International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-3, January 2020

Implementation of Black hole Attack for Random Mobility for Single and Multiple Connection in MANET

Sharma Hitesh Omprakash, Margam K. Suthar

Abstract*: Mobile Ad hoc network is a temporary network. It helps to communicate two or more devices for short range. Routing Protocols are use to establish a communication in MANET. As it is a open network , it has many vulnerabilities from security point. Black hole Attack is one of the major concern in MANET. In this paper, we have implemented Black hole Attack in random mobility environment and analyse its impact on MANET using various parameters for single and multiple connection in MANET. Black hole attack disturbs one of the connection in the network while remaining connection are unaffected. During our analysis, we found that performance result of black hole attack in multiple connection network give a similar kind of output mentioned in various research paper related to gray hole attack, which will make difficult to analysis the type of attack in the network.

Keywords *: MANET; Routing Protocols; AODV; Random Mobility; Security; Black hole Attack*

I. INTRODUCTION

Mobile Ad hoc Networkis a short range network used for device to device communication. The device which are also called as a node, does not require any router in the middle of source and destination. The neighbouring node its-self acts as intermediate node and forms a small network. The communication can be single or multiple communication in the network. Routing protocol provide the shortest path between the two communicating nodes. There are different routing protocols proposed in MANET based on the type of network. This type of small networks are open to many security threats. Black hole attack is a common threat which reduce the performance of the network

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author
Sharma Hitesh Omprakash*, Student, GTU Graduate School of Engineering and Technology, Gandhinagar, India. Email: hiteshsharma720@gmail.com
Margam K. Suthar, Assistant Professor, Gujarat Technological University, Ahmedabad, India. Email: ap_1mcwt@gtu.edu.in

II. AD HOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV falls under the category of reactive routing protocols, which finds the shortest path and broadcast RREQ (Route to Request) packet when the communication between the nodes is required. As shown in the (Fig.1), Source node which is Node S, broadcast RREQ packet to find the path for the destination node which is Node D. If the neighbouring node does not have the destination node, it forwards the RREQ packet and also stores the path of the RREQ packet. When destination receives the RREQ packet, it forwards a RREP (Route to Reply) packet in the inverse direction of the same path of RREQ packet by selecting the shortest path.

Once the communication is established, the destination node start receiving the data packet from thesource node.

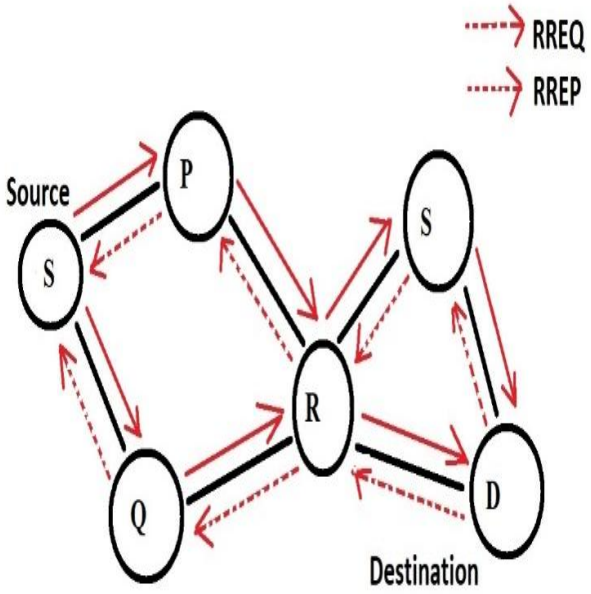

Fig. 1.AODV Protocol broadcasting RREQ and RREP

III. BLACK HOLE ATTACK

Node which does not work like a trusted node and either drop the packets or forward to the unknown node can be considered s malicious node.

Black hole node initially sends the fake RREP to the source node during the connection establishing process as a shortest node to the destination. When the source node start sending the data packet after establishing the connection via black hole node, then it does not forward the packets to the destination and start dropping all the packets.

