Detection and Prevention of Blackhole Attack in MANET Network

Varun Talati[1], Makarand Thorat[2], Kunal Yadav[3], Ranjit Mane[4]

[1]Varun Talati, Student, Dept. of Computer Engineering, Bharati Vidyapeeth College of Engineering, Maharashtra, India.
[2]Makarand Thorat, Student, Dept. of Computer Engineering, Bharati Vidyapeeth College of Engineering,Maharashtra, India.
[3]Kunal Yadav, Student, Dept. of Computer Engineering, Bharati Vidyapeeth College of Engineering, Maharashtra, India.
[4]Prof. Ranjit Mane, Professor, Dept. of Computer Engineering, Bharati Vidyapeeth College of Engineering,Maharashtra, India.

---***---

Abstract - *MANET i.e. Mobile Ad Hoc Network is a type of Ad Hoc network. As the name suggests, the Manet network is a wireless network and does not necessarily require infrastructure and architecture as prerequisites for its implementation. In this network, every node acts as a router, and data transfer for out of reach nodes is carried by the neighboring nodes. It is an open-medium, dynamic topology network. Since this is a wireless network with the features mentioned above, it lacks defense measures and network security. So it is prone to various attacks like DOS, Blackhole Attack, etc. The Manet network uses Adhoc On-Demand Distance Vector (AODV) routing protocol. AODV is gravely influenced by the blackhole attack because of its architecture and work.*

Key Words: Blackhole Attack, AODV Protocol, MANET Network, IDSAODV, IIDSAODV.

1. INTRODUCTION

An ad hoc network is formed spontaneously when devices/nodes communicate with one another spontaneously and wirelessly. They are also known as unplanned networks and are wireless. They transfer data with the help of neighboring, since every node serves as a node as well as router, eliminating the need of access points as in wireless LANs for data transfer coordination. The routing produces the routing tables and determines the routing activity of data between the nodes.

It is a decentralized Ad Hoc Network. In this network, routing of nodes is carried out by forwarding data for another node. Making the path determined for the forward nodes dynamic.

AODV is Ad hoc On-Demand Distance Vector routing protocol for Manet i.e. Mobile Ad hoc Networks and other wireless networks, it is a low power & low data rate wireless ad hoc network. It is a self-starting mechanism in wireless networks. AODV maintain a routing table at each node.

TCL is Tool Command language. It's a high-level, general-purpose, interpreted, dynamic programing language. It casts everything into the mold of command and uses different C & C++ libraries both pre-defined and user-defined linked into its main program reducing the redundancy and optimizes the program.

It predicts the behavior of an artificial or simulated computer network with n number of nodes and protocols. The user can choose the network type, protocol, and methods for the simulation. There are various libraries and other accessibilities in NS 2.3.5 & NS 3. It contains various C & C++ libraries.

2. MANET NETWORK USING AODV PROTOCOL

Ad Hoc On-Demand Distance Vector (AODV) is mainly used in Manet Networks as a routing protocols. It uses two sorts of messages, Route Request (RREQ) message and Route Reply (RREP) message, to get paths between nodes. Route Error (RERR) is employed to take care of and recover these paths. Hello message is employed to notify neighbor nodes of a few node's existences. AODV is susceptible to different types of attacks which will affect its performance under different performance metrics

Unlike infrastructure-based wireless networks, a mobile unplanned network or MANET doesn't depend upon a hard and fast infrastructure for its networking operation. MANET is a network in which a group of mobile nodes communicates with one another over wireless links. A node can communicate with other nodes that lie in its communication range. If a node wants to speak with a node that's indirectly within its communication range, it uses intermediate nodes as routers.

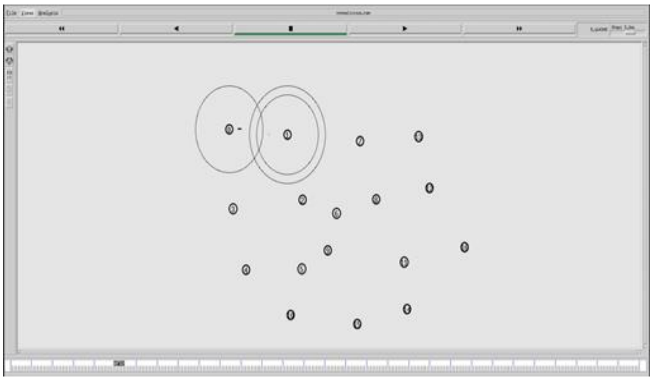


Fig -1: MANET network

Steps to create a Manet Network:

1. The channel type is set as wireless network.

2. Then we create the interface for the network by declaring Radio Propagation Model, Mac Type, Interface Queue Type, Link Layer Type, Antenna Model, Maximum Number of Packets, Number of Mobile Nodes, and Routing Protocols.

