Performance Analysis of Black Hole Attacks For Different Mobile Ad Hoc Networks

Danista Khan

Department of Electrical Engineering
The University of Lahore, Lahore, Pakistan

ABSTRACT

In order to configure nodes, Mobile Ad-Hoc Networks (MANETs) adapt a dynamic topology without any centralized system. This means that without any existing infrastructure they basically form a dynamic wireless link so that the MANET's nodes can communicate with each other. The nodes can enter or leave a MANET at their own liberty. As MANETs lack centralized system, so they are bare to various security attacks such as Black Hole, Sybil and byzantine. These attacks damage the network topology, which becomes the cause of network degradation and data loss. In Black Hole attack, the node generally declares itself having the shortest possible path for all the destinations in the network. This malicious node degrades the network performance as it misuses the routing protocol by absorbing all the data packets of the network. This paper evaluates the performance degradation in MANETs when the black hole is placed under different network scenario.

Keywords: *AODV, DoS attacks, black hole attack, MANET*

1. INTRODUCTION

In a MANET [7], mobile nodes do not have any proper network architecture. In this network, the nodes configure themselves autonomously and move around by following mobility models such as random waypoint [17]. Due to the mobility of the nodes in MANETs, the topology of the network is always dynamic as any node can enter the network at any time and can become part of it [10]. For data packets to be sent to destinations that are far from source nodes, the in-between nodes that are part of the network behave as routers. As MANETs do not need any preexisting infrastructure so they can be cheaply deployed and can be used in education, cellular extensions, smart buildings and military battlefields [11].

The communication between nodes in MANETs is done by following network layered routing protocol, which comprises of three categories that are Proactive, Reactive and Hybrid. In Reactive protocols, route is decided only when the source node desires to send data to the destination node such as DSR, AODV.

✉ danista91@gmail.com

In Proactive protocols, all possible paths of the network are initially established and stored in the tables. The paths are then updated periodically as the nodes move in the network, which consumes the bandwidth and power. Examples are: DBF, DSDV, and WRP. The qualities of both reactive and proactive protocols combine to make Hybrid protocols. Examples are: TORA, ZRP [8] [9]. In MANETs, these routing protocols do not have any security mechanism to protect themselves from different network layered attacks like Black Hole, Byzantine, Hello flood attack, Selective forwarding and Wormholes. Day by day, the scientists are proposing different techniques to secure MANETs from these Black Hole attacks [1-6][18]. In this paper we have done the performance analysis of MANETs when they are introduced with Black Hole attacks. The results of which can be used to propose a technique to isolate and overcome Black Hole attacks in MANETs.

Rest of the paper is divided as follows. Ad hoc on demand distance vector (AODV) protocol and black hole attacks are discussed in section II. While the performance metrics used for evaluation for different network scenarios are discussed in III. The results are presented in section IV. In the last section, conclusion and future work is discussed.

2. BLACK HOLE AND AODV PROTOCOL

2.1. AODV

The AODV protocol consists of two phases.

A. Route discovery

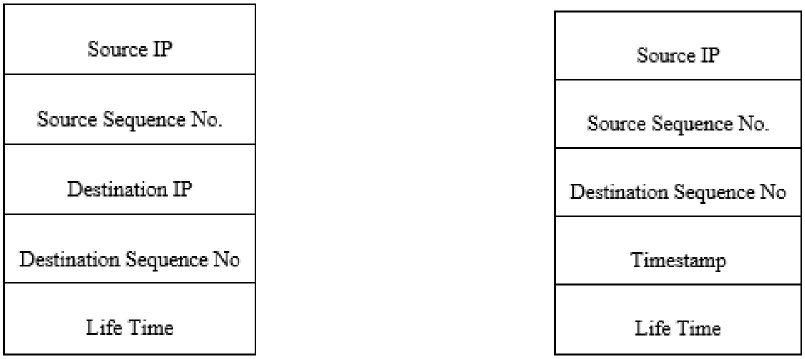
In route discovery, source node broadcasts Route Request (RREQ) packet in the network. On receiving the RREQ, nodes check their routing tables to find the route to destination node [15][18]. If there is a fresh route in the routing table, it replies the source with Route Reply Packet(RREP) packet. On receiving multiple path requests, the source node selects that node which has the shortest path and initiates transmitting data packets in the direction of selected route. Fig. 1 [18] shows the information in packets of RREQ and RREQ.