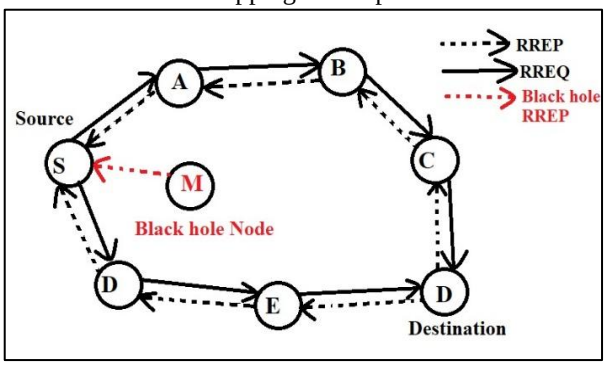

Fig. 2.Black hole Attacker node

Fig.2 shows the Black hole Attacker node in the network which sends fake RREP to the source node to establish the connection via itself and drops the packets.

IV. IMPLEMENTATION OF BLACK HOLE ATTACK

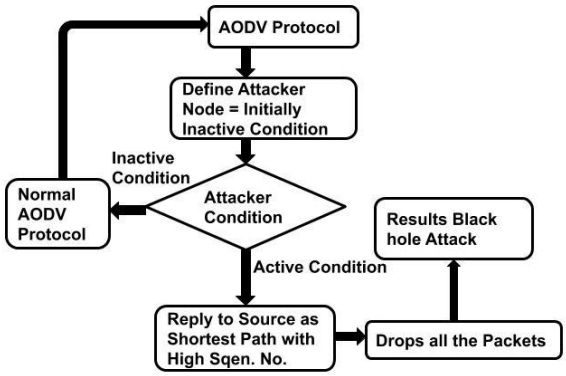

Fig. 3.Flow of implementation of black hole attack

We have made change in the AODV Routing protocol as per the characteristics of black hole attack in the Network Simulator 2.35 as the shown in the (Fig.3)

V. SIMULATION DETAILS

Table- I: Simulation Details of the Network

Simulation Parametres	Value
Simulator Tool	Network Simulator 2.35
Routing Protocol	AODV
Network Area	800 x 800 meters
Mobility Model	Random Mobility
MAC Type	MAC/802_11
Packet Size	512 bytes
Traffic Agent	UDP
Traffic Application	CBR
Speed	1 m/sec to 100 m/sec
Simulation Time	100 seconds

The Operating System which we have used is Ubuntu 16.04. We have used Network Simulator 2.35 for the simulation. For random mobility scenario , where the path of are completely unknown and the move randomly in the network area of 800m x 800m , when done 10 times simulation of each set of node and taken the average result of them. This method provide us a real like network environment. Here, we have taken three network scenarios **(1)** Multiple Connection of source and destination for AODV without black hole attack **(2)** single connection with black hole attack and **(3)** multiple connection with black hole attack.

Note: In the Graph, **AODV** denote for network performance of without attack AODV routing protocol ; **BH Attack Single Connection** denotes for Black hole Attack in the network with single source and destination; and **BH Attack Multiple Connection** denotes for Black hole Attack in the network with more than one (multiple) source and destination.

VI. RESULTS

A. Throughput is calculated by the number of bytes which are being received at the destination node from the source node per second. (Fig.3) shows the throughput of the network during without attack with multiple connection of source and destination and also when black hole attack is performed on the same network for single and multiple connection.

B. Packet Delivery Ratiois calculated by the ratio of the total number of packets sent by the source node to the total number of packets received by the destination node. (Fig.4) shows the comparison of packet delivery ratio of the three different network.

C. Packet Dropping Ratio is the ratio of total number of packets not received by the destination which are sent by source node. (Fig.5) shows the comparison of packet dropping ratio of the three different network.

D. Routing Overhead is measured by number of packets required for the communication in the network. (Fig.6) shows the routing overhead comparison of the three network. As the number of connection increases, then the routing overhead also increases.

In random mobility scenario, the nodes are continuously in motion with non-uniform speed so their connection with the neighbouring node keep on forming and disconnecting. This results in more number of RREQ and RREP packets to be broadcasted in the network for connection between source and destination which results in high routing overhead.

