A Review: Attacks and Its Solution over Mobile Ad-Hoc Network

Ankit Mehto¹, Prof. Hitesh Gupta²

¹M.Tech Computer Science & Engineering Department in Patel Institute of Technology, Bhopal, India

Abstract— Mobile Ad-hoc network (MANET), a new form of Ad-hoc Network has gained the attention of today’s research efforts and automotive industries to improve road safety and enable a wide variety of value-added services. It needs security to implement the wireless environment and serves users with safety and non-safety applications. Many forms of attacks against MANET have emerged recently that attempt to compromise the security of such networks. Such security attacks on MANET may lead to catastrophic results such as the loss of lives or loss of revenue for those value-added services. In this paper, we discuss some of the main security threats that can be exploited in MANET and present the corresponding security solutions that can be implemented to thwart those attacks.

Keywords—MANET, Ad-hoc network, Security, attacks

I. INTRODUCTION

With rapid development of wireless technology, the Mobile Ad-hoc Network (MANET) has emerged as a new type of wireless network. The world today is living a combat, and the battle field lies on the roads, the estimated number of deaths is about 1.2 million people yearly worldwide [1]. MANETs are new type of networks which are expected to support a large spectrum of mobile distributed applications. A mobile ad-hoc network is a collection of mobile nodes or routers connected with an automatic system. There nodes does not user any wired media as a link. MANET is type of wireless network so it uses the wireless links. The combination of this structure makes the random graph having vertices and links. Here node can freely moves anywhere in the network so it also change the location of node in graph. This is a major cause by which the network can use without pre analysis [2]. It is also called the ad-network. Due to its Dynamic topology property MANET has various applications such as military area, rescue operations, natural disaster recovery etc. apart from that it can also install in the office, home or a small area of city [3].

II. EXTERNAL VS INTERNAL ATTACKS

The attacks can also be classified into external attacks and internal attacks, according the domain of the attacks. Nodes that do not belong to the domain of the network carry out external attacks. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more harmful when compared with outside attacks since the insider knows valuable and secret information, and possesses confidential access rights.

III. ACTIVE VS PASSIVE ATTACK

The attacks in MANET can generally be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.
IV. WORMHOLE ATTACK

Mobile ad hoc network [4] is a self-configuring network that is formed automatically by a set of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is prepared with a wireless transmitter and receiver, which allow it to communicate with other nodes in its range. In order for a node to forward a packet to a node that is out of its radio range, the support of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology normally changes due to the mobility of mobile nodes in the network.

In a wormhole attack, two attacker nodes join together. One attacker node receives packets at one point and “tunnels” them to another attacker node via a private network connection, and then replays them into the network.

Wormhole attack is a relay-based attack that can disrupt the routing protocol and therefore disrupt or breakdown a network and due to this reason this attack is serious. We can use 4 steps to explain about a general wormhole attack[5,7].

1. An attacker has two trusted nodes in two different locations of a network with a direct link between the two nodes.
2. The attacker records packets at one location of a network.
3. The attacker then tunnels the recorded packets to a different location.
4. The attacker re-transmits those packets back into the network location from step 1.

Figure 2 shows the simple worm hole in the network. Here node 2 and node 8 create the tunnel in order to work as a malicious node. Both nodes give the illusion to another node that there is a shortest path. But this shortest path does not exist and attack can easily perform by the attacker.

There are three types of wormhole attacks are available[6]. There are classified on the basis of its Nodes. There are open wormhole attack, half open wormhole attack and closed wormhole.

A. Open Wormhole Attack: In this type of attack both nodes are available in the network in order to complete the communication in the network. Here both nodes can change the data as well as show them self in route discovery path.

B. Half Open Wormhole Attack: In this type of attack one node is open in network in order to spoil the integrity of data.

C. Closed Wormhole Attack: When the tunnel has formed then both node hide then self from the
network but act for modifying the data. They help of verification of digital signature by which malicious node will unable to attack in the network.

VII. CONCLUSION
After this study it seems to be that there are so many attacks are available in order to do the malicious activity in the mobile ad-hoc network. Some of these problems has sort out by many researchers. This paper throws some light on the various attacks in MANET and some methodology in order to prevent these attacks from spoiling the integrity of data.

VIII. ACKNOWLEDGEMENT
I would like to say thanks to my guide “Prof. Hitesh Gupta” who gives their knowledge and time in order to complete this paper. This paper will never complete without the support faculty member of CSE department of PCST, Bhopal.

REFERENCES