Analysis and Prevention of Security Issues in Manets

Jyoti Goyat¹, Bhanu Priya², Swati³
¹Guru Jambheshwar University, INDIA
²,³Department of CS, C.R.M. Jat P.G College Hisar, INDIA

ABSTRACT

Security is a paramount concern in mobile ad hoc network (MANET) because of its intrinsic vulnerabilities. These vulnerabilities are nature of MANET structure that cannot be removed. As a result, attacks with malicious intent have been and will be devised to exploit these vulnerabilities and to disturb MANET operations. In this paper, we analyze the security problems in MANET, security threats and present a few detection and prevention directions. As MANET is quickly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication.

Keywords: Mobile ad hoc networks, routing protocols, nodes

I. INTRODUCTION

Wireless Mobile Ad-hoc Networks (or simply MANET) are networks consisting of entirely mobile nodes that communicate with each other on-the-move without base stations. This technology, is a self-configuring infrastructure less network of mobile devices connected by wireless links that provides convenient communications and could be very useful to for many applications especially when the infrastructure networks is not feasible.

MANETS are often defined as follows “mobile adhoc network is an autonomous system of mobile routers and associated hosts connected by the wireless links -the union of which forms an arbitrary graph”. The routers are free to move randomly and organize themselves arbitrarily on which bases the network wireless topology may change rapidly and unpredictably.

With the increase of portable devices as well as progress in wireless communication, ad hoc network is gaining importance with the increasing number of widespread applications. Ad-hoc network can be applied anywhere where there is little or no communication infrastructure or existing infrastructure is expensive or inconvenient to use. The set of applications for MANET is ranging from large scale, mobile, highly dynamic networks to small static networks that are constrained by power sources. The different types of MANET applications include:

- Search and rescue operations
- Sensor networks
- Automotive Applications
- Military battlefield

MANETS having lots of features which are being described as follows:

- Autonomous terminal: A node may function as both host and a router.
• Distributed Operations: since there is no fixed network the control and management operations are distributed among the terminals.
• Multi-hop routing: multi hop routing involves traversing multiple links to reach destination.
• Dynamic network topology: Because of mobile nodes network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time.
• Energy-constrained operation: Some or all of the nodes in MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

This paper is divided into different sections. Section II consists of Problem definition. Section III describes the security challenges in Mobile Ad hoc networks. Section IV consists security issues. After that section V describes the security approaches for detection and prevention. Security requirements based on approaches are classified in section VI. Finally, the paper conclusion is being defined in section VII.

II. PROBLEM DEFINITION

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. Wireless links also 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. Due to the security vulnerability of the routing protocols MANET is unprotected against attacks by the malicious nodes. Wormhole attack against the network integrity absorbs all the packets in the network. Since the data packets do not reach the destination node, so data loss will occur. As well as it degrades the performance of the network in terms of packet loss, throughput, end-to-end delay and network load.

III. SECURITY CHALLENGES IN MANET

Security in MANET is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assured that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats. MANETs are very flexible for the nodes i.e. nodes can freely join and leave the network. There is no main body that keeps watching on the nodes entering and leaving the network. All these weaknesses of MANETs make it vulnerable to attacks and these are discussed below.

• Non secure boundaries: MANET is vulnerable to different kind of attacks due to no secure boundary. The nature of MANET, nodes have the freedom to join and leave inside the network. Node can join a network automatically if the network is in the radio range of the node, thus it can communicate with other nodes in the network. Due to no secure boundaries, MANET is more susceptible to attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity. There is no protection against attacks like firewalls or access control, which may result the vulnerability of MANET to attacks[1].
• Compromised Node: Some of the attacks are to get access inside the network in order to get control over the node in the network using unfair means to carry out their malicious activities. Mobile nodes in MANET are free to move, join or leave the network in other words the mobile nodes are autonomous[2]. Due to this autonomous factor for mobile nodes it is very difficult for the nodes to prevent malicious activity it is communicating with. Ad-hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity.
• No Central Management: MANET is a self-configurable network, which consists of Mobile nodes where the communication among these mobile nodes is done without a central control. Each and every node act as router and can forward and receive packets[3]. MANET works without any preexisting infrastructure. This lack of centralized management leads MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly dynamic and for large scale ad hoc network is very difficult due to no central management.
• Problem of Scalability: In traditional networks, where the network is build and each machine is connected to the other machine with help of wire. The network and the scale of the network, while designing it is defined and that do not change much during the use. In other words we can say that the scalability of the network is defined in the beginning phase of the designing of the network. The case is quite opposite in MANETs because the nodes are mobile and due to their mobility in MANETs, the scale of the MANETs is changing. It is too hard to know and predict the numbers of nodes in the MANETs in the future. The nodes are free to move in and out of the ad hoc network which makes the ad hoc network very much scalable.

