1

Introduction

A wireless communication network is a computer network that uses a wireless connection between network nodes. Wireless networking is a method to connect telecommunications networks, and business installations or to connect between various equipment locations, to avoid the costly process of introducing cables. Examples of wireless communication networks include cellular networks, wireless local area networks (WLANs), wireless ad-hoc networks, wireless sensor networks, vehicular communication networks, and satellite communication networks. Wireless communication networks are becoming ubiquitous with the increasing of mobile Internet applications, advances of technological development in radio communications and communication infrastructure backbones, as well as mobile wireless devices and consumer electronics [1]. Over the last three decades, we have witnessed several critical moments for the evolution of next generation wireless communication networks. During the 1990s, we witnessed the popularity of personal computers and Internet access for common households as well as the accessible of 2G cellular wireless communications. During the 2000s, we witnessed the tremendous increasing e-commerce on the Internet and the deployment of 3G cellular wireless communications, as well as WLANs for mobile Internet. Since 2010, we have witnessed increasing bandwidth and quality-of-service for 4G cellular wireless communications with more and more applications on the mobile Internet. The wireless communication technology is continuing to be advanced to the next generation with high capacity, low latency, and low energy consumption, for better implementation of Internet of things and many other new service capabilities. From the beginning, security for wireless communication networks has always been a critical issue. In this chapter, a brief introduction will be given on wireless communication networks and basic concepts on wireless communication network security.

1.1 General Computer Communication Network Architecture

1.1.1 Wired Communication Network Infrastructure

Computer communication networks interconnect a collection of network nodes including computer and communication devices, routers, gateways, and switches [2]. The Internet can be considered as the largest computer network that interconnects billions of autonomous nodes around the globe. Obviously, standalone computer is not the only type

Security in Wireless Communication Networks, First Edition. Yi Qian, Feng Ye, and Hsiao-Hwa Chen.

Companion website: www.wiley.com/go/qian/sec51

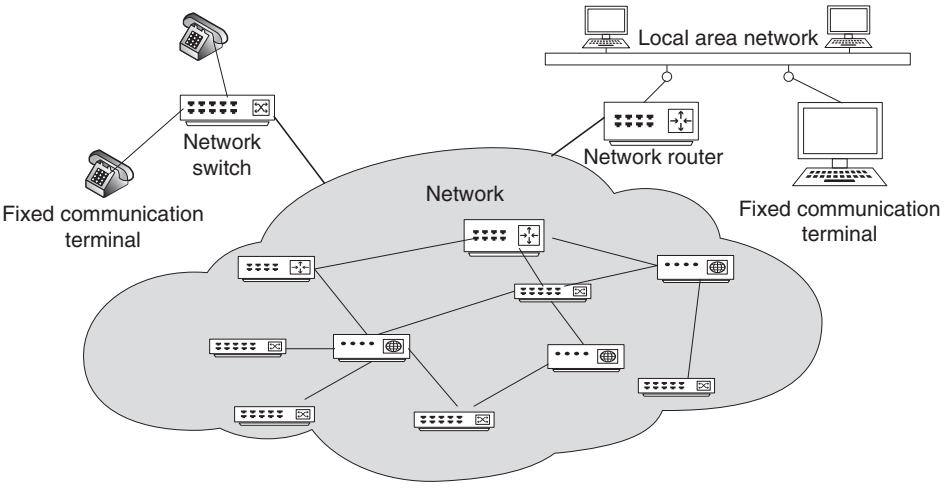

Figure 1.1 Traditional wired networks.

of device that has network access. Smart phones, tablets, smart sensors, vehicles, and many other devices are also connected to computer networks. With the network, data collection and data exchange can be enabled to support further control required by some services. Computer networks have been developed and deployed for many years. In general, computer networks are comprised of wired networks and wireless networks. Although wireless networks are more accessible to regular users in today's communications, the backbone infrastructures still rely significantly on wired networks. Figure 1.1 shows a generic framework of traditional wired networks. User equipment in wired networks is referred to as *fixed communication terminals* due to limited mobility. In the early days, user equipment such as land-line telephones and desktop computers are directly connected to a network switch or a network router through physical network cables. In modern data centers and cloud computing centers, the servers are also hard wired to switches or routers. The core network consists of many switches and routers that are interconnected with physical medium, such as copper wire, Ethernet cable, fiber optics, etc.

