RESEARCH ARTICLE OPEN ACCESS

An Improved MANET Protocol with Enhanced Throughput to Prevent Black Hole Attack

Sakshi Jindal, Prof. Jyotsna Sengupta
Department of Computer Science
Punjabi University, Patiala
Punjab – India

ABSTRACT

Security in MANET is an important concern that is needed to be researched through. Due to security vulnerabilities in the routing protocol currently, these networks are unprotected to various routing attacks. One of the major attacks on MANET is black hole attack which is a Denial-of-Service attack. Due to its nature, the attack makes the source node send all the data packets to a Black-hole node that ends up dropping all the packets. In this particular paper, AODV and OLSR routing protocols under Black hole attack are investigated using NS-3 simulator. After studying the resulting graphs of these protocols, the effect of black hole attack on MANET using these protocols is investigated. The simulation results for both the protocols are compared and drawbacks are found out. Then, the work is done on the more vulnerable protocol to this attack i.e. AODV and a new improved protocol i.e. IAODV protocol is proposed that overcome the drawbacks of existing protocol to some extent. At last, the graphs of improved protocol and the existing protocol are compared through which it was found that the throughput of IAODV has increased in comparison to AODV protocol.

***Keywords* --** *MANETs, Black Hole Attack, Routing Protocols, AODV, OLSR, Network Simulator-3 (NS-3)*

I. INTRODUCTION

A. *Mobile Ad-Hoc Network (MANET)*

Mobile Ad-Hoc Network is decentralized wireless system. In MANET, when a node wants to communicate with another node, then both the nodes must lie within the radio range to start the process of communication. The intermediate nodes within the network help in routing the packets from the source node to the destination node. This network is self-organized and self-governing. Nodes are independent to play the role of router and host at the same time. The network can be set up anywhere without any geographical restrictions. Routing protocols is one of the challenging and interesting research areas.

Security in MANET is the important concern for the basic functionality of the network. The availability of network services and integrity of the data can be achieved by assuring that the security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management and no clear defence mechanism. Wireless links make it easier for the attacker to go inside the network and get access to the ongoing communication as mobile nodes present within the range of wireless link can overhear and even participate in the network. MANET must have a secure way for transmission and communication and this is a quite challenging and vital issue as threats of attack on the Mobile Network are increasing.

B. *Black Hole Attack*

In the black hole attack, the malicious node produces itself as a node for routing data to the destination node. When source node send route request, the malicious node receive it and send response to source node that it has created the shortest path. The malicious node create fake route for destination node. When the malicious node receives data sent by source node, it will drop the data packets, retrieve information from the data packet and modify it. And the data packet never reaches to the destination.

In Fig. 1, node S sends request to nodes 2 and 4 to find out the path to node D and request is shown by blue arrows. As node 4 is malicious node it produces itself as a node for routing to the destination node and send fake reply to node S which is shown by red arrow. Actual reply by Node D is shown by yellow arrows. Fake reply reaches earlier than actual reply to Node S due to which node S sends data packets to node 4 which will never reach to node D as desired.

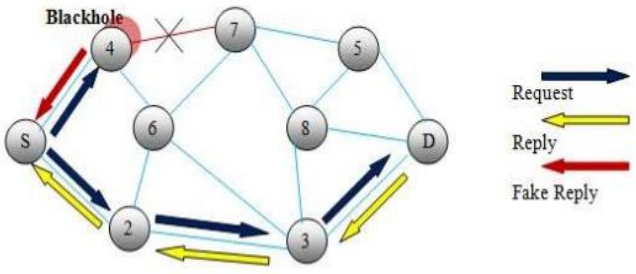

Fig. 1 Black Hole Attack

C. *Routing Protocols*

Routing protocol is classified into three approaches: reactive routing protocol, Proactive routing protocol and hybrid routing protocol.

1) ***Reactive Routing Protocols:*** Reactive protocols are also known as source initiated protocols. These protocols form the routes as and when required. When a node wants to send data to some other node, this protocol first initiates route discovery process to find out the path to the destination node. This path remains applicable till the destination is accessible or the route is not required any more.

2) ***Proactive Routing Protocols:*** Proactive protocols also known as table driven protocols maintain up-to-date and reliable routing information about all the nodes in an ad-hoc network. In this protocol, each node builds its out routing table which can be used to find out the path to the destination. Whenever there is any variation in the network topology, the routing tables of the entire network are updated.

