Tarandeep Kaur, Amarvir Singh / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 4, Jul-Aug 2013, pp.1324-1328

Performance Evaluation of MANET with Black Hole Attack Using Routing Protocols

Tarandeep Kaur[1], Amarvir Singh[2]
[1, 2] Punjabi university, DEPT. of Computer science, Patiala, India

ABSTRACT

Mobile Ad hoc networks (MANET) are collection of wireless nodes that communicate with each other with the help of wireless links. MANET is vulnerable to different attacks due to its feature open medium, dynamic topology, no central authority and no clear defense mechanism. One of the attacks is black hole attack in which a malicious node intercepts the packets being transmitted to another node in the network. As the data packets do not reach the destination, Data loss occurs which affects the performance of network badly. Our aim of the paper is to analyze the impact of the Black hole attack on MANET performance and how it affects the various performance metrics of the network by comparing the network performance with and without black hole nodes.

Keywords- Black hole attack, Manet, Routing protocols.

I. INTRODUCTION

MANET is considered a collection of wireless mobile nodes that communicate with each other without the use of a network infrastructure or central base station. Mobile nodes dynamically create routes among themselves to form own wireless network on the fly and organize themselves into a network. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network that may not be within direct wireless transmission range of each other. These infrastructure-less mobile nodes in ad hoc networks dynamically create routes among themselves to form own wireless network on the fly. Different applications of MANET are sensor networks, vehicle to vehicle communication, military battlefields and emergency services. These wireless links makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Black hole attack is one kind of attack that a MANET suffers from. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept.

This paper is divided into seven sections. Section 2 describes the black hole attack occurring in the network and the security issues related to the Attack. Section 3 consists of types of routing protocols that are used to find the secure path between the source and the destination node. Section 4 is of the previous work done on black hole attack. Section 5 consists of simulation methodology for analyzing the network with black hole attack and without black hole attack. Section 6 gives simulation results of our proposed model. Finally, the paper is concluded in section 7.

1.1 BLACK HOLE ATTACK

Black hole attack is an attack in which malicious node uses its routing protocol to advertise itself for having the shortest path with minimum hops to the destination node whose data packet it wants to take away. In this way attacker node is always available to the nodes whose packets it wants to retain.

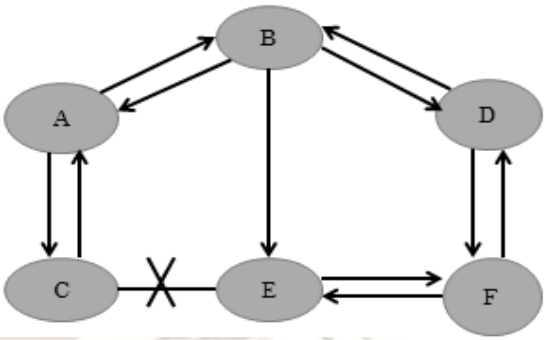

Fig. 1.1

In figure 1.1 Node A want to send data packets to node D and initiate the route discovery mechanism by sending a Route request message to all the nodes in the network. Node C is a malicious node it presents itself for having a shortest route to the destination node as soon as it receives route request (RREQ) message. It will then respond to node A before any other node responds. In this way node A will think that this is the only shortest route and thus will complete its route discovery mechanism. Node A will ignore all other replies and will start sending data packets to node C. In this way all the data packet will be intercepted by node C.

Due to these attacks, transmission of the data between the source and destination has become insecure. These attacker nodes exploit the network by becoming the part of the network. One of the reasons that make the network more susceptible to these attacks is its wireless links due to which attacker

nodes go inside the network and starts intercepting the packets being transmitted which leads to data loss.

1.2 ROUTING PROTOCOLS

The primary goal of routing protocols is to securely deliver the data packets by finding a shortest path between source and destination with minimum hops. A MANET protocol work for small sized network to large sized network. Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are typically table driven. Examples of this type include Optimized link state routing (OLSR), Destination Sequence Distance Vector (DSDV) protocols. Reactive or source-initiated on demand protocols, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes Zone Routing Protocol (ZRP).

II. RELATED WORK

Mohammad Al-Shurman [2] has proposed solution in which host node sends a packet that includes the packet id and sequence number to destination node through three different paths. When any intermediate node or malicious node has a route to the destination node will reply to that packet. Once the source node collects all the reply from the intermediate nodes, source node will check for the secure route to the destination.

Sanjay Ramaswamy [6] proposed a solution for multiple black hole nodes in a network. He modified AODV routing protocol by introducing new concept of data routing information table and cross checking. In DRI table, every intermediate node maintains a DRI table which will record information about the node traversed before and node traversed after the intermediate node. Once the data is transmitted cross checking is done to check the data loss occurred during the transmission.

