# An Overview of security issues in Network and Types of Attacks in Network

Lipi Kothari
*Assistant Professor, Department of Information Technology, Silver Oak College of Engineering and Technology, Ahmedabad, India*

***Abstract*- Mobile ad hoc networks (MANETs) can be defined as a collection of large number of mobile nodes that form temporary network without aid of any existing network infrastructure or central access point. Each node participating in the network acts both as host and a router and must therefore is willing to forward to packets for other nodes. The characteristics of MANETs such as: dynamic topology, node mobility, provides large number of degree of freedom and self-organizing capability of that make it completely different from other network. Due to the nature of MANETs, to design and development of secure routing is challenging task for researcher in an open and distributed communication environments.**

***Index Terms*- MANETs, Security, Cryptography, Attacks, Network , Routing Protocol.**

## I. INTRODUCTION

In these years, progresses of wireless technology and increasing popularity of wireless devices, made wireless networks so popular. Mobile Ad Hoc Network (MANET) is an infrastructure-independent network with wireless mobile nodes. MANET is a kind of Ad Hoc networks with special characteristics like open network boundary, dynamic topology, distributed network, fast and quick implementation and hop-by-hop communications. These characteristics of MANET made it popular, especially in military and disaster management applications. Since MANETs are self-configured, self-optimized, and self-healing infrastructure-less network, with unmannered and dynamic change of topology, these Routing protocols play very important role in adapting such scenarios avoiding link failures and other changing network topology.

Compared to the traditional wireless and wired networks, MANETs is prone to larger security vulnerabilities and attacks because of certain features of MANET like no centralized authorities, distribution cooperation, open and shared network wireless medium, severe resource restriction, and high dynamic nature of network topology. These factors have made MANETs to receive great attentions and also because of their capabilities of self-configuration and self-maintenance.

This paper is organized in Sections. Section II has covered Routing Protocols, its types and sub-types, Section III has covered Attacks in MANET, and Section IV has covered Security Services in MANETs, Section V has covered benefits of network security followed by Conclusion in Section VI.

## II. ROUTING PROTOCOL

Routing Protocols in MANETs are basically classified in 3 types:

### A. Proactive Routing Protocol:

These protocols refers its routing table for determining routes and thus are called “table-driven”[4]. Nodes or Mobile devices maintainother node information inside network and update this info periodically. This Routing information of every other node is kept inside a routing table and as the network topology is dynamic and changes regularly, the network routing information is also updated periodically. The advantage of these routing protocols is that, ready routes are available to all destinations but these protocols increase the computational and communication overheads which consume the scarce resource of the devices such as bandwidth, processing power and battery unnecessarily.

### B. Reactive Routing Protocol

These are on-demand routing protocols[4] i.e. when the mobile device has the packets for the destination node, it only then searches for the routes and

establishes the connection between the source and destination nodes. These protocol generally include following components:

Route Discovery: The sendertransmits a Route Request message to find route to destination, if not known earlier. Thereceiving node replies with a Route Reply (RREP) packet through which the link is established between the two. Oncethe connection is established, the data is sent through that route.

Route Maitenance: Due to dynamic nature of the network,many link get broken and many new links are formed. Broken link can result into transmission failure. Route Maintenance is thus a mechanism through which the broken link is handled.

C. Hybrid Routing Protocol

The Hybrid routing protocols combines the advantages of the two protocols. These types of protocols maintain the routes to their neighbors which are one or two hops away and for any further destination a route request is sent as sent in "Reactive Routing Protocols".

## III. ATTACKS IN MANETS

"Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

### 3.1. Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. These attacks can be classified into further following types:

Some active attacks are spoofing attack, Wormhole attack, Modification, Denial of services, Sinkhole, and Sybil attack.

a. Spoofing

When a malicious node miss-present his identity, so that the sender change the topology

b. Modification

When malicious node performs some modification in the routing route, so that sender sends the message through the long route. This attack cause communication delay occurred between sender and receiver.

c. Wormhole

This attack is also called the tunnelling attack. In this attack an attacker receives a packet at one point and tunnels it to another malicious node in the network. So that a beginner assumes that he found the shortest path in the network.

d. Fabrication

A malicious node generates the false routing message. This means it generate the incorrect information about the route between devices.

e. Denial of services

In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response.

f. Sinkhole

Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In this attack, a node tries to attract the data to it from his all neighbouring node. Selective modification, forwarding or dropping of data can be done by using this attack.

g. Sybil

This attack related to the multiple copies of malicious nodes. The Sybil attack can be happen due to malicious node shares its secret key with other malicious nodes. In this way the number of malicious node is increased in the network and the probability of the attack is also increases. If we used the multipath routing, then the possibility of selecting a path malicious node will be increased in the network.

