

Chapter 7

Wireless Network Security: An Overview

Danda B. Rawat, Gongjun Yan, Bhed Bahadur Bista,
and Vigyan “Vigs” Chandra

Contents

7.1	Introduction.....	200
7.2	Cellular Telephone Networks.....	201
7.2.1	Security Issues in Cellular Networks.....	204
7.2.1.1	Security in RANs.....	205
7.2.1.2	Security in CNs.....	205
7.2.1.3	Cellular Network Security Architecture.....	205
7.2.1.4	Wireless Application Protocol.....	206
7.3	Worldwide Interoperability for Microwave Access.....	207
7.4	Wireless Local Area Networks.....	208
7.4.1	WLAN in AP Mode.....	208
7.4.2	WLANs in Ad Hoc Mode.....	210
7.4.3	Security Attacks in WLANs.....	211
7.4.3.1	Network Traffic Analysis.....	211
7.4.3.2	Passive Eavesdropping.....	211
7.4.3.3	Active Eavesdropping.....	211
7.4.3.4	Unauthorized Access or War-Xing.....	211
7.4.3.5	Man-in-the-Middle Attacks.....	211
7.4.3.6	Session Hijacking.....	211
7.4.3.7	Replay Attacks and Rouge AP.....	211
7.4.3.8	DoS Attacks.....	212
7.4.4	Security in WLAN 802.11.....	212
7.4.4.1	802.11 Authentication.....	212
7.4.4.2	Wired Equivalent Privacy.....	212

7.4.4.3	IEEE 802.1x: Extensible Authentication Protocol over LAN	213
7.4.4.4	IEEE 802.11i Standard	214
7.4.5	Best Practices	214
7.4.6	Protocol for Carrying Authentication for Network Access	215
7.5	Wireless Personal Area Networks (PANs)	216
7.5.1	IEEE 802.15: PANs	216
7.5.2	Bluetooth Network Security	216
7.5.3	IEEE 802.15.4: ZigBee Security	216
7.5.4	UWB Security	217
7.6	Best Practices for Mobile Device Security	217
7.6.1	Devices Choice	217
7.6.2	Enable Encryption	217
7.6.3	Configure Wireless Networks for Authentication	217
7.6.4	Enable and Utilize Remote Wipe Capabilities	218
7.6.5	Limit Third-Party Apps	218
7.6.6	Implement Firewall Policies	218
7.6.7	Implement Intrusion Prevention Software	218
7.6.8	Bluetooth Policies	218
7.7	Summary	218
	References	219

7.1 Introduction

Wireless communications is the fastest growing segment of the communication industry. Wireless technologies and applications have been widely deployed in various areas. Successful deployment of wireless local area networks (WLANs) in the unlicensed industrial, scientific, and medical (ISM) band and cellular wireless telephone networks in the licensed band during the past decades have shown the widespread use of wireless technologies and applications. Numerous wireless applications and technologies are under development and deployment. Wireless networks consist of various types of devices that communicate without a wired medium. Generally, wireless networks can be categorized into two different types based on the structure of the networks: infrastructure-based wireless networks and infrastructureless wireless networks [1].

An infrastructure-based wireless network has a central unit through which client stations communicate with each other. Cellular telephone systems such as Global System for Mobile Communications (GSM) or code-division multiple access (CDMA) and the IEEE 802.11 WLAN in access point (AP) mode and the IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMAX) are some examples of infrastructure-based wireless networks. GSM, CDMA, and their variants are the most widely deployed cellular communication technologies that made mobile communications possible. GSM and CDMA use base stations through which mobile phones communicate with each other. Generally, cellular wireless networks cover a wide area and are known as wireless wide-area networks. Similarly, the WiMAX network also has centralized base stations used by wireless clients when they communicate with each other. The coverage area of WiMAX is closer to metropolitan areas and is known as a wireless metropolitan area network (WMAN). WLANs in infrastructure mode use centralized wireless APs through which wireless client stations communicate with each other. As the centralized base stations or APs in infrastructure-based wireless networks are mostly static and costly, such networks require serious and careful topology design for better performance and coverage.

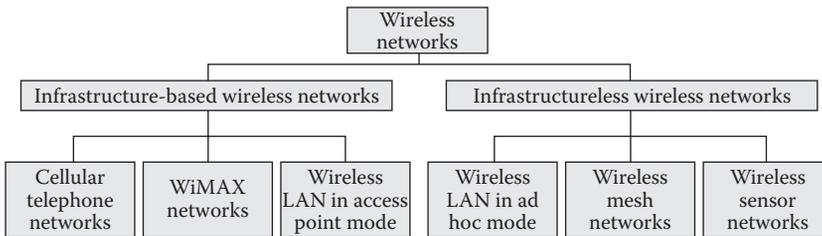


Figure 7.1 Classification of wireless networks.

An infrastructureless wireless network does not contain any centralized infrastructure, and thus, wireless client stations communicate with each other directly in a peer-to-peer manner. These types of networks are also known as wireless ad hoc networks. The network topology of the wireless ad hoc network is dynamic and changes constantly, and the participating wireless stations adapt to changes in topology on the fly [2,3].

Subcategories of wireless networks under centralized infrastructure-based and infrastructureless wireless networks are depicted in [Figure 7.1](#). Cellular networks are for voice communications but also carry data. WiMAX, on the other hand, is for last-mile Internet delivery for a larger coverage area. WLANs are for data communication within smaller areas, typically for office and residential use. However, voice-over-Wi-Fi is also part of WLANs. Recent advancements have shown that infrastructure-based wireless networks support both voice and data communications.

Infrastructure-based wireless networks need fixed infrastructures such as base stations in cellular telephone networks and WiMAX networks, or WAPs in WLANs to facilitate communications among mobile users. The stationary equipment serves as a backbone for these kinds of wireless networks. Mobile users connect to this equipment through wireless links and can move anywhere within a coverage area of a base station. They can also move from one base station's coverage area to another by using handover features. For example, a cellular telephone system consists of a fixed base station for a region called a cell [1], and each cell can handle a number of mobile users. While communicating, mobile users can move within a coverage area of a base station and from one base station to another by using roaming features. To cover a large area and a large number of users, multiple base stations are needed, and base stations are connected with each other by a reliable wired or wireless link to provide seamless wireless service. Interconnecting links should be robust in terms of reliability, efficiency, fault tolerance, transmission range, etc., to provide uninterrupted service [4,7].

7.2 Cellular Telephone Networks

Cellular communication has become an important part of our daily life. At present, almost 2.3 billion users have subscribed for telephone services. It is predicted by Gartner that, by 2013, mobile devices such as personal digital assistants will surpass personal computers for Internet browsing as cellular telephone networks offer mobile communications. Cellular telephone communications use a base station to cover a certain area known as *cell* [1]. Mobile users connect to their base station to communicate with each other. They can move within a cell during communications and can move from one cell to another using handover technique without breaking communications. Wireless systems are prone to interference from other users who share the same frequency for communications. To avoid interference between cells, adjacent cells use different frequencies, as shown in [Figure 7.2](#).

