Simulation And Analysis Of Performance Parameters For Black Hole And Flooding Attack In MANET Using AODV Protocol

Swati Jain, Dr Naveen Hemrajani, Dr. Sumit Srivastava

Abstract: As the increase of wireless networks, use of mobile phones, smart devices are gaining popularity so the adhoc network is also a uprising field. Each device in a MANET is free to move independently in any direction, linking to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router.. This paper describes the features, application, flooding attack and black hole attack in the MANET implemented on AODV protocol. The simulation work is carried out in Network Simulator (NS2.34). The performance analysis is done for 3, 5 and 10 nodes. The average delay, routing overhead, packet drop rate and packet delivery rate are calculated. By the simulation it has been evaluated that in flooding attack the routing overhead is more as compared to the black hole attack. A comparative study is also done on these parameters for all three scenarios.

Index Terms: MANET, Wireless Networks, Ad hoc Networking, Routing overhead, Packet Delivery Rate.

1. 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 i.e. the node receive the data and forwards it to neighboring node in the path for the further transmission so that it can be reached to the particular destination. 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.

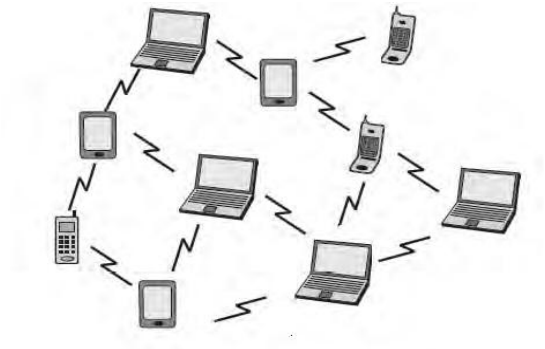

Fig:-1. Mobile Adhoc Network

1.1Characteristics of MANET

1. No Centralized Administration – Each node in the MANET has its own communication capabilities for forwarding the data traffic over the network and adjusts according the topology.

2. Flexibility- MANET enables fast organization of the ad hoc network. When a node is to be associated with the network it should have the limited wireless communication range i.e. such node which can be available nearby.

3. Peer to peer connectivity of the nodes- In MANET the nodes neighbor to each other forms a set for communication to which request response messages are flooded.

4. Resource constraints- The node may have limited energy so this may limit the functionality of the network.

5. Dynamic Network topology-A node discovers the service of a nearby node using the service discovery protocol.

6. Heterogeneous Nodes – In the MANET architecture any node can participate in forwarding thee data packets, the node can be PCs, smart phones, smart tablets, embedded systems.

- M.Tech Scholar, Department of Computer Sc. & Engineering, Suresh Gyan Vihar University, Jaipur zenswati@rediffmail.com
- Professor, Department Of Computer Sc. & Engineering, Suresh Gyan Vihar University, Jaipur naven_h@yahoo.com
- Associate Professor, Department of Computer Science & Engineering, Manipal University, Jaipur sumit.310879@gmail.com

1.2 Applications

Adhoc networks can be established anywhere where the nodes can join and leave the network at any point of time. The applications of the MANET are in Military, Emergency Services, Commercial environments etc .Using the adhoc network the communication among the soldiers, vehicles, and headquarters of military can be possible as this area do not have the proper establishment of the base station for the communication. Search and rescue, recovery from disasters like fire, flood, volcano eruption, earthquake, etc in case of emergency. In vehicular management to manage road traffic and accidents, inter-vehicle communication.

2. Ad-hoc On-demand Distance Vector Protocol

AODV protocol is designed for the mobile ad-hoc network. The algorithm works on demand i.e. the route calculation from source to destination is done only when the node desires. It maintains these active routes in the routing table for a pre-specified expiration time and uses destination sequence numbers for each route entry. It adapts quickly to dynamic link conditions. In this protocol if the source node desires to route a packet to the destination node it broadcast a RREQ (route request) packet across the network. Every node in the network receives the broadcasted RREQ packet and updates their information maintained in the routing table. The node sends route reply (RREP) message if it is a destination node or if it has a route to the destination with corresponding sequence number greater than or equal to the one contained in the RREQ. The protocol is vulnerable to routing attacks because of dynamic topology and the network is infrastructure less.

