ordinating encryption processes. It's quite apparent that 1G cellular was designed to carry voice, not data.

1G systems at one time covered most of the U.S. Today, however, they exist only in areas having low population density, where it's not feasible to upgrade the infrastructure to newer digital systems.

Second-Generation Cellular

Not too long ago, digital cellular became available, allowing both the voice and control channels to make use of digital signing. The first phase of this totally digital system is referred to as second-generation cellular (**2G cellular**). Most of the telecommunications operators today have 2G systems, with various enhancements occurring periodically.

The use of digital signaling for the voice channels allows for more efficient modulation. This makes it possible to support more phone calls and data over a lower frequency spectrum. In fact, 2G systems enable enhanced services—such as short messaging, authentication, and phone software updates—to be accessed wirelessly.

Enhanced versions of 2G systems (sometimes referred to as 2.5G) include even better modulation, which increases data rates and spectrum efficiency. For example, the General Packet Radio Service (GPRS) offers high-speed data rates over a global system for mobile communications (GSM) network. Maximum data rates over GPRS are 171.2 kbps. The use of GPRS, however, requires a specialized mobile phone. Also, the Enhanced Data Rate for Global Evolution (EDGE) enhances GSM using 8-level PSK, where each transmitted symbol represents 3 data bits. This results in a maximum data rate of 474 kbps.

Third-Generation Cellular

Many of the telecommunications operators are now beginning to offer what's known as third-generation cellular (**3G cellular**), with even better support for data communications. The Universal Mobile

Exhibit 1010
Page 211 of 292

Telecommunications System (UMTS) is capable of 2-Mbps data rates for in-building implementations, up to 384 kbps in urban areas, and 144 kbps in rural areas. As a result, 3G is able to support multimedia applications.

There has been considerable argument in the wireless industry on whether 3G will replace 802.11 (Wi-Fi) wireless LAN technology. With higher data rates for indoor use, 3G is an alternative to wireless LANs. 802.11 continues, however, to have performance upgrades that significantly exceed 3G. For example, the 802.11a standard specifies data rates of 54 Mbps, which is much higher than 3G. Also, wireless LANs are much less expensive to deploy.

Wireless LANs, however, are not practical for providing coverage over wide areas. There would be too much infrastructure. 3G makes use of existing cell tower sites and distribution systems. Expenses of modifying 1G and 2G cellular systems to 3G are still high, but it's the most feasible method for providing wireless networking over wide areas.

Thus, both 3G and wireless LAN systems complement each other. This has prompted standards groups and manufacturers to find ways to seamlessly integrate 3G and wireless LANs. In fact, mobile phones and PDAs are available today that implement both technologies. With this capability, a user can roam outside the range of a wireless LAN and automatically associate with a cellular system. The problem is that standards that define this form of roaming are not yet available, which requires the user to carefully choose service providers that support the phone or PDA of choice.

Short Message Service (SMS) Applications

One of the most common services for wireless WANs is short message service (SMS), which is a text messaging sys-

Exhibit 1010
Page 212 of 292

tem capable of sending a couple hundred characters at a time. SMS is a wireless form of the familiar instant messaging that is available from many of the ISPs. The following are additional applications of SMS for use with wireless WANs:

- Content delivery— SMS enables the efficient delivery of updates for user devices. For example, a user can download new ring tones and fancy backgrounds to her phone over SMS. In addition, SMS makes it possible for users to query databases and news feeds. For example, you can keep up with the latest breaking news by receiving instant updates through SMS.
- Alerts— Most operators offer a variety of alerts, such as voicemail waiting, sports scores, current stock prices, and other reminders. This allows you to receive updates when something that you define as important occurs.
- Interaction— Some television shows allow interactivity among viewers and hosts through SMS. This enables participation of the audience, which dramatically increases the viewing audience size
- Application integration— It's feasible for developers to integrate SMS into many corporate applications. For example, a company can have a sales management system that enables sales representatives to track customers and products. A company can usually easily add SMS to these applications. For example, the addition of an alert mechanism would be beneficial. Sales representatives would be notified that a product has gone on sale.