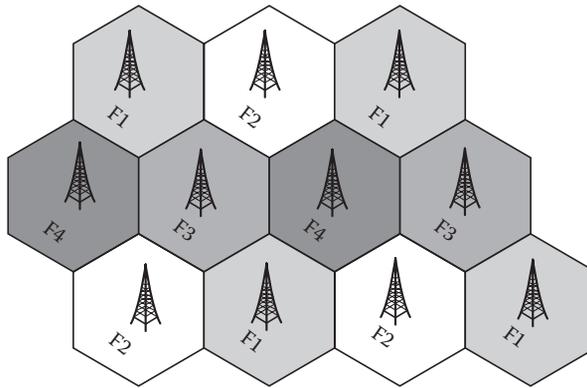


Figure 7.2 Cells with different frequencies in cellular telephone networks.

Cellular networks have been commercially available since the early 1980s. Japan implemented cellular telephone systems in 1979 and became the first country to deploy a cellular telephone network. European countries implemented Nordic Mobile Telephony in 1982. The United States deployed Advanced Mobile Phone System (AMPS) as the first cellular telephone network in 1983 [4].

There are different generations of cellular telephone systems [1,4]. First-generation (1G) wireless telephone networks were the first cellular networks that are commercially available. A 1G network was able to transmit voice with maximum speed of about 9.6 kb/s. 1G telecommunication networks used analog modulation to transmit voice and are regarded as analog telecommunication networks.

The 1G cellular system has some limitations such as poor voice quality, no support of encryption, inefficient use of frequency spectrum, and poor interference-handling techniques. Personal communication services introduced the concept of digital modulation, in which the voice was converted into digital code and became the second-generation (2G) cellular telephone system. 2G being digital addressed some of the limitations of 1G and was deployed using different signal representation and transmission techniques.

In the United States, CDMA, North American Time-Division Multiple Access, and Digital AMPS (D-AMPS) have been deployed as the 2G cellular network. In Europe, time-division-multiplexing-based GSM has been deployed, whereas in Japan, Personal Digital Cellular has been deployed. The GSM-based cellular system has become the most widely adopted 2G technology in the world.

2G's primary focus was voice communications, although it served as a remedy for the several limitations of 1G. Active research for data communications, along with voice communication service, resulted in data services over 2G being developed and became 2.5G. 1xEV-DO and 1xEV-DV have been deployed as 2.5G in the United States. 1xEV-DV uses a single radio-frequency channel for data and voice, whereas 1xEV-DO uses separate channels for data and voice.

High-speed circuit switched data (HSCSD), General Packet Radio Service (GPRS), and Enhanced Data Rate for GSM Evolution (EDGE) have been deployed in Europe. HSCSD was the first attempt at providing data at high-speed data communication over GSM with speeds of up to 115 kb/s.

However, this technique cannot support large bursts of data. The GPRS can support large burst data transfers, and it had a service GPRS support node (SGSN) for security mobility and

access control and a Gateway GPRS support node (GGSN) to connect to external packet switched networks. EDGE provides data rates of up to 384 kb/s. Cellular digital packet data detect idle voice channels and use them to transmit data without disturbing voice communications.

The third-generation (3G) cellular system was developed with the goal of providing fast Internet connectivity, enhanced voice communication, video telephone, etc. CDMA2000 in the United States, Wideband CDMA (WCDMA) in Europe, and Time-Division Synchronous CDMA in China were deployed as 3G cellular networks. This process started in 1992 and resulted in a new network infrastructure called International Mobile Telecommunications 2000 (IMT-2000). IMT-2000 aimed the following [5,6]:

- To offer wide range of services over a wide coverage area
- To provide the best quality of service (QoS) possible
- To accommodate a variety of mobile users and stations
- To admit the provision of service among different networks
- To provide an open architecture and a modular structure

3G has been deployed in most countries and is being used in major communication networks. Service providers have already started deploying fourth-generation (4G) cellular communication systems, which offer data rates of up to 20 Mb/s and support mobile communication in moving vehicles with speed up to 250 km/h.

4G aims to incorporate high QoS and mobility in which a mobile user terminal will always select the best possible access available. 4G also aims to use mobile Internet Protocol (IP) with the IPv6 address scheme, in which each mobile device will have its own globally unique IP address.

It is important to understand the architecture of cellular networks to see its related security issues. A cellular network has two main parts [7]:

- Radio access network (RAN)
- Core network (CN)

Mobile users gain access wirelessly to the cellular network via the RAN, as shown in [Figure 7.3](#). The RAN is connected to the CN. The CN is connected to the Internet via gateways through which mobile users can receive multimedia services. The CN is also connected to a public switched telephone network (PSTN). A PSTN is a circuit switched telephone public telephone network that is used to deliver calls to landline telephones. It uses a set of signaling protocols called Signaling No. 7 (SS7) that is defined by the International Telecommunication Union. SS7 provides telephony functions. The CN provides the interface for the communication among mobile users and landline telephone users.

The RAN consists of existing GPRS, GSM, or CDMA cellular telephone networks in which the radio network controller or base station connector is connected to packet switched CN to provide the interaction between the RAN and the CN.

The CN consists of circuit switch networks, packet switched networks, and IP multimedia networks. The high-end network servers facilitate the CN and provide several functions through the home location register to maintain subscriber information, the visitor location register to maintain temporary data of subscribers, the mobile switching center (MSC) to interface the RAN and the CN, and the gateway switching center to route the calls to the actual location of mobile users [8].

Every subscriber is permanently assigned to a home network and is also affiliated with a visiting network onto which it can roam. The home network is responsible in maintaining subscriber

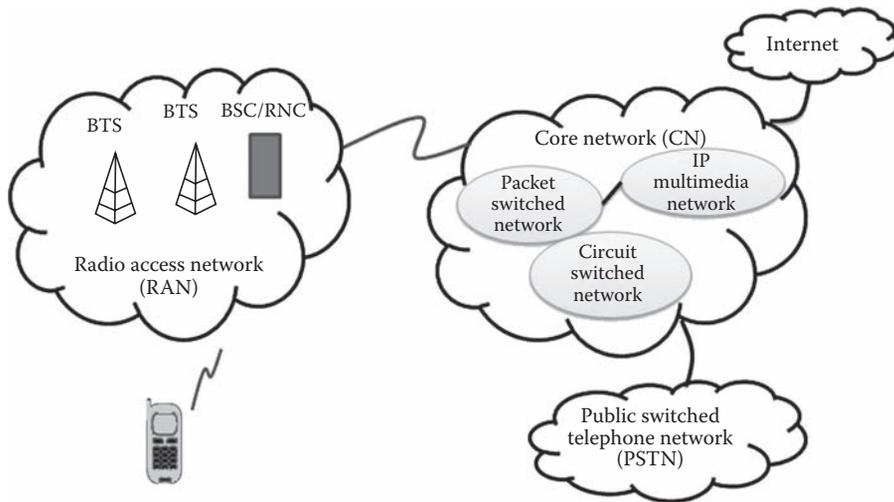


Figure 7.3 Cellular telephone network architecture.

profile and current location. The visiting network is the network where a mobile user is currently roaming. It is important to note that the visiting networks provide all the functionality to mobile users on behalf of the home network.

