MANET REACTIVE ROUTING PROTOCOLS NODE MOBILITY VARIATION EFFECT IN ANALYSING THE IMPACT OF BLACK HOLE ATTACK.

E.O. Ochola*, L.F. Mejaele*†, M.M. Eloff and J.A. van der Poll*****

* *School of Computing, University of South Africa, P O Box 392, Pretoria, 0003, South Africa. Email: ocholeo@unisa.ac.za*
† *Dept. of Mathematics and Computer Science, National University of Lesotho, Roma, Lesotho. Email: mejaele2004@gmail.com*
** *Institute for Corporate Citizenship, University of South Africa, Pretoria, 0003, South Africa. Email: eloffmm@unisa.ac.za*
*** *Graduate School of Business Leadership, University of South Africa, Midrand, South Africa. Email: vdpolja@unisa.ac.za*

Abstract: MANETs are exposed to numerous security threats due to their characteristic features, which include absence of centralised control unit, open communication media, infrastructure-less and dynamic topology. One of commonest attack is known as black hole attack, which mostly targets the MANETs reactive routing protocols, such as AODV and DSR. Simulation scenarios of AODV and DSR based MANET were conducted using Network Simulator 2 (NS-2) and NS-3, while introducing the black hole attack in each of the scenarios, to analyse the protocols' performances. The different scenarios are generated by changing the mobility (locations) of the nodes. The performance metrics that are used to do the analysis are throughput, end-to-end delay and packet delivery ratio. The simulation results showed 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 a destination without checking the routing table, and therefore shortens the route discovery process. The results also showed that throughput decreases slightly when mobility of the nodes is increased in the network. The increase in the speed of the nodes decreases both packet delivery ratio and end-to-end delay. The closer the black hole node was to the source node requesting the transmission, the worse the impact. A focused analysis on AODV indicates that, even with the introduction of relatively few black hole nodes to the network, there still exist a potential to bring significant disruptions to communication.

Key words: MANET security, reactive routing protocols, black hole attack, mobility.

1. INTRODUCTION

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 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 Figure 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 constrained in terms of bandwidth and battery power [2, 3].

MANETs are suitable for providing 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

Based on: "Effect of Varying Mobility in the Analysis of Black Hole Attack on MANET Reactive Routing protocols", by E.O. Ochola, L.F. Mejaele, M.M. Eloff and J.A. van der Poll which appeared in the Proceedings of Information Security South African (ISSA) 2016, Johannesburg, 17 & 18 August 2016.

network infrastructure in disaster recovery operations where temporary network infrastructure is immediately needed [4, 5].

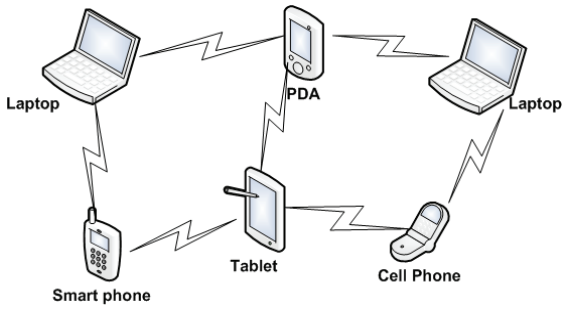

Figure 1: Mobile Ad-hoc Network

The features of MANETs expose them to many security attacks compared to other traditional networks. The high mobility and dynamic topology of MANETs makes 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 constrained 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 a 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 MANET's 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 2 discusses the vulnerabilities of MANETs that expose them to attacks. Section 3 describes routing in MANETs and discusses the different categories of routing protocols, focusing more on reactive routing protocols. Section 4 explains black hole attack, and describes some of the solutions that have been suggested to lessen the impact of the attack. Section 5 gives the simulation structure used to perform the analysis, presents the results obtained from the simulations and gives the analysis of the results. Section 6 concludes the paper.

2. 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 MANETs' vulnerabilities are presented as follows:

2.1 Lack of secure boundaries

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

2.2 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 centralized management delays the nodes' 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 centralized authority can sometimes lead to decentralised decision-making. In MANETs, important algorithms depend on all nodes participating cooperatively. Hence, the attacker can take advantage of this vulnerability and execute attacks that can ensure that the nodes are not cooperative [9].

