UNISA university of south africa

A COMPARISON OF AODV AND DSR UNDER ATTACK BY BLACK HOLE NODES IN A NS-3 SIMULATION

---

by

THOMAS EDWARD FOGWELL

Dissertation submitted in fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in

COMPUTER SCIENCE

at the

SCHOOL OF COMPUTING

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: MR ELISHA OKETCH OCHOLA

DECEMBER 2018

Declaration

I declare that this dissertation, which I submit herewith for the research qualification

Master of Science degree in Computer Science

to the School of Computing, University of South Africa, is apart from the recognised assistance of my supervisors, my own work, and that all the sources that I have referenced or from which I have quoted have been indicated and acknowledged by means of complete citations. I further declare that I have not previously submitted this work, or part of it, for examination at the University of South Africa for another qualification or at any other institution of higher education.

Candidate

Date

Acknowledgements

My special thanks are extended to Mr Elisha Ochola for years of guidance through my higher education. I would also like to thank my friends for not leaving me after missing so many events to work on this dissertation. Lastly thanks to my family for always being supportive and celebrating my success.

Contributions

The following peer-reviewed conference papers were published as a contribution of this study:

1. T. E. Fogwell and E. O. Ochola. A Comparison of Ad Hoc On-Demand Distance Vector and Dynamic Source Routing Under Attack by Black Hole Nodes in an NS-3 Simulation. *Proceedings of the 3rd International Conference on The Internet, Cyber Security and Information Systems*, University of Botswana conference Centre, Gaborone, Botswana, pages 1-11, 2018. ISBN 978-99968-2-0-033-5

2. T. E. Fogwell and E. O. Ochola. Location Based Analysis of AODV Performance in the Presence of Black Hole Nodes, *IEEE International Conference on Advances in Computing, Communication and Engineering*, Durban, South Africa, pages 24-29, 2016. ISBN: 987-1-5090-2576-6

3. T. E. Fogwell and E. O. Ochola. Comparison Analysis of AODV and DSR Under Attack by Black Hole Nodes in a NS3 Simulation, *Proceedings of the 14th International Conference on Cyber Warefare and Security*, Stellenbosch University, Cape Town, South Africa, pages 574-587, 2019. ISBN: 978-1-912764-11-2

The main contribution of the study is an extensive simulation result of the performance of AODV and DSR under different mobility models that has revealed instances where AODV performs better than DSR, contrary to the general opinion that puts DSR always above AODV in performance under black hole attack, as analysed in the literature review section. The results, therefore, indicate when MANET protocols are compared that various mobility models should be used for simulation to obtain unbiased results.

Abstract

Mobility and portability of wireless communication devices in Mobile Ad Hoc Networks (MANETs) have introduced data security threats. These threats are due to the utilisation of multiple hops resulting from limited transmission ranges between the source and destination nodes.

This study aims to prove the impact black hole attacks can have on MANETs, more specifically, how attacks impact two different reactive protocols. It is envisioned that a comparative analysis of two protocols, AODV and DSR, will assist the audience understand their side by side performance while under attack with nodes using varying models of mobility. The simulation criteria used have network conditions favourable for optimum functioning of reactive protocols. Optimal conditions for the functioning of reactive protocols include densely distributed nodes that do not move sporadically.

The simulation is conducted using ns-3 and NetAnim. It involves the use of a base implementation of AODV and DSR using ns-3 as a benchmark for the effects that black hole nodes introduce into a network. Similarly, the AODV and DSR implementation that have black hole nodes present in the network is included, in order to measure the effects of the black hole nodes. Thereafter, the performance of these

protocols is compared when under attack, keeping the environment the same.

Results generated from this study indicate that DSR outperforms AODV while having black hole nodes in the node population under various configurations. The dominance of DSR is ascribed to the fact that DSR can keep several routes and make a decision on those routes, while AODV gives more responsibility to the network for the best route. This means that, changing the hop count to a low value can fool the source node to choose the route.

Keywords: AODV; DSR; MANET Protocol Comparison; MANET security; ns-3; Black Hole attack; AODV vs DSR; Simulation

Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

AODV Ad-Hoc On-Demand Distance Vector

CBR Constant Bit Rate

DDoS Distributed Denial of Service

DoS Denial of Service

DSR Dynamic Source Routing

FTP File Transfer Protocol

HTTP HyperText Transfer Protocol

IP Internet Protocol

MANET Mobile Ad Hoc Network

OSI Open Systems Interconnection

QoS Quality of Service

RREQ Route Request

VOIP Voice over IP

1 Introduction

1.1 Research Focus

This research study is focused on Mobile Ad Hoc Network (MANET) protocols and security. A mobile ad-hoc network is a self-configuring infrastructureless network of mobile devices connected via wireless links. The term "infrastructureless", which is used in the definition of MANET, is an important attribute of the network that gives it a vast list of applications where it can be used. The network can be established in areas with no or minimal infrastructure; in fact, only the mobile devices or nodes are required. Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are examples of reactive on-demand routing protocols. This type of protocol discovers routes as they are needed by sending route requests; it is for this reason that they are named reactive. These protocols are vulnerable to attacks, and emphasis is placed on determining the impact of specific attacks on reactive routing protocols in MANETs while under different movement scenarios.

1.2 Problem Statement

Wireless communication devices in MANETs have data security threats introduced by their mobility and portability. The threats are due to the utilisation of multiple hops as a result of limited transmission ranges between the source and destination nodes.

One of the most severe attacks is the black hole attack, which falls under the attack category of a disruptive attack [1]. This type of attack involves a node that replies to a route request and states that it is the destination or it has a route to the destination at a low cost. Thereafter this node drops all the packets it receives; the black hole analogy originates from this behaviour. There are different variants of this attack, in simple terms, it is a node that does not at all deliver packets to the correct destination.

By accurately detecting and eliminating black hole nodes the performance of MANETs under attack by a black hole can be improved. That is, indications are that inaccurate black hole attack detection and elimination in MANETs have led to a decrease in network performance. As MANETs are becoming more prosperous and stable, security has become a lingering concern.

From a research gap perspective, it is generalised that DSR always performs better than AODV whenever a network is under black hole

attack. However, this may not be true under certain scenarios.

1.3 Scope of Research

The study explores the AODV and DSR routing protocols, as well as black hole node as a security concern.

1.3.1 Research Questions

The research sought to answer the following research questions:

i. What is the impact black hole- and similar types of attacks have on a MANET?

ii. What solutions are available for addressing the attacks?

iii. How are various on-demand routing protocols affected by these attacks?

iv. How do different protocols compare with each other while under attack?

v. Is the impact of the attack the same under different network conditions?

1.3.2 Research Objectives

This research is aimed at:

i. To investigate the impact of black hole attack on MANETs by simulating multiple protocols under normal conditions.

ii. To compare and analyse the performance of multiple protocols while under black hole attack.

1.3.3 Research Deliverable

The research study produced simulation results comparing AODV and DSR routing protocols while under attack along with benchmark baseline results. The attack used involves introducing a low number of black hole nodes into networks using previously mentioned protocols.

1.4 Dissertation Outline

The remainder of the study includes the Research Methodology in section 2, Literature Review in section 3, Experimentation in section 4, Results in section 5, Evaluation of Results in section 6 and finally the Conclusion in section 7.

2 Research Methodology

In this section, the process followed to investigate the attack from related works was explained. Thereafter, this information was used to create a model for simulating a MANET scenario under pre-determined conditions prior to the evaluation of the generated data and results. The literature review provides the much needed context under which a scenario is modelled so as to experiment the protocol's functionality while introducing the security issues at hand. The creation of an enabling environment where the standard and under attack conditions are compared allows the impact of the attack on the protocol's performance to be measured. Data was generated via a simulation tool called ns-3 and analysed via output generated by ns-3 simulation programs. In a nutshell, the methodology commences with a literature review, which is followed by experimentation and analysis of the experimental results, before a conclusion is drawn from the analysed data.

2.1 Literature Review

It is expected that the literature review provides the reader with existing simulation scenarios as well as the corresponding data analysis and results. Similarly, possible solutions and observations from related

literature sources was analysed. The review also covers the respective individual inspection and comparative analysis of AODV and DSR. The review goes into detail about the type of attacks, which helps create clarity to what is described in the analysis to follow when the black hole attack is compared to other attacks. The AODV and DSR protocols are investigated in more detail followed by papers who compare the two protocols, this data can be used to validate the results.

2.2 Experimentation

The experimentation component was conducted via simulation and modelling. The modelling involves the clarification of the simulation boundaries and expected results. The simulation criteria used is targeted at having network conditions that are favourable to the MANET protocol and function optimally. This means that the conditions should not affect the normal operation of the MANET. Optimal conditions for DSR include densely distributed nodes that do not move sporadically, while more sporadic nodes favour AODV. The simulations were conducted using ns-3 and NetAnim. ns-3 is a discrete event network simulator for Internet systems, targeted primarily at research and educational use. The simulations involve the use of a base implementation of MANET protocols from ns-3 (version 3.26), which are used

as a benchmark for the effects that black hole nodes introduce into a network. Similarly, the MANET protocol implementation that has black hole nodes present in the network is also performed in order to measure the effects brought about by the introduction of black hole nodes.

2.3 Evaluation of Results

It is expected that experimental and simulation data that is based on our proposed steps enable conclusions to be drawn about the performance of the protocols under normal and attack conditions. This data can then be used to compare different protocols under attack, which indicate whether the attack has similar severity for each protocol. A literature review has confirmed the baseline results indicating the non-presence of any attacks. The evaluation was done in sections related to different mobility models because the data indicate important results for each model, which allowed the comparison of the protocols in more depth. Furthermore, the details of each configuration were discussed for the said model which allowed the complete comparison of models and configurations to later be used for the conclusion.

2.4 Summary

This chapter provided us with an approach to our study. As per [2], there are two different types of studies, solution-seeking and knowledge-seeking. This study is classified as a knowledge-seeking study which looks to find comparative information regarding two protocols. To retrieve this information we use literature reviews with experimentation to obtain information relevant to the progress of the MANET field.

3 Literature Review

In this study, research is being undertaken on two popular protocols, namely AODV and DSR. In particular, the literature review explored each of the protocols in detail; AODV in section 3.2 and DSR in section 3.3, followed by a comparison of the protocols in section 3.4. Prior to this discussion ,the types of attacks were investigated in section 3.1.

3.1 Type of attacks

There are multiple types of attacks, but the authors in [3] simplified the relevant attacks into two categories. That is, routing disruption attacks where packet routes are disrupted causing loss of packets or incorrectly routed packets and resource consumption attacks where data is injected to use up resources. Both attacks deny service and are thus labelled Denial of Service (DoS) attacks; in addition, the black hole attack has been confirmed as a DoS attack [4]. This study specifically explores the black hole attack, which is described as a node that pretends to have new low-cost routes to all nodes and absorbs network traffic as discussed in [5], [1]. The most well-known essential building blocks for information security are confidentiality, integrity, availability and non-repudiation [6]. DoS attacks fall under the availability block when

the service availability has been compromised. When considering the Open Systems Interconnection (OSI) model, the focus is placed on the network layer as this is where black hole attacks occur.

Studies focused on the investigation of the enhancement of attacks such as the black hole attack have proposed a new black hole attack variant called **deep black hole attack** [7], [8]. This type of an attack advertises fake route reply messages more aggressively; in fact, such an attack has been shown through simulation studies to possess a more devastating effect on the network than the standard black hole- and selfish-node attacks. The [7], [8] results emanating from studies involving the experimentation of the DSR protocol have revealed that standard black hole attacks and other attacks with a similar attack vector can be improved and thus enable additional damage to be dealt with.

The authors in [9] performed a study using **Distributed DoS attacks** to drain batteries of devices by consuming resources that do not benefit the network. This study has shown that the attack vectors do not have to be limited to the network; this evidenced by fact that the attack on battery life of the physical device in use is also a vulnerability for a misbehaving protocol.

An attack that is similar to the black hole attack is the **wormhole**

attack. According to [10], wormhole attacks involve two malicious nodes that form a tunnel and transmit information from another exit point. An analysis of the AODV and DSR protocols shows that the route discovery will contain route through the wormhole if the packets are tunneled to an entirely different area in a network. Once this trust has been achieved by this malicious node, all the traffic to the malicious node can be dropped thus causing damage to the performance of the network. Alternatively, the malicious node can perform some malicious activity with all the packets that pass through the wormhole.

Another type of attack is the **pollution attack**, which is mentioned by [6]. This attack occurs when a malicious node injects meaningless data into the network. These pollution packets then propagate through the network depleting network resources. A solution, which demonstrates time-based authentication along with random linear transformations to defend against the attack, has been mentioned [11].

A comparative analysis of the following six different attacks has been undertaken: Route Request (RREQ) flood-, Sink Hole-, Black hole-, Selfish Node-, Hello Flood- and Selective forwarding attacks [1]. These attacks are discussed in more detail below.

Route request attacks affect reactive routing protocols by generating multiple RREQ messages, which have higher priority than data

packets. After the route is maintained, the attacker sends useless data packets that cause the node to stop processing legitimate packets.

Sinkhole attacks occur when a node notifies that it has a low-cost route to the destination and sends this routing information to its neighbours. Neighbour nodes start sending all packets through this node; depending on the implementation, if the node drops all packets it becomes a black hole attack.

Selfish node attacks are merely nodes that act correctly in the network but do not forward data packets to the destination. The node, depending on its motives, has the ability to drop packets that are routed through the node to preserve its resources.

Hello messages in AODV are controlled message that are broadcast to neighbours in the network. From these messages, nodes can create new routing table entries or refresh old entries of neighbours. The **hello flood attack** would disrupt the resources of the node to update the table entries. Such an attack primarily generates overhead onto the function of the node. [12] investigated HELLO flooding as well and from results concluded that AODV degraded while under attack.

Selective forwarding is similar to selfish node attacks in a sense that the node is choosy when forwarding messages and drops some of those messages. The number of messages dropped depend on the ma-

licious node setup or configuration. These type of attacks are difficult to detect.

The differences between grey, black and selfish nodes have been described [13]. Grey nodes drop RREQ messages. A type of Selfish node drops route requests intermittently to conserve their resources; another type of selfish node also drops packets intermittently to save their resources. While, black hole nodes drop packets steadily. **Grey nodes** do not want to be considered for routes and thus exclude all RREQ messages except for data designated to that node.

RREQ and data flooding attacks have been explored further and results have revealed that flooding attacks can negatively affect the performance of mobile ad hoc networks when AODV and DSR were tested; such a result is in fact viewed as a significant security threat in the network [14].

3.2 Ad Hoc On-Demand Distance Vector

AODV is an on-demand routing protocol used in MANETs. It involves the protocol sending out a route request message to the network on every request. If the message is received by the destination, the node responds with a route reply message. The source then uses the route received to send data to the destination. If the route is broken, a route

error message is sent, and a new route request is initialised. The AODV protocol also broadcasts hello messages to neighbours to update its routing tables. To present this study with accurate simulation criteria, ways in which other related works simulated the attack were explored.

Dokurer et al. [5] have completed simulations using ns-2 with the AODV protocol. Following the introduction of the black hole nodes into the populations, the behaviour of the nodes were tested before continuing with the larger datasets. Thereafter, multiple configurations were used during the simulations. The first configuration entails a small number of nodes in fixed positions, sending UDP packets of size 512 bytes. This simulation was then run for 20 seconds in a 200 by the 200-meter grid; however, the network worked as usual when the attack was introduced. Results generated seems to indicate that the position of the black hole impacts the network. To this end, the population was increased to 20 nodes wherein even numbered nodes would transmit data to odd-numbered nodes. The new configuration used was a 750x750-meter grid, and the simulations ran for 500 seconds. A choice was made not to send data in the last 50 seconds and wait for buffers in the network to be emptied after the last transmission. It was evident from a comparative analysis of the network calculations and the results that clearing the buffers did not affect the network calcu-

lations. A total of 100 simulations were completed for each simulation and nodes were placed in different positions for each simulation thus allowing random movement of each node. A data rate of 10 Kbps was used and a 3.46% packet loss was achieved when the network was not under attack; this was used as a baseline. Calculations of the overall packet loss and packet loss per black hole revealed significant impact from the attack. The results indicated an 89.95% packet loss, partially caused by black holes and partially by network congestion. It was interesting to note that the time an RREP would be received had an average of 1.27 seconds after sending the RREQ while not attacked, and 0.209 seconds when a black hole responded. This was ascribed to the black hole nodes not checking tables. However, this is not a substantial measure since a destination node next to a source node would give the same results. When a solution was proposed to take the second route received after sending an RREQ improvements were noticed. Although the results improved by 19%, their baseline performance decreased by 4%. No mention of a timer was made to indicate the time it would take to wait for the second route; this could cause problems if the population is sparse. The result of the proposed solution had 71.09% packet loss, which is an improvement of 18.86%. It was aptly demonstrated 10.8% of the nodes in the simulations are one

hop from each other, which could indicate that black holes near to the source have a more significant impact. Moreover, no explanation was provided as to why the authors solution to use the second route received is so useful. When using a third route, which has the options of longer hops, the results indicates better performance when that third route is chosen. Showing an increase in performance when the black hole is not close to the source.

The study by Ehsan et al. [1] completed simulations in ns-2.34 with the AODV protocol. A variety of attacks on the protocol were tested and were compared with each other. The attacks were found to be: black hole attack, sinkhole attack, selfish node behaviour, RREQ flood, hello flood, and selective forwarding attack. During the simulations the packet efficiency, routing overhead and throughput were used to measure performance. Whereas packet efficiency was defined as the proportion of the number of packets which arrived at the destination to the number of packets departed from the source, routing overhead was defined as the ratio of the number of routing protocol control packets transmitted to the number of data packets. Throughput was on the other hand defined as the total amount of data regarding the bytes received by the destination per second. Data was sent from 30% of the nodes in the simulation. A fixed grid of 500x500-meters was used

and a single attacker was introduced into the population at one time. The packet size used was 512 bytes, with Constant Bit Rate (CBR) rates of 0.25 and 0.5 were used. Traffic was transmitted at a constant bit rate. The node density was changed during the simulations at increments of 10, from 10 to 50 nodes. The nodes have a fixed range of 50 meters, and the Random Waypoint mobility model in ns-2 was used to move the nodes randomly. During the simulations, different pause times of increments of 20 were used, starting from zero to 80. The nodes generated traffic at different times during the simulation. Each simulation was run for 100 seconds. The simulations compared one baseline simulation with six other simulations, each from a different attack. It was found that when packet efficiency was compared with pause time (the time for which the nodes are stationary), the efficiency decreased and that the impact of a black hole- and sinkhole attacks were the most drastic of the six. When the mobility was decreased (i.e. when the pause time was increased), the packet efficiency improved, albeit not substantial, after the pause time of 40 seconds. When comparing results from packet efficiency to node density the packet efficiency of data below 30 nodes was found to be very poor, and this was attributed to the possible existence of disconnections in the network. Such a claim is strange since the inferior performance of

the AODV baseline on a sparse network was not ascribed to disconnections; an attacked AODV network is also more likely to trigger an attacking node when the population is not dense. From the data, it was concluded that only sink- and black hole attacks performed better with fewer nodes. For the routing overhead versus node density, the hello packet flood attack generated the most overhead. Second place went to sink- and black hole nodes because they send false replies to the route requests according to the authors. A comparison of throughput versus node density of the sink- and black hole attacks gave rise to a substantially more significant impact compared to the other attacks. Similar results were observed the pause time was increased (i.e. when the node mobility was decreased).