B. Route Maintenance

In MANET, the topology of the network is dynamic due to the mobility of nodes[16], so the paths keep on changing between source and destination. Route Error (RERR) packet is generated when the route breaks so that new routes can be found immediately.

1. Black hole (BH) attack

It is a denial of service (DoS) attack. In this attack, services of the network become unavailable due to one or more malicious nodes [12-14]. In this attack, malicious node declares itself as having the authentic and nearest route to destination. Thus the intermediate nodes start sending all the data packets for the destination in its direction. For this, the attacker has to continually monitor the network traffic, and when the source node generates any RREQ it replies with a fake RREP with highest sequence number so that it can be selected for the shortest path. Source node then starts sending to malicious node,



(a) RREQ (b) RREP

Fig. 1. Packet of AODV protocol

which then drop all the packets that it has recieved thus degrading the network performance

Fig. 2 explains how the malicious node starts receiving data packets. The ‘S’ node want to send data to node’ D’ so it initiates route discovery phase of AODV protocol in the network by distributing RREQ packet, which is then received by ‘B’ node and ‘1’ node [18].

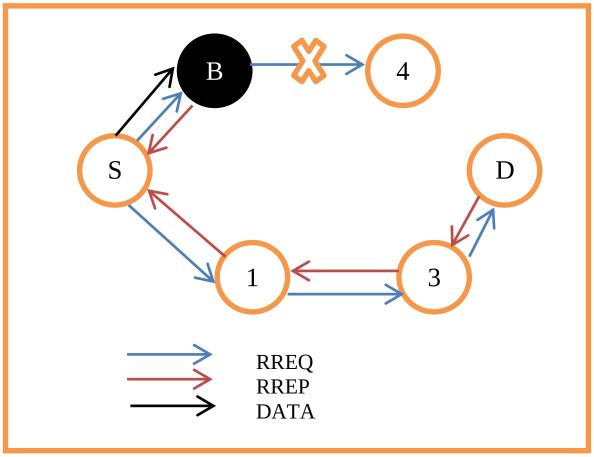


Fig. 2. BH attack in AODV

The malicious ‘B’ node generates RREP packet immediately with highest sequence number, without even checking its routing table. As ‘S’ node gets RREP from ’B’ node instantly, the ‘S’ node assumes that ‘B’ node is providing the shortest path to ’D’ node. Thus, ‘S’ node initiates sending data in the direction of ’B’ node, which then drops the data packets instead of forwarding them to ‘D’ node. This results in degradation of network’s throughput by exploiting routing of AODV protocol.

3. PERFORMANCE METRICS AND NETWORK SCENARIOS

A. Performance metrics

The performance of MANET under malicious node attack is done by calculating the following metrics:

1) *Packet Delivery Ratio (PDR):* The proportion of successful packets received by destination to total number of packets transmitted by source. Packets may not be received due to poor wireless connections or absorbing of traffic by malicious node. PDR can be calculated as:

PDR=Packets Received ÷ Packets Sent (1)

2) *End- End Delay (EED):* The time delay that occurs in the transmission of packet from source to destination. Delay can be due to a propagation, queuing, processing or retransmission delay. EED can be calculated as:

EED= No of links (Propagation delay+ queuing delay+ Processing delay+ Transmission delay) (2)

3) *Packet Drop:* Number of packets that were not successfully received by the destination due to malicious nodes or poor connections. It can be calculated as:

Packet Drop= Packet Sent – Packet Delivered (3)

4) *Average Throughput*

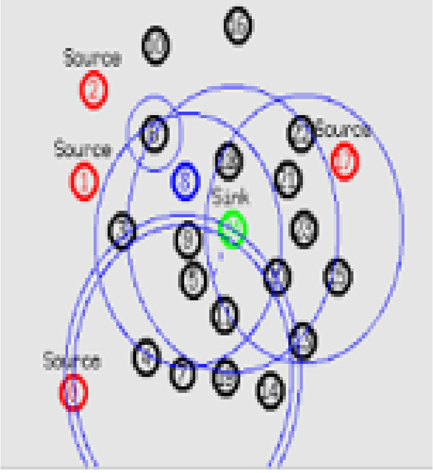
The bits of data transferred from source to sink in a defined time.