2.3 Threats 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].

2.4 Restricted power supply

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

3. 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 categorized into proactive, reactive and hybrid protocols based on the way paths are established and maintained by the nodes [6]. The hierarchy of the protocols is shown in Figure 2, illustrating the two reactive routing protocols discussed and analysed in this paper.

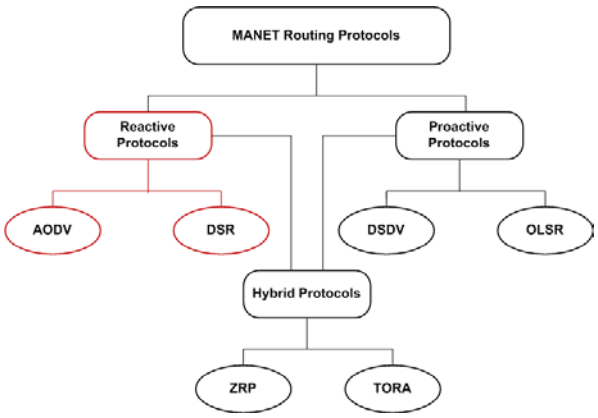

Figure 2: MANET protocols hierarchy

3.1 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.

3.2 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]. Figure 3 summarises the route discovery process in reactive protocols.

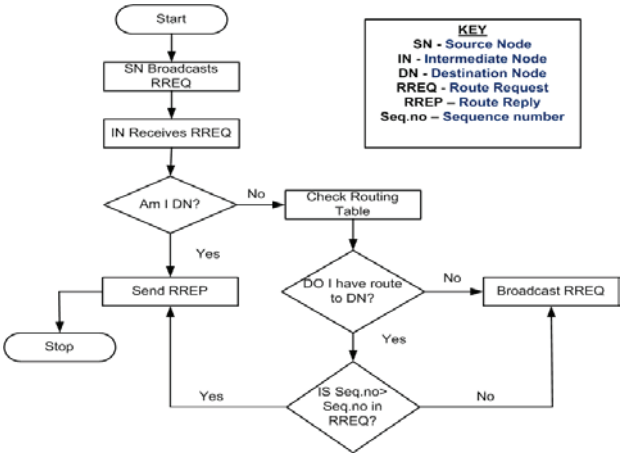

Figure 3: Route discovery in reactive protocols

Route Maintenance: During operation, if the source node changes position, it has to establish a new route to the destination by reinitiating route discovery process. But if an intermediate node or a destination node changes position, then any node that notices a damaged link sends a route error (RERR) packet. A RERR packet is relayed to every node that utilizes the affected link for their communication to other nodes. When a RERR packet is received by the source node, it can stop sending the data, or send a new RREQ packet [20].

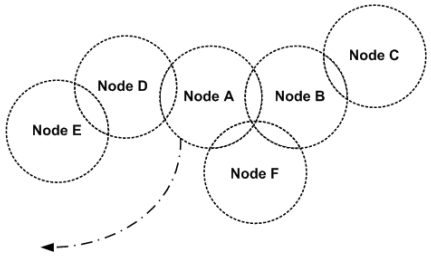

Figure 4: Route maintenance in reactive protocols

In Figure 4, if Node A leaves the network, Node F which is in the communication range of Node A and Node B will not get a HELLO message from Node A, and that is how node F discovers that Node A has moved. The route through Node A is then marked as invalid by Node F and a RERR message is transmitted to Node B to notify it that Node A is not a neighbour anymore.

3.3 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].

4. 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].

4.1 Black hole attack categories

The black hole attack can also be classified into two categories based on the cause of the attack: Black hole attack caused by RREP and that caused by RREQ [13] as illustrated in Figure 5 and Figure 6 respectively.

