Vol. 1, Issue III, April 2013
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Security of Mobile Ad-hoc Networks- A Challenging Task

Sandeep[1], Rupesh Kumar[2], Raksha[3]

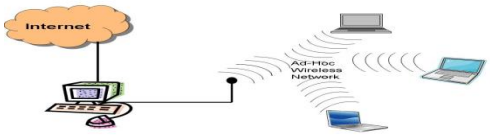
[1]M.Tech (CSE), Department of Computer Science and Application
KU, Kurukshetra, India.
[2]M.Tech (CSE), Department of Computer Science and Application
KU, Kurukshetra, India.
[3]M.Tech (CSE), Department of Computer Science and Application
KU, Kurukshetra, India.
angel.boy0702@gmail.com[1], rupeshdagar@gamil.com[2], raksha.sindhu23@gmail.com[3]

Abstract: *Low prices and high data rates of wireless communication devices like wireless modems and wireless LANs has led to the rapid growth of mobile computing as well as Ad-hoc networks in the last few years. Security is a core issue with mobile ad-hoc networks because all the network services are configured on the fly. MANETS are vulnerable to security threats due to their inherent characteristics of Open medium, Dynamic Topology and Lack of centralized control. This paper firstly focuses on the security criteria of mobile networks. Then we learn about the main attack types that exist in it. Finally at the end a survey of current security solutions to rectify these attacks is presented.*

Keywords: *Mobile Ad Hoc Network, Dynamic Firewall, Secured Network Architecture, Security, Intrusion Detection, Secure Routing.*

1. INTRODUCTION

A mobile ad-hoc network is collection of mobile/semi mobile nodes, forming a temporary network. Each node in such a network has a transmission range, which is limited by the transmission power, attenuation and interference. Each of the nodes has a wireless interface and communicates with each other over either radio or infrared. Laptop computers or personal digital assistants that communicate directly with each other are some examples of nodes in ad-hoc network. Nodes in ad-hoc network are often mobile, but can consist of stationary nodes, such as access points to internet. In MANETs, each node operates as an end system and a router for all other nodes in the network discovering their communication routes by themselves.



Example of Ad-hoc Networks

It is a temporary network that can be established on demand and disappears when there is no need. Nodes in MANET are free to move and organize themselves in arbitrary fashion. Mobile Ad-hoc networks take advantages of wireless communication medium.

Characteristics of Mobile Ad-hoc Networks: The salient characteristics of ad-hoc network are as follows:

- **Dynamic Topologies:** In MANETs, nodes can join and leave the network dynamically and can move independently [1].
- **Wireless Links:** As the nodes in such networks are interconnected through wireless interface that makes it highly susceptible to link attacks.
- **Cooperativeness:** In MANETs, some nodes may become malicious nodes which disrupt the network operation by changing routing information etc [2].
- **Bandwidth Constrained and Variable Capacity Links:** These networks possess significantly lower capacity than infrastructure based networks.
- **Energy Constrained Operation:** A great limitation to the lifetime of these networks is

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

the energy possessed by them in terms of batteries or other exhaustible means.

- **Limited Physical Security:** Mobile wireless networks are more prone to physical security threats than wired networks. There is increased possibility of eavesdropping, spoofing, and denial-of-service type attacks.

A. Security Issues:

There were so many research areas in MANET in that security is the major concern among others. The scope of securing MANET is mentioned here:

- ✓ Securing MANETs is great challenge for many years due to the absence of proper infrastructure and its open type of network.
- ✓ Previous security measures in MANETs are not effective in the challenging world with advancement in technology.
- ✓ Many layers often prone to attacks man in middle attack or multilayer attack, so proposal should concentrate on these layers.
- ✓ The proper intelligent approach of securing MANETs has not yet discovered.

Theft is likely to occur with wireless devices because of their ability of being portable. Fraud and theft may be committed by authorized and unauthorized people; however, authorized users are more likely to carry out such acts. Malicious hackers, called as crackers sometimes, are individuals who break into a system without authorization, for personal gain or to do harm [3]. Malicious hackers are individuals from outside of an agency or organization. Such hackers may gain access to the wireless network access point by eavesdropping on wireless device communications. Theft of service occurs when an unauthorized user gains access to the network and consumes network resources [4].

