Implementation of Multiple Blackhole Attack in AODV Routing Protocol in MANET

Mohammed Motorwala
Computer Engineering Department (Cyber Security)
GTU-Graduate School of Engineering and Technology, Ahmedabad, India

Prof. Rutika Ghariya
Computer Engineering Department (Cyber Security)
GTU-Graduate School of Engineering and Technology, Ahmedabad, India

Abstract- MANET (mobile ad hoc network) is a form of self-configuring temporary local area network. MANET is a multi-hop network, which doesn't require any fixed infrastructure for wireless communication. MANET topology changes frequently due to its dynamic nature. The AODV routing protocol determines the route only if it's needed. MANETs don't have precise security methods which makes them vulnerable. Blackhole attacks reduces the network performance by disrupting the flow of data. In this paper, different blackhole attack detection algorithms are reviewed, and implementation of multiple blackhole attack is performed considering two different scenarios (a) blackhole attack in single connection (b) blackhole attack in multiple connection. The performance of network is observed and analyzed in both the scenarios with and without blackhole attack.

Keywords – MANET; AODV; Blackhole attack; NS2; Routing Protocols, RREQ, RREP, UDP, RIP, TCP.

I. INTRODUCTION

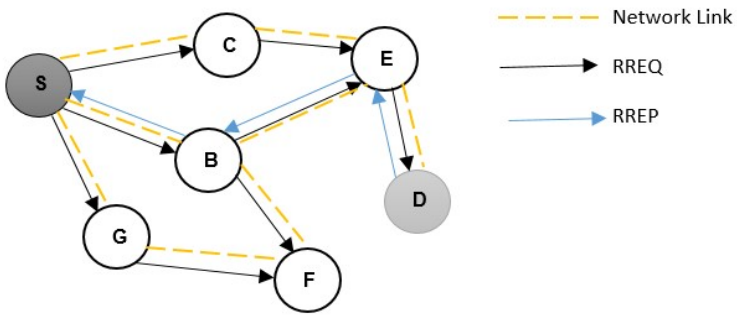
Today wireless communication has become an active field of research considering the great penetration and use of mobile devices in everyday life [1]. MANET is a multi-hop network, with no any fixed infrastructure for wireless communication. Also, at any point of time in network the nodes are allowed to move in and out of it. Maintaining security in such a volatile and dynamic environment is a difficult task and has become an important area of research [1]. The shortest path between two communicating nodes is provided by routing protocol. Blackhole attack is one of the important issues in wireless networks. In this paper, various detection techniques for blackhole attack are discussed.

II. ROUTING PROTOCOL

The networks were small in size initially so, the routing was done manually. With the increase in size of the network there was a need of automated routing management. The main task of the routing algorithm is to give the optimal/shortest path from source node to destination node. The automated routing algorithms have better accuracy but are less secure. So, to find the safest path is more important than the optimal/shortest path. Some of the routing protocols are Ad hoc On Demand Distance Vector Routing (AODV), Optimised Link State Routing (OLSR), Dynamic Source Routing (DSR) and Global State Routing (GSR). Our main focus will be on AODV Routing Protocol.

2.1 AODV Routing Protocol

It is type of reacting routing protocol which provides the shortest path from source to destination. In AODV routing protocol the source node broadcasts RREQ (Route to Request) packet to find the destination node, if the neighboring



node doesn't have the address the packet is forwarded. When it reaches to desired node, the destination node reply back with RREP (Route to Reply) packet in reverse order of same path with shortest distance. AODV routing protocol consumes less energy, reduces the routing overhead and is more adaptable to dynamic network.

Figure 1. AODV Routing Protocol

III. BLACKHOLE ATTACK

In simple words, the node which starts dropping all the packets in the network is blackhole attack node. At the time of RREP, fake RREP request is sent by malicious node (Node E) to the Source node (Node S) to specify that it has the shortest path to destination (Node D).