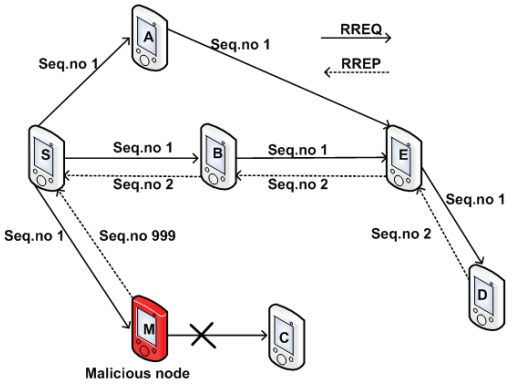

Figure 5: Black hole attack via RREP

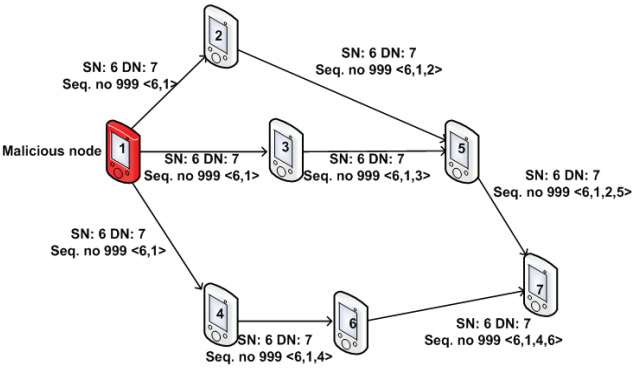

Figure 6: Black hole attack through RREQ

In Figure 5, the black hole sends a forged RREP message pretending to have a fresh and short path to the destination. This means the black hole always returns a positive RREP even when it has no valid route to the destination. The data packets that are transmitted to the destination will therefore pass through a malicious node which will silently absorb or discard them. In Figure 6, the black hole sends a forged RREQ message to attack a target node in the network. This black hole pretends to be rebroadcasting the RREQ packet that originated from a target node in the network. It then adds itself as the next hop in the route record, so the entire messages destined to the target node will pass through it and it will discard the messages.

4.2 Black hole attack mitigations

There has been various research carried out to discover and mitigate the black hole attack in MANETs [29]. The techniques were tested on AODV-based MANET. However, none of the existing black hole attack mitigations provide a solution that prioritises the detection and elimination of a malicious node based on its closure proximity to the source node, yet such closeness during route discovery process is considered to be more dangerous to the network performance. Some of the mitigation techniques, with similar omissions are discussed below:

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.

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.

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.

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.

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 neighbouring 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 neighbouring 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 recognized as malicious are ignored, and the routes will only be selected through trusted nodes. A trust based solution approach is further suggested in [28] where each node calculates a trust value of neighbouring nodes. If trust goes below a certain threshold, then the node discards the neighbour from future routes. This solution was simulated on NS2 and showed much better results in scenarios where the AODV protocol is under attack.

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 source's 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 recognize a suspicious reply.

The omission of black hole attack analysis based on the malicious node's location from the source node in the discussed existing solution approaches makes it necessary to conduct such experiments as presented in section 5.2.

5. SIMULATIONS AND RESULTS

This section presents and discusses simulation results that were conducted under varied parameters, to analyse the performance of selected reactive routing protocols (AODV and DSR). The simulations were carried out at different node mobility speed and the network performance were analysed under normal condition (i.e., no black hole node), and when under attack by a black hole node. AODV routing protocol was given further attention under different setup, as discussed in section 5.2, after it performed dismally in comparison to DSR, as presented in section 5.1.

5.1 AODV vs DSR in a highly dynamic network

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. Figure 7 illustrates NS-2 simulation process.

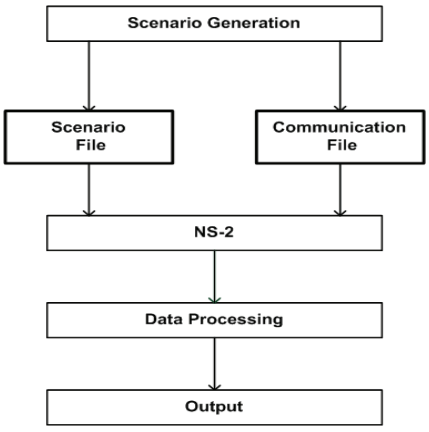

Figure 7: NS-2 Simulation Process

The simulation parameters used in this sub-section are shown in Table 1.

Table 1: AODV and DSR simulation parameters

Parameter:	Values:
Simulator	NS-2.35
Mobility Model	Random Waypoint [13]
Simulation Time	500 seconds
Terrain Area	670m x 670m
Number of nodes	20
Number of black hole nodes	1
Traffic Type	CBR (UDP)
Packet Size	512 bytes
Routing Protocols	AODV, DSR
Transmission Rate	4 packets/sec
Maximum Speed	20 – 80 m/s
Pause Time	0 seconds
Transmission Range	250m

Sub-section results analysis: 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.