3) ***Hybrid Protocols:*** Hybrid protocols combine the features of both the reactive and proactive routing protocols. Nodes belonging to a particular geographical region are considered to be in the same zone and are proactive in nature. Whereas the communication between the nodes located in different zones is done reactively.

D. *Ad-hoc On Demand Vector (AODV) Routing Protocol*

AODV is a reactive routing protocol that is adapted to work in a mobile environment. AODV discovers and maintain route to destination only when node wants to send packets to the destination. Sequence numbers ensure the freshness of route between the two nodes. This routing protocol uses control messages such as routing request (RREQ), routing reply (RREP), route error (RERR), HELLO message.

1) Routing Request: Whenever a source node wants to communicate with another node for which it has no routing information, Route Discovery process is initiated by broadcasting a Route Request (RREQ) packet to its neighbours. RREQ message contains the following fields:

Source Address
Request ID
Source Sequence No.
Destination Address
Destination Sequence No.
Hop Count

***2)* Routing Reply:** If the node that receives the RREQ is the destination node or has valid route to the destination then it will send RREP message to the source node. RREP message contains the following fields:

Source Address	Destination Address	Destination Sequence No.	Hop Count	Life-Time

3) Route Error: All nodes in the network have their own neighbourhood. When a node in an active route gets lost, a route error (RERR) message is generated to notify nodes on both sides of the link that the link is lost.

4) Hello Message: Each node can get to know its own neighbourhood by local broadcasting HELLO messages. Although AODV is reactive protocol it uses periodic HELLO messages to inform the neighbours that the link is still alive. HELLO messages will never be forwarded because they are broadcasted with TTL=1. When a node receives this message, it will refresh the corresponding lifetime of the neighbour information in the routing table.

E. *Optimized Link State Routing (OLSR) Protocol*

OLSR is a table- driven proactive routing protocol. This protocol is an optimization over the classical link state algorithm tailored to the requirements of a mobile wireless LAN. It is based on multi –point relays (MPRs) technique to reach all the nodes in the network with a limited number of broadcasts. This technique substantially reduces the message overhead as compared to classical flooding mechanism, where every node forwards each message when it receives first copy of the message. In this protocol, link sate information is generated only by nodes selected as MPRs. OLSR provides optimal routes in terms of number of hops. The network topology information is maintained by periodically exchanging link state information. OLSR used three types of control messages i.e. HELLO, Topology information (TC) and Multiple Interface Declaration (MID).

1) Hello Message: HELLO message is send periodically to all the neighbours of a node. This message contains information about all the neighbouring nodes, the nodes that are chosen as MPRs and a list of neighbours whose bidirectional links have not yet been confirmed. Upon receiving the HELLO message, the node should update the neighbour information corresponding to the sender node address.

2) Topology Information (TC): Information about the network can be extracted from the topology control packets. These packets contain information about the MPRSelector set of node that are broadcasted in the network, both periodically and when any changes are detected in the MPRSelector set. These packets are flooded in the network using MPR mechanism. Every node in the network receives TC packet, using which nodes build a topology table.

3) Multiple Interface Declaration (MID): Each node in the network maintains interface information about other nodes in the network. This information is extracted from MID message that is broadcasted by the nodes with multiple interfaces participating in MANETs. This interface information is used for routing table calculations. A node which has only a single interface address participating in MANET must not generate MID message. Also, a node with more interfaces but only one interface is participating in MANET and running OLSR, must not generate MID message. MID messages are broadcasted and retransmitted by the MPRs to spread the message in the entire network.

II. PROPOSED ALGORITHM FOR IMPROVED AODV (IAODV) ROUTING PROTOCOL

1. If route to destination is available in routing table of source node, it will directly send the message to destination node.
2. If route not available, it will locally broadcast the route request packet.
3. Checking for the destination node,
   i. If destination node then destination node will send route reply (RREP) packet to the source node.
   ii. Else if malicious node then malicious node will drop the packet and send fake RREP packet to source node.
   iii. Else go to step 2.
4. If RREP received by source node,
   i. Is sent by destination node, establish main route from source to destination and send data.
   ii. Is fake, establish route from source to destination but data is dropped at malicious node instead of sending it to destination.

III. SIMULATION RESULTS

A. Simulation Implementation

Implementation of black hole attack is done using ns-3 simulator. For simulations, CBR traffic, UDP/IP and IEEE 802.11b MAC are used. The simulation network consists of 36 nodes which are arranged in the form of 6*6 grid and the distance between the nodes is 100. Constant position mobility model is being used for my scenario. The size of data payload is 512 bytes. In this scenario, 36 nodes have been taken out of which nodes 0-13 and 15-35 are simple nodes, and node 14 is malicious node. Node 0 is taken as source node and node 35 is taken as sink node (destination node).