B. Network Scenarios

*1) Network without Black Hole node:*For this model, 25 nodes are deployed in the network simulator NS -2.34. The node 25 acts as the destination node whereas node 0, 1, 2 and 17 behaves as source nodes. Node 0 transfers the data to node 13 by using node 7 as an intermediate node, node 1 uses node 3 as an intermediate node, node 2 directly sends the data and node 17 uses node 21 as an intermediate node to send the data to node 13. The nodes 0,4,22 and 2 are made mobile with the speed of 40m/s so that the simulation can be covered in a real mobile environment. This model is shown in Fig. 3.

*2) Network with Black Holes:*A number of nodes are introduced one by one in the network as black holes to evaluate the degradation in performance of network. Different simulations are performed to check the locations which degrades the performance of network the most. In the beginning, node 7 is introduced in the network as malicious node, after that node 3 is also activated as malicious node , then node 18 and in the end node 22 are introduced as a malicious node.The dropping packets by Black Hole nodes are shown in Fig. 4. The performance metrics are calculated with each black hole and the graphs are plotted as shown in the next section. It is analyzed that there is a huge amount of packet drop when black holes are placed near sources.

3) Varying network size with Black Holes: After introducing black holes in the network, the size of the network is changed to check the effect of malicious node on the size of network. The node size is varied from 10 to 25 and then 50 with the same traffic. It is analyzed that the performance of the smallest network is degraded the most by black holes.



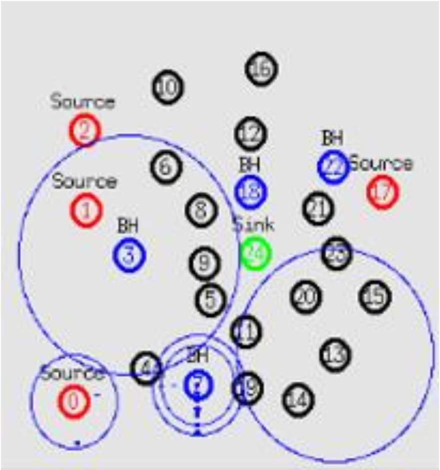


Fig. 3. Network without Black Hole

Fig.4. Network with Black Hole

4. SIMULATIONS AND RESULTS

All the network scenarios in Section III are simulated in network simulator 2.34. The results are generated using the AWK files on the trace files to calculate the throughput, PDR, packet drop and EED. Table 1 summarizes the parameters used in NS2.34

Table 1. Simulation Parameters

Simulator	NS-2.34
Protocol	AODV
No. of nodes	10-50
No. of black holes	0-4
Simulation area	1000m*1000m
Mobility	20m/s
Simulation time	20s
Mobility model	Random Waypoint
Traffic Source	CBR

A) Performance analysis with increasing number of black holes

In the graphs shown in the Fig. 5-8, it can be observed that by increasing the number of BH in network, performance of network is degrading. Throughput, EED and PDR are decreasing whereas packet drop is increasing.

