Effect of Varying Node Mobility in the Analysis of Black Hole Attack on MANET Reactive Routing Protocols

Lineo Mejaele[*Ψ] and Elisha Oketch Ochola[*]
[*]School of Computing, University of South Africa, Pretoria, South Africa
[Ψ]Mathematics and Computer Science Department, National University of Lesotho, Roma, Lesotho
Email: 48082236@mylife.unisa.ac.za, Ocholeo@unisa.ac.za

***Abstract*— Mobile Ad-hoc Networks (MANETs) features such as open medium, dynamic topology, lack of centralised management and lack of infrastructure expose them to a number of security attacks. Black hole attack is one type of attack that is more common in MANET reactive routing protocols such as Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR). Black hole attack takes advantage of route discovery process in reactive routing protocols. In this type of attack, a malicious node misleads other nodes in the network by pretending to have the shortest and updated route to a target node whose packets it wants to interrupt. It then redirects all packets destined to a target node to itself and discards them instead of forwarding. This paper analyses the performance of AODV and DSR when attacked by black hole, by varying the mobility of the nodes in the network. The analysis is carried out by simulating scenarios of AODV based MANET and DSR based MANET using Network Simulator 2 (NS-2) and introducing the black hole attack in each of the scenarios. The different scenarios are generated by changing the mobility of the nodes. The performance metrics that are used to do the analysis are throughput, packet delivery ratio and end-to-end delay. The simulation results show that the performance of both AODV and DSR degrades in the presence of black hole attack. Throughput and packet delivery ratio decrease when the network is attacked by black hole because the malicious node absorbs or discards some of the packets. End-to-end delay is also reduced in the presence of a black hole attack because a malicious node pretends to have a valid route to destination without checking the routing table, and therefore shortens the route discovery process. The results also show that throughput decreases slightly when mobility of the nodes is increased in the network. The increase in the speed of the nodes decreases both end-to-end delay and packet delivery ratio.**

Keywords-MANET; Reactive Routing Protocols; Black Hole Attack; Mobility

I. INTRODUCTION

The success of any kind of a network is intensely determined by the confidence people have in its security, it is therefore very crucial for both wired and wireless networks to be secured so as to offer protected communication [1]. Mobile Ad-hoc Network (MANET) is a group of mobile devices that can spontaneously interconnect and share resources via wireless communication channels, with no fixed network infrastructure or central management. MANETs can be assembled quickly with little cost because they do not require central monitoring or fixed network infrastructure. Mobile nodes in MANET do not necessarily have to be of the same type. They can be PDAs, laptops, mobile phones, routers and printers, as illustrated by Fig.1. The nodes are equipped with antennas which operate as wireless transmitters and receivers. The antennas may be omnidirectional, highly directional, or a combination. The mobile nodes are resource constraint in terms of bandwidth and battery power [2, 3].

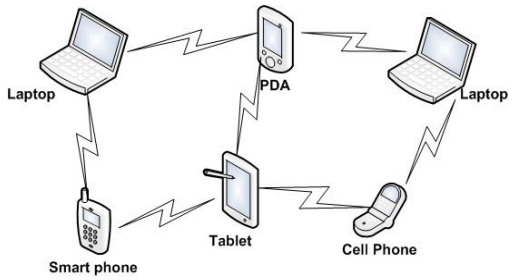

Figure 1. Mobile Ad-hoc Network

MANET is suitable to provide communications in many applications, particularly in cases where it is not possible to setup a network infrastructure. For instance, in a military operation, where there may be geographical barriers between participants, MANET can be setup to facilitate communication. Also because it is easy to set up, it may be of assistance to replace the damaged network infrastructure in disaster recovery operations where temporary network infrastructure is immediately needed [4, 5].