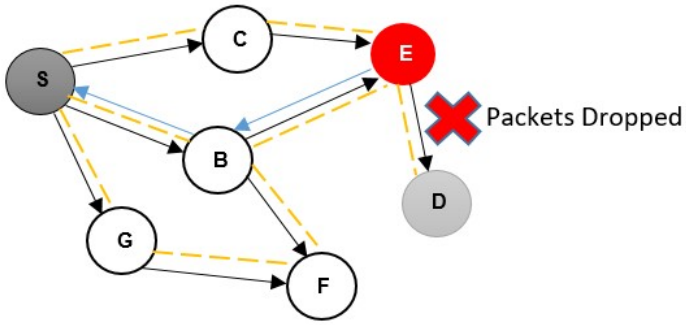


Figure 2. Blackhole Attack

Source node trusting the malicious node sends all the packets to destination via this blackhole attack node which ends in dropping all the packets in the network.

Ordinary blackhole attack node discards all the packet, passive blackhole node receives a data packet and discards it and active blackhole node receives the RREQ packets and reply with fake/false RREP packet.

IV. LITERATURE REVIEW

In [1], the security challenges in Manet are discussed. All the different types of attacks possible in Manet are reviewed. This paper deals with all the types of attacks related with the layers of Manet. The main aim of the authors was to discuss security challenges in Manet.

In [2], implementation of blackhole attack is done in random mobility. Here, two different scenarios are considered i.e. single connection and multiple connections and blackhole attack is performed in both single and multiple connection and their results are compared. Single connection means there is only path rom source to destination

whereas; in multiple connections there is more than one path. It is clear from the results that the network performs better when there is multiple connections. If in multiple connections blackhole node disrupts the flow of the network, the packets are transmitted from the different path in the network. In results, throughput and packet delivery ratio has better ratio in multiple connections.

In [3], a network backbone node is created and a concept of restricted IP is used. A request for new restricted IP is made from the source node and backbone node provides it an unused IP. If a source node wants to communicate with RIP its sends a request to backbone network. No same RIP are assigned for transmission. Source node sends request to sink node for further communication and RIP doesn't wait for long period of time. If RIP is used by the attacker and once source node receives request from sink node, the detection process starts if request is received from the source node and RIP. The node will be blocked if the dummy packet is lost which was sent by the source node.

In [4], TCP Vegas algorithm is used to detect the blackhole attack node. TCP Vegas is different from the traditional TCP. TCP Vegas deals with the delay rather than dropping the packets. It emphasize on the packet delay algorithm. TCP Vegas algorithm is used in place of typical TCP. After the simulation process, the result was not very clear. There was no improvement in performance of the network while in blackhole attack using TCP Vegas. TCP Vegas algorithm doesn't outperform the traditional TCP. Hence, there was no better result to conclude that TCP Vegas is better than TCP algorithm.

In [5], the sequence numbers are used to detect if there is any malicious node in the network. In this an algorithm takes the sequence number received form the next hope nodes in order to detect the blackhole node. As soon as, RREP with suspicious sequence number is received the detection process starts. It again broadcasts the RREQ to verify whether it was received from the blackhole node and then the path is discarded. When the source node receives the destination sequence number higher than the expected sequence number the node is considered as malicious node or blackhole attack node.

In [6], a concept of trusted node is implemented in order to detect the blackhole node. When the source node request for the destination path to transfer the packet, it looks for the trusted node. When the source node sends the RREQ packet it looks for the signed bit and checks whether that node is not blacklisted. If the sign bit for that particular node is equal to 1 and is trusted by the neighbor then the node is trusted by the source node and data is transfer is transferred from that path. If the signed bit is not equal to 1, then the path is considered as unsecure path or that node is considered as the malicious node.

V. IMPLEMENTATION

Here, implementation of multiple blackhole attack node in a network is performed. Network Simulator 2 tool is for simulation process. AODV Routing protocol is used, Network Area approx. 1500 x 1500 meters with UDP traffic Agent. Below screenshots of the model are depicted.

