ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(29), DOI: 10.17485/ijst/2015/v8i29/84653, November 2015* ISSN (Online) : 0974-5645

Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios

Christeena Joseph*, P. C. Kishoreraja, Radhika Baskar and M. Reji

Saveetha School of Engineering, Saveetha University, Chennai - 600072, Tamil Nadu, India;
christeena003@gmail.com, pckishoreraja@gmail.com, radhikabaskr@gmail.com, rejime@gmail.com

Abstract

Background/Objectives: Mobile Adhoc Networks (MANETS) are prone to different types of attacks due to lack of central monitoring facility. The objective is to investigate the effect of black hole attack on the network layer of MANET for different network scenarios. **Method:** A black hole attack is a network layer attack which utilizes the destination sequence number to claim that it has a fresh and a shortest path to the destination and consumes all the packets forwarded by the source. The various network scenarios of MANETS with AODV routing protocol are simulated using Network Simulator Version 2 (NS-2) to analyse the performance with and without the black hole attack. The scenarios are created by varying the number of nodes and nodes speed, varying position and number of the black hole nodes and number of flows. The performance parameters like PDR, delay, throughput, packet drop and control overhead are measured. **Findings:** The black hole attack degrades the network performance. The impact of attack is severe when the attacker is near to the source node, less severe when it is in midway between source and destination and has least effect when it is farther from the source. The overall throughput and PDR increases with the number of flows but reduces with the attack. With the increase in the black hole attackers, the PDR and throughput reduces and close to zero as the number of black hole nodes are maximum. The packet drop also increases with the attack. The overall delay factor varies based on the position of the attackers. Throughput, PDR and control overhead decreases with the network size due to congestion and average delay reduces with black hole attack as the black node sends the Route ERRor (RREP) without performing any route checking. As the mobility varies, the delay and packet drop increases but PDR and throughput decreases as the nodes moves randomly in all directions. **Conclusion:** The simulation results gives a very good comparison of performance of MANETS with and with out black hole attack for different network scenarios.

Keywords: AODV Protocol, Black Hole Attack, MANET, Network Scenarios, Performance Metrics

1. Introduction

One of the key issues of Adhoc network is that it is more prone to security threats due to insecure boundaries, threats from compromised nodes, lack of central monitoring system**,** restricted power supply, continuously changing topology, open medium and cooperative algorithms. MANETS are vulnerable to different types of DoS attack. Black hole attack is a network layer which uses destination sequence number to claim that it has a fresh and shortest path to the destination and consumes all the packets forwarded by the source node[1,2]. The aim of this paper is to study the impact of the black hole attack in the performance parameters of wireless ad hoc networks with AODV routing protocol for different scenarios like varying network traffic, network size, black hole nodes, mobility and position of attackers.

The rest of the paper is organized as follows. Section 2 provides an overview of security attacks in MANET Section 3 describes overview of AODV protocol Section 4 describes how the black hole attack is performed on AODV, Section 5 deals with performance parameters affected due to black hole attack, Section 6 presents the simulation scenarios and comparison of results and finally Section 7 discusses the conclusion with the plan for the future work.

* *Author for correspondence*

2. Security Attacks in MANET

MANETs are highly prone to attacks by malicious nodes that disrupt the communication in the network. Based on the nature, attacks can be classified as active attack which affects the normal functioning of the network by modifying the packets and passive attacks which intercepts the packets without disrupting the network activity[1,5]. Further based on where the attacks are initiated, it can be internal and external. External attacks are carried out by nodes that are not part of the network whereas internal attacks are done by the compromised nodes that are in the network[12]. Some attacks are classified according to the layer of occurrence[13,17]. Table 1 show the various attacks on the different layers of the network[14].

3. Overview of AODV Routing Protocol

The primary function of the routing protocol is to establish routes between the source-destination pair and delivery of messages to the correct destination. These protocols are basically classified in to three based on the routing procedure: Table Driven or Proactive, On Demand or Reactive and Hybrid. The basic difference between the proactive and reactive is that the routes to all nodes are determined and stored in each node table before transmission session in the former where as in the latter, it is determined when the source wants to send data to destination. Hybrid routing protocols utilizes the best features of both[7,11].