Hesiri Weerasinghe [4] studied the problem of cooperative black hole attack in MANET. He has compared the performance of the network in terms of throughput, end to end delay, packet loss and packet overhead by varying the number of black hole nodes, number of mobile nodes, mobility speed and the size of terrain area. Simulation results show greater reduction in terms of throughput and packet loss.

K. Lakshmi [7] proposed an algorithm named Prior_ReceiveReply with six steps. In first step current time is retrieved and that current time is added to the waiting time that is set for the source node to receive route request from the intermediate nodes. Second step is of storing the RREQ destination sequence number (DSN) and node ID into a table called RR table (Route Reply). Next third step is of identifying and removing the malicious node. The first entry in the RR table with the greatest DSN is of malicious node. If the difference between the DSN of source node and the first entry in RR table is much greater than remove that first entry from the RR table. In this way a malicious node is identified and removed. In next step, second entry with higher DSN in the RR table is selected. In the last step, with that entry the default process is continued.

Dinesh [5] analyzed the behavior of malicious node in different routing protocols in MANET. He proposed a solution for finding a safe route by waiting and checking the replies received from the intermediate nodes. He observed the network under varying network mobility with maximum speed of 10m/s. He concluded that AODV routing protocol results in a better performance with black hole nodes than DSR in terms of throughput.

III. SIMULATION METHODOLOGY

OPNET modeler 14.5 is used to develop the simulation and analysis for this paper. Six different scenarios have been created in which 60 mobile nodes have been kept in a campus network. Out of those 60 mobile nodes, 15 nodes are made black hole nodes or malicious nodes by changing some of their parameters. All these nodes are configured mobile by using profile configuration. Two different applications file transfer protocol (FTP) for heavy load and hypertext transfer protocol (HTTP) for heavy browsing are being used to analyze the performance. Simulation focuses on performance of network with and without black hole attack by changing the routing protocols. Three different routing protocols have been employed on these six scenarios. These routing protocols are Ad hoc on demand routing protocol (AODV), Optimized link state routing protocol (OLSR) and Dynamic source routing protocol (DSR). Network throughput, delay, and load are taken into account to perform simulation using routing protocols.

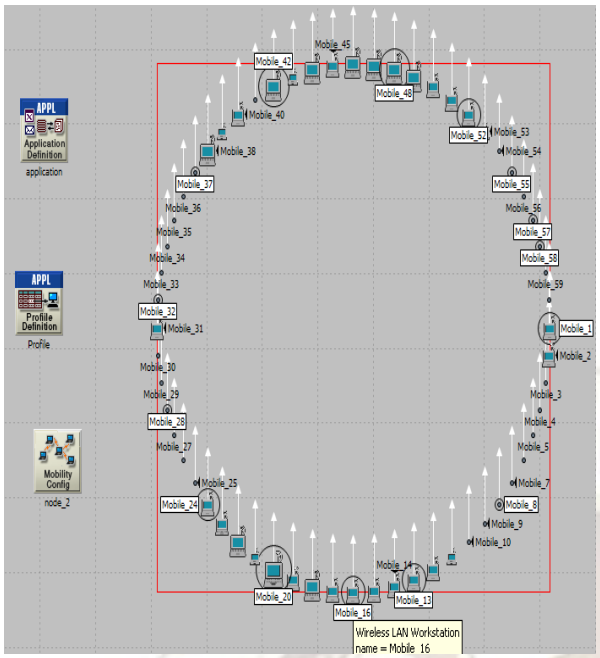

Fig 2. Network model

We use the following metrics to evaluate the protocols.

LOAD (BITS/SEC): Load represents the total load (in bits/sec) submitted to wireless LAN layers by all higher layers in all WLAN nodes of the network

THROUGHPUT: Throughput represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network.

DELAY (SEC): Delay represents the end to end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer. This delay includes medium access delay at the source MAC, reception of all the fragments individually, and transfers of the frames via AP, if access point functionality is enabled.

3.1 SIMULATION RESULTS

Simulation is done for 600 seconds for each scenario and overlaid statistics of these performance metrics for each protocol have been obtained.

Table 1. Simulation Parameters

Initial topology	Empty scenario
Size	10*10 km
Model family	MANET
Network scale	campus
Data rate	11 mbps
Speed	5m/s
Technology	WLAN (AD HOC)
Nodes	60
Attacker nodes	15
Mobility model	Random waypoint
Routing protocols	AODV,OLSR, DSR
Operational mode	802.11b
Packet inter-arrival time	Constant(0.03)
Packet size	Uniform(140,160)
Trajectory	Vector
Simulation time	600 seconds

The following graph depicts the nature of each routing protocol by taking into account the performance metrics with and without the attacker node.

