4

WIRELESS TRANSMISSION TECHNOLOGY AND SYSTEMS

4.1 INTRODUCTION

In this chapter we look at radio-channel-related issues. It should immediately be noted that to maximize the opportunity for widespread and cost-effective deployment of WSN, one needs to make use of existing and/or emerging commercial off-the-shelf (COTS) wireless communications and infrastructures rather than having to develop an entirely new, specially designed apparatus. WSNs can use a number of wireless COTS technologies, such as Bluetooth/Personal Area Networks (PANs), ZigBee, wireless LANs (WLAN)/hotspots, broadband wireless access (BWA)/WiMax, and 3G.

Given this pragmatic perspective, we focus here less on the science of radio transmission per se as a discrete system component and more on an integrated system-level view of the field. In other words, we explore the use of the just-named technologies as a plug-and-play system integration opportunity more than looking at the fundamentals of modulation, transmission, encoding, radio impairments, and so on. Stated differently, the developer of WSN systems should not be required to have a deep understanding of radio science (beyond basic issues such as power, range and coverage, bandwidth, performance, security, and a few other factors), but rather, which off-the-shelf wireless systems already defined by various standards bodies (e.g., Bluetooth, Wi-Fi, WiMax, ZigBee/IEEE 802.15.4) can be used by way of employing and/or integrating preconfigured chipsets and ICs (integrated circuits), antennas, drivers, and protocol machinery.

Wireless Sensor Networks: Technology, Protocols, and Applications, by Kazem Sohraby, Daniel Minoli, and Taieb Znati

Consistent with this perspective, in this chapter we look at some macro-level issues, while the chapters that follow provide more in-depth technical information. In Section 4.2 we provide a basic primer on radio technology; Appendix A provides some additional details related to modulation. In Section 4.3 we survey off-the-shelf technologies (IEEE family) that can be used by WSNs. Chapter 5 will expand on these concepts.

4.2 RADIO TECHNOLOGY PRIMER

This section comprises a terse primer on radio technology.

The electromagnetic spectrum provides an unguided medium (channel) for point-to-point and/or broadcast radio transmission. Radio transmission is usually (frequency)-bandlimited by design. The analog bandwidth of the channel (the slice of electromagnetic frequency domain used) determines how much information (analog or digital) can be transmitted over the channel. A transmission channel in general, and a radio-based channel in particular, is never perfect because it is subjected to external (and even internal) noise sources; noise has a tendency to degrade, disrupt, or otherwise affect the quality of an intelligence-bearing signal. A lot of radio-transmission engineering has to do with how to deal with the noise problem; the goal is nearly always to optimize the signal-to-noise ratio, subject to specified constraints (e.g., bandwidth requirements, cost, reliability, power consumption, equipment and antenna size).

4.2.1 Propagation and Propagation Impairments

Issues of interest in radio design include, among others, propagation, impairments, environment (i.e., indoors–outdoors, unobstructed–obstructed, benign–hostile, etc.), sensitivity, antenna design, channel bandwidth (analog and/or digital), and frequency of operation. Many design factors (e.g., propagation, attenuation, impairments) are related parametrically to the frequency band in use. In particular, directionality becomes more of an issue at higher frequency ranges; also, generally, bandwidth increases as one moves to higher-frequency bands (given that larger portions of the spectrum are in principle available). For the purpose of this primer, we focus on operation at 2.4 GHz. However, as noted, the commercial WSN developer need not worry about all of these issues at a fundamental level if he or she employs off-the-shelf technology (beyond basic considerations about distance, antenna type, bit-error rate, bandwidth, and power requirements[1]).

The most basic model of radio-wave propagation typically found in WSN environments involves the *direct* or *free-space wave* (see Figure 4.1). In this model, radio waves emanate from a point source of radio energy, traveling in all directions

[1]What we mean is that many of the relevant issues have already been studied, addressed, traded off, and optimized by the developers of the particular standard in question.

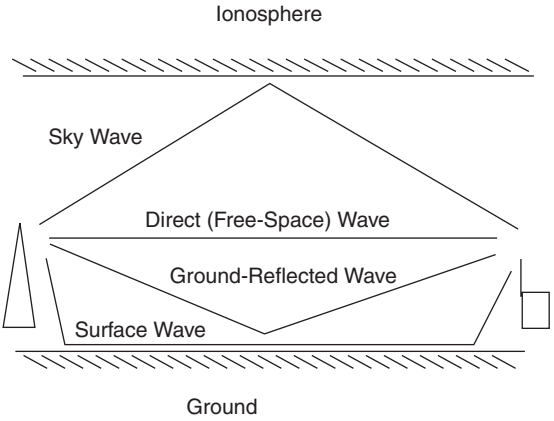


Figure 4.1 Radio propagation modes. [*Note:* For WSNs the direct (free-space) wave is the most common.]

in a straight line, filling the entire spherical volume of space with radio energy that varies in strength with a 1/(distance)^2 rule (or 20 dB per tenfold increase in distance) [4.1]; attenuation in environments that are not free space (e.g., waters, coaxial cable, heavily wooded areas, confined rooms or structures) is considerably more severe.

Three basic physical mechanisms affect radio propagation [4.2]:

1. *Reflection*. A propagating wave impinges on an object that is large compared to the wavelength. (e.g., the surface of the Earth, buildings, walls).
2. *Diffraction*. A radio path between the transmitter and receiver is obstructed by a surface with sharp irregular edges; waves bend around the obstacle, even when line of sight (LOS) does not exist.
3. *Scattering*. Objects smaller than the wavelength of the propagating wave are encountered along the way (e.g., foliage, street signs, lampposts).

These phenomena cause radio signal distortions and signal fading as described in Table 4.1. Signal strength fluctuations caused by the fact that the composite signal received comprises a number of components from the various sources of reflections from different directions as well as scattered and/or diffracted signal components affect both mobile and stationary receivers, whether the receivers are indoors or outdoors. In this phenomenon, called *multipath*, signal fluctuations can be as much as 30 to 40 dB. The intrinsic electromagnetic (radio) signal strength attenuation caused by these phenomena is called a *large-scale effect*; signal-strength fluctuations related with the motion of the broadcasting or receiving antenna are called *small-scale effects*.

Reflection, diffraction, and scattering all give rise to additional radio propagation paths beyond the direct line-of-sight path between the radio transmitter and receiver;

TABLE 4.1 Basic Phenomena Affecting Signals

Phenomenon	Description
Reflection	A phenomenon that occurs when a propagating electromagnetic wave impinges upon an object that is large compared to the wavelength of the propagating wave. Reflections occur from the surface of the Earth and from buildings and walls.
Diffraction	A phenomenon that occurs when the radio path between the transmitter and receiver is obstructed by a surface that has sharp irregularities (edges). The secondary waves resulting from the obstructing surface are present throughout the space and even behind the obstacle, giving rise to a bending of waves around the obstacle, even when a line-of-sight path does not exist between transmitter and receiver. At high frequencies, diffraction, like reflection, depends on the geometry of the object as well as the amplitude, phase, and polarization of the incident wave at the point of diffraction.
Scattering	A phenomenon that occurs when the medium through which the wave travels consists of objects with dimensions that are small compared to the wavelength and where the number of obstacles per unit volume is large. Scattered waves are produced by rough surfaces, small objects, or by other irregularities in the channel. In practice, foliage, street signs, and lampposts induce scattering in a mobile communications system.

Source: Adapted from [4.3].

multipath arises when more than one path is available for radio signal propagation [4.3]. Metallic materials as well as dielectrics (or electrical insulators) cause reflections. When multiple signal propagation paths exist, the actual signal level received is the vector sum of all the signals incident from any direction or angle of arrival. Some signals will aid (constructively reinforce) the direct path; others will subtract (destructively interfere with or vector-cancel out) from the direct signal path (see Table 4.2).

TABLE 4.2 Multipath Types

Type	Description
Specular multipath	Arises from discrete, coherent reflections from smooth metal surfaces. Can cause complete signal outages and radio dead spots within a building; the problem is especially difficult in underpasses, tunnels, stairwells, and small enclosed rooms.
Diffuse multipath	Arises from diffuse scatterers and sources of diffraction (the visible glint of sunlight off a choppy sea is an example of diffuse multipath). It gives rise to a background noise level of interference.

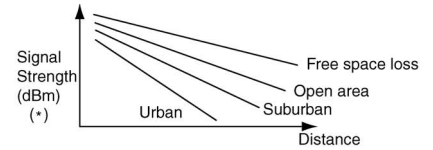
TABLE 4.3 Fade Factors

Type	Description
Large-scale fades	Attenuation: in free space, power decreases as a function of $1/d^2$ (d = distance from the transmitting antenna)
	Shadows: signals blocked by obstructing structures
Small-scale fades	Rapid changes in signal strength over a small area or time interval due to multipath
	Random frequency modulation due to varying Doppler shifts on different multipath signals
	Time dispersion (echoes) caused by multipath propagation delays:
	Multipath propagation yields signal paths of different paths with different times of arrival at the receiver
	Spreads (smears) the signal; can cause intersymbol interference and limits the maximum symbol rate (signals related to previous bit or symbol interfere with the next symbol)
	Typical values of delay spread: open spaces, <0.2 μs; suburban spaces, 0.5 μs; urban spaces, 3 μs
	Frequency-selective fading and Rayleigh fading:
	Combination of direct and out-of-phase reflected waves at the receiver yields attenuated signals.
	Addressed via antenna diversity (use two antennas a quarter-wavelength separated to combine received signals) and/or equalization (subtract delayed and attenuated images of the direct signal from the received signal—should be done adaptively to determine what these subtractions should be, since they change as the mobile devices moves around).

The impact of mobility on transmission characteristics is fairly difficult to model exactly. Channel performance varies with user location and time, and the radio propagation pattern is complex. One needs to deal with multipath scattering from nearby objects, shadowing from dominant objects, and attenuation effects from various physical phenomena. All of these factors result in rapid fluctuations of received power; even when the device mobile is stationary, the signals received may fade, due to movement of surrounding objects [4.2]. Table 4.3 highlights some of the issues.

Figure 4.2 describes pictorially issues related to outdoor propagation. For indoor propagation applications, the signal decays much faster: walls, floors, and furniture attenuate or scatter radio signals; also, the coverage is restricted to the local environment by walls and the like. The path loss formula is [4.2]

$$\text{path loss} = \text{unit loss} + 10n\log(d) = kF + IW$$

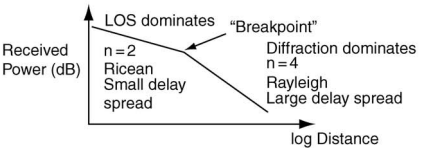


(*) Relative power of received signal compared to power at ref. distance from transmitter

Received Power $P_r = Kd^{-n}$, $n = 2$ in free space, $3 \le n \le 4$ typically

BER = f(signal stength)

Error rates increase as SNR decreases



Item	Macrocell	Microcell
Cell Radius	1 to 20 km	0.1 to 1 km
Tx Power	1 to 10 W	0.1 to 1 W
Fading	Rayleigh	Ricean
RMS Delay Spread	0.1 to 10 μs	10 to 100 ns
Max. Bit Rate	0.3 mbps	1 mbps

Figure 4.2 Outdoor radio propagation. (Based in part on [4.2].)

where unit loss = power loss (dB) at a 1-m distance (30 dB)
n = power-delay index
d = distance between transmitter and receiver
k = number of floors that the signal traverses
F = loss per floor
I = number of walls that the signal traverses
W = loss per wall

Additional contributing factors include the following [4.2]:

- People moving around (additional multipath-induced attenuation of up to 10 dB)
- Buildings with few metal and hard partitions: root-mean-square (rms) delay spread of 30 to 60 ns (equaling several Mbps without equalization)
- Buildings with metal or open aisles: rms delay spread of up to 300 ns (hundreds of kbps without equalization)
- Between floors:
  - Concrete or steel flooring yields less attenuation than that of steel plate flooring
  - Metallic-tinted windows yield greater attenuation
  - 15 dB for first-floor separation, 6 to 10 dB for the next four floors, 1 to 2 dB for each additional floor of separation

The indoor signal strength received depends on the office plan, construction materials, density of personnel, furniture, and so on (e.g., wall losses, 10 to 15 dB; floor losses, 12 to 27 dB; delay spread, varies between 15 and 100 ns, requiring sophisticated equalization techniques to achieve acceptable bit-error rates). Table 4.4 depicts signal attenuation values for signals typically used in networking and telecom applications. A drawback of higher-frequency bands (e.g., 5 GHz for IEEE 802.11a applications) compared to lower-frequency bands (e.g., 2.4 GHz for

TABLE 4.4 Signal Attenuation Due to Typical Obstacles

Wall Type	Frequency	Transmission Loss (dB)
Exterior wood frame wall	800 MHz	4–7
	5–6 GHz	9–18
Brick, exterior	4–6 GHz	14
Concrete block, interior	2.4 GHz	5
	5 GHz	5–10
Gypsum board, interior	2.4 GHz	3
	5 GHz	5
Wooden floors	5 GHz	9
Concrete floors	900 MHz	13

IEEE 802.11b/g applications) is the shorter wavelength of the signal at the higher band. It turns out that short-wavelength signals have more difficulty propagating through physical obstructions encountered in an office (walls, floors, and furniture) than do those at longer wavelengths.

There are few "RF-friendly" buildings that are free of multipath reflections, reflections from internal partitions, absorption from various office materials, diffraction around sharp corners, and scattering from wall, ceiling, or floor surfaces. Radio-wave propagation inside smooth-walled metal buildings can be so problematic that radio dead spots can exist to the point where the signal is virtually nonexistent. The dead spots arise because of almost perfect, lossless reflections from smooth metal walls, ceilings, or fixtures that interfere with signals radiated directly. The dead spots exist in three-dimensional space within the building, and motions of only a few inches can alter reception from a state of no signal to a state of full signal. Proper functioning of the radio communication link requires that multipath be minimized or eliminated [4.1]. Figure 4.3 depicts a simple example of indoor multipath.

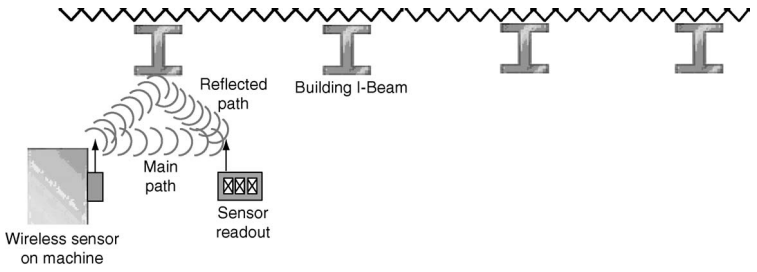


Figure 4.3 Indoor interference: reflected signal creates multipath interference. A factory building I-beam reflects transmission of wireless sensor data to a digital readout. The readout receives both the main and reflected signals that interfere with each other, disrupting the display. The readout can be moved out of the reflected signal path. Typically, movement of only a few inches is all that is required for better signal reception. If the readout cannot be moved, repositioning the antenna will have the same effect. With interference eliminated, the readout works normally (From [4.4].).