Many web sites use Wireless Markup Language (WML) to transform regular web pages into a format that is more easily read on a small device, such as a PDA or cell phone. WML also reduces the graphics on the page to compensate for the slower data rates of wireless WAN technologies.

Exhibit 1010
Page 213 of 292

note



For more information on instant messaging applications, check out the Instant Messaging Planet at **http://www.instantmessagingplanet.com**.

Space-Based Wireless WANs

In addition to the land-based cellular systems, the use of space-based systems provides a means for networking users over wide areas.

Satellites

The use of satellites for broadcasting television and other communications has been around for several decades. Not until recently, however, did satellite systems provide users with connections to the Internet. (See **Figure 7-7**.) Data rates are appreciable, with up to 1.5-Mbps downloads.

Figure 7-7. Satellite System Dramatically Extends the Coverage of a Wireless WAN

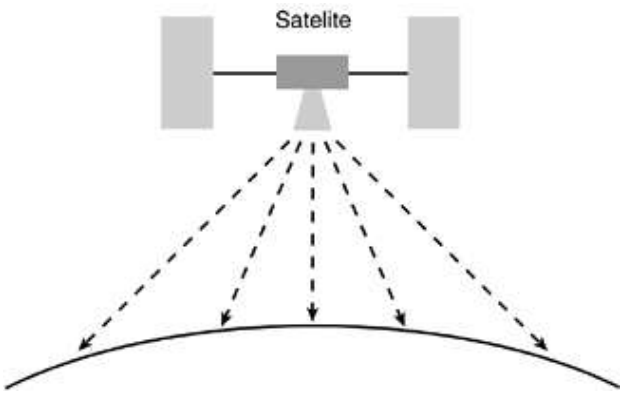


Exhibit 1010
Page 214 of 292

Some satellite systems support two-way exchange of data, allowing a user to send data up to the satellite (and vice versa). For example, a user's mobile device can transmit a web page request up to the satellite, and the satellite retransmits it down to the appropriate Earth station. The Earth station then sends the web page through the satellite and back down to the user. Other satellite systems, however, only support a downlink. A user's device must request the web page through another network, such as a telephone link, and the satellite broadcasts the page to the user.

By incorporating active radio repeaters in man-made, Earth-orbiting satellites, it is possible to provide broadcast and point-to-point communications over large areas of the Earth's surface. The broadcast capability of the satellite repeater is unique and, by suitable selection of satellite antenna patterns, it can be arranged to cover a well-defined area.

Satellites are located at various points in the geostationary orbit depending on the system mission requirement. To obtain global coverage, a minimum of three satellites is required. To obtain reasonably constant RF signal levels, however, four satellites are employed. This also provides some freedom in positioning.

With satellite communications, favorable frequencies are used: power efficiency, minimal propagation distortions, and minimal susceptibility to noise and interference. Unfortunately, terrestrial systems tend to favor these frequencies as well. Space is an international domain, and the International Telecommunications Union (ITU) controls satellite frequencies.

The band of frequencies between 450 MHz and 20 GHz is the most suitable for an Earth-space-Earth radio link. It is not practical to establish links to an Earth terminal located in a climatic region of heavy rainfall at frequencies higher than 20 GHz if consistent availability is expected.

Exhibit 1010
Page 215 of 292

For all operating bands, the lowest-frequency spectrum is used for the downlink because it has the most severe power constraints. Lower frequencies are less sensitive to free-space attenuation when compared to the higher-uplink frequencies. Losses are easier to overcome in the uplink with the higher transmit power available at the Earth station.

The satellite acts as a signal repeater. Signals sent to it on the uplink are rebroadcast back to Earth on the downlink. The device that handles this action is referred as a transponder. The satellite transponder is analogous to a repeater in a terrestrial communications link; it must receive, amplify, and retransmit signals from Earth terminals. A satellite transponder is capable of acting as a transponder for one or more RF communications links.

Low-altitude satellites, which can have circular, polar, or inclined orbits, have orbital periods of fewer than 24 hours. Therefore, they appear to move when seen from the Earth's surface. These orbits are useful for surveillance purposes, and can be used to provide communications at extreme north and south latitudes.

