Performance Analysis of Mobile Ad Hoc Network in the Presence of Wormhole Attack

F. Anne Jenefer & D. Vydeki
E-mail : annejenefer@gmail.com, vydeki.d@srmeaswari.ac.in

Abstract – Mobile Ad-Hoc Network (MANET) is a group of wireless mobile nodes connected to each other without any central administrator. Nodes can move from one place to another in the network or may leave or join the network at any time. Due to this the topology of the network changes rapidly. Due to the absence of central administrator the MANETs are vulnerable to attacks. In this paper, performance comparison of MANET in the presence and absence of two types of wormhole attack such as replay and tunneling has been carried out. The performance of the network is measured using metrics like Average End-to-End Delay, Throughput and Jitter by varying the number of nodes and number of attackers. The experimental results prove that the network performance is severely affected in the presence of wormhole attack.

Keywords – AODV, Mobile Ad-hoc Networks, Wormhole, tunneling, replay

I. INTRODUCTION

Ad hoc wireless network is an autonomous self-organizing system of mobile nodes connected by wireless links where nodes not in direct range can communicate via intermediate nodes. A common technique used in routing protocols for ad hoc wireless networks is to establish the routing paths on demand, as opposed to continually maintaining a complete routing table. A significant concern in routing is the ability to function in the presence of failures which include nodes that drop, modify, or mis-route packets in an attempt to disrupt the routing service.

A MANET is a collection of wireless devices moving in seemingly random directions and communicating with one another without the aid of an established infrastructure. To extend the reachability of a node, the other nodes in the network act as routers. Since MANETs can be set up easily, they have a wide range of applications, especially in military operations and disaster relief efforts. However, MANETs are more vulnerable to security attacks both in wired and wireless networks, distributed and cooperative sharing of channels and other resources, and power and computation constraints.

MANETs has advantages like simple, cheap and fast setup of networks, more robust concerning failure of single component due to decentralized structure. Because of these they are used in many applications like wireless sensor networks, rescue operations, sports events and conferences etc.

II. WORMHOLE ATTACK

Wormhole is a severe type of attack, where two attackers are connected to each other through high speed off-channel link. The wormhole node receives the packet at one location and sends it to other wormhole node through high speed off-channel link. The worst can happen that nodes can be in dilemma that they are close to the destination even though they are at far distance. Wormhole refers to an attack on MANET routing protocols in which colluding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbours but are actually distant from one another. This shortcut is created by connecting the purported neighbours through a covert communication channel. It highly degrades the performance of the networks.

A wormhole allows an attacker to create two attacker controlled choke points to which traffic is attracted and which can be utilized by the attacker to degrade or analyze traffic at a desired time. The covert communication channel used by the attackers could be a separate communication mechanism not generally used by the network, forming an out-of-band wormhole attack. On the other hand, an in-band wormhole attack uses the primary link layer to develop the covert tunnel.

For launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link called as the wormhole link. The wormhole link can be established by a variety
of means, e.g., by using an ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

Wormhole node affects the routing and other connectivity based protocols in the network. Once the wormhole link is established, the wormhole nodes can start dropping packets and cause network disruption. They can also spy on the packets going through and use the large amount of collected information to break any network security. The wormhole attack will also affect connectivity-based localization algorithms and protocols based on localization, like geographic routing, will find many inconsistencies resulting in further network disruption.

Fig.1: Wormhole Attack.

Fig.1 shows the wormhole attack in MANET. The nodes a, b, c, d and e are involved in communication in the network. Here, X and Y are the wormhole nodes and they form a link between them called wormhole link. Through this wormhole link the wormhole node tunnels the data packets from one end to another.

Types of wormhole attacks are:

**All Pass:** The wormhole nodes will pass all the packets irrespective of their size.

**All Drop:** All the packets are dropped by wormhole nodes in the network.

**Threshold:** The Wormhole node drops all the packets size greater than or equal to the threshold value.

**Replay:** The Packets are replayed by the wormhole node after tunnelling in the network.

**Tunnelling:** The Wormhole node tunnels the packet from one point to another through the wormhole link in the network.

**Propagation Delay:** The propagation delay in the network is increased due to the wormhole nodes.

Fig.2: Wormhole-Tunnelling Attack.