3. 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 forged 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 Black hole in the AODV Protocol - The attacker can send a fake RREP to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and the attacker can misuse or discard the traffic.

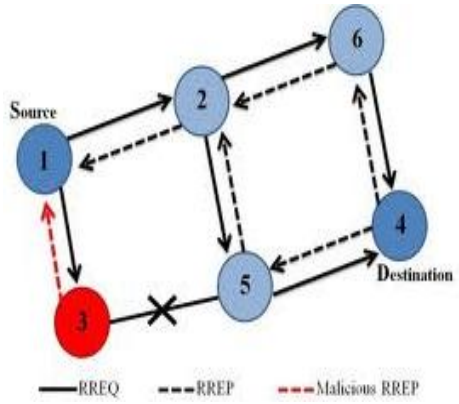

Fig. 2:- Black hole attack

4. Performance Analysis in AODV protocol

For the performance evaluation in the AODV protocol the simulation is performed in NS2. The work is carried out for three, five and ten nodes. During the simulation some parameters are defined which are stated in the table below:

Simulator Used	NS2(version 2.34)
Routing Protocol	AODV
Topography Area	500*500
Simulation Time	150ms
Maximum Bandwidth	2Mbps
Number of Mobile Nodes	10
Traffic type	Constant Bit Rate
Packet Size	1000 bytes

Table1. Simulation Parameters

A network of small size is setup that contains 3, 5 and 10 nodes. The constant bit rate (CBR) application creates packet through connection based on UDP, as it is connectionless protocol and easy to carry out the black hole attack analysis .CBR packet size chosen is 1000bytes. The simulation is carried out for 100 ms and 150ms. Positions of the nodes are defined manually in Tcl script. The values which are calculated during the simulation are Packet Delivery Rate, Average Delay, Routing overhead and Dropped packet Ratio. First of all the parameters are evaluated for the AODV protocol when it works normally. In this the routing overhead for three nodes is 0.03% of the total packet transmitted which means when network consist of small number of nodes the control packets transmitted are less as compared to the large number of nodes. The packet delivery rate is 50.90% for the three nodes which shows only these packets are correctly received in three node network scenario and with ten nodes the delivery ratio dropped to 16.12%

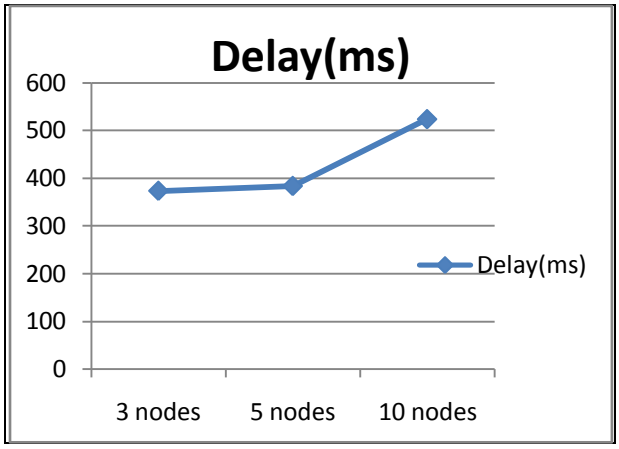

Fig3. Delay when AODV works normally

In second scenario a large number of packets are flooded into the network by a malicious node. Figure 4 shows the flow of data from a malicious node to the other node in the network. Initially the node broadcast the route request message in the network. The figure 5 shows that the node again and again forwards the request message and thus attacked on the network consuming network bandwidth, battery power of other