Error bursts are an outcome of fades in radio channels. Doppler-induced frequency or phase shifts due to motion can also cause loss of synchronization. Errors increase as the bit period approaches the delay spread. The typical acceptable BER for data communications is 10^{-6}; in some wireless situations this goal may not be met on a consistent basis. Strategies for overcoming errors include antenna diversity, forward error correction techniques, and traditional automatic repeat request (retransmission protocol for blocks in error) [4.2]. The outdoor-to-indoor penetration or *building loss* depends on building materials, orientation, layout, height, percentage of windows, and transmission frequency. The strength of the signal received increases with increasing building height; the penetration loss decreases with increasing frequency (e.g., 6 dB loss through windows).

In an industrial environment, care is needed when placing sensors in order to minimize interference. One needs to keep WNs away from other sources of radio-frequency interference (RFI), such as brush-type electrical motors, other radio transmitters or transceivers, or unshielded computer equipment and/or cables. Sensors that must be located near such devices should connect to the transceiver via a short piece of shielded cable so that they can stay as far away as possible from the source of the RFI. In a factory environment, large iron and steel structures may create multipath problems. As noted, multipath propagation occurs when nearby metal reflects the radio signal in the same way that a mirror reflects light. The receiver detects multiple signals simultaneously—the original and the reflections—and cannot decode any of them. Moving the receiving or transmitting antenna just a few inches is sometimes enough to fix this problem [4.4]. More generally, RF multipath problems can be mitigated in a number of ways [4.1]:

1. *Radio system design:* redundant paths for each receiver, if possible
2. *Antenna system design:* dual diversity antennas used at each receiver
3. *Signal/waveform design:* spread-spectrum radio design with the highest feasible chip rate
4. *Building/environment design:* not much can be done in this area unless RF-friendly greenfield buildings are constructed

Interference can also be caused by other legitimate or illegitimate users of a given frequency band. Interference can occur when a user starts to broadcast signal in a band while in proximity to other transmitters and/or receivers. (The scope of proximity depends on the frequency band, the power utilized by transmitting entities, and the modulation scheme, among other factors.) In the United States, most frequency bands are assigned by the Federal Communications Commission (FCC) to a specific (private) user or organization; (a few) other frequency bands can be utilized by anyone. In the former, while interference can be caused by accidental spillage of signal and/or malicious injection (e.g., jamming), the source of the interference can be stopped legally (or militarily). In the latter case there is no recourse because the band is open to anyone and coexistence is managed by ‘‘good

citizenship." In the latter case, unfortunately there is also intraband interference between various technologies (e.g., IEEE 802.15.1 Bluetooth technology can interfere with IEEE 802.11b/g-based systems). As just stated, most frequency bands require a license from the FCC (the license is needed for transmission, but generally not for reception). The license is granted (usually for a fee) to a specific user and/or organization. Use of the industrial, scientific and medical (ISM) band (at 2.4 GHz—more exactly, 2.412 to 2.484 GHz), and of the Unlicensed Network Information Infrastructure (U-NII) band (at 5 GHz) does not require a license. However, there still are technical guidelines that must be followed in terms of the radiated power, radiation pattern, and so on.

The current frequency-assignment system under which the FCC operates was formulated in the 1920s; under this system, different radio bands are assigned to different services and licenses are then required to operate inside those bands [4.45]. In recent years there has been interest on the part of the FCC to explore innovative ways to open new spectrum to commercial unlicensed use. Examples include the release of new spectrum in the 5-GHz U-NII band in 2003 as well as the opening up of 7.5 GHz of bandwidth for ultrawideband (UWB) signaling in the region between 3.1 and 10.6 GHz. Although the power levels allowed for UWB are extremely low—a roof of −41 dBm—the move marked the first time the FCC had allowed unlicensed use across otherwise licensed bands [4.45]. Cognitive radio (CR) technology is a new way to look at this issue (this topic is discussed later in the chapter).

4.2.2 Modulation

Modulation is the overlay of an intelligent signal over an underlying carrying signal, which is then transmitted over the medium in question (be it a cable, wireless, or fiber-optic medium). Baseband applications are those applications where the coded signal is carried directly over a medium without having to overlay it onto a carrier signal. Non-baseband systems use modulation; baseband systems do not. In traditional environments modulation allows transmission over long distances (e.g., tens to hundreds of miles); baseband systems usually are limited to the carriage of information over a fraction of a mile. Traditional wired LAN systems are baseband systems: The signal is encoded by some appropriate mechanism (e.g., Manchester encoding) and then transmitted over unshielded twisted-pair cable. Analog radio and TV transmission use modulation.

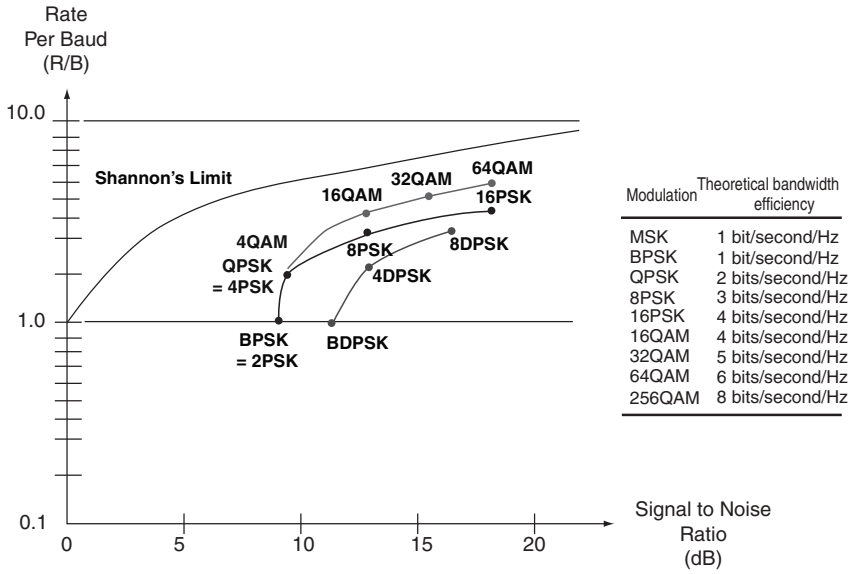
Three types of modulation typically used in radio applications are amplitude modulation (AM), frequency modulation (FM), and phase modulation (PM). In AM, the amplitude of the carrying signal is modulated (summed over or superimposed) by (the amplitude of) the incoming intelligence-bearing signal. In FM, the frequency of the carrying signal is modulated (summed over or superimposed) by (the frequency of) the incoming intelligence-bearing signal. In PM, the phase of the carrying signal is modulated (summed over or superimposed) by (the phase of) the incoming intelligence-bearing signal.

In an AM environment, when the incoming intelligence-bearing signal is digital (a sequence of 0 and 1 values), the modulation process is called *amplitude shift keying* (ASK). In an FM environment, when the incoming intelligence-bearing signal is digital, the modulation process is called *frequency shift keying* (FSK). In a PM environment, when the incoming intelligence-bearing signal is digital, the modulation process is called *phase shift keying* (PSK). When the incoming signal is interpreted as a sequence of n bits at a time (e.g., 00, 01, 10, 11; or 000, 001, 010, 011) and a combination of PSK and ASK techniques are used, the modulation process is called *quadrature amplitude modulation* (QAM). *Note:* In a digital environment the concept of the carrying signal, which was so prominent in the analog context, degenerates and the process is seen as giving rise to a sequence of discrete states (implemented in amplitude, frequency, or phase values). In all of these cases the modulation is said to be digital. In these situations the design goal is to maximize channel throughput by making the incoming digital signal pulse as dense as possible (time axis as small as possible) or by finding a way to encode groups of incoming bits over a single signal change (also known as *baud*).

The maximum digital capacity C of a single-carrier system with spectral bandwidth W is defined by *Shannon's equation:*

$$C = W \log_2(1 + S/N)$$

S is the signal power received and N is the noise power (the channel here is assumed to be an additive white Gaussian noise channel). In a typical environment, the log term usually ranges from 1 to 10, depending on the modulation technique (the signal-to-noise ratio is usually between -1 and 20). Figure 4.4 depicts some typical



Modulation	Theoretical bandwidth efficiency
MSK	1 bit/second/Hz
BPSK	1 bit/second/Hz
QPSK	2 bits/second/Hz
8PSK	3 bits/second/Hz
16PSK	4 bits/second/Hz
16QAM	4 bits/second/Hz
32QAM	5 bits/second/Hz
64QAM	6 bits/second/Hz
256QAM	8 bits/second/Hz

Figure 4.4 Efficiency of typical (wireless) modulation schemes.

digital modulation schemes in terms of their efficiency as measured by the bit rate per baud (in this context, 1 baud equates to 1 hertz). Typically, in wireless communication it is desirable to maximize the bandwidth efficiency; in traditional wireless communication, sophisticated (high-complexity) modulation methods are used to maximize the link throughput. For example, 64-point quadrature amplitude modulation (64 QAM) is used in WLANs operating with the IEEE 802.11a to achieve 54 Mbps throughput in a 20-MHz channel. High efficiency, however, comes with a price: first, the circuit complexity goes up considerably; second, the power consumption increases when one targets a high channel throughput. As might be expected, high throughput and efficiency are also desirable in WSNs; however, a trade-off between efficiency and power must be accepted: Schemes that support high efficiency require complex designs (read ''high-count transistor chipsets'') and fairly high power consumption. Research has shown that advanced modulation results in degraded energy efficiency for systems operating with short packets and/or a low duty cycle [4.5].

Spread-spectrum modulation techniques have a higher effective signal-to-noise ratio than narrowband techniques, but require more channel bandwidth. Direct-sequence spread spectrum (DSSS) is one of the two common spread-spectrum techniques (it being used, for example, in commercial implementation of the WLAN standards, including ZigBee). Frequency hopping spread spectrum (FHSS) is the other technique (it is used in the Bluetooth environment for PANs). In DSSS, the incoming data stream is hashed by a pseudorandom sequence that generates a sequence of output microbits or chips that are distributed across the underlying broadband channel. To the casual eye, these distributed microbits appear like noise. Fairly complex digital signal processing functions are needed to recover the original signal; processing must occur at the chip rate, and timing synchronization of all the nodes in the system must be within a fraction of the chip interval (which is the reciprocal of the chip rate).

Compared to DSSS systems, FHSS uses relatively low complexity baseband hardware. The synchnonization mechanism is also less complex; however, agile frequency hopping requires fast signaling settling. There are prima facie advantages in the use of FHSS for WSNs (e.g., improved multipath performance can be achieved with FHSS); however, the requirement for low-power operation and the widebandnature of operation gives rise to practical engineering challenges.

Appendix A provides some additional information related to modulation.

4.3 AVAILABLE WIRELESS TECHNOLOGIES

As we noted in passing in Chapter 3, two frequency bands are typically used by WNs: the ISM band and the U-NII band. As we just described, indoor and outdoor interference arises from both natural sources and/or phenomena (e.g., loss or attenuation, absorption, fading, multipath) as well as from other users in proximity utilizing these ''unprotected bands.'' A WSN will experience interference whether it uses one of the IEEE PAN/LAN/MAN technologies or even some other generic radio technology. For example, as noted above, other devices, such as Bluetooth-based PDAs and cellular phones, which share operating frequencies with wireless

sensors on both the ISM and UNII bands, can affect confined spaces (open spaces are subject to other issues). Microwave ovens, which operate at 2.45 GHz, may overwhelm many wireless technologies in the 2.4-GHz ISM band. On a manufacturing floor, improperly filtered electric motors may generate enough electrical noise to make wireless transmissions unreliable. Even the physical placement of a transmitter can cause a significant loss of signal [4.4].

Nonetheless, IEEE PAN/LAN/MAN technologies are broadly implemented technologies and are probably the ones utilized in the majority of (commercial) WSNs on a going-forward basis. Protocols determine the physical encoding of signal transmitted as well as the data link layer framing of the information; channel-sharing and data- and event-handling procedures are also specified by the protocol. There are several wireless protocols; the most widely used are (1) the IEEE 802.15.1 (also known as Bluetooth); (2) the IEEE 802.11a/b/g/n series of wireless LANs; (3) the IEEE 802.15.4 (ZigBee); (4) the MAN-scope IEEE 802.16 (also known as WiMax); and (5) radio-frequency identification (RFID) tagging. Each standard possesses different benefits and limitations. Figure 4.5 depicts graphically some of the features of these protocols see also Table 4.5).

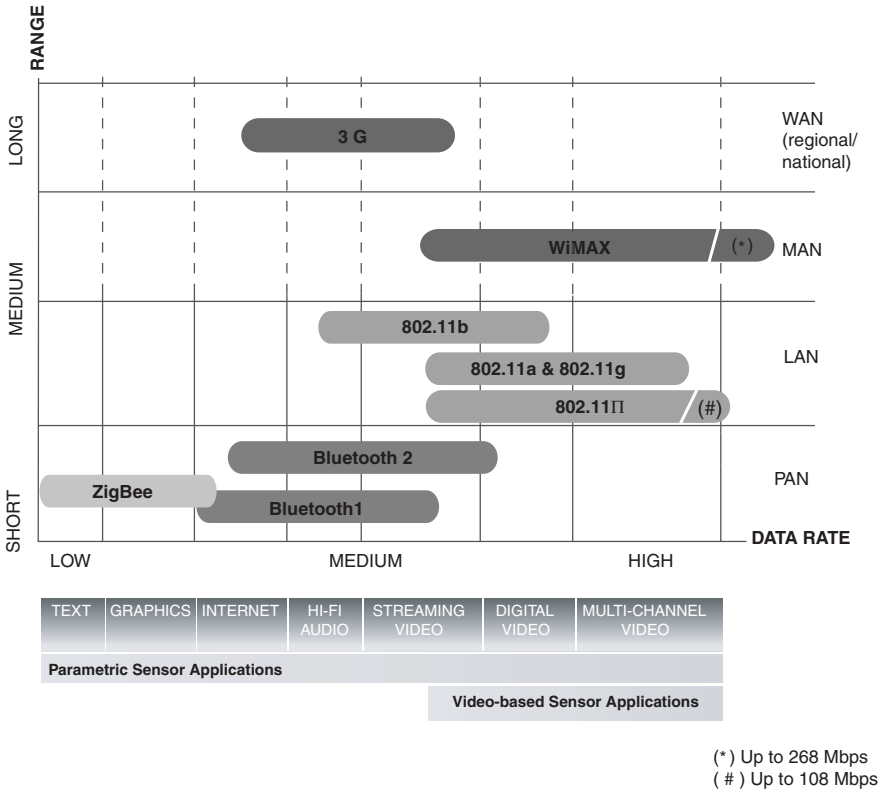


Figure 4.5 Graphical comparison of available protocols.