Fig.2 shows the wormhole-tunneling attack in MANET. As shown in the figure, the wormhole nodes creates a link between them called wormhole link and tunnels the packets from one end to another. Here, the nodes S2 and S9 act as the wormhole nodes in the network.

### III. PROPOSED SYSTEM

In this section the simulation of MANET and the associated parameters of the proposed system are discussed. The flow diagram for the proposed system is shown in fig.3.

Fig.3: Flow diagram of proposed system.

As shown in the figure first MANET is designed using the QualNet simulator. The network parameters such as routing protocols, data rate, etc. are given in the simulator for the designed network. The wormhole is designed by changing the properties of the node in the MAC layer. The MAC layer of the subnet is also changed for enabling the wormhole attack in the
network. The simulation time and the mobility speed of the nodes are given in the scenario properties and the network which is designed is simulated using the QualNet simulator.

A. Simulating MANET

MANET which is designed for analysis is simulated using the QualNet simulator, with different number of nodes such as 10, 20 and 30 nodes. For each network varying number of passive intruders were included. CBR traffic link was used for communicating between the nodes. Initially, MANETs without any attacks have been created for performance comparison. The network parameters such as throughput, end-to-end delay and jitter are used for analysis purpose. The nodes are grouped using the wireless subnet in the simulator.

Fig.4: MANET without Wormhole Attack.

Fig.4 shows the MANET without wormhole attack which is designed for analysis. The network with 10 nodes and 2 CBR links is shown here for example. Here, nodes 1 and 7 are the source nodes and the nodes 3 and 6 indicate the destination nodes. The subnets in the network are shown in the form of cloud which indicates the wireless link in the network. The CBR links are given with the data rate of 2 Mbps for the network with and without the wormhole attack.

Fig.5 shows the MANET with wormhole attack which is designed for analysis. The network with 10 nodes and 2 CBR links is shown for example. Here also the nodes 1 and 7 indicate the source nodes and the nodes 3 and 6 indicate the destination nodes. Nodes 9 and 10 indicate the wormhole nodes in the network which is shown in the form of daemon.

B. Simulation Parameters

The QualNet 5.2 simulator is used for simulation. The MAC protocol IEEE 802.11 was used with a data rate of 2 Mbps. The values of each parameter used in designing the network are shown in the fig.6.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terra in Size</td>
<td>1500m x 1500m</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>10, 20, 30</td>
</tr>
<tr>
<td>Number of Wormhole Nodes</td>
<td>2, 4, 6</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>CBR</td>
</tr>
<tr>
<td>Number of CBR Links</td>
<td>2, 4, 6</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random way Point</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>MAC</td>
<td>802.11</td>
</tr>
<tr>
<td>Packet Size</td>
<td>512 Bytes</td>
</tr>
<tr>
<td>Speed</td>
<td>0-10 m/s</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>300 sec</td>
</tr>
<tr>
<td>Attack Type</td>
<td>Wormhole</td>
</tr>
</tbody>
</table>

Fig.6: Simulation Parameters used for designing MANET.

C. Performance Metrics

Performance metrics which are considered to analyze the MANET are explained below.

Average End-to-End Delay: Average end-to-end delay is the average time it takes a data packet to reach to destination in seconds. It is calculated by subtracting “time at which first packet was transmitted by source” from “time at which first data packet arrived to destination”.

ISSN (Print): 2278-5140, Volume-2, Issue – 1, 2013
Throughput: Throughput is defined as total number of delivered data packets divided by the total duration of simulation time.

Jitter: Jitter is the variation in the time between packets arriving, caused by network congestion, and route changes.