The work presented by Alkatheiri et al. [13] tested grey holes, selfish nodes as well as black holes. Specifically, selfish nodes that do not participate in network discovery (type 1 selfish nodes) and selfish nodes that drop data packets selectively (type 2 selfish nodes), were tested. Ns-2 in a 1000x1000-meter grid containing 50 nodes was used. The nodes had a transmit range of 250 meters, pause time of 100 seconds and moved at a speed of 10 meters per second with the Random Waypoint mobility model. The simulations for 900 seconds were run and malicious nodes were increased by 10% to 40% of the

network contained nodes. The packet size used was 512Kb. The following was used as a measure of performance: packet delivery ratio, average end-to-end delay, average hop count, normalised routing overhead, and packet dropping rate. Unfortunately, no baseline results were made available for comparative purposes. The results obtained from the packet delivery ratio showed that black hole attacks had the most substantial impact on the network followed by selfish nodes type 2 attacks, and grey hole attacks. It was also noted that the delivery ratio decreased during all attacks. The results from the end-to-end delay performance measure indicated that black hole attacks caused minimal delay. The authors mentioned the reason for black hole attacks having the smallest delay was due to the fact that all the packets were dropped and the network was less occupied than usual. Selfish nodes type 2 were also low, which correlates with the results from the black hole attacks. Furthermore, results from the average hop count performance measure showed the impact black hole attacks have on the network. The hop count drastically decreased during black hole attacks with the second lowest hop count being recorded for selfish nodes type 2. Grey hole attacks and selfish nodes type 1 were found to possess low impact since standard data packets traversed through the network commonly. The results indicated substantial declines in nor-

malised routing overhead for grey hole attacks and selfish nodes type 1, because the attacks dropping route discovery packets. The black hole nodes and selfish nodes type 1 do not affect routing packets and thus indicate optimal performance. The results from the packet drop rate performance measure came as no surprises since the black hole attacks turned out to be the most significantly impactful. The results showed selfish type 2 as the second most significant impact.

The authors in [15] used ns-3 to simulate black hole attacks along with Jellyfish attacks in a mobile ad hoc network. 25 nodes in a 25x100-meter grid with a Constant Position mobility model was used. Thus, the network was static. The simulations was run for 20 seconds and a single malicious node was only inserted into the network. The authors found that black hole nodes increase network capacity. The cause is explained by the attack dropping route discovery packets from the network. This behaviour denies multi-hop flows while allowing single-hop flows.

Attack detection is an approach that has been adopted for tackling security related issues in MANET. The study in [16] has highlighted the use of intrusion detection as a combination of anomaly-based and knowledge-based detection for identifying black holes in a MANET. The advantage of this approach is that it can be used for multiple

attacks, and the test results proved to be promising. Another study [17] has reported success with intrusion detection simulations. An Intrusion Detection System with the help of genetic algorithms, which monitors the behaviour of nodes to make better decisions, is presented in [18]. This solution was simulated and showed very positive results.

The detection and prevention of flooding attacks using Support Vector Machine, which also applies machine learning, was proposed in [19]. The authors used ns-3 and found improved results from a previous similar attempt and in general good results for an Intrusion Detection System.

The authors in [20] used machine learning and corresponding models to identify black hole nodes and their simulation results revealed an improvement in black hole node identification. The study [20] employed a hybrid from the study in [21] with their Support Vector Machines that also apply a trust scheme.

A method to monitor the sequence number of route request messages was introduced in [22] whereby the route request message gets discarded if anomalies are found. The authors investigated sink hole nodes, which necessarily have the same behaviour as black hole nodes. This method of detection is simple and simulation results were found to be positive.

The authors in [23] categorised selfish node behaviour into two broad categories, namely: credit-based schemes and reputation based schemes. In credit-based schemes, nodes get an incentive for good behaviour; however, this approach has specific hardware requirements. The other reputation based scheme has more promise. This scheme makes sure that a node sends data and then rates the node, while its second module uses this rating to find paths. The use of ns-2 while adding the 2ACK scheme to the node monitoring part of the watchdog overcomes shortcomings and provides promising results.

An interesting solution from [24] uses reputation implemented with block chain to build a decentralised and publicly verifiable record of nodes' reputations.

A key management scheme for nodes authenticating nodes was suggested in [25]. This builds a secure network and naturally excludes unauthorised nodes. This approach does not deal with the attack per se but instead looks for methods to prevent the attack. The solution was not simulated, and network overhead was not determined.

The research presented in [26] suggests a solution that secures the network using cryptography by introducing a centralised trust authority for critical negotiations to authenticate nodes.

The application of cryptography to create a secure network is fur-

ther suggested in [27]. The authors implemented a security scheme that uses digital signatures and hash chains for authentication and security. The solution was simulated and corresponding results showed less overhead while securing the network. However, this method requires a central authority server.

Changing the AODV protocol by adding weights to the route request reply message ratios was suggested in [28]. The updated protocol needs to inject additional messages to retrieve the node weights. Based on the feedback, a node that indicates undesirable ratios is less likely to be used.

A solution introducing security agents into the network to detect black hole nodes is suggested in [29]. This method requires changes to the standard AODV packets and introduces security agents who monitor the MANET and send notifications when black hole nodes are found. The simulation results show that the technique works well for both single and cooperative black hole attacks.

The survey conducted in [30] suggests securing the network using cryptography in multiple protocols, as well as providing reputation based solutions. It also presents a comparison of different solutions. The authors have argued that the reputation based solutions offer the most successful solutions against black hole attacks, an argument that

is strongly support by this author.

Authors in [31] proposed a solution involving the addition of an attribute of honesty to a node, and other nodes use this value to determine if the node should be used or not used for packet forwarding. This value is kept by other nodes and not the node under investigation. The provision of some rules for the "honesty" value calculation increased the throughput of the network, which was validated by the simulation results.

Authors in [32] suggest a trust-based solution where neighbouring nodes calculate a trust value of nodes around them. If the trust threshold goes below a predefined value, the node rejects the neighbour from forthcoming routes. This solution was simulated on ns-2 and showed much better results in scenarios when the AODV protocol is under attack.

A recommendation that simulation tools should have some standard to be able to compare results of simulation solutions for MANET security issues was presented in [33]. This is considered necessary in order to allow an accurate comparison of results from other related works and thus make convincing conclusive remarks.

A new concept of packet leashes is described in [34]. The attack solution was explicitly created for wormhole attacks that attract data

packets and tunnel the packets to a location not intended for the data. This solution is too specific to be reused for black hole attacks.

Changes to the AODV protocol involving an addition of timers to packets were made; these are presented in [19]. It collects data from different routes, and once the timeout is reached, an appropriate route is used. The simulation results are promising and the solution is simple.

Authors in [35] have proposed a second confirmation route request message in the network and found a path to the intermediate node (one sending a reply). Thus, the proposed solution has a reverse look up from the destination node, and it is quite complicated. Despite appearing to be promising, this solution was not implemented as it appears to create extra delays along with additional network traffic.

3.3 Dynamic Source Routing

DSR is an on-demand routing protocol used in MANETs. This protocol sends out a route request message to all nodes in the network and each node receiving the request will add themselves into the route and forward the message to their neighbours. If the node is the destination, or if the node has the route to the destination it sends a route reply to the source. The source collects multiple route replies, and can afford to choose and reuse routes in the network. If a route is broken, a route

error message is sent and a new route request is initiated.

The authors in [36] have carried out simulations and compared flooding attacks with black hole attacks in DSR and found that flooding attacks are more dangerous while black hole nodes cause more damage. The authors used ns-2 for their simulations and simulated RREQ flooding attacks along with black hole attacks on a mobile ad hoc network using DSR protocol. Their simulation employed a 1000x1000-meter grid with 50 nodes. Those nodes moved between 1 and 10 meters per second with a Random Waypoint mobility model. The packet size was 64 bytes with a buffer size of 4 packets per second. The simulations ran for 300 seconds at a time. The authors used packet loss rate, average end-to-end delay and throughput to measure the performance of the protocol. Their simulation results indicated that, during the RREQ flood attack, an initial rapid increase in the packet loss rate which eventually reached a plateau of less than 100% was recorded when the flood frequency was increased. The black hole attacks had a significant decrease in throughput when the black holes increased over a period of time. It was concluded that the flooding attack is more harmful than black hole attacks.

In [37], simulations have confirmed that performance deteriorates while under attack from black hole. The ns-2 simulation tool was used

in a 670x670-meter grid, with 20 nodes. The nodes moved at 20 meters per second, and the simulations lasted for 500 seconds. The packets were 512 bytes and sent at a rate of 4 packets per second. Throughput, end-to-end delay and packet delivery ratio was used for measuring performance. Results of this study [37] indicated throughput, end-to-end delay and packet delivery ratio reduced in the presence of a black hole. More specifically, whereas the throughput and end-to-end delay decreased by 32% and 78%, respectively, the delivery ration decreased by 31%.

Several protocols (Gradient-Based Routing (GBR), DSR and Greedy Forwarding (GF)) were compared [38]. Their simulations were done in WSNet, an event-driven simulator, in a 100x100-meter grid containing 300 nodes. Other than running 100 simulations for 100 seconds each, the average delivery ratio, the average degree of nodes and average path length, were used as performance measures. Results obtained indicate that the average delivery ratio decreased when the number of compromised nodes was increased. It is noteworthy that the compromised nodes that are close to the destination received more packets for retransmission, and this caused the attacks to be more active when closer to the destination node.

General detection of malicious nodes is proposed by [39]. They

specifically looked at grey- and black hole attacks. This is an exciting approach to being able to detect or mitigate misbehaving nodes, in general, has many benefits to a MANET. [40] proposes an adaptive approach to detect malicious nodes by monitoring the next hop in the current node path.

Another approach for deterring malicious nodes involves authentication of the network. To this end, an addition of authenticity to routes by adding verification packets to identify if they are from trusted nodes has been suggested and an improved performance of DSR while under black hole attack was demonstrated [41]. A similar solution involving the addition of a validity value in a route reply message has also been proposed [42]. The previously mentioned validity value is controlled by the first next-hop along with the route reply to warrants that there is no black hole attack along the route. Only routes with valid validity values were considered and no simulations were undertaken.

A cryptography solution has not been tested against attacks despite having being proposed as a potential solution [43]. The introduction of the overhead has apparently increased performance of the network while malicious nodes are present [43].

An interesting approach to validate sequence numbers by having strict increment operations with an end-to-end acknowledgement that

detects incorrect information has been reported [44]. Although the solution has a small impact on the operation of DSR, it has shown excellent performance.

Trust-based solutions add some element of trust between nodes to adapt to misbehaving nodes and discard them from the network. The authors [45] have proposed a method where nodes monitor traffic from their neighbours to validate if their behaviour is malicious. The simulations have shown that malicious nodes could successfully find and mitigate black hole attacks.

An association based routing whereby nodes classify their neighbours into three different associations and use this mapping for routing transactions in DSR has been proposed [46]. Through simulation, an increase in routing security was confirmed. This approach will isolate misbehaving nodes over time.

An addition of a list of known black hole nodes, an enhancement of DSR that avoids these nodes, has been suggested [47]. Other work relating to the enhancements for the protocols to improve performance by addressing link breakage and introducing feedback loops has been reported [48], [49]. These type of enhancements show that the base protocols are still being developed.

3.4 AODV vs DSR

From [50], we have concluded that the protocols are capable of delivering a quality of service (QoS) strong enough for voice over IP. The analysis helps to achieve a better understanding of the standard protocols and their performance. This work [50], used the OPNET Modeler to complete simulations in a 2000x2000-meter grid consisting of 30 nodes. The nodes were moving with the Random Waypoint mobility model running from 0 to 15 meters per second. Traffic was generated using FTP, HTTP and VOIP protocols. The primary network parameters for QoS performance that were compared are: voice throughput, number of packets dropped, HTTP object response time, end-to-end voice delay, and others. It was found that the route discovery and the number of hops are higher for DSR. However, AODVs respective values, which increased during the simulation, was ascribed to how DSR caches routes while AODV does not. It was found that DSR sends the most routing traffic, as well as the most routing errors. DSR has a more substantial delay in VOIP data transmission as it caches the route and old routes can be used which cause retransmissions. On the other hand, AODV is more reactive to network changes, which decrease voice end-to-end delay. Overall, AODV also has less jitter. DSR drops more data because of buffer overflows and retrans-

missions. In conclusion, AODV was recommended by the authors for VOIP data [50].

A comparison of the performance of AODV and DSR were compared revealed that a black hole attack gave rise to a significant decrease in delivery ratios, with both protocols performing poorly [51]. However, a hybrid hierarchical routing protocol sharing benefits from both AODV and DSR performed slightly better.

It has been confirmed that AODV and DSR are both affected by black hole attack, although AODV performs better [4]. The ns-2 simulator with high and low density of nodes in their simulation in a 670x670-meter grid was used. The DSR was found to possess data loss of 55% to 60% while AODV had data loss of 45% to 50% in the presence of black holes. No mention was made under which node density these results were obtained; it is plausible that an average over both was used.

A comparative analysis in [52] indicates that DSR outperforms AODV. An ns-3 in a 1500x300-meter grid with 50 nodes and a transmission range of 250m as well as the Random Waypoint mobility model were used. A comparison of AODV and DSR under wormhole and black hole attacks and their simulations show that black hole attacks affected AODV much more than wormhole attacks [53]. The study

in [10] simulated wormhole attacks and the data indicated that the DSR is more affected than AODV. From this analysis, we can expect either AODV or DSR could perform negatively, while under attack by black hole attacks.

From [54] AODV and DSR are compared using the Random Way-point model and they concluded that AODV has less impact when under attack from a black hole, than DSR. This data helped identify a model bias in research with MANET's.

3.5 Theoretical Foundation

As discussed in [55] there are five types of theory. These theory types are described briefly here.

The **analysis theory type** involves only analysis and description of the theory. Generally, this theory type is used when very little is known about the phenomena in question. The **explanation theory type** involves explaining a theory without any testing or predicting. This theory type is typically used when the phenomena in question are understood. The **prediction theory type** involves predicting outcomes of a phenomena with testable propositions. This theory type is typically used when parts of a system is a black box and outcomes are observed or predicted instead of explained. The **explanation and**

prediction theory type combines details from the explanation and prediction theory types to provide predictions, testable propositions and causal explanations. This theory type implies both understandings of underlying causes and prediction as well as descriptions of theoretical constructs and the relationships among them. The **design and action theory type** involves instructions on how to build and deploy a theory. This theory type is typically used when the phenomena can be built.

This research is based on multiple theory types, more specific explanation, prediction, design and action theory types. The reason being that we describe how AODV and DSR function and how the black hole attack affects the protocols followed by an implementation of the attack in both protocols with simulation results to compare the impact on the two protocols.

3.6 Summary

From this literature review, we can expect either AODV or DSR could perform worse, while under attack by black hole attacks. The report of the existing related works presents different observations, which informed our study to conduct such simulations in favourable setups for accurate results analysis.

The data obtained from other teams is used to build the simulation

criteria. This is done to ensure that the results are comparable and that we can clearly see our data is confirmed by other studies.

4 Experimentation

In this study, simulations were used to experiment with the performance of two reactive routing protocols. The performance of these protocols was measured under different conditions and by being attacked by introducing a black hole node in the node population. When using simulations, the results are expected to be reproducible. The simulations used in this study have the same underlying structure, since they developed by the ns team, and can, therefore, be used to reproduce the results using the open source code with the configuration supplied in the simulation criteria section 4.1. The simulation configuration is relatively easy to configure and to execute. When using simulations, it is possible for the conditions or configuration to become unrealistic. Even though this might be the case, we aimed to determine the performance of the protocols and match them against each other by using conditions that are as closely realistic as possible.

The ns-3 simulation platform was used, more specifically version 3.26. The source code for the protocols and testing examples are available from their mercurial repository. The manet-routing-compare example was modified for this experiment. This implementation uses an OnOffHelper class, which enables us to use the ns-3 OnOffAppli-

cation feature. As the name suggests, this feature generates traffic in a pattern that switches on and off. The duration of each state can be configured. When in the on state, traffic is generated according to a configurable data rate and packet size. The traffic is generated to a single destination. The configuration used for the simulation is ten source and sink nodes, which are in the On state for one second. The rate configured is 2048 bits per second with a packet size of 64. The maximum received rate for a simulation is therefore 20.48-kilobits per second. This maximum value was used to determine the percentage of throughput for each protocol.

The black hole nodes were introduced into the system by modifying the node implementation in the network model network/model/node.cc and network/model/node.h. A variable was introduced here to set a node with a status of malicious or not malicious. Inside the AODV protocol, changes were made to the aodv/model/aodv-routing-protocol.cc class where we enabled a variable for the node to act maliciously or normally. The black hole node will respond to route requests and drop traffic designated to pass through it. Similarly, for DSR, two classes were modified to replicate the behaviour, namely dsr/model/dsr-options.cc and dsr/model/dsr-routing.cc.

4.1 Simulation Criteria

The simulation criteria used is a network of 50, and 100 nodes simulations, each moving at 20 or 200 meters per second in area size of 300x1500-meters. The area is defined by a position allocator and the Random Rectangle Position Allocator was used for all simulations. The allocator allocates random positions within the x and y parameters supplied to it. The nodes have a data rate of 11 Mbps while using the Range Propagation Loss Model in ns-3 to add signal propagation loss. The simulation is run for 200 seconds at a time, where the first 100 seconds is used for the network to move randomly. The network has ten sources and sinks nodes for random transmission through the network. Three mobility models where used to create four different sets of data for each model. The models used are listed in subsections below. For each of the mobility models, a different configuration was used. From related works, AODV and DSR perform differently when node speed and density is changed (see section 3). The node speed values chosen was 20 meters per second, which supplies a standard speed scenario, and 200 meters per second, which supplies an abnormal speed scenario. Node density was set at 50 nodes, which supplies a standard density scenario, and 100 nodes which supplies a dense population scenario. Results were calculated during the simulation and consisted of

receive rate and packets received per node. This data was logged per second during the simulation.

4.1.1 Random Direction 2D Mobility Model

This mobility model has three parameters, namely "pause", "speed" and "bounds". From the ns-3 documentation, movement of objects is based on random direction and speed. Each object will pause for a configured delay before travelling in a random direction and speed until a boundary has been reached. After which it will pause, select a new direction and speed and start travelling again. For this simulation, two second pause time and various speeds were used. This model has the most straightforward movements of all models described in this study.

4.1.2 Random Waypoint Mobility Model

This mobility model has three parameters, namely "pause", "speed" and "PositionAllocator". From the ns-3 documentation, each object starts by pausing when the time is zero for the span of the variable "pause", after pausing the object will choose a new waypoint through the PositionAllocator and a new random speed through the "speed" parameter and begin moving toward that waypoint at a constant speed.

When it reaches the destination, it repeats the same process by pausing. Movement is bound by the allocator. The distance travelled by the object is random, .i.e. the distance can be short or long and will be recalculated if a boundary is reached. For this simulation, a zero pause time and various speeds were used.

4.1.3 Random Walk 2D Mobility Model

This mobility model has seven parameters, namely "pause", "speed", "time", 'distance", "mode", "direction" and "bounds". From the ns-3 documentation, each object travels with a speed and direction determined at random via the parameters until a set distance has been walked or a set amount of time has been reached. If the object hits one of the boundaries, it will be bounce on the boundary based on a reflexive angle and speed. This model is frequently recognised as the Brownian motion model. The only parameters changed for this model were speed and boundaries. The rest of the parameters were left as default values (Time = [1s]; Distance = [1m]; Mode = [Distance]; Direction = [Min = 0.0, Max = 6.283184]).