Table 1. Attacks on different layers of Network

Layer	Types of Attack	Description
MAC layer	Jamming	Malicious node damages the transmitted packets by causing interference to the communication frequency and hence prevents the reception of legitimate packets
Network layer	Black hole attack	The attacker uses the routing protocol and forges the RREP to advertise itself as having latest path to the destination and consumes the packets without forwarding
	Worm hole attack	This attack is carried out by a malicious node by collecting packets at one location and tunnelling them to different location, where these packets are replayed into the network.
	Byzantine attack	This attack is carried out by selfish nodes which are not bothered by its own resource consumption. The attack may be carried out in collusion and disrupts network activity by creating routing loops, dropping packets forwarding packets.
	Resource consumption attack	The attacker waste resources of other nodes in the network by sending unnecessary requests for routes, beacon packets or stale packets.
	Routing attack	Attacks are mounted on the routing protocols for disrupting network normal functioning
	Gray hole attack	Malicious node selectively drops the packets.
Transport layer	Session hijacking	The attacker spoofs the victim's IP address, and then performs a DoS attack on the victim.
Application layer	Repudiation	Repudiation attacks refer as denial of participation in the communication and the attacker node keep accessing the system as a selfish node.
Multi-Layer attack	Denial of Service(DoS)	DoS attacks prevent the legitimate and authorized users from the services offered by the network.
	SYN Flooding	SYN packets are sending to victim by malicious node by spoofing the return addresses of the SYN packets.
	Distributed DoS attack	DoS attack carried out by cooperative malicious nodes
	Impersonation	A compromised node gets access to the network management system and changes the configuration of the system as a privileged user.

AODV protocol is an on demand routing protocol. The route is established only when it is required by a source node for transmitting data packet and the routes are maintained until it is required for transmission. The most recent path to the destination is determined by AODV protocol by using the destination sequence number In AODV every mobile node maintains a routing table that stores the next hop information for a route to the destination node.

When a source node wishes to route a packet to a destination node, it initiates the route discovery process if a fresh route to the destination is not available in the table[8–10]. The working of the AODV is as follows. A source node broadcasts a RREQ (Route Request) packet to one hop neighbour nodes. The fields pertaining to RREQ packet are source ID, source sequence number, hop count Destination ID, Destination sequence number, Broadcast ID, and time to live. The identifier for the RREQ is source ID - Broad cast ID pair. A node may receive the same RREQ several times and can be discarded by checking the RREQ identifier. Every node that receives the packet, checks if it is the destination for that packet and if so it unicast a RREP packet to the source. If it is not the destination, it checks whether it has a path to the destination, else broadcast the packets to its neighbours. If the routing table has an entry to the destination, the next step is to compare the sequence number in the table to that of the RREQ packet. If the sequence number present in the table is less or equal than the RREQ packet, then the node broadcasts the request to its neighbours by incrementing the hop count, else it indicates the route is a fresh route and forwards the packet to the destination. Each intermediate node which receives the RREQ sets up a reverse route entry for the source node in its table so that RREP can be send to the source in this route. This table will have the information of source ID, source sequence number, hop count to source node, address of the node from which the RREQ is received and time to live. The table entry will deleted automatically if the RREP is not received with in time to live. Upon receiving the RREQ the destination node creates the RREP packet. The RREP has the information of source ID, destination ID, destination's latest sequence number and hop count The RREP packet from the destination is sent as unicast to the source through the intermediate nodes. Each intermediate node which receives the RREP makes a forward route entry to the destination and data packets are sending to the destination according to this route information. The forward route entry has the information of destination D, next hop, hop count to the destination and life time for the entry. The source node then updates the information and sends the data packets through this route. The node forwards the first RREP it receives from multiple RREP or may forward another RREP if it has greater sequence number or hop count and in a way reduces the number of RREPs forwarded to the source.

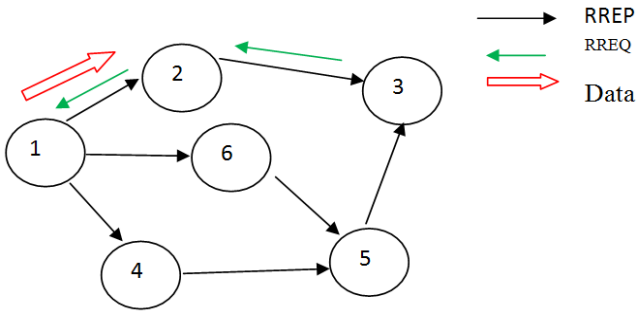


Figure 1. Mechanism of route discovery in AODV protocol.