IP-based servers such as DNS, Dynamic Host Configuration Protocol (DHCP), and RADIUS servers interact with the gateways and provide control and management functions needed for mobile users while getting service from the Internet.

7.2.1 Security Issues in Cellular Networks

Multiple entities are incorporated in cellular telephone networks, and the infrastructure for supporting these services is massive and complex. IP multimedia Internet connection with the CN in a telephone network presents a big challenge for the network to provide security. Wireless networks, in general, have many limitations compared to wired networks [6,7]:

- Radio signal travels through an open wireless access medium such as air
- Limited bandwidth shared by many mobile users
- Mobility in wireless networks makes the system more complex
- Mobile stations run on limited time batteries resulting in power issue in wireless systems
- Small mobile devices have limited processing capabilities
- Unreliable network connection for mobile users

Apart from the above listed limitations, several security issues need to be considered when deploying a cellular network. There are varieties of attacks in the wireless cellular network:

1. Denial of service (DOS) caused by sending excessive data to the network so that the legitimate users are unable to access network resources.
2. Distributed DOS is a result of attack by multiple DoS attackers.
3. Channel jamming by sending a high power signal over the channel that denies access to the network.

4. Unauthorized access to the network by illegitimate users.
5. Eavesdropping in wireless communications.
6. Message replay: it can be done even if the transmission is encrypted by sending an encrypted message repeatedly.
7. Man-in-the-middle attack: attacker poses as a relay station between a sender and a receiver.
8. Session hijacking: hijack the established session and pretend as a legitimate user.

7.2.1.1 Security in RANs

In RANs, mobile users connect with each other wirelessly through a base station. A determined attacker with a radio transmitter/receiver can easily capture the radio signal transmitted on the air. In 1G and 2G systems, there was no encryption mechanism to hide voice from a malicious user and no guard mechanism against eavesdropping on conversations between the mobile user and the base station. Because of the lack of security provision in 1G and 2G cellular telephone systems, the attacker can not only enjoy wireless service without paying for any service usage fees but can also entice mobile users through a rouge or false base station to get secret information. The 3G cellular system has security provision to prevent these types of attacks. It has an encryption mechanism with integrity keys (IKs) to encrypt the conversation, and thus, the attacker cannot change the conversation between the mobile user and the base station. 3G has also improved radio network security. However, it still cannot prevent DOS attacks when a large number of requests are sent from the RAN to the visiting MSC, in which the MSC needs to verify every request through an authentication process. Because of excessive requests and authentication, the MSC may fail to serve legitimate users.

7.2.1.2 Security in CNs

CN security deals with security issues at the service node and wire-line-signaling message between service nodes. Protection is provided for the services that use the Mobile Application Part (MAP) protocol. Security for the MAP protocol is provided either through MAP security (MAPSec) when the MAP runs on the SS7 protocol stack or IPSec when the MAP runs on top of the IP. 3G also lacks in security for all types of signaling messages. However, the end-to-end security (EndSec) protocol proposed in [9] can prevent misrouting the signal.

Internet connectivity through a mobile device introduces the biggest threat to cellular network security. Any attacks that are possible on the Internet can now be entered into the CN via gateways located between the CN and the Internet. One example of this is the attack to the E-911 service [10]. Short message and voice conversation still use the same channel, resulting in contention and collision between them. Preclusion of the entire CN (servers for PSTN, circuit, and packet switched network services) from attacks that are coming through the Internet link is an important consideration. As the PSTN uses the SS7 protocol that does not have any authentication mechanism and transmits voice messages in plain text, the attacker can easily introduce fake messages or attack by DOS. Only a limited amount of research has been undertaken for securing PSTN [11].

As mentioned above, the cellular network has many new services, and the security architecture needs to provide security for all these services.

7.2.1.3 Cellular Network Security Architecture

A cellular network security architecture consists of five sets of features, as shown in [Figure 7.4](#).

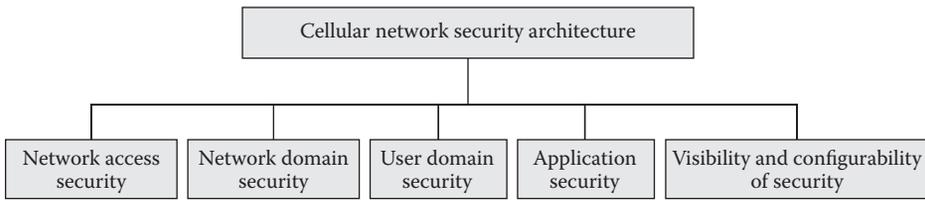


Figure 7.4 Cellular network security architecture.

Network access security is responsible for providing authentication of user and mobile device, confidentiality, and integrity. It enables mobile users to access cellular network services securely. International Mobile Equipment Identifier and secret cipher key (CK) are used to provide confidentiality of both the device and the user. The challenge response method using a secret key is used to achieve authentication. It is worth noting that the Authentication and Key Agreement provides mutual authentication for the user and the network. A CK and an IK for which the user and the network agree are used until their time expires. Integrity protection in a cellular network is necessary as control signaling communications between a mobile station and a network is sensitive. An integrity algorithm and IK provide the integrity service.

Network domain security enables nodes in the service provider to securely exchange the signaling data and prevent attacks on the wired networks.

User domain security enables mobile stations to securely connect to the base station and prevent external attacks.

Application security provides secure mechanisms to the exchange of messages between users of the user domain and services of the service provider domain for different applications.

The feature of *visibility and configurability of security* allows users to query what security features are available to them and what features they can use.

7.2.1.4 Wireless Application Protocol

Cellular networks are connected to the Internet through CNs to provide Internet access to mobile users using the Wireless Application Protocol (WAP) [12]. Thus, it is important to understand the security mechanisms of the protocol used to access the Internet via the CN. WAP is an open specification protocol, meaning that it is independent of the underlying networks. It is platform- and technology-independent and thus provides Internet access service to users who use WCDMA, CMDA 2000, UMTS, or any operating systems such as Windows CE, PALM OS, etc. The first version of WAP (WAP1) was released in 1998. WAP1 considers that a wireless mobile device has limited power and other resources and has limited security features and thus communicates through other gateways while communicating with the servers. The second version of WAP (WAP2) was released in 2002. It assumes that mobile devices are powerful. It has better security features and allows mobile users to directly communicate with the servers.

WAP2 protocol stack/layers shown in [Figure 7.5](#) are briefly discussed as follows:

1. *Wireless application environment (WAE)*: This layer is like an application layer in the OSI reference model and provides an environment for WAP applications such as web applications.
2. *Hypertext Transfer Protocol*: This layer deals with a platform-independent protocol that is used for transferring web content/pages.

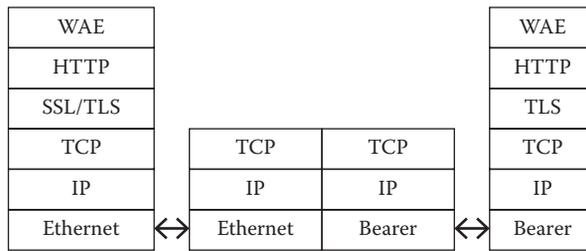


Figure 7.5 WAP2 protocol stack.