The features of MANETs expose them to many security attacks compared to other traditional networks. The high mobility and dynamic topology of MANETs make routing to be very challenging, that is why early research on MANET mostly concentrated on developing routing mechanisms that are efficient for a dynamic and resource constraint MANET. The security of protocols was given less attention when MANET routing protocols were defined. Black hole attack aims to disrupt the routing process of MANETs [1] .

This paper aims to analyse the performance of MANET reactive routing protocols when attacked by the black hole. The two reactive routing protocols that are compared in the analysis are Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR). The mobility of the nodes in the network is varied during the analysis to determine the impact that mobility has on MANETôs performance and to discover the protocol that is more preferable in a high mobility network. The effect of black hole attack is tested on reactive

routing protocols because black hole attack targets route discovery process and can easily attack reactive protocols since they discover the routes frequently.

The rest of the paper is structured as follows: Section II discusses the vulnerabilities of MANETs that expose them to attacks. Section III describes routing in MANETs and discusses the different categories of routing protocols, focusing more on reactive routing protocols. Section IV explains black hole attack, and describes some of the solutions that have been suggested to lessen the impact of the attack. Section V gives the simulation structure used to perform the analysis, presents the results obtained from the simulations and gives the analysis of the results. Section VI concludes the paper.

II. VULNERABILITIES OF MANETS

It is quite challenging to maintain security in MANETs because they have far more vulnerabilities than wired networks [6]. Any weakness in security system is vulnerability. Some MANETsô vulnerabilities are presented as follows:

A. Lack of Secure Boundaries

The nodes in MANET are at liberty to move inside the network, join and leave the network any time. This makes it challenging to establish a security wall as compared to traditional wired networks that have a clear line of defense. In order to attack wired networks the adversaries must physically enter into the network medium, pass through firewalls and gateways before they have access to practice malicious behaviour to the target nodes in the network. However, in MANET the adversary can communicate with nodes within its transmission range, and become part of the network without any physical access to the network. The absence of secure boundaries causes MANET to be attacked at any time by any malicious node that is within the transmission range of any node in the network [7].

B. Lack of Centralised Management Facility

There is no central equipment such as a server for monitoring the nodes in the network and this increases the vulnerability problems of MANETs. Firstly, it becomes very difficult to detect the attacks in the absence of central control because the traffic in an ad-hoc network is very dynamic [8]. Secondly, lack of centralised management delays the nodesô trust management. It becomes difficult to prior classify the nodes as trustworthy or untrustworthy because the security of the nodes cannot be presumed. Consequently, the nodes cannot be distinguished as trusted or non-trusted. Thirdly, lack of centralised authority can sometimes lead to decentralised decision-making. In MANETs, important algorithms depend on all nodes participating cooperatively, so the attacker can take advantage of this vulnerability and execute attacks that can ensure that the nodes are not cooperative [9].

C. Threads from Compromised Nodes in the Network

Each mobile node operates independently, which means it is free to join or leave the network at any time. It therefore becomes difficult for the nodes to set rules and strategies that can prevent malicious behaviour of other nodes in the mobile network. Also, due to freedom of movement of the nodes, a compromised node can target different nodes in the network. Hence, it becomes quite challenging to identify malicious actions of a compromised node in the network, particularly in a huge network. As a result, internal attacks from nodes that have been compromised are more severe than external attacks because they are not easily identified due to the fact that a compromised node operated normally before it could be compromised [7].

D. Restricted Power Supply

Mobile devices in MANET get energy from batteries or other exhaustible means, so their energy is limited. This energy restriction can cause denial of service by the attacker; since the attacker is aware of the battery restriction, it can endlessly forward packets to the target node or make the target node to be involved in some time consuming activities. This will cause battery power to be exhausted and the target node will not operate anymore. Again, the limited power supply may cause a node in MANET to behave selfishly by not participating cooperatively in the network activities as a way to save its limited battery. This becomes a problem particularly when it is essential for the node to cooperate with other nodes [10].

