Chapter 13

Intrusion Detection in MANET for Network Layer

Sambhu Dahal
Biju Patnaik University of Technology, India

Niranjan K. Ray
Silicon Institute of Technology, India

ABSTRACT

Mobile Ad Hoc Networks (MANETs) have become a major next generation wireless networking technology. MANETs are vulnerable to attacks in network layer. MANETs are infrastructure-less network in which the topology is constantly changing which makes it easy for the intruders to attack. Security is always an important issue especially for the case of Mobile Ad Hoc Network (MANET) because the structure of the network makes it an easy target for attackers. The inherently vulnerable characteristics of wireless ad hoc networks make them susceptible to attacks, and it may be too late before any counter action can take effect. It can also be observed that each type of attack affects the network characteristics and behavior differently. So we need to study all the types of attack and then we study the intrusion detection and protection mechanism. Intrusion Detection Systems (IDSs) can monitor audit data, look for intrusions to the system, and initiate a proper response.

1. INTRODUCTION

The concept of mobile wireless devices working together was proposed in the 1990s. MANET stand for Mobile Ad Hoc Network, has uses in various fields of life. It has been used in military for the timely flow of information and command in the battle which may lead to the success of the mission. We can use MANETs (Mohapatra & Krishnamurthy, 2005) for establishing communication networks and providing rescue services in natural disaster such as earthquakes and floods. In MANET each device is free to move independently in any direction (Jayakumar & Gopinath, 2007). Each node in MANET act as a router to forward the packet from one node to another till it reaches the destination node. As we can see that MANETs is a boon to the society but it also have some drawbacks. The major challenge for MANETs is security. Mobile nodes within one another’s radio range can communicate through wireless

DOI: 10.4018/978-1-5225-0486-3.ch013
Intrusion Detection in MANET for Network Layer

Figure 1. Mobile ad hoc network

links and thus dynamically form a network. Wireless devices that are not in direct range communicate via intermediate devices which is known as multi hop communication. In MANETs the intruder can compromise the operation of the network by attacking at any of the physical, MAC or network layer. In network layer, the routing protocol is vulnerable because we need to use cooperative routing algorithm. Here in MANET standard information security measures such as encryption and authentication does not provide complete protection, so we need to use intrusion detection and protection mechanism to secure MANETs. MANETs are very flexible as the nodes can freely join and leave the network. There is no main body which keep track of the nodes entering and leaving the network like routers and gateway in wired network.

In MANETs node can automatically join the network, if the node is in the radio range. MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious (Buttyan & Hubaux, 2007). Due to no secure boundaries, MANET is more susceptible to attacks. The attack can be passive or active, leakage of information, false message reply, denial of service or changing the data integrity. In MANETs there is no protection against attacks like firewalls or access control, which result the vulnerability of MANETs to attack. Spoofing of nodes identity, data tempering, confidential information leakage and impersonating node are the results of such attacks when security is compromised. Here the attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network.

MANET is a self-configurable network, which consist of Mobile nodes where the communication among the mobile nodes is done without a central control. Each and every node acts as a router for receiving and forwarding the packets without any preexisting infrastructure. It is very difficult to detect the attacks in MANETs due to lack of centralized management. The networking technology was there for a long time and the networking paradigm has shifted from fixed to wireless network in the last decade. Since there is change in networking paradigm from fixed to wireless, we still consider intrusion detection and prevention as one of the basic layers of defence. Intrusion detection in MANETs is complex and challenging than in a fixed network because it is difficult to collect audit data from the network, and apply the techniques of Intrusion Detection to detect intrusion with a low rate of false positives and an effective response to intrusion. MANETs lack the concentration point where monitoring and collection of audit data can be performed. Here the nodes require to cooperate for routing and act as a router, creat-