Chapter L
Security in Mobile Ad Hoc Networks

Ekata Mehul
Gujarat University, India

Vikram Limaye
India

ABSTRACT

Securing a "Wireless Ad Hoc Network" (WAHN) is a major concern of network administrators. This is particularly so in case of the wireless networks due to their unique characteristics that varies from the traditional networks. For example, WAHN are vulnerable to internal as well as external attacks relatively easily, as compared with traditional networks, because of their ability to be accessible from anywhere within their range. Many solutions have been proposed in this area and they are also being continuously improved. Most of these solutions involve encryption; secure routing, quality of service, and so forth. However, each of these solutions is designed to operate in a particular situation; and it may fail to work successfully in other scenarios. This particular research work offers an alternate to improving the trustworthiness of the neighbourhood and securing the routing procedure. This security is achieved by dynamically computing the trust in neighbours and selecting the most secure route from the available ones for the data transfer. There is also a provision to detect the compromised node and virtually removing it from the network.

INTRODUCTION

Securing a "Wireless Ad Hoc Network" (WAHN) is a major concern of network administrators due to their unique characteristics that varies from the traditional networks. This chapter proposes a scheme of calculating trustworthiness of the network neighbourhood and securing its routing process. In last few years, the popularity of wireless network has grown to an enormous extent. Features like spaghetti free networks, mobility, ease of use and accessibility, are the major reasons for the increased use of wireless networks. Wireless Networks provides flexible data communication system, which uses wireless media such as radio frequency technology to transmit and receive data over the air.

Wireless networks offer the following advantages over the traditional wired networks:

1. **Mobility:** It provides real time access to the mobile users – anytime, anywhere. This mobility supports productivity and service opportunities, which were not possible with wired networks.

2. **Installation and Speed of Simplicity:** Wireless systems can be installed rapidly and easily, it eliminates the need of the cables as well.
3. **Reach of the Network:** We can connect and extend our network to places, which can not be wired.
4. **Flexibility:** Wireless networks are more flexible and easily adapt system and configuration changes.
5. **Reduced cost of ownership:** Apart from the initial investment, overall installation and life cycle costs are very less than that of wired networks.
6. **Scalability:** Wireless systems can be configured in various topologies depending on required applications and installations. It ranges from peer-to-peer network for a small number of users to large infrastructure networks to enable roaming over a broad area.

Wireless networks are telephone or computer networks that use radio as their carrier or physical layer [3]. These radio waves simply perform the function of delivering energy to a remote receiver. The data is modulated on the radio carrier so that it can be accurately extracted at the other end. Multiple radio carriers with different frequencies can exist in the same space at the same time without interfering with each other. The receiver tunes into one of the radio waves to receive the data at the intended frequency.

Wireless LAN technology makes it possible for two or more computer to communicate using standard network protocols without network cables [4]. Computers are connected using Multiple Network Access points. A single access point covers large area. All wired and wireless computers can access the Internet through single software access point.

There are some limitations of the wireless networks, which sometimes override the above-mentioned advantages, are as follows: [14]

1. **Limited Bandwidth:** Wireless communications requires radio spectrum, which is very less and not able to support unlimited available wireless applications. The bandwidth is scares and hence, it is expensive.
2. **Coverage Problems:** Radio signals are attenuated and reflected by the obstacles. At higher frequencies, due to diffraction and reflections, coverage problems increases.
3. **Hostile Radio Channel:** Because of the coverage and obstacle problems, it is difficult to achieve the quality of the radio signals. As a result efficient mechanism like error corrections systems, interleavers, equalisers and adaptive antennas are required to overcome such difficulties.
4. **Inadequate Battery Power:** Generally, small and lightweight portable devices are preferred in mobile wireless communication. Thus, the power consumption is an issue and the battery technology has not evolved at the pace of semiconductor technology. [14] This forces users to have low power transmitters and less powerful computational devices.

Mobile Ad Hoc Networks

MANET – Mobile Ad Hoc Networking is a new concept in a wireless communication world, where the networks are formed and destroyed on the fly without any centralized control. It is an autonomous system of mobile routers connected by wireless links.

In MANET, nodes are in transition and pose a dynamic network topology where a node can join and leave the network at any point of time. Due to limited transmission range, hop-by-hop data communication is required, where a data packet reaches its destination after travelling several nodes in between. Thus, each intermediate node acts as a router.

Security Issues in Mobile Ad Hoc Networks

Security is vital in Ad Hoc Networks. Securing the Ad Hoc Networks starts from the neighbour verification in the local community also termed as a cluster – collection of wireless nodes in a particular group. Mobility and limited range of bandwidth makes it difficult to detect the malicious activity in a self-organised network [1]. The security issues involve the activities like node authentication, key management, trust establishment, secure routing protocols and handling the node misbehaviour and traffic analysis.

Security Goals

Security is the utmost concern for ad hoc networks, especially for the security-sensitive applications [13]. Following attributes are generally considered to secure an ad hoc network.

- **Availability:** Ensures the survivability of network services even in case denial of service attacks, which can be launched at any layer.