2. SECURITY ATTACKS IN MANETS

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on mechanisms of the ad hoc network such as routing. Whereas the second level of attacks damages the security mechanisms employed in the network. The attacks in Mobile Ad-hoc networks are divided into two major groups.

A. Internal Attacks

Internal attacks directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes[1,2].

B. External attacks

These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc [2]. External attacks prevent the network from normal communication. External attacks can be classified into two categories:

1) Passive attacks

A passive attack is one that doesn't 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 discover the important information from routed traffic [2, 5, and 6].

2) Active Attacks

Active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks [2, 7, 10]. These attacks generate unauthorized access to network that helps the attacker to make effects like DoS effect, congestion, modification of packets etc.

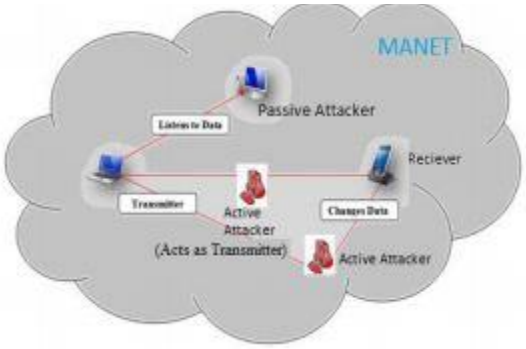


Figure 1: Active and Passive attacks in MANETs

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Active attacks are classified as:

- **Dropping Attacks:** Compromised nodes or selfish nodes can drop all packets that are not destined for them. These attacks can prevent end-to-end communication between nodes, if the dropping node is at a critical point [5].
- **Modification Attacks:** These attacks modify packets and disrupt the overall communication between network nodes. E.g.: Sinkhole attacks
- **Fabrication Attacks:** In fabrication attack, the attacker send fake message to the neighboring nodes without receiving any related message.
- **Timing Attacks:** In this category of attacks, attackers make other nodes attracted towards it by advertising itself as a node closer to the actual node.

3. TYPES OF ACTIVE ATTACKS ON VARIOUS LAYERS IN PROTOCOL STACK

These attacks can occur in different layers of the network protocol stack.

Table 1: Attacks on the Protocol Stack

Layer	Types of Attacks
Application	Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attack, SYN Flooding attack
Network	Blackhole, wormhole, Sinkhole, Link spoofing, Rushing Attack, Replay attacks, Link Withholding, Resource Consumption Attack, Sybil attack
Data Link	Selfish misbehaviour, malicious behaviour, traffic analysis
Physical	Eavesdropping, jamming, active interference

A. Attacks at Physical Layer

The attacks on physical layer are hardware oriented and they need help from hardware sources to come into effect [7]. Some of the attacks identified at physical layer include interference, jamming, eavesdropping etc.

1) Eavesdropping

Eavesdropping can also be defined as interception and reading of messages and conversations by unintended receivers [7].

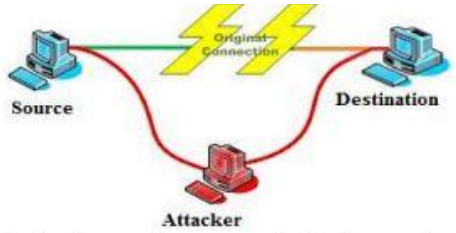


Fig 2: Attacker attack on communication between Source and destination

2) Jamming

Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. In this type of attack, the jammer transmits signals along with security threats.

3) Active Interference

An active interference is a denial of service attack in which Attacker can change the order of messages or attempt to replay old messages. [7]

B. Attacks at Data link / MAC layer

MAC layer attacks can be classified as to what effect it has on the state of the network as a whole.

1) Selfish Misbehavior of Nodes

Attacks under this category, directly affects the self performance of nodes and does not interfere with the operation of the network [7]. It may include two important factors.

- Conservation of battery power
- Gaining unfair share of bandwidth

2) Malicious Behavior of nodes

The aim of malicious node is to disrupt normal operation of routing protocol. Attacks of such type are fall into following categories.

- **Denial of Service (DoS):** These types of threats produced a malicious action with the help of compromised nodes that forms

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

severe security risks. The compromised route appears like a normal route but leads to severe problems.

- **Attacks on Network integrity:** Network integrity is an important issue, in order to provide secure communication and quality of service in network.
- **Misdirecting traffic:** A malicious node advertises wrong routing information in order to get secure data before the actual route.