TABLE 4.5 Wireless Protocol Comparison

	IEEE Standard		
Property	802.11	802.15.1/Bluetooth	802.15.4/ZigBee
Range (m)	~100	~10 to 100	~10
Data throughput (Mbps)	~2 to 54	~1 to 3	~0.25
Power consumption	Medium	Low	Ultralow
Battery life measured in:	Minutes to hours	Hours to days	Days to years
Size relationship	Large	Smaller	Smallest
Cost/complexity ratio	>6	1	0.2

Source: [4.4].

The IEEE 802.15.4 standard supports a maximum data rate of 250 kbps, with rates as low as 20 kbps (slower than most telephone modems); however, it has the lowest power requirement of the group. ZigBee devices are designed to run several years on a single set of batteries, making them ideal candidates for unattended or difficult-to-reach locations. Bluetooth is a short-range communication protocol widely used in cellular-type phones and PDAs (has a range of about 10 m, or a maximum of 100 m with power boost); it operates in the 2.4-GHz ISM band and has a bandwidth of approximately 1 to 3 Mbps. IEEE 802.11a/b/g/n is a collection of related technologies that operate in the 2.4-GHz ISM band, the 5-GHz ISM band, and the 5-GHz U-NII bands; it provides the highest power and longest range of the common unlicensed wireless technologies. Transmission data rates can reach 54 Mbps (twice as much with the latest IEEE 802.11n protocol). Typically, hardware implementation of some or all of 802.11 protocols comes preinstalled on most new laptop computers; the technology is often also available for PDAs and cellular phones. RFID is the one form of wireless sensing that requires no power in the tag; it is a passive technology used for labeling and tracking. The RFID tag is the sensor; the sensor responds when power is beamed to it through the reading device. Current RFID tags can hold only 96 bits of information, but newer tags that support 128 and 256 bits are becoming available [4.4]. Most RFID tags have *integrated circuits* (ICs), microelectronic semiconductor devices with a large number of interconnected transistors and other components. Although the topic of RFIDs is not covered further in this book, a glossary of basic terms is included in Table 4.6 for completeness [4.41].

The subsections that follow provide additional details on these standardized wireless technologies. We partition the discussion into campus and MAN/WAN application spaces.

4.3.1 Campus Applications

Campus sensor communications can occur over Bluetooth, wireless LAN (WLAN), ZigBee, or WiMax/hotspot systems.

TABLE 4.6 RFID Glossary[a]

Active tag	An RFID tag that comes with a battery that is used to power the microchip's circuitry and transmit a signal to a reader. Active tags can be read from 100 ft or more away, but they are expensive—more than $20 each. Tags are used for tracking expensive items over long ranges. For instance, the U.S. military uses active tags to track containers of supplies arriving in ports.
Automatic identification	(a.k.a. automatic data capture) A method of collecting data and entering them directly into computer systems without human involvement. Technologies normally considered part of auto-ID include bar codes, biometrics, RFID, and voice recognition.
Backscatter	A method of communication between tags and readers. RFID tags using backscatter technology reflect back to the reader a portion of the radio waves that reach them. The signal reflected is modulated to transmit data. Tags using backscatter technology can be either passive or active, but either way, they are more expensive than tags that use inductive coupling.
Chipless RFID tag	An RFID tag that does not depend on an integrated microchip. Instead, the tag uses materials that reflect back a portion of the radio waves beamed at them. A computer takes a snapshot of the waves beamed back and uses it like a fingerprint to identify the object with the tag. Companies are experimenting with embedding RF reflecting fibers in paper to prevent unauthorized photocopying of certain documents. But chipless tags are not useful in the supply chain because even though they are inexpensive, they cannot communicate a unique serial number that can be stored in a database.
Closed-loop systems	RFID tracking systems set up within a company. Since the item being tracked never leaves the company's control, the company does not need to worry about using technology based on open standards.
Contactless smart card	A credit card or loyalty card that contains an RFID chip to transmit information to a reader without having to be swiped through a reader. Such cards can speed checkout, providing consumers with more convenience.
EEPROM (electrically erasable programmable read-only memory)	A nonvolatile storage device on microchips. Usually, bytes can be erased and reprogrammed individually. RFID tags that use EEPROM are more expensive than factory-programmed tags, but they offer more flexibility because the end user can write an ID number to the tag at the time the tag is going to be used.
Electromagnetic compatibility (EMC)	The ability of a system or product to function properly in an environment where other electromagnetic devices are used and not itself be a source of electromagnetic interference.
Electromagnetic interference (EMI)	Interference caused when the radio waves of one device distort the waves of another. Cells phones, wireless computers, and even robots in factories can produce radio waves that interfere with RFID tags.

TABLE 4.6 (*Continued*)

Electronic article surveillance (EAS)	Simple electronic tags that can be turned on or off. When an item is purchased (or borrowed from a library), the tag is turned off. When someone passes a gate area holding an item with a tag that has not been turned off, an alarm sounds. EAS tags are embedded in the packaging of most pharmaceuticals.
Electronic product code (EPC)	A 96-bit code created by the auto-ID center that will one day replace bar codes. The EPC has digits to identify the manufacturer, product category, and the individual item. It is backed by the Uniform Code Council and the European Article Numbering Association the two main bodies that oversee bar code standards.
Error-correcting code	A code stored on an RFID tag to enable a reader to determine the value of missing or garbled bits of data. It is needed because a reader might misinterpret some data from the tag and think that a Rolex watch is actually a pair of socks.
Error-correcting mode	A mode of data transmission between the tag and the reader in which errors or missing data are corrected automatically.
Error-correcting protocol	A set of rules used by readers to interpret data correctly from the tag.
Excite	A reader is said to "excite" a passive tag when the reader transmits RF energy to wake up the tag and enable it to transmit back.
Factory programming	The process of writing the identification number into a silicon microchip at the time the chip is made, as is necessary for some read-only tags.
Field programming	Tags that use EEPROM, or nonvolatile memory, can be programmed after being shipped from the factory.
GTAG (global tag)	A standardization initiative of the Uniform Code Council and the European Article Numbering Association for asset tracking and logistics based on RFID. The GTAG initiative is supported by Philips Semiconductors, Intermec, and Gemplus, three major RFID tag makers.
High-frequency tags	Tags that operate typically at 13.56 MHz. They can be read from about 10 ft away and transmit data faster, but they consume more power than do low-frequency tags.
Inductive coupling	A method of transmitting data between tags and readers in which the antenna from the reader picks up changes in a tag's antenna.
Low-frequency tags	Tags that typically operate at 125 kHz. The main disadvantages of low-frequency tags are that they have to be read from within 3 ft and the rate of data transfer is slow. But they are less expensive than high-frequency tags and less subject to interference.
Memory	The amount of data that can be stored on a tag.
Microwave tags	Radio-frequency tags that operate at 5.8 GHz. They have very high transfer rates and can be read from away as far as 30 ft, but they use a lot of power and are expensive.
Multiple-access schemes	Methods of increasing the amount of data that can be transmitted wirelessly within the same frequency spectrum. RFID readers use time-division multiple access (TDMA), meaning that they read tags at different times to avoid interfering with one another.

(*Continued*)

TABLE 4.6 (*Continued*)

Nominal range	The read range at which a tag can be read reliably.
Null spot	Area in the reader field that does not receive radio waves. This is essentially the reader's blind spot. It is a phenomenon common to ultrahigh-frequency systems.
Object name service (ONS)	An auto-ID center–designed system for looking up unique electronic product codes and pointing computers to information about the item associated with the code. ONS is similar to the domain name service, which points computers to sites on the Internet.
Passive tag	An RFID tag without a battery. When radio waves from the reader reach the chip's antenna, it creates a magnetic field. The tag draws power from the field and is able to send back information stored on the chip. At this juncture simple passive tags cost from about 50 cents to several dollars.
Patch antenna	A small square antenna made from a solid piece of metal or foil.
Power level	The amount of RF energy radiated from a reader or an active tag. The higher the power output, the longer the read range, but most governments regulate power levels to avoid interference with other devices.
Programming	Writing data to an RFID tag.
Proximity sensor	A device that detects the presence of an object and signals another device. Proximity sensors are often used on manufacturing lines to alert robots or routing devices on a conveyor to the presence of an object.
Read	The process of turning radio waves from a tag into bits of information that can be used by computer systems.
Read range	The distance from which a reader can communicate with a tag. Active tags have a longer read range than passive tags because they use a battery to transmit signals to the reader. With passive tags, the read range is influenced by frequency, reader output power, antenna design, and method of powering up the tag. Low-frequency tags use inductive coupling (see above), which requires the tag to be within a few feet of the reader.
Read rate	The maximum rate at which data can be read from a tag, expressed in bits or bytes per second.
Reader (also called an interrogator)	The reader communicates with an RFID tag via radio waves and passes the information in digital form to a computer system.
Reader field	The area of coverage. Tags outside the reader field do not receive radio waves and cannot be read.
Read-only tag	A tag that contains data that cannot be changed unless the microchip is reprogrammed electronically.
Read–write tag	An RFID tag that can store new information on its microchip. San Francisco International Airport uses a read–write tag for security. When a bag is scanned for explosives, the information on the tag is changed to indicate that it has been checked. The tag is scanned again before it is loaded on a plane. Read–write tags are more expensive than read-only tags and therefore are of limited use for supply chain tracking.

TABLE 4.6 (*Continued*)

RFID tag	A microchip attached to an antenna that picks up signals from and sends signals to a reader. The tag contains a unique serial number but may have other information, such as a customer's account number. Tags come in many forms, such as smart labels that are stuck on boxes, smart cards and keychain wands for paying for things, and a box that you stick on your windshield to enable you to pay tolls without stopping. RFID tags can be active tags, passive tags, or semipassive tags.
RFID tags' frequency	RFID tags use low, high, ultrahigh, and microwave frequencies. Each frequency has advantages and disadvantages that make them more suitable for some applications than for others.
Scanner	An electronic device that can send and receive radio waves. When combined with a digital signal processor that turns the waves into bits of information, the scanner is called a reader or interrogator.
Semipassive tag	Similar to active tags, but the battery is used to run the microchip's circuitry but not to communicate with the reader. Some semipassive tags sleep until they are woken up by a signal from the reader, which conserves battery life. Semipassive tags cost $1 or more.
Sensor	A device that responds to a physical stimulus and produces an electronic signal. Sensors are increasingly being combined with RFID tags to detect the presence of a stimulus at an identifiable location.
Silent commerce	This term covers all business solutions enabled by tagging, tracking, sensing, and other technologies, including RFID, which make everyday objects intelligent and interactive. When combined with continuous and pervasive Internet connectivity, they form a new infrastructure that enables companies to collect data and deliver services without human interaction.
Smart label	A label that contains an RFID tag. It is considered "smart" because it can store information, such as a unique serial number, and communicate with a reader.
Tag antenna	The antenna is the conductive element that enables the tag to send and receive data. Passive tags usually have a coiled antenna that couples with the coiled antenna of the reader to form a magnetic field. The tag draws power from this field.
Time-division multiple access (TDMA)	A method of solving the problem of the signals of two readers colliding. Algorithms are used to make sure that readers attempt to read tags at different times.
Transponder	A radio transmitter–receiver that is activated when it receives a predetermined signal. RFID tags are sometimes referred to as transponders.
Ultrahigh frequency (UHF) tag	Typically, tags that operate between 866 and 930 MHz. They can send information faster and farther than can high- and low-frequency tags. UHF tags are also more expensive than low-frequency tags, and they use more power.

(*Continued*)

TABLE 4.6 (*Continued*)

Uniform Code Council (UCC)	The nonprofit organization that overseas the Uniform Product Code, the bar code standard used in North America.
Uniform Product Code (UPC)	The bar code standard used in North America. It is administered by the Uniform Code Council.
Write rate	The rate at which information is transferred to a tag, written into the tag's memory and verified as being correct.

Source: [4.41].

[a]RFID is a method of identifying unique items using radio waves. Typically, a reader communicates with a tag, which holds digital information in a microchip; however, there are chipless forms of RFID tags that use material to reflect back a portion of the radio waves beamed at them.

Bluetooth Bluetooth is a specification for short-range RF-based connectivity for portable personal devices. It is a short-range wireless data exchange protocol designed for a small variety of tasks, such as synchronization, voice headsets, cell modem calls, and mouse and keyboard input. The specification began as a de facto industry standard; more recently, IEEE Project 802.15.1 developed a wireless PAN standard based on the Bluetooth v1.1 Foundation Specifications. The IEEE 802.15.1 standard was published in 2002. Bluetooth is directed principally to the support of personal communication devices such as telephones, printers, headsets, and PC keyboards and mice. The technology has restricted performance characteristics by design; hence, its applicability to WSN is rather limited in most cases. For these same environments, ZigBee is probably a better solution; however, given the popularity and longevity of the standard, it is given some coverage here.

As part of its effort, the IEEE has reviewed and provided a standard adaptation of the Bluetooth Specification v1.1 Foundation media access control (MAC) (L2CAP, LMP, and baseband) and the physical layer (PHY) (radio). Also specified is a clause on service access points (SAPs), which includes a LLC–MAC interface for the ISO/IEC 8802-2 LLC. A normative annex that provides a protocol implementation conformance statement (PICS) proforma has been developed. Also specified is an informative high-level behavioral ITU-T Z.100 specification and description language (SDL) model for an integrated Bluetooth MAC sublayer [4.6].

The Bluetooth specification defines a low-power, low-cost technology that provides a standardized platform for eliminating cables between mobile devices and facilitating connections between products. The system uses omnidirectional radio waves that can transmit through walls and other nonmetal barriers. Unlike other wireless standards, the Bluetooth wireless specification includes both link layer and application layer definitions for product developers. Radios that comply with the Bluetooth wireless specification operate in the unlicensed, 2.4-GHz ISM radio spectrum, ensuring communication compatibility worldwide.

Bluetooth radios use a spread-spectrum, frequency-hopping, full-duplex signal. While point-to-point connections are supported, the specification allows up to seven simultaneous connections to be established and maintained by a single radio [4.7]. AFH (adaptive frequency hopping), available with newer versions, allows for more

graceful coexistence with IEEE 802.11 WLAN systems. The signal hops among 79 frequencies at 1-MHz intervals to give an acceptable degree of interference immunity between multiple Bluetooth devices and between a Bluetooth device and a WLAN device (at least in the case where not all the available frequencies are used by the WLAN—this is probably the case in a SOHO environment, where only one or two access points are used at a location). To minimize interference with other protocols that use the same band, the protocol can changes channels up to 1600 times per second. If there is interference from other devices, the transmission does not stop, but its speed is downgraded.