The other two messages used are Route ERRor (RERR) and Hello messages. The RERR is transmitted to notify the link failure to all the other nodes. Upon receiving RERR, a node makes its route to the destination invalid by setting hop count as ∞. When the source receives the RERR, it initiates a new route discovery process for destination. The HELLO messages are sending periodically for monitoring links to the neighbours and failure to receive HELLO messages are confirmed as link failures. Figure 1 illustrates the working of AODV protocol. AODV is a simple routing protocol with good packet delivery ratio, less end-end delay, less packet drop and routing overhead. The link failure feature makes it efficient in the high mobility scenarios. AODV uses limited band width that is available in the media and the operation is loop free.

4. Black Hole Attack on AODV Protocol

In MANET, nodes within the wireless transmission ranges can communicate directly whereas nodes outside each other's range depend upon intermediate nodes to relay messages by hop method[1,17]. Thus each node acts as both sender and router. AODV protocol is prone to black hole attack as it has no security mechanisms and black hole nodes can perform many attacks by not adhering

to rules of AODV protocol[3,6]. A black hole attack is DoS attack, where a malicious node claims that it has a fresh route to the destination and absorbs the packets without forwarding to the destination. Figure 2 illustrates the black hole attack. Node **1** wants to send the packets to the destination node **3**. Initially it broadcasts the RREQ. The nodes **2**, **4** and **M** receive it. Node 6 becomes malicious node **M** and immediately sends a RREP packet to **1**, claiming it has the fresh path to the destination without even checking the routing table. Since node **1** receives the RREP packet ahead of nodes **2** and **4**, it starts sending the packets to **3** through **M** assuming that it to be the shortest route. Malicious node **M** absorbs all the data packets without forwarding to destination and behaves like a black hole.

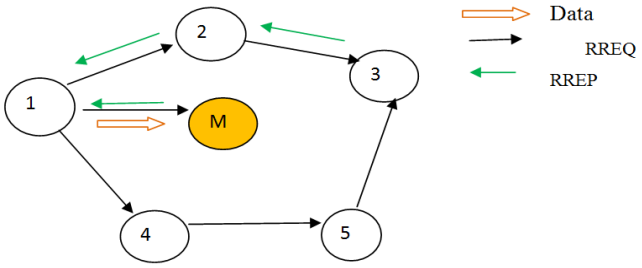


Figure 2. Black hole attack in AODV.

5. Performance Parameters of Wireless Adhoc Networks

The black hole attacks have severe impact on the performance of the wireless ad hoc networks. The parameters that credit the network performance are packet delivery ratio, Throughput, Delay, Jitter, Normalised Control Overhead, Packet Drop, Reachability, Hop Count and Neighbour node density. The black hole attack can cause adverse effect on these performance metrics. A brief discussion on the parameters is given below.

5.1 Packet Delivery Ratio

It is the ratio of the number of delivered data packet to the destination to the packets send by source. ∑ Number of packet received/∑ Number of packet sends. The packet delivery ratio decreases when there is a malicious node in the network because some of the packets are dropped by the black hole node[6].

5.2 Delay

The average time taken by a data packet to reach the destination node[8]. It includes the delay in the path finding process and in the queue. The end to end delay decreases with black hole attack as the black node replies immediately without checking the routing table.

5.3 Packet Drop

It is the total number of packets dropped due to reasons like time expiration, collision and congestion in the queue. The packet drop is very high when black-hole node is present in the network as the black hole node consumes the packets.

5.4 Throughput

Throughput is amount of data transferred from source to destination in a given amount of time. It is measured in kbps. The throughput of the network decreases considerably due to black hole effect[8].

5.5 Jitter

It is the time duration between arriving packets, caused by network congestion, route changes. The average jitter between the nodes is more without the Black hole attack due to the fact that black hole nodes provide the path with fewer numbers of nodes.

5.6 Control Overhead

It is the ratio of the control packets to the total number of the received data packets.

5.7 Normalized Routing Overhead

It is the average ratio of total routing control packets transmitted to the total data packets received at the destination[10]. It should be lower for efficient network and it increases with black hole attack.

5.8 Energy Consumption

It is the average energy used by the node in the network[15]. It decreases with black hole attack because the packets transmitted between source and destination gets dropped which leads to less transmission between the nodes.

5.9 Hop Count

It is number of nodes traversed by a packet to reach the destination[15]. The hop count reduces with black hole attack as it claims shortest path.

5.10 Reachability

It is ratio of successful routes to the available routes[15]. With the increase in black hole nodes, reachability degrades.

5.11 Neighbour Node Density

It is the number of neighbouring nodes corresponding to a node[15]. The neighbour Node Density reduces with increase in black hole nodes.