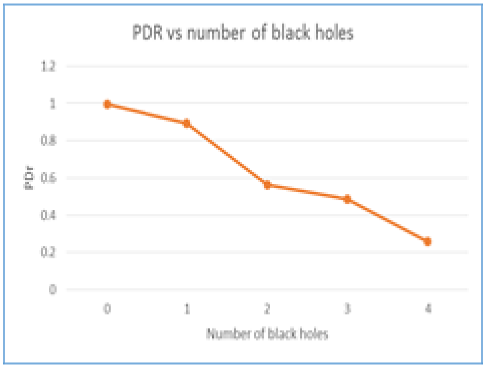


Fig.5. PDR vs no of black holes

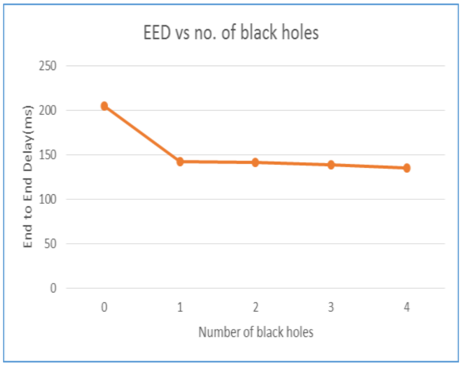


Fig. 6. EED vs no of black holes

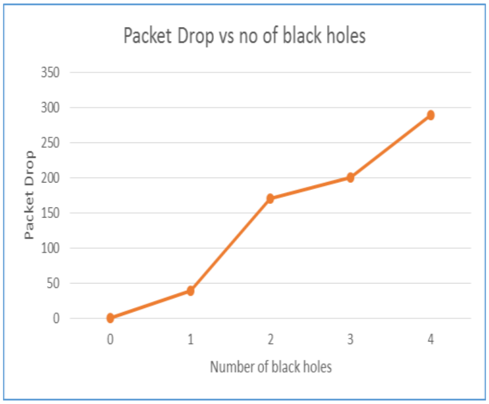


Fig.7. Packet Drop vs no of black Holes

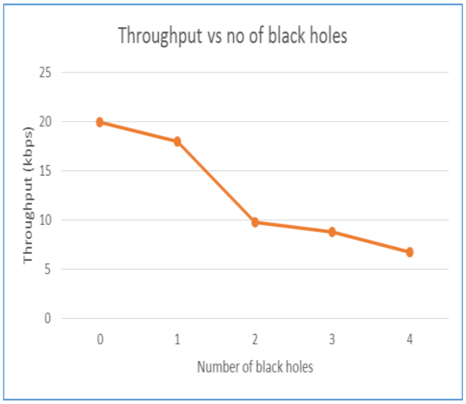


Fig.8. Throughput vs no of BH

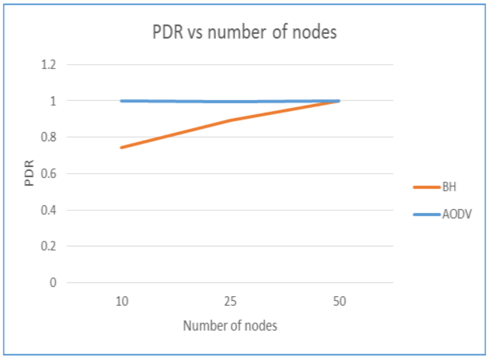


Fig. 9. PDR vs no of nodes

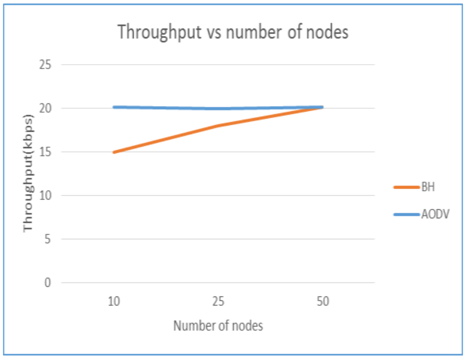


Fig. 10. Throughput vs no of nodes

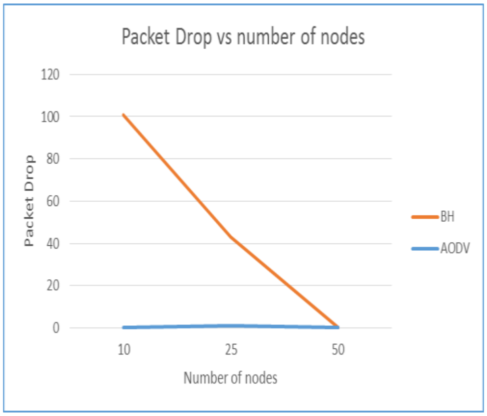


Fig. 11. Packet Drop vs no of nodes

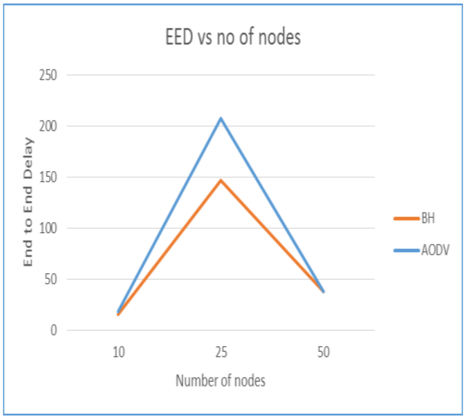


Fig.12. EED vs no of nodes

B) Performance analysis with increasing network sizes

The plots are shown in Fig. 9-12 for comparison. The comparison of performance metrics of networks with and without Black Holes. The size of the network is varied and it is observed that black hole degrades performance of smaller networks more as compared to larger networks.