3) Traffic Analysis

Traffic analysis in ad hoc networks may reveal following type of information.

- Location of nodes
- Network topology being used.
- Roles played by nodes
- Available source an destination nodes

C. Attacks at Network Layer

The network layer protocols enable the MANET nodes to be connected with another through hop-by-hop [5, 7]. The basic idea behind network layer attacks is to inject itself in the active path from source to destination or to absorb network traffic.

1) Black hole Attack

The black hole attack has two properties. (1) the node exploits the mobile ad hoc routing protocol such as AODV to advertise itself as having a valid route to a destination node even though the route is spurious (2) the attacker consumes the intercepted packets without forwarding any one of them.

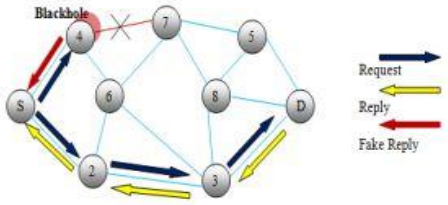


Fig 4: Blackhole Attack

2) Wormhole Attack

An attacker records packets at one location in the network and tunnels them to another location.

3) Byzantine Attack

A compromised intermediate node alone or a set of compromised intermediate nodes carry out attacks such as creating routing loops forwarding packets through non-optimal paths or selectively dropping packets.

4) Resource Consumption Attack

This is also known as the sleep deprivation attack. An attacker can attempt to consume battery life by requesting excessive route discovery or by forwarding unnecessary packets to the victim node.

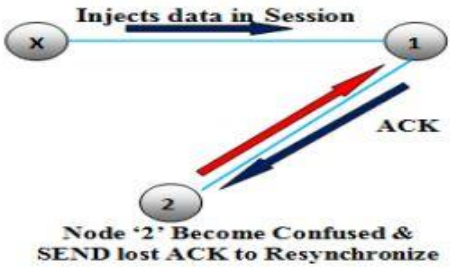
5) Routing Table Overflow Attack

To make routing table overflow attack a success, the attacker tries to create routes to nonexistent nodes to the authorized nodes present in the network.

D. Attacks at Transport Layer

1) Session Hijacking

Session hijacking has a plus point that most communications are protected at session setup but not thereafter. In the TCP session hijacking attack the attacker spoofs the victims IP address, determines the correct sequence number that is expected by the target and then performs a DOS attack on the victim.



2) SYN Flooding Attack

The SYN flooding attacks are the type of (DoS) attacks, in which attacker creates a large number of half opened TCP connection with victim node. These half opened connection never completes the handshake to fully open the connection.

E. Attacks at Application Layer

Application layer protocols are also vulnerable to many DoS attacks. It supports protocols such as HTTP, SMTP, TALNET and FTP, which provides many vulnerabilities and access points for attackers.

1) Malicious code attacks

Malicious code attacks include worms, spywares, Viruses, and Trojan horses, all can attack both operating system and user application.

2) Repudiation attacks

Repudiation refers to a denying participation in all or part of the communications.

4. COUNTERMEASURES

Network operation can easily be put in danger if countermeasures are not imparted. Hence a variety of

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

security mechanisms have been developed to prevent various malicious attacks. These are as described below:

Preventive Mechanism

In preventive mechanism the conventional approaches such as authentication access control encryption and digital signature are used to provide first line of defense.

Reactive Mechanism

Reactive mechanism uses the schemes like intrusion detection system (IDS), cooperation enforcement mechanisms, dynamic firewall etc. in MANET.

COUNTERMEASURES AT PHYSICAL LAYER

Spread spectrum technologies can be used to make it difficult to detect or jam signals. They changes frequency in a random fashion or spread it to a wider spectrum that makes the capture of signal difficult. The FHSS [8] (Frequency Hopping Spread Spectrum) makes the signal unintelligible to the eavesdroppers. On the other hand DSSS [7] (Direct Sequence Spread Spectrum) represents each data bit in the original signal by multiple bits in the transmitted signal.

COUNTERMEASURES AT DATA LINK LAYER

Link layer protocols help to discover one hop neighbors, help in handling fair channel access frame error control and in maintaining good neighbor connections. Moreover, Selfish nodes could disobey the channel access rule cheat back-off values and so on in order to maximize their own throughput. Neighbors should keep a vigil over these misbehaviors. Here attack occurs in IEEE 802.11 MAC protocols. A security extension to 802.11 is proposed in[9]. The original 802.11 back-off scheme is modified in such a way that the receiver instead of setting an arbitrary timer value on its own provides the back-off timer at the sender. Encryption of the frames at data link layer prevents traffic analysis.