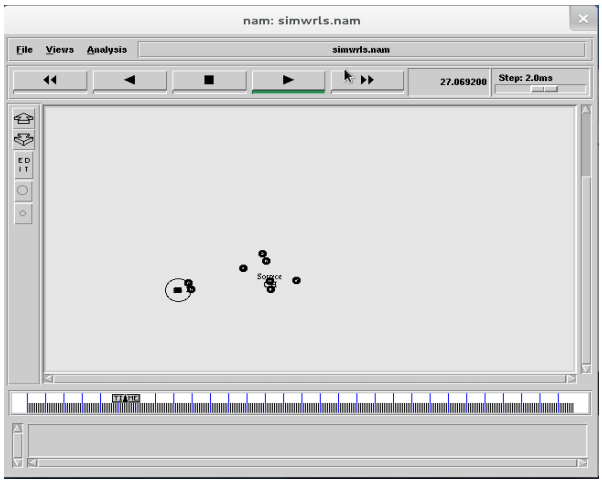

Fig. 4 Malicious node broadcast messages to nodes

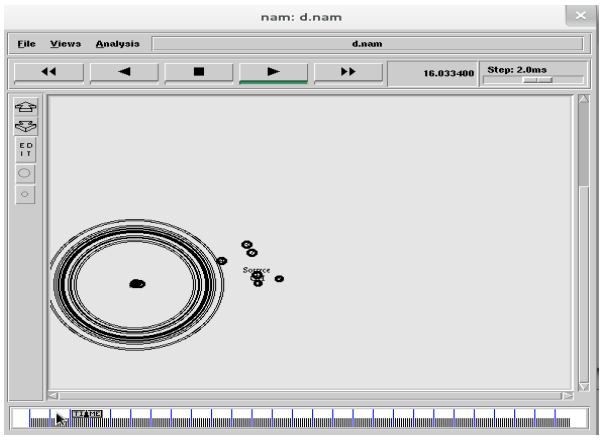

Fig5. Flooding of Packets in network

So in this case the routing overhead is also increased for the small number of nodes. For ten nodes this value becomes 30.08%, for five nodes the value is 21.87 and for three nodes it is 2.39%. The figure 6 shows the increase in overhead

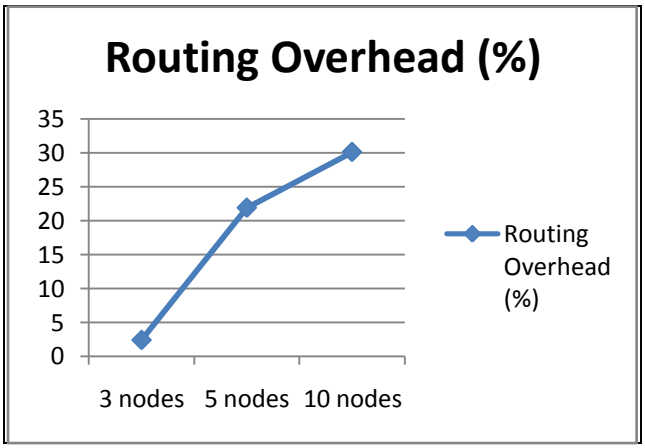

Fig.6. Routing Overhead when packets are flooded

In third scenario a black node is inserted into the network. Node 1 is source node, node 3 is destination and node 0 is the malicious node which is inserted into the network and attacks the network and degrades performance. Figure 7 shows the transfer of the packets from node 1 to node 3, in between node 2 act as intermediated node.

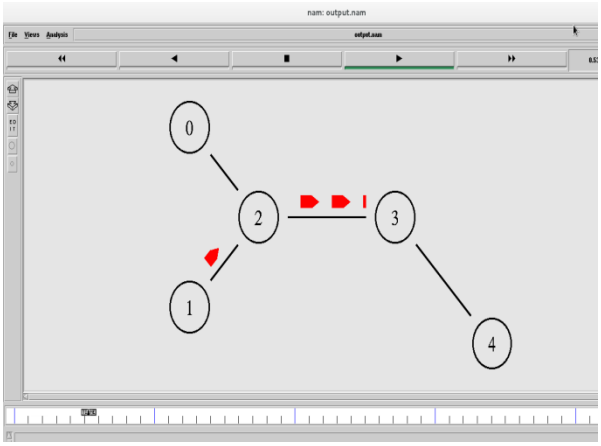

Fig7. Node1 transfer packet to node3

Initially the packets are transmitted by node at constant bit rate .The size of packets are 1000bytes. The simulation is run for 5 seconds. After 1 second the black node0 starts attacking. It senses the network and transmission of the data from node1 to node 3 via node 2, so node 0 start sending malicious packet into the network and drop the packet. Figure 8 shows the behavior of the black node.