Bluetooth version 1.2 allowed a maximum data rate of 1 Mbps; this results in an effective throughput of about 723 kbps. In late 2004, a new version of Bluetooth known as Bluetooth version 2 was ratified; among other features it included enhanced data rate (EDR). With EDR the maximum data rate is able to reach 3 Mbps (throughput of 2.1 Mbps) within a range of 10 m (up to 100 m with a power boost). Older and newer Bluetooth devices can work together with no special effort [4.8]. Because a device such as a telephone headset can transmit the same information faster with Bluetooth 2.0 + EDR, it uses less energy, since the radio is on for shorter periods of time. The data rate is improved by more efficient coding of the data sent across the air; this also means that for the same amount of data, the radio will be active less of the time, thus reducing the power consumption [4.7]. Newer Bluetooth devices are efficient at using small amounts of power when not actively transmitting: for example, the headset is able to burst two to three times more data in a transmission and is able to sleep longer between transmissions. Noteworthy features of Bluetooth core specification version 2.0 + EDR include:

- Three times faster transmission speed than that of preexisting technology
- Lower power consumption through a reduced duty cycle
- Simplification of multilink applications due to increased available bandwidth
- Backwardly compatible to earlier versions
- Improved bit-error-rate performance

Hardware developers were shifting from Bluetooth 1.1 to Bluetooth 1.2 in the recent past; Bluetooth 2.0 products were being introduced at press time. To be exact, version 2.0 devices have a higher power consumption; however, the fact that the transmission rate is three times faster (thereby reducing the transmission burst times) effectively reduces consumption to half that of 1.x devices. Devices are able to establish a trusted relationship; a device that wants to communicate only with a trusted device can authenticate the identity of the other device cryptographically. Trusted devices may also encrypt the data that they exchange over the air.

A Bluetooth device playing the role of "master" can communicate with up to seven devices playing the role of "slave" (groups of up to eight devices are called *piconets*). At any given instant in time, data can be transferred between the master and one slave; but the master switches rapidly from slave to slave in a round-robin fashion. (Simultaneous transmission from the master to multiple slaves is possible but is not used much

in practice.) The Bluetooth specification also makes it possible to connect two or more piconets to form a *scatternet*, with some devices acting as a bridge by simultaneously implementing the master role in one piconet and the slave role in another piconet.

The Bluetooth SIG recently established a road map for future improvements to Bluetooth. Priorities for 2005 included quality of service (QoS), security, and power consumption; priorities for 2006 were to include multicast, additional security, and long-range performance. The Bluetooth SIG is also working with developers of UWB to ensure backward compatibility with the new standard. UWB is a short-distance wireless protocol capable of transmitting up to 100 Mbps of data a distance of about 10 m; Bluetooth is only capable of 1 to 3 Mbps over the same distance. It is conceivable that Bluetooth could be supplanted by this faster technology, so the Bluetooth SIG is working to make sure that UWB is backwardly compatible with current Bluetooth devices (at present, two groups are competing for their technology to be ratified as the UWB standard). Depending on the usage cases, technologies such as ZigBee and UWB can be either complementary or overlapping [4.7]. It is hypothetically possible that Bluetooth wireless technology and UWB could converge, but work and agreements will need to take place to make this happen. The immediate problems for UWB—the two competing standards and the lack of the international regulatory approval—need to be resolved for the idea of convergence to be interesting for Bluetooth wireless technology.

WLAN The following are areas where advances in wireless LAN (WLAN) is taking place:

1. Higher WLAN speeds to support an adequate number of users in high-density environments and also voice over IP (VoIP) users. The transition to an IEEE 802.11g and/or 802.11n environment is a basic necessity in a high-density and/or high-bandwidth context.
2. Support of QoS over the wireless (and also core intranet) infrastructure. The deployment of IEEE 802.11e QoS-supporting technology is another basic necessity.
3. Secure communications is highly desirable. The deployment of IEEE 802.11i security capabilities is yet another requirement.
4. Roaming between access points, floors, and subnets is needed, as is a handoff to a cellular service when corporate WLAN service is no longer available or generally, for WN mobility situations. The deployment of IEEE 802.11r roaming capabilities addresses this requirement (capabilities not expected to be available and/or implemented until sometime in the future). Roaming also brings up the question of whether a traditional IP solution is adequate or if one needs to utilize Mobile IP (MIP) (IETF RFC 3344) [4.9]; this is a fairly complex issue.

The IEEE 802.11b and 802.11g specifications postulate a partitioning of the spectrum into 14 overlapping staggered channels whose center frequencies are

5 MHz apart; within this partitioning of the ISM spectrum, channels 1, 6, and 11 (and if available in the regulatory domain, channel 14) do not overlap. These channels (or other sets with similar gaps) can be used so that multiple networks can operate in close proximity without interfering with each other (see Figure 4.6).

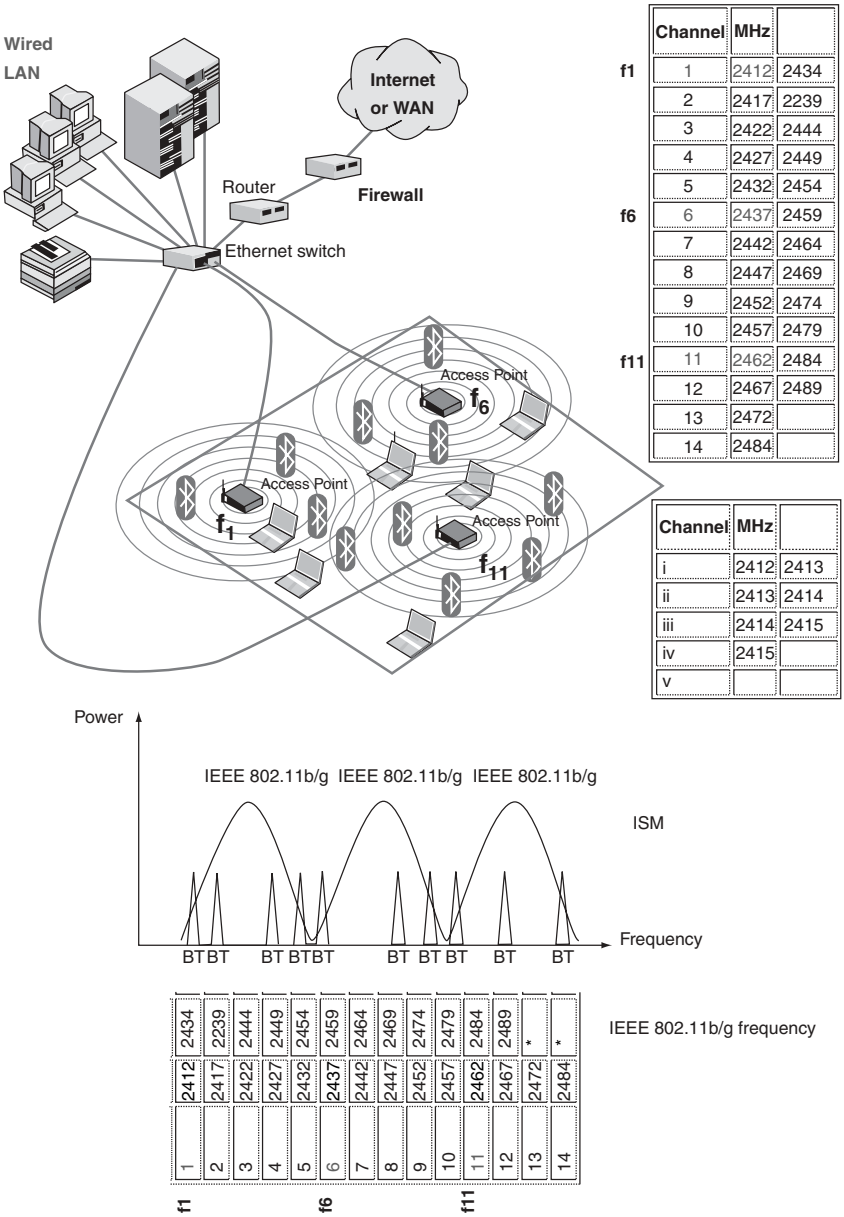


Figure 4.6 IEEE 802.11b/g frequency bands, typical topology, and bluetooth interaction.

TABLE 4.7 IEEE WLAN-Relevant Frequencies in Various Parts of the World

Channel	MHz	U.S.	Canada	Europe (ETSI)	Spain	France	Japan
1	2412	×	×	×		×	×
2	2417	×	×	×		×	×
3	2422	×	×	×		×	×
4	2427	×	×	×		×	×
5	2432	×	×	×		×	×
6	2437	×	×	×		×	×
7	2442	×	×	×		×	×
8	2447	×	×	×		×	×
9	2452	×	×	×		×	×
10	2457	×	×	×	×	×	×
11	2462	×	×	×	×	×	×
12	2467			×		×	×
13	2472			×		×	×
14[a]	2484						

[a]Channel 14, where available, is restricted to 802.11b operation.

The spectral mask for 802.11b requires that the signal be at least 30 dB down from its peak energy at ±11 MHz from the center frequency and at least 50 dB down from its peak energy at ±22 MHz from the center frequency. Note that if the transmitter is sufficiently powerful, the signal can be relatively strong even beyond the ±22-MHz point (e.g., a powerful transmitter on channel 6 can easily overwhelm a weaker transmitter on channel 11); in most situations, however, the signal in a given channel is sufficiently attenuated to interfere only minimally with a transmitter on any other channel.

The channels that are available for use in a particular country differ according to the regulations of that country. Table 4.7 identifies IEEE-relevant frequencies in various parts of the world. In the United States, for example, FCC regulations allow only channels 1 to 11 to be used. Channels 10 and 11 are the only channels that work in all parts of the world, because Spain has not licensed channels 1 to 9 for 802.11b operation.

The UNII band used in the IEEE 802.11a context is in the range 5.15 to 5.85 GHz. The 802.11a standard uses 300 MHz of bandwidth; the spectrum is divided into three *domains*, each having restrictions imposed on the maximum output power allowed. The first 100 MHz in the lower-frequency portion is restricted to a maximum power output of 50 mW; the second 100 MHz has a higher maximum, 250 mW; and the third, 100 MHz, intended primarily for outdoor applications, has a maximum power output of 1.0 W. It is generally recognized that the higher-frequency UNII band is limited intrinsically to shorter ranges than the ISM band, due to higher path loss, limiting the utility of 802.11a relative to that of 802.11b/g in the WSN context, except for within-building applications. In particular, there is an increase of excess path loss with frequency. Table 4.8 provides a comparison

TABLE 4.8 A Comparison of IEEE 802.11b/g and IEEE 802.11a

	802.11b/802.11g	802.11a
Available bandwidth	83.5 MHz	300 MHz
Unlicensed frequencies of operation	2.4–2.4835 GHz	5.15–5.35 GHz, 5.725–5.825 GHz
Number of non-overlapping channels	3 (indoor–outdoor)	4 (indoor–outdoor)
Data rate per channel	1, 2, 5.5, 11, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps
Modulation	DSSS	OFDM

between IEEE 802.11b/g and IEEE 802.11a. The IEEE 802.11a protocol uses a complex digital modulation method: specifically, orthogonal frequency-division multiplexing (OFDM); this digital modulation method requires more linearity in amplifiers because of the higher peak-to-average power ratio of the OFDM signal transmitted. In addition, better phase noise performance is required because of the closely spaced overlapping carriers. These issues tend to add to the implementation cost of 802.11a products. Although IEEE 802.11a was approved in the late 1990s, new product development has proceeded much more slowly than with 802.11b/g, due to the cost and complexity of implementation.

Frequency-division multiplexing (FDM) is a multiplexing technology that transmits multiple signals from or for different users simultaneously over a single transmission path, such as a cable or wireless system (commercial FM radio is an example). Each signal occupies its own unique frequency range (carrier), which is modulated by the data (text, voice, video, etc.). The OFDM spread-spectrum technique distributes the data over a large number of carriers that are spaced apart at precise frequencies. This spacing provides the orthogonality, which prevents the demodulators from seeing frequencies other than their own. The benefits of OFDM are high spectral efficiency, resiliency to RF interference, and lower multipath distortion. This is useful because in a typical terrestrial broadcasting scenario there are multipath channels (i.e., the signal transmitted arrives at the receiver using various paths of different length). Since multiple versions of the signal interfere with each other [intersymbol interference (ISI)] it becomes difficult to extract the original information. OFDM is the modulation technique used for digital television in Europe, Japan, and Australia [4.10].

As stated previously, a drawback of 5 GHz is that higher-frequency signals experience more difficulties propagating through physical obstructions encountered in an office (walls, floors, and furniture) than do those at 2.4 GHz. There is an intrinsic degradation in throughput as the distance between the transmitter and receiver increases. See Figure 4.7 for a comparison of the two standards or bands with regard to propagation or performance and distance. An advantage of 802.11a is its ability to deal with delay spread and multipath reflection effects: The slower symbol rate and placement of significant guard time around each symbol reduces

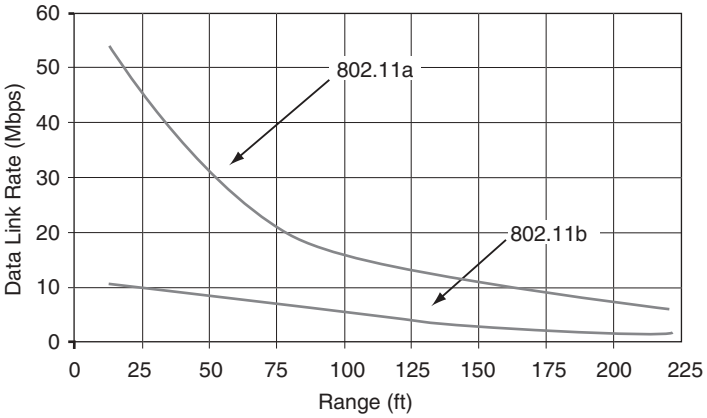


Figure 4.7 Performance characteristics of IEEE 802.11a: throughput comparison versus distance (indoor applications).

the ISI caused by multipath interference; by contrast, 802.11b networks are generally range limited by multipath interference rather than the loss of signal strength over distance.