3. *Transport layer security (TLS)*: This is the fourth-layer (from bottom) protocol that provides security features such as confidentiality, integrity, and authentication. TSL used in WAP2 is known as profiled TLS, which consists of a cipher and authentication suites, session resume from identification suites, and tunneling capability.
4. *Transport Control Protocol (TCP)*: This is the third-layer (from bottom) protocol that is a standard reliable TCP.
5. IP: This is the second-layer (from bottom) protocol that is responsible for routing data in a network.
6. Bearer Protocol: This is the lowest level protocol that can be used by any wireless techniques (e.g., CDMA, GSM, WCDMA, etc.) used in cellular telephone networks.

Overall, multiple layers of the protocol stacked with multiple layers of encryption address the security issues in existing 3G wireless cellular networks, which consume more power and introduce high transmission delay. In 4G, only one layer is responsible for encrypting data using interlayer security [13], which reduces communications delay.

7.3 Worldwide Interoperability for Microwave Access

WiMAX [14] is a WMAN that can offer data transfer rates of up to 75 Mb/s or an area of radius of about 50 km (30 mi.) and is part of 4G wireless communication technology. WiMAX was released in December 2001 as an IEEE 802.16 standard. The IEEE 802.16 uses three major frequency bands: 10–66 GHz (licensed bands), 2–11 GHz (licensed bands), and 2–11 GHz (unlicensed bands).

WiMAX still has some shortcomings in terms of security as designers have incorporated the use of the preexisting standard Data over Cable Service Interface Specifications (DOCSIS) that was used in cable communication [15]. Among different IEEE 802.16 standards, 802.16a/d standards make use of public-key encryption keys (which are exchanged at connection setup time), and the base station authenticates the clients using 56-bit data encryption standard-based digital certificates [15]. However, it does not provide adequate protection against data forgery. IEEE 802.16e implements a 128-bit encryption key mode based on the Advanced Encryption Standard (AES) to remove the flaws that are present in 802.16a/d. The man-in-the-middle attacks launched using rouge base stations are mitigated by client-to-base-station and base-station-to-client authentication [15].

7.4 Wireless Local Area Networks

The successful deployment of WLANs in the past decade is due to their advantages such as flexibility, scalability, mobility, and freedom from wires, which wired networks lack [16]. Wireless networks are easy to install in rural areas, where wired network infrastructures are either difficult or impossible to create due to physical obstacles. Wireless networks are easily scalable, flexible, and esthetic since wireless devices communicate using mainly either radio frequency (RF) or infrared frequency.

The main standard in the WLAN is IEEE 802.11 and is also known as Wi-Fi, that is, IEEE-standardized WLAN in 1999. Wireless communications were tested in 1971 by a researcher at the University of Hawaii. The recent standard of the WLAN is IEEE 802.11-2007. IEEE 802.11 WLANs can be configured to operate in an infrastructure (AP) mode or in an ad hoc mode.

7.4.1 WLAN in AP Mode

WLANs in AP mode consist of wireless client stations (STAs) and an AP in which clients are equipped with wireless adapters that allow wireless communication among other wireless stations. In this case, the AP functions like a regular switch or router in a wired network for the wireless client stations. In AP-mode WLANs, all communications pass through an AP, meaning that wireless clients cannot communicate with each other directly.

The basic structure of a WLAN is called the basic service set (BSS), as shown in [Figure 7.6](#), in which the network consists of an AP and several wireless devices. In order to form a wireless network, the AP continually broadcasts its service set identifier (SSID), which is the logical name of the wireless network. This allows wireless client stations to locate and join the wireless network. The area covered by a transmission range of an AP is called the basic service area.

A WLAN operating in AP mode is connected to a wired network through an AP. Thus, the AP is a gateway for wireless client stations to join a wired network. One example is shown in [Figure 7.6](#) where the AP is connected to a wired network through a switch.

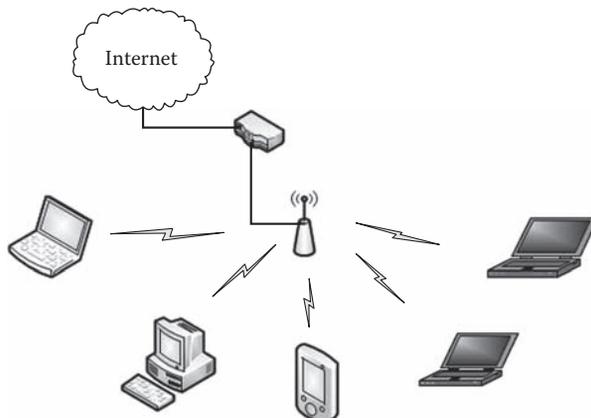


Figure 7.6 WLAN in AP mode (also known as BSS).

For roaming support, BSSs can be combined to form an extended service set (ESS). In ESSs, APs are connected to a single-backbone system to provide roaming (moving from one BSS to another BSS) for wireless client stations (STAs), as shown in [Figure 7.7](#).

In order to avoid interference, WAPs should be configured in such a way that they transmit in nonoverlapping adjacent channels, as shown in [Figures 7.7](#) and [7.8](#). If multiple APs overlap transmission ranges in the same channel, the performance of the WLAN will be significantly degraded [16].

Channel occupancy information along with the MAC address, received signal strength indication, vendor information, network types (infrastructure or ad hoc), privacy/security mode, scan time, etc., can be easily obtained using freely available tools such as inSSIDer [17], as shown in [Figure 7.9](#). The inSSIDer is a freeware wireless auditing tool that is compatible with many vendors' wireless adaptors. It can be downloaded from the MetaGeek web site [18]. Using the result of the inSSIDer, the network administrator can change the orientation or position of a WAP or clients to increase the signal strength. Furthermore, one can change the security features to secure the wireless network and channel used for wireless transmission to have the least interference in a wireless network.

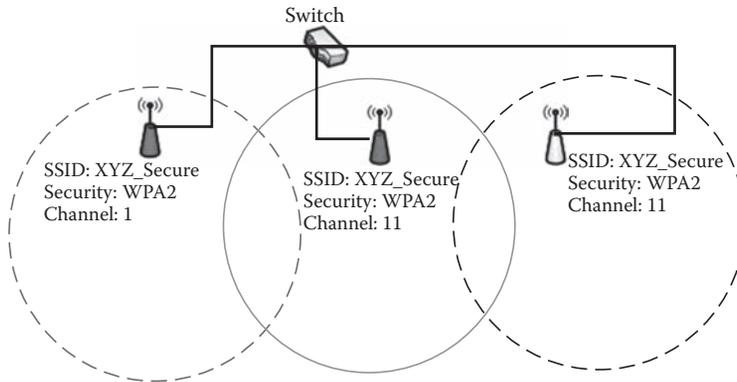


Figure 7.7 ESS.

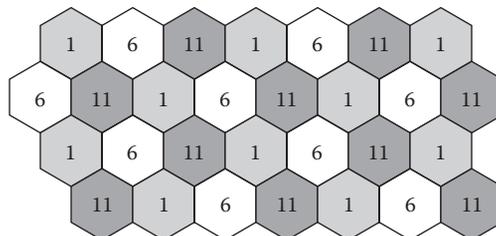


Figure 7.8 WLAN channel assignment for multiple APs.