1.1.2 Wireless Communication Network Infrastructure

Computer and communication nodes access a wireless communication network through wireless links. However, despite the name, most wireless communication systems only deploy wireless components at the edge of the communication infrastructure, as shown in Figure 1.2. The core network in a general wireless communication infrastructure is a wired network. For example, in a cellular network, its core infrastructure is connected by fiber optic cables and Ethernet. Users are aware of the wireless access only from their user equipment, such as smart phones, tablets, laptops, etc. The wireless access is provided with extra components and resources to the core network infrastructure. The extra components and resources include:

- *Wireless transceivers*: base stations, access point (AP), mobile stations (MSs), etc.
- *Management entities*: mobility management, power management, radio resource management, security management, etc.

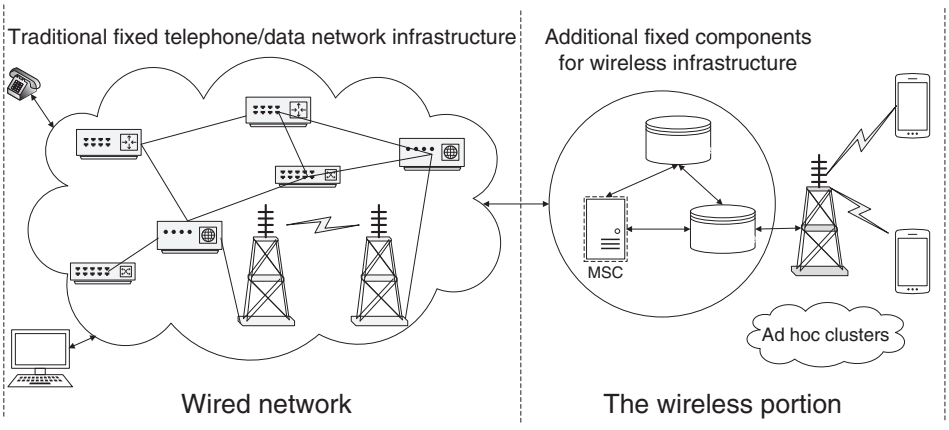

Figure 1.2 Positioning of wireless networks.

- *Spectrum*: radio frequency bands for data transmission and possible air interface.
- *Deployment*: spectrum reuse in communications, wireless network design, etc.

One advantage of wireless communication networks is flexible access from user equipment. Network access can be provided to any user who is within the radio coverage. Therefore, wireless access is more flexible and more convenient compared with wired access. Wireless users would not be restricted by the limited number of Ethernet ports or not long enough cables. The deployment cost of wireless communications is also less than that of wired communications in most cases. For example, a home Wi-Fi network can be established with a single Wi-Fi router, while a traditional Ethernet based home network would require a bulk of Ethernet cables.

1.2 Different Types of Wireless Communication Systems

1.2.1 Classification of Wireless Communication Systems

Wireless communication systems can be classified in several ways, based on *coverage, topology*, or *mobility*, as illustrated in Figure 1.3.

1.2.1.1 Based on Coverage

Wireless communications systems are classified into *wireless personal area networks (WPANs)*, *wireless local area networks (WLANs)*, and *wireless wide area networks (WWANs)*. This classification depends on wireless technology limitations as well as its supporting applications. For example, while both Bluetooth and Wi-Fi can provide a radio coverage large enough for an office, only Wi-Fi is considered as a WLAN. Subtle differences exist due to other classification criteria as well. In some classification, wireless metropolitan area networks may be listed as one type of wireless communication system. Wide area networks in traditional wired computer networks are usually the backbone infrastructure. However, a wireless metropolitan area network has the largest coverage before it is connected to the