### 3.2. Passive attack

The names of some passive attacks are traffic analysis, Eavesdropping, and Monitoring.

a. Traffic analysis

In the traffic analysis attack, an attacker tries to sense the communication path between the sender and receiver. An attacker can found the amount of data which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis.

b. Eavesdropping

This is a passive attack, which occurred in the mobile ad-hoc network. The main aim of this attack is to find out some secret or confidential information from communication. This secrete information may be privet or public key of sender or receiver or any secrete data.

c. Monitoring

In this attack in which attacker can read the confidential data, but he cannot edit the data or cannot modify the data.

3.2. Passive Attacks

In passive attacks the attacker does not perturb the routing protocol, instead try to extract the valuable information like node hierarchy and network topology from it. Passive attack is in nature of eavesdropping on, or monitoring of, transmission. The goal of opponent is to obtained information that is being transmitted. Passive attacks are very difficult to detect because they do not involve any alteration of data.

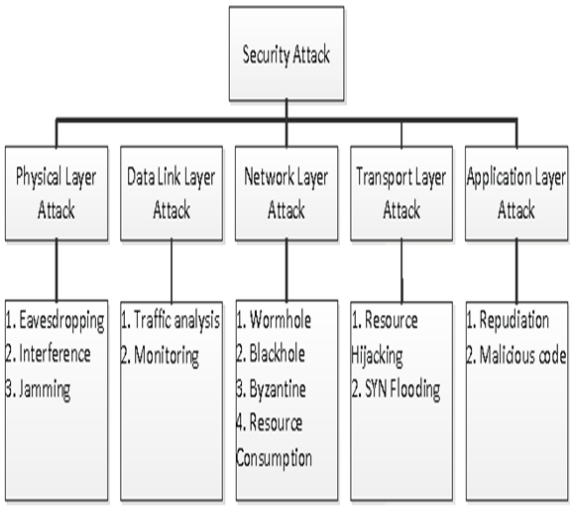


Figure 1: Classification of security Attacks

Attacks can also be categorized on the basis of its source, behavior and nodes. Figure-3, shows such categorization:

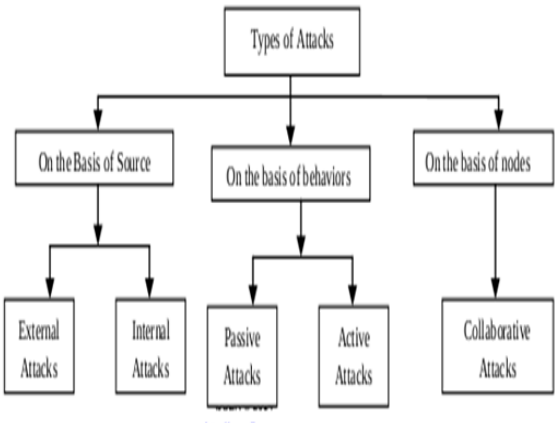


Figure 2: Categorization of Attacks in MANETs

On the Basis of Source: On the basis of source, attacks can be classified as external and internal attacks. External attacks are caused by the nodes which are not a part of the network. External attackers are the aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks are caused by the nodes which are a part of the network. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromisng a current node and using it as a basis to conduct its malicious behaviors.

II. On the basis of Behavior: A passive attack attempts to retrieve valuable information by listening to traffic channel without proper authorization, but does not affect system resources and the normal functioning of the network. Passive attacks are very hard to detect because they do not involve any alteration of the data. An active attack attempts to change or destroy the system resources. It gains an authentication and tries to affect or disrupt the normal functioning of the network services by injecting or modifying arbitrary packets of the data being exchanged in the network. An active attack involves information interruption, modification, or fabrication.

