR Journal of Engineering*, 2(4), pp. 568-572.

KUMARI, R. & CHUGH, A. 2018. Distributed Denial of Service Attack Detection, Prevention and Secure Communication in MANET. *International Journal of Computer Science Trends and Technology (IJCST)*, 8(1), pp. 24-28.

KUROSAWA, S., NAKAYAMA, H., KATO, N., JAMALIPOUR, A. & NEMOTO, Y. 2007. Detecting Black Hole Attack on AODV-based Mobile Ad-hoc Networks by Dynamic Learning Method. *International Journal of Network Security*, 5(3), pp. 338-346.

KUYORO, S., ALEBURU, D., EZE, M. & OSISANWO, F. 2018. Impact of Black Hole Attack on Reactive and Proactive Routing Protocols in MANET. *International Journal of Scientific & Engineering Research*, 9(4), pp. 1568-1572.

LAXMAN, M. 2014. Security Issues in Mobile Ad-hoc Networks. *International Journal of Computer Science and Mobile Computing*, 3(5), pp. 1022-1024.

LAZOS, L. & KRUNZ, M. 2011. Selective jamming/dropping insider attacks in wireless mesh networks. *IEEE Network*, 25(1), pp. 30-34.

LIU, G., YAN, Z. &PEDRYCZ, W. 2018. Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey. *Journal of Network and Computer Applications*, 105, pp. 105-122.

LIU, H. & SHANG, Z. 2015. Comparing the Performance of the Ad-hoc Network under Attacks on Different Routing Protocol. *IJSIA*, 9(6), pp. 195-208.

MANOHAR, B. & KUMAR, N. 2019. Review On Byzantine Attack in MANET and Solution to Avoid. *International Research Journal of Engineering and Technology (IRJET)*, 6(1), pp. 1033-1035.

MANOHARAN, R. & ILAVARASAN, E. 2010. Impact of Mobility on the Performance of Multicast Routing Protocols in MANET. *International Journal of Wireless & Mobile Networks*, 2(2), pp. 110-119.

MAYANK, M. & GUPTA, S. 2015. Performance evaluation of DSR, AODV and DSDV routing protocol for wireless ad-hoc network. 2015 *IEEE International Conference on Computational Intelligence AND Communication Technology*, pp. 416-421.

MEJAELE, L. & OCHOLA, E. 2015. Analysing the impact of black hole attack on DSR-based MANET: The hidden network destructor. *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec).*

MISTRY, N., JINWALA, D. & ZAVERI, M. 2010. Improving AODV Protocol against Black Hole Attacks. *International Multi-Conference of Engineers and Computer Scientists*.

MOHAMMAD, A., MAHMOOD, A. & VEMURU, S. 2018. Providing Security Towards the MANETs Based on Chaotic Maps and Its Performance. *Lecture Notes in Electrical Engineering*, pp. 145-152.

MOHAN, S. & NIRMAL, K. 2013. Cryptographic Approach to Overcome Black Hole Attack in MANETs. *International Journal of Innovations in Engineering and Technology*, 2(3), pp. 86-92.

MOHANAPRIYA, M. & KRISHNAMURTHI, I. 2014. Modified DSR protocol for detection and removal of selective black hole attack in MANET. *Computers & Electrical Engineering*, 40(2), pp. 530-538.

MOHEBI, A. & SCOTT, S. 2013. A Survey on Detecting Black-hole Methods in Mobile Ad-hoc Networks. *International Journal of Innovative Ideas*, 13(2), pp. 55-63.

NAAZ, S. 2014. Routing in Vehicular Ad Hoc Network (VANET). *International Journal of Advanced Research in Computer Science and Software Engineering*, pp.1-5.

NABOU, A., LAANAOUI, M. & OUZZIF, M. 2018. Evaluation of Manet routing protocols under black hole attack using AODV And OLSR in NS3. *2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*.