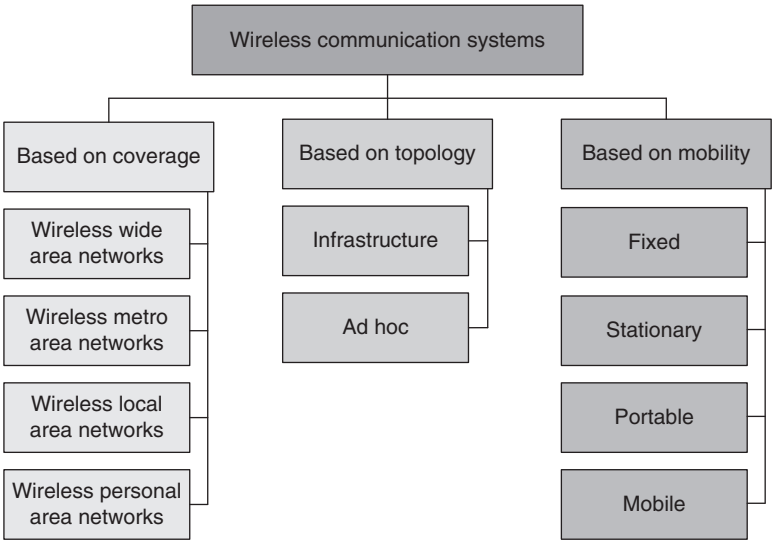

Figure 1.3 Classification of wireless communication systems.

wide area network backbone. Thus, without loss of generality, both wireless metropolitan area networks and WWANs will be considered the same (as WWANs) in this book.

1.2.1.2 Based on Topology

Wireless communication systems are classified into *infrastructure* based and *ad-hoc* based. An infrastructure based wireless communication system requires a fixed backbone communication infrastructure. For example, a cellular network has wireless access from user equipment, but it requires a fixed base station and a backbone network infrastructure. A home Wi-Fi has wireless access from user equipment, but it requires a fixed router that is hard-wired to an Internet service provider. An ad-hoc wireless communication system does not require a fixed infrastructure. For example, a wireless headphone may be connected to a smart phone using Bluetooth technology. In this communication system, data communication between the headphone and the smart phone is wireless based on Bluetooth technology, while a fixed infrastructure is not required for neither end.

1.2.1.3 Based on Mobility

Wireless communication systems are classified into *fixed*, *stationary*, *portable*, and *mobile*. A fixed wireless communication system indicates fixed deployment of equipment. For example, cellular base stations that are micro-wave based only. A stationary wireless communication system indicates a semi-fixed deployment of equipment. For example, a temporary relay vehicle for cellular systems. A portable wireless communication system indicates a more flexible deployment of equipment, with communications enabled when users are not moving fast. For example, users in a home Wi-Fi may have network service with their portable devices. A mobile wireless communication system requires support for services during high speed movement. For example, a general cellular network is a mobile system since services are provided to users, whether moving or not, as long as they are within the radio coverage.

1.2.2 Wireless Personal Area Networks

A WPAN can be used for communications among the personal devices themselves. Therefore, a WPAN usually has an ad-hoc topology. As shown in Figure 1.4, master–slave mode and mesh mode are the two types of ad-hoc networks that can be applied for WPANs. A master–slave ad-hoc network consists of a master node and multiple slave nodes. The master node defines a *cell* or *piconet*. The slave nodes within the piconet connect to the master device. A WPAN based on Bluetooth typically applies master–slave mode. For example, if a wireless headphone is connected to a smart phone using Bluetooth, then the smart phone is the master node where the headphone is a slave node. The user may also connect a Bluetooth keyboard to the same smart phone as a slave node. Some WPANs apply mesh mode, where nodes are interconnected with wireless links without forming a specific cell or piconet, for example, sensor networks, radio-frequency identification (RFID), vehicular ad-hoc networks, etc.

1.2.3 Wireless Local Area Networks

WLANs are infrastructure based wireless communication systems. They are normally built on top of a wired local area network (LAN). One of the typical WLAN settings is a home Wi-Fi, which forms one basic service set (BSS) that includes one AP and multiple user devices. The AP may have extra Ethernet ports to support wired access from servers, desktops, and other devices. As shown in Figure 1.5, a WLAN may have extended service set (ESS) that supports multiple BSSs, similar to a traditional Ethernet based LAN. All APs are interconnected, in most cases through wired connection. A user may be within the radio coverage of multiple APs, nonetheless, each user belongs to one BSS only at a time. That is to say, each user can have access to one AP only in an ESS.