One type of special interest to public data communications is the geostationary orbit. A satellite in such an orbit has a 24-hour period at an altitude of 22,300 miles and remains over a fixed location on the equator. As a result, the satellite appears motionless to an observer on Earth.

Actually, the satellite does not remain truly fixed. Even if the orbit were perfectly circular and at precisely the right altitude, natural phenomena (because of low-level lunar and planetary-gravitational fields and solar-radiation pressure) introduce slight drifts in the orbit. This slow and minor drift is corrected from time-to-time by small onboard thrusters activated by ground stations.

Because of the long RF path involved (approximately 22,300 statute miles from an Earth terminal to a satellite in geostationary orbit), a

Exhibit 1010
Page 216 of 292

transmission delay of approximately 100 ms is experienced between an Earth terminal and the satellite. This results in an approximate Earth-to-Earth-delay of 200 ms. This causes the system to be inefficient for use with protocols, such as 802.11, that require a response after each packet of information is transmitted before transmitting the next packet. In fact, most networking protocols do not work efficiently over satellite links because the protocols expect timely acknowledgments from the destination.

Meteor Burst Communications

Billions of tiny microscopic meteors enter the Earth's atmosphere. In fact, meteors fall often throughout the day over all parts of the world. As these meteors penetrate the atmosphere, at a high altitude, they ionize into a gas. This gas is seen as a shooting star, which is an uncommon and large meteor as compared to most others.

Known as a poor man's satellite system, meteor burst communications (see **Figure 7-8**) bounce RF signals off meteor trails. This enables a long-haul (1,500 mile) wireless- data transmission link without the expense of launching and maintaining a satellite.

Figure 7-8. Meteor Burst Systems Use Meteor Trails to Reflect Signals Back to Earth

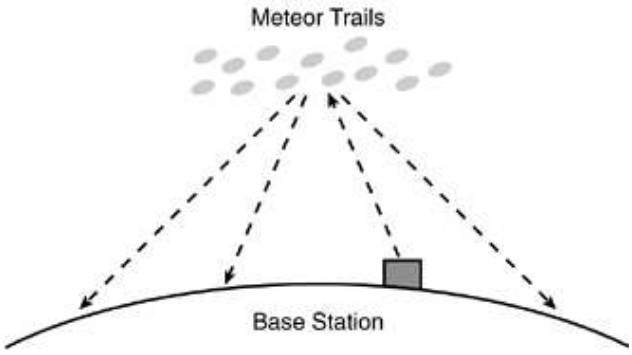


Exhibit 1010
Page 217 of 292

Meteor burst communications direct a 40 to 50 MHz radio wave—modulated with a data signal— at the ionized gas. The radio signal then reflects off the gas and is directed back to Earth. The availability of meteor trails is good but they are present only often enough to rely on 300 to 2400 bps. This is extremely slow, even compared to telephone modems.

However, the cost of deploying meteor burst equipment is so low compared to satellite systems that low-performance applications, such as telemetry, are feasible. Meteor burst, for example, works well for transmitting snow levels from remote mountainous areas to monitoring centers.

Exhibit 1010
Page 218 of 292

Wireless WAN Technologies

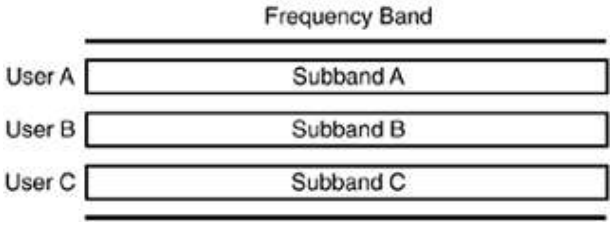
Wireless WANs make use of technologies that focus on modulation of voice and data. As discussed in **Chapter 2**, "Wireless System Architecture: How Wireless Works," modulation converts digital signals that represent information inside a computer into either RF or light signals. Wireless WANs exclusively use RF signals designed to accommodate many users. Each user has a dedicated channel, and this is different from wireless LANs, where all users share one channel. This significantly reduces interference between wireless WAN user devices and base stations.

Take a closer look at the different modulation techniques.