Throughput: The simulation results of Figure 8 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. AODV's throughput drops drastically compared to DSR's throughput.

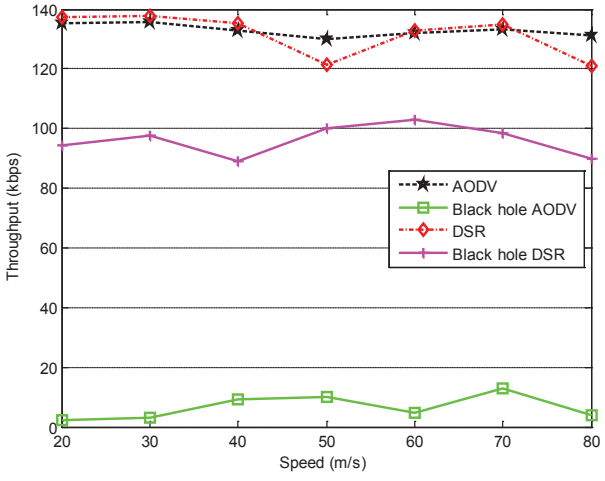

Figure 8: Throughput AODV vs. DSR

Packet delivery ratio: When the mobility of the nodes is increased packet delivery ratio decreases a little, as illustrated in Figure 9. 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 nodes' 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.

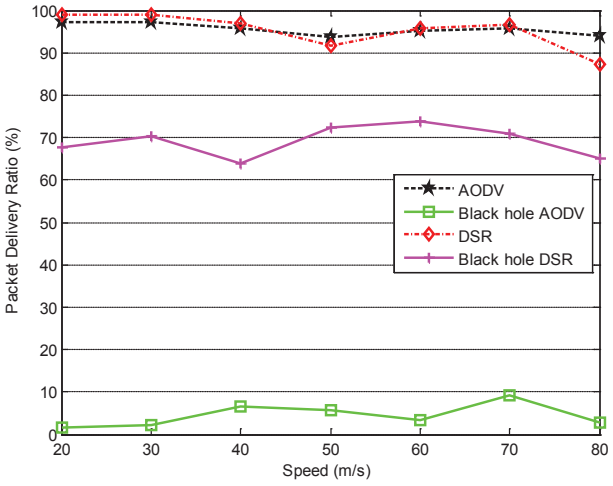

Figure 9: Packet delivery ratio AODV vs. DSR

End-to-end delay: Figure 10 shows that end-to-end delay decreases with increase in speed because the nodes' 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.

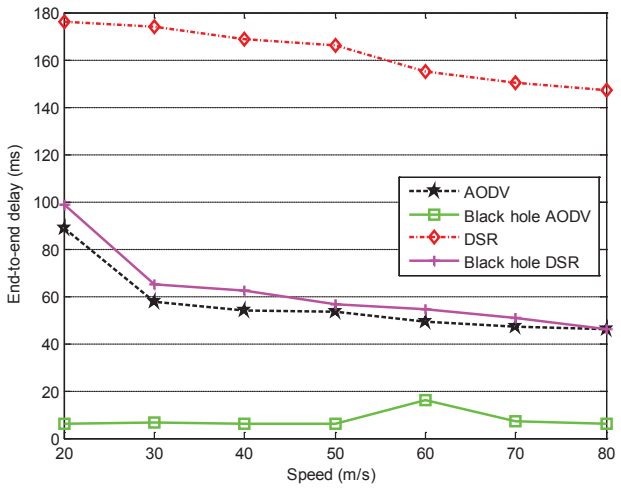

Figure 10: End-to-end delay AODV vs. DSR

5.2 A focus on AODV at low mobility and dense network

This sub-section presents the simulation of a black hole node implementation which was done through the modification of the existing AODV implementation, according to the NS 3.16 version. A modification to the routing protocol to include a black hole node was achieved through the introduction of a black hole flag to the node that exhibits black hole attack features, i.e., that which replies positively to every received route request, thereby acting as the communication end point. Figure 11 shows the simulation network grid, and a node's transmission range within the grid. Figure 12 is an illustration of a route chosen by the AODV routing protocol for a successful PING, which originates from node 0 to node 99. The route followed by the packet keeps on changing as the network topology changes, and with the introduction of a black hole node in the network, the malicious node may attract traffic to form part of the intermediaries. The effectiveness of a black hole node is determined by its grid position at the time of packet transmission in relation to the source and destination nodes positions. Nodes were set to have minimal movements according to the implemented mobility model. Applicable modifications to the simulation setup were done as shown in Table 2.