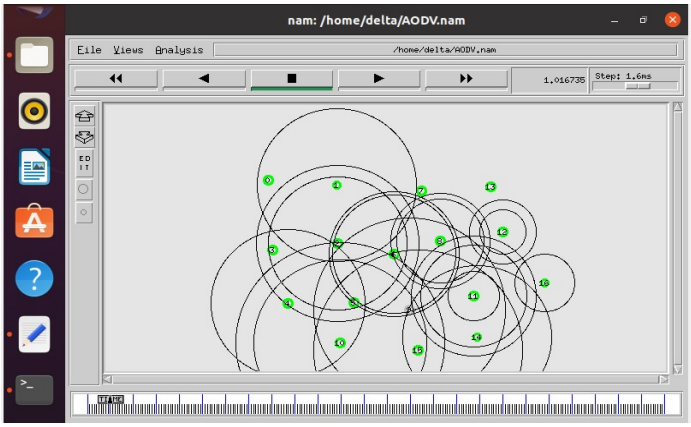


Figure 3. Simulation of network in absence of blackhole attack

Two different scenarios are considered for this implementation work (a) Single connection in absence and presence of blackhole attack, (b) Multiple connections in absence and presence of blackhole attack. The performance of network has been analyzed considering three parameters i.e. throughput, packet delivery ratio and energy consumption of nodes in network.

VI. SIMULATION DETAILS

Table-I: Simulation details of Network

Simulation Parameters	**Value**
Simulator Tool	Network Simulator 2.35
Routing Protocol	AODV
Area of Network	1500 x 1500 meters
Traffic Agent	UDP
MAC Type	MAC/802_11
Packet Size	1500

The Operating System used is Ubuntu 20.04. Network Simulator 2.35 is used for the network simulation. The paths of nodes are completely unknown and the move randomly in the network area of 1500m x 1500m, average result of 10 simulations is considered. Here, two network scenarios are examined (a) Single connection in absence and presence of blackhole attack (2) Multiple connection in absence and presence of blackhole attack. Graphs are generated with the help of xgraph in Ubuntu 20.04.
Note: Changes have been made in AODV Routing protocol in accordance to blackhole attack characteristics.

VII. RESULT

1. Throughput
The ratio of number of bytes received at destination node to source node per second. Fig. 4, 5, 10, 11 shows the throughput of network for both the scenarios in absence and presence of blackhole attack.

2. Packet Delivery Ratio
The ratio of total number of delivered packets to destination node from source node. Fig. 6, 7, 12, 13 shows the packet delivery ratio for both the scenarios in absence and presence of blackhole attack.

3. *Energy Consumption*
The percentage of energy consumed by the nodes at the time of simulation. Fig. 8, 9, 14, 15 shows the energy consumption of nodes in network for both the scenarios in absence and presence of blackhole attack.

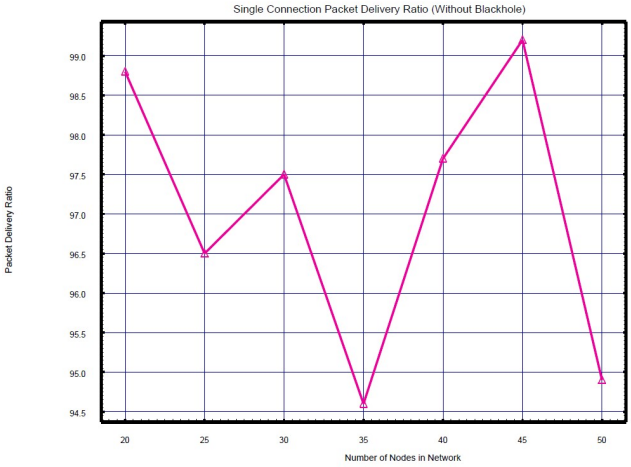


Figure 4. Single Connection Throughput

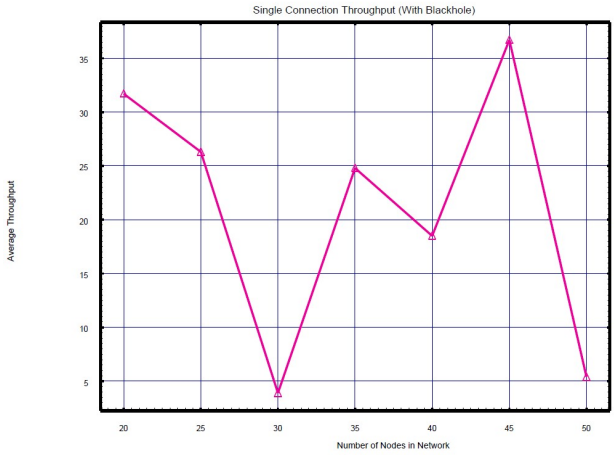


Figure 5. Single Connection Throughput (with blackhole)

