Identification and Prevention of Black Hole Attacks on AODV Based MANETs

Prof V N Jokare, Prof V R Marathe, Prof F M Valsangkar

Department of Electronics and Telecommunication Engineering, N B Navale Sinhgad College of Engineering, Solapur, Maharashtra, India

Abstract- **Mobile Ad-hoc Networks (MANETs) allow mobile hosts to initiate communications with each other over a network without an established infrastructure or a central network authority. Because of this, MANETs have dynamic topologies because nodes can easily join or leave the network at any time. From a security design perspective, MANETs are vulnerable to various types of malicious attacks. As are result, Ad-hoc Ondemand Distance Vector (AODV), which is one of the standard MANET protocols, can be attacked by malicious nodes. A black hole attack is one type of malicious attack that can be easily employed against data routing in MANETs. A black hole node replies to route requests rapidly with the shortest path and the highest destination sequence number. The black hole node does not have an active route to a specified destination associated with it and it drops all of the data packets that it receives. This project describes simulation of identification and prevention of Black hole attack on AODV protocol based on MANET. The simulation is carried out with NS-2.35. Three network scenarios are simulated and the performance parameters like average delay, average throughput, packet drop rate and packet delivery rate are analyzed and compared By the simulation it has been evaluated that in flooding attack the routing overhead is more as compared to the black hole attack. This show that the flooding attack can also make system more vulnerable as this causes more consumption of bandwidth, unnecessary battery utilization of devices, clogs the network. The packet delivery ratio in scenario when black node attacked is less and in flooded situation it is greater than black hole attack which shows that more packets are correctly received by the destination in flooding attack as compared to black hole attack Throughput is maximum with detected and prevented black hole attack scenario.**

Keywords **– Mobile Ad-hoc Network (MANET); Ad-hoc On demand Distance Vector (AODV); Black Hole attack**

I. INTRODUCTION

Mobile Ad-hoc Network is a collection of the mobile nodes that is formed without the support of any existing network infrastructure. The MANET is self configurable network, in which nodes connect and disconnect from the other nodes in the network automatically at any point of time. The characteristics of the MANETs are flexibility, distributed operation, addressing mobility, node to node connectivity, etc. Routing of the data in the MANETs are done on the basis of the node discovery and then transmission i.e. the node receive the request message and forwards it to neighboring node in the path for the further transmission so that it can be reached to the particular destination and with help of route reply message the communication takes place. Each node work as a relay agent to route the data traffic. As MANET is dynamic in nature so it is accessible to all the users it may be a legitimate user or the malicious node which reproduce the data or attack in the network. For the connection between the nodes the routing protocols are required .In MANET these are such as AODV (Ad-hoc On Demand Routing protocol), OLSR (Optimized Link State Routing), DSDV (Destination-Sequenced Distance-Vector) etc.

MANET suffer from security attacks because of its features like open medium, dynamic change in topology, lack of central authority for the management and monitoring, distributed operation , lack of infrastructure. So MANET is susceptible to various attacks. In black hole attack, a malicious node uses its routing protocol to advertise itself for having the shortest path to the destination node it wants to intercept. The malicious node advertises availability of fresh routes to the other nodes irrespective of checking its routing table. In this way attacker node indicate the route availability as reply to the route request messages and thus capture the data packet and retain it.

In this project the black hole attack is simulated using the Network Simulator NS2.35. The black node is inserted into the network and the performance is evaluated for AODV protocol. The rest of the paper is organized as follows. Proposed methodology is explained in section II. Experimental results are presented in section III. Concluding remarks are given in section IV.

II. PROPOSED ALGORITHM

2. Black Hole Attack

In black hole attack, a malicious node uses its routing protocol to advertise itself for having the shortest path to the destination node it wants to intercept. The malicious node advertises availability of fresh routes to the other nodes irrespective of checking its routing table. In this way attacker node indicate the route availability as reply to the route request messages and thus capture the data packet and retain it. In protocol which is based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node, hence a malicious and forget route is created. When this route is establish, now it’s up to the node whether to drop all the packets or forward it to the unknown address