Frequency Division Multiple Access

Frequency division multiple access (FDMA) divides a wide-frequency band into smaller subbands, where each user transmits voice and data over their assigned subband. All users transmit their signals simultaneously. **Figure 7-9** illustrates this concept. Traditional 1G cellular systems use FDMA for sending data.

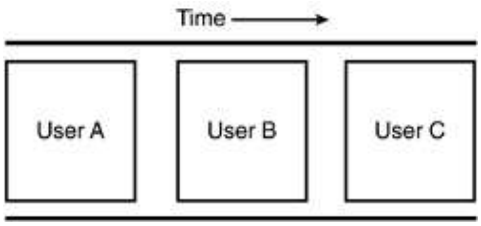
Figure 7-9. FDMA Allows Simultaneous Transmissions Because Users Do Not Operate in the Same Part of the Frequency Spectrum



Time Division Multiple Access

As shown in **Figure 7-10**, time division multiple access (TDMA) keeps users separate by allowing only one user to transmit at any give time. Each user has an assigned time slot for transmission. Some of the older telecommunications operators utilize TDMA to offer voice and data connections over wireless WANs. For example, T1 circuits make use of TDMA for combining separate user connections over the same circuit.

Figure 7-10. TDMA Makes Users Transmit Only During Their Assigned Time Slot

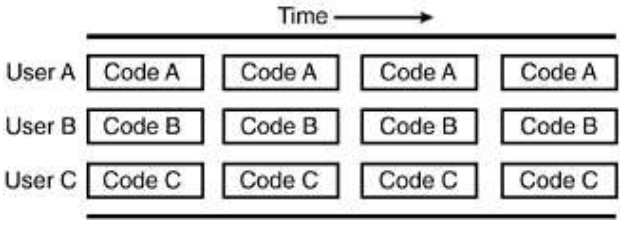


Code Division Multiple Access

Similar to FDMA, code division multiple access (CDMA) allows simultaneous transmissions. (See **Figure 7-11**.) The difference, however, is that CDMA users can occupy the entire frequency band at the same time. The users do not experience any interference, because each user modulates her signals using a different code. An advantage of CDMA is that user devices can connect to multiple base stations because of separate codes. This increases performance and reliability. Cellular systems predominately make use of CDMA wireless networks.

Figure 7-11. CDMA Assigns a Code to Each User, Which Makes It Possible for Users to Transmit Simultaneously Without Interference

Exhibit 1010
Page 220 of 292



Spatial Division Multiple Access (SDMA)

SDMA accommodates multiple users by focusing a beam for each user. This is common in satellite systems. Some SDMA systems are adaptive, where the radio beams follow movement of the user. Other systems require the user device to re-associate with the next beam as users move.

note



Some wireless WAN devices, such as mobile phones, have multiple modes or bands and support more than one technology. For example, a single mobile phone can support both TDMA and CDMA. The phone automatically switches from one technology to the other depending on which network is available.

Exhibit 1010
Page 221 of 292

Chapter Summary

Wireless WANs include cellular towers, parabolic antennae, satellites, and telecommunications infrastructure. Most wireless WAN applications make use of outdoor connections, but some indoor facilities, such as airports and convention centers, deploy wireless WANs when large numbers of subscribers are present. Wireless WAN infrastructure is expensive compared to other types of wireless networks, but wireless WANs are the most feasible for covering countries and continents. Cellular and satellite systems are the most common forms of wireless WANs capable of providing moderate performance. Meteor burst communications is less expensive, but offers only low performance.

Exhibit 1010
Page 222 of 292

Chapter Review Questions

You can find the answers to the following questions in **Appendix A**, "Answers to Chapter Review Questions."

1:	What types of user devices are most common with wireless WANs?
2:	Why do wireless WAN operators always charge for services?
3:	Why must you be careful when selecting a wireless WAN radio NIC for your user device?
4:	What is an advantage of a satellite system?
5:	Which generation of cellular systems offers data rates up to 2 Mbps?
6:	Which type of wireless WAN system is most common?
7:	Which of the two following cellular systems offers the highest data rates: GPRS or UMTS?
8:	What is the primary issue with meteor burst communications?
9:	True or false: FDMA requires users to take turns transmitting signals.

