Security Issues in Mobile Ad-Hoc Networks

*Kishore Dasari, **Tammineedi Venkata Satya Vivek

1,2Dept. of CSE, KL University, Vaddeswaram, Vijayawada, AP, India

Abstract

In this survey paper we have studied about different Mobile Ad-hoc networks in the infrastructure less wireless network. In a network the mobile nodes move rapidly from one node to the another. The application of MANET requires very good efficient group communication for the data transfer. The security constraints taking place in the MANET is very low when compared to the wired network. This survey paper is discussing not only the different Mobile Ad-hoc networks, but also about the different attacks in the MANET layers. These attacks in the MANET layers are may be active or passive. The passive attacks does not alter by the attacker. The main focus of the active attacks is on the network layer protocols.

Keywords

Spoofing, Sinkhole, Location Disclosure, DOS, Man-in-Middle Attack

I. Introduction

The Mobile Ad Hoc Network is infrastructure less wireless network and having self-configure and self-organisation nodes. The self-configuration consists of two stages. First one is internal a device. This is issue to more utilise a set of auto-configurable parameters at different layers in MANET. Second one is external to a device. Here interaction with external device and support to re-configuration. Each node in the MANET having own energy resources and processing capability. The wireless environment can change dynamically.

In this network, mobile nodes are moving rapidly. MANET application requires very efficient group communication for data transfer. Any mobile network has common characteristic and constraint, i.e. energy. The nodes does not having own energy generating devices. MANET can be easily established in any emergency situations. This technology was used in battle field, later spread to entire field of communications. Basically MANET is three types, first one is vehicular Ad Hoc Networks are used for inter vehicle communication and communication between vehicle and roadside devices. Second one is intelligent vehicular Ad Hoc Networks, these are having artificial intelligent programs, which help to vehicle driving persons during collisions and accidents. Third one is internet based MANET.

The security in MANET is low when compared to wired network. In this paper discussed about different attacks in MANET layers. The attacks are passive or active. A passive attack does not interrupt the normal operations in MANET. The attacker observing which type of data and what data exchanging between the sender and receiver. In this attack the packet does not altered by attacker. Traffic analysis, traffic monitoring and eavesdropping some of the passive attacks. The active attacks mainly focus on the network layer protocols. The various attacks possible in routing protocols. These are wormhole attacks, Blackhole attacks, Sybil attacks, etc. The attacks on routing protocols, the malicious nodes or compromised nodes can modify routing information and sequence number in the packet. And these nodes create loops at the packet forwarding. Some attacks given in the Table-1

II. Physical Layer Attacks

Eavesdropping is the major attack in any communication that is listen the messages or conversations an illegally. The MANET communication established by using radio signals. These are easy to kept by the unauthorised connectivity. Sometimes these unauthorised nodes are transmitting modified signals and fake messages. Signal jamming also physical layer attack, the attacker used very strong and powerful transmitter, which generates strong signals compare to actual signals. The noise generated by the unwanted powerful signals. These jamming devices are freely available in the market in present days. Basically the jammers are classifying four types; these are constant jammers, deceptive jammers, random jammers and reactive jammers. The constant jammer can produce radio signals, and these signals cannot follow any MAC protocols. The deceptive jammers are transmitting the semi valid packets. The packet has a valid header but the payload is useless.

III. Link Layer Attacks

The Mobile Ad Hoc Network is wireless and an open multipoint p2p network. In the MANET each node connects with one are more neighbour nodes with help of Link Layer Protocols. The attackers concentrate on the disrupting. The IEEE 802.11 working comity proposed two different algorithms for access mechanisms. First one is distributed coordination function (DCF), i.e. fully distributed access protocol. The second one is Point Coordination Function (PCF), i.e. centralized access protocol. The DCF resolving channel contention among multiple wireless host with CSMA/CA. The communication between nodes in wireless network with help of RTS, CTS, DATA, ACKs. The shortest inter frame space (SIFS), i.e. space between RTS and CTS, CTS and DATA, DATA and ACKs. The longest inter frame space between ACK and RTS. In this network the communication with help of intermediate nodes. For example, node A and node C communicate with help of intermediate node B.

