A Detail Qualitative Survey on Attacks in Mobile Ad-hoc Networks (MANET)

Himanshi¹, Mintu Singh²

M-Tech. Student, Department of CSE, Echelon Institute of Technology, Faridabad, India¹
Assistant Professor Department of CSE, Echelon Institute of Technology, Faridabad, India²

Abstract: Mobile ad hoc networks (MANET) has risen as a major next generation wireless networking technology. This network is a network of mobile nodes with dynamic structure. Here each node acts as a router for forwarding data to other nodes. Due its dynamic nature, security has become a primary concern to provide protected communication between different nodes in ad hoc networks. There are a number of challenges in security design as ad hoc network is a decentralized network. There are five layers in MANET and each of these layer is vulnerable to various attacks. In this paper we discuss about various attacks and their protection mechanisms.

I. INTRODUCTION

Wireless networks are classified into two broad categories: infrastructure less networks and infrastructure based networks. The infrastructure based networks can make the use of fixed base stations which are responsible for coordinating communication among two or more mobile hosts. Infrastructure less wireless networks is a type of network of mobile nodes with no central coordinator. MANET (Mobile ad-hoc network) comes under the category of infrastructure less or non-infrastructure wireless networks.

The term ad-hoc means temporary i.e. a mobile ad-hoc network is a temporary network of various mobile nodes without any central coordinator [1]. These networks do not depend on any hardware. A MANET is a self-governing network in which each node acts as a router to forward message to other node that are not within the same communication range. MANET follows a dynamic topology because every node always moves arbitrarily in the network [2].

Therefore, a node can change its link to other node frequently. Because of dynamic topology MANET has various applications such as in military area, rescue operations, natural disaster recovery etc. apart from these MANET can also install in the office, home or a small area of city. Though, MANET supports mobility and portability but is more vulnerable and susceptible to various types of security attacks. MANET not only inherits all the security attacks found in both wired and wireless networks, but it also introduces some of the security attacks unique to itself.

With the knowledge of some commonly used attacking schemes, a researcher might have a better understanding of how mobile ad hoc networks could be susceptible to the attackers, and thus leads to the development of more reliable security measures in protecting them [2]. The main aim of this study is to inspect some of the important issues that might be related to security attacks in MANET and some of the existing detection and mitigation schemes [3].

II. ATTACKS IN MANETS

Mobile ad-hoc networks are vulnerable to numerous attacks not only from outside but also from inside i.e. within the network. The attacks in MANET are divided into two major categories:
A. Active Attacks
Active attacks disturb the operation of communication in the network. An active attack could stop the message flow between the nodes. An active attack can modify the data packet or drop the packet in the network. Hence active attacks disturb the normal functionality of a MANET.

2.) Greyhole attack
Greyhole attack is a special kind of blackhole attack. In this attack, an attacker becomes the part of the routes in the network i.e. captures the route then drops data packets selectively [2]. One can’t predict the probability of losing data packets. In greyhole attack, attacker node first agrees to forward packets and then refuses to do so, which leads to dropping of data packets.

The Gray Hole attack has two phases: In the first phase, an attacker node exploits the AODV protocol to act as having a valid route to the destination node, with the goal of interrupting data packets, even though the route is spurious. In the second phase, the attacker node drops the interrupted data packets with a certain probability. Greyhole attack is more difficult to detect as compared to black hole attack in which the attacker node drops the received data packets with certainty.

B. Blackhole attack
In this attack, attacker node announces that it has an optimum route to the node whose packet it wants to use. On receiving side, attacker node sends a fake reply with extremely short route. If the node has been able to make its place between the communicating nodes, then it can do anything with the packets passing between them [1]. A black hole node acts as having a path with the highest sequence number to the destination. The attacker node could use this position in a number of ways. In wormhole attack, it copies the data packets at one location and replays them without any changes at different location or within the same network.

2.) Greyhole attack
Greyhole attack is a special kind of blackhole attack. In this attack, an attacker becomes the part of the routes in the network i.e. captures the route then drops data packets selectively [2]. One can’t predict the probability of losing data packets. In greyhole attack, attacker node first agrees to forward packets and then refuses to do so, which leads to dropping of data packets.