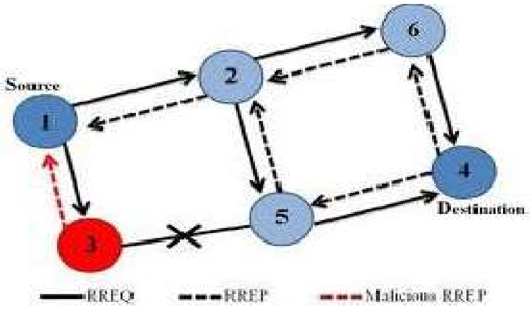


Fig1. Black Hole Attack

2.1 Simulation of Black Hole Attack

2.1.1 Black Hole Attack in AODV

The black hole attack is simulated in the AODV routing protocol is based on the reactive approach, the route between the nodes for the communication is established on demand i.e. whenever the node requires the route it broadcast a route request message in the network. In response to the route request a route reply message is forwarded by the intermediate node .This intermediate node work as a relay agent in forwarding the packet to reach to the destination and when this intermediate node work against the forwarding rules in the network which in turn causes performance degradation over the network.

When AODV protocol is used in MANET for the communication three types of control messages are used RREQ, RREP and RERR. In general when the nodes communicate they are classified as source node, which want to send the data to the other node i.e. the receiver or destination node. [1]In between the source and destination there lies the intermediate node. To discover the path in MANET all the nodes work in cooperation with the help of these control messages. The AODV protocol uses the destination sequence number for each route entry, this sequence number provide loop free connection and is the shortest path. AODV also has feature of less bandwidth utilization, low processing, less memory overhead. The source node broadcast the RREQ message in the network .This RREQ message is propagated from the source and forwarded by the other intermediate nodes. The intermediate node then further broadcast this message to its neighboring node. This process continues until the packet is received by the destination or intermediate node. The route entry in the routing table must be a valid entry; means the entry stated in table must form below a threshold value. As the RREQ packet travels through the network, the hop count is increased by one at the intermediate node. If a RREQ message with same ID is received by the node then that packet is discarded.

When intermediate node or destination receive the RREQ message and has a fresh valid route to the destination, they create RREP route reply message and send it as a reply to that RREQ message. The node also saves the entry of hops count, source address and sequence number of the destination node. Afterwards the RREP messages are forwarded by intermediate node, these nodes update their routing tables, which is ACTIVE_ROUTE_TIMEOUT constant value of the protocol. With the help of the unicasted RREP message the route is chosen by the second packet to reach to destination.

The black hole attack in AODV protocol absorbs the network load and drops the packets. When a malicious node is added in the network scenario the node act as legitimate user and participate in the network where the packets are dropped or corrupted by this node. In the black hole attack the malicious node wait for the neighbors to broadcast route request control message. As it receive the RREQ message it send a false RREP packet with the modified sequence number. After receiving the RREP message the source assumes that node is having the fresh route for the destination node. [4]The source node discards the packets from the other nodes and start forwarding the packets to the malicious node. In this way the malicious node succeeded in taking all the routes towards it. It does not allow forwarding the packet anywhere. This is how the black hole attack is introduced in the AODV protocol.

2.1.2 Simulation of Black Hole Attack in AODV

The simulation is done using Network Simulator version 2.35.in the work done the black hole behavior in wireless adhoc network that uses AODV protocol is implemented. All the routing protocols in NS are installed in the directory. The changes are done in the source file named as aodv.cc and aodv.h. The simulated work shows the functioning of AODV protocol when works normally the implementation is done for 20, 25 and 30 nodes. The flooding is also performed on the protocol. A comparative study at different parameters like end to end delay, packet delivery ratio and throughput is done when the AODV protocol function in a normal behavior and when the black hole node is introduced.

For the simulation the network scenario is designed for the small number of nodes i.e. up to 20 nodes. The UDP connection is established between the nodes. UDP is chosen as no acknowledgement overhead is there in the network. The TCP requires the connection to be established with the help of three way handshaking and for each message sent there must be acknowledgment. CBR application is attached with the connection which generates the packets at the constant bit rate. The duration of the simulation is 100 seconds.

For the simulation following three scenarios are considered

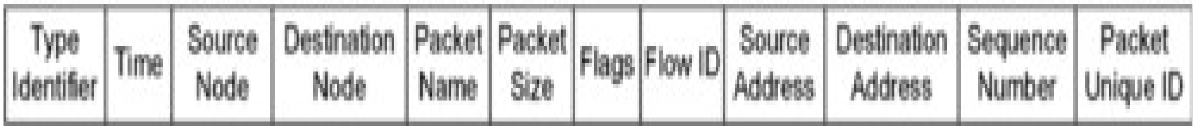
A. In the **first scenario** the functioning of AODV routing protocol is considered. The numbers of the nodes on which the simulation is done and is tested are twenty, twenty five and thirty nodes. The positions of the nodes are defined manually in the scenario.