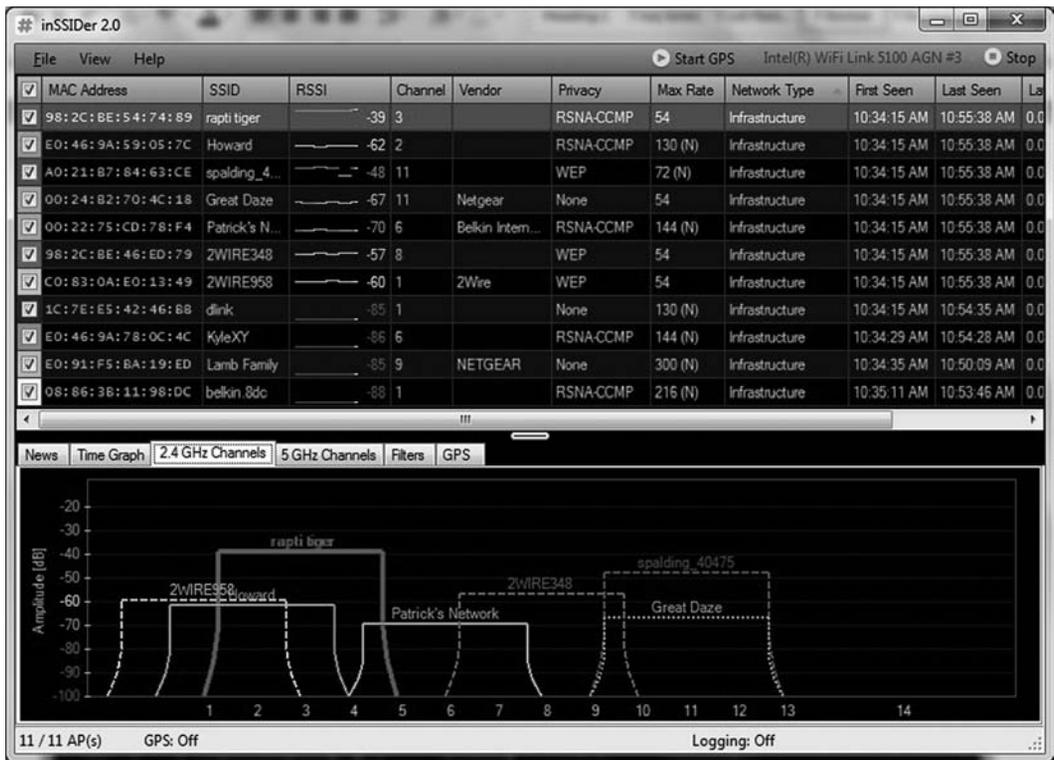


Figure 7.9 WLAN channel assignment for multiple APs.

7.4.2 WLANs in Ad Hoc Mode

When wireless devices communicate with each other directly without using centralized AP as shown in [Figure 7.10](#), the WLAN configuration is called an independent BSS (IBSS).

One of the ad hoc wireless nodes (e.g., computer) should be configured to provide SSID for wireless ad hoc networking.

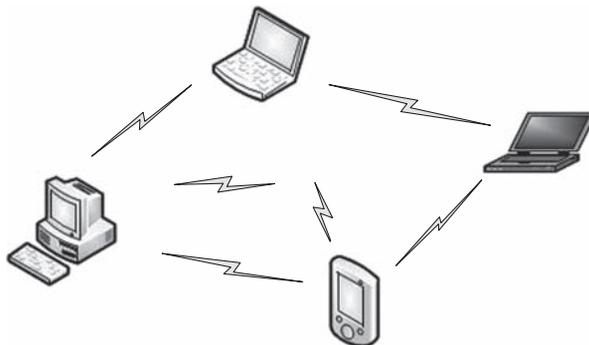


Figure 7.10 WLAN in ad hoc mode: IBSS.

7.4.3 Security Attacks in WLANs

As in other wireless networks, the medium used to transfer data from a source to a destination is the RF signal. The RF signal in a WLAN is also freely available and thus makes the WLAN susceptible to attack if it is not properly configured to secure transmission. Typical transmit power of APs lies in the range of 50–100 mW [maximum allowed range by the Federal Communications Commission (FCC) in the United States is 4 W], and the range of AP is about 300–1800 ft. [19].

After successful deployment of WLAN and handheld devices, wireless applications and devices increased exponentially, which has created major security-related issues in the network. The following is the list of most common attack types in wireless networks [16,17].

7.4.3.1 Network Traffic Analysis

To find information of the target network, the attacker uses the statistics of network connectivity, activity, AP location, SSID, etc.

7.4.3.2 Passive Eavesdropping

Attackers sniff the packet transmitted over the network and extract the network information. Networks with unencrypted setup are the victims of this type of attacks. Attackers use the extracted information to attack the network.

7.4.3.3 Active Eavesdropping

In this type of attack, the attacker tries to inject a complete packet in the data stream to change the data on the packet. Both unencrypted and encrypted types of networks can be victims of this type of attack.

7.4.3.4 Unauthorized Access or War-Xing

Unauthorized access attack can be just for free Internet access [20,21] using unauthorized login. Information about the wireless network can be obtained by War-Xing (wardriving, warwalking, warcycling, warflying, etc.) [20].

7.4.3.5 Man-in-the-Middle Attacks

In this type of attack, the attacker stays between the intended transmitter and receiver, and works as a relay station. The attacker (relay station) manipulates and pretends to be an intended sender.

7.4.3.6 Session Hijacking

In this type of attack, the attacker hijacks an authorized session and pretends to be an intended sender.

7.4.3.7 Replay Attacks and Rogue AP

In replay attacks, the attacker sends a legitimate packet several times or changes the content of the packet before transmitting it. In this type of attack, attackers set a wireless device as AP

(called rouge AP) using a special type of software and entice the legitimate users to get secret information. By imposing mutual authentication between AP and network devices, rouge AP and reply attack can be solved.

7.4.3.8 DoS Attacks

In this type of attack, the attacker sends noise continually on a specific channel to ruin network performance. RF jamming is an example of DoS attack in the wireless network [16,22].

7.4.4 Security in WLAN 802.11

The IEEE 802.11 standard consists of three layers:

1. *Physical layer*: it is responsible for providing an interface to exchange frames with the upper MAC layer.
2. *MAC layer*: it provides the functionality needed to control media access and allow reliable transfer of frames to the upper layers.
3. *Logical link control (LLC) layer*: it provides connection-oriented service to the upper layers. It also provides addressing and data link control through the LLC.