III. ROUTING IN MANETS

The topology of MANETs keeps changing rapidly due to free movement of nodes joining and leaving the network any time. Routing is important in order to discover the recent topology so that an updated route to a certain node can be established and a message relayed to the correct destination [3, 11]. The traditional routing protocols such as distance vector and link state protocols that have been structured for hard wired networks cannot be directly applied to MANETs. This is because of mobility and dynamic topology, which are the fundamental characteristics of MANETs [12]. In order to overcome routing challenges in MANETs and attain effective routing, a number of routing protocols are defined specifically for MANETs. These protocols can be categorised into proactive, reactive and hybrid protocols based on the way paths are established and maintained by the nodes [13]. The hierarchy of the protocols is shown in Fig. 2. The reactive routing protocols discussed in this paper are shown in red in Fig. 2.

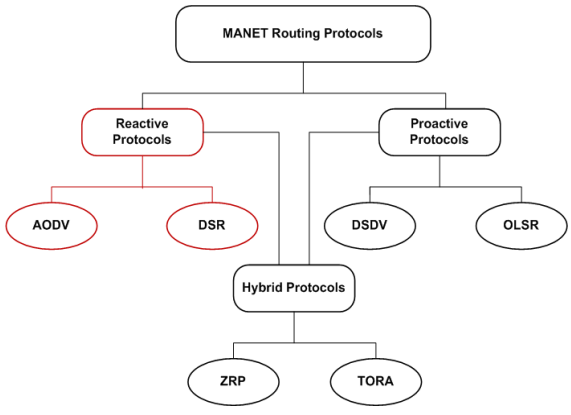

Figure 2. MANET Protocols Hierarchy

A. Proactive Protocols

These are table-driven routing protocols that try to keep a record of fresh and updated network routes. All the nodes in the network have a table to store the routing information [8]. The nodes exchange topology information so that they can all have the same view of the network. The exchanged information helps to reflect any changes in the topology. Whenever a node needs to send messages, it just searches the routing table for the path to the destination. The sending of the message is not delayed by the remote route discovery [11]. Maintaining an up-to-date topology in the routing tables causes a high control overhead.

B. Hybrid Protocols

Hybrid protocols are a mixture of proactive and reactive protocols. Their design merges the benefits of both proactive and reactive protocols to yield better results [14]. The hierarchical network model is used to structure majority of hybrid routing protocols. Firstly, all the routing information that is unknown is acquired by using proactive routing. Then reactive routing mechanisms are used to maintain the routing information when the topology changes [15].

C. Reactive Protocols

Reactive protocols are on demand routing protocols. As the name suggests, the routes to destination nodes are established only when the nodes must send data to destination whose route is unknown. This implies that the source node initiates the searching of routing paths only when needed. When a node wants to send data to a destination node, it starts a route discovery process within the network. Comparative to proactive protocols, the control overhead in reactive protocols is reduced; however the route searching process that occurs before data packets can be forwarded may cause source node to suffer long delays [16]. Reactive protocols use route discovery and route maintenance processes as explained below:

Route Discovery: Route discovery process is a cycle that involves a broadcast route request and a unicast reply that consists of paths that have been discovered [17]. All the nodes in the network keep a record in a routing table. This record consists of information about neighbouring nodes that can forward the packets so that they reach the destination. When a source node wants to send data packets to a destination node, and there is no routing information regarding the destination node in the routing table, the source node initiates a route discovery process [18]. In discovering the route, a source node broadcasts route request (RREQ) packet [19].

When the RREQ packet reaches any node in the network, the node compares the destination IP address to its IP address to determine whether it is the destination node. The node sends back a route reply (RREP) packet if it is the destination, but if it is not, it searches for a route to the destination in its routing table. If there is no route, it broadcasts the RREQ packet to nearby nodes. If there is a route to destination in its routing table, a node compares a RREQ packet sequence number with the destination sequence number in the table to find if the route is updated. The route in the routing table is considered fresh and updated if the destination sequence number in the table is higher than the sequence number attached to the RREQ packet. The intermediate node with an updated route uses the opposite route to send a unicast RREP packet to the source node, and once the source node has received a RREP packet, it begins to send messages through this route. If the route in the table is not fresh enough, the node further sends the RREQ packet to its neighbours [18, 20].