IV. SECURITY ISSUES IN MANETS

a) Security threat: An action taken against a target with the intention of doing harm is security threat in MANETs[8][9].

External attacks are carried out by nodes that do not belong to the domain of the network. It causes congestion, sends false routing information or causes unavailability of services.
**Internal attacks** are from compromised nodes or malicious nodes, which are actually part of the network. In an internal attack, the malicious node from the network gains unauthorized access, analyzes traffic between other nodes and may participate in other network activities.

**Passive attack**: A passive attack does not alter the data transmitted within the network. But it includes the unauthorized “listening” to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to gather information about the network and communication patterns between the communication parties.

**Active attack** involves information interruption, modification or fabrication thus disrupting the normal functionality of MANET. The information which is routing through the nodes in MANET is altered by an attacker node. Attacker node also streams some false information in the network [11][12].

<table>
<thead>
<tr>
<th>Passive Attacks</th>
<th>Eavesdropping, traffic analysis, monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Attacks</td>
<td>Jamming, spoofing, modification, replaying, DoS</td>
</tr>
</tbody>
</table>

Table: shows security attacks classification.

**b) MANET Routing Protocol:**

- **Proactive routing or Table driven routing protocols**: In these routing protocols each node in the network refreshes its routing information of the network so that every node can operate with consistent and up-to-date routing tables and when a node needs to send some data or information then there is minimum delay but substantial fraction of control information for discovering the route in the whole network. Examples for these protocols are DSDV, WRP, OLSR, TBRPF etc[6].

- **Reactive routing or On-Demand routing protocols**: In these routing protocols, nodes do not periodically update the routing information but maintain routes information to get destination when it needs to send required data packets. These protocols consume much less bandwidth. Examples that can be considered for reactive routing are DSR, AODV, TORA etc[6].

- **Hybrid routing protocols**: In this type of routing protocol is the combination of the above two categories. They typically offer means to switch dynamically between the reactive and proactive parts of the protocol. For instance, table-driven protocols could be used between networks and on-demand protocols inside the networks or vice versa.

**c) Routing Protocol Attacks**: Routing is one of the most vital mechanisms in the ad hoc networks. Improper and insecure routing mechanisms render such networks vulnerable to many security attacks. One of the basic elements in the routing mechanism is the routing message, which is used to establish and maintain relationships between nodes in the networks. The importance of the routing message has made it a main target for the attackers to launch attacks against the ad hoc networks. Attacks against the routing messages could be launched in many forms[10].

  i) **Attacks using Modification**: In case of modification type of attacks, attackers make some changes to the routing messages and passed among the nodes, due to this way it become the cause of traffic subversion, as well as traffic redirection and also act as a Denial of Service (DoS) attacks. There are some of these types of attacks are given below:

  • Route sequence numbers modification: In this case an attacker (i.e. malicious node) used to modify the sequence number in the route request packets.

  • Hop count modification attack: In this case attacker mostly changes hop count value and due to this way it will become the cause of attract traffic. They are mainly used to include new routes in order to reset the value of hop count field to a lower value of a RREQ (route request) packet or sometime even it is used to set to zero.

  • Source route modification attack: In this type of attack, attacker (malicious node) modifies source address and move traffic towards its own destination.

  ii) **Attacks using Fabrication**: In this type of attacks, where an attacker as a malicious node try to inject wrong messages or fake routing packets in order to disrupt the routing process and malicious nodes also could fabricate their own packets to cause chaos in the network operations. The fabrication attacks are very much difficult to detect in the MANETs. Attacks using fabrication process are discussed very well in [5] and [6].

  • Sleep deprivation attacks: The aim is to drain off limited resources in the mobile ad hoc nodes (e.g. the battery powers), by constantly makes them busy processing unnecessary packets. Sleep deprivation attacks might be launched by flooding the targeted node with unnecessary routing packets.
In fabrication attack: A malicious node can also attempt to create routes to nodes that do not exist. As a result the routing table of nodes are full and do not register the new routes and this attack is effective in table driven protocol where every node keeps an up to date route to all the other nodes in network.

iii) Spoofing: This occurs when a malicious node pretends other node’s identity at times. This in turn misguides a non-malicious node in order to alter the vision of the network topology that it can gather.

iv) Rushing: An offensive that can be carried out against on-demand routing protocols is the rushing attack. Typically, on-demand routing protocols state that nodes must forward only the first received Route Request from each route discovery; all further received Route requests are ignored. An attacker which receives a route request packet from the initiating node floods the packet quickly throughout the network before other nodes which also receive the same route request packet can react.

d) Attacks at different layers of network

The characteristics of MANETs make them susceptible to many new attacks. These attacks can occur in different layers of network model.