4.2 Simulation Snapshots

This section gives the reader visual context of the NetAnim tool, as well as how the network grid looks like with nodes and traffic. The images in this section were taken from simulation results generated for this study. The NetAnim tool was used as a visual aid while simulating the network to ensure the network criteria are valid, and the simulations are sound.

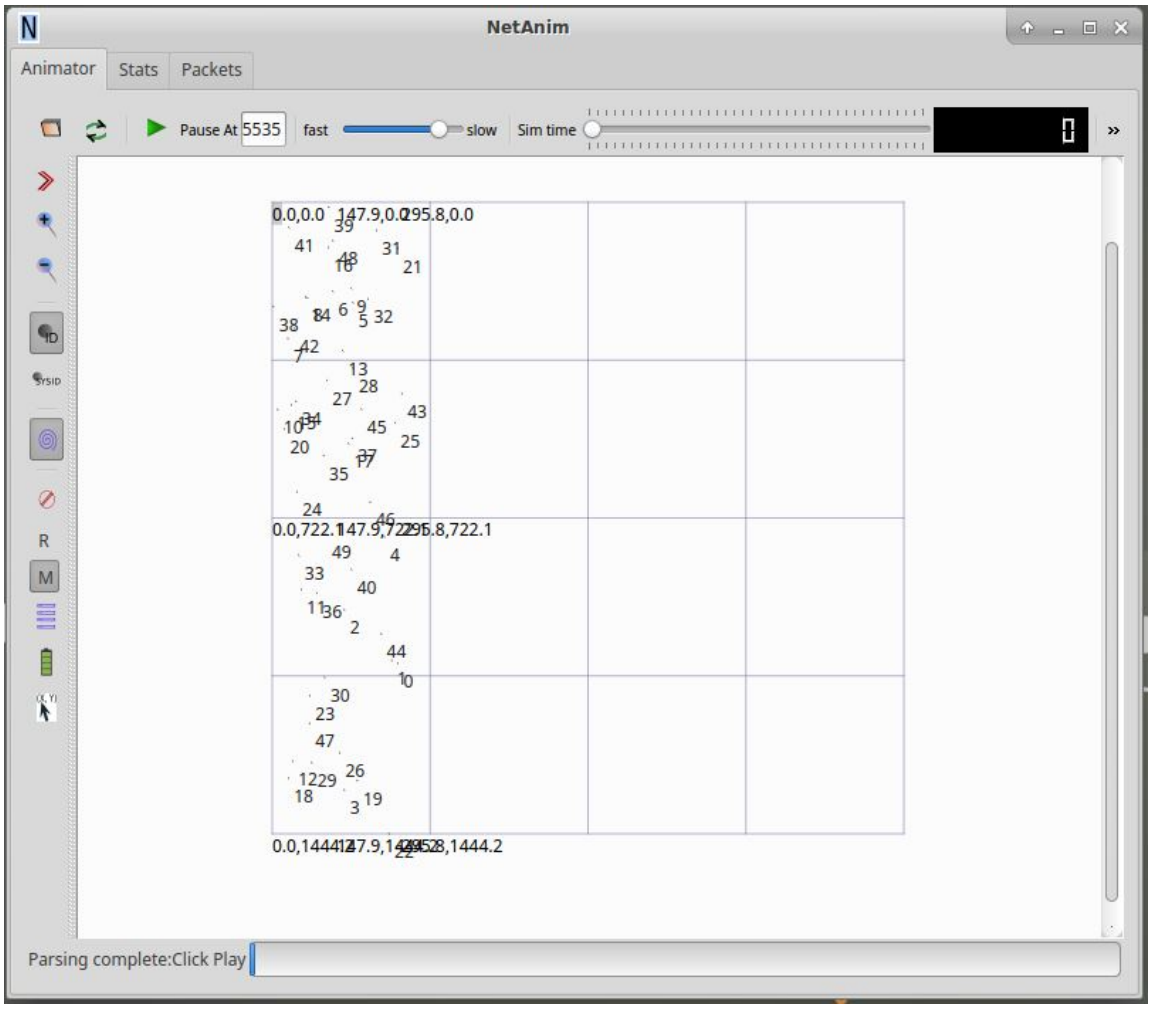

Figure 4.1: Snapshot of the NetAnim grid with nodes

In figure 4.1 is a screen shot of the NetAnim program interpreting an XML file output from ns-3. The image contains the grid layout used for the simulations along with the initial node placement.

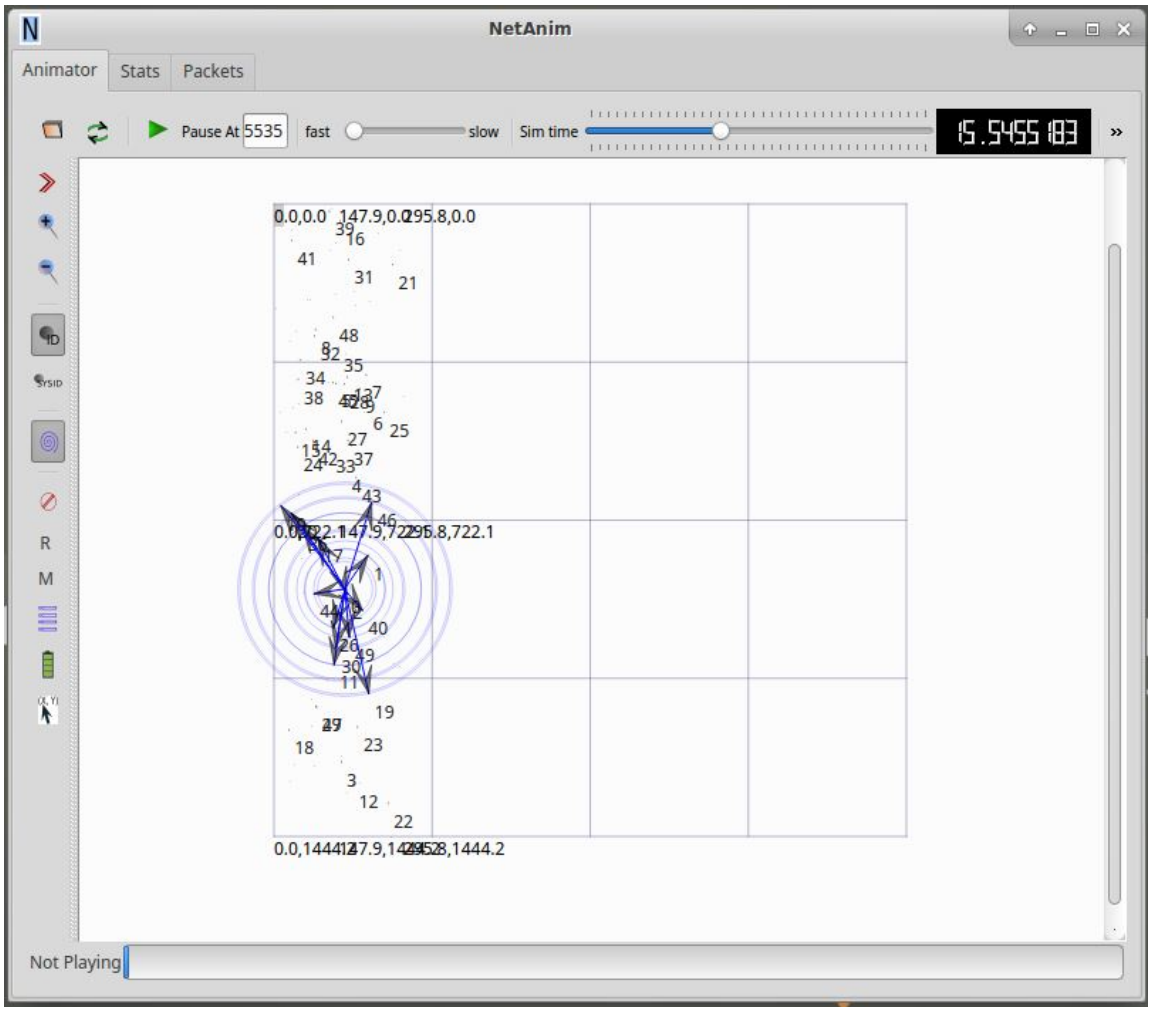

Figure 4.2: Snapshot of the NetAnim grid with traffic

NetAnim plays simulations back by showing how traffic traversed through the network. Each ring in figure 4.2 indicates a neighbour node which is in range of the broadcasting node. Also included is an arrow which represents a packet from the source node to its neighbour nodes. From this image it is easy to see that multiple nodes were reachable by the broadcasting node.

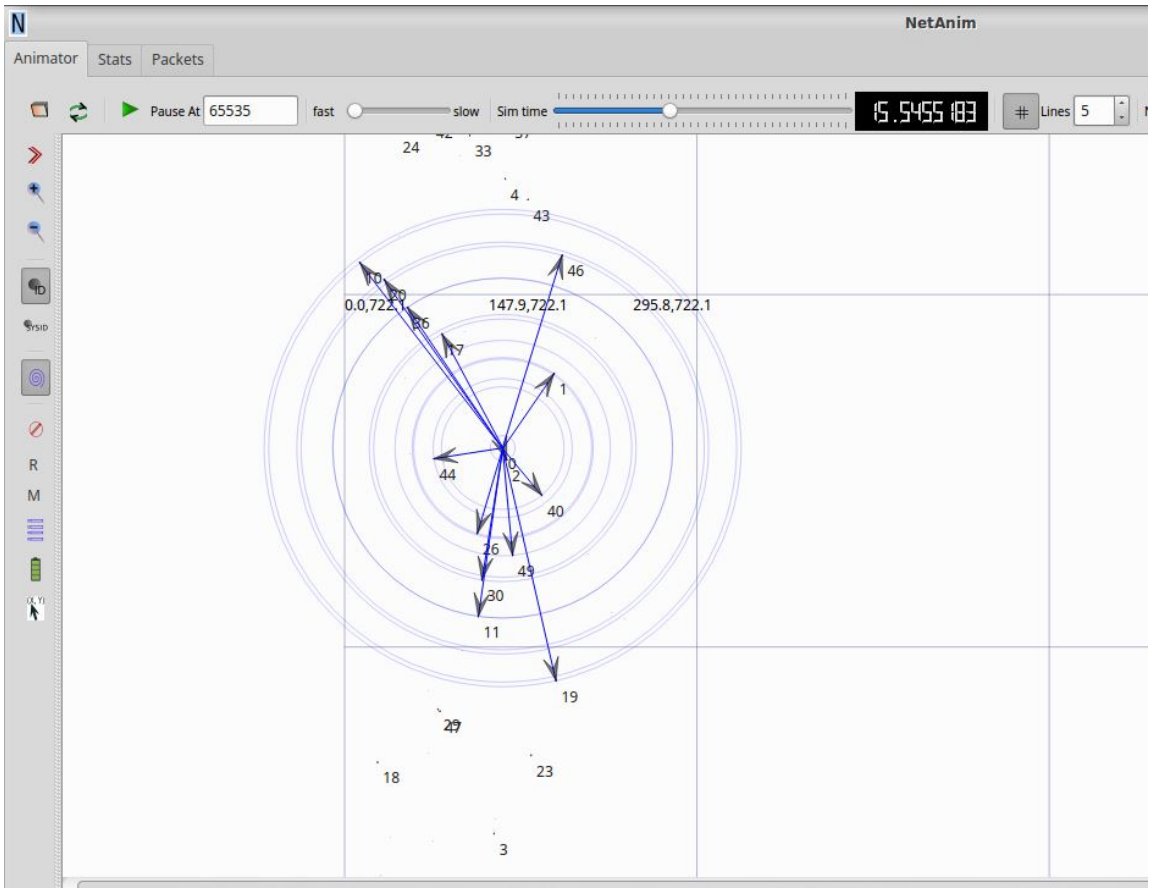

Figure 4.3: Snapshot of the NetAnim grid with traffic zoomed

Figure 4.3 is a zoomed version of figure 4.2 for presentation purposes.

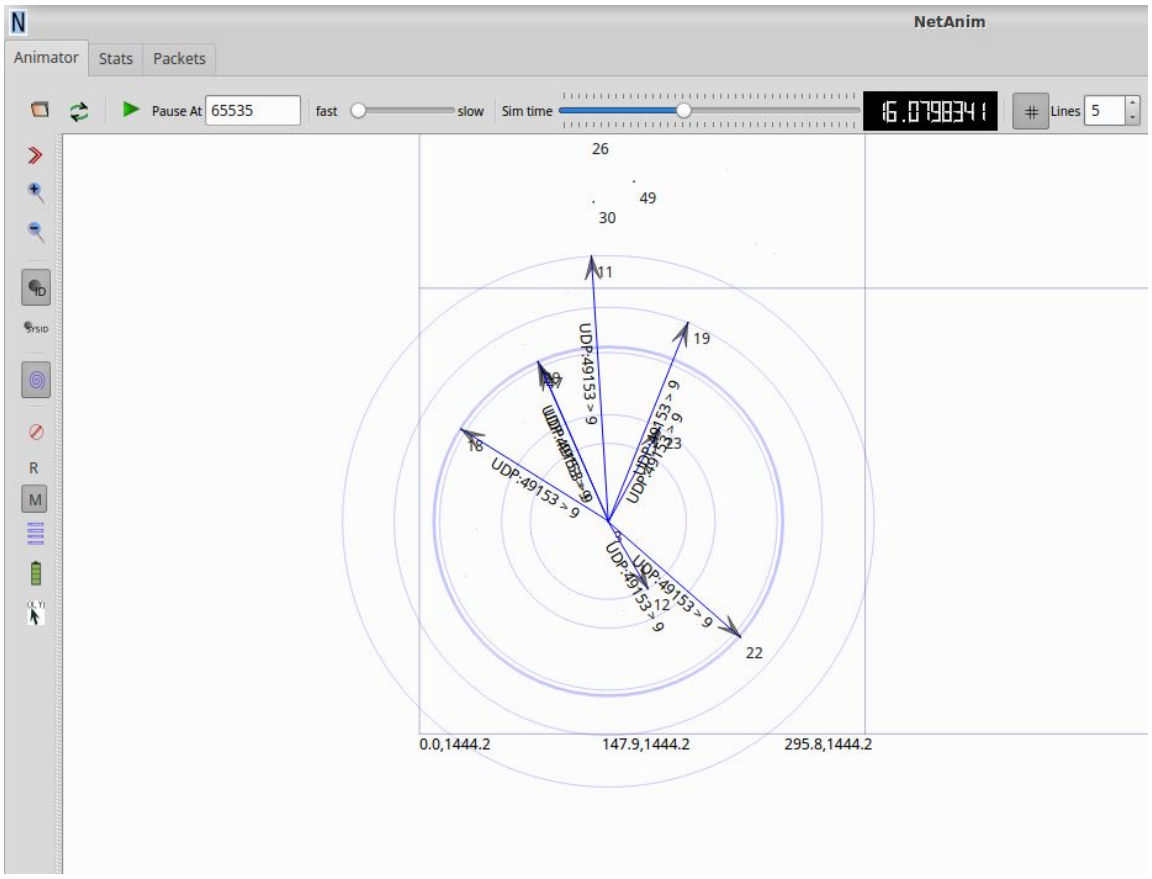

Figure 4.4: Snapshot of the NetAnim grid with traffic meta data zoomed

Another feature of NetAnim is to show the packet details on each arrow for each step in the simulation. Figure 4.4 indicates what a packet would look like with meta data enabled.

5 Results and Discussion

The results are divided into three sections, one for each mobility model. Each mobility model has four different configurations with which the simulations were executed. Each of the configurations were run without malicious nodes and with a single malicious node in the population. The data that contains the attack was averaged over five simulations where the malicious node was placed in a random position each time. This was done to average the effect of the attack over multiple positions since the position of the black hole can affect the network in different ways. For example, a black hole close to the source node will cause more damage than the one that is further away from a source node. For all graphs, the y-axis is the bytes receive rate calculated as the number of packets received while the x-axis represents time. For the simulation, the data starts transmission after 100 seconds, the values were shifted to zero for ease of presentation. It is noteworthy that when the population density was increased, the number of malicious nodes stayed constant as it was not a percentage of the population. This implies that simulations with higher node density possess a lower malicious node ratio.

5.1 Random Direction 2D Mobility Model

Table 5.1: Random Direction Summary table

Protocol	Speed	Density	Receive Rate[Avg. Kbs]	Through Put[%]	BH
AODV	20	50	14.05	68.6	0
DSR	20	50	15.44	75.39	0
AODV	20	50	8.064	39.37	1
DSR	20	50	13.67	66.74	1
AODV	20	100	14.05	68.6	0
DSR	20	100	15.44	75.39	0
AODV	20	100	7	34.17	1
DSR	20	100	12.99	63.42	1
AODV	200	100	10.22	49.9	0
DSR	200	100	9.52	46.48	0
AODV	200	100	7.79	38.03	1
DSR	200	100	8.84	43.16	1
AODV	200	50	10.22	49.9	0
DSR	200	50	9.52	46.48	0
AODV	200	50	7.57	36.96	1
DSR	200	50	9.19	44.87	1

The simulation for this mobility model shows the impact of the attack as well as clear trends during network configuration changes. As shown in Table 5.1, four simulations with a different configuration that were completed are observed. The movement of these nodes are based on the direction and continued to move in that direction until a boundary is reached. The node movements are less sporadic than those of the Waypoint mobility model. Whereas all nodes will move in a direction

until a boundary is hit, the Waypoint model will move in short or long distances making the movement more unpredictable.