7.4.4.1 802.11 Authentication

Wireless clients must be authenticated and associated before any data transmissions. In WLANs, there are two types of authentication, that is, open authentication and shared key authentication [16,23]. Open authentication is actually no authentication at all. Any clients can be authenticated and associated in the open authentication system. In shared key authentication, when the client wants to connect to the AP, it sends a request to the AP. Once the AP receives a request, it sends a packet in unencrypted text as a challenge message. The client then encrypts this message a preshared key and sends it back to the AP. The AP decrypts it and compares it with that sent previously as a challenge. If both texts match, the client will be authenticated; otherwise, connection will be denied. In actual data transmission, wired equivalent privacy (WEP) can be used in both preshared and open authentication. It is worth noting that open key authentication is more secure than the preshared key because the latter does not have a challenge response and does not expose the WEP key to traffic sniffers [24].

7.4.4.2 Wired Equivalent Privacy

WEP was designed to provide the security level that is available in wired networks. It has three goals to achieve for WLANs: confidentiality, availability, and integrity of information [16,23]. However, WEP was proved to be breakable and thus is now considered insecure for many reasons; nonetheless, it is used to provide general security instead of leaving the network insecure. WEP provides encryption only between the wireless client station and the AP. When data travel over the wired network, it is unencrypted.

As shown in [Figure 7.11](#), WEP uses stream cipher RC4 (Ron's Code 4) for the encryption. RC4 needs an initial vector (IV) as a seed, which is used along with the shared WEP key to

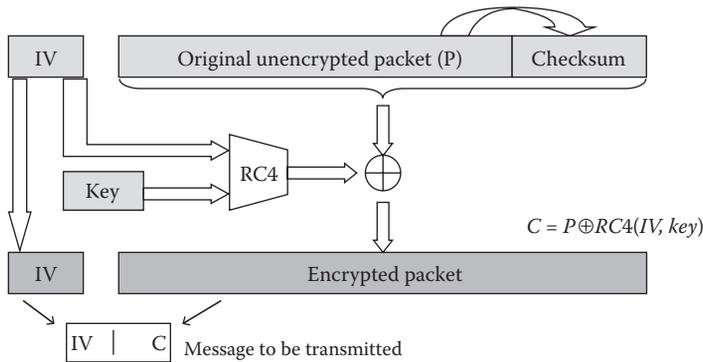


Figure 7.11 WEP packet encryption.

encrypt and decrypt the packets. From the packet to be transmitted, a checksum (cyclical redundancy checking) is calculated and attached with the payload. An exclusive OR (XOR) operation is performed between the payload and RC4 stream (generated from the shared key and the IV) to generate an encrypted packet. The unencrypted IV is appended with an encrypted packet, and the combined packet is transmitted over the wireless network. At the receiving end, reverse process takes place for decrypting the packet.

The IV is 40 bits long, and the key length is 40 bits in WEP and is 104 bits in WEP2. Using freely available tools, anyone can break WEP security used in a WLAN. After collecting a sufficient number of packets (20,000–100,000 packets), one can easily break the WEP key using freely available tools such as BackTrack, Russix, and Aircrack-ng [17].

When a WEP key is fixed, mathematically, if the same IV is used to encrypt two different packets, you can know P_2 when you have C_1 , C_2 , and P_1 [17,22,23], that is,

$$C_1 \text{ XOR } C_2 = P_1 \text{ XOR } P_2.$$

Because of many weaknesses in WEP, the WLAN was designed with Wi-Fi protected access (WPA) security modes.

7.4.4.3 IEEE 802.1x: Extensible Authentication Protocol over LAN

The IEEE 802.1x is port-based authentication to authenticate users in IEEE 802 networks. The Extensible Authentication Protocol (EAP) allows any of the encryption schemes to be implemented on top of it, adding flexibility to the security design module. The Remote Authentication Dial-In User Service (RADIUS) server is used for authentication in the 802.1x framework to provide authentication, authorization, and accounting (AAA) service for network clients, as shown in Figure 7.12 [17,22–25]. The 802.1x framework defines three entities/ports, that is, supplicant (client STA that wants to be authenticated), authenticator (AP that connects the supplicant to the wired network), and authentication server (performs the authentication process from the supplicant based on their credentials) [22,23].

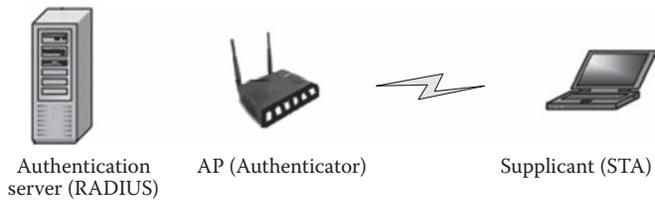


Figure 7.12 802.1x authentication.

7.4.4.4 IEEE 802.11i Standard

The IEEE 802.11i, which was released in June 2004, improves authentication, integrity, and data transfer in WLANs. To get rid of WEP weaknesses, the Wi-Fi Alliance developed WPA, which was released in April 2003. Vendors or Wi-Fi Alliance implemented the full specifications under the name WPA2, that is, 802.11i [16,17,22,23].

Two methods of authentication are supported in IEEE 802.11i:

- 802.1x and EAP to authenticate users: this is described above.
- Per-session-key per-device authentication: this is an alternative method of authentication to the first method. Similar to WEP, the shared key called group master key, with pair transient key and pair session key, is used for authentication and data encryption.

Michael algorithm is used to solve the integrity problem with WEP, which protects both the header and data. The IEEE 802.11i specifies three protocols [16,23]:

- Temporal Key Integrity Management: it provides a short-term solution that fixes all WEP weaknesses using per-packet key mixing, message integrity check, and a rekeying mechanism.
- Wireless Robust Authenticated Protocol: it was introduced to get the benefits of AES in WLAN Offset Codebook mode of AES.
- Counter with Cipher Block Chaining Message Authentication Code Protocol [26]: it uses AES for encryption and requires hardware upgrade to support the new encryption algorithm. It is considered to be the best solution to secure wireless data transfer under 802.11i.

Robust secure/security network (RSN) is part of the IEEE 802.11i standard that provides mechanism to create a secure communication channel between an AP and wireless clients by broadcasting an *RSN Information Element* message across the wireless network.

7.4.5 Best Practices

There is not a single solution that can completely secure a wireless network. Therefore, we need to follow best practices [16,17,22,23], which are given as follows:

- Define, enforce, and monitor a wireless security policy: the policy should cover all wireless services and users such as Wi-Fi and Bluetooth services and users.
- Always conduct a site survey to collect the information about all WAPs and Wi-Fi devices, which helps to eliminate rouge APs and unauthorized users.