III. On the basis of Nodes: In these types of attacks, there are numerous nodes involved during the attack. These nodes can be physically existent or not existing at all.

## IV. SERVICES IN MANETS

The aim of a security service is to secure network before any attack happened and made it harder for a malicious node to breaks the security of the network Due to special features of MANET, providing these services faced lots of challenges. For securing MANET a trade-off between these services must be provided, which means if one service guarantees without noticing other services, security system will fail. Providing a trade-off between these security services is depended on network application, but the problem is to provide services one by one in MANET and presenting a way to guarantee each service. We discuss five important security services and their challenges as follows:

Availability:
According to this service, each authorized node must have access to all data and services in the network. Availability challenge arises due to MANET's dynamic topology and open boundary. Accessing time, which is the time needed for a node to access the network services or data is important, because time is one of the security parameters. By using lots of security and authentication levels, this service is disregarded as passing security levels needs time.

Authentication:
The goal of this service is to provide trustable communications between two different nodes. When a node receives packets from a source, it must be sure about identity of the source node. One way to provide this service is using certifications, whoever in absence of central control unit, key distribution and key management are challengeable.

Data confidentially:
According to this service, each node or application must have access to specified services that it has the permission to access. Most of services that are provided by data confidentially use encryption methods but in MANET as there is no central management, key distribution faced lots of challenges and in some cases impossible.

Integrity:
According to integrity security service, just authorized nodes can create, edit or delete packets. As an example, Man In -The -Middle attack is against this service. In this attack, the attacker captures all packets and then removes or modifies them.

Non-Repudiation:
By using this service, neither source nor destination can repudiate their behaviour or data. In other words, if a node receives a packet from node 2, and sends a reply, node 2 cannot repudiate the packet that it has been sent.

## V. BENEFITS OF NETWORK SECURITY

- Network Security helps in protecting personal data of clients existing on network.
- Network Security facilitates protection of information that is shared between computers on the network.
- Hacking attempts or virus / spyware attacks from the internet will not be able to harm physical computers. External possible attacks are prevented.
- Network Security provides different levels of access. If there are various computers attached to a network, there may be some computers that may have greater access to information than others.
- Private networks can be provided protection from external attacks by closing them off from internet. Network Security makes them safe from virus attacks, etc.

## VI CONCLUSION

In this paper we addressed existing potential security threats in MANETs. In this study we found that most of the work on MANET security focused on single layer attacks i.e. active and passive attacks. In the meanwhile some attacks involving multiple nodes have received little attention since they are surprising and combined attacks i.e. collaborative attacks. There have been no proper definition and categorization of these kinds of collaborative attacks in MANETs. Thus, protection of communication system against these types of attacks is a challenging task. Therefore, deep study on collaborative attacks and development of new protocols/algorithms/model to manage these attacks is the need of hour. Development of a multi-fence security solution that is embedded into possibly every component in the

network, resulting in depth protection that offer multiple line of defense against many known and unknown security threats is also given importance. Further, there is also a need to develop a detection and defense mechanism for managing messages in secure manner.

REFERENCES

[1] Mohan V. Pawar, Anuradha, A. 2001.Network Security and Types of Attacks in Network. International Conference on Intelligent Computing, Communication & Convergence.

[2] Lakshit Prashar, Raj Kamal Kapur. Performance Analysis of Routing Protocols under Different Types of Attacks in MANETs. IEEE,2016.

[3] Komal Gandhi. Network Security Problems and Security Attacks. IEEE,2016.

[4] Resul Daş,Abubakar Karabade, Gurkan Tuna , Common Network Attack Types and Defense Mechanisms. IEEE,2015.

[5] Umesh Kumar Singh , Kailash Phuleria ,Shailja Sharma & D.N. Goswami . An analysis of Security Attacks found in Mobile Ad-hoc Network.European Journal of Economics, International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014 ISSN 2229-5518.

[6] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M. An Overview Of security Problems in MANET. IEEE.

[7] Vikaram Agrawal , Hiral Chauhan. An Overview of security issues in Mobile Ad hoc Networks. International Journal of Computer Engineering and Science, August- 2014.

[8] Ali Dorri and Seyed Reza Kamel and Esmail kheyrkha. Security Challenges In Mobile ADHoc Networks: A Survey, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015.