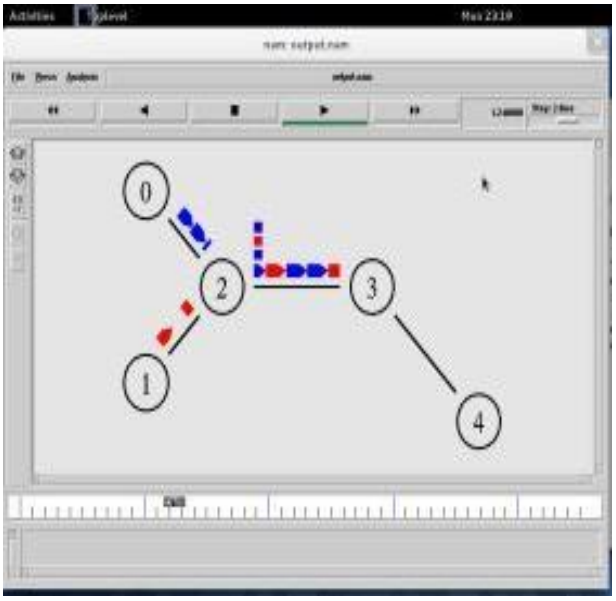

Fig 8. Black Node 0 attacking with false data packets

During the simulation various performance parameters are studied in all the three scenarios with different number of nodes. A comparative study is done for four parameters packet delivery rate, routing overhead, Delay and Dropped packet rate. By the simulation it is evaluated that in flooding scenario as more messages are flooded this increase the routing overhead as compared to the black node scenario.

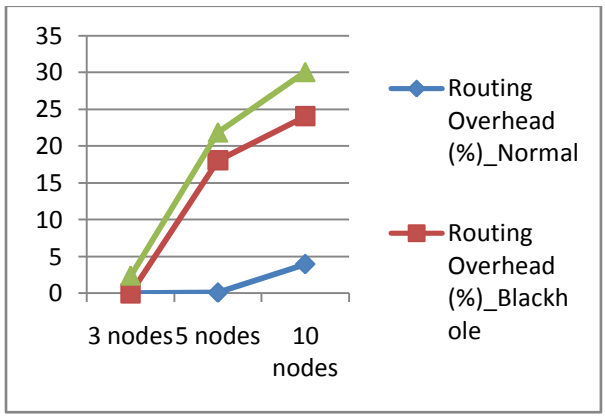

Fig 9. Comparison of Routing Overhead

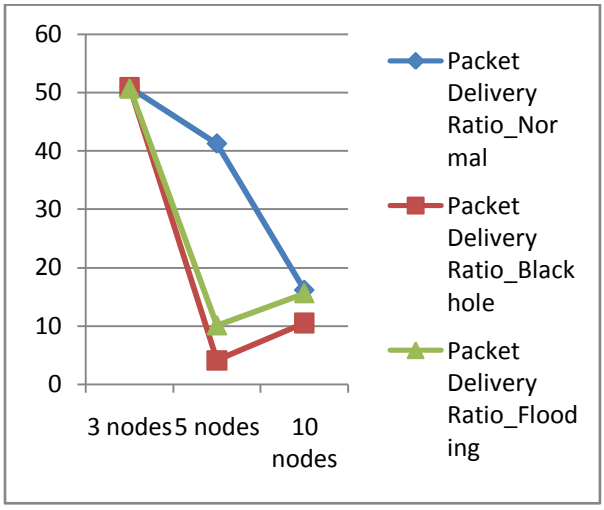

Fig 10. Comparison on Packet Delivery Rate

References

[1]. Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao ; A survey of black hole attacks in wireless mobile ad hoc networks ; Human-centric Computing and Information Sciences 2011

[2]. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester; An Overview of Mobile Ad Hoc Networks: Applications and Challenges

[3]. Siddhu Warrier; report on Characterisation and Applications of MANET Routing Algorithms in Wireless Sensor Networks

[4]. Sem_H Dokurer "Simulation Of Black Hole Attack In Wireless Ad-Hoc Networks" [5] http://www.isi.edu/nsnam/vint

[5]. Teerawat Issariyakul ,Ekram Hossain "Introduction to Network Simulator NS2"

[6]. Mangesh Ghonge, Prof. S. U. Nimbhorkar"Simulation of AODV under Blackhole Attack in MANET"

[7]. http://www.ns2ultimate.com