<table>
<thead>
<tr>
<th>Layers</th>
<th>Types of Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Malicious code, Data corruption, viruses and worms</td>
</tr>
<tr>
<td>Transport</td>
<td>Session hijacking attack, SYN Flooding</td>
</tr>
<tr>
<td>Network</td>
<td>Blackhole, wormhole, Sinkhole, Link spoofing, Rushing Attack, Replay attacks, Sybil attack</td>
</tr>
<tr>
<td>Data</td>
<td>malicious behavior, traffic analysis</td>
</tr>
<tr>
<td>Physical</td>
<td>Eavesdropping, jamming,</td>
</tr>
</tbody>
</table>

Table: Layers of the network protocol stack.

V. SECURITY APPROACHES

Fundamental challenges in security design for MANET is to maintain network performance with full security strength, because when more security features are introduced in the network, increases computation, communication and management overhead which can affect the network performance. Security involves two approaches:

- Proactive: This approach attempt to the security threats in the first place through various cryptographic techniques.
- Reactive: First detect the threat then react accordingly. Due to the absence of a clear line of defense, a complete security solution for MANET should involve both approaches. So the way to check the security is Prevention, Detection and Reaction.

Try to increase the difficulties for the attacker to penetrate the system but intrusion free system is not feasible, so the detection component play an important role to detect the attacker so that proper action can be taken to avoid persistent adverse effects. Prevention can be achieve by secure Adhoc routing protocols that prevent the attackers from installing incorrect routing states at other nodes. These protocols employ different cryptographic primitives:

- HMAC (Message authentication codes)
- Digital Signature
- Hash Chain

Because the wireless channel is open, each node can perform localized detection by overhearing ongoing transmission and evaluating the behavior of its neighbors but its accuracy is limited by a no. of factors such as channel error, interference and mobility. A malicious node may also abuse the security solutions and intentionally accuse legitimate nodes, In order to address such issues, the detection results at individual nodes can be integrated and refined in a distributed manner to achieve consensus among a group of nodes. An alternative approach relies on explicit acknowledgement from the destination and/or intermediate nodes to the source so that the source can figure out where the packet was dropped. Once a malicious node is detected certain actions are triggered to protect the network from future attacks launched by this node the reaction component is related to the prevention component in the security system. Once multiple nodes in a local neighborhood have reached consensus that one of their neighbors is malicious, they collectively revoke the certificate of the malicious node. The malicious node is isolated in the network as it cannot participate in the routing or packet forwarding operations in the future. The path rater allows each node to maintain its own rating for every other node it knows about. A node slowly increases the rating of well-behaved nodes overtime, but dramatically decreases the rating of a malicious node that is detected by its watchdog. Based on rating source always selects the path with the highest average rating.

VI. SECURITY REQUIREMENTS IN MANETs

There are different security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment that are being described as follows. These mechanisms prevent, detect, and respond to security attacks [4].

- Availability ensures the survivability of network services despite denial of service attacks. It assures that the services of the system are available at all times and are not denied to authorize users. A denial of service attack could be launched at any layer of an ad hoc network.
- Confidentiality ensures that certain information is never disclosed to unauthorized entities. In MANETs, this is
more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed.

- **Integrity** guarantees that a message being transferred is never corrupted. And Message being transmitted is never altered. A message could be corrupted because of being failures, such as radio propagation impairment, or because of malicious attacks on the network.

- **Authentication** Assure that an entity of concern or the origin of a communication is what it claims to be or from. It enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

- **Non-repudiation** ensures that sending and receiving parties can never deny ever sending or receiving the message. Non-repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.

**VII. CONCLUSION**

MANETs is a growth area of research. The paper inspects the security issues in the mobile ad hoc networks, which may be a main disturbance to its operation. To accomplish this goal, a study is being done in gathering information related to various types of attacks and solutions. Due to the mobility and open media nature, the mobile ad hoc networks are more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network.

MANET has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. Security of MANET is one of the important features for its deployment. Finally the paper analyzed the behavior and challenges of security threats in mobile ad hoc networks with prevention and detection.

However, in short, this paper concluded that the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET.

**REFERENCES**