Table 1: Different Types of Attacks in Layers

<table>
<thead>
<tr>
<th>S.NO</th>
<th>ATTACK</th>
<th>LAYER</th>
<th>ACTIVE/PASSIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Eavesdropping</td>
<td>Physical Layer</td>
<td>Passive</td>
</tr>
<tr>
<td>2.</td>
<td>Traffic Analysis</td>
<td>Link Layer</td>
<td>Passive</td>
</tr>
<tr>
<td>3.</td>
<td>Monitoring</td>
<td>Link Layer</td>
<td>Passive</td>
</tr>
<tr>
<td>4.</td>
<td>Spoofing</td>
<td>Network layer</td>
<td>Active</td>
</tr>
<tr>
<td>5.</td>
<td>Wormhole</td>
<td>Network layer</td>
<td>Active</td>
</tr>
<tr>
<td>6.</td>
<td>Sinkhole</td>
<td>Network layer</td>
<td>Active</td>
</tr>
<tr>
<td>7.</td>
<td>Sybil</td>
<td>Network layer</td>
<td>Active</td>
</tr>
<tr>
<td>8.</td>
<td>Blackhole</td>
<td>Network layer</td>
<td>Active</td>
</tr>
</tbody>
</table>
9. Location disclosure Network layer Active
10. Session hijacking Transport layer Active
11. SYN flooding Transport layer Active
12. DoS Multi-layer Active
13. Man-in-middle Multi-layer Active

### A. Traffic Analysis

The attacker can get the information about the communication parties and routing information from traffic monitoring and analysis. These attacks not only in MANET, but also in any wireless networks, such as a wireless LAN, wireless sensor network also suffer from these attacks.

### B. Disruption MAC

The MAC (IEEE 802.11) protocols might be cooperative behaviour among all nodes in the Mobile Ad Hoc Network. The MANET link layer protocol operation does not follow by malicious or selfish nodes. These selfish nodes are not participating any packet forwarding. The nodes are interrupt the reservation based or contention MAC protocols. The malicious node or selfish nodes does not follow the protocol specifications when packet forwarding. For example, the malicious node can corrupt the frames by changing of bits. In the MAC protocol SIFS or exploit its binary exponential backoff scheme to generate the denial-of-service attacks.

### C. WEP Weakness

This specifies the wired equivalent privacy operation in the MANET. In the wired network all nodes are connect by some of wired protocol. That type of network access to easy to detects the misbehaving nodes. Cryptography key size in wired network is near or more than 128-bit, but in wireless LAN-802.11WEP key size is 40-bit. The key size is one of the weaknesses. It is provide privacy by transmitting encrypted radio signals. The WEP protocol does not specify any key management scheme for security.

### IV. Network Layer Attacks

Mainly the network layer performs routing operations. Different types of attacks are targeting the network layer. The attackers are injecting a malicious node M into network. The malicious node M absorbs the routing information and network traffic. Sometime the attackers can create routing loopholes, and then congestion occurs. Routing table overflow attacks possible in table driven protocols. Some malicious nodes try to create new route. The table driven routing protocols are getting routing information before the route be used. The attacker sends the excessive route advertisements. That is motivated to table overflow.

### A. Wormhole Attacks

In this attack a malicious node got packets at one location in the network and tunnels them to another location in same network. The tunnel between two malicious nodes is referred as wormhole. The attacker can create a tunnel with help of wired or high power radio communication signals. This attacker can attack with more than one malicious node. The attacker can’t any modification to the packet. In this attack the packet transmit very fast through tunnel.

### B. Blackhole Attacks

The Blackhole attack, the malicious node can send fake replay to source or which node sends RREQ, which is short route or destination node. If the source node sending packet to malicious node then it will drop the packet. The attack has two different properties. First one is, the node exploits the MANET touting protocol such as AODV, to advertise itself having a short route to destination. Second one is, the attacker can receive packets and simply drop.

### C. Resource Consumption Attacks

The malicious node or compromised node can attempt to consume energy resources by forwarding unnecessary packets and discovering routes.

### D. Rushing attacks

The two malicious nodes use the tunnel process to form a wormhole. A dedicated channel between two ends of wormhole and this helps
to forward packets very fast throughout network.

![Fig. 4:](image)

For example, the above figure source and destinations are S, D respectively. The node 3 is malicious node. The source node S send route request to their neighbour nodes 1, 2, 3 respectively. These nodes send RREQ massage to their neighbours. But node 3 send rushed RREQ to their connected nodes and forwarded the RREQs like 4, 5.