- Configure APs and user stations for security:
 - Change the WEP key on a regular basis in home networks to weaken the chances of being attacked.
 - Configure the AP to stop broadcasting its SSID to hide your network.
 - Turn off “ad hoc” mode operation.
 - Implement layers of security schemes such as MAC address filtering and protocol filtering, along with WEP and SSID hiding.
 - Deploy a wireless intrusion detection system to identify or log threats and attacks. Analyze log and resolve incidents in a timely manner.
 - Define and develop institution-wide policies with detailed procedures regarding wireless devices and usage.
 - Conduct regular security awareness and training sessions for both system administrators and users to make them become aware of recent advances in computer network and wireless security. Train users not to respond to social engineering or phishing emails.
 - Define acceptable encryption and authentication protocols:
 - Implement WPA or WPA2 wherever possible.
 - Use strong encryption with at least 128-bit keys (WPA, AES recommended).
 - Turn off “open” authentication.
 - Deploy a layer-3 virtual private network for wireless communication.
 - DHCP: Use static IP addresses instead of DHCP. As DHCP automatically provides an IP address to anyone (authorized or not) and facilitates access to your wireless network, it creates a big threat to the network from unauthorized users.
 - Plan for AP coverage to radiate out toward windows but not beyond.
 - Use directional antennas for wireless devices to better contain and control the RF array and thus prevent unauthorized access.
 - Use remote authentication dial-in user service, which can be built into an AP or provided via a separate server. RADIUS is an additional authentication step. Interface this authentication server to a user database to ensure that the requesting user is authorized.
 - Force periodic (every 15 min or so) reauthentication for all wireless users.
 - Implement physical security controls: because of small size and portability of wireless devices, they are easy to steal or lose so it is recommended to implement strong physical security controls (such as guard, video camera, and locks) to prevent theft of equipment and unauthorized access.
 - To secure wireless network through lost or stolen devices, implement device-independent authentication.

7.4.6 Protocol for Carrying Authentication for Network Access

Protocol for Carrying Authentication for Network Access (PANA) is the recent proposal to enhance wireless security mechanisms through improved authorization between WLAN clients and AAA servers over IP-based networks [27]. In other words, PANA carries EAP to perform authentication between the access network and the wireless client. After successful PANA authentication, the client is authorized to receive an IP forwarding service from the network.

PANA is the network-layer protocol and is intended to authenticate PaC (PANA Client) with a PANA authentication agent (PAA) in situations where no prior trust between PAA and PaC exists. PANA consists of four parts, that is, a wireless client known as PaC (PANA Client); an

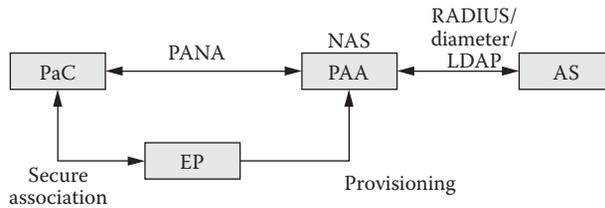


Figure 7.13 PANA framework.

enforcement point, which is the physical point where inbound and outbound traffic filters are applied; a PAA representing access authority on the network; and the AAA servers. Using an initial sequence number and cookie-based authentication between PAA and PaC, PANA can provide a mechanism to prevent DoS attacks [27,28]. The PANA framework is shown in Figure 7.13.

7.5 Wireless Personal Area Networks (PANs)

7.5.1 IEEE 802.15: PANs

Personal area networks (PANs) span a small area within personal premises such as a home or an office [29]. Mostly, they are formed by using peer-to-peer basis or master–slave basis. Bluetooth, ZigBee, and ultrawideband (UWB) networks are some examples of PANs.

7.5.2 Bluetooth Network Security

Bluetooth is an example of a wireless PAN in which clients use a *pairing* process to establish encryption and authentication between two devices. Bluetooth operates in an ISM radio band. The association process takes about up to 4 s. Bluetooth devices form a master/slave-like structure while pairing and use 48-bit hardware address of a master, shared 128-bit random number, and a user-specified personal identification number (PIN) of up to 128 bits. Some Bluetooth devices only allow 1–4-digit PINs. Hardware address and random number are exchanged using plain text, and a user-specified PIN is entered by users similar to the password. It is assumed that the Bluetooth network is secured; unfortunately, it is possible to break a Bluetooth network [30] by sniffing the packet for a PIN when a 1- to 4-digit PIN is used. Exploiting vendor-specific flaws such as default setting of allowing any pairing, attackers exploit Bluetooth devices. In order to protect the Bluetooth network, users need to change the default setting and choose strong PINs.

7.5.3 IEEE 802.15.4: ZigBee Security

To provide security in the ZigBee network [31], it is built on top of the IEEE 802.15.4AES-128 algorithm. ZigBee operates in the ISM radio bands, and its data transmission rates vary from 20 to 900 kb/s. Two devices take about 30 ms to get associated. To provide network security, ZigBee runs in two different security modes, that is, residential mode and commercial mode.

In residential mode, all users use a predeployed key for the entire PAN and for all applications. Residential mode security protects the PAN from external eavesdroppers; however, it does

not provide security from the user within the same PAN. In commercial mode, the coordinator node in a trust center is used to preshare the two master keys that provide extra security on top of the residential mode. This method is costly since infrastructure is needed to have a centralized coordinator node for the trust center to store sessions for each link.

7.5.4 UWB Security

UWB radios use low transmit power; as a result, they have a low coverage area. To attack this type of networks, the attacker should be close enough to the UWB network. The FCC in the United States authorizes unlicensed use of UWB in the range of 3.1–10.6 GHz. There are no standard security modes in UWB networks. According to WiMedia [32], there are three levels of link-layer security: (1) *Security Level 0*, in which communication is fully unencrypted; (2) *Security Level 1*, which has both encrypted communications with AES-128 for encrypted links and unencrypted communications for unencrypted links; and (3) *Security Level 2*, in which all communications must be encrypted with AES-128.

7.6 Best Practices for Mobile Device Security

This section presents best practices for securing wireless or mobile devices in general. There is no perfect method to protect wireless networks and mobile devices/users, and thus, it is recommended to use multiple techniques and best practices.

7.6.1 Devices Choice

All devices are not designed equally when it comes to security. Wireless mobile devices for users should be chosen based on the security requirements. Wireless security configuration in mobile devices is highly dependent on the security features that are available on them. For example, iPods are not as secure as BlackBerry devices because iPods are built for general users who are not concerned with security, and BlackBerry devices are designed for enterprise users who need a higher level of security.

7.6.2 Enable Encryption

Encryption enables strong security features in mobile devices and mandates it for all users to provide security for the network. In general, many organizations do not enforce or mandate encryption through policies for mobile devices and users.

7.6.3 Configure Wireless Networks for Authentication

The best practice for mobile device security is to enable device authentication so that lost devices cannot be easily accessed by any person that finds or steals a device. The survey result published in September 2008 by Credent Technologies shows that, in a 6-month period, more than 31,000 passengers left their mobile devices in a taxicab. The fact of the matter is that these devices are too easy to lose, and they can be used to enter the network if authentication is not enabled.

7.6.4 Enable and Utilize Remote Wipe Capabilities

It is best practice to enable remote access to disable devices and wipe out data in the case of loss or theft. With the remote wiping capability, the user or network administrator would be able to delete data in the stolen or lost devices to protect these devices from malicious use. Additionally, the network administrator should be able and available to take necessary steps to wipe out the wireless/mobile device.

7.6.5 Limit Third-Party Apps

There are several applications available for smartphones. These apps provide many features but can also easily provide backdoors or security loopholes, which are the biggest threat to the privacy and security of the organization. There should be policy and recommendation to control the installation of unsigned third-party applications to prevent attackers from requisitioning control of wireless/mobile devices.

7.6.6 Implement Firewall Policies

It is recommended to set up firewall policies for traffic coming from smartphones to provide security to the network, as well as to the mobile devices.