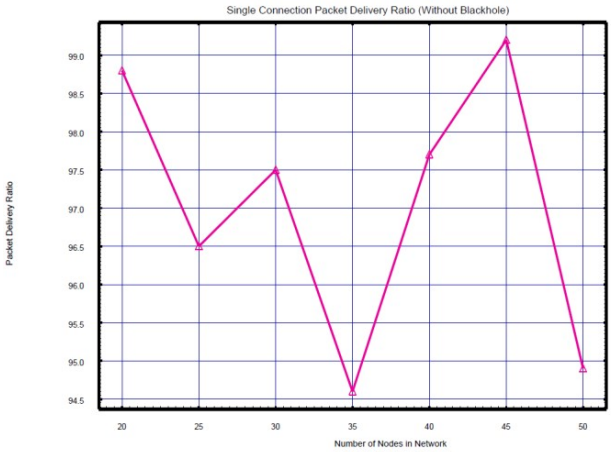


Figure 6. Single Connection packet delivery ratio

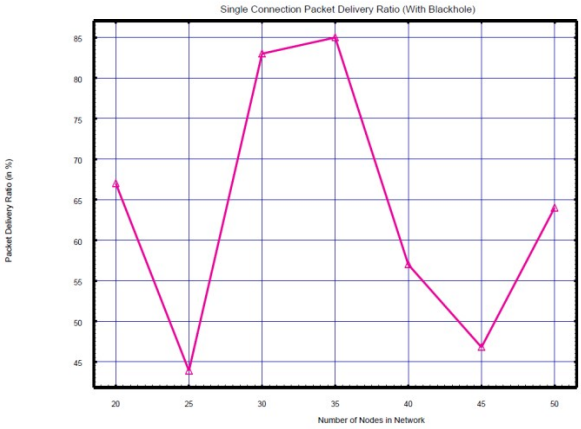


Figure 6. Single Connection packet delivery ratio (with blackhole)

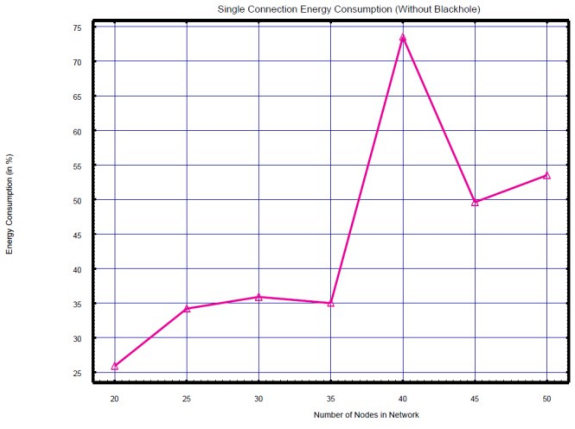


Figure 7. Single Connection Energy Consumption

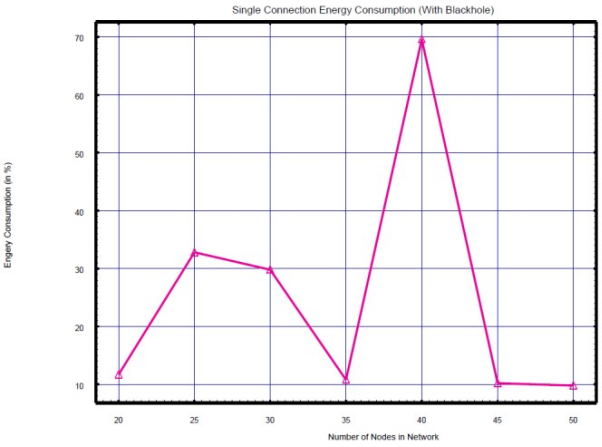


Figure 8.Single Connection Energy Consumption (with Blackhole)