B. In **second scenario** the black hole attack is simulated in the network on the nodes and the performance parameters are evaluated. This node drops the packet and make the network malfunction which in turn degrades the performance of the network. This black hole node also corrupts the packets which are passed on to the destination node from the source node.

C. In the **third scenario** the black hole node is detected in the network and the performance in comparison with above two scenario is better as evaluated and shown in result.

Various values are set for replicating the identified scenario like the channel type, propagation model, network interface, topography area, end of simulation time etc. The positions of all the nodes are set manually at the design time of the simulation.

As the black hole node is inserted in the code and the scenarios are executed the trace file and network animator file are generated. [3]The general format of the trace string in the trace file is shown below:



Type Identifier	Time	Source Node	Destination Node	Packet Name	Packet Size	Flags	Flow ID	Source Address	Destination Address	Sequence Number	Packet Unique ID

Fig. 2 Trace String Format

Using the network animator the simulation can be visualized. The simulation results in network animator for the 25 nodes are shown in figure 3. Here the node 1 is source node the location of the node is fixed .This node produces the flooding attack in the network. Initially the node is broadcasting the request message to all the nodes in the network.

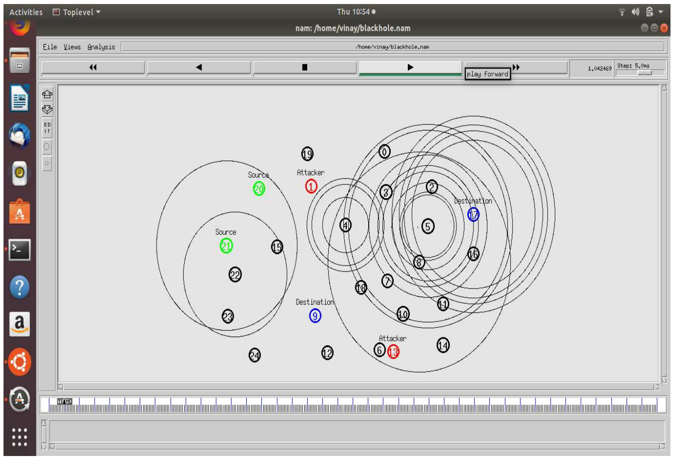


Fig. 3 25 Nodes Simulation

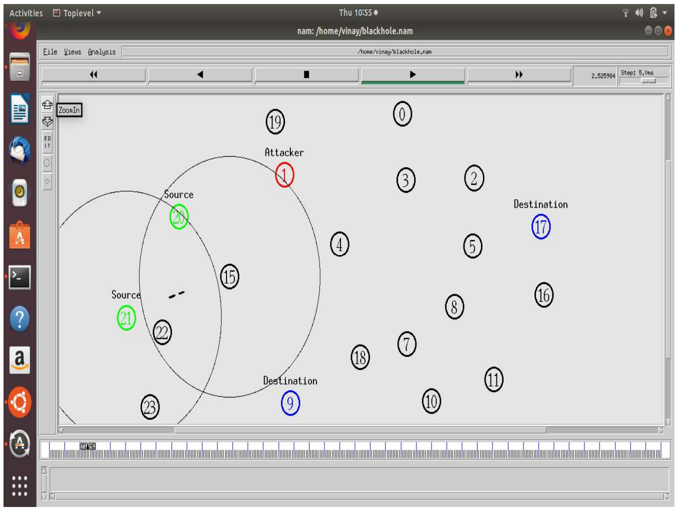


Fig. 4 Malicious Node is flooding the message

In this scenario the attacker or black hole node is inserted in the network. The figure 4 shows the flow of message from the source node 21 to the destination node 17 via intermediate node15. In this node 1 is a malicious node which inserts false packet and drops the packet which are forwarded by intermediate node. The simulation is run for 100 seconds. After 10 seconds the malicious node gets active and drops the packets in between the communication.

2.2 Performance Analysis on Various parameters

The network is simulated in NS2 for the three scenarios. With first scenario the normal functioning of the AODV protocol is studied. In second scenario the black hole attack is introduced in the network by a malicious node and in the last (third) scenario a node which behaves as a black hole is detected in the network. For the performance evaluation in the AODV protocol the simulation is performed in NS2. The work is carried out for twenty, twenty five and thirty nodes. The comparative study has been done based on the values of parameters (Packet Delivery Rate, End to end Delay and Throughput etc) which are calculated during the simulation. The characteristics of those parameters are mentioned below:

End to end Delay (in ms) it is measured as the time the packet is received minus the time the packet is sent.

