BLACK HOLE ATTACK SIMULATION IN ADHOC NETWORK

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

[1]*Makarand Thorat, Student, Dept. of Computer Engineering, Bharati Vidyapeeth College of Engineering, Maharashtra, India.*
[2]*Varun Talati, Student, Dept. of Computer Engineering, Bharati Vidyapeeeth 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 - Mobile Wireless Ad Hoc Networks (MANETs) is a simple yet versatile wireless network that can be implemented without certain prerequisites in infrastructure and architecture to support the same, where every node imbibes a router-like behavior. Information and data transfer for nodes out of range, detect neighboring nodes, through which data is transmitted. Features such as open medium, dynamic topology, lack of defensive measures, make the network vulnerable to foreign attacks affecting the integrity of its data and data transmission. To avoid such a harmful effect, the On-demand Distance Vector routing i.e. AODV routing protocol, is a simple way to do so. The AODV is gravely influenced by an infamous attack, where a malicious node sends a forged route reply as a message that is a brief and fresh route to the destination node.

Key Words: AdHoc Network, Black-Hole Attack,Manet Network, AODV protocol.

1. INTRODUCTION

An ad hoc network is one that's spontaneously formed when devices connect and communicate with one another. The term unplanned may be a Latin word that literally means "for this," implying improvised or impromptu. Unplanned networks are mostly wireless local area networks (LANs). The devices communicate with one another directly rather than counting on a base station or access points as in wireless LANs for data transfer co-ordination. Routing activity is completed by determining the route using the routing algorithm and forwarding data to other devices via this route.

A mobile ad hoc network which is decentralized. In this network, routing of nodes is done by forwarding data for another nodes. Hence the path determined for the forward nodes is determined dynamically.

2. AODV Protocol

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.

3. TCL

TCL is Tool Command language. It's a high level, general purpose, interpreted, dynamic programing language. It casts everything into the mould of a 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.

4. Network Simulator

It is a software that predicts behaviour of an artificial or simulated computer network with as many nodes and protocols. The user can choose the network type, protocol and methods of their choice for the simulation. There are various libraries and other accessibilities in NS 2.3.5 & NS 3. It contains various C & C++ libraries.

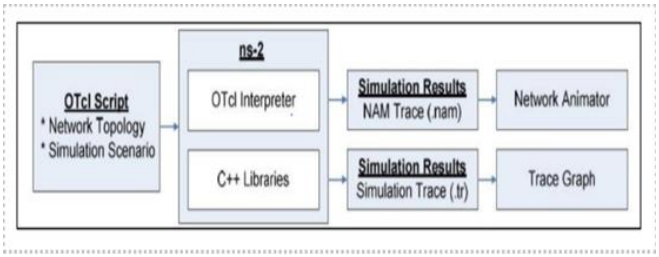
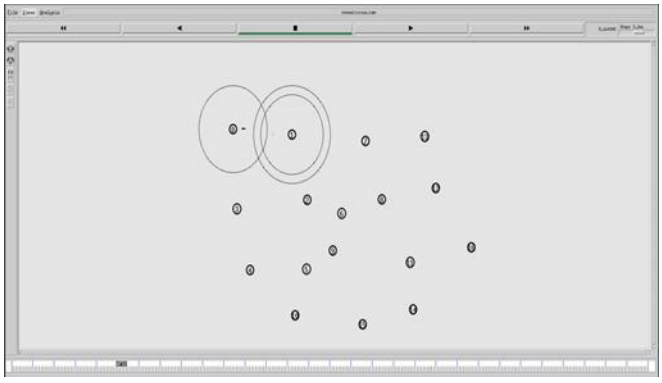


Fig. 1 Activity Diagram creation of a Manet Network

5. Manet Network using AODV Protocol

Ad Hoc On-Demand Distance Vector (AODV) is one among the foremost commonly used reactive 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 neighbour nodes a few node's existence. AODV is susceptible to differing 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 group of mobile nodes communicate 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.



Steps to create a Manet Network:

1. First, we need to setup the channel type as Wireless Channel since the network is Adhoc.
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 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.

6. Simulation of Black-Hole Attack

This simulation is done to detect a Manet Adhoc network using AODV protocol under packet drop and loss conditions also known as Black hole Attack. It is determined on the basis of various factors such as end to end peer connection, packet delivery and loss, ratio of packets sent to packets dropped and lost.

Security in MANET is an important task in preventing the harm that would be caused by malicious nodes within the network. Flooding attack is one among DoS attacks that aim to exhaust the network resources by flooding the network with tons of faux packets and messages.

The native AODV is an on-demand routing protocol, which finds the shortest possible path between nodes within the network, but it lacks a mechanism to detect and stop the Flooding attack.

There are two sorts of attacks in MANET: Passive attacks and Active attacks. In Passive attacks, the attacker nodes only gather information and data about other nodes within the network without affecting the network operations. Samples of these Passive attacks are Monitoring, Eavesdropping, and Traffic Analysis. On the other hand, in Active attacks, the attacker nodes affects the network operation by dropping, modifying, and delaying packets or by changing the route of the packets. Samples of Active attacks are Sybil attack, Wormhole attack, Spoofing attack, Black-Holes and Grey-Holes attack, and Flooding attack

7. Advantages

1. The mobile nodes can dynamically self-organize in arbitrary temporary network topology.
2. Router Free Connection to the internet without any wireless router is the main advantage of using a mobile ad hoc network. Because of this, running an ad hoc network can be more affordable than traditional network.
3. AODV does not put any overheads on the data packets as it does not uses source routing tables.
4. AODV can respond quickly to topological changes that affect the active routes because of its adaptability to dynamic networks.
5. AODV is loop free, self-starting, and scales to large number of mobile nodes.

8. Disadvantages

1. Due to no clear secure boundary, MANET is susceptible to various kinds of attacks.

2. Since mobile nodes in MANET are independent to move, join, or leave the network, Hence the mobile nodes are autonomous, it is very difficult for the nodes to avoid malicious behavior of the nodes with which they are communicating.

3. AODV have an efficient route technique. It produces routing information demand.

4. Does not support aggregate routing in immediate nodes

9. Conclusion

In this study, we simulated a black hole attack in an AODV network. For this purpose, we implemented an AODV protocol that acts as a Manet Network in NS2.35. We understood the steps required to create a Manet network and induce an attacker node in it to. We observed the working of a Manet network as well as how it is affected by black hole attack.

10. 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.

11. 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