Now-emerging multiple-input, multiple-output (MIMO) systems use multiple antennas to transmit and receive radio signals. MIMO methods increase the throughput and quality of the signals received. IEEE 802.11n uses MIMO techniques. For example, MIMO–OFDM will allow service providers to deploy a broadband wireless access (BWA) system that has non-line-of-sight (NLOS) functionality. Specifically, MIMO–OFDM takes advantage of the multipath properties of environments using base station antennas that do not have LOS. As noted, in multipath environments the original signal and the individual echoes each arrive at the receiver antenna at slightly different times, causing the echoes to interfere with one another, thus degrading signal quality. The MIMO system uses multiple antennas to transmit data simultaneously in small segments to the receiver, which can process the data flows and put them back together. This process, called *spatial multiplexing*, increases the data-transmission speed proportionally by a factor equal to the number of antennas transmitting. In addition, since all data are transmitted both in the same frequency band and with separate spatial signatures, this technique utilizes the spectrum fairly efficiently [4.10].

ZigBee In this section we provide a brief description of ZigBee. ZigBee is the only standards-based technology designed to address the unique needs of low-cost, low-power WSNs for remote monitoring, home control, and building automation network applications in the industrial and consumer markets [4.11]. The wireless systems discussed in previous subsections provide high data rates at the expense of power consumption, application complexity, and cost. However, there are many wireless monitoring and control applications for industrial and home markets that require longer battery life, lower data rates, and less complexity

than those made available by existing wireless standards. For commercial success one needs a standards-based wireless technology that has performance characteristics that closely meet the requirements for reliability, security, low power, and low cost [4.12], [4.40].

For such wireless applications a targeted standard has been developed by the IEEE [4.13]. The IEEE 802.15 Task Group 4 was chartered to investigate a low-data-rate solution with multimonth to multiyear battery life and very low complexity. The standard is intended to operate in an unlicensed international frequency band. Potential applications fot this standard are home automation, wireless sensors, interactive toys, smart badges, and remote controls. The scope of the task group has been to define the physical layer (PHY) and the media access control (MAC) [4.14]. This standards-based interoperable wireless technology is optimized to address the specific needs of low-data-rate wireless control and sensor-based networks [4.12]. Functionality defined by the ZigBee Alliance is used at the upper layers.

The ZigBee Alliance ratified the first ZigBee specification in 2004, making the development and deployment of power-efficient, cost-effective, low-data-rate monitoring, control, and sensing networks a reality. ZigBee/IEEE 802.15.4 is expected to become the leading wireless technology for a plethora of uses, ranging from building automation to industrial and residential applications. Developers were anticipating ZigBee-compliant consumer products as quickly as early 2005 [4.11]. A graphical representation of the areas of responsibility between the IEEE standard, ZigBee Alliance, and user is presented in Figure 4.8; the definition of the application profiles is organized by the ZigBee Alliance [4.11], [4.42].

Hotspot/WiMax In recent years service providers have deployed IEEE 802.11b/11g-based hotspot services to support Internet access and VoIP applications [4.15]. Furthermore, there is interest in delivering metro-wide Internet/VoIP services using WiMax (IEEE 802.16-based) connectivity. Since WiMax is newer, we focus here on this technology (see Table 4.9 for a technical comparison of WiMax to Wi-Fi [4.16]).

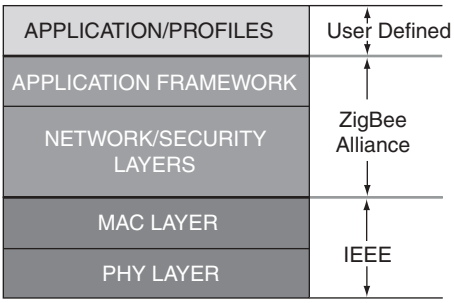


Figure 4.8 ZigBee protocol stack.

TABLE 4.9 Comparative Overview of Wi-Fi and Mobile WiMax Technology

	Wi-Fi Based on 802.11	WiMax Based on 802.16e-2005
Spectrum	Unlicensed, 2.4 GHz (ISM band) and 5.8 GHz (UNII band)	Licensed less than 6 GHz
Range and coverage	Typically less than 100 meters	PMP, NLOS typically 1 to 10 km depending on frequency and terrain characteristics. Point-to-point, LOS up to 50 km
Applications	Indoor WLAN, fixed and nomadic usage model	Outdoor WMAN, fixed, nomadic, portable, and mobile applications
Peak downstream data rate	Up to 54 Mbps in 20 MHz channel BW	Up to 50 Mbps in 10 MHz channel BW
QoS	802.11e provides better QoS support than 802.11a,b,g but only set traffic priorities (up to 8). It is not deterministic, so it is possible for one connection or traffic type to override and starve another connection	Provides guaranteed service levels for specific types of traffic on a connection-by-connection basis. 802.16 uses priority, committed, and peak information rates and can meet specific latency and jitter requirements for specific types of traffic. Can also regenerate network clocks over the air
Privacy and security	WEP uses a repetitive key and is easily defeated. This has been upgraded to WPA and WPA2 with 802.11i	802.16 has two data encryption modes: mandatory 56-bit DES and 128 AES. Also supports device base station, subscriber station, and user authentication. Has secure key exchange and is 802.1x compliant
Latency	CSMA/CA approach for scheduling increases latency with multiple connections. Latency is not deterministic and therefore, adversely affects QoS	Uses a grant-request mechanism as opposed to CSMA/CA; this eliminates delays with multiple users sharing the same channel. This is necessary to support latency sensitive traffic such as VoIP
System gain	System gain is limited by transmit power limits in the unlicensed 2.4 and 5 GHz bands, thus limiting the range capability of 802.11. Support for MIMO in 802.11n will improve this somewhat. Lack of support for subchannelization limits uplink system gain with battery-operated laptops as subscriber stations	Licensed frequency bands permits higher base station Tx power. Subchannelization provides increased system gain in the uplink direction. Adaptive antenna systems including MIMO, beamforming, space-time coding (STC), and spatial multiplexing (SM) also enhance system gain and range
Support for battery-operated handsets	Subchannelization is not supported so subscriber station Tx power must be sufficient to transmit full channel. This is satisfactory for a laptop with a large battery or	Uplink subchannelization reduces Tx power requirements for battery-operated subscriber devices. Various sleep mode options are available to conserve battery life

TABLE 4.9 (*Continued*)

	access to AC power, but not acceptable for mobile handhelds, PDAs, etc. Also no sleep mode	
Multipath immunity	OFDM with a FFT size of 64 provides some immunity to multipath	S-OFDMA with FFT size of 512 to 2048 FFT for channel BWs from 5 to 20 MHz
Interference immunity	802.11 does not have support for transmit power control (TPC) or dynamic channel selection (DCS). Some of these issues are addressed with 802.11h	Aided by transmit power control, subchannelization and support for adaptive antenna systems

Source: WiMax Forum.

The IEEE 802.16 Working Group has developed a point-to-multipoint (PMP) broadband wireless access standard for systems in the frequency ranges 10 to 66 GHz and sub-11 GHz. This technology is targeted to metropolitan area environments. The IEEE 802.16 standard covers both the MAC and PHY layers. A number of PHY considerations were taken into account for the target environment. At higher frequencies, line of sight (LOS) is a must. This requirement eases the effect of multipath, allowing for wide channels, typically greater than 10 MHz in bandwidth. This gives the IEEE 802.16 protocol the ability to provide very high capacity links on both the uplink and downlink. For sub-11 GHz, non-line-of-sight (NLOS) capability is a requirement. The original IEEE 802.16 MAC was enhanced to accommodate different PHYs and services, which address the needs of different metropolitan environments. The standard is designed to accommodate either time-division duplexing (TDD) or frequency-division duplexing (FDD) deployments, allowing for both full- and half-duplex terminals in the FDD case [4.16]. IEEE 802.16a has a LOS radius of 50 km and an NLOS of 10 km or thereabouts, depending on the types of obstacles in the topography. WiMax is the marketing name of the IEEE 802.16 standard.

The MAC was designed specifically for the PMP wireless access environment. It supports higher layer or transport protocols, such as ATM, Ethernet, and IP, and is designed to accommodate easily future protocols that have not yet been developed. The MAC is designed for high bit rates (up to 268 Mbps each way) and operates on a broadband physical layer, while delivering ATM-compatible QoS, UGS (unsolicited grant service), rtPS (real-time polling service), nrtPS (non-real-time polling service), and best effort services. The frame structure allows terminals to be dynamically assigned uplink and downlink burst profiles according to their link conditions. This allows a trade-off between capacity and robustness in real time and provides roughly a two-fold increase in capacity on average compared to nonadaptive systems while maintaining appropriate link availability. The 802.16 MAC uses a variable-length protocol data unit (PDU) along with a number of other concepts that greatly increase the efficiency of the standard. Multiple MAC PDUs may be concatenated into a single burst to save PHY overhead. Additionally, multiple

service data units (SDUs) for the same service may be concatenated into a single MAC PDU, saving on MAC header overhead. Fragmentation allows large SDUs to be sent across frame boundaries to guarantee the QoS of competing services. Payload header suppression can be used to reduce the overhead caused by the redundant portions of SDU headers. The MAC uses a self-correcting bandwidth request–grant scheme that eliminates the overhead and delay of acknowledgments while allowing better QoS handling than that of traditional acknowledgment schemes. Terminals have a variety of options for requesting bandwidth, depending on the QoS and traffic parameters of their services. Terminals can be polled individually or in groups; they can steal bandwidth already allocated to make requests for more; they can signal the need to be polled, and they can piggyback requests for bandwidth [4.16].

A typical WiMax network consists of a base station supported by a tower- or building-mounted antenna. The base station connects to the appropriate terrestrial network (PSTN, Internet, etc.) Applications include, but are not limited to, point-to-point communication between stations, point-to-multipoint communication between the base station and clients, backhaul services for Wi-Fi (802.11) hotspots, broadband Internet services to home users, private-line services for users in remote locations, and metro-wide WSN applications.

4.3.2 MAN/WAN Applications

MAN/WAN sensor communications can occur over WiMax/hotspots or 3G systems. After a brief discussion of a brand-new (but speculative) technology, cognitive radios (CRs), in the remainder of the section we focus on the evolution of cellular networks in terms of the desire to provide a lateral data channel that supports any number of applications, including WSNs.

Cognitive Radios and IEEE 802.22 With the plethora of wireless services that are becoming available, stakeholders believe that the limiting factor at this time is the scarcity of radio spectrum. Studies have shown that most of this spectrum scarcity is concentrated in the unlicensed bands; this is where the major advancements in spectrum use have taken place (e.g., Wi-Fi, cordless phones). Licensed bands, however, typically experience considerable underutilization. CR-based approaches represent a new paradigm in wireless communications that aims at utilizing the large amount of underused spectrum in an intelligent way while not interfering with other incumbent devices in frequency bands already licensed for specific uses [4.43].

The IEEE 802.22 wireless regional area network (WRAN) standard is the first worldwide project to employ CR concepts for dynamically sharing spectrum with television broadcast signals. IEEE 802.22 seeks to develop a standard for a cognitive radio-based PHY–MAC–air interface for use by license-exempt devices on a noninterfering basis in spectrum allocated to the television broadcast service. This standard specifies the air interface, including the MAC and PHY, of fixed point-to-multipoint wireless regional area networks operating in the VHF–UHF TV broadcast bands between 54 and 862 MHz. This standard is intended to enable

deployment of interoperable IEEE 802 multivendor wireless regional area network products, to facilitate competition in broadband access by providing alternatives to wireline broadband access and extending the deployability of such systems into diverse geographic areas, including sparsely populated rural areas, while preventing harmful interference to incumbent licensed services in the TV broadcast bands [4.44].

There is a large untapped market for broadband wireless access in rural and other unserved or underserved areas where wired infrastructure cannot be deployed economically. Products based on this standard will be able to serve those markets and increase the efficiency of spectrum utilization in spectrum currently allocated to, but unused by, the TV broadcast service. WRAN supports an approach for operation over large, potentially sparsely populated areas (e.g., rural areas), taking advantage of the favorable propagation characteristics in the VHF and low-UHF TV bands. The unique requirements of operating on a strict noninterference basis in spectrum assigned to, but unused by, the incumbent licensed services requires a new approach using purpose-designed cognitive radio techniques that will permeate both the PHY and MAC layers [4.44]. In principle, this wireless service can also be used to support metro-area WSNs.

Cognitive radio—where a device can sense its environment and location and then alter its power, frequency, modulation, and other parameters so as to dynamically reuse available spectrum—is now just emerging. CR can, in theory, allow multidimensional reuse of spectrum in space, frequency, and time, obliterating the spectrum and bandwidth limitations that have slowed broadband wireless development in the United States and elsewhere. This new technology is in a way similar to *software-defined radio* (SDR). With SDR the software embedded in a radio cell phone, for example, can define the parameters under which the phone should operate in real time as its user moves from place to place; traditional cell phone parameters, by contrast, are relatively fixed in terms of frequency band and protocol. A SDR is a flexible wireless communications device that implements its signal processing entirely in software: Software radios can easily change such features as modulation, bandwidth, and coding, which are fixed in more traditional radios. The basic technology of software radio is now being deployed in military and commercial applications. CR is even more advanced than SDR: CR, as noted, can sense its environment and learn from it [4.45]. The FCC is currently investigating commercial applications, and the Defense Advanced Research Projects Agency is proposing military applications (under the XG—or next-generation communications—program). DARPA's aim is to develop technology that allows multiple users to share spectrum in a way that coexists with, and complements, sharing protocols included in today's Wi-Fi technologies. Work on CR and IEEE 802.22 is currently under way.

3G Cellular Networks Over the past decade, mobile communications technology has evolved from first-generation (1G) analog voice-only communications to second-generation (2G) digital, voice, and data communications. The demand for more cost-effective and feature-enhanced mobile applications has led to the

development of new-generation wireless systems (or simply 3G). State-of-the-art 3G handsets are designed to provide multimegabit Internet access with an ''always on'' feature and data rates of up to 2.048 Mbps [4.17].

In reference to cellular applications, the core network of traditional cellular systems is typically based on a circuit-switched architecture similar to that utilized in wireline networks. Wireless service providers are now in the process of evolving their core networks to IP technology. Wireless telecommunications started as a subdiscipline of wireline telephony, and the absence of global standards resulted in regional standardization. Two major mobile telecommunications standards have emerged: time-division multiple access/code-division multiple access (TDMA/CDMA) developed by the Telecommunications Industry Association (TIA) in North America, and Global System for Mobile Communications (GSM) developed by the European Telecommunications Standards Institute (ETSI) in Europe. As one moves toward third-generation (3G) wireless services, there is a need to develop standards that are more global in scope [4.18].