Route Maintanance: During operation, any node that notices a damaged link sends a route error (RERR) packet. A RERR packet is relayed to every node that utilises the affected link for their communication to other nodes [20].

IV. Black Hole Attack

The proper functioning of MANETs depends on the mutual agreement and understanding between the nodes in the network; however some nodes may become malicious and misbehave. Black hole attack is one of the harmful attacks caused by a malicious node that misbehaves in a network [21]. A malicious node exploits the process of discovering routes in reactive routing protocols. When a source node broadcasts a route request, a malicious node misleads other nodes by claiming to have the best path to the destination. The best path is determined by the shortness and freshness of the route. It achieves this by unicasting false route replies, directing data packets to be routed through it and just discarding them instead of forwarding [22]. A malicious node can work independently to launch the attack, and this is referred to as single black hole attack, or malicious nodes can work as a group and the attack is referred to as cooperative black hole attack [15].

A. Black Hole Attack Mitigations

There has been various research carried out to discover and mitigate the black hole attack in MANETs. The techniques were tested on AODV- based MANET. Some of the mitigation techniques are discussed below:

1) Detection, Prevention and Reactive AODV(DPRAODV)

In [23], DPRAODV is proposed. In this scheme, AODV protocol is modified to have a new control packet called ALARM and a threshold value. A threshold value is the average of the difference of destination sequence number in the routing table and sequence number in the RREP packet. In the usual operation of AODV, the node that gets a RREP packet checks the value of sequence number in its routing table. The sequence number of RREP packet has to be higher than the sequence number value in the routing table in order for RREP to be accepted. In DPRAODV, there is an extra threshold value that is matched to RREP sequence number, and if RREP sequence number is greater than the threshold value, then the sender is considered malicious and added to the black list. The neighbouring nodes are notified using an ALARM packet so that the RREP packet from the malicious node is not processed and gets blocked. Automatically, the threshold value gets updated using the data collected in the time interval. This updating of the threshold value helps to detect and stop black hole attacks. The ALARM packet contains the black list that has a malicious node. This list assists the neighbouring nodes not accept any RREP packet sent by a malicious node. Any node that gets a RREP packet looks into the black list and if the

reply comes from a node that has been blacklisted, it is ignored and further replies from that node will be discarded. Thus the ALARM packet isolates a malicious node from the network.

2) Intrusion Detection System AODV (IDSAODV)

IDSAODV is proposed in [24] in order to decrease the impact of black hole. This is achieved by altering the way normal AODV updates the routing process. The routing update process is modified by adding a procedure to disregard the route that is established first. The tactic applied in this method is that the network that is attacked has many RREP packets from various paths, so is assumed that the first RREP packet is generated by a malicious node. The assumption is based on the fact that a black hole node just sends a fake RREP packet, without searching through the routing table. Therefore, to avoid updating routing table with wrong route entry, the first RREP is ignored. This method improves packet delivery but it has limitations that; the first RREP can be received from an intermediate node that has an updated route to the destination node, or if RREP message from a malicious node can arrive second at the source node, the method is not able to detect the attack.

3) Enhanced AODV (EAODV)

In [25], the authors proposed EAODV. Similar to IDSAODV, EAODV allows numerous RREPs from various paths to lighten the effect of black hole attack. This method makes an assumption that eventually the actual destination node will unicast a RREP packet, so the source node overlooks all previous RREP entries, including the ones from malicious node and takes the latest RREP packet. The source node keeps on updating its routing table with RREPs being received until a RREP from the actual destination is received. Then all RREPs get analysed and suspicious nodes are discovered and isolated from the network. The limitation to this method is that it adds two processes that increase delay and exhaust energy of the nodes.