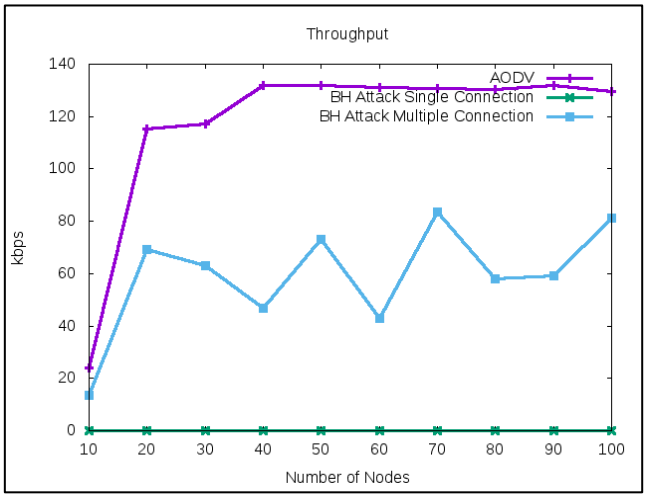

Fig. 4.Throughput

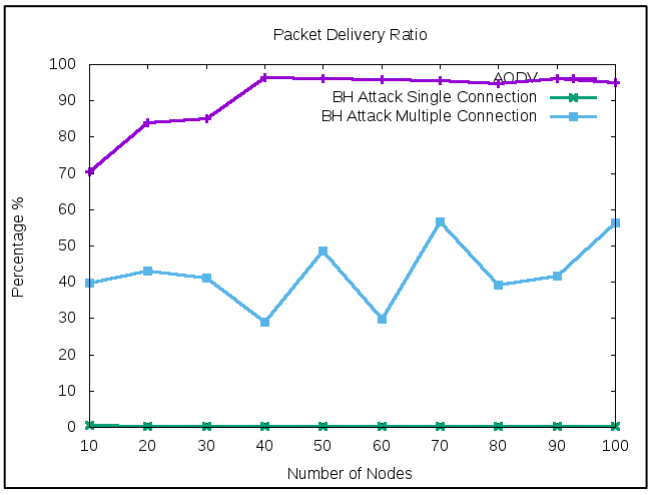

Fig. 5.Packet Delivery Ratio

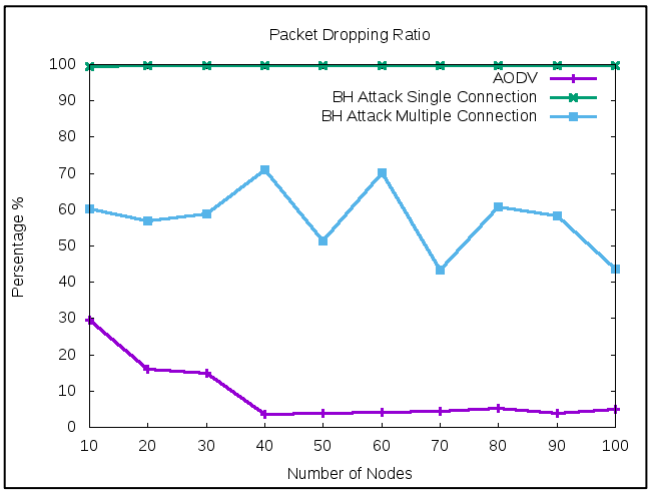

Fig. 6.Packet Dropping Ratio

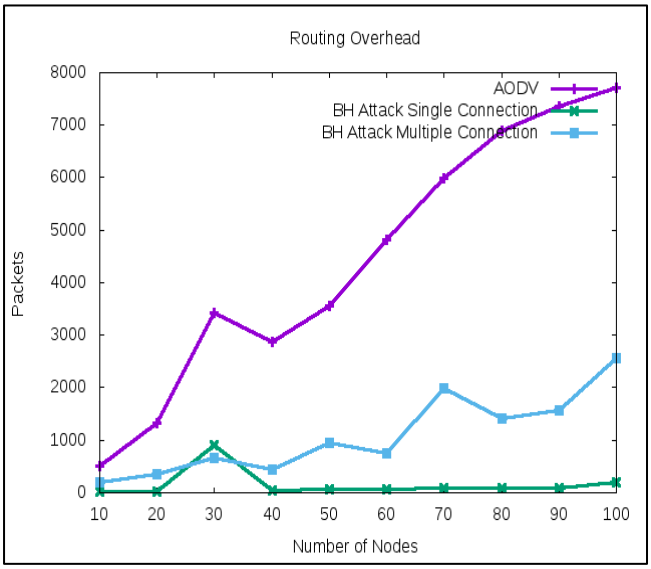

Fig. 7.Routing Overhead

VII. CONCLUSION

Parameters	AODV without Attack	Black hole Attack (Single Connection in the Network)	Black hole Attack (Multiple Connection in the Network)
Throughput	High	Low	Medium
Packet Delivery Ratio	High	Low	Medium
Packet Dropping Ratio	Low	High	Medium
Routing Overhead	High	Low	Low

AODV Routing Protocols have better performance for random mobility scenario. When black hole attack is done on the same network for a single connection in the network, it drops all the packets received from the source node which results in high packet dropping ratio and low packet delivery ratio and low throughput. Black hole attack in a network with multiple connection results in medium packet dropping ratio and packet delivery ratio. The network does not collapse in this condition but it decrease the performance of the network. When we look at the performance of black hole attack in a network with multiple connection and gray hole attack (as per the study[5] [6]), it become difficult to recognize that which attack is performed in the network. This is a serious security challenge which is needed to be solved.

REFERENCES

1. Ndajah, Peter , Matine, Abdoul Ousmane, Hounkonnou, Mahouton Norbert , " Black Hole Attack Prevention in Wireless Peer-to-Peer Networks: A New Strategy " , International Journal of Wireless Information Networks , 2019
2. Natarajan, K. , Mahadevan, G. , " Mobility based performance analysis of MANET routing protocols " , International Journal of Computer Applications , 2017
3. Khan, D. , & Jamil, M. , " Study of detecting and overcoming black hole attacks in MANET: A review " , International Symposium on Wireless Systems and Networks , 2017
4. Sachin Lalar , Arun Kumar Yadav , " Comparative Study of Routing Protocols in MANET " , ORIENTAL JOURNAL OF COMPUTER SCIENCE & TECHNOLOGY , 2017.