5.12 Path Optimality

It is defined as the ratio of the shortest path with black hole nodes to the shortest path length without the black hole nodes[15]. As black hole nodes increases, Path Optimality decreases.

5.13 Network Load

It is the total traffic in bits per seconds received by the entire network from higher layer of MAC which is accepted and queued for transmission. The network load decreases with a black hole attack.

6. Simulation Model

The NS-2 (Network Simulator Version 2) is an object-oriented, discrete event driven network simulator developed at UC Berkeley written in C++ and OTcl and is available as open source. It is widely used for simulating wired and wireless networks. It follows the layered approach and has protocols for governing the networks[16]. The simulation is done using NS-2 to analyse the performance of wireless ad hoc network with and without the black hole attack. At the physical and data link layer IEEE 802.11 is used. The channel is wireless channel with Two Ray Ground Propagation model. The protocol used at the network layer is AODV. The AODV protocol can model the behaviour of nodes as normal nodes or black hole. The traffic pattern was generated using CBR as the data source and UDP protocol is used for transporting the data and the packet size is of 512 bytes. The simulations are done for different scenarios by varying the number of nodes, mobility of the nodes, position of the black hole node, the number of flows and the number of black hole nodes. All the simulations are carried out with simulation profile given in the Table 2. The performance comparison of wireless adhoc network with AODV routing protocol without and with black hole is carried out based on the parameters like PDR, delay, throughput and packet drop.

6.1 Simulation Profile

Table 2. Simulation parameters

Simulation Parameter	Value
Simulation Area	1000*1000 m
Routing Protocol	AODV
Traffic Source	CBR
Number of nodes	50,100,150
Size of data packet	512
Node Placement	Random
Simulation time	200s
Connection time	25s
Speed	0, 5m/s,10 m/s
Number of flows	2- 5
Number of black hole nodes	1-5
Movement model	Random way point
Pause time	20s

6.2 Simulation and Results

In this study the simulations are carried for different scenarios to evaluate and compare the performance of the network with AODV routing protocol with and without the black hole attack. Various scenarios are simulated to see the effect of the black hole attack on the parameters like PDR, delay, throughput, packet drop, control overhead and normalized routing overhead. Figure 3 represents the simulation of Black hole node in an adhoc network with AODV protocol.

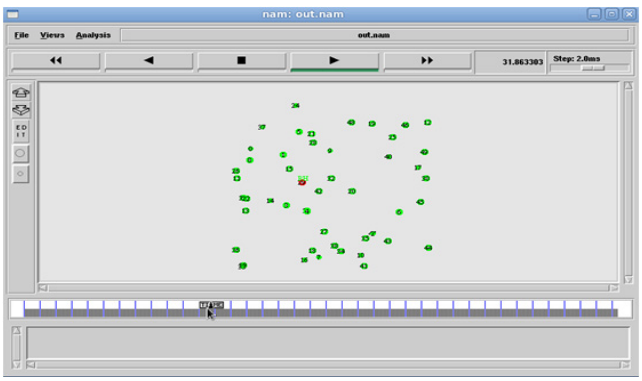


Figure 3. Simulation of Black hole attack.

6.2.1 Scenario 1: Position of the Attacker

The simulations are done with black hole attacker on different positions and therefore to study the impact on the performance parameters. The positions are fixed near and far from the source node and also midway between source node and destination node. All the 150 nodes including the attacker are stationary and the number of connections is 3. From the simulations it is seen that the impact of attack is severe when the attacker is near to the source node, less severe when it is in midway between source and destination and has least effect when it is farther from the source. Table 3 shows the performance variation of the network with respect to the position of the attacker.

Table 3. Variation of network parameters with respect to position of the attacker.

Parameter	No Attack	Near Source	Midway	Far from source
PDR	65	21	35	50
Throughput	61819	17995	29991	42545
Delay	0.0087	0.0060	0.0098	0.0108
Packet Drop	130	240	203	187

6.2.2 Scenario 2: Variation in the Network Traffic

The effect of the variation in the network traffic on the performance parameters is studied. The traffic is varied by varying the number of flows keeping all the 150 nodes

Figure 4. Variation of network parameters with varying traffic.

stationary. The connections are fixed to 2, 3, 4 and 5. The performance parameters like Packet Delivery ratio, Packet Drop, Throughput and delay are analysed for black hole attack and no attack condition. The black hole node is also kept stationary. It is clear from the simulation that the overall throughput and packet delivery ratio increases with the number of flows but reduces with the attack. The delay decreases with the attack as the black hole does send the highest destination sequence number without verifying the route to the destination. The packet drop increases with the attack. The Figure 4 shows the impact of attack on the parameters PDR, Delay, Throughput, Packet drop. The packet delivery ratio is least with 2 flows scenario. This is due to the proximity of the black hole node to the source node.