4) Secure AODV (SAODV)

The authors in [26] proposed a secure routing protocol, SAODV that addresses black hole attack in AODV. The difference between AODV and SAODV is that in SAODV, there are random numbers that are used to verify the destination node. An extra verification packet is introduced in the route discovery process. After getting a RREP packet, the source node stores it in the routing table, then sends an instant verification packet using reverse route of received RREP. The verification packet consists of a random number created by the source node. When two or more verification packets from the source node are received at the destination node, coming from different routes, the destination node stores them in its routing table and checks whether the contents contain the same random numbers. If the verification packets contain same random numbers along different paths, the verification confirm packet is sent by the destination node to the source node. The confirm packet consists of random number generated by destination node. If the verification confirm packet contains different random numbers, the source node will wait until at least two or more verification confirm packets contain same random numbers. When two or more verification confirm packets with the same random numbers are received by the source node, it will use the shortest route to send data to the destination node. The security mechanism in this protocol is that malicious node pretending to be the destination node will not send the correct verification confirm packet to the source node.

5) Trust-based Approach

The authors in [27] suggested a trust based approach to mitigate the black hole attack. In this approach, every node keeps a trust value on all its neighbours. The trust value is computed as the proportion of discarded packets to forwarded packets. Each node ensures that the neighbouring node forwards the packets sent to it, unless the packet is destined to the neighboring node. As a way to ensure that the packets are forwarded, each node implements a caching mechanism by storing the packet being forwarded to the neighbouring node in its cache, and then promiscuously monitoring the neighbouring node to check whether it forwards the packet. If the neighbouring node forwards the packet, it compares it with the packet stored in its cache, and the node assumes the packet has been forwarded if they match. Else, after a set time the node assumes the packet has been discarded by its neighbour and the neigbouring node is suspected to be malicious. All the nodes in the network will get to know the behaviour of the neighbouring nodes, and can therefore periodically assign trust values that represent the trustworthiness of the neighbouring nodes. All RREP packets from a node that has been recognised as malicious are ignored, and the routes will only be selected through trusted nodes.

6) Solution Using Packet Sequence Number

In the regular operation of AODV, the source node compares the value of RREP sequence number with sequence number in its routing table. The RREP packet is accepted only if its sequence number has a value higher than the sequence number in sourceôs routing table. A solution that requires the use of two additional small tables in every node is proposed in [5]. The sequence number for the last packet sent by a node is to be recorded in one table and another table should record the sequence number for last packet received from every node. Every time a packet is received or sent by a node, the tables are updated. During route discovery process, the source node broadcasts a RREQ packet to nearby nodes. The destination node or the intermediate node that has a fresh route to the destination will reply to the sender with RREP packet that contains the last packet sequence number received from the source node. The source node will therefore verify that the sequence number of RREP received matches the record it has in the table, and if it does not, the RREP packet is suspected to be from a malicious node. Since the sequence number is already part of communication in the base protocol, this solution does not increase overhead to the transmission channel. It makes it easy to recognise a suspicious reply.

V. SIMULATIONS AND RESULTS

The results are obtained from simulations implemented on Network Simulator 2 (NS-2) and are presented using graphs. NS-2 is distributed freely and is an open source environment which allows the creation of new protocols, and modification

of existing ones, so it is possible to introduce a black hole attack in NS-2 by modifying its source code [28]. A typical simulation with NS-2 consists of creating a scenario file that defines the position and movement patterns of the nodes, and a communication file that defines connection and traffic in the network. Each run of simulation produces a detailed trace file that shows events (such as number of packets delivered successfully) happening during simulation. Fig. 3 illustrates NS-2 simulation process.