In the late 1990s there were discussions on the development of standards for a 3G mobile system with a *core network* based on evolutions of the GSM and an *access network* based on all the radio access technologies (i.e., both frequency- and time-division duplex modes) supported by the plethora of different carriers (in different countries). This project was called the Third Generation Partnership Project (3GPP) [4.19]. Around the turn of this decade, the American National Standards Institute (ANSI) decided to establish the Third Generation Partnership Project 2 (3GPP2), a 3G partnership initiative for evolved ANSI/TIA/Electronics Industry Association (EIA) networks [4.20]. In addition, there also was the establishment of a strategic group called International Mobile Telecommunications-2000 (IMT-2000) within the International Telecommunication Union (ITU) [4.21], which focused its work on defining interfaces between 3G networks evolved from GSM on the one hand and ANSI on the other, with the goal of enabling seamless roaming between 3GPP and 3GPP2 networks. Because of the worldwide (''universal'') roaming characteristic, 3GPP started referring to 3G mobile systems as the Universal Mobile Telecommunication System (UMTS) [4.22]. Since then, there has been advocacy for and progress toward an *all-IP UMTS network architecture*. The all-IP UMTS specifications replaced the earlier circuit-switched transport technologies by utilizing packet-switched transport technologies, and introduce multimedia support in the UMTS core network [4.22].

Figure 4.9 depicts some basic industry transition paths to 3G wireless. As implied in the preceding paragraph, currently the 3G world is split into two camps: the cdma2000, which is an evolution of the IS-95 standard, and the wideband code division multiple access (W-CDMA)/time-division synchronous CDMA (TD-SCDMA)/enhanced data rates for GSM evolution (EDGE) camp, whose standards are improvements of GSM, IS-136, and packet data cellular (PDC)—these are all second-generation standards. In the United States, Verizon Wireless and Sprint PCS were the first two carriers to develop 3G networks. The other major carriers have already advanced to the 2.5G technology, with the vision to soon join the 3G community [4.17].

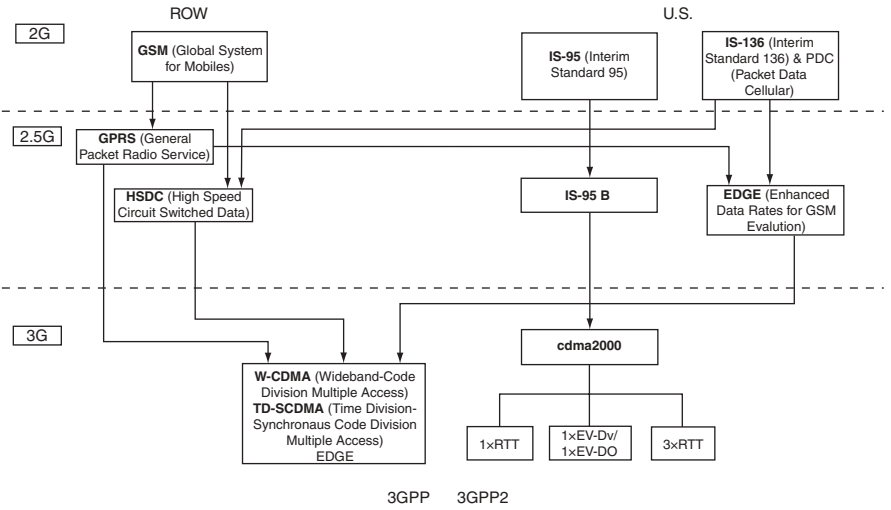


Figure 4.9 Migration path(s) to 3G wireless networks.

The original scope of 3GPP was to produce globally applicable technical specifications and technical reports for a 3G mobile system based on evolved GSM core networks and the radio access technologies that they support [i.e., universal terrestrial radio access (UTRA), both FDD and TDD modes]. The scope was subsequently amended to include maintenance and development of the GSM technical specifications and technical reports, including evolved radio access technologies [e.g., general packet radio service (GPRS) and EDGE] [4.23]. 3GPP and 3GPP2 also address the issue of the limited data throughput capabilities of 2G/2.5G systems, motivating providers to start work on 3G wideband radio technologies that can provide higher data rates (e.g., for Internet access, messaging, location-based services). This work resulted in 3G wireless radio technologies that provide data rates of 144 kbps for vehicular, 384 kbps for pedestrian, and 2 Mbps for indoor environments, and meet the ITU IMT-2000 requirements. Clearly, these channels can be utilized for WSN applications. Now that the radio technology standards to support higher data rates have been developed, the providers are focusing on development of standards for all-IP networks [4.18].

3GPP The basic characteristics of an all-IP network are end-to-end IP connectivity, distributed control and services, and gateways to legacy networks [4.18]. As noted earlier in the chapter, there are two major protocol suites for supporting VoIP: session initiation protocol (SIP), standardized by the IETF, and H.323, standardized by the ITU. It was decided in 3GPP to use only SIP as the call control protocol between terminals and the mobile network. Interworking with other H.323 terminals (e.g., fixed H.323 hosts) is performed by a dedicated server in the network. New elements in this architecture, compared to a traditional 2G cellular network, are as follows (see also Figure 4.10) [4.22]:

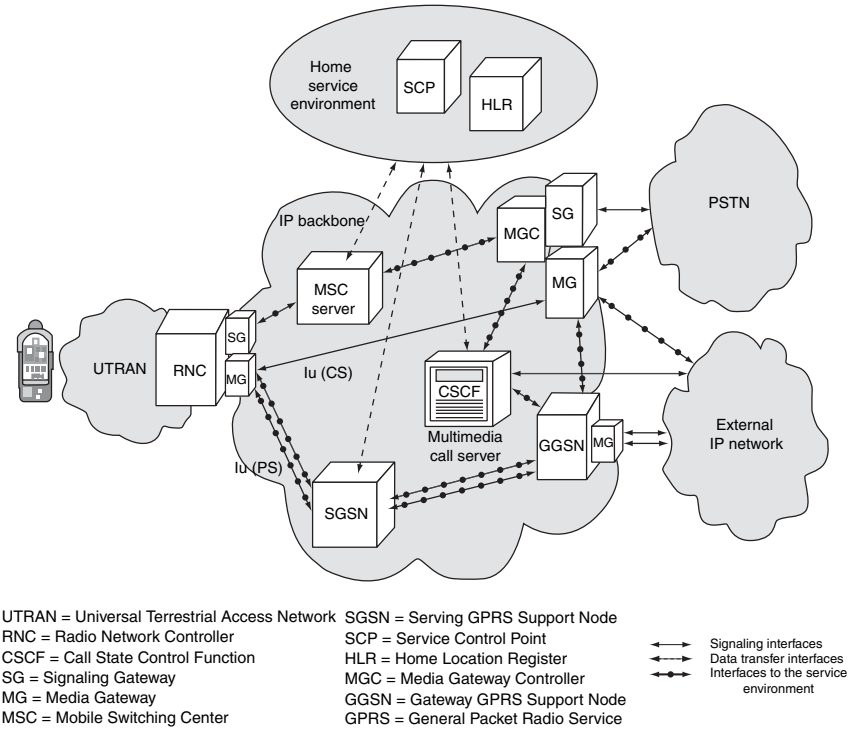


Figure 4.10 All-IP 3G cellular service. (From [4.22].)

1. *Mobile switching center* (*MSC*) *server.* The MSC server controls all calls coming from circuit-switched mobile terminals and mobile-terminated calls from a PSTN/GSM network to a circuit-switched terminal. The MSC server interacts with the media gateway control function (MGCF) for calls to and from the PSTN. There is a functional split of the MSC, where the call control and services part is maintained in the MSC server, and the switch is replaced by an IP router [Media Gateway (MG)]. This functional split reduces the deployment cost and guarantees the support of all existing services.
2. *Call state control function* (*CSCF*). The CSCF is an SIP server that provides or controls multimedia services for packet-switched (IP) terminals, both mobile and fixed.
3. *MG at the Universal Terrestrial Access Network* (*UTRAN*) *side*. The MG transforms VoIP packets into UMTS radio frames. The MG is controlled by the MGCF by means of Media Gateway Control Protocol ITU H.248. The media gateway is added to fulfill the second requirement. In Figure 4.10 the MG is drawn at the UTRAN side of the Iu interface, hence the Iu interface between the core network and UTRAN is IP-based. The MG can also be located at the core network side of the Iu interface (without impact on the UTRAN).

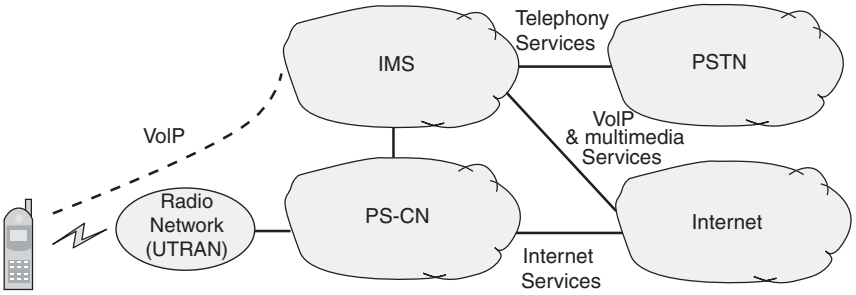
4. *MG at the PSTN side*. All calls coming from the PSTN are translated to VoIP calls for transport in the UMTS core network. This MG is controlled by the MGCF using the ITU H.248 protocol.
5. *Signaling gateway* (*SG*). An SG relays all call-related signaling to and from the PSTN and UTRAN on an IP bearer and sends the signaling data to the MGCF. The SG does not perform any translation at the signaling level.
6. *MGCF*. The first task of the MGCF is to control the MGs via H.248. Also, the MGCF performs translation at the call control signaling level between ISDN user part (ISUP) signaling used in the PSTN and SIP signaling used in the UMTS multimedia domain.
7. *Home subscriber server* (*HSS*). The HSS is the extension of the home location register (HLR) database with the subscribers' multimedia profile data.

For the transport of data traffic, UMTS uses the General Packet Radio Service (GPRS) network. For voice calls there are two options: for packet-switched mobile terminals, voice data are transported over the GPRS network using the GPRS tunneling protocol (GTP) on top of IP; all mobility is addressed by the GPRS protocols. For circuit-switched mobile terminals, voice samples are transported over IP between the MGs using the Iu frame protocol; in the latter case there is no tunneling; hence mobility has to be solved in a different way, by media gateway handovers.

An essential architectural principle of the 3GPP framework is to provide separation of service control from connection control. 3GPP started with GPRS as the core packet network and overlaid it with call control and gateway functions required for supporting VoIP and other multimedia services. The functions are provided via IETF-developed protocols to maintain compatibility with the industry direction in all-IP networks. These new networks also provide VoIP capabilities; the same capabilities that support VoIP can also support WSNs. To support VoIP, call control functions are provided by the call state control function (CSCF) (refer to Figure 4.10). The mobile terminal communicates with the CSCF via SIP protocols. The CSCF performs call control functions, service switching functions, address translation functions, and vocoder negotiation functions. For communication to the public-switched telephone network (PSTN) and legacy networks, PSTN gateways are utilized. To support roaming to 2G wireless networks, roaming gateway functions are also provided. The serving GPRS support node (SGSN) uses existing GSM registration and authentication schemes to verify the identity of the data user. This makes the SGSN access-technology-dependent. The GPRS HLR is enhanced for services that use IP protocols. The data terminal makes itself known to the packet network by doing a *GPRS-attach*. The IP address is anchored in the GPRS gateway node, GGSN, during the entire data session. This limits the mobility of the data terminal to within GPRS-based networks. To provide mobility with other networks, a MIP foreign agent can be incorporated in the GGSN [4.18].

3G Release 1999 was the first release of the 3GPP specifications; it was essentially a consolidation of the underlying GSM specifications and the development of the new UTRAN radio access network. The foundations were laid for future high-speed traffic transfer in both circuit- and packet-switched modes. That release was followed over the years by Releases 4, 5, and 6 [4.23]. Release 1999 was an introductory specification on the architecture of the UMTS network. According to Release 1999, UMTS comprises a UTRAN and two core networks [circuit-switched core network (CS-CN) and packet-switched core network (PS-CN)], which link up to services networks such as the PSTN and the Internet. Thus, using both traditional circuit- and modern packet-switched networks, UMTS Release 1999 supports various services, including voice, data (fax, SMS), and Internet access. Later, Release 4 adapted to the same architecture added more services to the UMTS network. The coexistence of two core networks, however, signified many limitations compared to competitive 3G systems, especially in video and multimedia services. Release 5 was a solution to the limitations that came along to modernize the UMTS architecture currently employed in 3G networks around the world. In this final phase, the PS-CN dominates the CS-CN and takes responsibility for telephony services. Systems based on UMTS Release 5 have much lower infrastructure and maintenance costs and provide enhanced services. Release 6 added additional capabilities [4.17].

As seen at the macro level in Figure 4.11, a new component is added to the basic UMTS architecture: the supplementary IP Multimedia Subsystem (IMS). IMS aims at supporting both telephony and multimedia services. IMS's role in UMTS architecture is to interact with both the PSTN and the Internet to provide all types of multimedia services to users. The CSCF element in the IMS infrastructure is responsible for signaling messages between all IMS components in order to control multimedia sessions originated by the user. Consequently, there is a proxy-CSCF (P-CSCF), an interrogating-CSCF (I-CSCF), and a serving-CSCF (S-CSCF), all responsible for particular signaling functions using SIP. The P-CSCF's responsibility



UTRAN = UMTS Terrestrial Access Network
PS-CN = Packet Switched Core Network
IMS = IP Multimedia Subsystem

Figure 4.11 UMTS Release 5 basic architecture.

is to act as the QoS enforcement point and to provide local control for emergency services. I-CSCF is an optional component that interacts with the HSS to find the location of the S-CSCF (it is optional because the P-CSCF can be set up to negotiate directly with the S-CSCF). The S-CSCF controls all the session management functions for the IMS. Depending on the capabilities of the IMS and the capacity requirements, there may be more than one S-CSCF node, and others can eventually be added to the system. The function of the HSS is to handle all user information, such as subscription and location queries. The HSS communicates with the CSCFs via an IP-based protocol called Cx interface; all other IMS components interact with each other via SIP. The media gateway control function (MGCF) is in charge of controlling one or more MGs; the MGCF interacts with the S-CSCF and the transport signaling gateway (T-SGW). MGs are bit processors for end-to-end users; their function is to convert PCM in the PSTN to IP-based formats, and vice versa. Finally, the T-SGW is included in the IMS because of the need to convert signaling system number 7 (SS7) to IP since the PSTN is only SS7-compatible [4.17].

3GPP2 3GPP2 has also undertaken work to enhance the IP architecture for multimedia services (including voice). The approach here is to capitalize on the synergies of Internet technologies and to use a single network for all services. 3GPP2 has created a new packet data architecture building on the CDMA 2G and 3G air interface data services. 3GPP2 has taken advantage of 3G high data rates and existing work in IETF on MIP to enhance the network architecture to provide IP capabilities. One advantage of using IETF protocols is ease in interworking and roaming with other IP networks. The other major advantage is that it can provide private network access (virtual private networking) via a MIP tunnel with IP security [4.18].