NABOU, A., LAANAOUI, M. & OUZZIF, M. 2019. Effect of Single and Cooperative Black Hole Attack in MANET using OLSR protocol. *2nd International Conference on Networking, Information Systems & Security*, pp. 1-5.

NEERAJ, A. & BARWAR, N. 2014. Evaluation of AODV, OLSR and ZRP Routing Protocols under Black hole attack. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 3(4), pp. 285–288.

NEWMAN, I. & BENZ, C. 1998. Qualitative-quantitative research methodology. Carbondale, Ill.: Southern Illinois University Press.

NISAR, M.A., MEHMOOD, A. & NADEEM, A. 2013. A Review and performance analysis of mobility models for MANETs: A case study. *International Conference on Information and Communication Technologies*, 1(6).

NURCAHYANI, I. & HARTADI, H. 2018. Performance Analysis of Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) Under Black Hole Attacks in Mobile Ad Hoc Network (MANET). *2018 International Symposium on Electronics and Smart Devices (ISESD)*.

PANDA, N. & PATTANAYAK, B. 2018. Analysis of Blackhole Attack in AODV and DSR. *International Journal of Electrical and Computer Engineering (IJECE),* 8(5), pp. 3093-3102.

PANDA, N., PATRA, B. & HOTA, S. 2020. MANET Routing Attacks and Their Countermeasures: A Survey. *Journal of Critical Reviews*, 7(13), pp. 2777-2792.

PATEL, R. & KAMBOJ, P. 2017. A Survey on Contemporary MANET Security: Approaches for Securing the MANET. *International Journal of Engineering and Technology*, 9(1), pp. 98-112.

POLVERINI, D., ARDENTE, F., SANCHEZ, I., MATHIEUX, F., TECCHIO, P. & BESLAY, L. 2018. Resource efficiency, privacy, and security by design: A first experience on enterprise servers and data storage products triggered by a policy process. *Computers & Security*, 76, pp. 295-310.

POOJA, V., ROHIT, T., REDDY, N. & SUDESHNA, S. 2018. Mobile Ad-hoc Networks Security Aspects in Black Hole Attack. *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pp. 26-30.

PRAVEEN, K., GURURAJ, H. & RAMESH, B. 2016. Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols. *International Conference on Computational Modelling and Security*, 85, pp. 325-330.

RAJ, P. & SWADAS, P. 2009. A dynamic learning system against Black Hole attack in AODV based MANETs. *International journal of computer science issues*, 2, pp. 54-59.

RAMAMOORTHY, H. & DEVI, D., 2013. A New Proposal for Route Finding in Mobile Ad-Hoc Networks. *International Journal of Computer Network and Information Security*, 5(7), pp. 1-8.

RANGARAJ, J. & ANITHA, M. 2017. Performance analysis of proactive and reactive protocol under different mobility models for MANET. 2017*. International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC).*

RAZA, N., UMAR AFTAB, M., QASIM AKBAR, M., ASHRAF, O. & IRFAN, M. 2016. Mobile Ad-hoc Networks Applications and Its Challenges. *Communications and Network*, 8(3), pp. 131-136.

ROHAL, P., DAHIYA, R. & DAHIYA, P. 2013. Study and Analysis of Throughput, Delay and Packet Delivery Ratio in MANET for Topology Based Routing Protocols (AODV, DSR and DSDV). *International Journal for Advance Research in Engineering and Technology*, pp. 54-58.

SAETANG, W. & CHAROENPANYASAK, S. 2012. CAODV Free Black Hole Attack in Ad-hoc Network. *International Conference on Computer Networks and Communication Systems*, 35, pp. 63-68.

SALEHI, M & SAMAVATI, O. 2012. DSR vs OLSR: Simulation-Based Comparison of Ad Hoc Reactive and Proactive Algorithms under the Effect of New Routing Attacks. *2012 Sixth International Conference on Next Generation Mobile Applications, Services and Technologies*, pp. 100-105.