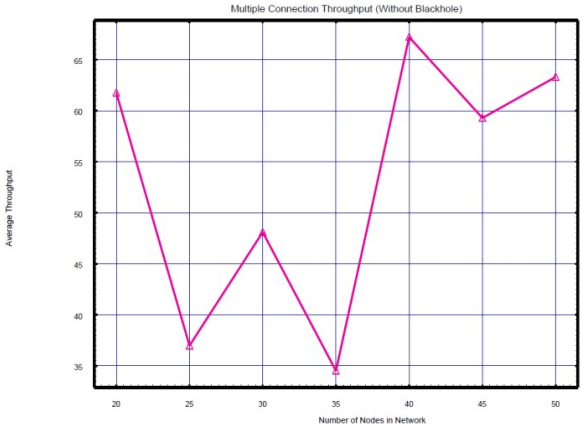


Figure 9. Multiple Connection Throughput

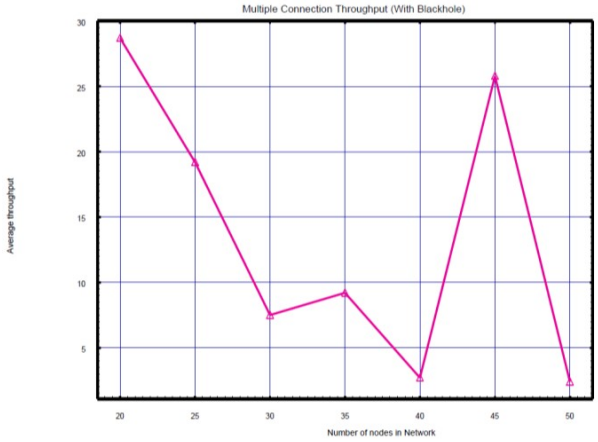


Figure 10. Multiple Connection Throughput (with blackhole)

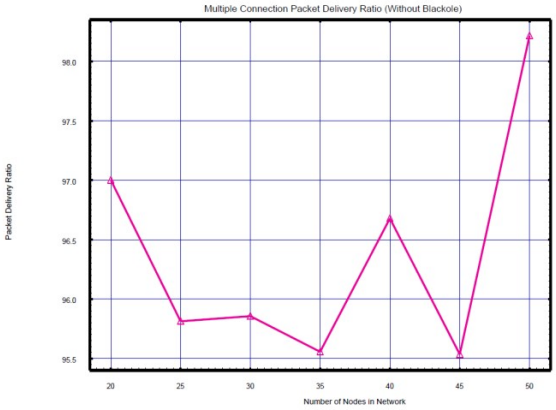


Figure 11. Multiple Connection Packet Delivery Ratio

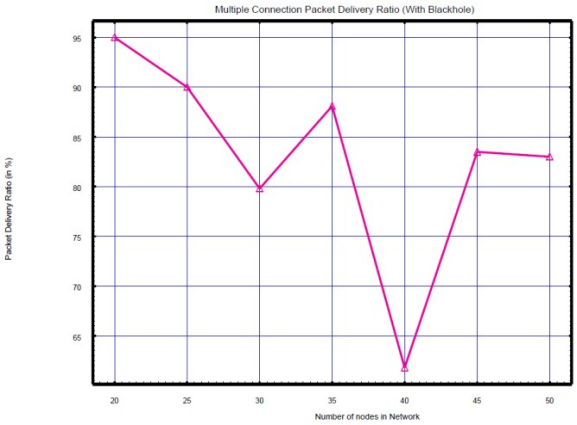


Figure 12. Multiple Connection Packet Delivery Ratio (with blackhole)

