SURVEY ON ATTACKS AND SECURITY ISSUES IN MOBILE Ad Hoc NETWORKS

1 S. Sandhya Rani
B.Tech, M.Tech, (Phd)
Assistant Professor
Department of CSE
MREC(A)-Hyderabad

2 Dr. G. Apparao Naidu
B.Tech, M.Tech, Phd
Professor
Department of CSE
JBIT- Hyderabad

3 Dr. V. UshaShree
B.Tech, M.Tech, Phd
Professor
Department of ECE
VJIT-Hyderabad

Abstract: Mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. In this paper, the security issues and their current solutions in the mobile ad hoc network have been discussed. Owe to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. We first analyze the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. Then we discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally we survey the current security solutions for the mobile ad hoc network.

Key Words: Mobile Ad Hoc Network, Security, Intrusion Detection, Secure Routing

1. Introduction
An autonomous system of mobile hosts connected by wireless links, often called Mobile Ad hoc Networks’ (MANETs). Recent computer networks have introduced a new technology for future wireless communication, a mobile ad hoc network (MANET). Ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. Nodes in ad hoc network are mobile and they can communicate with each other within radio range through direct wireless links or multichip routing. Mobile ad hoc networks (MANETs) represent complex distributed systems that comprise wireless mobile nodes.
that can freely and dynamically self-organize into arbitrary and temporary, “ad-hoc” network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure “

**Characteristics of MANET**

1. No fixed infrastructure
2. Dynamic changing topology Mobile devices join/leave the network unexpectedly they can also move freely
3. Energy-constrained
4. Limited bandwidth
5. Each node also serves as router Help to relay packets received from neighbors

**Interoperation with the Internet**

---

2. **Security issues in Mobile Ad Hoc Network**

**Availability:** ensures the survivability of network services despite denial of service attacks.

**Authentication:** enables a node to ensure the identity of the peer node it is communicating with.

**Non-repudiation:** ensures that the origin of a message cannot deny having sent the message.

**Confidentiality:** Ensures that secret information or data is never disclosed to unauthorized devices.

**Integrity:** Ensures that a message received is not corrupted.

---

### Table: Security issues

<table>
<thead>
<tr>
<th>Layer</th>
<th>Security issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Detecting and preventing viruses, worms, malicious</td>
</tr>
<tr>
<td></td>
<td>codes, and application abuses</td>
</tr>
<tr>
<td>Transport</td>
<td>Authenticating and securing end-to-end communications</td>
</tr>
<tr>
<td></td>
<td>through data encryption</td>
</tr>
<tr>
<td>Network</td>
<td>Protecting the ad hoc routing and forwarding protocols</td>
</tr>
<tr>
<td>Link</td>
<td>Protecting the wireless MAC protocol and providing</td>
</tr>
<tr>
<td></td>
<td>link-layer security support</td>
</tr>
<tr>
<td>Physical</td>
<td>Preventing signal jamming denial-of-service attacks</td>
</tr>
</tbody>
</table>

---

**Fig 1:- Example MANET**
Table 1: Security Issues in Mobile Ad Hoc Network

Threats
- Attacks
  – External attacks
  – Internal attacks
  – Passive attacks
  – Active attacks
- Misbehavior

3. Threats from Compromised nodes Inside the Network

In this section we discussed about the link attacks the link attacks place their emphasis on the links between the nodes, and try to perform some malicious behaviors to make destruction to the links. However, there are some other attacks that aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further malicious actions. This vulnerability can be viewed as the threats that come from the compromised nodes inside the network.

Since mobile nodes are autonomous units that can join or leave the network with freedom, it is hard for the nodes themselves to work out some effective policies to prevent the possible malicious behaviors from all the nodes it communicate with because of the behavioral diversity of different nodes. Furthermore, because of the mobility of the ad hoc network, a compromised node can frequently change its attack target and perform malicious behavior to different node in the network, thus it is very difficult to track the malicious behavior performed by a compromised node especially in a large scale ad hoc network. Therefore, threats from compromised nodes inside the network are far more dangerous than the attacks from outside the network, and these attacks are much harder to detect because they come from the compromised nodes, which behave well before they are compromised.