TABLE 1
SIMULATION PARAMETERS

Simulator	NS-3 (version 3.20)
Simulation Time	50 s
Number of Nodes	36
Distance between Nodes	100m
Routing Protocols	AODV, OLSR
Traffic	CBR
Mobility Model	Constant Position Mobility Model
No. of Malicious Nodes	1

Three performance parameters are taken into consideration for the evaluation of the performance of routing protocols i.e. packet drop ratio, average delay and throughput.

B. Comparison of AODV and OLSR Routing Protocols under Black Hole Attack

***1) Packet Drop Ratio*:** Packet drop ratio is the ratio between the number of packets lost and the total number of packets sent by the source node. Fig. 2 shows the packet drop ratio of AODV and OLSR under black hole attack. Simulation result shows that AODV routing protocol has higher packet drop ratio than OLSR routing protocol under black hole attack. It can be seen in the figure below there is no packet drop in OLSR up to 13 seconds. There after packets start dropping but still the packet drop remains lesser than that of AODV.

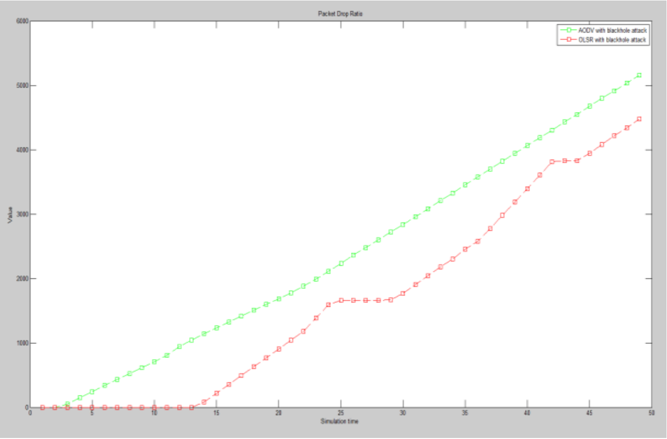

Fig. 2 Packet Drop Ratio of AODV and OLSR under Black hole attack

***2) Average Delay*:** Average delay is the time for a data packet to be transmitted over the network from source to destination. Fig. 3 shows the average delay of AODV and OLSR under black hole attack. Simulation result shows that OLSR has higher delay in comparison to AODV under black hole attack as a lot of time is consumed in developing routing tables and then applying the algorithm to find shortest and the best route from source to destination.

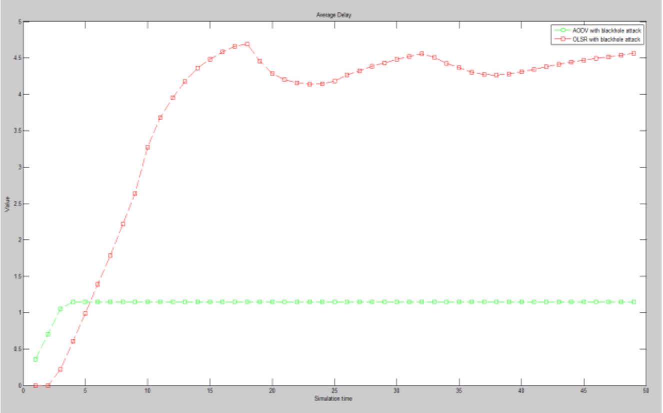

Fig. 3 Average Delay of AODV and OLSR under Black hole attack

3) ***Throughput:*** Throughput is the average rate of successful delivery of the message from source to destination over the communication channel. Fig. 4 shows throughput of AODV and OLSR under black hole attack. Simulation result shows that throughput of OLSR is higher than that of OLSR under black hole attack. In the figure below, it can be seen that the throughput of AODV become constant after 2-3 seconds of simulation and the throughput of OLSR is 0 in starting few seconds then it increased above AODV.