COUNTERMEASURES AT NETWORK LAYER

.A variety of security threats are imposed in this layer. First line of defense is there with the use of Routing protocols. The active attack like modification of messages during routing can be prevented through source authentication and message integrity mechanism. For example: message authentication code, digital signature, hash functions etc. is used for this purpose. IPSec is most commonly used on the network layer in Internet that could be used in MANET to provide certain level of confidentiality.

COUNTERMEASURES AT TRANSPORT LAYER

Transport layer is vulnerable against SYN flooding attack and session hijacking attack. Secure Socket Layer (SSL) [10] Transport Layer Security (TLS) [10] and Private Communications Technology (PCT) [10] protocols were designed on the basis of public key cryptography to prevent these attacks.

- ✓ **SSL**

SSL is an Internet protocol that provides authenticity and secrecy for session based communication. The security model of SSL is that it encrypts the channel by enciphering the bits that go through that channel. The operation of SSL involves a combination of public key cryptography and secret key encryption to provide data confidentiality through encryption.

- ✓ **TLS**

TLS is almost identical to Secure Sockets Layer version 3 (SSLv3). TLS differs from SSL in only the following ways:

- The protocol can be extended by adding new authentication methods to its operation.
- It improves performance over SSL by using session caching.

- ✓ **PCT**

PCT was a variant of SSL version 2. Like SSLv2 PCT operated TCP for reliable network connections and could be used both for authenticating communication sessions and for encrypting data to ensure the privacy of such sessions.

COUNTERMEASURES AT APPLICATION LAYER

Firewall provides protection against some of these attacks. Use of Anti-spyware software can detect spyware and malicious programs running on the system. Another mechanism called Intrusion Detection System (IDS) is effective to prevent certain attacks such as trying to gain unauthorized access to a service pretending like a legitimate user etc.

5. CONCLUSION

Security is the main issue in Mobile Ad hoc Networks. In this report the various attacks at different layers in MANET are discussed earlier and then the countermeasures against these attacks are

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

studied. The attacks and countermeasures at various layers in MANET are summarized in Table.

Layers	Attacks	Solutions
Physical Layer	Jamming, Interception, Eavesdropping	Using spread spectrum mechanisms e.g. FHSS, DSSS etc.
Data Link Layer	Traffic Analysis Disruption MAC WEP weakness	Traffic padding traffic Routing, Modify Back-off mechanism.
Network layer	Routing Protocol attacks Wormhole, blackhole, Byzantine Flooding, resource consumption impersonation, location disclosure attacks etc.	Source authentication and message integrity mechanisms to prevent routing message modification SAODV SAR ARAN to overcome blackhole impersonation attacks.
Transport Layer	Session hijacking attack, SYN flooding attack.	Authentication and securing end-to-end or point-to-point communication SSL TLS SET PCT etc.
Application Layer	Repudiation	Code cooperation enforcement mechanisms, firewalls, IDS etc.

REFERENCES

[1] **Mohammad Ilyas, "The Handbook of Ad Hoc Wireless Networks",**

[2] **Amitabh Mishra, "SECURITY AND QUALITY OF SERVICE IN AD HOC WIRELESS NETWORKS" (chapter 1, 3), ISBN- 13 978-0-521-87824-1 Handbook.**

[3] **NIST Special Publication 46, Security for Telecommuting and Broadband Communications, National Institute for Standards and Technology.**

[4] **Norton, P., and Stockman, M. Peter Norton s Network Security Fundamentals. 2000.**

[5] **Ad hoc network specific attacks held by Adam Burg**

[6] **Panagiotis Papadimitratos and Zygmunt J. Haas "Securing Mobile Ad Hoc Networks".**

[7] **Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta,"Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks a Survey"**

[8] **W. Stallings Wireless Communication and Networks Pearson Education 2002.**

[9] **P. Kyasanur and N. Vaidya Detection and Handling of MAC Layer Misbehavior in Wireless Networks DCC 2003.**

[10] **Sean Convery Network Security Architectures Cisco Press 2004.**