1.2.4 Wireless Wide Area Networks

WWAN has the largest service coverage in all wireless communication systems. As shown in Figure 1.6, a general architecture of WWANs has different components at the radio level, the network level, and the management level.

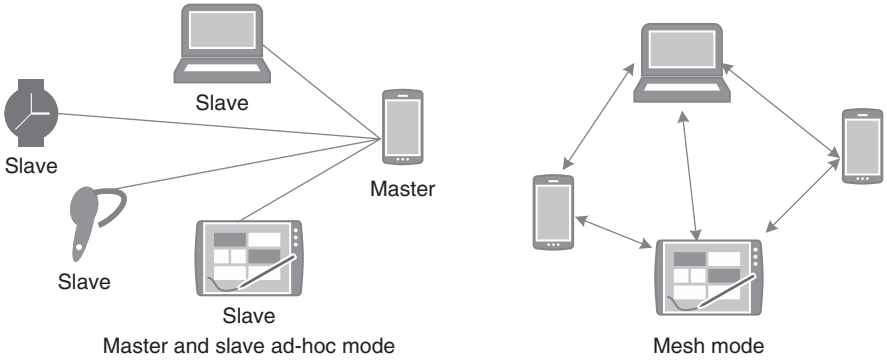

Figure 1.4 Architecture of wireless personal area networks.

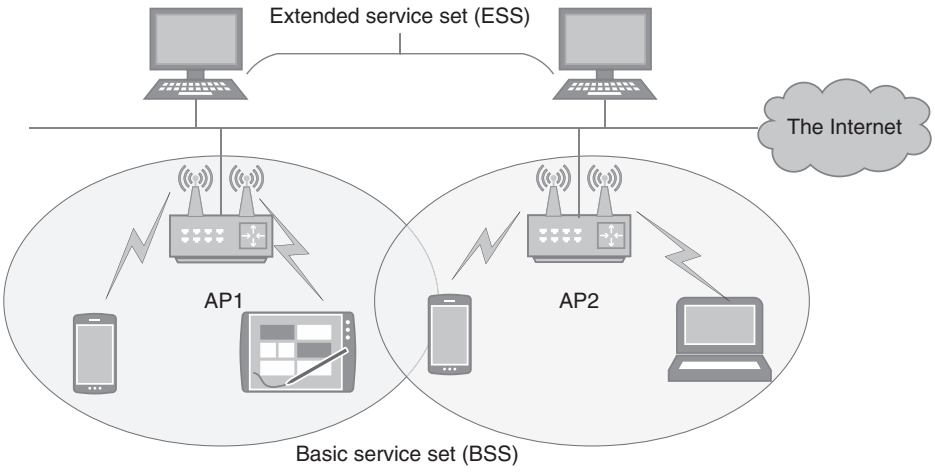

Figure 1.5 Architecture of wireless local area networks.

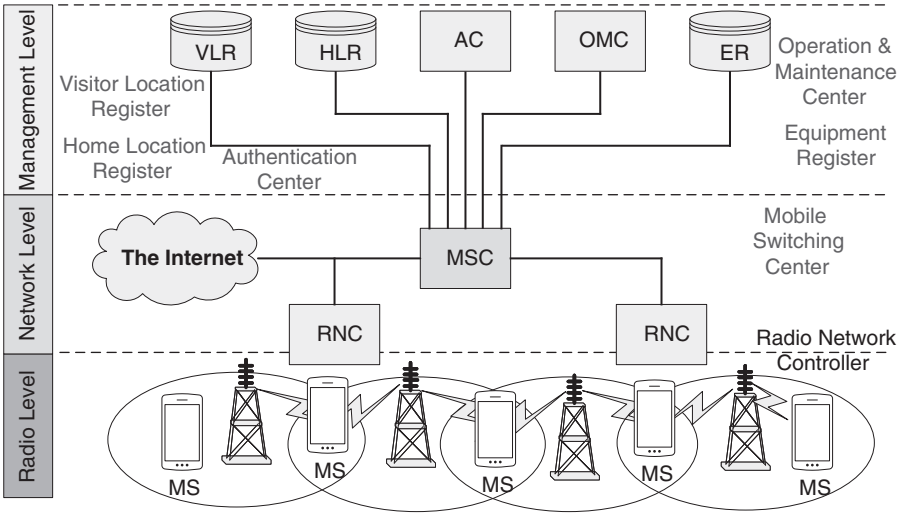

Figure 1.6 Architecture of wireless wide area networks.