5.1.1 Normal speed and normal density

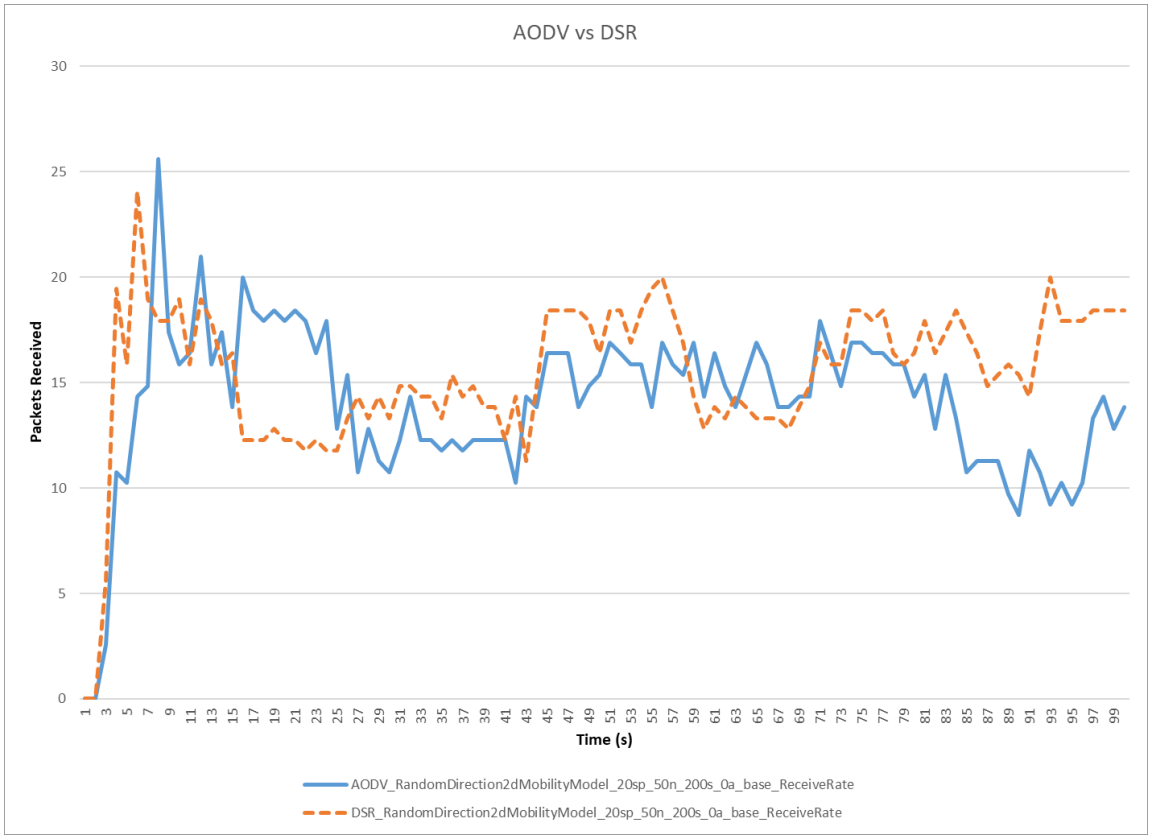

Figure 5.1: Random Direction; 20 m/s; 50 nodes; 0 bh

As shown in Figure 5.1, during the baseline of this simulation, DSR outperformed AODV marginally with 6.79% more throughput in the network.

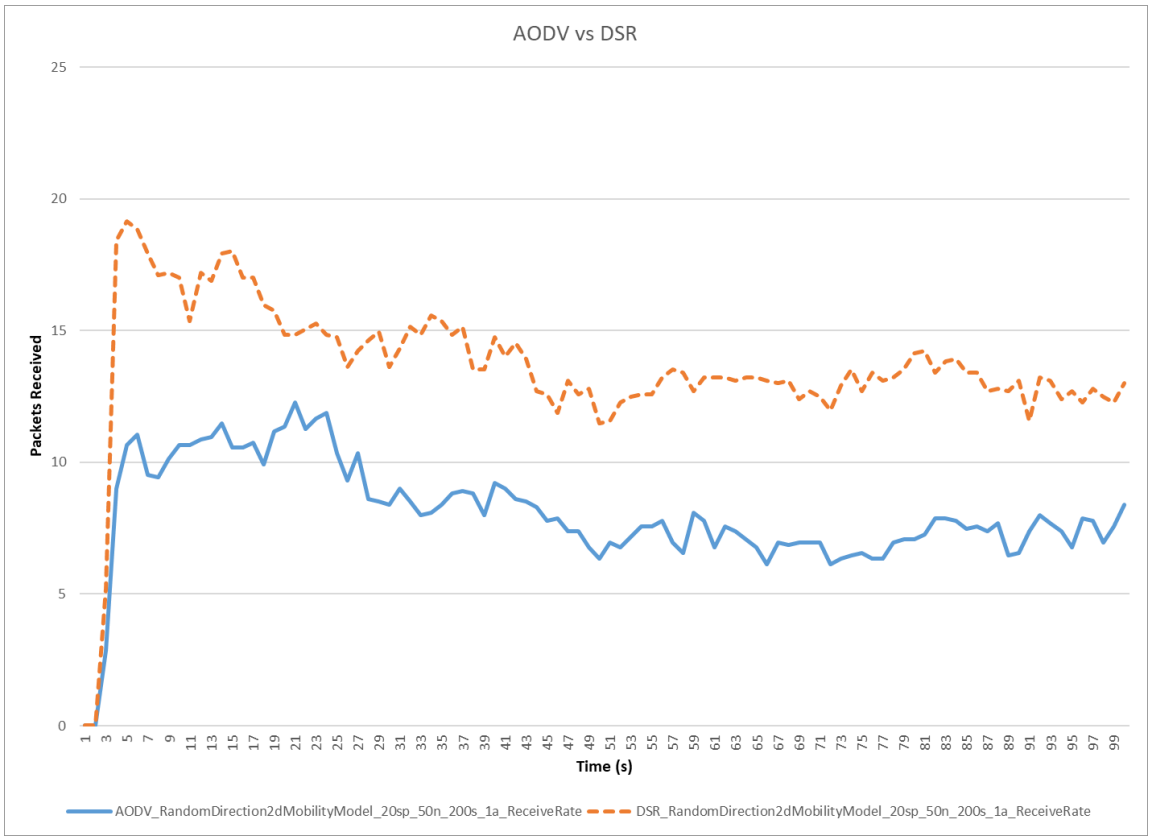

Figure 5.2: Random Direction; 20 m/s; 50 nodes; 1 bh

While under attack, AODV performance dropped by 29.23% indicating a significant impact on the performance, while DSR showed an 8.65% decrease in performance (see Figure 5.2). Under this configuration, DSR had the least amount of impact while under attack. The results indicate a resilience to the attack from the DSR protocol while under this configuration.

5.1.2 Normal speed and high density

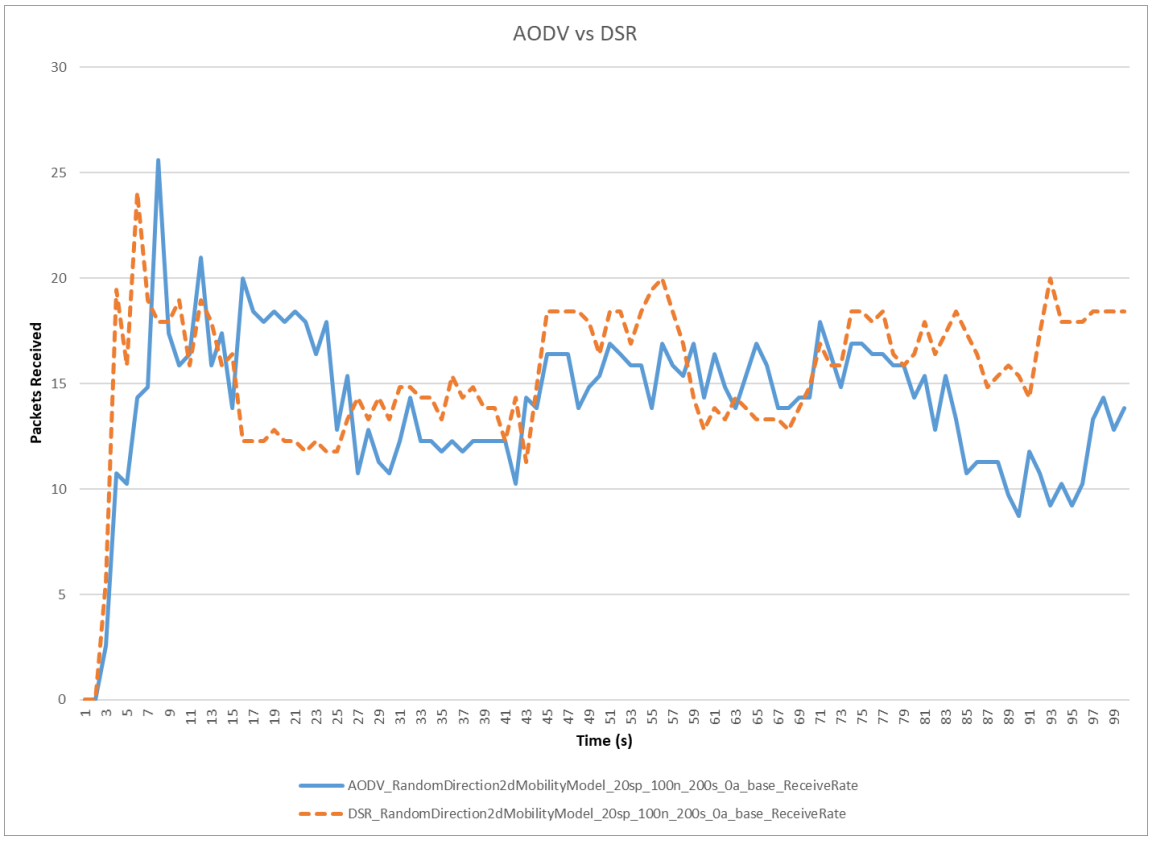

Figure 5.3: Random Direction; 20 m/s; 100 nodes; 0 bh

During the baseline of this simulation, DSR outperformed AODV marginally with 6.79% more throughput in the network (see Figure 5.3). The results show there was no impact on the performance when the node density was increased. This is due to the distribution of source and sinks nodes creating the same network as before.

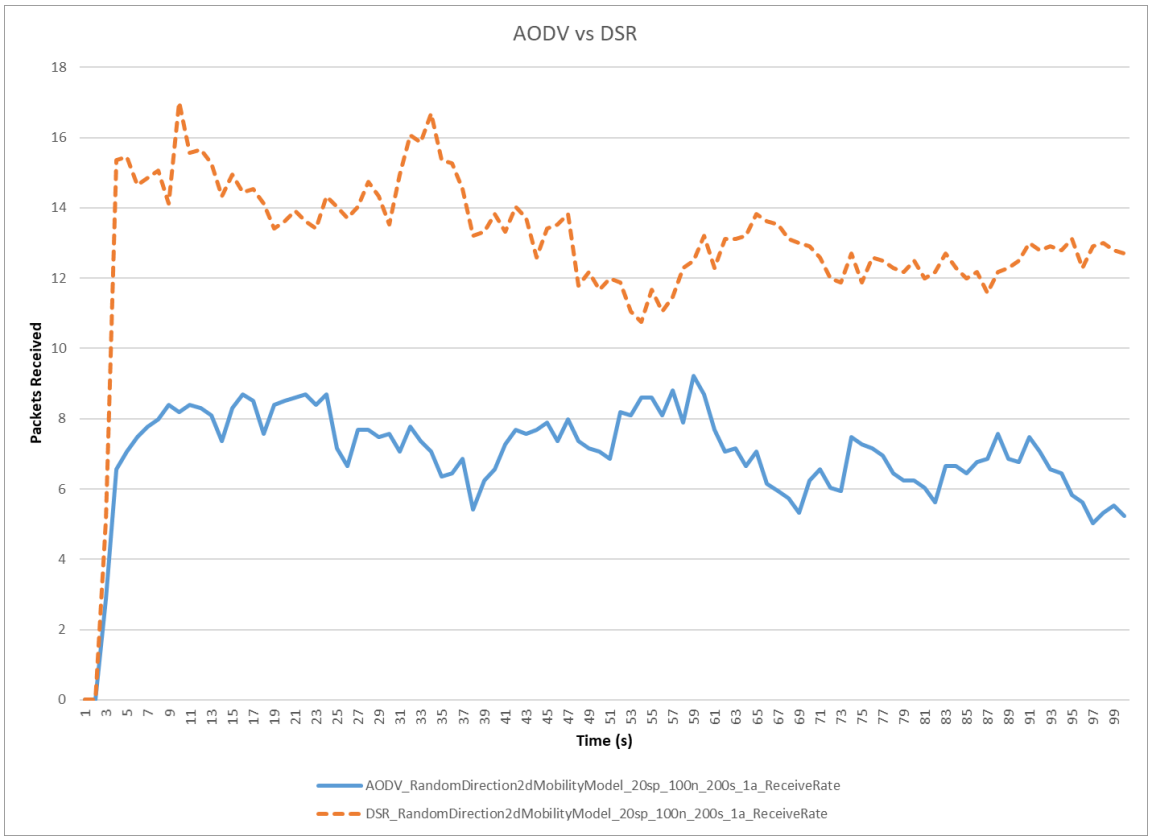

Figure 5.4: Random Direction; 20 m/s; 100 nodes; 1 bh

As shown in Figure 5.4, while under attack, AODV performance dropped by 34.43% indicating a significant impact to the performance. The DSR on the other hand showed an 11.97% decrease in performance. Under this configuration, DSR had the least amount of impact while under attack. The results indicate a resilience to the attack from the DSR protocol while under this configuration, while both protocols perform worse in a denser population.

5.1.3 High speed and high density

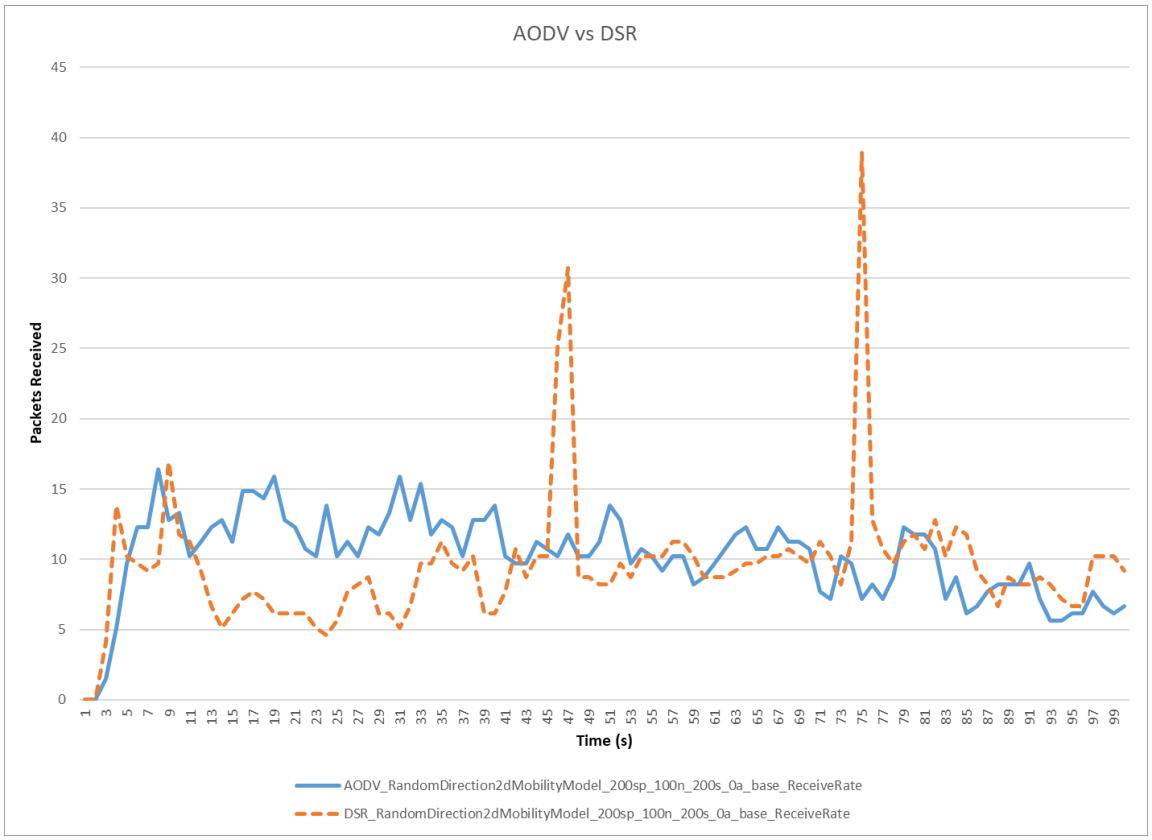

Figure 5.5: Random Direction; 200 m/s; 100 nodes; 0 bh

According to Figure 5.5, AODV outperformed DSR marginally with 3.42% more throughput in the network during the baseline of this simulation. As the nodes start to move more sporadically, an increase in AODV performance is observed.

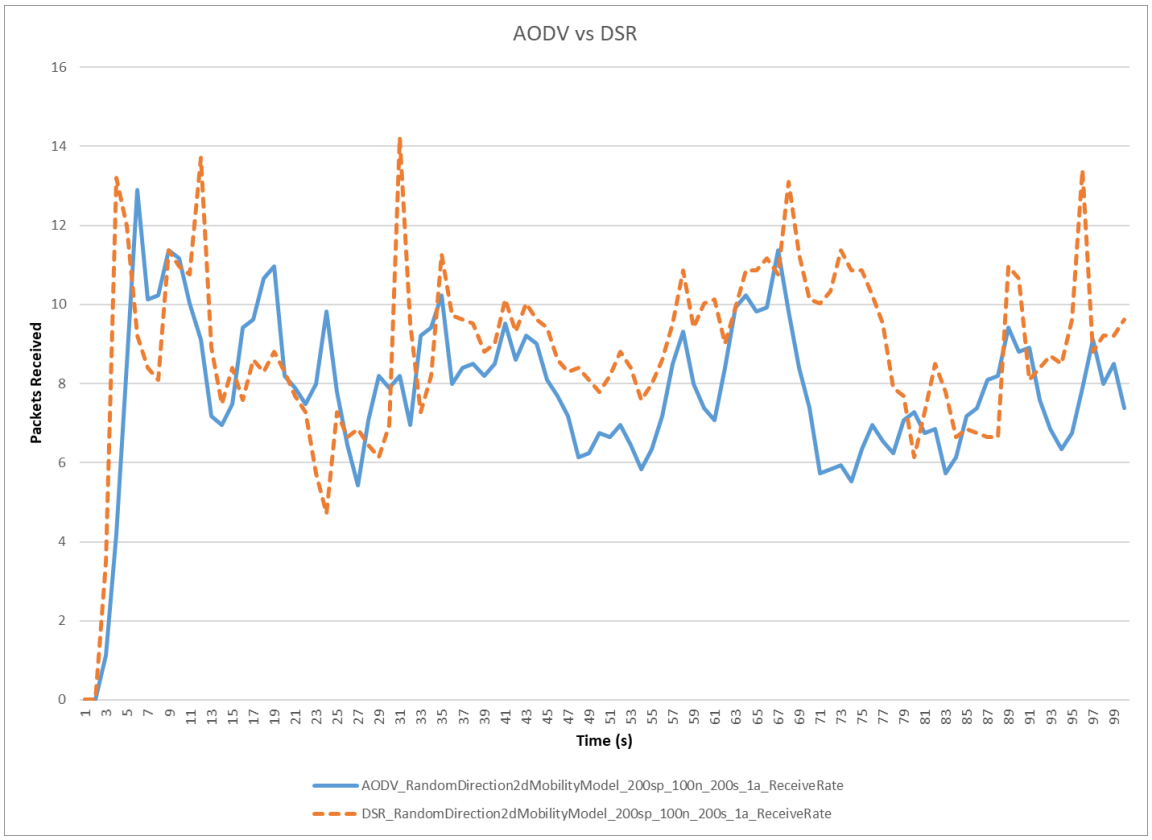

Figure 5.6: Random Direction; 200 m/s; 100 nodes; 1 bh

When under attack, AODV performance dropped by 11.87% indicating an impact to the performance, while DSR showed a 3.32% decrease in performance (see Figure 5.6). Under this configuration, DSR had the least amount of impact when under attack.