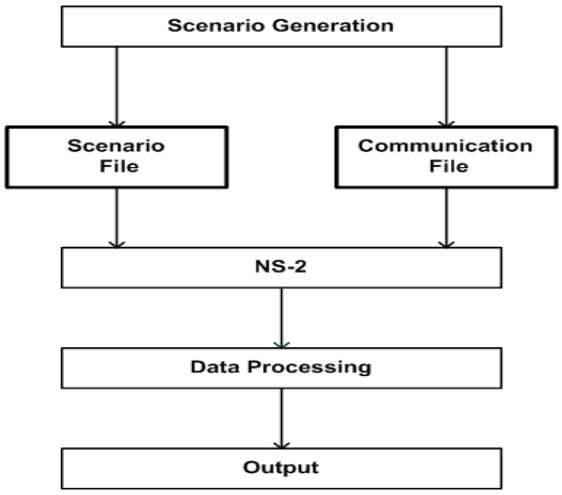

Figure 3. NS-2 Simulation Process

The simulation parameters used in this study are shown in Table I.

TABLE I. SIMULATION PARAMETERS

Parameter	Values
Simulator	NS-2.35
Mobility Model	Random Waypoint
Simulation Time	500 seconds
Terrain Area	670m x 670m
Number of nodes	20
Number of malicious nodes	1
Traffic Type	CBR (UDP)
Packet Size	512 bytes
Routing Protocols	AODV, DSR
Transmission Rate	4 packets/sec
Maximum Speed	20 ï 80 m/s
Pause Time	0 seconds
Transmission Range	250m

The performance metrics used are throughput, packet delivery ratio and end-to-end delay. In order to analyse the effect of mobility, the speed at which the nodes move was varied from 20m/s to 80m/s to create different scenarios. The total number of nodes and maximum number of connections were kept constant at 20 and 10 respectively. The results show the effect of mobility for both AODV and DSR protocols when the network is under a black hole attack and when there is no black hole attack.

A. Throughput

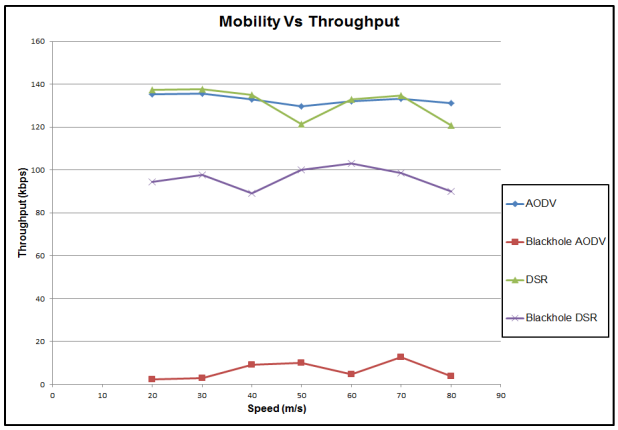

Figure 4. Throughput AODV vs. DSR

The simulation results of Fig. 4 show that increasing the speed of the nodes in the network does not bring significant change in throughput. For both protocols, throughput decreases slightly. This is caused by the rapid change of positions of the nodes, which may cause the path to the destination to change while some packets have been transmitted from the source node using the old route. Therefore the transmitted packets get lost on the way. Throughput of the network under black hole attack decreases because the malicious node discards some of the packets. AODVôs throughput drops drastically compared to DSRôs throughput.