The radio level provides wireless access to user equipment, or mobile stations (MSs), which can be a mobile phone, a smart watch, a vehicle, etc. MSs access to WWAN through points of access in the infrastructure. Point of access is the physical radio transceiver. It creates the air interface and communications with MSs. Points of access could be base stations, base transceiver subsystem, mobile data base station, AP, NodeB, eNodeB, etc., depending on the wireless technology it is deployed.

The network level is the backbone infrastructure that connects all switches and routers in the network. A radio network controller (RNC) bridges the radio level and the network level. RNC provides spectrum and power management to base stations, as well as other issues in wireless access. A mobile switching center (MSC) in the network level is a mobile

data intermediate system that bridges the network level and the management level in cellular communication systems. MSC manages mobility of devices and keeps track of the location of MSs. MSC also ensures security by using the authentication center and equipment register in the management level to prevent fraudulent devices from using the network.

The management level performs administrative operations of network service providers, such as accounting and billing. In a cellular communication system, the management level includes visitor location register, home location register, authentication center, operation and maintenance center, and equipment register.

1.3 Network Security and Wireless Security

1.3.1 Network Security

Network security is subject to the context in which it is used. Network security is also dictated by the needs of individuals, customs and laws of a region, and policies of an organization. There are different kinds of security breaches. For example, an unauthorized person gets access to confidential records across a network. A malicious user picks up and modifies an authorization file over a network. Or a data file has been received however the sender denies having sent it. All of those examples are security attacks in different ways. In general, *network security is defined as protection of networks and their services from unauthorized modification, destruction, or disclosure*. Network security provides assurance that the network performs its critical functions correctly, with no harmful side-effects [3]. Network security focuses mainly on networks, network protocols, and network applications. It includes all network devices, all applications, an data utilizing a network. For example, routers, switches, smart phones, tablets, etc.

Figure 1.7 illustrates the generic security terminology in a communication network system. As shown in the system, information is usually the target of security attacks. In order to protect the information, requirements and policies are first needed to be specified. Those are the overall and detailed plan for what the potential risks are, and what to protect.

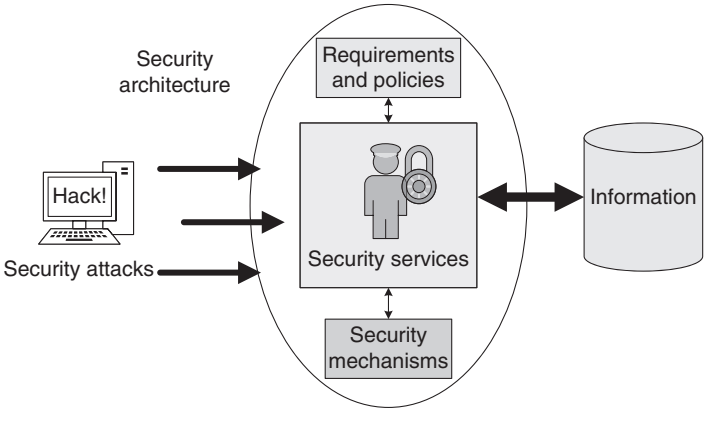

Figure 1.7 Generic security terminology.

This is a statement of what is allowed and what is not. Security services required by a system could be developed based on specific requirements and policies. For example, security services are confidentiality, integrity, availability, etc. Many security mechanisms are developed to provide various security services. Carefully designed security mechanisms detect, prevent, or recover a communication network system from security attacks. In most cases, multiple security mechanisms must be deployed together to provide just one security service. There is no single security mechanism can provide all security services in a communication network system. All the requirements and policies, security services, and security mechanism, form a security architecture of a communication network system.