5.1.4 High speed and normal density

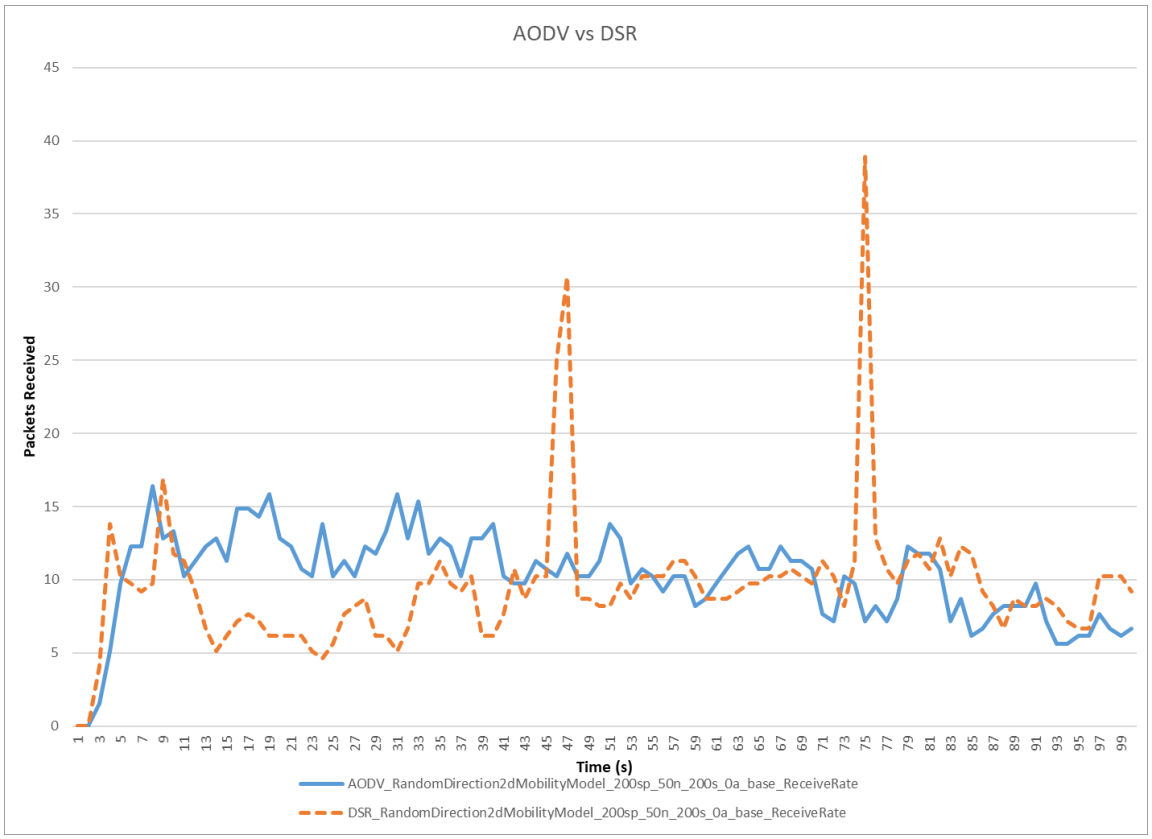

Figure 5.7: Random Direction; 200 m/s; 50 nodes; 0 bh

As observed in Figure 5.7, AODV outperformed DSR marginally with 3.42% more throughput in the network during the baseline of this simulation. Likewise an increase in the node density did not affect the base simulation.

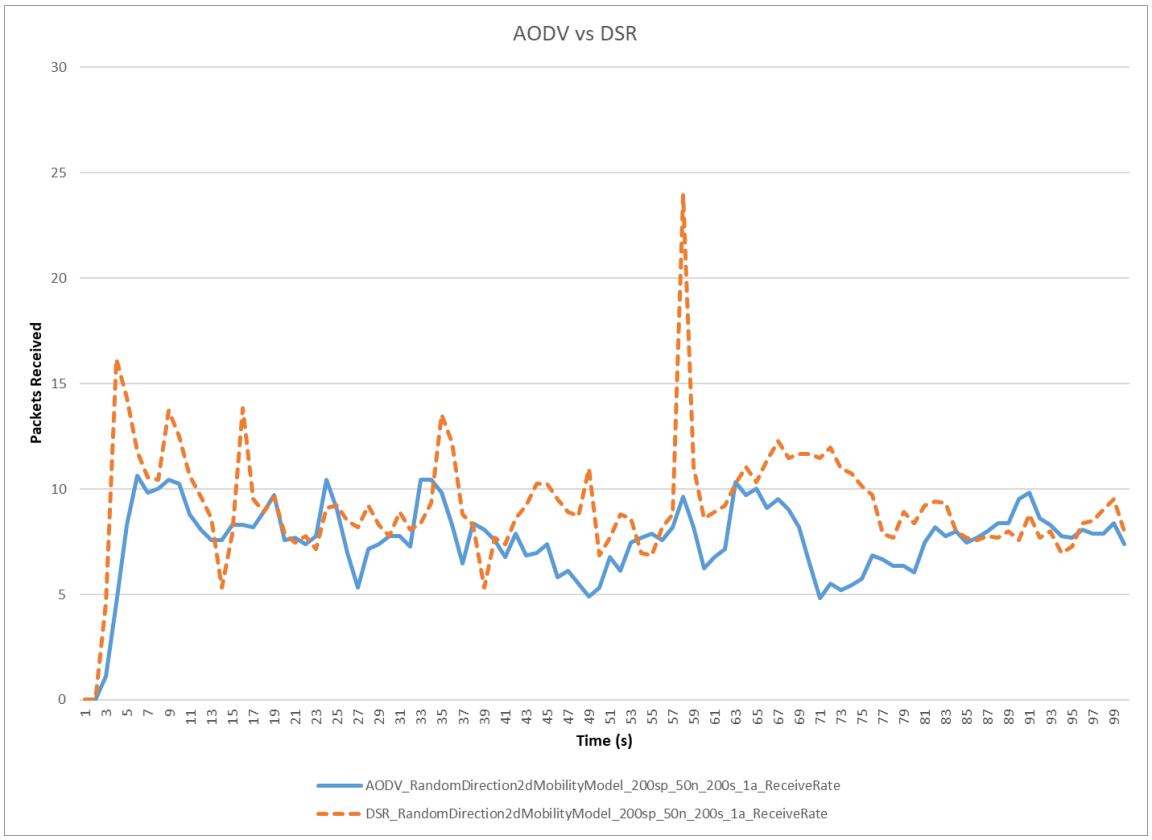

Figure 5.8: Random Direction; 200 m/s; 50 nodes; 1bh

AODV performance dropped by 12.94% indicating a moderate impact to the performance, while DSR performance showed a 1.61% decrease while under attack (see Figure 5.8). Under this configuration, DSR had the least amount of impact while under attack.

5.2 Random Waypoint Mobility Model

Table 5.2: Random Waypoint Summary table

Protocol	Speed	Density	Receive Rate[Avg. Kbs]	Through Put[%]	BH
AODV	20	50	15.18	74.12	0
DSR	20	50	13.39	65.38	0
AODV	20	50	10.03	48.97	1
DSR	20	50	12.54	61.23	1
AODV	20	100	15.18	74.12	0
DSR	20	100	13.39	65.38	0
AODV	20	100	9.51	46.43	1
DSR	20	100	12.61	61.57	1
AODV	200	100	10.47	51.12	0
DSR	200	100	8.41	41.06	0
AODV	200	100	7.88	38.47	1
DSR	200	100	8.75	42.72	1
AODV	200	50	10.47	51.12	0
DSR	200	50	8.41	41.06	0
AODV	200	50	7.74	37.79	1
DSR	200	50	8.43	41.16	1

The simulation for this mobility model indicated the precise impact of the attack as well as clear impact during network configuration changes. As shown in Table 5.2, four simulations with a different configuration was completed. The movement of these nodes are based on waypoints with random direction, making the movement sporadic and it is expected that AODV performs better in this configuration. Each of those is described in more detail in the following sections.

5.2.1 Normal speed and normal density

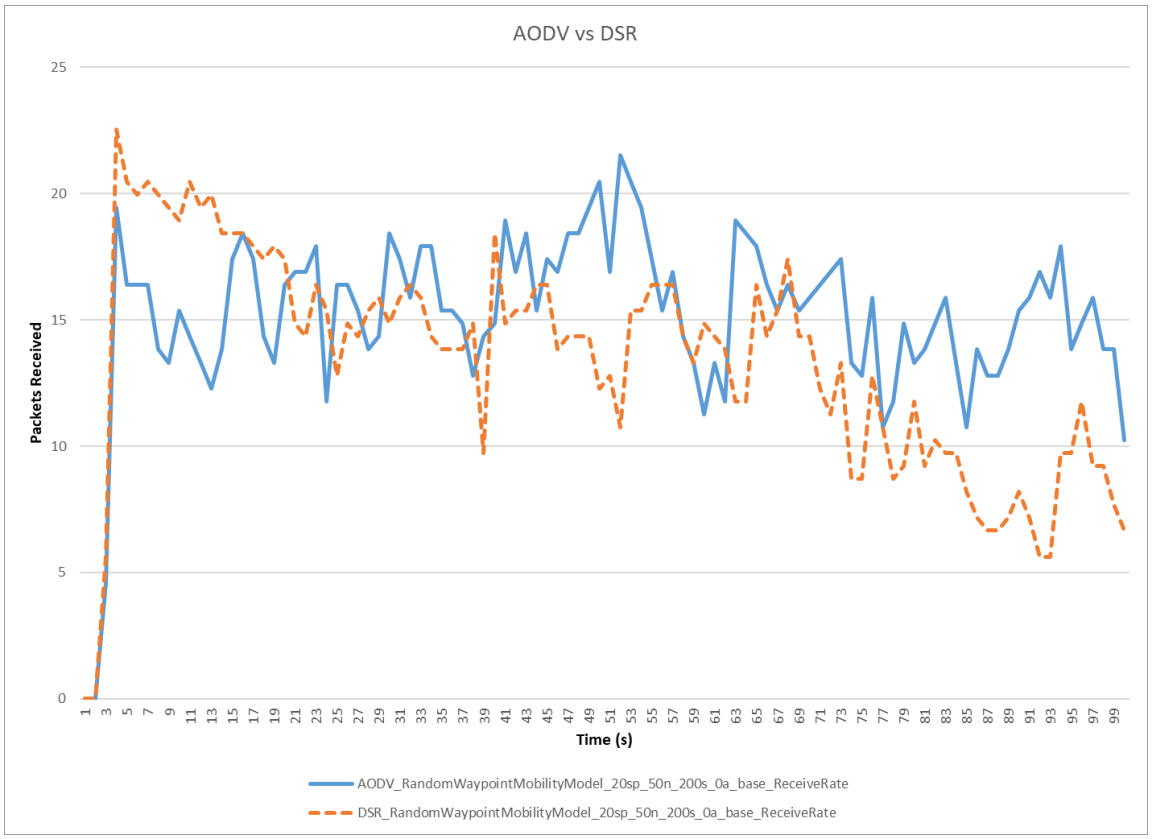

Figure 5.9: Random Waypoint; 20 m/s; 50 nodes; 0 bh

During the baseline of this simulation, AODV outperformed DSR with 8.74% more throughput in the network (see Figure 5.9).

Figure 5.10: Random Waypoint; 20 m/s; 50 nodes; 1 bh

While under attack, AODV performance dropped by 25.15% indicating a significant impact to the performance, while DSR showed a 4.15% decrease in performance (see in Figure 5.10). Under this configuration, DSR indicates the least amount of impact while under attack.

5.2.2 Normal speed and high density

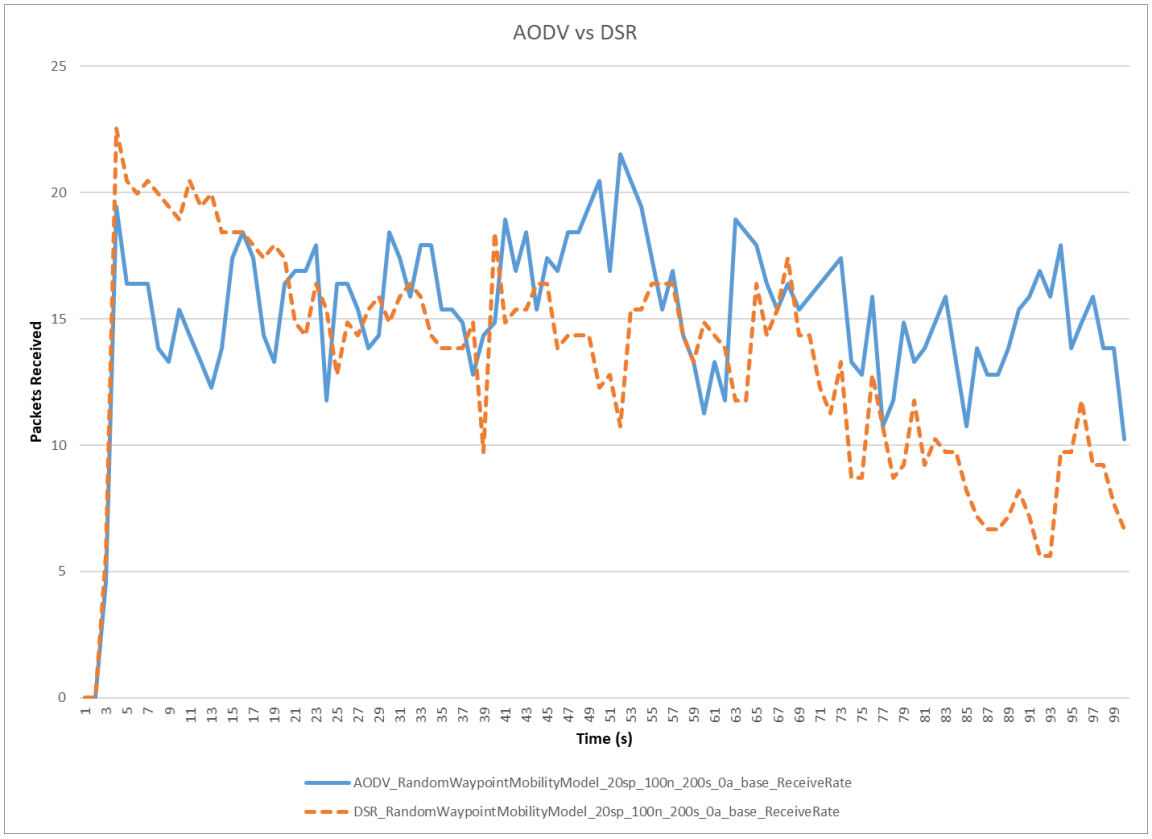

Figure 5.11: Random Waypoint; 20 m/s; 100 nodes; 0 bh

During the baseline of this simulation, AODV outperformed DSR with 8.74% more throughput in the network (see Figure 5.11). It is important to note that with double the number of nodes the performance of the protocols remained the same. This is because the random network is repeated and the source and sink node distribution are identical to those of the first instance. The routes chosen, and discovery was also the same.

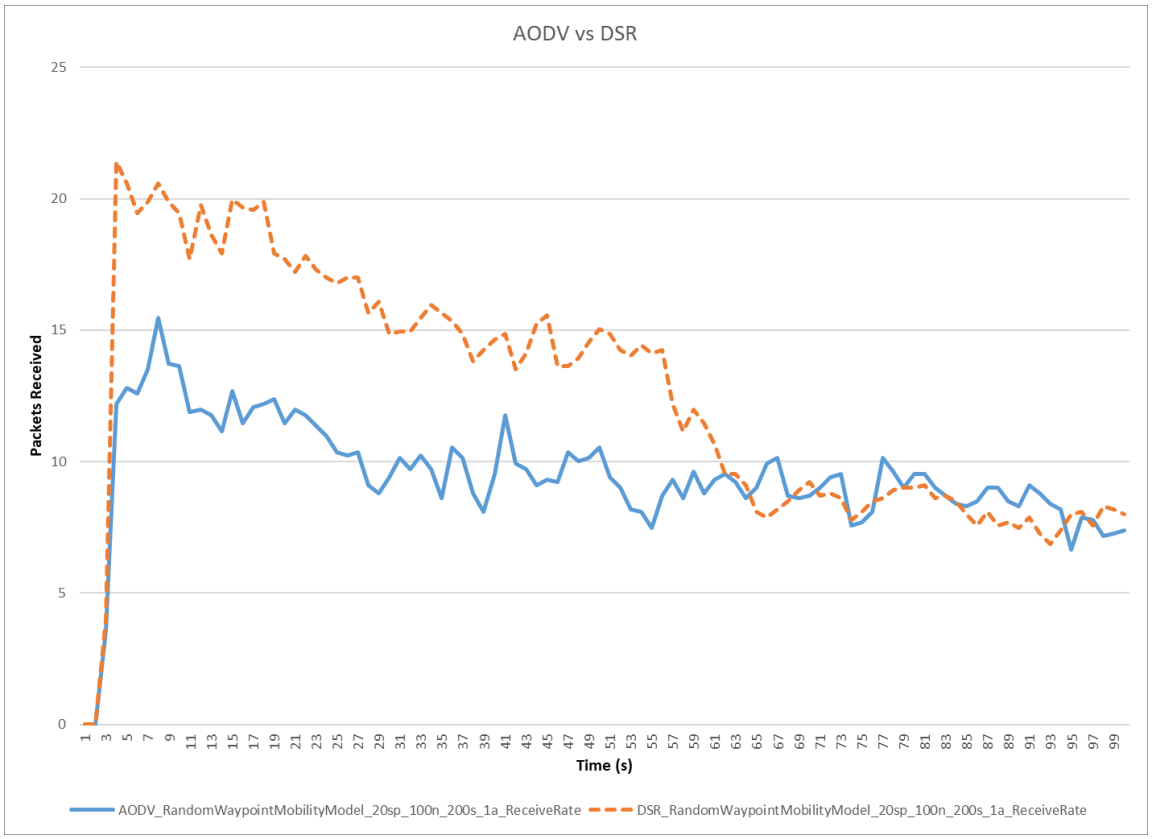

Figure 5.12: Random Waypoint; 20 m/s; 100 nodes; 1bh

While under attack, AODV performance dropped by 27.69% indicating a significant impact to the performance, while DSR showed a 3.81% decrease in performance (see Figure 5.12). The impact of the attack with additional nodes showed a decrease in damage to the DSR protocol as other routes could be used. AODV overly performed worse with additional nodes. This is because the position of the black hole has an impact on the effectiveness of the attack, and for the simulation, the malicious node was moved to random positions in the network in

order to accommodate this effect into the data. Under this configuration, DSR indicates the least amount of impact while under attack.

