Impact of Jamming Attack in Performance of Mobile Ad hoc Networks

Jagat Singh [1], Sachin Gupta [2]
Department of Computer science and Engineering
Assistant Professor [2]
MVN University
Palwal - India

ABSTRACT
MANETs have unique characteristics like dynamic topology, wireless radio medium, limited resources and lack of centralized administration; as a result, they are vulnerable to different types of attacks in different layers of protocol stack. Each node in a MANET is capable of acting as a router. The necessity for a secure MANET networks is powerfully tied to the security and privacy features. This Jamming attacks are one of them. These occur by transmitting continuous radio ways to inhibit the transmission among sender and receiver. These attacks affect the network by decreasing the network performance. Previously there had been considerable research in the field of increasing the performance of network by using routing protocols. In this paper we are analyzing the performance of Vehicular ad hoc networks under jamming attack. This work includes a network with high mobility, using IEEE Along g standard with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. Video conferencing and FTP with high data rate are being generated in the network. For the Simulation purpose we employed OPNET (Optimized Network Engineering Tool) MODELER 14.5 is used for simulation. The performance of network is measured with respect to the QoS parameters like, network load, retransmission attempts, media access delay and. Throughput

Keywords:- AODV,FTP,MANET,OPNET.

I. INTRODUCTION

Ad-Hoc networks have no infrastructure where the nodes are free to join and left the network. The nodes are connected with each other through a wireless link. A node can serve as a router to forward the data to the neighbors’ nodes. Therefore this kind of network is also known as infrastructure less networks. These networks have no centralized administration. Ad-Hoc networks have the capabilities to handle any malfunctioning in the nodes or any changes that its experience due to topology changes. Whenever a node in the network is down or leaves the network that causes the link between other nodes is broken. The affected nodes in the network simply request for new routes and new links are established Ad-Hoc network can be categorized in to static Ad-Hoc network (SANET) and Mobile Ad-Hoc network (MANET). In our research work we are improving the performance of mobile ad hoc networks under jamming attack by using an integrated approach. The proposed work includes a network with high mobility, using IEEE Along g standard with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. FTP and Video conferencing with high data rate are being generated in the network.

Figure1. Mobile Ad hoc Network
II. JAMMING ATTACK

Jamming attack deliberately transmits of radio signals to disrupt the whole communications by decreasing the signal-to-noise ratio. The term jamming is used to differentiate it from unintentional jamming which called interference. In MANET Jamming is a serious threat to its security. Jammers constantly send.

![Figure 2: Jamming Attack](image)

III. LITERATURE REVIEW

Sisi Liu et al. (2012) addresses the problem of mitigating DoS attacks manifested in the form of jamming. The author considered a sophisticated adversary who has knowledge of the protocol specifics and of the cryptographic quantities used to secure network operations. This type of adversary cannot be prevented by anti jamming techniques that rely spread spectrum. The author proposed a new security metrics to quantify the ability of the adversary to deny access to the control channel, and introduced a randomized distributed scheme that allows nodes to establish and maintain the control channel in the presence of the jammer. The proposed method is applicable to networks with static or dynamically allocated spectrum. Furthermore, two algorithms for unique identification of the set of compromised nodes were proposed, one for independently acting nodes and one for colluding nodes[19]. Dorus.R et al. (2013) proposes a mechanism for preventing jamming attacks on wireless networks, examine the detection efficiency of jamming attack and communication overhead of the wireless network using proactive and reactive protocols. RSA algorithm is used and analyzed for providing data packets integrity information during wireless transmission. Through simulation and performance analysis, the implemented prevention mechanism and the integrity preservation provides higher packet delivery ratio in proactive routing protocol (OLSR) than reactive routing protocol (AODV). Nadeem Sufyan et al. (2013) investigates a multi-modal scheme that models different jamming attacks by discovering the correlation between three parameters: packet delivery ratio, signal strength variation, and pulse width of the received signal.

A. Simulation Tool used:

This section describes the simulation tool used along with the proposed method.

OPNET modeler v14.5 is extensive and a very powerful simulation tool with wide variety of possibilities. The entire heterogeneous networks with various routing protocols can be simulated using OPNET. High level of user interface is use in OPNET which is constructed from C and C++ source code blocks.