5. CONCLUSION

The results of all the simulated network scenarios show that a malicious node degrades the overall performance of network. It replies to every source in its vicinity that it has the shortest path by sending the largest sequence number, thus absorbing all the data traffic. With the increase in no. of black hole nodes near source, PDR, EED and throughput of the network decreases whereas with the increase in size of network, PDR and throughput improves. These results can be utilized to propose a novel scheme that can be used to isolate MANETs from this DOS attack.

REFERENCES

[1] Babu, M. Rajesh, and G. Usha. "A Novel Honeypot Based Detection and Isolation Approach (NHBADI) To Detect and Isolate Black Hole Attacks in MANET." *Wireless Personal Communications* 90, no. 2 (2016): 831-845.

[2] Biswas, Suparna, Tanumoy Nag, and Sarmistha Neogy. "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET." In *Applications and Innovations in Mobile Computing (AIMoC), 2014*, pp. 157-164. IEEE, 2014.

[3] Chaubey, Nirbhay, Akshai Aggarwal, Savita Gandhi, and Keyurbhai A. Jani. "Performance analysis of TSDRP and AODV routing protocol under black hole attacks in manets by varying network size." In *Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on*, pp. 320-324. IEEE, 2015..

[4] Tan, Seryvuth, and Keecheon Kim. "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs." In *ICT Convergence (ICTC), 2013 International Conference on*, pp. 1027-1032. IEEE, 2013.

[5] Siddiqua, Ayesha, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm." In *Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on*, pp. 421-425. IEEE, 2015.

[6] Jain, Sakshi, and Ajay Khuteta. "Detecting and overcoming blackhole attack in mobile Adhoc Network." In *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on*, pp. 225-229. IEEE, 2015.
[7] Macker, Joseph. "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations." (1999).
[8] Shendurkar, Ankita M., and Nitin R. Chopde. "A review of black hole and worm hole attack on AODV routing protocol in MANET." *International Journal of Engineering Trends and Technology (IJETT)–Volume* 9 (2014): 394-399.
[9] Changela, Heta, and Amit Lathigara. "Algorithm to Detect and Overcome the Black Hole Attack in MANETs." *International Journal of Computer Applications* 124, no. 8 (2015).
[10] Arora, Saurabh, and Inderveer Chana. "A survey of clustering techniques for big data analysis." In *Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference-*, pp. 59-65. IEEE, 2014.
[11] Ranjan, Rakesh, Nirnemesh Kumar Singh, and Ajay Singh. "Security issues of black hole attacks in MANET." In *Computing, Communication & Automation (ICCCA), 2015 International Conference on*, pp. 452-457. IEEE, 2015..
[12] Singh, Gurnam, and Gursewak Singh. "Improvement of Network Efficiency by Preventing Black Hole Attack in Manet." *International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278* 3075.
[13] Bhole, A. T., & Patil, P. N. (2012). Study of blackhole attack in MANET. *International Journal of Engineering and Innovative Technology (IJEIT) Volume*, *2*, 99-102.
[14] Sirohi, Neeraj Kumar, and Divakar Yadav. "International Journal of Software and Web Sciences (IJSWS) www. iasir. net." (2015).
[15] Sharma, S. and Gupta, R., 2009. Simulation study of blackhole attack in the mobile ad hoc networks. *Journal of Engineering Science and Technology*, *4*(2), pp.243-250.
[16] Mandala, Satria, Abdul Hanan Abdullah, Abdul Samad Ismail, Habibollah Haron, Md Asri Ngadi, and Yahaya Coulibaly. "A review of blackhole attack in mobile adhoc network." In *Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), 2013 3rd International Conference on*, pp. 339-344. IEEE, 2013.
[17] Kumar, MK Jeya, and R. S. Rajesh. "Performance analysis of MANET routing protocols in different mobility models." *IJCSNS International Journal of Computer Science and Network Security* 9, no. 2 (2009): 22-29.
[18] Khan, Danista, and Mahzaib Jamil. "Study of detecting and overcoming black hole attacks in MANET: A review." *Wireless Systems and Networks (ISWSN), 2017 International Symposium on*. IEEE, 2017.