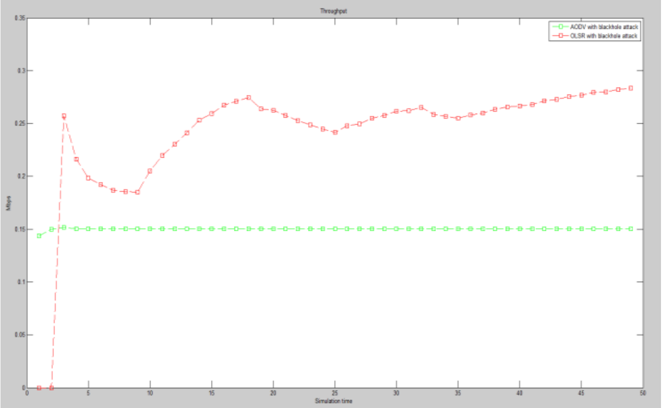

Fig. 4 Throughput of AODV and OLSR under Black hole attack

From the above comparison it has been that AODV is more vulnerable to Black hole attack than OLSR routing protocol as throughput of AODV is much lesser than OLSR. Now, AODV and IAODV protocols are compared using same performance parameters as above.

C. Comparison of AODV and IAODV Routing Protocols under Black Hole Attack

1) ***Packet Drop Ratio:*** Fig. 5 shows the packet drop ratio of AODV and IAODV under black hole attack. Simulation result shows there is very less improvement in packet drop ratio in IAODV than AODV under black hole attack. There is minute improvement in IAODV with respect to packet drop ratio in comparison to the AODV routing protocol.

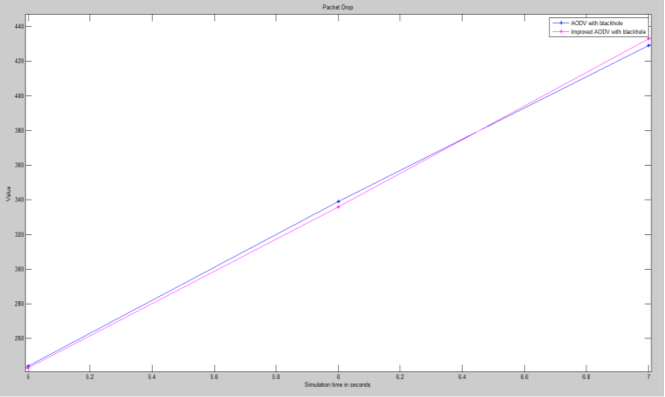

Fig. 5 Packet drop Ratio of AODV and IAODV under Black hole attack

2) ***Average Delay:*** Fig. 6 shows the delay of AODV routing protocol and IAODV routing protocol under black hole attack. Simulation result shows that the average delay in IAODV is lesser than that of AODV under black hole attack. In the figure below it can be seen that at 5 seconds of simulation time the average delay of AODV is above 1.15 and average delay of IAODV is below the value 1.15.

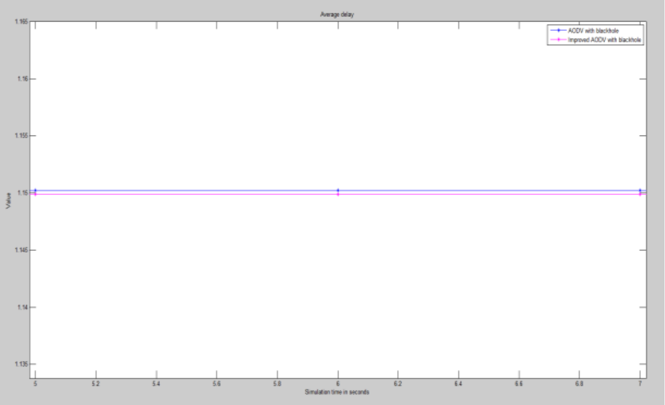

Fig. 6 Average Delay of AODV and IAODV under Black hole attack

3) ***Throughput:*** Fig. 7 shows the throughput of AODV routing protocol and IAODV routing protocol under black hole attack. Simulation result shows that throughput of IAODV is higher as compared to AODV under black hole attack. In the figure below, it can be seen that there is great improvement in IAODV routing protocol in terms of throughput than AODV protocol under black hole attack.