In the 3GPP2 architecture, IP connectivity reaches all the way to the base station transceiver (BTS). Both the base station controller (BSC) and BTS are contained in the IP-based radio access network node. This means that the BSC will be a router-based IP node containing some critical radio control functions (e.g., power control, soft handoff frame selection). The remaining control functions, such as call and session control, mobility management, and gateway functions, are moved out to the managed IP network. This allows for a distributed and modular control architecture. Since much of the communication will be between wireless and legacy terminals, gateway functions are provided for roaming to 2G wireless networks and interworking with the PSTN. In the 3GPP2 architecture, the mobile terminal uses mobile-IP-based protocols to identify itself. The packet data serving node (PDSN) contains a MIP foreign agent (FA) functionality. When the mobile terminal attaches to the FA, the FA establishes a mobile IP tunnel to the home agent (HA) and sends a registration message to the HA. The HA accesses the authorization, authentication, and accounting (AAA) server to authenticate the mobile terminal. The IP address of the mobile terminal is now anchored in the HA for the duration of the data session. The data device connected to the mobile terminal can be handed over to any other access device that supports mobile IP. Thus, this approach can provide mobility across different access networks (wireless, wireline, etc.). However, since it

essentially uses address translation to provide mobility, it cannot do fast handoff, due to the latency of address updates from distant agents [4.18].

Comparison of Services The 3GPP and 3GPP2 architectures are different because of the underlying base networks and evolution strategies. In 3GPP, GPRS-based mobility was already defined, so the IP network enhancements were considered on top of GPRS. On the other hand, 3GPP2 needed to develop a mobility mechanism for packet data since one did not exist previously. As noted, 3GPP2 has decided to use MIP as the basis for packet data mobility [4.18].

To illustrate the similarities and differences of the two approaches, mobility needs to be addressed at three levels: air-interface mobility, link-level mobility, and network-level mobility. Air-interface mobility supports cell-to-cell handoff within a radio access network. Link-level mobility maintains a point-to-point protocol (PPP) context across multiple radio access networks. Network-level mobility provides mobility across networks. In both approaches, air-interface mobility is handled in the radio access network. Air-interface mobility is specific to the radio technology, therefore harmonization of the two depends on the harmonization efforts under way for global CDMA. In 3GPP, link-level mobility is handled by GTP; this protocol is used to provide mobility to other 3GPP-defined networks. The 3GPP architecture also provides an option in which an FA may be located in the GGSN. This allows roaming from GPRS-based networks to other IP access networks. In 3GPP2, link-level mobility is provided by defining a tunneling protocol as an extension of MIP. The MIP architecture allows the mobile device to have a point of presence and to roam across any IP network. Registration and authentication in the 3GPP architecture for access and data networks are integrated and utilize the schemes used for wireless. In the 3GPP2 architecture, the registration and authentication for access and data networks are performed separately. For a data network, authentication and registration as defined in MIP are used; hence, the data architecture is access-independent [4.18].

3G Operators After many delays, 3G networks are now being rolled out. 3G wireless networks offer all the normal mobile telephony services plus high-speed data access. 3G operators may initially limit data access to their own branded data services or at least price open Internet access significantly higher than access to their own traditional data services. The mobile market, however, is competitive, and there are consumer and business requirements for access to the open Internet. In fact, flat-rate bundles for data access services are already available in some markets. This data-channel access can be used to support VoIP services [4.24]. Wireless operators that are looking to continue to displace wireline voice revenues as their business posture need to reduce their overall delivery costs as users move from 2G TDM to 3G VoIP [4.25]. Below we look briefly at the VoIP possibilities because a successful commercial ‘‘play’’ in this space would accelerate the deployment (and ubiquity) of 3G services, thereby indirectly opening up an opportunity for WSN applications.

For example, equipment upgrades can introduce high-speed data capabilities to UMTS networks. Specifically, new technologies now becoming available enable carriers to provide new ''blended lifestyle services'' via any wireline, wireless, or Wi-Fi/WiMax endpoint by providing a variety of 3GPP IMS functional elements (as discussed previously), including the call session control functions, media resource function controller, policy decision function, and breakout gateway control function. Because this equipment expands the data channel on 3G cellular networks, these upgrades also lay the foundation for operators to introduce VoIP and more advanced multimedia services on their mobile networks (here one can transmit IP-voice datagrams over the data channel). VoIP over 3G gives operators the ability to support a greater number of voice users at a lower cost, in turn helping to ensure that voice services can continue to be delivered profitably. Some researchers estimate that 3G wireless can deliver voice by way of VoIP for a quarter of the cost per minute compared to 2G TDM methods [4.25].

For mobile operators that have invested heavily in 2G and 3G cellular networks, there may be relatively little incentive to offer VoIP services according to observers (their existing networks already deliver better-quality voice services at lower cost than VoIP can achieve today). However, VoIP may look more attractive to those service providers seeking to bypass mobile operators' traditional voice tariffs, particularly if an opportunity to undercut those tariffs using VoIP arises due to significant drops in 3G data pricing. A number of mobile operators have launched unlimited-use data tariffs that could make them vulnerable to customers using VoIP to cut their spend [4.26]. 3G service-provider VoIP offerings could appear in the United States in the 2008 or 2009 time frame. That would come after operators upgrade their 2.5G/3G networks. For example, upgrades to 1xEV-DO provide peak data rates of about 1.8 Mbps compared to typical rates of 300 to 400 kbps for the current generation of 1xEV-DO [4.27].

Calculations of the threat to 3G revenues from broadband wireless (WiMax) have focused mainly on data, but as some 3G carriers start to put VoIP in a more central position in their strategies, they could find that this service segment is also affected. The 3G UMTS and CDMA technologies may have been the first to promise both voice and broadband-class data on one network and device, but the emergence of usable VoW has also moved formerly data-only approaches into this space. A potential early limit on VoIP over 3G data access could be the limited upstream capability of the initial 3G services. W-CDMA can deliver up to 384 kbps downstream but only 64 kbps upstream; it is preferable to have data rates exceeding 64 kbps, but if that is all that is available, one can make do for most VoIP services [4.24]. Road maps for data networks such as CDMA EVDO (evolution—data only) and UMTS's data-only strand, TDD,[2] now include VoIP [4.25].

[2]UMTS TDD mobile broadband technology is a packet data implementation of the international 3GPP UMTS standard. Unlike W-CDMA, which uses FDD (frequency division), UMTS TDD is designed to work in a single unpaired frequency band. One of the largest benefits of using TDD is that it supports variable asymmetry, meaning that an operator can dictate how much capacity is allocated to downlink versus uplink. As the traffic patterns for data typically heavily favor the downlink, this results in better use of spectrum assets and higher efficiency [4.23].

1. The shift is already visible in the CDMA market, even without taking into account challenges from broadband wireless. New EV-DO equipment aims at peak data rates of 3.1 Mbps and supports VoIP. As such, it could perhaps make a further upgrade to the next CDMA generation, EV-DV (evolution—data and voice) unnecessary. This equipment was expected to start shipping in 2006, and although EV-DO with VoIP will take advantage of the spectral efficiencies of CDMA less well than EV-DV, this will be outweighed by early availability and lower prices [4.25].
2. In the UMTS space, manufacturers have already developed a TDD mobile handset offering VoIP as well as the usual broadband packet-based services, and providers have completed the first successful transmission of a call from a mobile VoIP handset over UMTS TDD and claim that the network is ideal for voice because it features high capacity, low latency, and low power requirements. Their services will be more compelling if they can offer voice, and therefore they will be less likely to opt for a pure IP solution such as 802.16 instead of TDD. TDD-ready handsets are currently becoming commercially available [4.25].

Hotspot/WiMax Operators For operators considering deployment of broadband wireless access technologies (e.g., WiMax), being able to offer VoIP could strengthen the business case for investing in such networks by moving operators beyond a focus on low-margin Internet access. Fixed/wireline operators have shown interest in use of wireless VoIP in trying to defend against fixed mobile substitution by developing services that combine VoIP over WLAN/hotspot/WiMax with cellular voice elsewhere [4.24,4.26]. Again, a successful VoIP application would drive deployment, which can be advantageous to WSN applications.

Fixed-Mobile Convergence Operators Recently, there has been interest in fixed-mobile convergence (FMC). Mobile network operators plan to leverage emerging IMS service platforms to deliver ''one phone, one number'' telephony over both fixed and mobile infrastructure. This means that a mobile handset will use 2G/3G mobile infrastructure when the user is outdoors and VoIP over Wi-Fi when the user is at work or at home. Mobile operators see IMS and FMC as an opportunity to take additional market share from traditional fixed-line operators. However, once high-speed Internet access becomes available on mobile phones, a plethora of VoIP services will follow [4.24].

Most telephone calls originate from inside buildings, where cellular mobile coverage is poorest. As such, residential users are often forced to keep their fixed-line services for use when they are at home; the same applies in office buildings, with the added problem that wireless operators have not been in a position to offer the Centrex or PBX features that enterprises require. In theory, however, that could change with the advent of IMS and FMC [4.24].

To enable converged handsets, FMC relies on broadband Internet access for the fixed portion and WLANs now and WiMax in the future for the mobile portion. WLANs are deployed at a large percentage of enterprises, and home-based Wi-Fi

setups are spreading rapidly. Broadband Internet access is also available in thousands of public hotspots. The first round of convergence depends on handsets that support 2G, 3G, and Wi-Fi connections on the same phone. Mobile operators then use an IMS platform to transparently combine regular mobile service on their 2G or 3G mobile network with VoIP services over Wi-Fi and/or fixed broadband access. Because of the fact that the mobile portion of FMC uses the existing mobile number and the existing mobile switching network elements, mobile operators have an advantage [4.24].

Without broadband Internet access, VoIP service providers are less of a threat to mobile operators' FMC services. The business proposition of fixed-mobile convergence is to hit the sweet spot of high convenience and low cost [4.24]. VoIP vendors will be in a better position to provide their own FMC if WiMax delivers on its promise of wireless broadband Internet access; however, widespread WiMax deployment is expected to take a number of years. Instead, the VoIP competitive threat may be enabled by the mobile operators' own data services [4.24]. A successful VoIP penetration could indirectly drive WSN applications by building out the infrastructure.

4.4 CONCLUSION

In this chapter we looked at radio transmission issues. To maximize the opportunity for widespread and cost-effective deployment of WSN, plans are to use existing and/or emerging COTS wireless communications and infrastructures rather than having to develop an entirely new, specially designed apparatus. WSNs can use a number of wireless COTS technologies, such as Bluetooth, ZigBee, WLAN/hotspots, WiMax, and 3G.

APPENDIX A: MODULATION BASICS

Modulation Capsule We have indicated that WSNs implementers will probably use off-the-shelf radio technology such as ZibBee, WiMax, Wi-Fi, or 3G; this means that they do not necessarily have to worry about the fundamental aspects of radio science and modulation. However, a brief discussion of modulation is in order. Table 4A.1 lists some key terms related to modulation, from various sources, including [4.34], [4.37], and [4.38]. In the context of digital transmission and modulation, the related topic of digital encoding is also of interest.

A basic technique used in radio transmission is phase-shift keying (PSK), mentioned in the body of the chapter (Table 4A.1 lists a number of approaches, but PSK is a fundamental methodology). In PSK the frequency and amplitude of the carrying signal are both kept constant. Phase-coherent PSK utilizes two defined signals: A logic 0 is represented by a π-degree phase shift, and a logic 0 is represented by a 0-degree phase shift; this is, however, a complex situation for the

TABLE 4A.1 Basic Modulation Terminology

(Multiple) phase-shift keying (M-PSK)	(e.g., 8-PSK) In digital transmission, angle modulation in which the phase of the carrier is discretely varied in relation either to a *reference phase* or to *the phase of the immediately preceding signal element*, in accordance with data being transmitted. In a communications system, the representing of characters, such as bits or quaternary digits, by a shift in the phase of an electromagnetic carrier wave with respect to a reference, by an amount corresponding to the symbol being encoded. For M-ary PSK, M different phases are required, and every n(where $M = 2^n$) bits of the binary bit stream are coded as one signal that is transmitted as $A \sin(\omega t + \theta_j)$ $j = 1, \ldots, M$. The output is a baseband representation of the modulated signal. The M-ary number parameter, M, is the number of points in the signal constellation. Baseband M-ary phase-shift keying modulation with a phase offset of Θ maps an integer m between 0 and $M-1$ to the complex value $\exp(j\Theta + j2\pi m/M)$. The modulator accepts binary representations of integers between 0 and $M-1$. It modulates each group of K bits, called a binary *word*. The input can be either a vector of length K or a frame-based column vector whose length is an integer multiple of K. *Note 1:* BPSK is the same as 2-PSK; QPSK is the same as 4-PSK; 8-ary-PSK is the same as 8-PSK. (Q = quarternary.) *Note 2:* For example, when encoding bits, the phase shift could be 0° for encoding a "0" and π for encoding a "1," or the phase shift could be $-\pi/2$ for "0" and $+\pi/2$ for "1", thus making the representations for 0 and 1 a total of π apart. *Note 3:* In PSK systems designed so that the carrier can assume only two different phase angles, each change of phase carries one bit of information (i.e., the bit rate equals the modulation rate); if the number of recognizable phase angles is increased to four, 2 bits of information can be encoded into each signal element; similarly, eight phase angles can encode 3 bits in each signal element.
(Noncoherent) differentially detected DPSK (DDPSK)	(e.g., 8-DPSK) Phase-shift keying that is used for digital transmission in which the phase of the carrier is varied discretely in relation to the *phase of the immediately preceding signal element* and in accordance with the data being transmitted.
Binary PSK (BPSK)	*See* (Multiple) phase-shift keying (M-PSK), Note 1. For binary PSK (BPSK): $S_0(t) = A \cos \omega t$ represents binary 0 $S_1(t) = A \cos(\omega t + \pi)$ represents binary 1 A BPSK modulator modulates a signal using the binary phase-shift keying method. The output of the modulator is a baseband representation of the signal modulated. The input