3. Then the Global Variables for the network are initialized followed by the creation of GOD.

4. Then the network channels are created, and nodes are attached to them.

5. Then the Nodes are configured and given origin coordinates.

6. Now, the traffic flow between the nodes is configured and the global time for simulation of the network is then set.

7. In this way the basic Manet Network was created.

3. SIMULATION OF BLACKHOLE ATTACK

After following the above steps, our Manet network is ready. Now we add a malicious node to simulate a Blackhole attack which will carry out packet-loss and disturb the dataflow of the network.

1. To add the malicious node, we first create a attacker node boolean variable in the aodv class
2. Creating constructor value for the attacker node
3. Initiating The attacker node in the command method
4. Giving the Attacker nodes the capabilities to drop the packet
5. Adding the code for the attacker node to attract the packets to itself which are not meant for it

Below are the screenshots of a Blackhole attack under simulation.

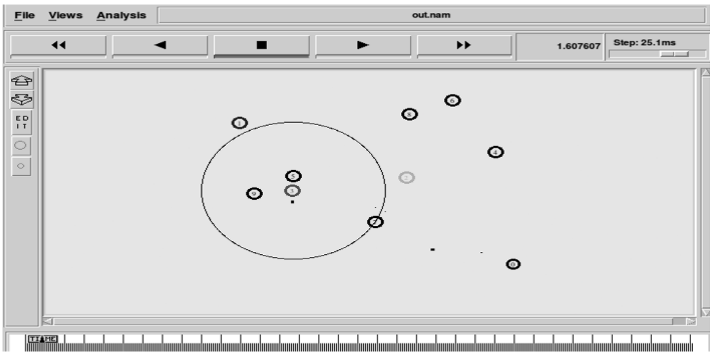


Fig -2: Simulation of Blackhole Attack

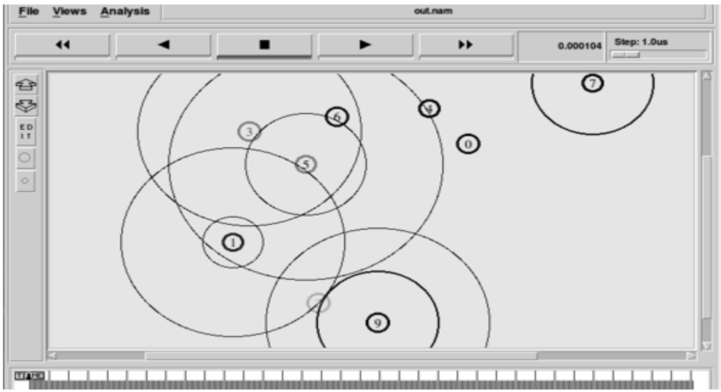


Fig -3: Simulation of Blackhole Attack

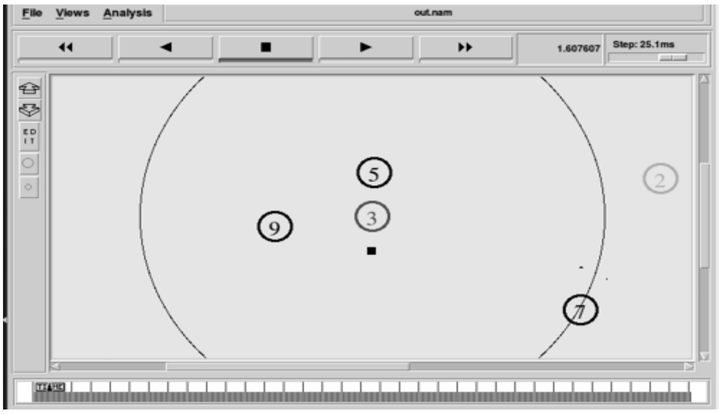


Fig -4: Simulation of Blackhole Attack

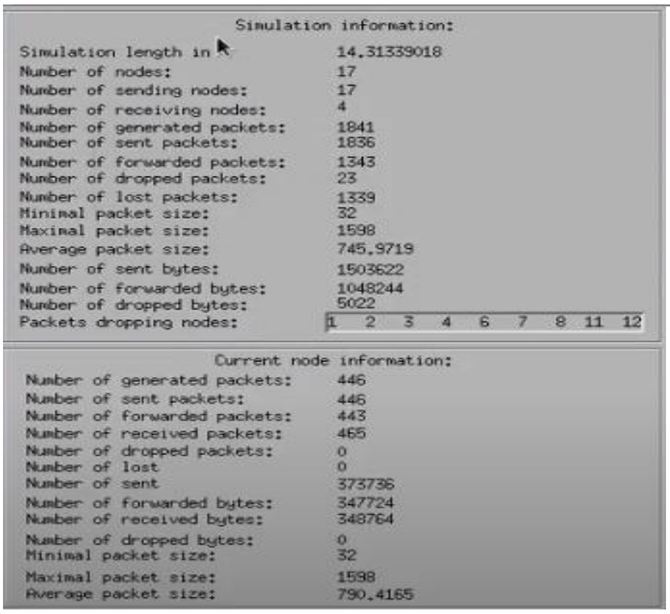
4. DETECTING THE BLACKHOLE ATTACK

Blackhole attack is a DDoS type of attack which mainly focuses on attracting the packets to itself which are not meant for that attacker node and then drop them instead of relaying them to another node/ destination.

Since the packet-loss is usual in a wireless network, it is a bit difficult to detect a Blackhole attack.

We will be using tracegraph to detect if there is a Blackhole attack being carried out in the Manet Network. Using tracegraph, we get the statistics of different parameter like number of nodes, number of sending and receiving nodes, number of generated packets, forwarded packets, sent packets, dropped packets, lost packets, etc. With the help of these statistics, it becomes possible to detect if a Blackhole attack is being carried out in the Manet network.

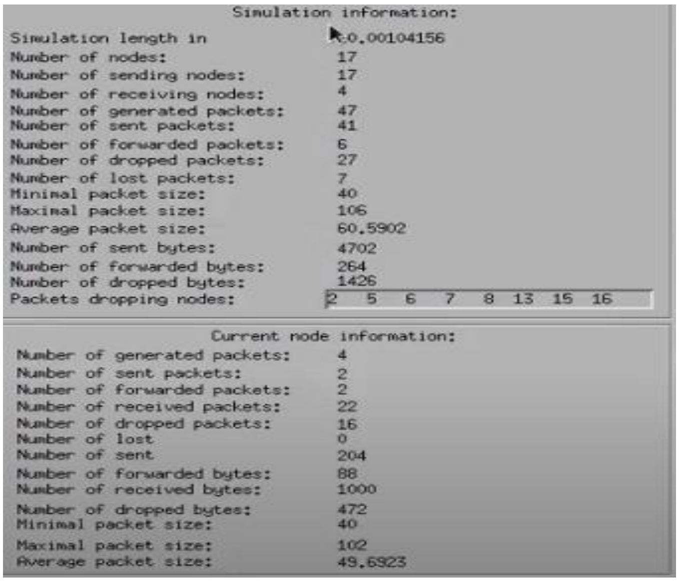
Below are the two screenshots of tracegraph results of two networks, one with Blackhole attack and the other without. It is clearly seen from the statics the ratio of the packets loss and drop in both the network is drastically changing.



```
                 Simulation information:
Simulation length in                14.31339018
Number of nodes:                    17
Number of sending nodes:            17
Number of receiving nodes:          4
Number of generated packets:        1841
Number of sent packets:             1836
Number of forwarded packets:        1343
Number of dropped packets:          23