Table 2: Modified AODV simulation parameters

Parameter:	Values:
Simulator	NS-3.16
Mobility Model	Random Walk [13]
Number of nodes	100
Number of black hole nodes	1
Routing Protocols	AODV

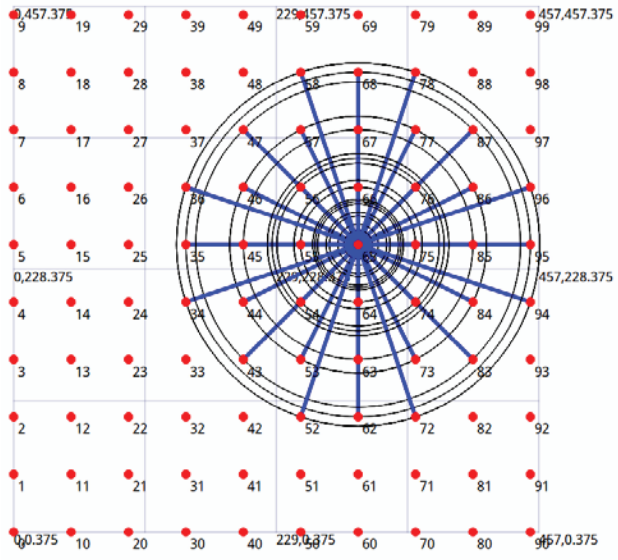

Figure 11: Simulation grid and node range

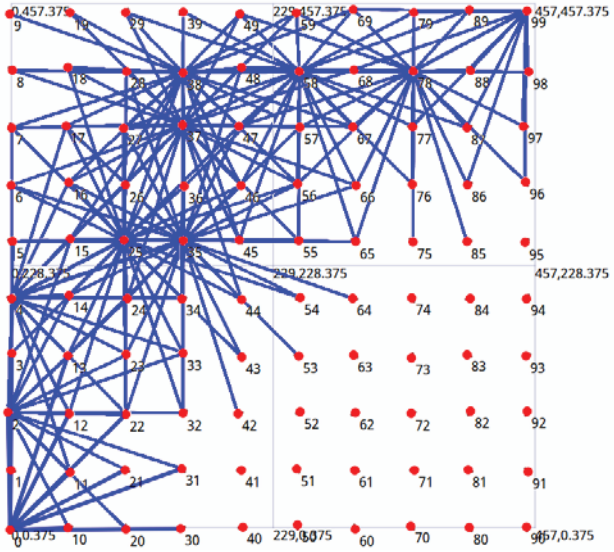

Figure 12: Ping message transmissions

Sub-section evaluation of results: Simulation runs were conducted in a network with and without a black hole node. The scenarios in which black hole nodes were present indicated that the attack had a devastating effect on the network performance. This was evident by the fact that all the traffics that were destined for node 99 via a black hole were dropped at the malicious node. However, there were successful packet delivery in scenarios where the black hole node was not an intermediary during the packet relay, e.g., when the malicious node was at the grid peripheries. Though, this didn't occur in most of the simulation runs due to the long transmission ranges of the nodes, which mostly enabled black hole nodes to be involved in the route. But, with shorter transmission ranges or densely populated network, there could be scenarios of missing black hole along the route, which leads to successfully transmission. However, even with no packet drops from attackers, few cases of unsuccessful packet delivery could be recorded due to the nature of MANETs such as wireless channel errors and path breaks as a result of dynamic topology, leading to generations of RERR message notifications.

Black hole nodes which were located closer to the source node at the time of transmissions caused great negative impacts to the network performance, as shown in Figure 13, an example of which was when node 25 in Figure 12 was selected as the black hole. Figure 13 shows a complete communication breakdown when the black hole node was introduced. The performance of an attack free network is also shown in the figure, on how MANET performed normally under similar settings. However, with increased number of PING requests and having the black hole positioned further away from the source node, the network had normal packet transmissions for a while, until the black hole node was finally encountered, as shown in Figure 14. An example of which was when node 73 in Figure 12 was set as the black hole. This is an indication of possibly not being able to notice the

existence of black hole nodes in a network, unless they are encountered along the route.