1.3.2 Security Threats in Wireless Networks

Some security threats are generic in computer networks, for example, hardware sabotage, data leakage, etc. However, wireless networks have unique issues because of the shared transmission medium. Therefore, it is easier for a malicious user to get attached to wireless networks. Even if an access to a wireless communication network system is not granted due to authentication and access control, malicious users may still monitor data traffic by eavesdropping certain radio frequencies. A malicious user may also launch active attacks more easily to a wireless communication network system. For example, a malicious user could continuously send strong signals to jam a radio spectrum. Therefore, vulnerabilities and security problems in wireless communication networks are to be addressed from different aspects.

- Wireless networks suffer from limited coverage and harshness of the radio channels in physical layer. Therefore transmission in wireless networks has relatively high error rates with little to none guarantee of channel quality. Because of that, it is hard to tell denial of service (DoS) attack (an attack to make network resource unavailable to intended users) from channel degradation.
- Wireless networks require decentralized medium access mechanism in medium access control (MAC) layer because of open "broadcast" medium. Fundamental types of medium access mechanisms include frequency division multiple access (FDMA), time division multiple access (TDMA), code division multiple access (CDMA), space division multiple access (SDMA), etc. Besides access control, several other aspects, such as throughput, delay, and quality of service (QoS), also need to be addressed in MAC layer.
- Wireless networks need to deal with mobility of users. On one hand, mobility is a revolutionary advantage of wireless networks. MSs in wireless networks are not restrained to certain deployments; they are free to move within the coverage of the networks. On the other hand, mobility introduces management problems for wireless networks. For example, location tracking and handoff management as MSs move. When the scale of wireless network is large, more issues come to database management.
- Wireless networks need to manage transmission power and radio resources. Generally speaking, raising transmission power level can increase transmission quality for one link. However, interference to other users will be increased thus reducing the transmission quality of other users. Coverage of a wireless network is limited, and it is common that a MS roams from one base station to another one. The process of a MS moving from one

base station to another base station is called handoff. Bear in mind that wireless signals do not have clear boundaries; therefore handoff decision must be carefully made. If a MS moves frequently around the overlap region of two base stations, insufficient handoffs will interrupt transmission, while unnecessary handoffs can increase load to the system.

- Wireless networks are versatile. There is no single type of wireless access available everywhere. Cellular service providers adopt different kinds of wireless technologies. Therefore, very few cell phones can roam across the globe successfully. Even Wi-Fi has different specifications in each AP. For this reason, network design and deployment are to be carefully planned in wireless networks. Besides, spectrum resource is also scarce, therefore coexistence of users and interference among users must be carefully addressed.
- Security concerns in network operations and management need to be addressed in wireless networks. On one hand, network operators need to enable resources and services to MSs safely and privately. On the other hand, network operators also need to authenticate legitimate MSs, especially the roaming ones. Correct accounting and billing for subscribers are based on secure network operations and management.
- Service discovery and data management are problems to be addressed in some wireless networks, e.g. sensor networks and RFIDs. For example, how is data maintained? How to ensure integrity and confidentiality of data? Moreover, a mobile device needs to be lightweight with reasonably long battery life. Therefore, energy efficient designs of software and protocols are unique for wireless networks. While many of these security problems have been studied in wired networks, the solutions proposed there are in general too computationally demanding to work for wireless networks, because mobile devices have limited computational resources and power supply. Communications must also be minimized due to scarce spectrum resource.

1.4 Summary

This chapter gives an introduction on general communication network architectures and wireless communication architectures, as well as security threats in wireless communications networks. The same security objectives that exist in wireline communication networks are also needed for wireless networks. They must be addressed in the context of wireless specific characteristics such as physical layer issues, MAC layer issues, mobility management, radio resource and power management, wireless network design and deployment, wireless network operations and management, wireless application issues, etc. The next chapter provides more security concepts that will be mostly concerned in wireless communication networks. It is recommended to read more on the topics of wireless communication networks for better understanding of security in wireless networks [4–6].