The Gray Hole attack has two phases: In the first phase, an attacker node exploits the AODV protocol to act as having a valid route to the destination node, with the goal of interrupting data packets, even though the route is spurious. In the second phase, the attacker node drops the interrupted data packets with a certain probability. Greyhole attack is more difficult to detect as compared to black hole attack in which the attacker node drops the received data packets with certainty.
4.) Sinkhole attack
In this attack, an attacker node provides wrong routing information in order to present itself a specific node and hence receives the whole network traffic. Once receiving the whole network traffic complicated packet traffic it modifies secret information such change the data or drop the packet to make network complicated. An attacker node tries to attract the secure data from all neighboring nodes.

In Sybil attack, an attacker may create multiple fake identities. The attacker node may present itself as a large number of nodes instead of a single node. These fake identities are called Sybil nodes. This attack may cause a lot of data packets to be routed towards the fake nodes.

5.) Rushing Attack
Rushing attack can also be known as a denial of service attack or novel attack. In rushing attack, an attacker node receives a route request packet from the source node and immediately flood it throughout the network before other nodes which also receive the same route request packet. These attacks are generally against the on-demand routing protocols.

6.) Sybil Attack
In MANET the transmission medium for data packets is air and they doesn’t have a centralized node to control the network. So the routing is based on some unique node address. This property of MANET can be used by the attacker for using fake identities. This means the attacker can either use a random identity or the identity of a legitimate node. This type of attack is known as Sybil attack.

7.) Jellyfish Attack
Jellyfish attack generally comes under the passive attack and also a type of denial of service attack. Jellyfish attack produces delay during the transmission and reception of data packets in the network. This attack is difficult to detect. Jellyfish attack is same as the blackhole attack with the only difference that is in blackhole attack attacker drops all data packets but in jellyfish attack node produces delay during forwarding of data packets.
Attacks at Application Layer

1.) Repudiation attack
Repudiation means denial of transmitting or receiving the data packet. In this type of attack, either a sender may deny that he send the packet or a receiver deny that he receives a data packet.

B. Passive Attacks
A passive attack is an unauthorized listening to the network. It does not change the data transmitted within the network. A passive attacker obtains the data exchanged in the network without disturbing the operation of communication.

Passive attack is difficult to detect because of the network operation itself does not get affected. These attacks can be controlled by using powerful encryption algorithm to encrypt the data which is being transmitted.

Passive attacks are further classified into two categories:

1.) Eavesdropping
Eavesdropping is an interception and reading of messages by an unauthorized receiver. The unintended receiver can easily intercept the communication which is on wireless medium by tuning up to proper frequency. The main aim of eavesdropping which is kept secret during the communication. The secret information can be private key, public key, password.

![Fig : Eavesdropping](image)

2.) Traffic Analysis
In this attack, for an attacker data packets and traffic patterns both are important. The attacker can obtain the confidential information about network topology by analyzing the traffic pattern. Using traffic analysis attack, an attacker may find about network topology, location of nodes, source and destination nodes.

### III. ATTACK DETECTION AND PREVENTION TECHNIQUES

<table>
<thead>
<tr>
<th>TABLE I. BLACKHOLE DETECTION/PREVENTION TECHNIQUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approach</td>
</tr>
<tr>
<td>Reply Packet Authenticity [22]</td>
</tr>
<tr>
<td>Last-Packet-Sequence-Numbers [23]</td>
</tr>
<tr>
<td>Common Neighbor Listening [25]</td>
</tr>
<tr>
<td>Information (DRI) and Cross checking using FREQ and FREP [26]</td>
</tr>
<tr>
<td>Method</td>
</tr>
<tr>
<td>---------------------------------</td>
</tr>
<tr>
<td>Route Confirmation Request-Reply [27]</td>
</tr>
<tr>
<td>Dynamic Training Method [27]</td>
</tr>
<tr>
<td>SAODV [28]</td>
</tr>
<tr>
<td>AODVSABH [29]</td>
</tr>
<tr>
<td>MOSAODV [30]</td>
</tr>
<tr>
<td>DPRAODV [31]</td>
</tr>
<tr>
<td>Voting System [33]</td>
</tr>
</tbody>
</table>