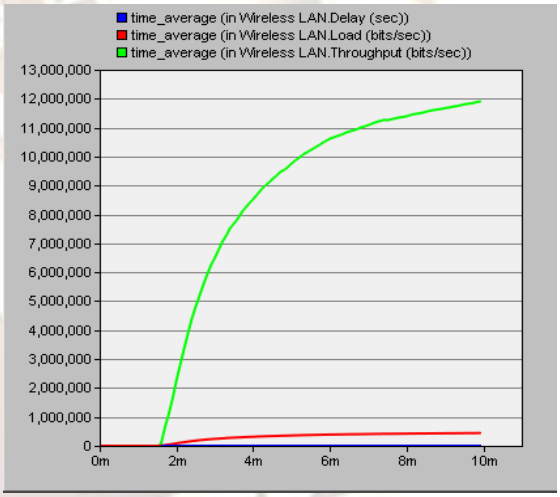

Fig.3 AODV without attacker nodes

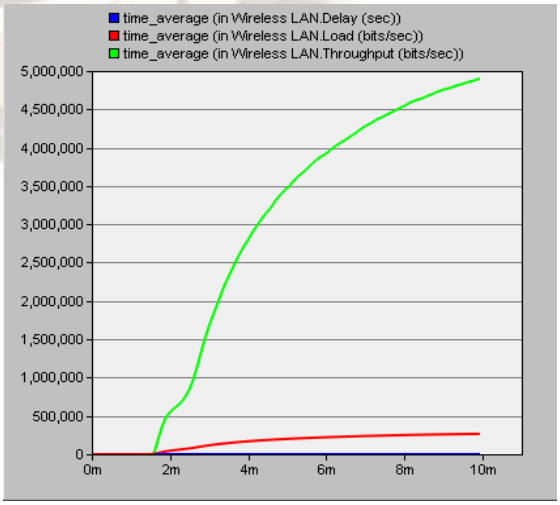

Fig.4 AODV with attacker nodes

Fig.3 and fig. 4 shows the impact of black hole attack on the network performance under AODV routing protocol. In fig.3, the throughput is high without attacker nodes than in fig.4 with attacker nodes. This is because of few packets are being forwarded and loss of data occurs. Because of the packets being discarded by the attacker nodes, shows an impact on throughput. When we compare the throughput of both the scenarios, we find a greater difference in throughput of both scenarios. All this leads to lesser load on the network with attack. Load which is 500,000 bits/sec without attack just remains 300,000 bits/sec with attack. This is because without the presence of the attacker nodes, the network load is high due to the proper routing of the packets to their destinations, but with attacker nodes discarding of the packets leads to the reduction in the network load.

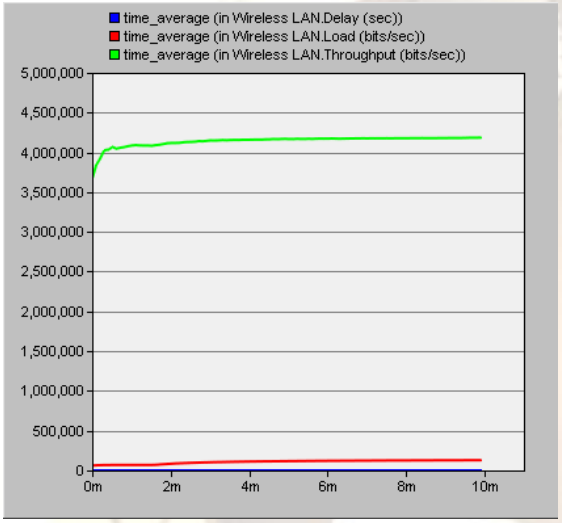

Fig.5 OLSR without attacker node

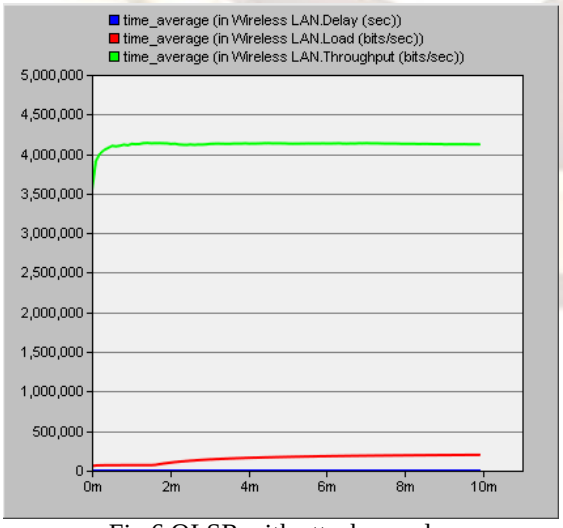

Fig.6 OLSR with attacker nodes

Fig.5 and fig.6 shows the impact of black hole attack on the network performance under OLSR routing protocol. As we compared the performance of the network with and without attacker nodes under OLSR routing protocol, the difference in the throughput is negligible. Same is in the case of network load; change in the network load with and without attacker nodes is negligible.

