IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

A literary review of MANET security

Nitika Sharma
nitika108.ns@gmail.com
J. C. Bose University of Science and Technology,
YMCA, Faridabad, Haryana

Dr. Rashmi Popli
rashmimukhija@gmail.com
J. C. Bose University of Science and Technology,
YMCA, Faridabad, Haryana

ABSTRACT

Mobile ad-hoc network is a wireless network that can be formed without any pre-existing infrastructure. MANET consist of both that is the legalized node and the malicious node and every node within the network acts as a router to relay packets to the destination. In this paper, current security threats and the various attacks in the MANET are investigated and various attacks such as active attack, passive attack, external attack, and internal attack.

Keywords— *MANET, Security, Attacks, Ad-Hoc Network*

1. INTRODUCTION

Mobile ad-hoc network (MANET) consists of multiple independent nodes which do not have any fixed infrastructure. Nodes can enter or leave the network freely. Like the cellular based network, nodes in MANET do not have any central base station. Every node in the ad hoc network act not only as a host but also as a router to relay packets to the destination. Nodes in ad-hoc require an efficient protocol to relay packets to the desired destination. MANET routing protocols can be characterized on various basis i.e. based on temporal information, on the basis of topology and based on utilization of resources. Ad-hoc networks do not have routes or any central access systems. So, during the route establishment procedure, intermediate nodes are used to relay route request packets. Multiple nodes in the network are used to establish a route between the source and the destination. This is the reason why an efficient routing protocol is required in MANET to transfer data packets.

2. CHARACTERISTICS OF AD-HOC NETWORK

- **Infrastructure-less:** Mobile ad-hoc network consists of multiple nodes that work independently and are not dependent on any fixed infrastructure.
- **Limited resources:** In Mobile ad-hoc network, there are various constraints on the usage of resources such as battery power, bandwidth, memory, computational power etc.
- **No central station:** In Cellular systems, there is a base station but in Mobile ad-hoc network, there is no base station as such. Every node in the network work independently and acts as a router to relay the data packet to the destination node.
- **Dynamic topology:** In Mobile ad-hoc network, any node can enter the network and any node can leave the network freely i.e. nodes are free to move arbitrarily. There is a frequent change of location which results in dynamic topology in MANET.

On the basis of routing information, MANET protocol can be classified as Proactive protocol, Reactive protocol and Hybrid protocol.

2.1 Proactive protocol

Proactive protocol follows a table-driven approach. In these protocols, every node maintains a table to store the information about other nodes and to store the network topology information. However, these protocols have various disadvantages such as storage issues and loss of bandwidth etc. An example of proactive protocols is DSDV (Destination Sequence distance vector) protocol.

2.2 Reactive protocol

Reactive protocols follow on-demand approach. Protocols that fall in this category do not maintain any topology information. A route from source to destination is established only when it is required. The required path information is acquired using a connection establishment process. An example of a reactive protocol is DSR (Dynamic Source Routing) protocol.

2.3 Hybrid protocol

Hybrid protocols combine the best features of proactive protocols and reactive protocols. Initially, the protocol uses a routing table information to establish a route from source to destination and then uses a reactive protocol for delivery of data packets. An example of a hybrid protocol is ZRP (Zone based Routing Protocol).

3. SECURITY CHALLENGES IN AD-HOC NETWORK

MANET is basically an infrastructure less network. So, routing in such an environment has various security challenges as compared to a wired network. There is no full proof security for the transmission of the data packet in the ad-hoc network. Data can be lost during transmission due to the mobile nature of both sender and receiver. Another challenge in MANET is the frequent change of topology within a network i.e. any node can enter or leave the network freely. Trust issues are also involved with the nodes in routing protocols as protocols assume every node as non-malicious. There are various protocols available to deal with the security of ad-hoc network such as SRP (Secure Routing Protocol), Sec AODV (Secure AODV) protocol etc. So, we just need to protect the network from malicious attacks, not only from external attacks but also from the internal malicious node attacks. There are various reasons for which the internal node becomes a compromised node in the network. Attacks in MANET can roughly be categorized as Active attack and Passive attack. The main concern regarding the security is that the transmission in between the two parties should satisfy security standards such as confidentiality, authentication, integrity, Non-repudiation etc. For achieving these safeguards, we need to safeguard the attacks at various layers.