B. Simulation Setup:

The simulation work focuses on analysing the performance of MANET under jamming attack. Therefore an Integrated approach is used to analyse the network performance under jamming attack. This approach includes:

- High data rate of 54mbps by using IEEE 802.11g standard [9]
- Network with high mobility [2]
- Improved parameter of AODV routing protocol
- Generation of high resolution video conferencing and FTP traffic.
Figure 3: Jamming attacks scenario in MANET

Table: MANET Simulation Parameters

<table>
<thead>
<tr>
<th>Examined Cases</th>
<th>Protocols AODV without Jamming Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Nodes</td>
<td>100 and 200</td>
</tr>
<tr>
<td>Types of Nodes</td>
<td>Mobile</td>
</tr>
<tr>
<td>Simulation Area</td>
<td>60*60 km</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>Mobility</td>
<td>Uniform(10-100) m/s</td>
</tr>
<tr>
<td>Pause Time</td>
<td>200 seconds</td>
</tr>
<tr>
<td>Performance Parameters</td>
<td>Throughput, Delay, Net.load</td>
</tr>
<tr>
<td>Trajectory</td>
<td>VECTOR</td>
</tr>
<tr>
<td>Long Retry Limit</td>
<td>4</td>
</tr>
<tr>
<td>Max Receive Lifetime</td>
<td>0.5 seconds</td>
</tr>
<tr>
<td>Buffer Size(bits)</td>
<td>25600</td>
</tr>
<tr>
<td>Mobility model used</td>
<td>Random waypoint</td>
</tr>
<tr>
<td>Data Type</td>
<td>Constant Bit Rate (CBR)</td>
</tr>
<tr>
<td>Packet Size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Traffic type</td>
<td>FTP, Http</td>
</tr>
<tr>
<td>Active Route Timeout</td>
<td>4 sec.</td>
</tr>
</tbody>
</table>

Table II: MANET Simulation Parameters for Jammer

<table>
<thead>
<tr>
<th>Examined Protocols Cases</th>
<th>AODV without Jamming Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Nodes</td>
<td>100 and 200</td>
</tr>
<tr>
<td>Types of Nodes</td>
<td>Mobile</td>
</tr>
<tr>
<td>Simulation Area</td>
<td>50*50 km</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>Mobility</td>
<td>Uniform(10-100) m/s</td>
</tr>
<tr>
<td>Pause Time</td>
<td>200 seconds</td>
</tr>
<tr>
<td>Performance Parameters</td>
<td>Throughput, Delay, Network load</td>
</tr>
<tr>
<td>No. of Jammers</td>
<td>10</td>
</tr>
<tr>
<td>Jammer Bandwidth</td>
<td>100,000</td>
</tr>
<tr>
<td>Jammer band base frequency</td>
<td>2,402</td>
</tr>
<tr>
<td>Jammer Transmitter Power</td>
<td>0.001</td>
</tr>
<tr>
<td>Trajectory</td>
<td>VECTOR</td>
</tr>
<tr>
<td>Data Type</td>
<td>Constant Bit Rate (CBR)</td>
</tr>
</tbody>
</table>

Hello interval(sec) | 1,2
Hello Loss | 3
Timeout Buffer | 2
Physical Characteristics | IEEE 802.11g (OFDM)
Data Rates(bps) | 54 Mbps
Transmit Power | 0.005
RTS Threshold | 1024
Packet-Reception Threshold | -95
Packet Size | 512 bytes  
---|---
Traffic type | FTP, Http  
Active Route Timeout(sec) | 4  
Hello interval(sec) | 1.2  
Hello Loss | 3  
Timeout Buffer | 2  
Physical Characteristics | IEEE 802.11g (OFDM)  
Data Rates(bps) | 54 Mbps  
Transmit Power | 0.005  
RTS Threshold | 1024  
Packet-Reception Threshold | -95  
Performance Parameters | Throughput, Delay, Network load  
Trajectory | VECTOR  
Long Retry Limit | 4  
Max Receive Lifetime (seconds) | 0.5  
Buffer Size(bits) | 25600  

**IV. RESULT**

**A. Delay:** Represents the end to end delay of all the packets received by the wireless LAN MACs of all MANET nodes in the network and forwarded to the higher layer. Jammers would affect the performance of system by increasing the delay as shown in the Fig. 4 and 5.

**B. Data dropped:** Total higher layer data traffic (in bits/sec) dropped by the all the WLAN MACs in the network as a result of consistently failing retransmissions. Jammers could affect the network by increasing Data dropped of network as shown in Fig. 6 and 7.

**C. Network Load:** Figure 8 and 9 shows that the network load of the normal network is noted as 22,340 bits/sec and with the jamming nodes in the network it is noted as 25840 bits/sec. The jamming attacker nodes drop the packets and not forwarding the packets for the other nodes.
V. CONCLUSION

Because of the wireless nature of mobile ad hoc networks, various attacks are performed to degrade the...
network performance. Jamming attack is one of them therefore e routing protocols are used to increase the network throughput. In this research work, Impact of Jamming Attack in Performance of Mobile Ad hoc Networks, Jammers attacks will have an effect on network’s performance as a result of the jammers interferes with the traditional operation of the network. The effect of attackers studied in this paper was by increasing delay, data dropped traffic received and sent and decreasing packet drop ratio of the network. In this research work, the network performance under jamming attack is analyzing by applying integrated approach. This approach includes a network with high mobility, IEEE 802.11g standard with max data rate, heavy traffic like FTP and video conferencing, improved AODV parameters and increased buffer size. In our paper, it was shown that jamming attack reduces the network throughput, retransmission attempts and increases the media access delay.

REFERENCES