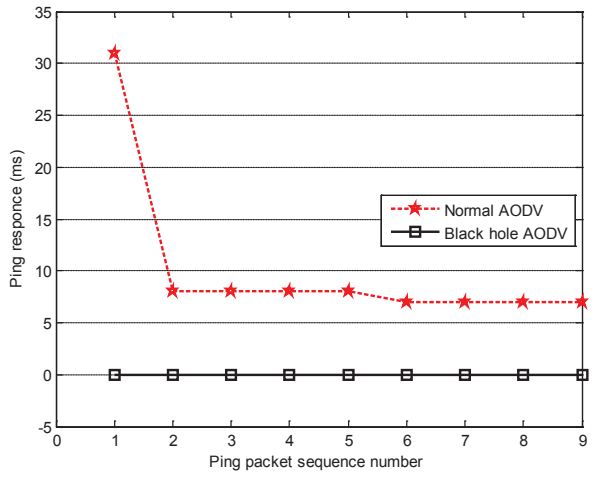

Figure 13: Effect of Black hole node closer to source node at transmit time

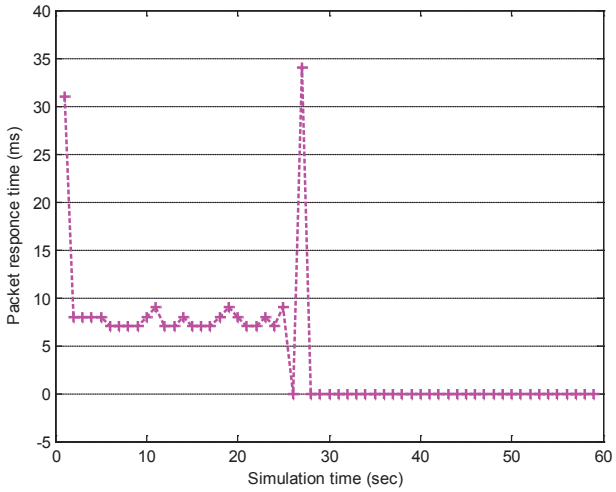

Figure 14: Effect of black hole node that is far away from the source node during message transmissions

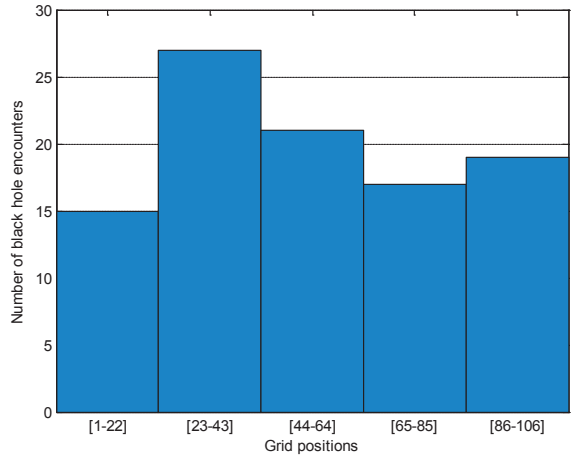

Figure 15: Black hole nodes' distribution on the grid

A histogram displaying the distribution of black hole nodes within the network grid is shown in Figure 15. The data were cumulated at the end of the simulation runs. These values depict a well distributed selection of black hole nodes over the network grid, as usually occur in the practical scenario. This is necessary in results validation.

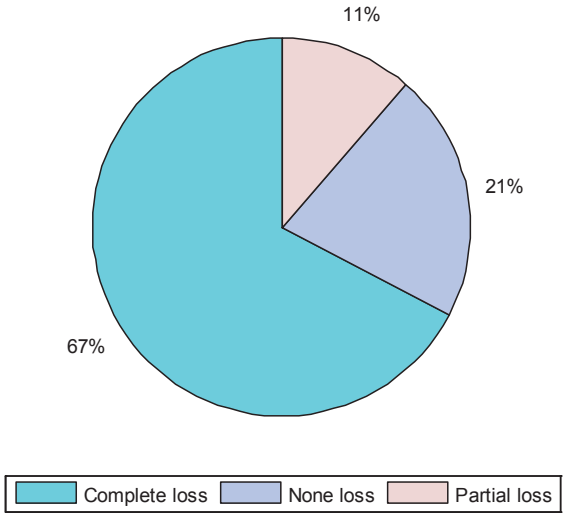

Figure 16: Data loss due to black hole attacks

Figure 16 presents the destructive nature of the attack, in which 67% of transmissions completely failed to be delivered, 11% of the transmitted packets experienced partial loss (i.e., delivered with errors), and only 21% of the transmission were successful. The successful packet deliveries occurred whenever a route didn't include a black hole node as an intermediary. However, all packets were dropped (i.e., complete loss) in all the cases where a black hole was part of the route during packet transmission. The data presented in Figure 16 was collected from the 100 simulation runs performed.