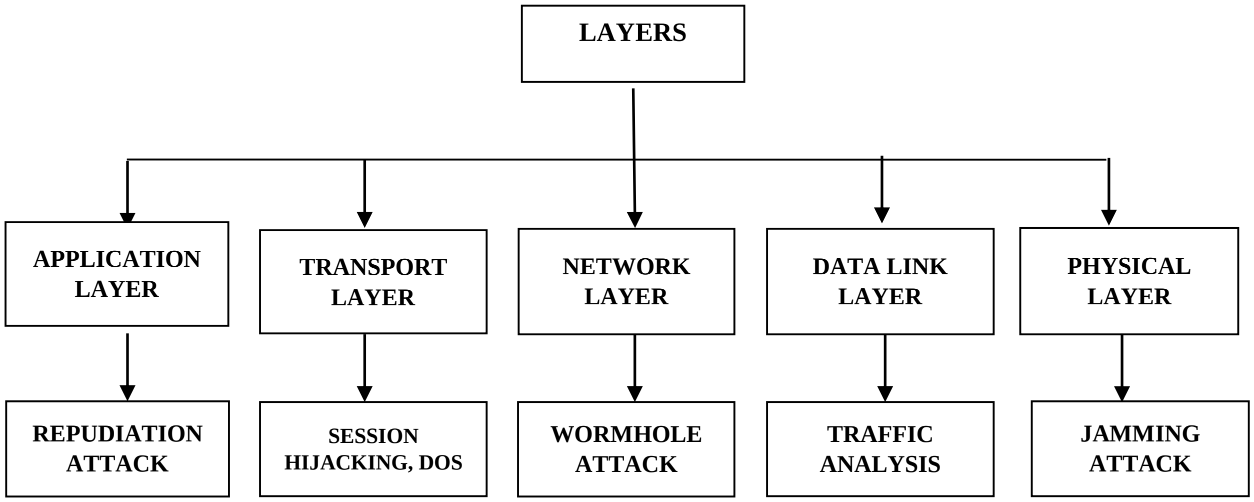

Fig. 1: Types of layers

3.1 Repudiation attack

In a repudiation attack, the user denies being the participant of any communication. The malicious node continuously accesses the system or actively participate in the communication and later denies being the participant in the communication. The user may have initiated any transaction or performed any action and later claiming that nothing as such has happened. We should ensure non-repudiation i.e. the user cannot deny after initiating a transaction or any other action. The digital documents need to be signed so that user, later on, cannot deny the authenticity of the document.

3.2 Session hijacking attack

Session hijacking is a type of security attack on the ongoing session in between 2 parties over a protected network. The attacker suspiciously gains the session id and masquerades as the legalized user of the network. The session ID is the valid token which is normally contained in the cookie. This is the reason why it is also called a cookie hijacking attack. The attacker node obtains the ID from the cookie and uses it to hijack the session. Man in the middle is a type of session hijacking attack. In Man in the middle attack, the malicious node injects itself in between the two legalized parties. The malicious node then intercepts the data and the confidential information exchanged in between two parties. The malicious actor can send or receive the confidential information that is meant for someone else. Session hijack can be or cannot be detected which purely depends on the technical knowledge of the user.

3.3 Denial of Service attack

In a DOS attack, the attacker node floods the network with unnecessary data packets then it can handle. By overloading the network, it becomes difficult for the network to function well. In this, the attacker basically prevents the legalized user to access the services. DOS attack can be launched in no of ways such as preventing an individual to access the services or flooding the network with data packets. The main aim of the DOS attack is to shut the network so that it is unavailable for the users. When DOS attack is launched with multiple computers attacking a single target node that is called as DDOS (Distributed Denial of Service) attack. A DDOS attack is more difficult to handle as the attacker is attacking with multiple IP addresses and it is difficult to track the addresses which are often spread worldwide. It is difficult to trace the source of the attack.