IV. SIMULATION TOOL

QUALNET is a commercial version of GloMoSim used by Scalable Network Technologies for their defence projects. It is a commercial network simulator from Scalable Network Technologies, Inc in 2000-2001. This tool is an extension of GloMoSim which is being commercialized. It is ultra high fidelity network simulation software that predicts wireless, wired and mixed-platform network and networking device performance. QualNet Developer is a network evaluation software that analyzes the performance of wired, wireless and hybrid network. QualNet supports thousands of nodes for simulation and also supports for 64 bit Operating system. It works on UNIX, Linux and MacOS and even can be deployed in live networks. They have separate licenses for Academics and others. QualNet is designed to simulate large-scale wired and wireless networks with thousands of mobile nodes, each of which may different communication capabilities via multihop ground, aircraft and satellite media. It uses the parallel simulation environment for complex systems (PARSEC) for basic operations, hence can run on distributed machines. QualNet includes a graphical user interface for creating the model and its specification. So, it is very easy to specify small to medium networks by using the GUI. Since it uses primarily Java for the GUI, it is available for Linux as well as for Windows.

The simulator itself is the specified target system optimized C program. Faster simulation speeds and greater scalability are achievable through smart architecture and optimized memory management of QualNet. It is not used much in research as it is not freely available, hence lesser support (code samples etc) available on Web. Simulation of wireless sensor networks is supported in Qualnet 4.5 (using ZigBee library). Simulation of GSM mobile networks also supported in QualNet simulator. Includes a variety of advanced libraries such as mesh networking, battery models, network security tool kit and a large number of protocols at different layers. It also includes a 3D visualizer for better visualization of a scenario. For beginners who want to evaluate and test different existing routing protocols, as it can be done with GUI, without writing even a single line of code. For implementing new protocols, Qualnet uses C/C++ and follows a procedural paradigm.

V. SIMULATION RESULTS

This section presents the simulation results to show the correctness of the observations discussed in this paper. The performance of the MANETs with and without the wormhole attacks are given below. The network is analyzed by comparing the performances of both the static and mobile nodes. For the different number of nodes and passive intruders the throughput, end-to-end delay and jitter are plotted. As per the analysis the network performances degrades with the increase in number of nodes and passive intruders. The delay and jitter for the network increases with the increase in number of nodes and intruders.

A. Static Nodes

The plots show the performance of the network for different number of nodes and passive intruders. The plots are shown both for the static and mobile nodes of MANET. In case of static nodes as shown in the fig.7 the throughput of the network increases with the decrease in number of nodes. The performances of the network with and without the passive intruders are compared here for analysis.

Fig.7: Throughput for Static Nodes.

Fig.8: End-to-End Delay for Static Nodes.
Fig. 8 shows the plot for end-to-end delay versus number of nodes. The delay in the network increases for the network with passive intruders and it is low for the network without any intruders.

Fig. 9 shows the performance graph of MANET for the static nodes. The network with and without passive intruders are compared for the network parameter jitter. The jitter increases for the network which includes the wormhole attack. And it is low for the network without any wormhole attack. As such for static nodes the analysis is done for the network with mobile nodes.

Fig. 9: Jitter for Static Nodes.

B. Mobile Nodes

Fig. 10: Throughput for Mobile Nodes.

Fig. 11: End-to-End Delay for Mobile Nodes.

Fig. 12: Jitter for Mobile Nodes.

The figures 10, 11 and 12 show the performance graph of MANET with the mobile nodes. The network with and without passive intruders are compared for the analysis purpose. The network parameters such as throughput, end-to-end delay and jitter are analyzed for the mobile nodes. As discussed for static nodes, mobile nodes also have increased throughput incase of network without any attack. The end-to-end delay and jitter of the network are increased for the network with passive intruders.

VI. CONCLUSION

In this paper, the performance of MANET with and without wormhole attack was analyzed. The simulation results show that the performance of the MANET degrades due to wormhole attack. The throughput of the network decreases with the increase in the number of attackers. The end-to-end delay and jitter increases with the increase in the number of attackers in the network.
The future includes the detection of such wormhole attacks in the MANETs by analyzing the various communication parameters such as link breakage in the network and the delay.

VII. REFERENCES