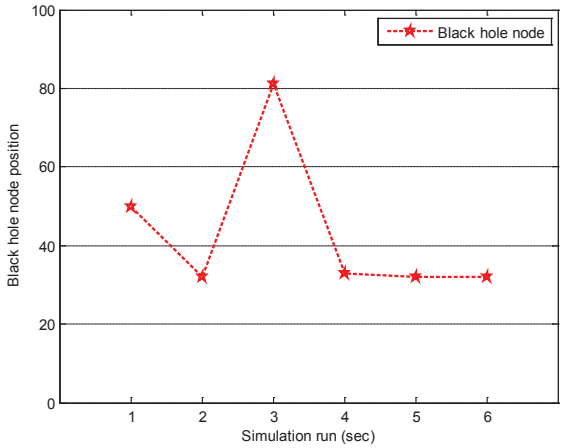

Figure 17: Black hole nodes with minimal impact

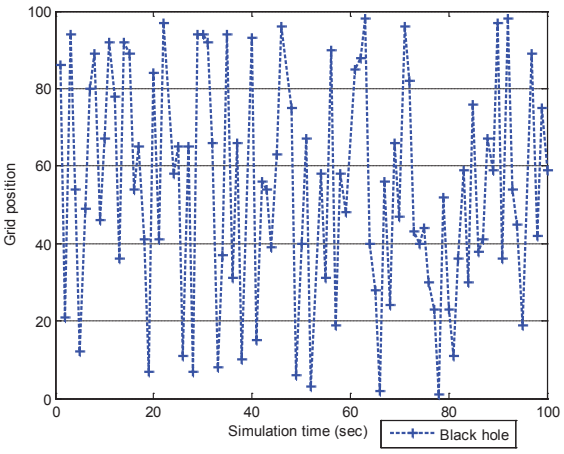

Figure 18: Black hole nodes with greatest negative impact

The black hole node position at the start of the simulation run had a contribution on to what extent the attack impact could be to the network performance. Figure 17 shows the initial black hole node positions which posted minimal interference to packet transmissions. This implied that the nodes mostly failed to be part of the routes during the simulation runs, when they originally occupied such locations on the grid, since communications were successful in those scenarios. The figure shows that the black hole nodes were mostly never encountered when they were initialised at the grid positions within node 20 to 40. Such consistency correlated with the minimal node mobility setup. The greatest attack impacts were recorded when the black hole nodes were initialised at positions shown in Figure 18. With malicious nodes occupying those positions at the beginning of each simulation run, most of the packets were never delivered, as they were consumed by the black hole nodes, an indication that an attacker was successful in attracting the traffic and thereby dropping the packets, a successful scenario of black hole attack execution.

6. CONCLUSION AND FUTURE WORK

The section presents the paper concluding remarks and gives the future research directions along the study focus area. Conclusions on the network performance comparisons between AODV and DSR routing protocols are presented in section 6.1. Whereas, concluding remarks focusing further on AODV routing, are similarly presented under section 6.2.

6.1 Joint analysis of AODV and DSR in a highly dynamic network

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.

6.2 Isolated AODV analysis at low mobility

Standard AODV: Ideal conditions (e.g., long transmission ranges, low node mobility and densely populated network) were setup to favour AODV routing protocol, which resulted to good performances, despite the dynamic topologies. It was found that long enough nodes' transmission ranges in a relatively less dynamic network, yielded AODV best performances. Such favoured AODV performance may be too good for the real world practical scenario, where devices settings are not necessarily uniform. The favourable settings were intentionally put in place to give the protocol an upper hand in the presence of an attacker in the network, so as to register some successful transmissions, for performance analysis purposes.

