Chapter VIII
Wireless Technologies for Mobile Computing

Biju Issac
Information Security Research (iSECURES) Lab and Swinburne University of Technology–Sarawak Campus, Malaysia

C.E. Tan
University Malaysia Sarawak, Malaysia

ABSTRACT

Mobility and computing were two concepts that never met a decade or two ago. But with the advent of new wireless technologies using radio propagation, the impossible is now becoming possible. Though there are many challenges to be overcome in terms of improving the bandwidth and security as with a wired network, the developments are quite encouraging. It would definitely dictate the way we do transactions in future. This chapter briefly explores some popular wireless technologies that aid in mobile computing, like 802.11 networks, Bluetooth networks, and HomeRF networks. Under 802.11 networks, we investigate the details of both infrastructure and ad hoc networks and its operations. The reader is thus made aware of these technologies briefly along with their performance, throughput, and security issues, which finally concludes with user preferences of these technologies.

INTRODUCTION

Wireless networks are generally implemented with a transmission system that uses radio waves for the carrier and this implementation usually is done at the physical layer of the network. These networks allow you to eliminate messy and intertwined cables. Wireless connections offer great mobility options, but on the negative side there can sometimes be other radio interference that might block or distort the original signal. Wireless networks can be commonly found on

college campuses, offices, and in public places like airports, coffee cafes, and so forth. Among the myriad of applications and services that are executed by mobile devices, network and data services are on the rise. According to a recent study by Cahners In-Stat Group, the number of subscribers to wireless data services will grow rapidly from 170 million worldwide in 2000 to more than 1.3 billion or more in 2004 and later years and the number of wireless messages sent per month will rise from 3 billion in early 2000 to 244 billion or more by 2005 and later years. That clearly trumpets the fact that mobile computing cannot be ignored! We plan to briefly investigate some selective wireless technologies that help mobile computing, like 802.11 networks (with infrastructure mode and ad hoc mode), Bluetooth, and HomeRF.

IEEE 802.11 INFRASTRUCTURE WIRELESS NETWORK

The IEEE 802.11 family consists of different standards. The initial standard was approved in 1997 and it backed wireless local area network medium access control (MAC) and physical layer (PHY) specifications that supported 1 Mbps and 2 Mbps data rate over the 2.4 GHz ISM band using frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS) as radio technologies, along with infrared technologies as well. WLAN (wireless local area network) configurations vary from simple, independent, peer-to-peer connections between a set of PCs, to more complex, intrabuilding infrastructure networks. There are also point-to-point and point-to-multipoint wireless solutions. A point-to-point solution is used to bridge between two local area networks and to provide an alternative to cable between two geographically distant locations. Point-to-multipoint solutions connect several, separate locations to one single location or building. Both point-to-point and point-to-multipoint can be based on the 802.11 standard. In a typical WLAN infrastructure configuration, there are two basic components: access points and wireless stations. An access point/base station connects to a local area network (LAN) by means of Ethernet cable. Usually installed in the ceiling or other specific locations, access points receive, buffer, and transmit data between the WLAN and the wired network infrastructure. A single access point supports on the average, 20 users and has a coverage varying from 20 meters in areas with obstacles (walls, stairways, elevators) and up to 100 meters in areas with clear line of sight. A building may require several access points to provide complete coverage and allow users to roam seamlessly between access points. A wireless network adapter connects users via an access point to the rest of the LAN. A wireless station can be a PC card in a laptop, an ISA, or PCI adapter in a desktop computer, or can be fully integrated within a handheld device. Security of a WLAN is of great concern with wired equivalent privacy (WEP) encryption design weakness. EAP-RADIUS server with temporal key integrity protocol (TKIP) is proposed as an interim solution to mitigate security attacks. As a long term solution, 802.11i is working on making advanced encryption standard (AES) as the future encryption standard (Gast, 2002). 802.11n provides higher throughput improvements and is intended to provide speeds up to 500 Mbps. We would like to investigate the co-existence scenarios of different 802.11 standards.

802.11 WLAN STANDARDS AND CO-EXISTENCE ANALYSIS

There are different wireless LAN technologies that the IEEE 802.11 standard supports in the unlicensed bands of 2.4 and 5 GHz. They share the same medium access control (MAC) over two PHY layer specifications: direct-sequence spread spectrum (DSSS) and frequency-hopping