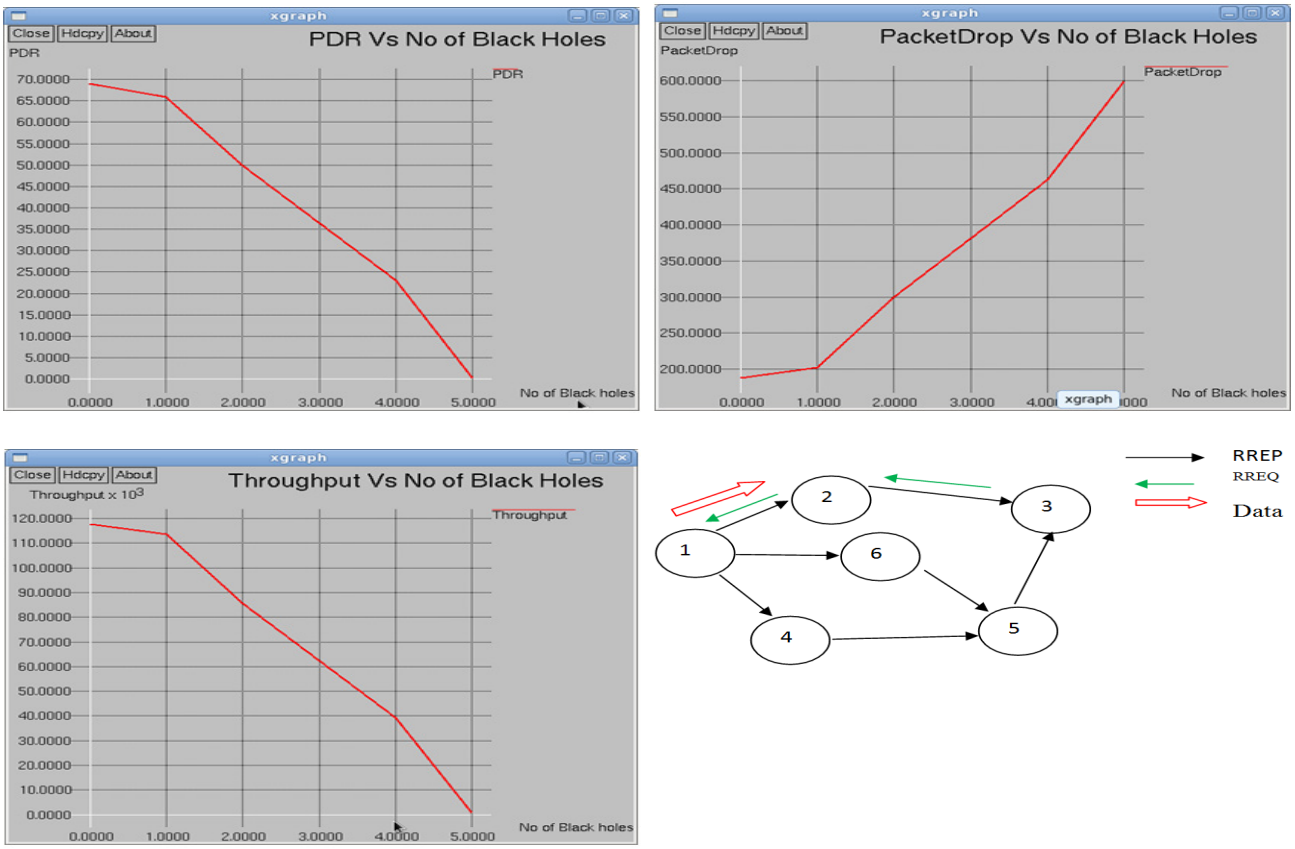


Figure 5. Variation of network parameters with varying number of black hole attacks.