5.2.3 High speed and high density

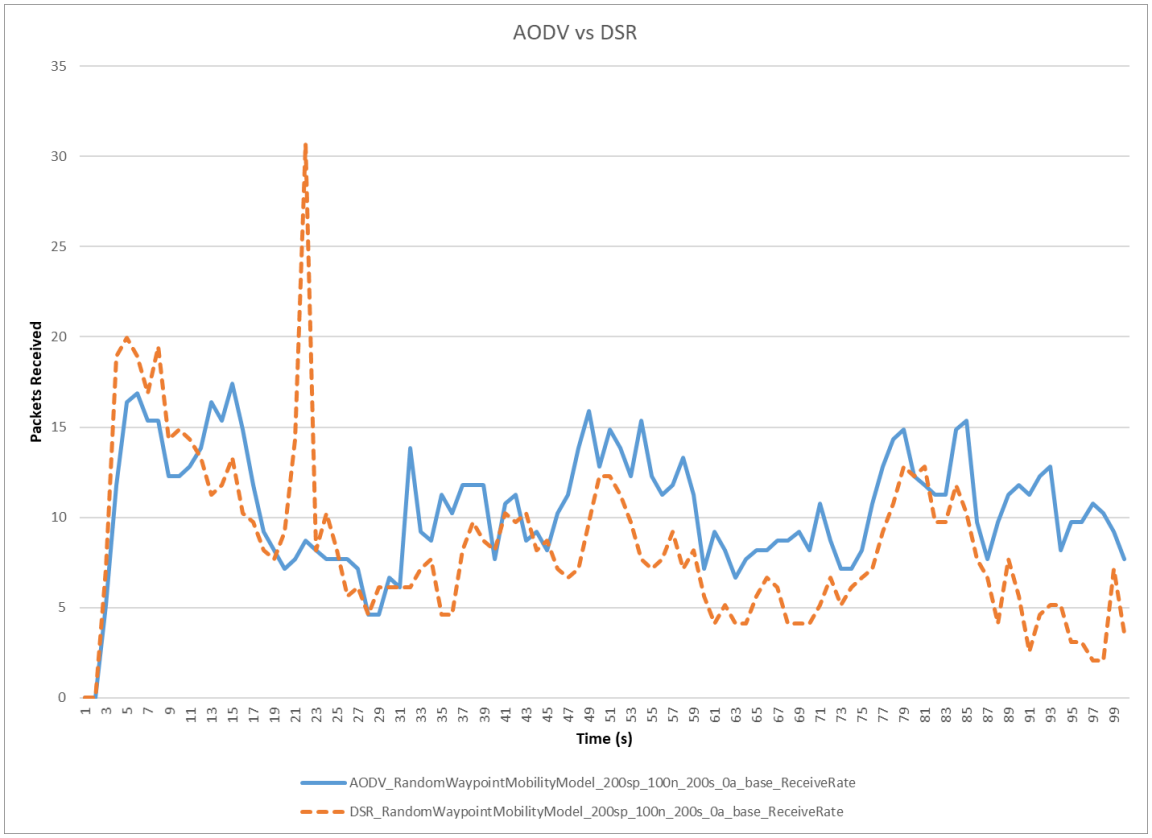

Figure 5.13: Random Waypoint; 200 m/s; 100 nodes; 0 bh

During the baseline of this simulation, AODV outperformed DSR with 10.06% more throughput in the network (see Figure 5.13). AODV is performing better when the nodes start moving with higher speeds, because of the agility of the protocol to adapt to constantly changing

networks easily. DSR, on the other hand, starts to perform worse as the network caches need to be refreshed as routes become invalid in a shorter period.

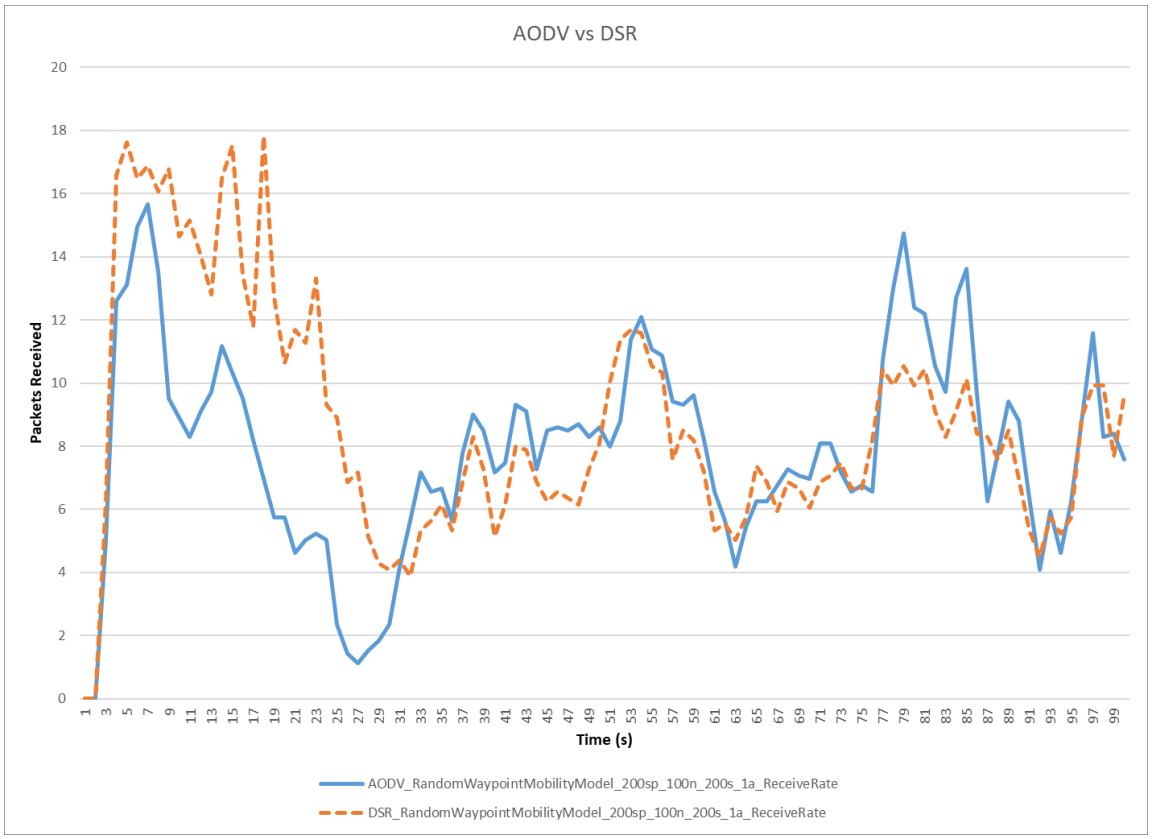

Figure 5.14: Random Waypoint; 200 m/s; 100 nodes; 1 bh

While under attack, AODV performance dropped by 12.65% indicating an impact to the performance, while DSR showed a 1.66% increase in performance (see Figure 5.14). As the nodes become more sporadic and the population denser, the effect of the attack decreases as the network links break more often. The black hole nodes were

not increased with the population size and with the higher speed the black hole node is not triggered as often. Since all attack scenarios are averaged over five simulation runs with the malicious node in different positions, it is possible for DSR to show an increase in performance when better routes were be chosen with the high-speed levels. Under this configuration, DSR indicates the least amount of impact while under attack.

5.2.4 High speed and normal density

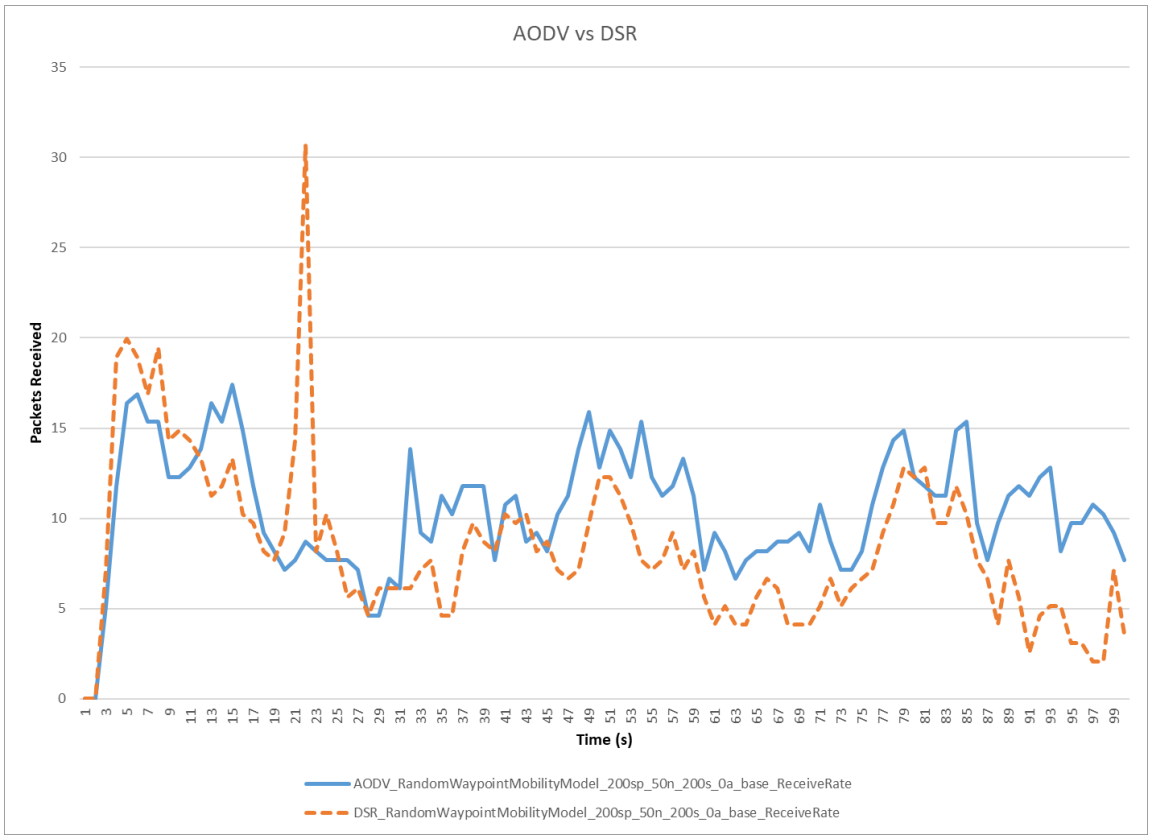

Figure 5.15: Random Waypoint; 200 m/s; 50 nodes; 0 bh

During the baseline of this simulation, AODV outperformed DSR with 10.06% more throughput in the network (see Figure 5.15). Once again the change in node density did not affect the baseline performance.

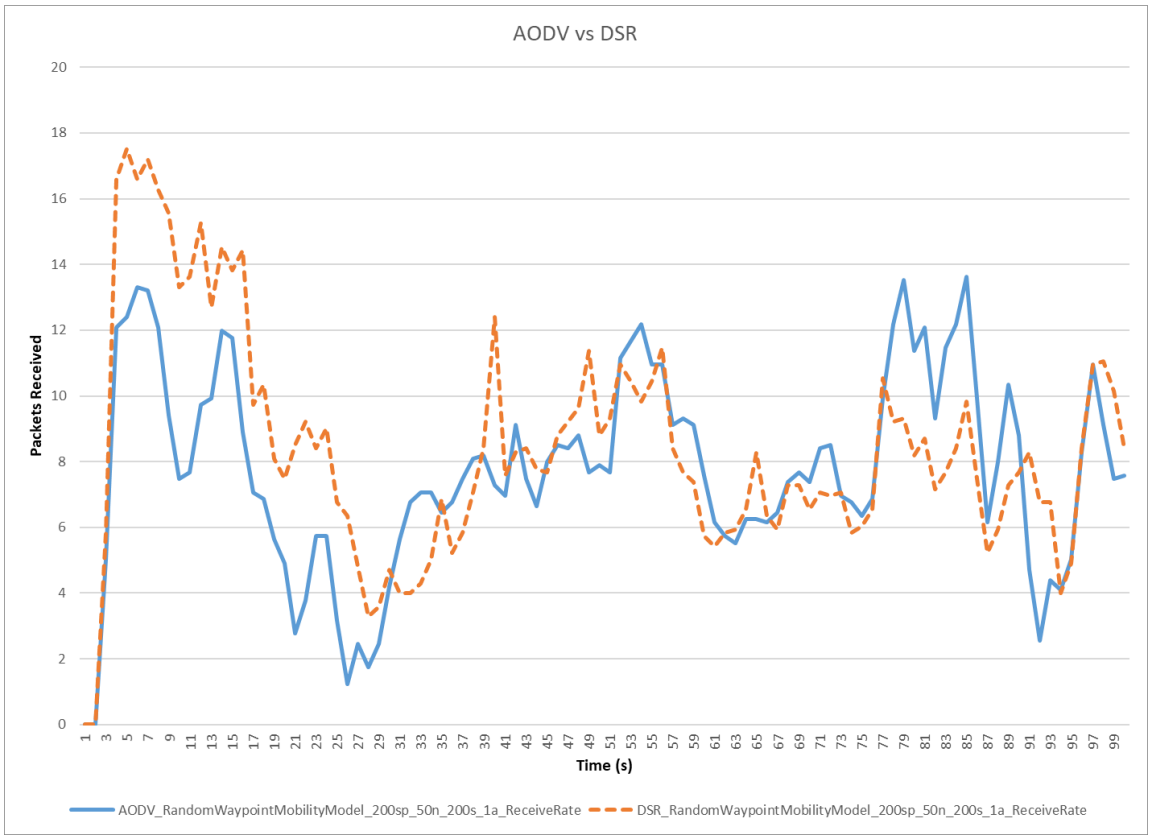

Figure 5.16: Random Waypoint; 200 m/s; 50 nodes; 1 bh

While under attack, AODV performance dropped by 13.33% indicating an impact to the performance, while DSR showed a 0.10% increase in performance (see Figure 5.16). AODV performed worse with more nodes as the probability of encountering a black hole node increased. DSR also performed weaker compared to a more dense population, indicating the black hole node is triggered more often. Under this configuration, DSR had the least amount of impact while under attack.

5.3 Random Walk 2D Mobility Model

Table 5.3: Random Walk Summary table

Protocol	Speed	Density	Receive Rate[Avg. Kbs]	Through Put[%]	BH
AODV	20	50	15.74	76.85	0
DSR	20	50	19.91	97.21	0
AODV	20	50	10.40	50.78	1
DSR	20	50	19.12	93.35	1
AODV	20	100	15.74	76.85	0
DSR	20	100	19.91	97.21	0
AODV	20	100	7.70	37.59	1
DSR	20	100	19.49	95.16	1
AODV	200	100	18.40	89.84	0
DSR	200	100	19.78	96.58	0
AODV	200	100	11.28	55.07	1
DSR	200	100	19.29	94.18	1
AODV	200	50	18.40	89.84	0
DSR	200	50	19.78	96.58	0
AODV	200	50	10.90	53.22	1
DSR	200	50	19.41	94.77	1

The simulation for this mobility model indicated a precise impact of the attack as well as clear impact during network configuration changes. According to Table 5.3, four simulations with a different configuration that was completed can be observed. The movement of these nodes are based on the Brownian model and nodes tend to move sporadically but not outside of the range of nodes. This causes a very high success rate for DSR as the nodes do not move sporadically outside of other

nodes ranges.

5.3.1 Normal speed and normal density

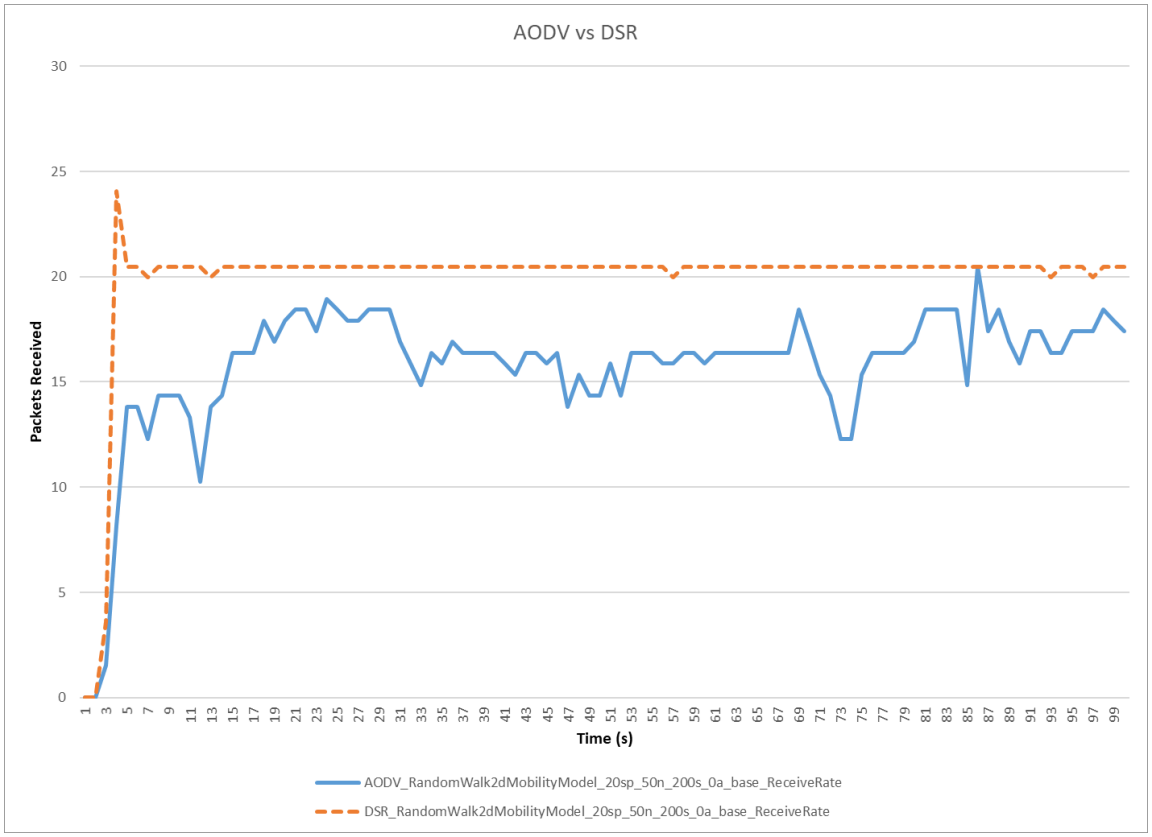

Figure 5.17: Random Walk; 20 m/s; 50 nodes; 0 bh

During the baseline of this simulation, DSR outperformed AODV significantly with 20.36% more throughput in the network. (see Figure 5.17)

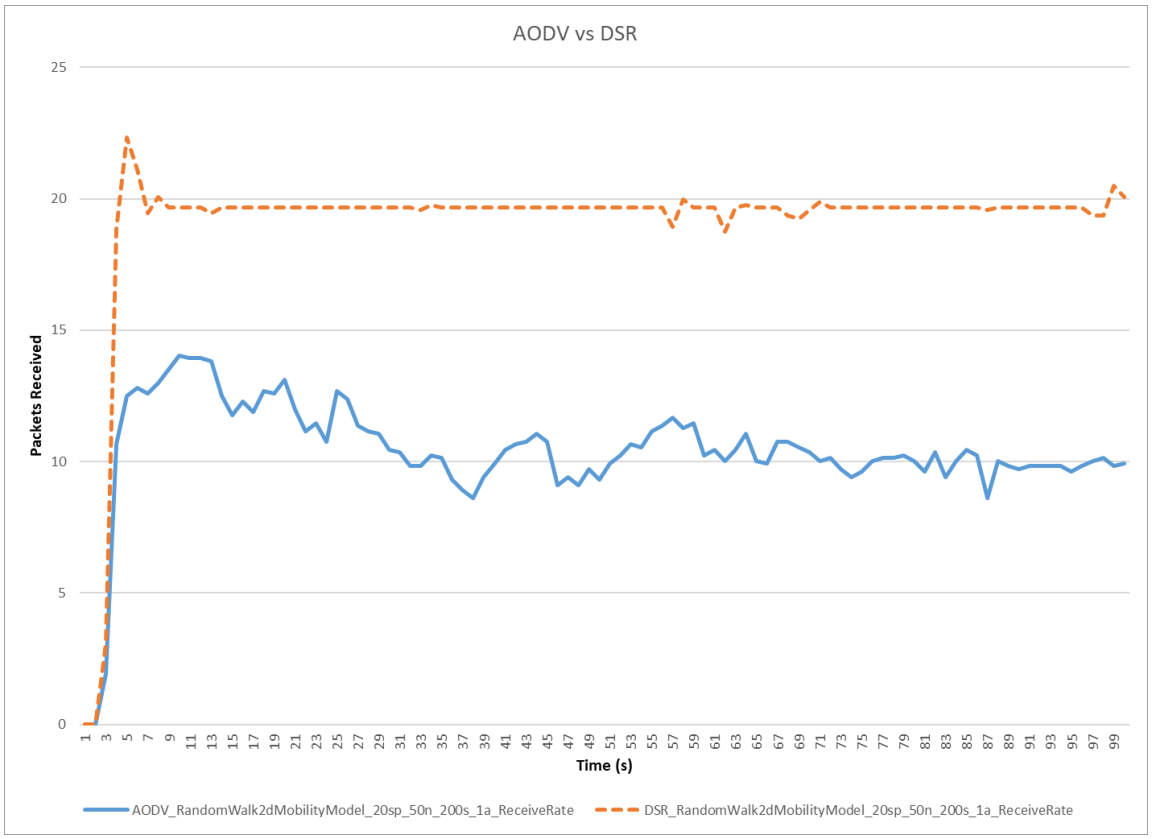

Figure 5.18: Random Walk; 20 m/s; 50 nodes; 1 bh

While under attack, AODV performance dropped by 26.07% indicating an impact to the performance, while DSR showed a 3.86% decrease in performance (see Figure 5.18). Under this configuration, DSR had the least amount of impact while under attack.