Number of lost packets:             1339
Minimal packet size:                32
Maximal packet size:                1598
Average packet size:                745.9719
Number of sent bytes:               1503622
Number of forwarded bytes:          1048244
Number of dropped bytes:            5022
Packets dropping nodes:             1  2  3  4  6  7  8  11  12

                Current node information:
 Number of generated packets:       446
 Number of sent packets:            446
 Number of forwarded packets:       443
 Number of received packets:        465
 Number of dropped packets:         0
 Number of lost                     0
 Number of sent                     373736
 Number of forwarded bytes:         347724
 Number of received bytes:          348764
 Number of dropped bytes:           0
 Minimal packet size:               32
 Maximal packet size:               1598
 Average packet size:               790.4165
```

Fig -5: Tracegraph statistics for healthy network



```
                 Simulation information:
Simulation length in                0.00104156
Number of nodes:                    17
Number of sending nodes:            17
Number of receiving nodes:          4
Number of generated packets:        47
Number of sent packets:             41
Number of forwarded packets:        6
Number of dropped packets:          27
Number of lost packets:             7
Minimal packet size:                40
Maximal packet size:                106
Average packet size:                60.5902
Number of sent bytes:               4702
Number of forwarded bytes:          264
Number of dropped bytes:            1426
Packets dropping nodes:             2  5  6  7  8  13  15  16

                Current node information:
 Number of generated packets:       4
 Number of sent packets:            2
 Number of forwarded packets:       2
 Number of received packets:        22
 Number of dropped packets:         16
 Number of lost                     0
 Number of sent                     204
 Number of forwarded bytes:         88
 Number of received bytes:          1000
 Number of dropped bytes:           472
 Minimal packet size:               40
 Maximal packet size:               102
 Average packet size:               49.6923
```

Fig -4: Tracegraph statistics for unhealthy network

5. ADVANTAGES

1. Manet network is flexible, that is it can be created with a mobile devices anywhere.
2. Manet networks are Scalable, it is very easy to add new nodes or remove nodes from a Manet network.
3. Manet networks are cost effective.
4. AODV supports loop free operation and provides easy scalability.
5. The routes are produced on demand in AODV routing protocol and sequence numbers are used to find the latest route.
6. IIDSAODV helps to prevent the attack by checking the credibility of the RERP message.