Packet Delivery Rate is the rate the packets are successfully received. This is equals to the total packets successfully received on the total number of packets sent. This performance metric gives an idea of the protocol performance of in terms of packet delivery.

Throughput is rate of successful message delivery over a communication channel.

These values are evaluated and thus the performance is analyzed in all these three scenarios. The value of delay is calculated in milliseconds, when there are 20 nodes, 25 nodes and 30 nodes in the network. The figure displays as the number of nodes are increased the delay in network also increases.

Scenario I: Below tabular/graphical representation shows the comparative study for twenty, twenty five and thirty nodes for the above parameters.

Scenario II: In which the black hole node is introduced in the network Below tabular/graphical representation shows the comparative study for twenty, twenty five and thirty nodes for the above parameters.

Scenario III: The node that exhibit the malicious behavior is detected in the network. With such node the performance of network is studied and it is analyzed that the network performance is better when there is detection of black holes in the network.

III. Experiment and Result

The Black hole attack is simulated and performance of the different scenario is analyzed on factors like packet delivery rate, end to end delay and throughput. The tool used in the project is Network Simulator version 2.35.The simulations is carried out using AODV protocol, for different scenario and is compared for different number of nodes. By the simulation it has been evaluated that Packet delivery ratio for 20 nodes without black hole (WBH) is 99.80, with black hole attack it is (BH) 23.22 and with detected black hole node(DBH) is 69.65 which is improved as compared to black hole attack. Similarly evaluated for 25 node and 30 nodes.

Throughput without black node attacked for 30 node is 51.44, in black hole flooded situation it is 41.64 and in detected black hole attach which shows that more packets are correctly received by the destination in flooding attack as compared to black hole attack.

Delay in normal working of protocol is 20.04ms, in black hole scenario it is 21.26ms and in detected Black node it is 19.98ms.

Below tabular/graphical representation shows the comparative study for twenty, twenty five and thirty nodes for the above parameters .

Table -1 Experiment Result

Parameters/Nodes	20 Nodes			25 Nodes			30 Nodes		
	WBH	BH	DBH	WBH	BH	DBH	WBH	BH	DBH
Packet Delivery Ratio	99.80	23.22	69.65	99.19	21.18	67.01	99.59	80.65	99.19
Throughput	51.53	24.54	48.22	51.21	14.65	34.61	51.44	41.64	51.23
End to End Delay	69.88	9.99	13.94	36.51	20.22	32.79	20.04	21.26	19.98

REFERENCES

[1]. Thi Ngoc Diep Pham and Chai Kiat Yeo "Detecting Colluding Black Hole and Grey Hole attacks in Delay Tolerant Networks" *IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 15, NO. 5, MAY 2016*

[2]. Elhadi M. Shakshuki, *Senior Member, IEEE*, Nan Kang, and Tarek R. Sheltami, *Member, IEEE* "EAACK—A Secure Intrusion-Detection System for MANETs*" IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013*

[3]. Sandeep Dhende, Sandeep Musale, Suresh Shirbahadurkar and Anand Najan, "SAODV: Black Hole and Gray Hole Attack Detection Protocol in MANETs" *IEEE WiSPNET 2017 CONFERENCE*

[4]. Feng Li, Yali Si, Ning Lu, Zhen Chen, and Limin Shen "A Security and Efficient Routing Scheme with Misbehavior Detection in Delay-Tolerant Networks" WILEY, *HINDAWI SECURITY AND COMMUNICATION NETWORKS VOLUME 2017, ARTICLE ID 2761486 https://doi.org/10.1155/2017/2761486*

[5]. John Tobin, Christina Thorpe, Damien Magoni, Liam Murphy "An Approach to Mitigate Multiple Malicious Node Black Hole Attacks on VANETs" *HAL ID: HAL-01577471 https://hal.archives-ouvertes.fr/hal-01577471 SUBMITTED ON 3 NOV 2017*

[6]. Taskeen Zaidi, Shubhang Giri, Shivam Chaurasia, Pragya Srivastava and Rishabh Kapoor "Malicious Node Detection Through Aodv in Vanet" *INTERNATIONAL JOURNAL OF AD HOC, SENSOR & UBIQUITOUS COMPUTING (IJASUC) VOL.9, NO.2, APRIL 2018*