5.3.2 Normal speed and high density

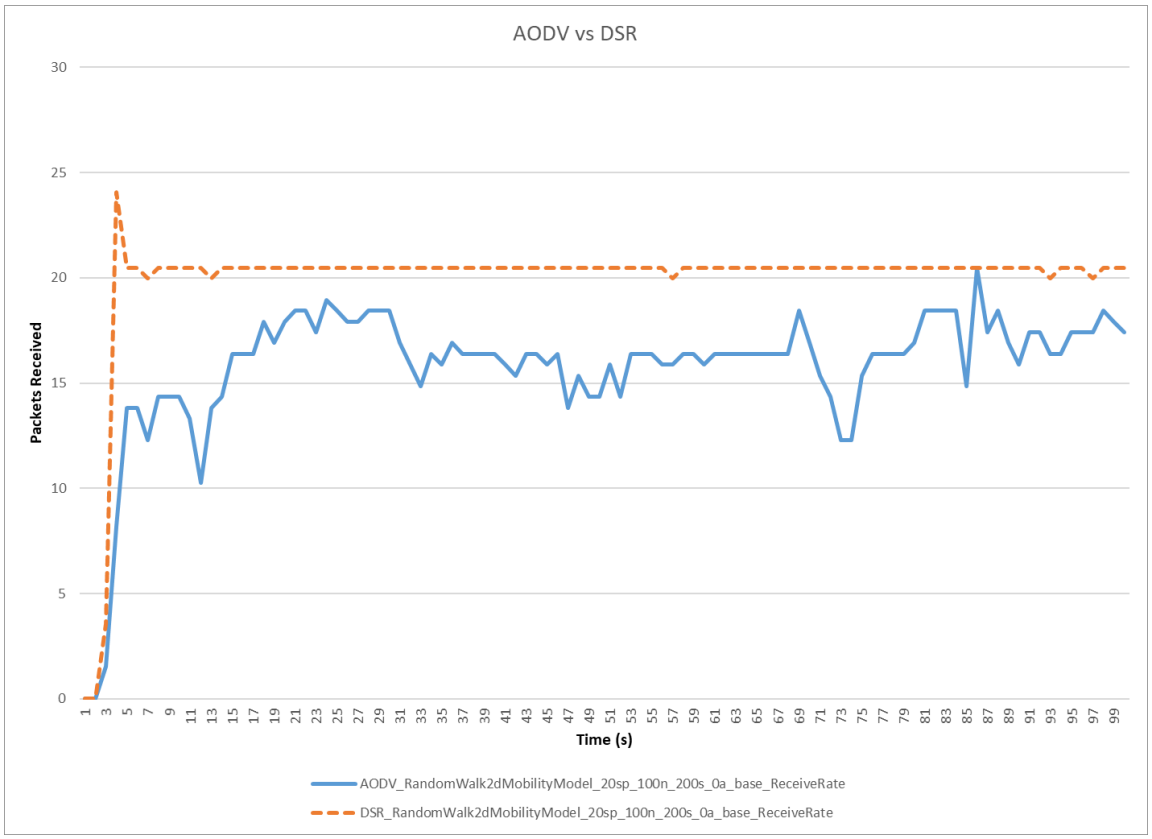

Figure 5.19: Random Walk; 20 m/s; 100 nodes; 0 bh

During the baseline of this simulation, DSR outperformed AODV significantly with 20.36% more throughput in the network (see in Figure 5.19). Increasing the node density did not affect the performance of the protocols. This is because the simulation source and sink nodes created the same routes in both simulations.

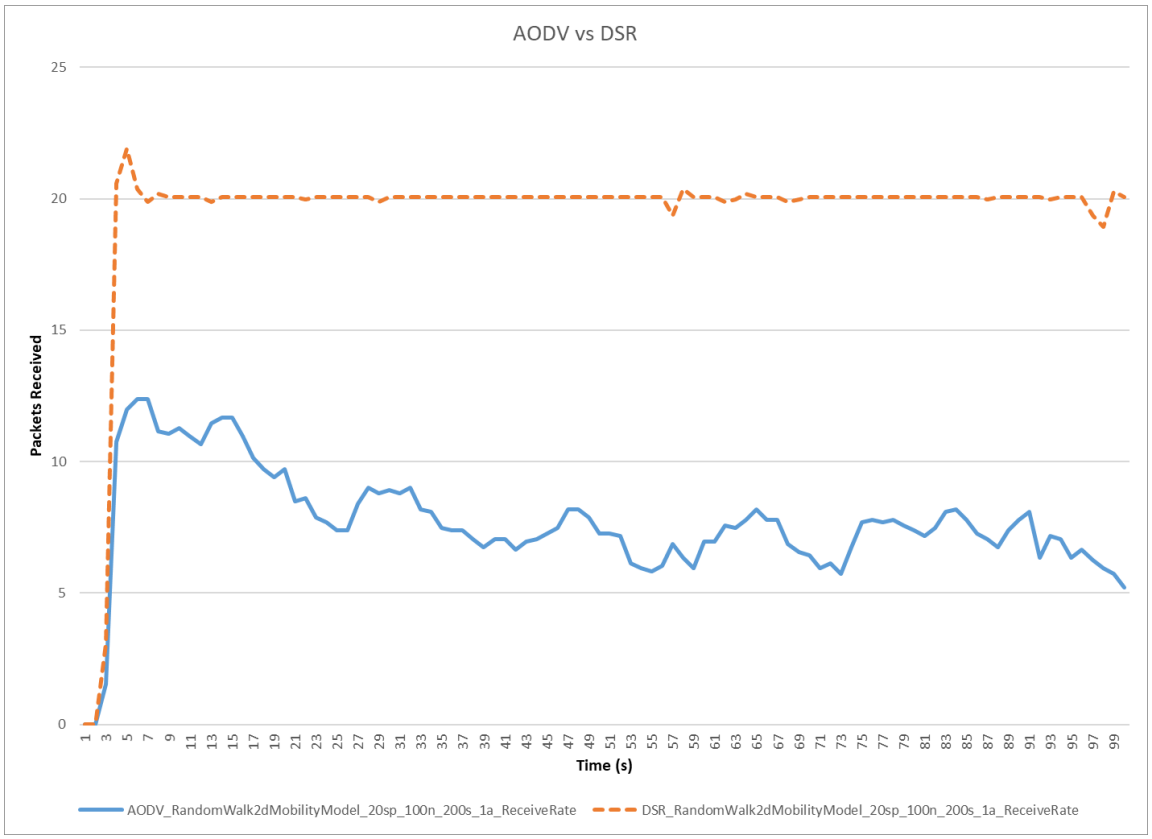

Figure 5.20: Random Walk; 20 m/s; 100 nodes; 1 bh

While under attack, AODV performance dropped by 39.26% indicating a severe impact to the performance, while DSR showed a 2.05% decrease in performance (see Figure 5.20). This is a significant impact to AODV, and this is caused by the malicious nodes being generated in between the source and sink nodes and not moving sporadically. Under this configuration, DSR had the least amount of impact while under attack.

5.3.3 High speed and high density

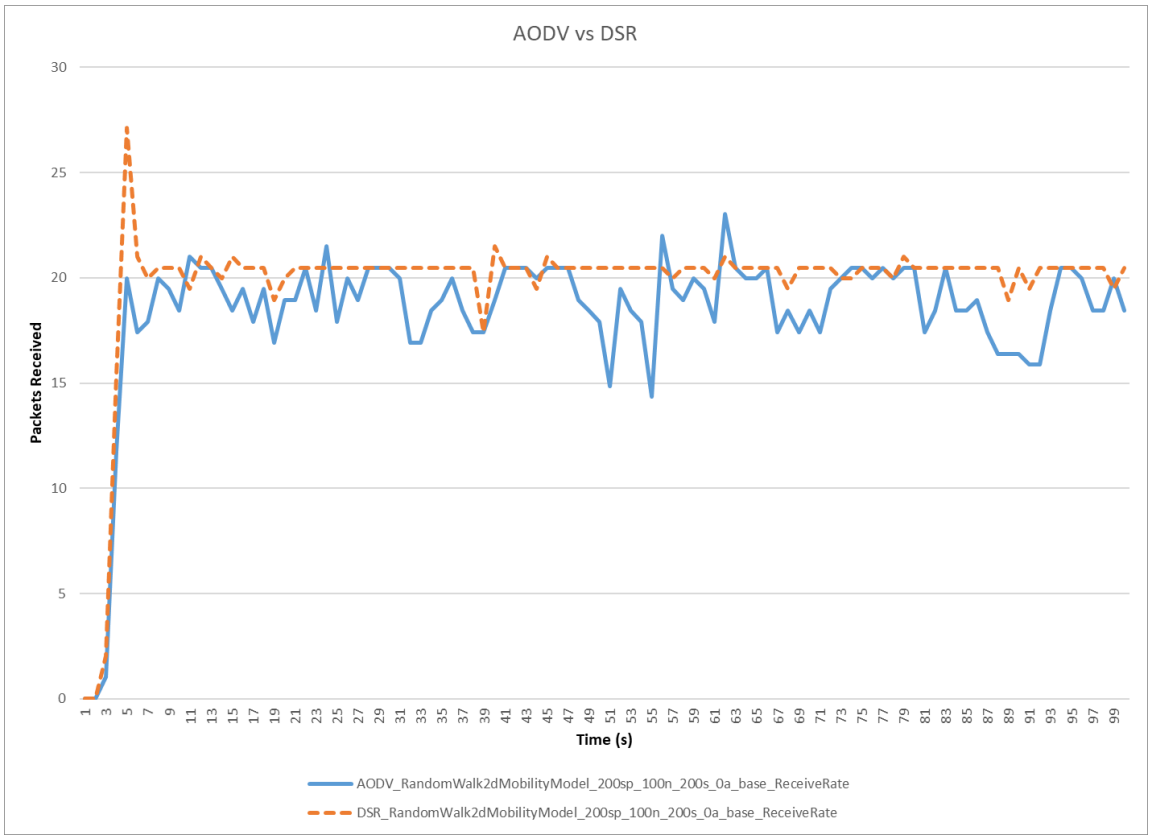

Figure 5.21: Random Walk; 200 m/s; 100 nodes; 0bh

During the baseline of this simulation, DSR outperformed AODV significantly with 6.74% more throughput in the network (see Figure 5.21). AODV performance shows an increase in node speed is increased.

Figure 5.22: Random Walk; 200 m/s; 100 nodes; 1 bh

While under attack, AODV performance dropped by 34.77% indicating an impact to the performance, while DSR showed a 2.4% decrease in performance (see Figure 5.22). Under this configuration, DSR had the least amount of impact while under attack.

5.3.4 High speed and normal density

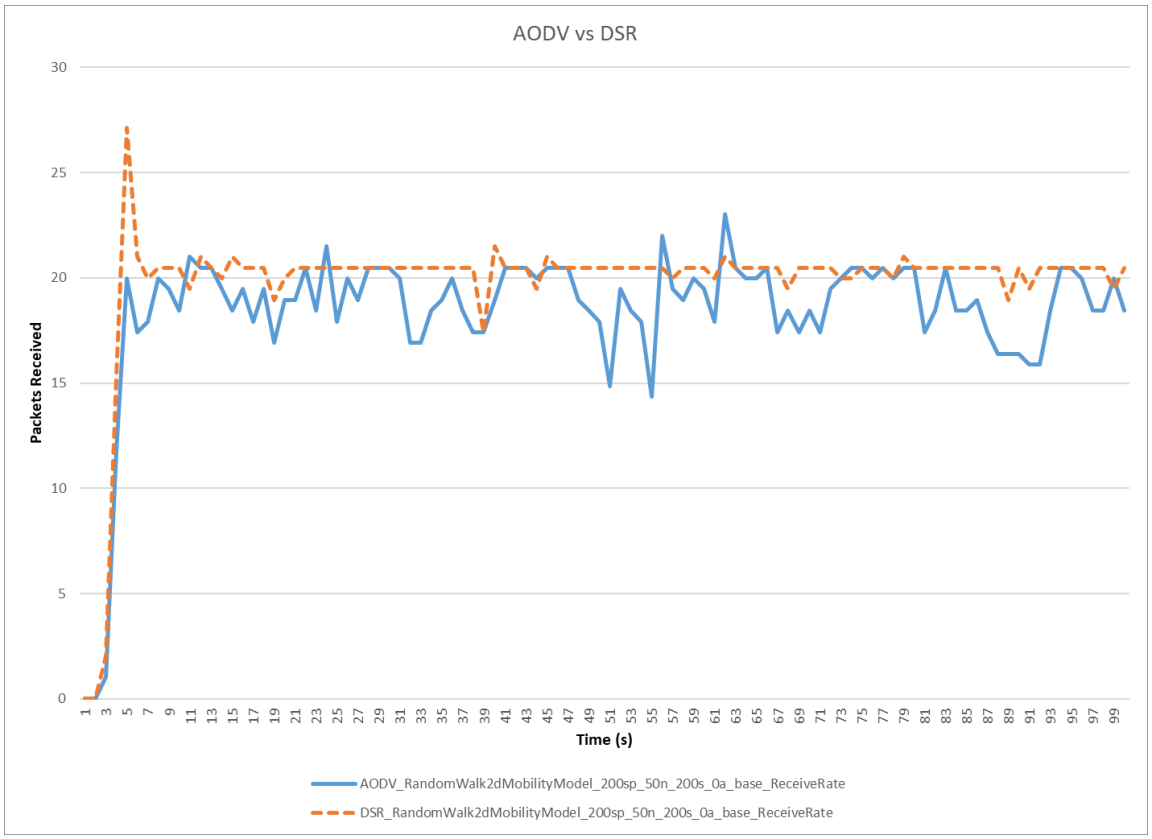

Figure 5.23: Random Walk; 200 m/s; 50 nodes; 0 bh

During the baseline of this simulation, DSR outperformed AODV significantly with 6.74% more throughput in the network (see Figure 5.23). The results again show no change when node density is decreased.

Figure 5.24: Random Walk; 200 m/s; 50 nodes; 1 bh

While under attack, AODV performance dropped by 36.62% indicating an impact to the performance, while DSR showed a 1.81% decrease in performance (see Figure 5.24). Under this configuration, DSR had the least amount of impact while under attack.

5.4 Summary

This chapter provided data necessary for the evaluation and discussion of the comparison between the performance of AODV and DSR while

under attack by black-hole nodes. From the results we can see AODV performed better than DSR for certain mobility models and in networks where the nodes are sparse and have high movement distances. This is because AODV performs better in rapidly changing networks since it does not cache roots like DSR does.

6 Evaluation and Discussion of Results

During simulations for DSR, it was noted that even though a black-hole node was in the path of a destination node, the source node did not necessarily choose the black hole node that causes disruption by dropping packets that it receives.

Results generated from this research study have shown that DSR is not affected as much by black hole attacks as AODV. The effectiveness of the attack was measured by performing a comparative analysis of the throughput of the protocol and the maximum throughput. The difference between the percentage (throughput/maximum throughput) values for a normal population and for a population with a black hole node allowed the impact of the attack to be measured with the view to compare the performance of AODV in relation to that of DSR.

Another comparison was completed, AODV and DSR are compared during all scenarios with no attacks. Moreover, the results revealed that the Random Direction 2D mobility Model is the fairest model with DSR outperforming AODV when the nodes are not sporadic while AODV outperforms DSR when the node speed increases. While the Random Waypoint mobility Model favours AODV during all configurations, the Random Walk 2D mobility Model favours DSR during

all configurations. A data set that benefits both protocols in different scenarios was used.

The standard deviation value of the throughput difference is included in the results below and show the deviation in the values (TP Diff columns) during all configurations, a small standard deviation indicates that the data is close to the mean value while a larger standard deviation indicates the data is spread out further from the mean value. As shown in Table 6.1, the decrease in performance for AODV for all scenarios has a mean value of 25.33% and a throughput difference standard deviation of 9.80. Moreover, the decrease in performance for DSR for all scenarios has a mean value of 3.48% and a throughput difference standard deviation of 3.51. This data indicates that DSR performs significantly better than AODV while under attack by a black hole node and that the DSR data is closer to the mean values than that of AODV.

Table 6.1: Simulation Summary table

Model	Speed	Density	AODV vs DSR	AODV TP Diff	DSR TP Diff
Direction	20	50	-6.79	-29.23	-8.65
Direction	20	100	-6.79	-34.43	-11.97
Direction	200	100	+3.42	-11.87	-3.32
Direction	200	50	+3.42	-12.94	-1.61
Waypoint	20	50	+8.74	-25.15	-4.15
Waypoint	20	100	+8.74	-27.69	-3.81
Waypoint	200	100	+10.06	-12.65	+1.66
Waypoint	200	50	+10.06	-13.33	+0.10
Walk	20	50	-20.36	-26.07	-3.86
Walk	20	100	-20.36	-39.26	-2.05
Walk	200	100	-6.74	-34.77	-2.4
Walk	200	50	-6.74	-36.62	-1.81

The TP in Table 6.1, refers to Through Put, and the term "diff" indicates the difference between the baseline and attack values. In the AODV vs DSR column, a positive value indicates additional throughput AODV has over DSR and a negative value indicates the additional throughput DSR has over AODV in the baseline experiments. I.e., positive values indicate AODV is performing better and negative values indicate DSR is performing better. The TP Diff columns indicate the throughput differences while under attack.

During the experiment, multiple configurations were used. These configurations are discussed in more detail in the following sections.

6.1 Random Direction 2D Mobility Model

6.1.1 Normal speed and normal density

Under normal speed and density, DSR outperformed AODV marginally during the baseline test, and AODV was severely impacted when a single black hole node was introduced. These conditions are meant to indicate a neutral comparison scenario. DSR performs well in this scenario because of the memory of routes and the fact that if the black hole was encountered it does not necessarily mean that DSR would choose the route with the black hole in it. Since the nodes are not moving sporadically, those routes will remain relevant for an extended period of time as opposed to when sporadic nodes are used. DSR operated above 66% throughput in the baseline as well as under attack; AODV dropped to below 40%, indicating the protocol has a weak throughput during attack in this configuration.