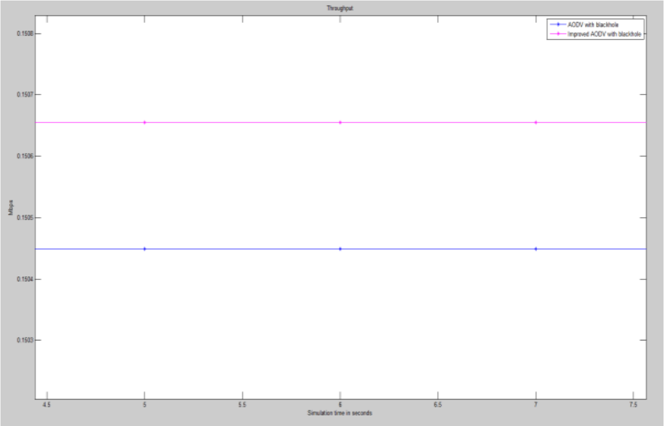

Fig. 7 Throughput of AODV and IAODV under Black hole attack

IV. CONCLUSION AND FUTURE WORK

Analysing the drawbacks of AODV and OLSR routing protocols, a new improved AODV protocol (IAODV) has been proposed. Using ns-3 simulator, the performance of AODV and OLSR under black hole attack is evaluated using packet drop ratio, average drop and throughput parameters. And these performance results are compared. From this comparison, it is found that packet drop ratio and throughput of AODV is lesser than that of OLSR and average delay of OLSR is much more than AODV. By seeing the drawbacks, it was decided to develop an improved protocol. IAODV (improved AODV) protocol has been proposed that overcome the drawbacks to some extent. Still, a lot of improvement is needed to be done.

Future researchers can work on other network attacks like wormhole attack, Sybil attack, DoS attack and also on black hole attack by using other routing protocols like DSR, ZRP, TORA and improving the protocols to overcome these attacks.

REFERENCES

[1] Goyal, Priyanka, Vinti Parmar, and Rahul Rishi. "Manet: vulnerabilities, challenges, attacks, application." *IJCEM International Journal of Computational Engineering & Management* 11.2011 (2011): 32-37.

[2] Agrawal, Sudhir, Sanjeev Jain, and Sanjeev Sharma. "A survey of routing attacks and security measures in mobile ad-hoc networks." *arXiv preprint arXiv:1105.5623* (2011).

[3] Singh, Manjeet, and Gaganpreet Kaur. "A surveys of attacks in MANET." *International Journal of Advanced Research in Computer Sciences and Software Engineering (IJARCSSE)* 3.6 (2013).

[4] Gurjar, A. A., and A. A. Dande. "Black hole attack in Manet's: A review study."*International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN* (2013): 2319-4413.

[5] Hashjin, Ali Akbar Arjmand, and Amir Najafi. "A Method to Cope with Black Holes' Attack in Mobile Networks and the Study of their Impact on the Basic Parameters of AODV and DSR Protocol." *Indian Journal of Science and Technology* 9.26 (2016).

[6] Sehgal, Akhilesh Kumar, Shivi Sharma, and P. G. Scholar. "To Study The Effect of Blackhole Attack on AODV, DSR and ZRP Protocols in MANET."*International Journal of Engineering Science* 4687 (2016).

[7] Singh, Er Amandeep, Er Abhinandan Bharti, and Naveen Dhillon. "Instruction Detection System for AODV Protocol in MANET."

[8] Sharma, Sheenu, and Roopam Gupta. "Simulation study of blackhole attack in the mobile ad hoc networks." *Journal of Engineering Science and Technology* 4.2 (2009): 243-250.

[9] Arora, Neeraj, and Dr NC Barwar. "Performance Analysis of DSDV, AODV and ZRP under Black hole attack." *International Journal of Engineering Research & Technology (IJERT)* 3.04 (2014).

[10] Gowrishankar, S., et al. "Scenario based Performance Analysis of AODV and OLSR in Mobile Ad hoc Networks." *Proceedings of the 24th South East Asia Regional Computer Conference*. Vol. 15. 2007.

[11] Malany, A. Boomarani, VR Sarma Dhulipala, and R. M. Chandrasekaran. "Throughput and delay comparison of MANET routing protocols." *Int. J. Open Problems Compt. Math* 2.3 (2009): 461-468.

[12] Yadav, Himani, and Rakesh Kuma. "Identification and Removal of Black Hole Attack for Secure Communication in MANETS." *International Journal of Computer Science and Telecommunications* 3.9 (2012): 60-67.

[13] Kaur, Harjeet, Varsha Sahni, and Manju Bala. "A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review." *Network* 4.3 (2013): 498-500.

[14] Gangoli, Sourabh, and Angad Singh. "Extensive Survey on Mobile Ad-Hoc Network Detection and Prevention." International Journal of Engineering Science 4877 (2016).

[15] Singh, S. K., and R. Gupta. "Performance Evaluation Of Ad-Hoc On Demand Routing Protocol (AODV) Using NS-3 Simulator."

[16] Karuturi Satish, K. Ramesh et al., "Intrusion Determent using Dempster-Shafer Theory in MANET Routing", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, no. 1, pp. 37-41, 2015.