5. Patil, S. U. , "Gray hole attack detection in MANETs", 2nd International Conference for Convergence in Technology, I2CT, January, 2017.
6. Sharma, Rupali, "Gray-hole Attack in Mobile Ad-hoc Networks : A Survey", International Journal of Computer Science and Information Technologies, 2016.
7. Rupali Sharma , " Gray-hole Attack in Mobile Ad-hoc Networks : A Survey "", International Journal of Computer Science and Information Technologies, Vol. 7 (3), 1457-1460 , 2016.

AUTHORS PROFILE

Sharma Hitesh Omprakash, was born in Dahod, Gujarat, India. 17th, May, 1994. He was brought up in Godhra, Gujarat and completed his schooling from Saint Arnold's High School, Godhra. He completed his Bachelor of Engineering in Electronics & Communication Engineering from Parul Institute of Engineering and Technology, Vadodara in 2017. Currently he is pursing Master of Engineering in Mobile Communication and Network Technology at GTU School of Engineering and Technology, Gandhinagar, Gujarat, India. His research area are Mobile Ad hoc Network, Network Security and Mitigation Techniques of MANET. He has a good knowledge of Network Simulator 2.35.

Margam K. Suthar was born in Visnagar, Gujarat in 1988. He received the B.E. degree in Electronic and Communication Engineering from Hemchandracharya North Gujarat University, Patan, in 2010, M.Tech degree in Electronic and Communication at Ganpat University, Kherva - 382711.Dist.Mehsana, Gujarat, India in 2012. He has two year of teaching experience in the field of Electronic and Communication. He is currently an ASSISTANT PROFESSOR, POST-GRADUATE RESEARCH CENTER FOR MOBILE COMPUTING & WIRELESS TECHNOLOGIES at Gujarat Technological University (GTU), Visat - Gandhinagar Highway Chandkheda, Ahmedabad – 382424 – Gujarat, India. He has authored and published / presented publications in reputed International Journals and Conferences.

His research interests include Mobile Computing, Wireless Technologies, ad-hoc Network, and Congestion Control and improve TCP/IP protocol for High Speed Network & Wireless Network.