6.2.3 Scenario 3: Variation in the Number of Black Hole Nodes

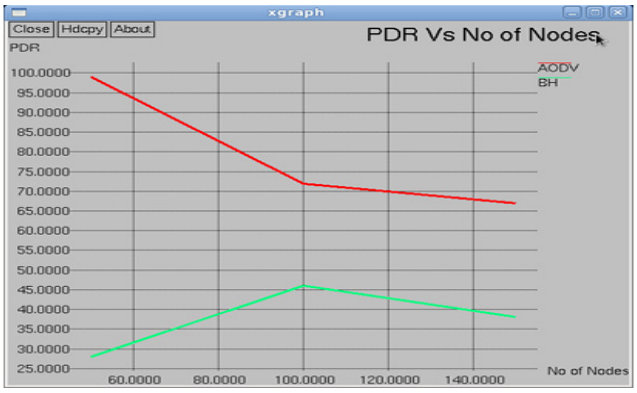
The simulation is carried out to study the impact of varying number of black hole attackers in the network. The number of flows is set to 4 and the numbers of black hole attacks are varied from 0 to 5. The performance of network with respect to PDR, delay, throughput and packet drop is analysed. As the number of black hole attackers increases, performance degradation in the network occurs as the packet delivery ratio and throughput decreases and close to zero as the number of black hole nodes is 5. The packet drop also increases. The overall delay factor varies based on the positions of the attackers and the time it takes to attack the network and divert the traffic towards itself. The variation in the network parameters with varying number of black hole attacks is shown in Figure 5.

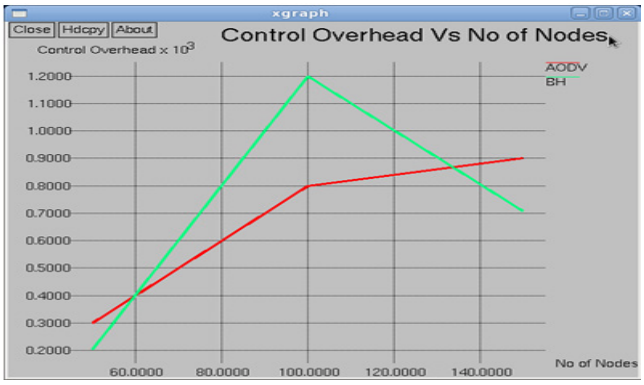
6.2.4 Scenario 4: Variation in the Network Size

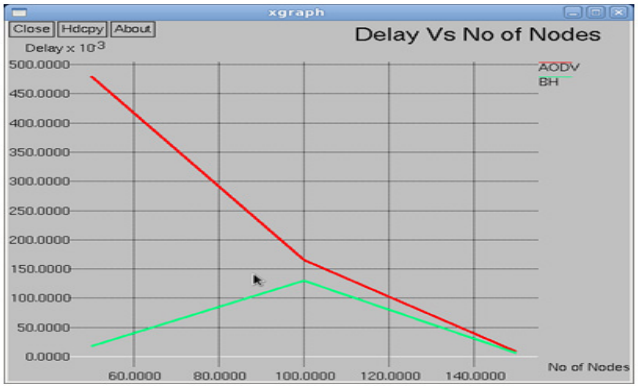
The network size is varied by changing the number of nodes to 75, 100 and 150. All the nodes are set as stationary and the numbers of connections are fixed as 3. It is evident from the simulations that throughput, PDR and control overhead decreases with the network size due to congestion and average delay reduces with black hole attack as the black node sends the RREP without performing any route checking. The normalized routing load also has increased with black hole attack. Figure 6 represents the variation of the parameters with variation in network size with and without attack.

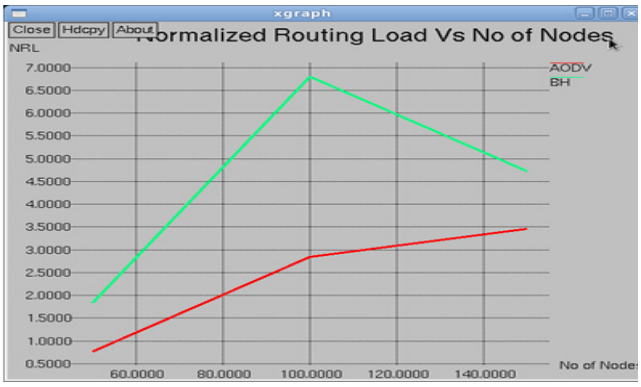
6.2.5 Scenario 5: Variation in the Mobility Speed

In scenario 5 the simulations are carried out for different mobility speeds of the nodes. The speeds are fixed to 0 m/s, 5 m/s and 10 m/s. The number of nodes, pause time and flows are fixed to 150, 10s and 3 respectively. As the mobility varies the delay and packet drop increses but the packet delivery ratio and throughput decreases as the nodes moves randomly in all directions degrading the performance. Figure 7 shows the variation of network parameters for different mobility speeds.