6.1.2 Normal speed and high density

When the density of the population was increased, both AODV and DSR had a decrease in performance, and this was likely due to the network becoming more congested with traffic from hello packets with regards to the AODV and route maintenance with regards to DSR.

DSR operated above 63% throughput in the baseline as well as under attack; AODV dropped to below 40% indicating the protocol has a weak throughput during attack in this configuration.

6.1.3 High speed and high density

When the nodes became sporadic, we could see a shift in the results, which indicate that AODV is performing better than DSR in the baseline test. In this scenario, AODV performs better since no cache or memory of routes is kept, and the behaviour is beneficial in networks where nodes are sporadic. When under attack, AODV was again severely affected and performed worse than DSR. While DSR performed poorly under sporadic movement, it still performed better than AODV. From the results, it can concluded that the efficiency in this scenario for both protocols is below 50%, which indicates a weak throughput during attack in this configuration.

6.1.4 Normal speed and normal density

When the population was decreased, AODV performed slightly worse than with a denser population, while DSR performed slightly better while under attack. The improvement in performance for DSR is likely due to the contribution to the reduction in overhead for maintaining

routes. On a different note, density did not make a difference for the ordinary operation but impacted the receive rate more than the lower density. This behaviour was not expected; it was thought that higher density might have a lower chance of triggering the black hole node. However, the attack results are showing differences for the configuration that supports the protocol evaluations. This is likely because of the overhead introduced by the additional nodes, and this overhead will affect both protocols. Both AODV and DSR operated below 50% throughput, indicating a weak throughput during attack in this configuration.

6.2 Random Waypoint Mobility Model

6.2.1 Normal speed and normal density

Under normal speed and density, AODV outperformed DSR. This is because the Random Waypoint mobility model is more sporadic with nodes moving to random waypoints and rebounding to a new random way-point and thus making the movement much more unpredictable. The Random Waypoint mobility model is popular amongst researchers and is a model that favours AODV the most from our baseline and attack perspective when compared with the performance of

AODV in the other models. When under attack, AODV was heavily impacted as with the previous mobility model; the throughput however remained above 40% with this mobility model. DSR operated above 61% throughput in the baseline as well as under attack, where AODV operated above 48%.

6.2.2 Normal speed and high density

Where the population increased the performance of AODV, the performance of the DSR dropped marginally. The decrease in performance can be attributed to the network overhead introduced. The DSR operated above 61% throughput in the baseline as well as under attack, whereas AODV operated above 46%.

6.2.3 High speed and high density

When the node speed was increased AODV performed better than the DSR. During this configuration, AODV had the best performance over DSR when not under attack for all the mobility models and configurations. This is due to the extreme movement of the nodes, which benefits AODV. The performance of both AODV and DSR is considerably lower when used with the Random Waypoint mobility model and nodes moving at an increased speed. These network conditions are

considered to be challenging. When under attack, a decrease in the performance of the AODV protocol follows a trend that is similar to the previous mobility model; on the other hand the DSR had a slight increase in performance. The lowest throughput DSR has shown was 41.06% and the performance of the protocol has minor changes under the most challenging conditions provided. The reason for the increase, we believe, is because DSR will not perform worse or better from this point on and the random variables are providing some conditions where DSR has a slightly better network performance during the black hole attack averaged over multiple runs. DSR operated above 41% throughput in the baseline as well as under attack, wheres AODV operated above 38% throughput thus indicating the protocol performance for both protocols under this configuration is relatively weak.

6.2.4 High speed and normal density

When the population decreased, once again AODV performed worse than DSR when under attack and a marginally lower performance was recorded when compared to a larger population. For reasons mentioned above, DSR once again showed a minor increase in performance. The population decrease had a negative effect on the AODV protocol when the nodes were sporadic. This behaviour is attributed to the harsh

speed of the nodes in a smaller network, which has an impact on network creation and maintenance, since the network zone that did not decrease the nodes were sparse and sporadic. The decrease was not observed with the Random direction mobility model. DSR operated above 41% throughput in the baseline as well as under attack, whereby AODV operated above 37% thus indicating the protocol performance for both protocols were relatively weak.

6.3 Random Walk 2D Mobility Model

6.3.1 Normal speed and normal density

During this configuration, DSR had the better performance over AODV when not under attack. This configuration had the best performance for DSR for all the mobility models and configurations. This is due to the extreme predictability of the nodes that favours the caches created by DSR. This mobility model also has the best performance for DSR from all of the mobility models used in this research. DSR operated above 93% throughput in the baseline as well as when under attack; on the other hand, AODV operated above 50% throughput thus indicating that the protocol performance for both protocols under this configuration is acceptable. This is especially true for DSR, which has

shown performance that is above 90% even when under attack; this suggests that applications for DSR with configuration and mobility used in this experiment are highly favourable towards DSR.

6.3.2 Normal speed and high density

When the population increased, DSR experienced a minor decrease in performance; however, AODV was found to experience the biggest impact from the attack in all configurations and mobility models used in this research. AODV does not cache routes it may continuously fail because of the same black hole in its path even though the black hole positions were randomised and averaged out. Whereas DSR operated above 95% throughput in the baseline as well as when under attack, AODV operated above 37% throughput thus indicating that AODV has a significantly worse performance compared to DSR with this configuration and mobility model. This is due to the caching DSR does and the fact that the nodes stay near their past locations when they move. For this configuration, DSR has a strong throughput while AODV has a very weak throughput.

6.3.3 High speed and high density

When the speed was increased, AODV was found to possess the highest throughput for all configurations and mobility models with this configuration at 89% throughput. This was however still lower than the DSRs throughput of 96%. When the attack was introduced, AODVs throughput was significantly affected due to the nodes movement being in close proximity with its previous location thus not acting truly sporadic like the other mobility models. While DSR had the same performance impact approximately, as with previous speeds, this behaviour is because the nodes do not move completely outside of their range the network does not often change which is very beneficial to the DSR caching mechanism. DSR operated above 94% throughput in the baseline as well as when under attack, and AODV operated above 55% throughput indicating that the protocol performance for both protocols is relatively acceptable.

6.3.4 High speed and normal density

As the density becomes more sparse, the AODV once again performed worse than for the more dense population. The attack had little impact on DSR during this configuration. As mentioned previously, the mobility model moves nodes in close proximity to its previous position,

which makes the network almost static when the network range is significant. The DSR operated above 94% throughput in the baseline as well as under attack; on the other hand, the AODV operated above 53% indicating that the protocol performance for both protocols could be acceptable for real world networks with networks performing like this configuration.

7 Conclusion

From the results, it was concluded that the DSR outperforms AODV while under black hole attack. Keeping this in mind, why was the attack so effective in AODV relative to its base performance? This was because of how AODV differs from DSR with regards to Route Request messages. DSR can keep several routes and decide on those routes, while AODV gives more responsibility to the network for choosing the best route; that is, changing the hop count to a low value can fool the source node to choose the route.

In the DSR, the node would have to return a route to the source through the black hole node, and this does not guarantee that the route was the best to the destination. The position of the black hole in the network also has an impact on performance; for the experiment, the position was moved randomly in the MANET. The effect of the attack was the average over multiple runs to remove black hole position bias from the comparison. As far as all the data is concerned, DSR performed best using the Random Walk mobility model. Highest throughput for both AODV and DSR were recorded. AODV performed better than DSR when using the Random Waypoint mobility model and sporadic nodes in the Random Direction mobility model. The

data represents AODV and DSR in neutral and challenging network scenarios. The baseline data has scenarios where AODV performs better than DSR and DSR performing better than AODV, thus creating a fair comparison. Therefore, it was concluded that the black hole attack in all conditions had a severe effect on AODV while DSR indicated a strong resilience to the attack.

From our results, we have answered our research questions and found an interesting observation from existing studies. There is a mobility model bias from researchers and it is possible for research data to indicate that AODV or DSR perform better while under attack from black hole nodes. This is because different mobility models impact the protocols differently and can, therefore, change the results.

8 Future Work

To continue with this study a further investigation of solutions for black hole attacks, and variants thereof can be done. The study could produce a comparison study of the performance of enhanced, which include solutions as well as protocol enhancements, AODV and DSR protocols to determine their latest resilience against attacks.

References

[1] H. Ehsan and F. A. Khan. Malicious AODV: Implementation and analysis of routing attacks in MANETs. In *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012*, pages 1181–1187. IEEE, 6 2012.

[2] Klaas-Jan Stol and Brian Fitzgerald. The abc of software engineering research. *ACM Trans. Softw. Eng. Methodol.*, 27(3):11:1–11:51, September 2018.

[3] H. Yih-Chun and A. Perrig. A survey of secure wireless ad hoc routing. *IEEE Security & Privacy Magazine*, 2(3):28–39, 2004.

[4] D. Mishra, Y. K. Jain, and S. Agrawal. Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET). *2009 International Conference on Advances in Computing Control and Telecommunication Technologies*, (i):621–623, 2009.

[5] S. Dokurer, Y. M. Erten, and C. E. Acar. Performance analy-

sis of ad-hoc networks under black hole attacks. In *Conference Proceedings - IEEE SOUTHEASTCON*, pages 148–153, 2007.

[6] M. Amir, D. M. Nagar, and V. Baghela. Secure DSR Routing Protocol Based on Homomorphic Digital Signature. *Proceedings of the International Conference on Advances in Information Communication Technology & Computing - AICTC '16*, pages 1–5, 2016.

[7] M. Salehi, H. Samavati, S. Technical, and M. Dehghan. Evaluation ofDSR Protocol under a New Black hole Attack. pages 640–644, 2012.

[8] M. Salehi and H. Samavati. DSR vs OLSR: Simulation based comparison of ad hoc reactive and proactive algorithms under the effect of new routing attacks. *Proceedings - 6th International Conference on Next Generation Mobile Applications, Services, and Technologies, NGMAST 2012*, pages 100–105, 2012.

[9] R. Upadhyay, S. Khan, H. Tripathi, and U. R. Bhatt. Detection and prevention of DDOS attack in WSN for AODV and DSR using battery drain. *2015 International Conference on Computing and Network Communications, CoCoNet 2015*, pages 446–451, 2016.

[10] R. Agrawal, R. Tripathi, and S. Tiwari. Performance evaluation

and comparison of AODV and DSR under adversarial environment. *Proceedings - 2011 International Conference on Computational Intelligence and Communication Systems, CICN 2011*, pages 596–600, 2011.

[11] J. Dong, R. Curtmola, and C. Nita-Rotaru. Practical defenses against pollution attacks in wireless network coding. *ACM Transactions on Information and System Security*, 14(1):1–31, 2011.

[12] O. Sbai and M. Elboukhari. A simulation analyse of MANET's RREQ Flooding and HELLO Flooding attacks with ns-3. pages 1–5, 2019.

[13] Mohammed Saeed A., J. Liu, and A. R. Sangi. AODV routing protocol under several routing attacks in MANETs. In *International Conference on Communication Technology Proceedings, ICCT*, pages 614–618, 2011.

[14] A. Bandyopadhyay, S. Vuppala, and P. Choudhury. A simulation analysis of flooding attack in MANET using NS-3. In *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011*, pages 1–5, 2011.

[15] N. Purohit, R. Sinha, and K. Maurya. Simulation study of black hole and jellyfish attack on MANET using NS3. In *2011 Nirma University International Conference on Engineering: Current Trends in Technology, NUiCONE 2011 - Conference Proceedings*, pages 1–5, 2011.

[16] A. Nadeem and M. Howarth. A generalized intrusion detection & prevention mechanism for securing MANETs. In *2009 International Conference on Ultra Modern Telecommunications and Workshops*, pages 1–6, 2009.

[17] N. U. R. A. Abdullah. Performance Measurement in. pages 406–410, 2009.

[18] K. S. Sujatha, V. Dharmar, and R. S. Bhuvaneswaran. Design of genetic algorithm based IDS for MANET. In *Recent Trends In Information Technology (ICRTIT), 2012 International Conference on*, pages 28–33, 2012.

[19] M. Patel, S. Sharma, and D. Sharan. Detection and Prevention of Flooding Attack Using SVM. In *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*, pages 533–537, 2013.

[20] M. Patel and S. Sharma. Detection of malicious attack in MANET a behavioral approach. *Proceedings of the 2013 3rd IEEE International Advance Computing Conference, IACC 2013*, pages 388–393, 2013.

[21] W. Li, A. Joshi, and T. Finin. SAT: an SVM-based automated trust management system for Mobile Ad-hoc Networks. In *2011 - MILCOM 2011 Military Communications Conference*, pages 1102–1107. IEEE, 11 2011.

[22] N. Gandhewar and R. Patel. Detection and prevention of sinkhole attack on AODV protocol in mobile adhoc network. In *Proceedings - 4th International Conference on Computational Intelligence and Communication Networks, CICN 2012*, pages 714–718, 2012.

[23] P. M. John, S. Arulnandhisivam, and V. Periyasamy. A secure intrusion-detection system using an acknowledgment-based approach for the detection of routing misbehavior in MANETS. *International Review on Computers and Software*, 9(8):1373–1383, 2014.

[24] B. David, R. Dowsley, and M. Larangeira. MARS: Monetized Adhoc Routing System (A Position Paper). *Proceedings of the 1st*

Workshop on Cryptocurrencies and Blockchains for Distributed Systems, pages 82–86, 2018.

[25] L. Zhou and Z. J. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, 1999.

[26] A. A. Pirzada and C. McDonald. Secure routing with the AODV protocol. In *2005 Asia-Pacific Conference on Communications*, volume 2005, pages 57–61, 2005.

[27] S. J. Soni and S. D. Nayak. Enhancing security features & performance of AODV protocol under attack for MANET. In *2013 International Conference on Intelligent Systems and Signal Processing, ISSP 2013*, pages 325–328, 2013.

[28] N. R. Yerneni and A. K. Sarje. Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc. *2012 3rd International Conference on Computing, Communication and Networking Technologies, ICCCNT 2012*, (July), 2012.

[29] V. Mohite and L. Ragha. Cooperative security agents for MANET. *Proceedings of the 2012 World Congress on Information and Communication Technologies, WICT 2012*, 1:549–554, 2012.

[30] P. G. Argyroudis and D. O'Mahony. Secure routing for mobile

ad hoc networks. *IEEE Communications Surveys and Tutorials*, 7(3):2–21, 2005.

[31] M. Medadian, A. Mebadi, and E. Shahri. Combat with black hole attack in AODV routing protocol. In *Proceedings - MICC 2009: 2009 IEEE 9th Malaysia International Conference on Communications with a Special Workshop on Digital TV Contents*, pages 530–535, 2009.

[32] F. Thachil and K. C. Shet. A trust based approach for AODV protocol to mitigate black hole attack in MANET. In *Proceedings: Turing 100 - International Conference on Computing Sciences, ICCS 2012*, pages 281–285, 2012.

[33] A. Hinds, S. Sotiriadis, N. Bessis, and N. Antonopoulos. Performance evaluation of security algorithms for the AODV MANET routing protocol. In *Proceedings - 3rd International Conference on Emerging Intelligent Data and Web Technologies, EIDWT 2012*, pages 311–315, 2012.

[34] Y.-C. Hu, A. Perrig, and D.B. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of*

the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), volume 3, pages 1976–1986, 2003.

[35] H. Deng, W. Li, and D. P. Agrawal. Routing security in wireless ad hoc networks. *IEEE Communications Magazine*, 40(10):70–75, 2002.

[36] J. Cai, P. Yi, Y. Tian, Y. Zhou, and N. Liu. The simulation and comparison of routing attacks on DSR protocol. *Proceedings - 5th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2009*, (60803117):2–5, 2009.

[37] L. Mejaele and E. O. Ochola. Analysing the impact of black hole attack on DSR-based MANET: The hidden network destructor. *2015 2nd International Conference on Information Security and Cyber Forensics, InfoSec 2015*, pages 140–144, 2016.

[38] O. Erdene-Ochir, M. Minier, F. Valois, and A. Kountouris. Resiliency of wireless sensor networks: Definitions and analyses. *ICT 2010: 2010 17th International Conference on Telecommunications*, pages 828–835, 2010.

[39] P. Rathiga and S. Sathappan. Hybrid detection of Black hole and

gray hole attacks in MANET. *2016 International Conference on Computation System and Information Technology for Sustainable Solutions, CSITSS 2016*, pages 135–140, 2016.

[40] J. Cai, P. Yi, J. Chen, Z. Wang, and N. Liu. An adaptive approach to detecting black and gray hole attacks in ad hoc network. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, (2009):775–780, 2010.

[41] A. Bhardwaj. Secure routing in DSR to mitigate black hole attack. *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies, ICCICCT 2014*, pages 985–989, 2014.

[42] S. R. Deshmukh and P. N. Chatur. Secure routing to avoid black hole affected routes in MANET. *2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016*, 2016.

[43] N. Vaishnav and H. Upadhyay. Secure Content Dissemination in Small Topological Environment by Enhancing Security of DSR. *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '16*, pages 1–4, 2016.

[44] J. Zhou, J. Chen, and H. Hu. for MANETs. (60673086):1569–1572, 2007.

[45] W. Gong, Z. You, D. Chen, X. Zhao, and K. Y. Gu, M.and Lam. Trust based malicious nodes detection in MANET. *2009 International Conference on E-Business and Information System Security, EBISS 2009*, pages 2–5, 2009.

[46] N. Bhalaji and A. Shanmugam. Association between nodes to combat blackhole attack in DSR based manet. *2009 IFIP International Conference on Wireless and Optical Communications Networks, WOCN 2009*, pages 0–4, 2009.

[47] P. N. Patil and A. T. Bhole. Black hole attack prevention in mobile Ad Hoc networks using route caching. *IFIP International Conference on Wireless and Optical Communications Networks, WOCN*, 2013.

[48] C. Chandra. Advance dynamic source routing (A-DSR) for multi hop ad hoc network and performance evaluation of proactive and reactive protocols. pages 0–5, 2014.

[49] L. Qin and T. Kunz. Pro-active route maintenance in DSR. *SIGMOBILE Mob. Comput. Commun. Rev.*, 6(3):79–89, 2002.

[50] H. Jasani. Evaluations of AODV and DSR for QOS requirements. *Proceedings of the 1st Annual conference on Research in information technology - RIIT '12*, page 1, 2012.

[51] P. R. Jasmine Jeni, A. Vimala Juliet, R. Parthasarathy, and A. Messiah Bose. Performance analysis of DOA and AODV routing protocols with black hole attack in MANET. In *2013 IEEE International Conference on "Smart Structures and Systems", ICSSS 2013*, pages 178–182, 2013.

[52] Y. Cheng, E. Çetinkaya, and J. Sterbenz. Dynamic Source Routing (DSR) Protocol Implementation in ns-3. *Proceedings of the Fifth International Conference on Simulation Tools and Techniques*, pages 367–374, 2012.

[53] L. Prashar and R. K. Kapur. Performance analysis of routing protocols under different types of attacks in MANETs. *2016 5th International Conference on Reliability, Infocom Technologies and Optimization, ICRITO 2016: Trends and Future Directions*, pages 405–408, 2016.

[54] I. Nurcahyani and H. Hartadi. Performance Analysis of Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Rout-

ing (DSR) Under Black Hole Attacks in Mobile Ad Hoc Network (MANET). *ISESD 2018 - International Symposium on Electronics and Smart Devices: Smart Devices for Big Data Analytic and Machine Learning*, pages 1–5, 2019.

[55] Shirley Gregor. The nature of theory in information systems. *MIS Quarterly*, 30(3):611–642, 2006.