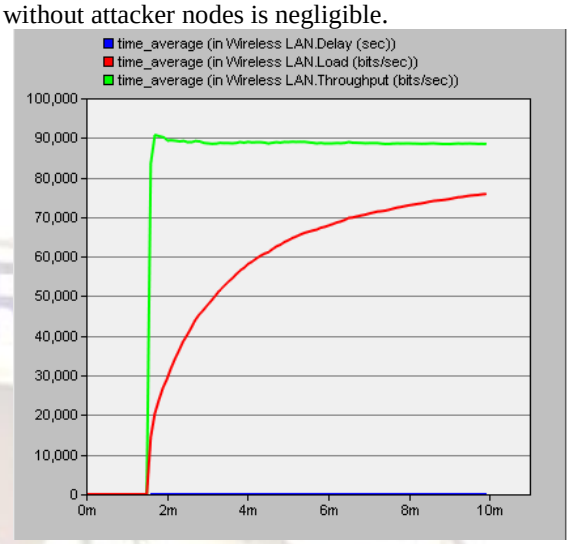

Fig.7 DSR without attacker node

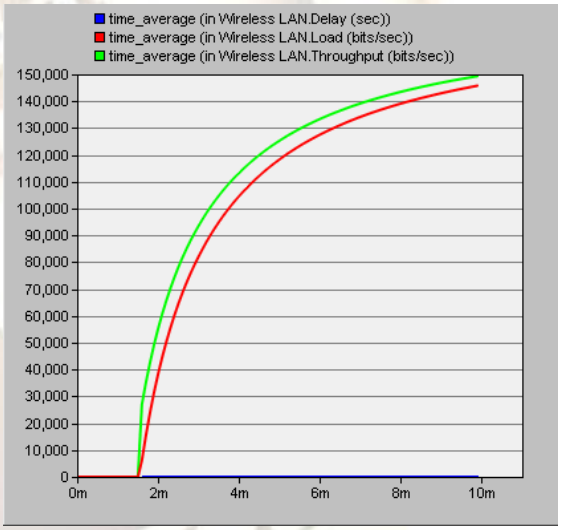

Fig. 8 DSR with attacker node

Fig.7 and fig.8 shows the impact of black hole attack on the network performance under DSR routing protocol. In Fig.7 green line depicts throughput without attacker nodes which first increases with a peak then remain constant for the rest of the time whereas in fig.8 throughput with attacker nodes keeps on increasing for the whole time. Red line depicts load on the network which slightly increases with the presence of attacker nodes.

IV. CONCLUSIONS

In this paper we analyze the impact of black hole attack on network performance in terms of throughput, delay and load under AODV, OLSR, DSR routing protocols. Simulation results show that when there are attacker nodes in the network it

decreases the overall performance of the network by intercepting the packets being routed from the source node to the destination node. The impact of attacker nodes on the network highly disrupts the performance which leads a greater data loss.

REFERENCES

Thesis:

[1] Irshad Ullah and Shoaib Ur Rehman, "Analysis of Black Hole Attack on Mobile Ad hoc Networks Using Different MANET Routing Protocols" *June 2010*

Journal Papers:

[2] Mohammad Al-Shurman and Seong Moo Yoo, "Black Hole Attack in Mobile Ad Hoc Networks," *42nd Annual South East Regional Conference*

[3] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," *IEEE Communications Magzine, vol. 40, no. 10, October 2002.*

[4] Hesiri Weerasinghe and Huirong Fu, Member of IEEE, Preventing Cooperative Black Hole Attacks in Mobile Adhoc Network Simulation implementation and Evaluation ,*IJSEA,Vol2,No.3,July 2008.*

[5] Dinesh Mishra, Yogendra Kumar Jain, Sudhir Agrawal, "Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET)" *International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2009.*

[6] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" *International Conference on Wireless Networks, Las Vegas, Nevada, USA.*

[7] K. Lakshmi, S.Manju Priya2 A.Jeevarathinam3 K.Rama4, K. Thilagam5 "Modified AODV Protocol against Black hole Attacks in MANET" *International Journal of Engineering and Technology Vol.2 (6), 2010.*