3.1 Vulnerabilities of the Mobile Ad Hoc Networks

As per previous discussion we can conclude that the mobile ad hoc network is insecure by its nature: there is no such a clear line of defense because of the freedom for the nodes to join, leave and move inside the network; some of the nodes may be compromised by the adversary and thus perform some malicious behaviors that are hard to detect; lack of centralized machinery may cause some problems when there is a need to have such a centralized coordinator; restricted
power supply can cause some selfish problems; and continuously changing scale of the network has set higher requirement to the scalability of the protocols and services in the mobile ad hoc network. As a result, compared with the wired network, the mobile ad hoc network will need more robust security scheme to ensure the security of it. In the next section, we will survey several security solutions that can provide some helps to improve the security environment in the ad hoc network.

Security Challenges of MANATS

1. Channel vulnerability – broadcast wireless channels allow message eavesdropping and injection easily.

2. Node vulnerability – nodes do not reside in physically protected places, thus easily fall under attack.

3. Absence of infrastructure – certification/ authentication authorities are absent.


5. Power and computational

Types of Attacks

There are two types of security attacks:

- passive
- Active

- In a passive attack, a malicious node either ignores operations supposed to be accomplished by it (examples: silent discard, partial routing information hiding), or listens to the channel, attempting to retrieve valuable information (example: eavesdropping).

- In a active attack, information is inserted to the network and thus the network operation or some nodes may be harmed. Examples are impersonation/spoofing, modification, fabrication and disclosure attack.

Fig :- 2 Rush Attacks in example mobile Ad Hoc Networks

4. Security criteria
Availability
The term *Availability* means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service.

Integrity
Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways:

- Malicious altering
- Accidental altering

A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

Authenticity
Authenticity is essentially assurance that participants in communication are genuine and not impersonators. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

Authorization
Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

Anonymity
Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be
kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

Security Criteria: Summary

We have discussed several main requirements that need to be achieved to ensure the security of the mobile ad hoc network. Moreover, there are some other security criteria that are more specialized and application-oriented, which include location privacy, self-stabilization and Byzantine Robustness, all of which are related to the routing protocol in the mobile ad hoc network. Having dealt with the main security criteria, we then move to the discussion on the main threats that violate the security criteria, which are generally called as attacks.

5. Security Solutions to the Mobile Ad Hoc Networks

We have discussed several vulnerabilities that potentially make the mobile ad hoc networks insecure in the previous section. However, it is far from our ultimate goal to secure the mobile ad hoc network if we merely know the existing vulnerabilities in it. As a result, we need to find some security solutions to the mobile ad hoc network. In this section, we survey some security schemes that can be useful to protect the mobile ad hoc network from malicious behaviors.

Fig 3: Combined mechanism to secure MANET

Denial of Service attack

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. A denial of service (DoS) attack is an attack that clogs up so much memory on the target system that it cannot serve its users, or it causes the target system to crash, reboot, or otherwise deny services to legitimate users. These days, DoS attacks are very common; indeed, just about every server is bound to experience such an attack at some time or another. Denial of Service can easily be launched and flood the network with spurious routing messages through a malicious node.
that gives incorrect updating information by pretending to be a legitimate change of routing information. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

6. Conclusion
Finally we conclude one can see that attacks against the ad hoc networks may vary depend on (1) which environment the attacks are launched, (2) what communication layer the attacks are targeting, and (3) what level of ad hoc network mechanisms are targeted and we try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Due to the mobility and open media nature, the mobile ad hoc networks are much 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. First we briefly introduce the basic characteristics of the mobile ad hoc network. 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.

7. References
2. S. A. Razak, S. M. Furnell, P. J. Brooke, Attacks against Mobile Ad Hoc Networks Routing Protocols”