Exhibit 1010
Page 223 of 292

10: How does CDMA keep users from interfering with each other?

Exhibit 1010
Page 224 of 292

Chapter 8. Wireless Network Security: Protecting Information Resources

What You Will Learn

After reading this chapter, you should be able to

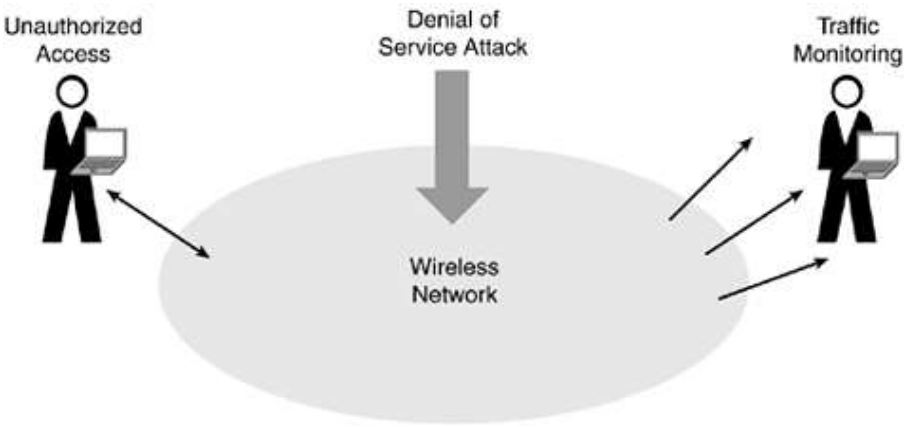
- Understand wireless security issues
- Describe methods to counter security problems
- Understand basic encryption and authentication technologies and standards

Security is vitally important for wireless networks, primarily because the communications signals are openly available as they propagate through the air. Companies and individuals using wireless networks must be aware of the potential issues and applicable countermeasures. This chapter discusses security threats and ways to tighten the security of a wireless network through the use of **encryption** and **authentication**.

Security Threats

As show in **Figure 8-1**, there are several forms of security threats to wireless networks. For example, **hackers** can steal information from a company, obtain unauthorized access to applications, and even disrupt operation of the network.

Figure 8-1. Threats to Wireless Network Security Include Passive Monitoring, Unauthorized Access, and Denial of Service (DoS)



Traffic Monitoring

An experienced hacker, or even casual **snooper**, can easily monitor unprotected wireless data packets using tools such as AirMagnet and AiroPeek, which fully disclose the contents of wireless data packets. For example, snoopers can monitor all transactions occurring over the wireless portion of the network several hundred feet away from the building that has the wireless LAN. Of course, the issue is that anyone

can identify usernames, passwords, credit card numbers, and so on. In fact, war drivers even post their finds on web sites, just for fun.

The solution to this problem is to, at a minimum, employ encryption between the wireless client device and the base station. Encryption alters data bits using a secret key. Because the key is secret, a hacker is not able to decipher the data. As a result, the use of effective encryption mechanisms upholds the privacy of data.

Unauthorized Access

Similar to monitoring a wireless application, someone can effortlessly access a corporate wireless network from outside the facility if the proper precautions are not taken. Someone can, for example, sit in a parked car and associate with one of the wireless base stations located inside a building. Without proper security, this person can access servers and applications residing on the corporate network. This is similar to letting a stranger inside your home or office.

Unfortunately, many companies deploy their wireless networks using the default, unsecured base station configurations, making it possible for anyone to interface with their application servers. In fact, you can go war driving and discover that 30 percent of the wireless LAN access points in an average city do not deploy any form of security. This allows anyone to access hard drives and use resources such as Internet connections.

The Windows XP operating system makes it easy to interface with wireless networks, especially on public wireless LANs. When a laptop associates with the wireless LAN, the user can navigate to any other laptop associated with the same wireless LAN. Without personal **firewall** protection, someone can browse through your hard drive. This is a tremendous security risk.

Even if you implement all security controls on access points, the possible connection of a **rogue access point** is a significant threat. (See