A Review on Security Techniques in MANET

Jayashree Agarkhed
Professor, Department of C.S.E, P.D.A College of Engineering, Kalaburagi, India.

Abstract—The Mobile ad hoc network (MANET) is more prone to various attacks due to its network characteristics such as unreliable of links, lack of centralized administration and mobile nodes in the network. The defense in the network has to be increased tremendously to face the bad attacks. In order to achieve security in MANET, availability, integrity, non-repudiation and authentication must be satisfied by the network. Providing authentication is the key issue in MANET during detection of correct route in infrastructure less network. This paper reviews various security attacks.

Keywords—Security, Ad hoc network, Routing, MANET

I. INTRODUCTION

MANET refers to the way the mobile networks encompass the wireless nodes with mobility for communication. Thus it consists of set of wireless nodes with mobility and ability of communicating with each other in a infrastructure network without centralized administration. Nodes organize themselves vigorously in random and leads to unstable topologies. MANET support range of applications like ad hoc gaming, intelligent system, smart agriculture, disaster recovery and forest monitoring. These applications demand a system that can transfer reliable information from a source to destination, mobile nodes. The mobile nodes may be subjected to a crucial attacked. It is so, because a node can receive a packet of data that is sent within its frequency range. Due to mobility of nodes, the intermediate node at any time can travel out of frequency range. The non existence of centralized control and predetermined infra structure allows any node to enter into the network.

In wired networks, measures have to be taken while communication occurs by use of firewalls and secured gateways which provide secure communication though network. In MANET, frequent change in topology leads to lot of vulnerabilities and provide chance to the attackers to collapse the network partially or fully. Thus there is a necessity to understanding of the various attack related problems allied with the MANET while routing the information [1].

The paper is organized in the following sections: Section II deals with the related work. Section III gives information about different types of attacks prone to routing. Section IV gives the security issues and challenges in MANETs. Section V details about security techniques in MANET and Section VI gives the conclusion part.

II. RELATED WORK

The main intend of ad hoc network is to provide efficient and robust operation in the network using routing protocols [2]. A number of the design challenges and characteristics of MANETs include

1. Wireless link: The wireless link availability is not reachable to everyone.
2. Secure boundaries: Lack of secure boundaries welcomes various threats and attacks within the network.
3. Infrastructure less: Specific infrastructure has not been defined.
4. Limitation in nodes: Nodes limitation will lead to less availability.
5. Link limitations: Link limitation will pose bandwidth limitation.
6. Multi-hop routing: This type of routing can cause fabricated routes within the network.
7. Dynamic topology of network: The topology of network changes frequently due to mobility behaviour of nodes in MANET.
8. Sharing communication medium: They are shared in nature and leads to more interference.
9. Openness of network architecture: It has open architecture in nature and hence is prone to many types of attacks.
10. Inflexible resource constraints: It has resources which are inflexible to use.

In [3] author has made survey on fundamental security issues on multi hop network connection in MANET. In [4] author has presented the range of security aspects in mobile ad hoc network and dealt with various characteristics and tools which can be used in MANET.

In [5] author has discussed some new security aspects in fixed infrastructure Wireless Sensor Networks (WSN) and MANETs. The design challenges, issues and services of secure group communication over the wireless network are given in detail in the work. Authors in [6] have discussed about the security challenges for secured transmission of information in MANET. Various security issues in MANET include availability, integrity, confidentiality, authentication, non-repudiation, scalability etc. A number of the techniques used for securing the MANET are prevention, performing detection and reaction approaches. These techniques to overcome attacks while routing in...
MANET reviewed in the literature are discussed in this paper discussed.

III. DIFFERENT TYPES OF ATTACKS
Attackers sensing the data traffic network as depicted in figure 1, continuously and intrude themselves into the route established between the source node and destination node. In this way attacker take the control of data traffic flowing in the network which is shown in figure 2.

1. Overflowing Routing Table: In a proactive routing the routing table is updated with information routed at regular intervals. This attack advertises extreme routes to overflow routing table information of the target node. It targets that creating of new routes and their implementation is prevented due the presence of enough routes and protocol is overwhelmed.