3.4 Wormhole attack

In the wormhole attack, the attacker node records the packet at one location in the network and tunnels it to other location in the network. The wormhole attack is launched by two or more nodes in the network. The attacker nodes establish a path between them called a Tunnel. The attacker node advertises itself that it has a shorter route to the destination, it then confuses the routing mechanisms and attracts all the traffic flows towards itself and tunnels it to another colliding attacker. The malicious node can selectively drop the packets and reintroduce them into the network.

3.5 Jamming attack

Jamming is one kind of Denial of Service attack in which the attacker prevents the other nodes from accessing the channel for communication. It attacks the real traffic source by not allowing it to send the packets and preventing the receiver node from receiving the legitimate packets. The attacker node keeps on monitoring the wireless medium.

4. PASSIVE ATTACK

In a passive attack, the malicious node does not initiate any malicious activity to disrupt the normal functioning of the network. It does not drop the packets or introduce any malicious packet in the network. It has no effect on the resources of the system and hence does not violate the confidentiality principle of the security goals. It is difficult to detect the attack because passive attack involves monitoring on the network. The aim of the attack is to steal valuable information or personal information like account details, password etc. and store them for future use. The passive attack can be like eavesdropping, Traffic analysis, snooping, the release of message content etc. We will now discuss them one by one in detail.

4.1 Eavesdropping

Eavesdropping refers to leakage of confidential information. In this, the malicious node gathers the confidential information or hear a private conversation in an illegal way and utilize it later. It involves real-time interception of private communication for example phone calls, messages, video conference etc.

4.2 Traffic analysis

It is a process of examining and monitoring the messages going on in between the network to deduce the encrypted messages. The messages are to be decoded or decrypted from patterns form to plain text. It basically involves recording, reviewing, monitoring and analyzing the traffic in the network.

4.3 Snooping

It involves casual observance or unauthorized access to another person's data or confidential information. Snooping requires a software program or application to keep track of ongoing activity on another computer or network device. Corporation tracks the internet usage of the employees or use of the device for organizational needs similarly, the government uses snooping technique to gather information related to crime and terrorism. Snooping basically is a program that performs monitoring on the network.

5. ACTIVE ATTACK

Active attack targets to disrupt the functioning of the network. In this attack, the malicious node tries to inject false packets or drop the packets from the network. It involves interception, message fabrication. The malicious node aims to destroy the resources of the network such as the bandwidth consumption, power consumption etc. The normal functioning of the network is interrupted by injecting unnecessary packets in the network for wasting the bandwidth, modifying the packets or by dropping the packets from the network. The active attack can be internal attacks, or they can be external attacks.

5.1 Internal attack

The internal attack is the most severe attack. Internal attacks are launched by the authorized nodes of the network and can participate in the functioning of the network. It is the most dangerous attack to be launched in the network. The outsider node can hijack any of the insider nodes of the network and use that node to launch an attack within the network. The node will behave as per the wish of the outsider malicious node. The hijacked node will behave as the compromised node or the misbehaving node. The compromised node can violate various security goals such as confidentiality, integrity and authentication. The misbehaving node can pass various communication keys that are used by two parties to outside intruders. Internal attack can be due to the selfishness of the node to preserve its power, bandwidth etc.

5.2 External attack

External attacks are the attacks that are launched by the malicious nodes outside the network. These nodes are not legitimate nodes and do not have legal access to the network. They are unauthorized nodes and are not allowed to participate in the normal functioning of the network. These attacks mainly aim to create congestion in the network, waste the bandwidth of the network, denying access to various operations of the network, and disrupt the overall functioning of the network. For example, bogus packet injection, denial of service are some of the attacks launched by external nodes.

6. CONCLUSION

An attempt has been made to present the security scenario in the mobile ad-hoc network. The paper also inspects the various security challenges in ad-hoc environment and depicts various attacks that threaten the ad-hoc network. The research in MANET is still in its early stage. There is a need for more secure and robust techniques to combat various security issues in the ad-hoc network. Although various security techniques have been introduced they have their own loopholes. Therefore, a stronger security technique needs to be implemented so that it can protect all the known and unknown attacks in the network.