SALEHI, M. & SAMAVATI, H. 2013. Injection and Evaluation of New Attacks on Ad-hoc Proactive Routing Algorithms. *International Journal for Information Security Research*, 3(2), pp. 285-293.

SALEHI, M., SAMAVATI, H. & DEHGHAN, M. 2011. Performance Assessment of OLSR Protocol under Routing Attacks. *Internet Technology and Secured Transactions (ICITST)*, pp. 791 - 796.

SARANYA, R. & RAJESH, R. 2018. Study of Black Hole and Gray Hole Attacks in MANET. *International Journal of Applied Engineering Research*, 13(24).

SARIKA, S., PRAVIN, A., VIJAYAKUMAR, A. & SELVAMANI, K. 2016. Security Issues in Mobile Ad Hoc Networks. *2nd International Conference on Intelligent Computing, Communication AND Convergence*, pp. 329-335.

SAUNDERS, M., LEWIS, P. & THORNHILL, A. 2012. Research methods for business students. Harlow, England: Pearson.

SELVAVINAYAKI, K. & KARTHIKEYAN, E. 2012. A Reliable Data Transmission Approach to Prevent Black Hole attack in MANET. *International Journal of Computer Science and Telecommunications*, 3(3).

SEN, J., KOILAKONDA, S. & UKIL, A. 2011. A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad-hoc Networks. *2011 Second International Conference on Intelligent Systems, Modelling and Simulation*.

SHABBIR, A., KHALID, F., SHAHEED, S.M., ABBAS, J. & ZIA-UL-HAQ, M. 2015. Security: A Core Issue in Mobile Ad hoc Networks. *Journal of Computer and Communications*, 3, pp. 41-66.

SHANKAR, A. & CHELLE, L. 2016. Performance comparison of AODV, DSR, DSDV and OLSR Manet routing protocols. *International Journal of Engineering Research*, 5(10), pp. 218–223.

SHARMA, G. & GUPTA, M. 2012. Black Hole Detection in MANET Using AODV Routing Protocol, *International Journal of Soft Computing and Engineering (IJSCE)*, 1(6), pp. 297-303

SHARMA, N. & SHARMA, A. 2012. The Black-Hole Node Attack in MANET. *2012 Second International Conference on Advanced Computing AND Communication Technologies*.

SHIVAHARE, B., WAHI, C. & SHIVHARE, S. 2012. Comparison Of Proactive and Reactive Routing Protocols in Mobile Ad-hoc Network Using Routing Protocol Property. *IJETAE*, 2(3), pp. 356-358.

SINGH, G. & KHURANA, R. 2017. Performance Evaluation of DSR, OLSR and ZRP using NETSIM Simulator. *International Journal of Advanced Research in Computer Science*, 8(3), pp. 346-349.

SINGH, H. 2011. An approach for detection and removal of Black Hole In MANETS. *International Journal of Research in ITAND Management (IJRIM)*, 1(2).

SINGH, J. & GUPTA, S. 2017. Impact of Jamming Attack in Performance of Mobile Ad hoc Networks. *International Journal of Computer Science Trends and Technology (IJCST)*, 5(3), pp.184-190.

SINGH, R. 2018. An Overview of MANET: Characteristics, Applications Attacks and Security Parameters as well as Security Mechanism. *Journal of Engineering and Technology*, 5(9), pp.1155-1159.

SINGH, S. & CHOUDHARY, D. 2017. AODV vs. OLSR: An Analytical Approach to Study Black Hole Attack. *International Journal of Computer Applications*, pp. 30-34.

SREEDHAR, C., VERMA, S. & KASIVISWANATH, N. 2012. A Novel Approach for Secure Routing in MANETs. *Engineering Science and Technology: An International Journal*, 2(5), pp. 928-934.