6. DISADVANTAGES

1. Manet has many vulnerabilities like compromised/easily manipulated malicious nodes, weak physical security, and no/minimal central management. All of these make MANET network weak.
2. Because of the On-Demand route property of AODV, sometimes the shortest route is lost due to traffic.
3. AODV does not have congestion control and avoidance mechanism to balance the traffic load in the network.
4. Sometimes, because of the double route checking of the RERP message in IISDAODV, there is delay in packet delivery.

7. PREVENTION OF BLACKHOLE ATTACK

IDSAODV is Intrusion Detection System for Adhoc On-Demand Distance Vector routing protocol. It is further improved and developed to IIDSAODV which reduces the effect of Blackhole Attack.

IDSAODV ignores the first route that was established to reduce the effects of the Blackhole attack and takes the second route generated/established. Since Blackhole Attack usually modifies the first route of the data-transfer from neighboring nodes, IDSAODV reduces the effect of Blackhole attack significantly. But, in some cases, if the destination node is near than the Blackhole attacker node, the first RREP message may come from the destination node and the latter from the Attacker node. So in this type of cases, IDSAODV fails.

To overcome this, improved IDSAODV i.e. IIDSAODV is used. In IIDSAODV, when the node receives the second RREP message, it initiates a check based on broadcasted and received sequence numbers. By doing this check, it calculates the difference between broadcast messages and received and then is compared to half of Highest Possible Sequence Number (HSN). The difference should be less than or equal to half of HSN to pass for this check.

In this way, Blackhole are prevented more significantly.
RREP: Route Reply message
RSN: Received destination sequence number
BSN: Broadcasted destination sequence number
Path1: Established by first RREP message
Path2: Established by second RREP message
HSN: Highest possible sequence number (32-bit
unsigned integer value i.e., 4294967295)
Step1: Source receives first RREP message
Step2: Source S checks the freshness of the RREP message (i.e., RSN >=
BSN).
Step3: If RSN >= BSN, Source S starts the
Transmission of data to Destination D through
Path1 and set count = 1.
Step4: If Source S receives a second RREP message then
Again step 2 is repeated and S checks its freshness.
Step5: If the second RREP message is fresh (i.e., RSN >= BSN)
then the count increases 1.
Step6: Then, the Source S implicates an extra check on second
RREP i.e.

If (count > 1 && ((RSN – BSN) <= (HSN/2))), then source S switches to path2.
Step7: If the check fails, path1 is selected.

8. CONCLUSION

Hence, in this paper we saw the simulation, detection and prevention of Blackhole Attack in Manet network. The MANET network was simulated in NS 2.3 using TCL and c++ libraries. Malicious attacker nodes were created in AODV protocol's class file and were given the capabilities to carry the Blackhole Attack. The Blackhole attack was detected using Tracegraph on different parameters like packets sent, received, dropped, lost, etc. The attack was prevented using the IDSAODV and IIDSAODS protocols.

9. ACKNOWLEDGEMENT

We express our deepest gratitude to our Project guide for providing technical support, guidance, encouragement and moral support in successful completion of the project and also for giving us time to time feedback.

10. REFERENCES

1. Adwan Yasin and Mahmoud Abu Zant "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique" Computer Science Department, Arab American University, Jenin, State of Palestine

2. S. Mirza and S. Z. Bakshi, "Introduction to MANET," International Research Journal of Engineering and Technology, vol. 5, no.1, pp. 17–20, 2018

3. N. Kalia and H. Sharma, "Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol," International Journal on Computer Science and Engineering, vol. 8, no. 5, pp. 160–174, 2016

4. M. Sathya and M. Priyadharshini, "Detection and removal of black hole attack in mobile ad-hoc networks using cooperative bait detection method scheme," International Journal of Scientific & Engineering Research, vol. 7, no. 3, pp. 81–85, 2016

5. Ankita Chaturved and Sanjiv Sharma "A new technique for preventing Blackhole Attack in Mobile Adhoc Network ", International Journal of Advances in Computer Science and Technology, 3(10), October 2014