**Notes:**
- Similar kind of approaches might imply that multiple methods have overlapping functionalities.
- Route Confirmation Request-Reply is a mechanism where nodes request confirmation messages to validate their routes.
- Dynamic Training Method could involve analyzing differences between sequence numbers.
- SAODV and AODVSABH are methods that seem to aim at reducing the number of false positives or controlling routes.
- MOSAODV focuses on saving RREP messages in a table after a specific time period.
- DPRAODV introduces a threshold mechanism for determining malicious nodes.
- Voting System involves cooperative voting among nodes to identify suspicious nodes.
<table>
<thead>
<tr>
<th>Approach</th>
<th>Description</th>
<th>Limitations</th>
<th>Approach</th>
<th>Description</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel-aware Detection Algorithm [41]</td>
<td>It uses two strategies for detecting misbehaving nodes: hop-by-hop loss observation by next hop (downstream node) and traffic monitoring by previous hop (upstream node).</td>
<td>Assumption is made that nodes have no energy constraints and source and destination know the forwarding path and IDs of forwarding nodes.</td>
<td>Trust-based approach that uses passive acknowledgement as it is simplest; Uses promiscuous mode to monitor the channel that allows a node to identify any transmitted packets irrelevant of the actual destination that they are intended for; thus, a node can ensure that packets it has sent to a neighboring node for forwarding are indeed forwarded; routing choices are made based on trust as well as hop-count, such that the selected next hop gives the shortest trusted path.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prelude and Postlude Messaging [38]</td>
<td>Before sending any block, source sends a prelude message to destination to alert it; neighbors monitor flow of traffic; after end of transmission, destination sends postlude message containing the number of packets received. If the data loss is out of tolerable range, initiate the process of detecting and removing all malicious nodes by aggregating response from monitoring nodes and the network.</td>
<td>Analysis of the proposed solution has not been done.</td>
<td>It is used only for detecting Packet forwarding misbehavior; monitoring overall traffic would be a better choice than monitoring only one node’s requests.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creating Proof Algorithm, Check up Algorithm and Diagnosis Algorithm [35,36]</td>
<td>Each node involved in a session must create a proof that it has received the message; When source node suspects some misbehavior, Checkup algorithm checks intermediate nodes; According to the facts returned by the Checkup algorithm, it traces the malicious node by Diagnosis algorithm.</td>
<td>May not detect all Malicious nodes.</td>
<td>One-way hash code is added to the data packets; when receiver receives packet, it checks the correctness of it by finding match of hash code; for correct data packet, it sends ACK to sender which checks the ACK is received within specific time; for incorrect packet receiver sends CONFIDENTIALITY LOST through intermediate nodes and sender switches to alternative intermediate node to send Packets.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The solution is not tested with higher density of nodes and adds to the routing overhead. |

| End-to-end | Source and destination nodes | May not work with many |

Simple acknowledgement and flow conservation [2] One-way hash code is added to the data packets; when receiver receives packet, it checks the correctness of it by finding match of hash code; for correct data packet, it sends ACK to sender which checks the ACK is received within specific time; for incorrect packet receiver sends CONFIDENTIALITY LOST through intermediate nodes and sender switches to alternative intermediate node to send Packets. | The solution is not tested with higher density of nodes and adds to the routing overhead. |
IV. CONCLUSION AND FUTURE WORK

The dynamic nature of MANET makes it vulnerable to attacks at different layers. One of the mostly attacked MANET layer is network layer. So, there is a need for secure environment for transmission of secure communications. In this paper, I have done a survey on network layer attacks and their possible detection mechanism. In future there can be several ways to defeat these protection mechanisms. So this is a further more potential area of research in which more powerful detection mechanisms can be invented.

REFERENCES