B. Packet Delivery Ratio

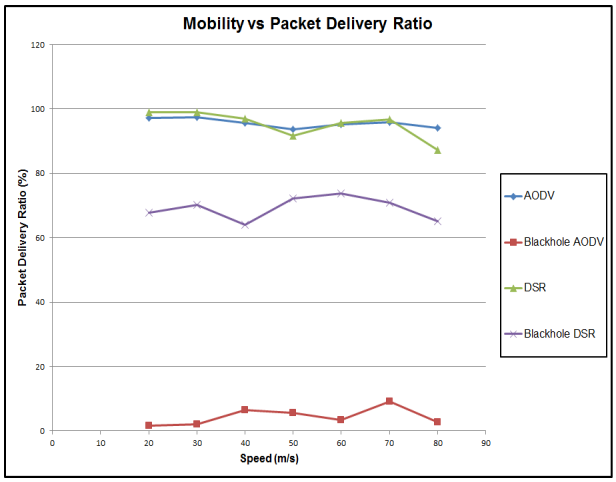

Figure 5. Packet Delivery Ratio AODV vs. DSR

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

C. *End-to-end Delay*

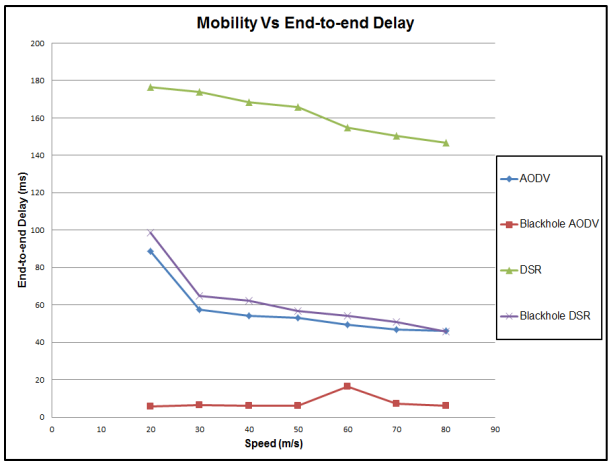

Figure 6. End-to-end Delay AODV vs. DSR

Fig. 6 shows that end-to-end delay decreases with increase in speed because the nodesô movement gets more frequent and the routing updates are regularly exchanged. When there is a black hole attack, end-to-end delay gets even lower because the malicious node pretends to have a valid route to the destination without checking in the routing table, so the route discovery process takes a shorter time.

VI. CONCLUSION

This paper has analysed the black hole attack on MANET reactive routing protocols (AODV and DSR). The analysis is done by varying the mobility of the nodes to determine the effect that mobility has on the way the protocols perform. The results obtained from simulations indicate that the performance of DSR degrades more than the performance of AODV when the speed of the nodes is increased, so it can be concluded that AODV is more preferred in a high mobility network. Furthermore, the results show that the black hole attack degrades the performance of both AODV-based MANET and DSR-based MANET, but the impact is more severe on AODV than DSR. It can therefore be concluded that DSR is more preferred in a network that is frequently attacked by the black hole.

ACKNOWLEDGMENT

We appreciate everyone who supported and encouraged us throughout this study. Most importantly, we thank the University of South Africa and the National university of Lesotho for providing necessary resources that supported the research.

REFERENCES

[1] C. Yu, T. K. Wu, R. Cheng and S. Chang, "A distributed and cooperative black hole node detection and elimination mechanism for ad hoc networks," Emerging Technologies in Knowledge Discovery and Data Mining, pp. 538-549, 2007.

[2] K. Osathanunkul and N. Zhang, "A countermeasure to black hole attacks in mobile ad hoc networks," in Networking, Sensing and Control (ICNSC), 2011 IEEE International Conference On, 2011, pp. 508-513.

[3] B. Wu, J. Chen, J. Wu and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in Wireless Network Security Springer, 2007, pp. 103-135.

[4] C. Rajabhushanam and A. Kathirvel, "Survey of wireless MANET application in battlefield operations," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 2, pp. 50-58, 2011.

[5] R. Mishra, S. Sharma and R. Agrawal, "Vulnerabilities and security for ad-hoc networks," in Networking and Information Technology (ICNIT), 2010 International Conference On, 2010, pp. 192-196.

[6] N. Sharma and A. Sharma, "The black-hole node attack in MANET," in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference On, 2012, pp. 546-550.