Standard AODV with black hole nodes: A different network performance was noted whenever a simulation run was conducted in the presence of a black hole node. The performance degradation impact depended on the attacker's position at the beginning of each simulation run. Total packet losses were registered whenever a black hole node was located closer to a source node during transmission, leading to the worst cases of network performances. However, successful communications were recorded whenever the black hole node was located far away from the source node, mostly at the grid peripheries. This meant that the malicious node was not encountered during the packet transmissions, as chances of having it as an intermediary node was reduced. The simulation setup was favourable to AODV routing protocol, with only 1% of the network nodes being set as a black hole in every simulation run. The real world practical network performance may be worse than the simulation tests results, since MANET are mostly deployed in hostile environments, which may have many malicious nodes at a given time, thereby completely halting the network operations, through cooperative black hole attack. In addition, the real world implementation scenario may show lower network performances, when more packets are dropped naturally due to channel errors, e.g., transmissions collisions due to the wireless media.

The results analysis confirms the need to investigate black hole attack solutions that have the ability to vary priorities (detection metrics parameters) based on the suspect's location from a source node. Implying that, a suspect closer to a transmitting node should receive higher penalties to be blacklisted earlier to avoid potential

devastating attacks. A future work will focus on proposing a black hole attack solution which takes into consideration the position of a potential black hole node during route discovery. Future works will also include comparisons of results obtained from simulation runs against those from real world experiments, under similar setups, to analyse simulation error margins. In addition, future work will consider experiments with different models of mobility and different traffic patterns.

7. 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", *Proceedings of the IEEE International Conference on Networking, Sensing and Control (ICNSC)*, pp. 508-513, 2011.

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

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

[5] R. Mishra, S. Sharma and R. Agrawal: "Vulnerabilities and security for ad-hoc networks", *Proceedings of the International Conference on Networking and Information Technology (ICNIT)*, pp. 192-196, 2010.

[6] N. Sharma and A. Sharma: "The black-hole node attack in MANET", *Proceedings of the 2nd International Conference on Advanced Computing & Communication Technologies (ACCT)*, pp. 546-550, 2012.

[7] Y. Rajesh and S. Anil: "Secure AODV protocol to mitigate black hole attack in Mobile Ad hoc Networks", *Proceedings of the 3rd International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1-4, 2012.

[8] I. Zaiba: "Security issues, challenges and solution in MANET", *International Journal of Computer Science and Technology*, Vol. 2 No. 4, pp. 108-112, 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, K. Phuleria, S. Sharma and D. Goswami: "An analysis of Security Attacks found in Mobile Ad-hoc Network", *International Journal of Advanced Research in Computer Science*, Vol. 5 No. 5, pp. 34-39, 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", *IEEE Wireless Communications*, Vol. 14 No. 5, pp. 85-91, 2007.

[13] M. K. J. Kumar and R. S. Rajesh: "Performance Analysis of MANET Routing Protocols in Different Mobility Models", *IJCSNS International Journal of Computer Science and Network Security*, Vol. 9 No. 2, pp. 22-29, 2009.

[14] V. C. Giruka and M. Singhal: "Secure Routing in Wireless Ad-Hoc Networks", *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", *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 902-906, 2012.

[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 No. 4, 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 MANETs*, Vol. 1 No. 4, pp. 211-218, 2010.

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

[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 No. 4, pp. 12-18, 2010.

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

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

[22] A. Vani and D. S. Rao: "Removal of black hole attack in ad hoc wireless networks to provide confidentiality security service", *International Journal of Engineering Science and Technology*, Vol. 3, pp.2377-2384, 2011.

[23] P. N. Raj and P. B. Swadas: "DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET", *IJCSI International Journal of Computer Science Issues*, Vol.2, pp.54-59, 2009.

[24] R. Suryawanshi and S. Tamhankar: "Performance Analysis and Minimization of Blackhole Attack in MANET", *International Journal of Engineering Research and Applications (IJERA)*, Vol.2 No. 4, pp.1430-1437, 2012.

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

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

[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].

[28] F. Thachil and K. C. Shet: "A Trust Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET", *Proceedings of the International Conference on Computing Sciences*, pp. 281-285, 2012.

[29] E. O. Ochola, M. M. Eloff and J. A. van der Poll: "Beyond Watchdog Schemes in Securing MANET's Reactive Protocols Operating on a Dynamic Transmission Power Control Technique", *Proceedings of the SAI Computing Conference*, pp. 637-643, 2016.