2. Poisoning Routing Table Attack: Nodes information in the route table can be corrupted by the route table poisoning attack in the network. This attack creates false routes by broadcasting false information about traffic and thus creates false entries in the routing tables of other nodes. Other way is to generate RREQ packets with a high priority sequences numbers thus leading to deletion of routes with low sequence numbers.

3. Attack by replication of packets: Replication done by replicating packets by an enemy node, using up extra bandwidth and energy of a node.

4. Rushing Attack: Protocols at route discovery use duplicate repression process [7]. When malicious node receives Route Request packet (RREQ), it floods the packet over network before the nodes which also received the same packets. The node on receiving original RREQ, assume that the just received packet as duplicate and discard the packet. Thus source node cannot find the secure routes.

5. Cache information corruption Attack
Routing table entries are updated frequently. Attacker corrupts routing information in cache while routing [8]. This happens when stored information in the routing tables is modified, deleted or injected with false information.

6. Location discovery attack: Intruder identifies the location of node or structure of network.

7. Black Hole: In this type, malicious node inserts fake route as shortest path to divert the network traffic or even inserts a malicious node.

8. Wormhole: In this type of attack, intruder say node X capture the data traffic and establish link with other node say Y. Then later inserts this link into network and controls all nodes in network connected to this link.

 MANETs are analyzed in two wide categories.

a. **Intrusion Detection System (IDS):** IDS is a security system used for identifying the violations made for security policies. Certain measures must be taken if the security is breached in the network. Various types of IDS include misuse-based, anomaly-based, specification-based system [9].

b. **Secure routing techniques:** These routing techniques are greatly required for known threats and attacks in MANET. It includes mechanisms on harder techniques like worm hole and rush attacks [10].

Apart from these mechanisms, various security techniques are to be considered as discussed next.

IV. SECURITY ISSUES AND CHALLENGES IN MANET

The following discussion highlights the various security issues and design challenges in MANET.

MANET is considered as self-configured network, connecting mobile nodes. Some of the security issues in MANET are listed according to network layers. The layers
of protocol stack in the network are included for considering the design issues in the MANET [11].

a. Application layer include detection and prevention of worms, viruses, malicious codes and application abuses.
b. Transport layer has authenticates and secures end-to-end information communication through data encryption.
c. Network layer include protection of the ad hoc wirelessly routing protocols.
d. Link layer include protection of the wireless MAC layer protocol and support link-layer security.
e. Physical layer has preventing signal jamming denial-of-service attacks.

V SECURITY TECHNIQUES IN WIRELESS ADHOC NETWORKS

There is need to provide security against these attacks and providing high information security in wireless mobile networks are major concern today. Major security mechanisms in are classified into broad categories. The major security techniques in MANET are.

a. Identity based cryptography:
It is a cryptographic method which includes public key for encrypting the files. This technique involves shared key generation, new master key sharing idea, certificate chaining method and private key method [12].

b. HMAC (Homomorphic Message Authentication Code):
It is a cryptographic solution under the network for inspection the authentication of the code inside the sensor nodes. This is a type of symmetric key solution method.

c. Digital signatures:
It is a symmetric based cryptographic method for encryption and decryption of the data within the network. It works against denial of service attack in MANET.

MANETS are usually more prone to physical threats as they have mobile devices connected together. They have movable platforms and therefore have more security threats in the network. MANET has got lot of vulnerabilities due to enormous functions like routing and packet forwarding etc.

The security goals are required in MANETs as there are sensitive in security applications. The well known features of MANETs are required for wireless technology in order to design the network solutions.

VI. CONCLUSION

MANETs have the capacity of self configuring of nodes and network maintenance. Nodes is MANET are subjected a lot of issue and challenges to make available a reliable transmission of information. Thus providing safety measures has turned out to be a major concern in wireless communication. In that aspect, major security issues and challenges have been addressed while designing of the protocols.

REFERENCES