Chapter VI
A Secure Characteristics of Wireless Ad-Hoc Networks

Sandip Vijay
I.I.T. Roorkee, India

S. C. Sharma
I.I.T. Roorkee, India

ABSTRACT

This chapter reviews the secure characteristics of mobile devices that can use wireless networks (ad-hoc) almost any where and any time, by using one or more wireless network technologies. Currently, most computers communicate with each other by using wired networks. This approach is well suited for stationary computers, but it is not appropriate for mobile devices. These technologies enable the use of infrastructured networks (3GPP) and ad-hoc networks. Furthermore, the authors describe the gateway specification, requirement for implementation for ad-hoc networks. The minimum, essential, and additional functional requirements for effective functionality of gateway are presented in tabular form. At the end, the future functional requirement and the features of multiple ad-hoc networks are also described.

INTRODUCTION TO WIRELESS AD-HOC NETWORKS

An ad-hoc network is a self-configuring network of wireless links connecting mobile nodes. These nodes may be routers and/or hosts. The mobile nodes communicate directly with each other and without the aid of access points, and therefore have no fixed infrastructure. They form an arbitrary **topology,** where the routers are free to move randomly and arrange themselves as required. First, the devices can freely move in the network, second, the devices can leave and join the network at any time. This type of network can change constantly. Finally, the network disappears when the last devices leave the network (Arkko, J. et al., 2004). The decentralized nature of wireless ad hoc networks makes them suitable for a va-

riety of applications where central nodes cannot be relied on, and may improve the scalability of wireless ad hoc networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified. Minimal configuration and quick deployment make ad hoc networks suitable for emergencies like natural disasters or military conflicts. The presence of a dynamic and adaptive routing protocol will enable ad hoc networks to be formed quickly (Buddhikot, M. et al., 2003).

Isolated wireless ad-hoc networks are not suitable for today's applications that require accessing services in the Internet. To overcome this limitation, one or more devices in the wireless ad-hoc network can provide a gateway to an external network. This external network can be the Internet or a local area network (LAN), which may or may not be an infrastructured network. Wireless networks are more vulnerable to misuse than wired networks. In a wireless network, all devices share the same radio band. If two or more devices transmit simultaneously, the communication fails. In addition, a malicious device may be present in the network. It can analyze the communication in the network and do several attacks by sending invalid data. It can masquerade as another device, or it may do various Man-in-the-Middle (**MitM**) or Denial-of-Service (**DoS**) attacks. In particular, it can even block all communication by constantly interfere the transmission. Several security mechanisms partially protect communication in WLAN. **WLAN** may provide security on the lower layers that corresponds the physical and link layers of the Open Systems Interconnection (OSI) reference model. These mechanisms protect communication authenticity, integrity and confidentiality by using cryptographic methods. Moreover, these mechanisms depend on the WLAN technology. On the other hand, security can be provided independently on upper layers. However, none of these mechanisms protect against DoS attacks because it is impossible to prevent a malicious device from interfering the transmission in a wireless ad-hoc network. It is also possible that not all devices can communicate directly in the wireless ad-hoc network. Such a scenario is shown in Fig. 1. in which device B can communicate with devices A and C directly, but devices A and C cannot communicate directly. This has an impact on the network-layer and application-layer protocols. In the network-layer, not all devices can communicate directly with each other by using IP addresses. Moreover, some applications do not work unless the communication is link-local. For example, Dynamic Configuration of **IPv4** Link-Local addresses requires link-local communication to successfully configure and maintain IPv4 addresses.

Routing enables communication between devices that cannot communicate directly. In the ad-hoc network, this is done by using an ad-hoc routing protocol. There are two types of routing protocols for ad-hoc networks: Proactive and Reactive. In proactive routing, routes are actively maintained, and they are available when needed. In reactive routing, routes are discovered on demand. An ad-hoc network can be isolated, or it can have a gateway that provides a connection to another network. Consequently, the devices must be able to communicate when the gateway is available and when it unavailable.

THE AD-HOC NETWORK ENVIRONMENT

This section introduces the gateway and its environment, and it describes the used ad-hoc network environment first from the lowest layer upwards and then from the logical point of view. The users use wireless devices to communicate with other users in proximity. The devices use Wireless Local Area Network (WLAN) to form a wireless ad-hoc network. The devices can be desktops, laptops, and mobile phones. The communication takes place within a group of two or more people. The communication group may be