**E. Sybil attack**

The Sybil attacker can generate fake identifications to number of additional nodes. Which node has fake identity that is called Sybil node which is difficult to discover the misbehaving nodes. The Sybil nodes steal the identity of the actual nodes. If the Sybil attacker can attack the MANET, then difficult to identify the path.

**F. Sinkhole Attacks**

The malicious nodes connects to the maximum possible nodes in the network. The neighbouring nodes send RREQ to malicious node then it will send RREP. The neighbouring node send packet to the malicious node or sinkhole node. The sinkhole node gets the secure information and drop the packets. The attacker can modify the sequence number in the RREQ in the DSR protocol.

**V. Transport Layer Attacks**

The transport layer protocol provides the setting and clearing end-to-end connection, flow control, congestion control and end-to-end reliable service on packet delivery. The MANET has high error rate compared with wired network.

**A. Session Hijacking**

In session hijacking attack, the attacker can spoof the victim’s IP address and sequence number that expected by the target. The malicious node sends data packet with sequence number but not expecting by the receiver, then receiver try to resynchronize the session to sender node, the process keep going. The attacker sends injected session data to node 1. Node 1 will send ACK to node2 for acknowledge the data. The ACK packet having sequence number, but the sequence number is not expecting by node2. Then node2 try to resynchronize the TCP session with node1 by sending an ACK packet with sequence number that is excepting by node2. These processes going on until node2 receive ACK packet from node1 with correct sequence number.

![Fig. 5:](image)

B. SYN Flooding Attack

This is one of the denial-off-service (DoS) attacks. Complete TCP connection having three way handshakes. In the hand shake duration, three different messages are exchanged.
1. Node a sends to node b, a SYM packet for connection
2. Node b sends back to node a SYN-ACK
3. Node a send ACK to node b, than connection established.

![Fig. 6:](image)

The attacker creates large number of half-opened TCP connections with a victim node. But not complete the handshake operation. The attacker create large amount of SYN packets and send to target node and get packet address of SYN packet by spoofing. The victim node sends SYN-ACK packets to malicious node after receive SYN packets. The victim node maintains the fixed size table to store SYN packets. The malicious does not send ACK to victim node. The half-opened connections expired within short amount of time. But the attacker can create SYN packets very fast compare to the connection expiration.

**VI. Application Layer Attacks**

In application layer, the virus, repudiation and worm attacks may possible. Malicious software or programs are spread in mobile networks. These virus and worm programs are easily spread one node to another node. The viruses are motivated to crash the entire system or particular data. The virus programs are easily available in today's internet world. The Code Red Worm is one of the powerful worms.

**VII. Multi Layer Attacks**

Some security attacks in MANET from multiple layers. For example, the Denial-of-Service (DoS) is different in each layer. In the application layer the malicious program can directed to DoS. At the transport layer the attacker can hijacking the sessions. In the link-layer, the attacker generates a malicious nodes occupy the channel. In the physical-layer, the attackers used the strong noise signal by using jammers. Other one of the multi-later attacks is man-in-middle attack. The communication between sender and receiver, the third party node should be participate in the communication illegally and modify
VIII. Conclusion

A Mobile Ad-Hoc Network (MANET) is a dynamic wireless network that can be formed without any pre-existing infrastructure in which each node can act as a router. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attacks. Due to the mobility and the open media nature, the mobile ad-hoc networks are more prone to security threats compared to the wired networks. Therefore security needs are higher in mobile ad-hoc networks compared to the traditional networks. In this paper we have investigated different attacks in MANETS that are going to take place in layers. There is a need of comprehensive security solution which can deal with attack the types of attacks. The counter measures of this attacks are specified in the coming journal.

References


Kishore Dasari received his MCA degree from the affiliated college of “ACHARYA NAGARJUNA UNIVERSITY, GUNTUR” and pursuing M.TECH degree from “KL UNIVERSITY, VIJAYAWADA”. His research areas include Cryptography, Mobile Ad Hoc Networks, Computer Networks.

Tammineedi Venkata Satya Vivek was born in 9th October,1990 in Bhimavaram Town. In 2012, he received his B.TECH degree in “Computer Science And Engineering” from the university college affiliated to JNTU Kakinada. Presently he is pursuing his M.TECH degree from “KL UNIVERSITY,VIJAYAWADA”. His research areas include Cryptography, Networks and Image Processing.