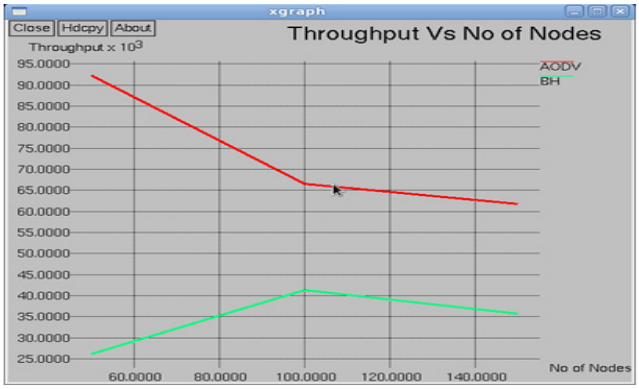
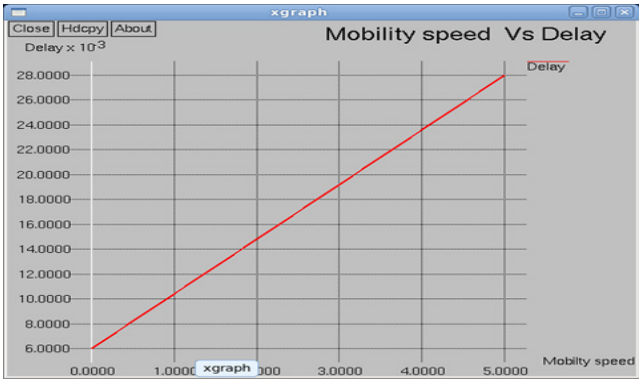
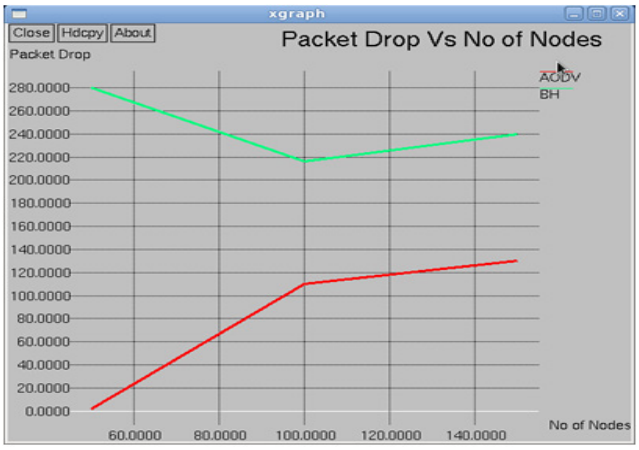
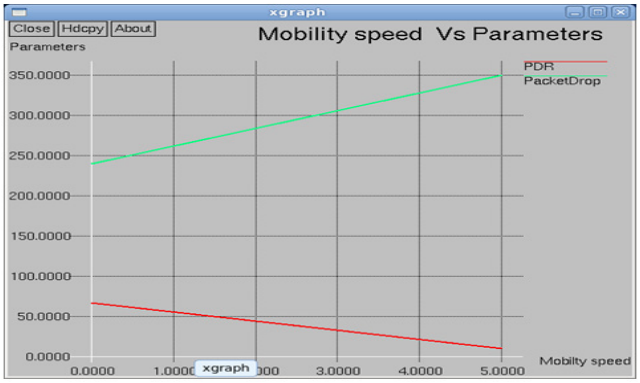


Figure 6. Variation of network parameters with network size.







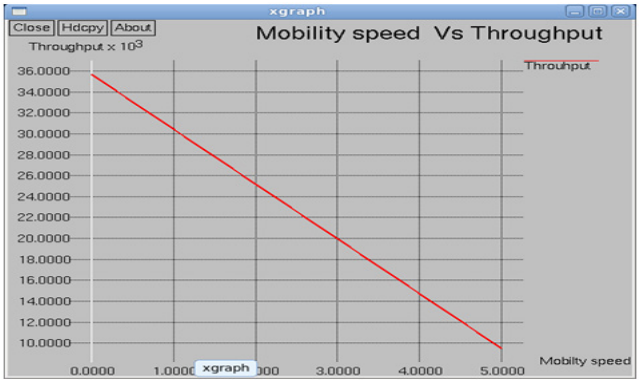


Figure 7. Variation of network parameters with varying mobilty speed.