7.6.7 Implement Intrusion Prevention Software

It is possible to run Metasploits on recent smartphones such as iPhones because smartphones are becoming powerful enough to run this. Smartphones can be exploited by hackers or attackers to attack the network system. Intrusion prevention systems can examine traffic coming through mobile devices and protect the system.

7.6.8 Bluetooth Policies

Bluetooth capabilities available on Wi-Fi devices and smartphones are easy to use for creating PANs. Hackers can take advantage of default always-on always-discoverable settings of Bluetooth to launch attacks. It is best practice to disable Bluetooth when it is not actively transmitting information and to switch Bluetooth devices to hidden mode. This type of configuration should be the part of the policy to limit the exposure of the wireless network and mobile devices within the organization.

7.7 Summary

This chapter provided an overview of concepts related to security features and issues in wireless voice and data communication networks. Discussions about why and how wireless networks are more vulnerable, as compared to wired networks, were presented. The combination of different systems within a wireless cellular network makes it complex and increases vulnerabilities and loopholes. Attackers can exploit the vulnerabilities available in any part of the network and can gain access to the network. The protocols and practices used to secure a wireless cellular network are presented. In order to secure a WiMAX network, the IEEE 802.16e standard that implements

a 128-bit encryption key mode based on the AES is used to remove the flaws that are present in older WiMAX IEEE 802.16a/d standards. In IEEE 802.11, WEP is an old security mode used to protect WLANs. It is not secure but is still widely used since it provides at least one level of security to the network. Recent advances in WLANs have improved its security schemes. The IEEE 802.11i is assumed to be a secured solution to fix most of the security holes found in its predecessor WEP. A recently proposed PANA framework with different protocols is used as a secure messaging system between wireless clients and wireless network access authority. To protect the network, different security schemes can be implemented in PANs, including Bluetooth, ZigBee, and UWB networks. Furthermore, best practices and recommendations to secure different wireless networks and devices were presented.

Wherever wireless networks are deployed, security vulnerability will always exist. Security attacks and vulnerabilities can only be mitigated if best practices, as well as correct policies and standards, are used. We discussed some of the important and best practices that can be implemented for improving mobile and wireless security. Wireless security will continue to be a research topic as long as there are ways to attack or obtain unauthorized access to wireless networks.

References

1. Goldsmith, A. *Wireless Communications*. Cambridge University Press, New York, 2005.
2. Rawat, D. B., D. C. Popescu, G. Yan, and S. Olariu. "Enhancing VANET performance by joint adaptation of transmission power and contention window Size." *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 9, pp. 1528–1535, September 2011.
3. Rawat, D. B., B. B. Bista, G. Yan, and M. C. Weigle. "Securing Vehicular Ad-Hoc Networks Against Malicious Drivers: A Probabilistic Approach." *Proceedings of the International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)*, pp. 146–151, Seoul, Korea, June 2011.
4. Lee, W. *Wireless and Cellular Telecommunications*. McGraw-Hill Press, New York, 2005.
5. Balderas-Contreras, T., and R. A. Cumplido-Parra. Security Architecture in UMTS Third Generation Cellular Networks, Coordinación de Ciencias Computacionales INAOE, Technical Report No. CCC-04-002 27, 2004.
6. Gardezi, A. I. *Security In Wireless Cellular Networks*. http://www.cs.wustl.edu/~jain/cse574-06/ftp/cellular_security/index.html, accessed December 10, 2011.
7. Yang, H., F. Ricciato, S. Lu, and L. Zhang. "Securing a wireless world." *Proceedings of the IEEE*, vol. 94, no. 2, 2006.
8. 3GPP, A guide to 3rd generation security. Technical Standard 3GPP TR 33.900 V1.2.0, 3G Partnership Project, January 2001.
9. Kotapati, K., P. Liu, and T. F. La Porta. "EndSec: An end-to-end message security protocol for mobile telecommunication networks." *Proceedings of the 2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2008.
10. Moore, D., V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver. "Inside the slammer worm." *IEEE Security and Privacy*, vol. 1, no. 4, pp. 33–39, 2003.
11. Moore, T., T. Kosloff, J. Keller, G. Manes, and S. Sheno. "Signaling System 7 (SS7) Network Security." *Proceedings of the IEEE 45th Midwest Symposium on Circuits and Systems*, August 2002.
12. Mann, S., and S. Sbihi. *The Wireless Application Protocol (WAP): A Wiley Tech Brief*. John Wiley Press, Hoboken, NJ, 2002.
13. Carneiro, G. "Cross-layer design in 4G wireless terminals." *IEEE Wireless Communications*, vol. 11, issue 2, 2004.
14. Pareek, D. *WiMAX: Taking Wireless to the MAX*. John Wiley Press, Hoboken, NJ, 2006.
15. Johnston D., and J. Walker. "Overview of IEEE 802.16 security." *IEEE Security and Privacy Magazine*, vol. 02, issue 3, pp. 40–48, June 2004.

16. Roshan, P., and J. Leary. *802.11 Wireless LAN Fundamentals*, CISCO, 2009.
17. Rawat, D. B. et al. Comprehensive ComTIA Security+ Lab Manual, 2012, in preparation.
18. inSSIDer Software URL. <http://www.metageek.net/products/inssider/>, accessed December 2011.
19. Arbaugh, W. A. "Wireless security is different." *Computer*, vol. 36, issue 8, pp. 99–101, August 2003.
20. Hurley, C., and F. Thornton. *WarDriving: Drive, Detect, Defend: A Guide to Wireless Security*. Syngress Publishing Press, Rockland, MA, 2004.
21. Potter, B. C. "Wireless security's future." *IEEE Security and Privacy Magazine*, vol. 1, issue 4, pp. 68–72, Aug. 2003.
22. Welch, D., and S. Lathrop. "Wireless security threat taxonomy." *Proceedings of the IEEE Information Assurance Workshop 2003*, pp. 76–83, June 2003.
23. Earle, A. E. *Wireless Security Handbook*. Auerbach Publications, Boca Raton, FL, 2005.
24. http://www.cs.wustl.edu/~jain/cse574-06/ftp/wireless_security/index.html-startawisp
25. RFC for RADIUS server URL: <http://www.ietf.org/rfc/rfc2865.txt>.
26. RFC for CCMP, <http://www.ietf.org/rfc/rfc3610.txt>.
27. Protocol for Carrying Authentication for Network Access (PANA) RFCURL. <http://tools.ietf.org/html/rfc5191>, accessed December 2011.
28. RFC for PANA Threat Analysis and Security Requirements, URL <http://www.armware.dk/RFC/rfc/rfc4016.html>.
29. Surhone, L. M., M. T. Timpledon, and S. Marseken. *Personal Area Network*. Betascript Publishers, Beau Bassing, Mauritius, 2010.
30. Shaked, Y., and A. Wool. "Cracking the bluetooth PIN." *Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services*, pp. 39–50, 2005.
31. Elahi, A., and A. Gschwender. *ZigBee Wireless Sensor and Control Network*. Pearson Education, Boston, 2009.
32. ECMA International URL, <http://www.ecma-international.org>, accessed December 2011.