Chapter 80
Privacy and Security of Wireless Communication Networks

Sattar B. Sadkhan
University of Babylon, Iraq

Nidaa A. Abbas
University of Babylon, Iraq

ABSTRACT

Wireless networks are inherently more vulnerable than their wired counterparts. In addition, complications arise in the presence of node mobility and dynamic network topology. Moreover, intermittent connectivity, whether caused by mobility or periodic node sleep, brings about additional challenges. At the same time, node resource constraints make direct adoption of existing security solutions difficult, if not impossible. Wireless Communication Network Security and Privacy analyze important problems in the realms of wireless networks and mobile computing. The Security aspects relate to authentication, access control and authorization, nonrepudation, privacy and confidentiality, integrity, and auditing. Privacy is an essential feature of any product or service.

WIRELESS COMMUNICATION NETWORKING AND TECHNOLOGIES

Wireless communications have become a very interesting sector for the provision of telecommunication services. Mobile networks are available almost anytime and anywhere. The popularity of wireless handheld devices is high. The services offered are strongly increasing. They vary from simple communication services to applications for special and sensitive purposes such as electronic commerce, medical services and digital cash (Thurwachter, 2002).

Due to low cost, low power consumption, flexible, no physical infrastructure and easy to deploy, wireless communications have been an admired research area over the past few years with tremendous growth in the population of wireless users. Nowadays, there are number of wireless technologies on hand for long range applications like cellular mobile, satellite communications, Radio Frequency (RF), and short range applications such as Bluetooth, Infrared (IR), Near Field Communication (NFC), ZigBee, Ultra Wide Band (UWB). These short range wireless technologies are being used in many wireless networks like

DOI: 10.4018/978-1-4666-8751-6.ch080

wireless local area networks (WLAN), wireless body area networks (WBANs), wireless personal area networks (WPANs), and, ad-hoc network (Tachikawa, 2002).

The IEEE 802.11 standard for wireless local area networks (also known as Wi-Fi) currently supports multiple over-the-air modulation techniques in the 2.4 GHz and 5 GHz frequency bands with speeds between 11 and 540 Mbit/s. In the most common setup, the infrastructure mode, a computer or a mobile phone connects to an access point, which offers further connection to the fixed Internet. The area covered by a single access point is known as a hotspot. The IEEE 802.11 standard also allows for mesh networks and for peer-to-peer (wireless ad hoc) connections (Chen, 2007).

In future wireless protocols and communication environments (networks), the security will play a key role in transmitted information operations. Cryptography is an essential part of today's users' needs, hence recent and future wireless communication systems have special needs for cryptography. Most of the widely used wireless communication systems support all different types of encryption. The user can select the best-suited algorithm for the needs of the application (McCabe, 2007).

Examples of Wireless Technologies

In this subsection we will give some examples of the well known wireless technologies, which have wide applications in many important fields.

Wi-Fi: To connect two devices wirelessly, we would typically require a Wi-Fi setup in which a router broadcasts a network and our devices - may be a PC, phone, laptop, or TV - all connect to the router. The router in turn, acts as starting point, enables the connected devices to communicate with each other. Opposed to this conventional way, with Wi-Fi Direct, compatible devices can be connected directly through generating their own wireless network. While most devices across gadget categories (TV, Printers, etc.) have Wi-Fi connectivity built-in as an option. Wi-Fi Direct will be the easiest way to share data. Wi-Fi, refers to interoperable implementations of the IEEE 802.11 Wireless LAN standards certified by the Wi-Fi Alliance (Abu-Rgheff, 2007).

Cellular Network: A cellular network is a radio network distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station. In a cellular network, each cell uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed bandwidth within each cell. When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission. Cellular networks offer a number of advantages over alternative solutions (Agrawal & Zeng, 2003):

- Flexible enough to use the features and functions of almost all public and private network.
- Increased capacity.
- Reduced power use.
- Larger coverage area
- Reduced interference from other signals

In a cellular radio system, a land area to be supplied with radio service is divided into regular shaped cells, which can be hexagonal, square, circular or some other regular shapes, although hexagonal cells are conventional. Each of these cells is assigned multiple frequencies ($f_1 - f_n$) which have corresponding radio base stations. The group of frequencies can be reused in other cells, provided that the same frequencies are not reused in adjacent neighboring cells as that would cause interference. The increased capacity in a cellular network, compared with a network with a single