7. Conclusion

In all the scenarios simulated and studied, it is noticed, with the black hole attack the network parameter degrades. With the increase in network traffic, throughput and PDR increases and packet drop decreases under no attack condition. It is also observed that when the attacker is near the source the impact is severe than it is farther. Similarly as the number of black hole increases, PDR and throughput decreases. In all the simulations the proximity of attacker to the sending node has impact on the average delay and it decreases with black hole attack. This is due of the fact that the black hole sends the RREP with highest destination sequence number without verifying for a route in its routing table. Many researchers have proposed different types of prevention schemes by modifying basic AODV protocol. The Intrusion Detection Systems (IDS)[4,18] can detect whether the network is under an attack, notify the network and hence able to isolate the attacker. The future work is to propose an Anomaly Intrusion Detection System (ADIS) with machine learning algorithm to detect, prevent the black hole attack and to find the source of attack. The anomaly detection system has advantage over signature and specification IDS is that it can detect unknown attacks. The anomaly detection method monitors and analyses the data packets for suspicious activities and compares it against an established normal traffic profile. Two threshold levels can be introduced to determine the normal behaviour. If the captured profile value goes beyond the threshold values, it can be considered as abnormal and an alarm packet can be send to the network so that the black hole node can be isolated. The machine learning algorithm is also included in IDS where in an application automatically learns from input and feedback to improvise its performance.

8. References

1. Tseng F-H, Cou L-D, Chao C. A survey of black hole attacks in wireless mobile ad hoc networks. Human Centric Computing and Information Sciences. A Springer Journal. 2011; 1:4. Available from: http://www.hcis-ournal.com/content/1/1/4
2. Sarma KJ. A survey of black hole attack detection in MANET. IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT); 2014. p. 202–5.
3. Sharma N, et al. The black hole node attack in MANET. IEEE Conference Proceedings of Advanced Computing and Communication Technologies (ACCT); 2012. p. 546–50.
4. Xenakis C, Panos C, Stavrakakis I. A comparative evaluation of intrusion detection architectures for mobile ad hoc networks. Computers and Security - COMPSEC. 2011; 30(1):63–80.
5. Mulert J, Welch I, Winston KG. Seah security threats and solutions in MANETs: A case study using AODV and SAODV. J Netw Comput Appl. 2012; 35(4):1249–59.
6. Ramaswamy S, et al. Prevention of cooperative black hole attacks in Wireless adhoc networks. International Conference on Wireless Networks; Las Vegas. 2003. p. 1–7.
7. Sun B, Guan Y, Chen J, Pooch UW. Detecting black-hole attack in mobile ad hoc networks. Proceedings of EPMCC; UK. 2003 Apr 22-25. p. 490–5.
8. Tamilselvan L, et al. Prevention of black hole attack in MANET. The 2nd International Conference on Wireless Broad Band and Ultra Wideband Communication (AusWireless 2007); 2007 Aug. p. 21.
9. Perkins CE, Das SR, Royer E. Adhoc on demand distance vector. 2000 Mar.
10. Yibeltal, et al. Preventing black hole attack in mobile adhoc networks using anomaly detection. 2nd International Conference on Future Computer and Communication; 2010. p. 672–6.
11. Abolhasan M, Wysocki T, Dutkiewicz E. A review of routing protocols for mobile ad hoc networks. Ad Hoc Networks. 2004; 2(1):1–22.
12. Narang EK, Sonal. A study of different attacks in wireless mobile adhoc networks and discussion about solutions of black hole attack on AODV protocol. International Journal of Advanced Research in Computer Engineering and Technology. 2013 Apr; 2(4):1601–6.
13. Rai AK, Tewari RR, Upadhyay SK. Different types of attacks on integrated MANET-internet communication. Int J Comput Sci Secur. 4(3):265–74.
14. Jawandhiya PM, et al. A survey of mobile ad hoc network attacks. International Journal of Engineering Science and Technology. 2010; 2(9):4063–71.

15. Nagpal CK, et al. A study of black hole attack on MANET performance. Int J Modern Education and Computer Science. 2012; 8:47–53.
16. Available from: http://nile.wpi.edu/NS
17. Amiri R, Rafsanjani MK, Khosravi E. Black hole attacks detection by invalid IP addresses in mobile ad hoc networks. Indian Journal of Science and Technology. 2014 Apr; 7(4):401–8.
18. Kishore Raja PC, et al. Efficient approaches to improve the performance metrics of wireless intrusion detection system. Int J Comput Appl. 2012; 57(3):19–27.