[7] Y. Rajesh and S. Anil, "Secure AODV ptotocol to mitigate black hole attack in Mobile Ad hoc Networks," ICCNT 2012 International Conference On, 2012, pp. 1-4.

[8] I. Zaiba, "Security issues, challenges and solution in MANET," vol. 2, pp. 108-109-112, 2011.

[9] P. Goyal, V. Parmar and R. Rishi, "Manet: vulnerabilities, challenges, attacks, application," IJCEM International Journal of Computational Engineering & Management, vol. 11, pp. 32-37, 2011.

[10] U. K. Singh, S. S. KailashPhuleria and D. Goswami, "An analysis of Security Attacks found in Mobile Ad-hoc Network," International Journal of Scientific & Engineering Research, vol. 5, pp. 43-46, 2014.

[11] W. Li and A. Joshi, "Security issues in mobile ad hoc networks-a survey," Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, pp. 1-23, 2008.

[12] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," Wireless Communications, IEEE, vol. 14, pp. 85-91, 2007.

[13] N. Sharma and A. Sharma, "The black-hole node attack in MANET," in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference On, 2012, pp. 546-550.

[14] V. C. Giruka and M. Singhal, "Secure Routing in Wireless Ad-Hoc Networks," in Signals and Communication Technology, pp. 137-158, 2007.

[15] P. K. Singh and G. Sharma, "An efficient prevention of black hole problem in AODV routing protocol in MANET," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference On, 2012, pp. 902-906.

[16] F. Tseng, L. Chou and H. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," Human-Centric Computing and Information Sciences, vol. 1, pp. 1-16, 2011.

[17] A. N. Thakare and M. Joshi, "Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks," IJCA Special Issue on ñMobile Adhoc Networksò, MANETs, pp. 211-218, 2010.

[18] R. Agrawal, R. Tripathi and S. Tiwari, "Performance evaluation and comparison of AODV and DSR under adversarial environment," in Computational Intelligence and Communication Networks (CICN), 2011 International Conference On, 2011, pp. 596-600.

[19] R. H. Jhaveri, A. D. Patel, J. D. Parmar and B. I. Shah, "MANET routing protocols and wormhole attack against AODV," International Journal of Computer Science and Network Security, vol. 10, pp. 12-18, 2010.

[20] N. Purohit, R. Sinha and K. Maurya, "Simulation study of black hole and jellyfish attack on MANET using NS3," in Engineering (NUiCONE), 2011 Nirma University International Conference On, 2011, pp. 1-5.

[21] M. Medadian, A. Mebadi and E. Shahri, "Combat with black hole attack in AODV routing protocol," in Communications (MICC), 2009 IEEE 9th Malaysia International Conference On, 2009, pp. 530-535.

[22] A. Vani and D. S. Rao, "Removal of black hole attack in ad hoc wireless networks to provide confidentiality security service," Int. J. Eng. Sci., vol. 3, pp.2377-2384, 2011.

[23] P. N. Raj and P. B. Swadas, "Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet," IJCSI, vol.3, pp.54-59, 2009.

[24] R. Suryawanshi and S. Tamhankar, "Performance Analysis and Minimization of Blackhole Attack in MANET," IJERA, vol.2, pp.1430-1437, July-August, 2012.

[25] Z. Ahmad, K. A. Jalil and J. Manan, "Black hole effect mitigation method in AODV routing protocol," in Information Assurance and Security (IAS), 2011 7th International Conference On, 2011, pp. 151-155.

[26] S. Lu, L. Li, K. Lam and L. Jia, "SAODV: A MANET routing protocol that can withstand black hole attack," in Computational Intelligence and Security, 2009. CIS'09. International Conference On, 2009, pp. 421-425.

[27] J. Pan and R.Jain, "A survey of network simulation tools: Current status and future development," Internet:http:// www1.cse.wustl.edu/~jain/cse567-08/ftp/simtools.pdf, Nov. 24, 2008 [May 5, 2016].