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

TAMILSELVAN, L. & SANKARANARAYANAN, V. 2007. Prevention of Black Hole Attack in MANET. *2nd International Conference on Wireless Broadband and Ultra-Wideband Communications*.

THANGARAJ, S., RENGARAJAN, A. & SELVANAYAKI, S. 2019. Comprehensive Learning on Characteristics, Applications, Issues and Limitations of Manets. *International Journal of Innovative Technology and Exploring Engineering*, 8(9), pp. 311-314.

UMAPARVATHI, M. & VARUGHESE, D. 2012. Two Tier Secure AODV against Black Hole attack in MANETs. *European Journal of Scientific Research*, 72(3), pp. 369-382.

VERMA, R., SHARMA, R. & SINGH, U. 2017. New Approach through Detection and Prevention of Wormhole Attack in MANET. *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*, pp. 526-531.

VINAYAGAM, P. 2014. Impact of Random Mobility Models on OLSR. *International Journal of Wireless & Mobile Networks*, 6(6), pp. 87-100.

WALIKAR, G. & BIRADAR, R. 2017. A survey on hybrid routing mechanisms in mobile ad hoc networks. *Journal of Network and Computer Applications*, 77, pp. 48-63.

WALLIMAN, N. 2017. Research methods. 2nd edition. London: Routledge.

WEERASINGHE, H. 2011. Preventing Cooperative Black Hole attacks in Mobile Ad-hoc Network. *IEEE International Conference on Communications*, pp. 24-28.

Appendices

Appendix 1 – TCL Script

TCL Script used to generate the .nam and .tr files used in the simulations of this study.

```
#===================================
#     Variables read in
#===================================
set interface [lindex $argv 0];
set protocol [lindex $argv 1];
set nodes [lindex $argv 2];
set connectionFile [lindex $argv 3];
set scenarioFile [lindex $argv 4];
set outputFile [lindex $argv 5];

#===================================
#     Simulation parameters setup
#===================================
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)     $interface                 ;# interface queue type
set val(rp)      $protocol                  ;# routing protocol
set val(ll)      LL                         ;# link layer type
set val(ant)     Antenna/OmniAntenna        ;# antenna model
set val(ifqlen)  50                         ;# max packet in ifq
set val(nn)      $nodes                     ;# number of mobilenodes
set val(x)       750                        ;# X dimension of topography
set val(y)       750                        ;# Y dimension of topography
set val(con)     $connectionFile            ;# Connection file
set val(src)     $scenarioFile              ;# Scenario
set val(stop)    500.0                      ;# time of simulation end

#===================================
#        Initialization
#===================================
#Create a ns simulator
set ns_ [new Simulator]

#Setup topography object
set topo       [new Topography]
$topo load_flatgrid $val(x) $val(y)
set god_ [create-god $val(nn)]

#Open the NS trace file
set tracefile [open $outputFile.tr w]
$ns_ trace-all $tracefile

#Open the NAM trace file
set namfile [open $outputFile.nam w]
$ns_ namtrace-all $namfile
$ns_ namtrace-all-wireless $namfile $val(x) $val(y)

set chan [new $val(chan)];#Create wireless channel
```

```
#===================================
#     Mobile node parameter setup
#===================================
$ns_ node-config -adhocRouting  $val(rp) \
                 -llType        $val(ll) \
                 -macType       $val(mac) \
                 -ifqType       $val(ifq) \
                 -ifqLen        $val(ifqlen) \
                 -antType       $val(ant) \
                 -propType      $val(prop) \
                 -phyType       $val(netif) \
                 -channel       $chan \
                 -topoInstance  $topo \
                 -agentTrace    ON \
                 -routerTrace   ON \
                 -macTrace      ON \
                 -movementTrace ON


#===================================
#        Nodes Definition
#===================================
for {set i 0} {$i < $val(nn) } {incr i} {
    set node_($i) [$ns_ node]
    $node_($i) random-motion 0 ;# disable random motion
}
$node_(1) color blue
$ns_ at 0.0 "$node_(1) color blue"
$ns_ at 0.0 "$node_(1) label SOURCE"

$node_(5) color green
$ns_ at 0.0 "$node_(5) color green"
$ns_ at 0.0 "$node_(5) label DESTINATION"

#===================================
#        Scenario Definition
#===================================
puts "Scenario Setup"
source $val(src)

#===================================
#        Connection Definition
#===================================
puts "Connection Setup"
source $val(con)

#===================================
#        Movement Definition
#===================================
puts "Movement Setup"
for {set i 0} {$i < $val(nn)} {incr i} {
    $ns_ initial_node_pos $node_($i) $val(nn)
}

#===================================
#        Blackhole nodes
#===================================
$node_(6) color red
$ns_ at 0.0 "$node_(6) color red"
$ns_ at 0.0 "$node_(6) label BLACKHOLE"
$ns_ at 0.0 "[$node_(6) set ragent_] blackhole"
```

```
#=================================
#        Termination
#=================================
#Define a 'finish' procedure
proc finish {} {
    global ns_ tracefile namfile outputFile
    $ns_ flush-trace
    close $tracefile
    close $namfile
    exec nam $outputFile.nam &
    exit 0
}
for {set i 0} {$i < $val(nn) } { incr i } {
    $ns_ at $val(stop) "\$node_($i) reset"
}
$ns_ at $val(stop) "$ns_ nam-end-wireless $val(stop)"
$ns_ at $val(stop) "finish"
$ns_ at $val(stop) "puts \"done\" ; $ns_ halt"
$ns_ run
```