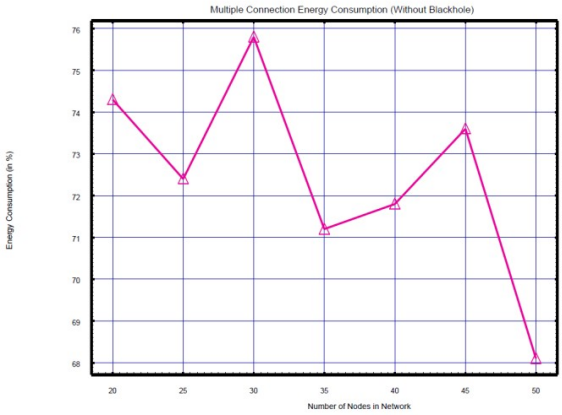


Figure 13. Multiple Connection Energy Consumption

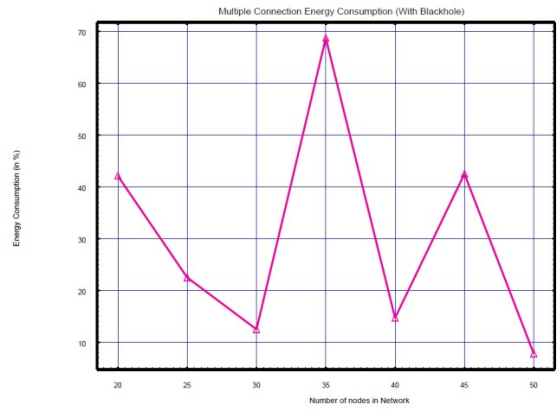


Figure 14. Multiple Connection Energy Consumption (with blackhole)

It is evident from the above figures that, when network is in blackhole attack, the performance of the network decreases. The network with no blackhole node has high throughput and high packet delivery ratio. The network with multiple blackhole nodes in both single and multiple connection has a lower performance ratio. It is transparent that the energy consumed by the nodes in absence of blackhole node is high than the energy absorbed in presence of blackhole node.

VIII. CONCLUSION

In this manet, its applications and characteristics have been discussed. The process of AODV routing protocol and Blackhole attack through related works understands the effect of malicious node behavior on AODV based MANET. A modified AODV protocol is simulated for analyzing the effects through a set of parameters. Results indicate the performance of the network in the simulated environment. There is a significant difference in the output of proposed algorithm as compared to normal AODV routing protocol. The throughput and packet delivery ratio is comparatively higher than the traditional AODV protocol. Manet is emerging technology nowadays, but also one of the major security concerned. There is a need of standard algorithm to secure the Manet from threats and attacks such as blackhole attack. To secure MANET and detecting blackhole attack with some other different attacks must be the future of wireless networks.

REFERENCES

[1] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. Altamimi, "Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs," *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 2019.

[2] Sharma Hitesh Omprakash, Margam K. Suthar, "Implementation of Black hole Attack for Random Mobility for Single and Multiple Connection in MANET", *International Journal of Innovative Technology and Exploring Engineering Regular Issue, vol.9,no. 3, pp.3299-3302, 2020.*

[3] Ashwini V. Jatti and V.J.K. Kishor Sonti, "Blackhole Attack Detection And Prevention Mechanism Using Ns2 Simulation", *International Journal Of Scientific & Technology Research, IJSTR,* 2019.

[4] Vedant sharma, Tanu shree, Renu, "An adaptive approach for Detecting Blackhole using TCP Analysis in MANETs*", International Conference on Data, Engineering and Applications, IDEA,* 2020.

[5] Sijan Shrestha, Ranjai Baidya, Bivek Giri, Dr. Anup Thapa, "Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol", *International Electrical Engineering Congress ,iEECON,* 2020

[6] Peter Ndajah, Abdoul Ousmane Matine, Mahouton Norbert Hounkonnou, "Black Hole Attack Prevention in Wireless Peer-to-Peer Networks: A New Strategy", *International Journal of Wireless Information Networks*, vol. 26, no. 1, pp. 48-60, 2018

[7] Ashok Koujalagi, "Considerable Detection of Black Hole Attack and Analyzing its Performance on AODV Routing Protocol in MANET (Mobile Ad Hoc Network)", *American Journal of Computer Science and Information Technology*, vol. 06, no. 02, 2018.

[8] Houda Moudnia, Mohamed Er-rouidib, Hicham Mouncifc, Benachir-El Hadadia, "Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET," *Procedia Computer Science, vol. 151, pp. 1176-1181,* 2019.