Appendix 2 – TCL Usage Command

These commands were used to call the TCL file and changes were made to these parameters to simulate the necessary scenarios.

```
ns      normal.tcl                              # TCL filename
        Queue/DropTail/PriQueue                 # interface
        AODV                                    # protocol
        20                                      # number of nodes
        "~/Connections/cbr_1_512.tcl"           # connection file location
        "~/Scenarios/sim1/sim1_20_20.tcl"       # scenario file location
        ~/Results/N_AODV_sim1_20_20             # result file location
```

Appendix 3 – AWK Script

AWK Script used to obtain information from the trace files.

```
BEGIN {
    seqno = -1;
    count = 0;
}

{
  event = $1
  time = $2
  node_id = $3
  pkt_size = $8
  level = $4

  if (level == "AGT" && event == "s" && $7 == "cbr") {
    sent++
    if (!startTime || (time < startTime)) {
      startTime = time
    }
  }
```

```
  if (level == "AGT" && event == "r" && $7 == "cbr") {
    receive++

    if (time > stopTime) {
      stopTime = time
    }
    recvdSize += pkt_size
  }

  if($4 == "AGT" && $1 == "s" && seqno < $6) {
    seqno = $6;
  }

 #end-to-end delay
  if($4 == "AGT" && $1 == "s") {
    start_time[$6] = $2;
  }
  else if(($7 == "cbr") && ($1 == "r"))    {
    end_time[$6] = $2;
  }
  else if($1 == "D" && $7 == "cbr")    {
    end_time[$6] = -1;
  }
}

END {
    for(i=0; i<=seqno; i++) {
          if(end_time[i] > 0) {
            delay[i] = end_time[i] - start_time[i];
            count++;
        }
        else {
            delay[i] = -1;
        }
    }

    for(i=0; i<=seqno; i++) {
        if(delay[i] > 0) {
            n_to_n_delay = n_to_n_delay + delay[i];
        }
    }

   n_to_n_delay = n_to_n_delay/count;

  print(substr(FILENAME, 0, length(FILENAME)-3),",",
sent,",",receive,",",(receive/sent),",",n_to_n_delay *
1000,",",(recvdSize/(stopTime-
startTime))*(8/1000),",",startTime,",",stopTime)

}
```