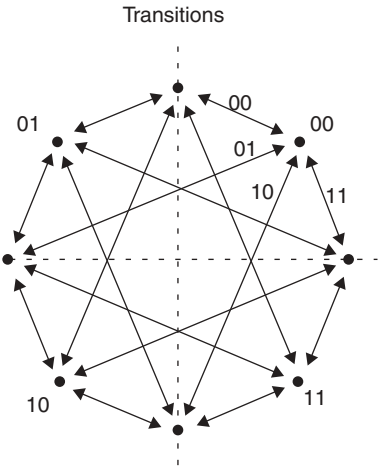
TABLE 4A.1 (*Continued*)

	is a discrete-time binary-valued signal. If the input bit is 0 or 1, respectively, the modulated symbol is $\exp(j\Theta)$ or $-\exp(j\Theta)$ respectively, where Θ is the phase offset parameter.
BPSK	*See* Binary PSK.
CDPSK	*See* Coherent(ly detected) DPSK.
Coherent	Pertaining to a fixed phase relationship between corresponding points on an electromagnetic wave. *Note:* A truly coherent wave would be perfectly coherent at all points in space. In practice, however, the region of high coherence may extend over only a finite distance.
Coherent demodulation	Demodulation using a carrier reference that is synchronized in frequency and phase to the carrier used in the modulation process.
Coherent(ly detected) DPSK (CDPSK)	(e.g., 8-CDPSK) Phase-shift keying that is used for digital transmission, in which the phase of the carrier is discretely modulated in *relation to the phase of a reference signal* and in accordance with data to be transmitted, and in which the modulated carrier is of constant amplitude and frequency. *Note:* A phase comparison is made of successive pulses, and information is recovered by examining the phase transitions between the carrier and successive pulses rather than by the absolute phases of the pulses.
DBPSK	*See* Differential binary phase-shift keying.
DDPSK	*See* (Noncoherent) differentially detected DPSK.
Differential(ly encoded) phase-shift keying (DPSK) modulation	A form of PSK in which the reference phase for a given interval is the phase of the signal during the preceding interval.
Differential binary phase-shift keying (DBPSK)	A DBPSK modulator modulates a signal using the differential space binary phase-shift keying method. The output is a baseband representation of the signal modulated. The input is a discrete-time binary-valued signal; the input can be either a scalar or a frame-based column vector. • If the first input bit is 0 or 1, respectively, the first symbol modulated is $\exp(j\Theta)$ or $-\exp(j\Theta)$, respectively, where Θ is the phase offset parameter. • If a successive input bit is 0 or 1, respectively, the symbol modulated is the previous modulated symbol multiplied by $\exp(j\Theta)$ or $-\exp(j\Theta)$, respectively.
Differential detection	As an alternative to recovering a coherent reference, some systems just compare the phase in the present interval to the phase in the previous intervals. The signal received in the preceding interval is delayed for one signal interval and is used as a reference to demodulate the signal in the next interval. Assuming that the data have been encoded in terms of phase shift instead of absolute phase positions,

(*Continued*)

TABLE 4A.1 (*Continued*)

	one can decode the data properly. Hence, this technique, referred to as *differential detection*, inherently requires differential encoding. In general, PSK systems require differential encoding since the receivers have no means of determining whether a recovered reference is a sine reference or a cosine reference. Furthermore, the polarity of the recovered reference is ambiguous. Thus, error probabilities for PSK systems are doubled automatically because of the differential encoding process. Differential detection, on the other hand, implies an even greater loss of performance since a noisy reference is used in the demodulation process. Typically, differential detection imposes a penalty of 1 to 2 dB in the SNR.
Differential modulation	Modulation in which the choice of the significant condition for for any signal element is dependent on the significant condition for the preceding signal element.
Differential quaternary phase-shift keying (DQPSK)	A modulator that modulates a signal using the differential quaternary phase-shift keying method. The input contains pairs of binary values. The output is a baseband representation of the signal modulated. The input can be either a vector of length 2 or a frame-based column vector whose length is an even integer. The figure below shows the signal constellation for the DQPSK modulation method when the phase offset parameter Θ is $\pi/4$. The arrows indicate the four possible transitions from each symbol to the next symbol.



DQPSK	*See* Differential quaternary phase shift keying.
ECC	*See* Forward error-correction coding.

TABLE 4A.1 (*Continued*)

Forward error-correction (FEC) coding	(a.k.a. error-correction coding) Achieved by adding redundancy, such as parity-check symbols, to a message before transmission.This redundancy provides the corresponding decoder at the receiver with information such that the receiver can detect and correct transmission errors. FEC has potential application whenever digital data move over an imperfect (e.g., noisy) channel, such as satellite communications systems, wireless LANs, WSNs, digital cellular communications, digital video broadcast, and others. Among the most powerful and common FECs today are Reed–Solomon (RS) codes, convolutional codes, and combinations of the two. M. Reed and G. Solomon developed the codes in 1960; the codes are the standard FECs for Intelsat and for digital video broadcasting applications. Convolutional codes are another group of powerful codes that became popular with introduction of the Viterbi decoding algorithm. The concatenation of these two Vcodes, Reed–Solomon–Viterbi (RSV), has for many years represented the state of the art in FEC [4.38].
M-ary differential phase-shift keying (M-DPSK)	The M-DPSK modulator modulates a signal using the *M*-ary differential phase-shift keying method. The output is a baseband representation of the signal modulated. The *M*-ary number parameter, *M*, is the number of possible output symbols that can immediately follow a given output symbol. The input must be a discrete-time signal. The modulator accepts binary representations of integers between 0 and $M-1$. It modulates each group of K bits, called a binary *word*. The input can be either a vector of length K or a frame-based column vector whose length is an integer multiple of K.
M-DPSK	*See M*-ary differential phase-shift keying.
M-PSK	*See* (Multiple) phase-shift keying.
Phase coherent (phase coherence)	The state in which two signals maintain a fixed phase relationship with each other or with a third signal that can serve as a reference for each.
Phase modulation (PM)	Angle modulation in which the phase angle of a carrier is caused to depart from its reference value by an amount proportional to the instantaneous value of the modulating signal.
Phase-shift keying (PSK)	The form of phase modulation in which the modulation function shifts the instantaneous phase of the modulated wave (signal) between predetermined discrete values (e.g., when encoding bits, the phase shift could be 0° for encoding a 0 and π for encodinga 1, or the phase shift could be $-\pi/2$ for 0 and $+\pi/2$ for 1, thus making the representations for 0 and 1 a total of π apart).
QAM	*See* Quadrature amplitude modulation.
QPSK	*See* Quaternary PSK.

(*Continued*)

TABLE 4A.1 (*Continued*)

Quadrature amplitude modulation (QAM)	To achieve higher-speed data communication, a combination of PSK and AM can be used, producing the QAM method. This makes use of 0-, π/2-, π-, $\frac{3}{2}\pi$-degree phase shifts together with ASK.
Quaternary PSK (QPSK)	*See also* (Multiple) phase-shift keying (M-PSK), Note 1. If we define four signals, each with a phase shift differing by 90°, we have quadrature phase-shift keying (QPSK). The input binary bit stream $\{dk\}$, $dk = 0,1,2,\ldots$, arrives at the modulator input at a rate of $1/T$ bps and is separated into two data streams $dI(t)$ and $dQ(t)$ containing odd and even bits, respectively: $d_1(t) = d_0,d_2,d_4,\ldots$ $d_0(t) = d_1,d_3,d_5,\ldots$

receiver because the phase shifts are from an absolute value (see Figure 4A.1). In differential PSK (DPSK) there is a phase shift relative to the previous logic bit transmitted. Binary 0 is a π/2-degree phase change from the previous logic bit and binary 1 is a $\frac{3}{2}\pi$-degree phase change from the previous logic bit; here, the receiver only needs to detect the phase change that took place from the preceding bit, rather than being compared to an absolute value that it, somehow, needs to know.

As noted in the preceding paragraph, it is often desirable to reduce the complexity of a receiver by removing some of the phase-tracking requirements on the demodulator. This can be done by differentially encoding the binary data prior to transmission; this process encodes the data not in the absolute phase of the transmitted symbol but in the phase difference between two consecutively transmitted symbols. In a PSK environment, this technique, known as *differentially encoded PSK* (DPSK), is typically applied to either BPSK or QPSK signal sets (see Figure 4A.2). There are two levels of simplification available in differentially encoded schemes.

1. *Coherently detected DPSK* uses a coherent signal to perform demodulation. The differential decoding simply allows for the removal of ambiguity at the receiver, due to symmetries in the transmitted signal set. The penalty taken

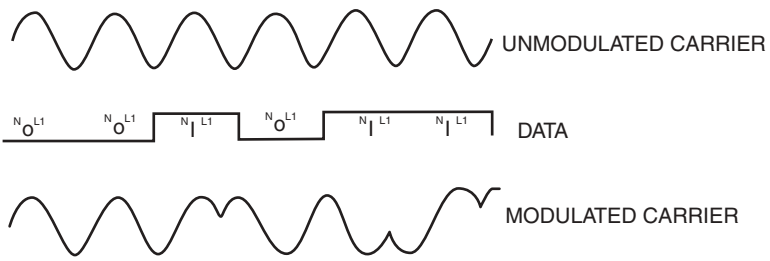


Figure 4A.1 PSK.

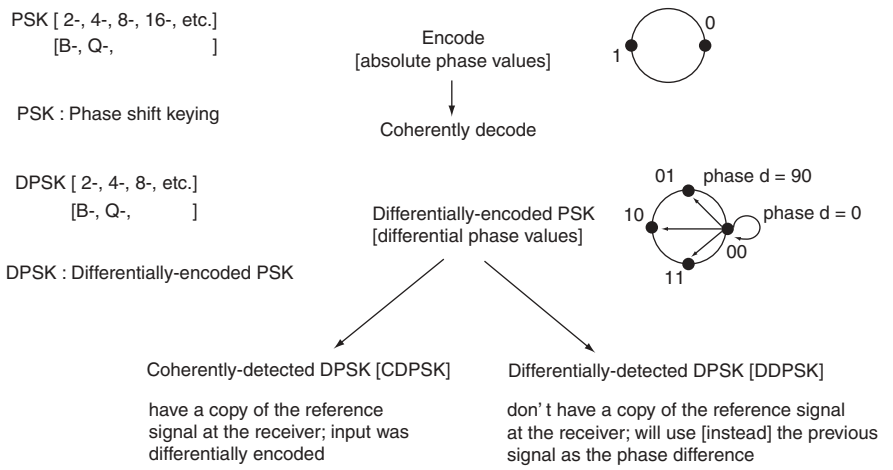


Figure 4A.2 Differentially encoded schemes.

for this simplification is typically about 1 to 2 dB of performance. Note that this performance loss is due to the fact that the effective bit error rate at the input of the decoder is approximately double that of nondifferentially encoded PSK. This is an inherent quality of the DPSK scheme, and cannot be avoided.

2. *Differentially detected DPSK* completely eliminates the coherent demodulation signal. This technique allows for further simplification at the receiver, but suffers slightly reduced performance relative to coherently detected DPSK. For both types of DPSK, the soft metric values depend on both the current and previous points received.

Encoding Capsule As stated earlier, in the context of digital transmission and modulation, digital encoding is the topic of focus. The science of digital encoding was developed in the late 1940s, with the development of Shannon's information theory. In 1948, Claude Shannon derived theoretical machinery that allows one to define the highest rate at which information can be transmitted reliably over a channel, and to compare the performance of a physical encoder–decoder with the limits of the medium. It is the challenge of the implementation engineer to come up with an encoder–decoder that is as close to "best" as possible while maintaining a reasonable level of complexity and cost [4.28–4.33]. Communication-system designers deal routinely with trade-offs among data reliability, efficient use of available spectrum, data throughput, and cost.

Forward error correction (FEC) is one of the most powerful tools available to address channel performance trade-offs, and better FEC yields more design options. For example, with 3 dB of coding gain one could increase range by 40%, reduce antenna size by 30%, reduce transmitter power by a factor of 2, and reduce the required noise figure of the receiver by 3 dB. Alternatively, one can use a

higher-order modulation scheme, which can reduce the required bandwidth by 50% or increase data throughput by a factor of 2 [4.38]. The most common FEC algorithms in use today are (1) the Reed–Solomon (RS) codes (developed the codes in 1960), (2) the convolutional codes, and (3) combinations of these two. Convolutional codes became popular with the introduction of the Viterbi decoding algorithm. The concatenation of these two codes, Reed–Solomon–Viterbi (RSV), has been for many years the best-in-breed algorithm.

Whereas the IEEE 802.11b/g standard does not include any FEC mechanisms, the 802.16a standard utilizes FEC to improve range and reduce bandwidth congestion associated with packet retransmissions. The default form of FEC is the well-known Reed–Solomon concatenated with Viterbi (RSV); as an option, the 802.16a standard also supports the higher-performing block product codes (BPCs), alternatively called block turbo codes (BTCs), turbo product codes (TPCs), or Tanner product codes [4.39]. As noted in the body of the chapter, the IEEE 802.16a standard offers significantly improved bit rates and distances.

Until 1990 it was a widely accepted that the performance point of a practical encoder–decoder operating on an additive white Gaussian noise (AWGN) channel could be no closer than about 3 dB from the theoretical performance limit, known as *channel capacity*. This point, for a fixed SNR, is known as the *practical capacity*, and until recently, it was regarded as a barrier beyond which practical systems could not perform (as we note below, progress has been made in this arena). Multipath channels represent an even greater technical challenge, as discussed above, since communicating over these channels is even more difficult.

The decade of the 1990s gave rise to changes in digital transmission practices that have been utilized since 1948. The concept of iterative decoding of concatenated codes, commonly referred to as *turbo coding*, has given the engineering community a way to rethink how one transmits information. In 1993, Claude Berrou, Alain Glavieux, and Punya Thitimajshima shattered the concept of practical capacity with an encoder–decoder that achieved a bit error rate of 10^{-5} within 1 dB of channel capacity [4.35,4.36]. Essentially overnight, engineers were offered about 2 dB of additional coding performance on the AWGN channel at the expense of increased decoding complexity. Furthermore, for the first time in history, a reasonably practical coding alternative was offered that performed so close to the theoretical "best" that significant, additional performance gains were essentially impossible. Any additional improvements would have to come, not in the form of gains in coding performance (at least not gains over 1 dB), but in the form of reduced system complexity. The complete algorithm employed by Berrou et al. consists of two concatenated, recursive convolutional encoders. Because the encoder consists of concatenated convolutional encoders, this class of turbo codes is known as *turbo convolutional codes* (TCCs). The decoding algorithm employs two soft-in, soft-out (SISO) decoding modules to form the confidence metric for each transmitted information bit. These SISOs operate in an iterative manner that requires, for each iteration, a complete forward and reverse traversal of the trellis. Furthermore, for each iteration, the confidence of every data bit must be calculated using a very complicated summation over the paths and states of the current trellis stage. The complexity of such an

algorithm, although acceptable for many software applications, is often restrictive in a hardware implementation [4.35,4.36].

Parallel, concatenated, convolutional turbo codes are good error-correction-coding technology but have limitations. The first problem was that more extensive computer simulation of the codes exposed a weakness in these codes. The performance of the codes at low bit error rates (BERs) was within 1 dB of capacity; however, the performance tailed off, or met an ''error floor,'' at high BERs, such that legacy codes such as the Reed–Solomon were still superior. The second problem was that the complexity of the required SISO decoder was such that a cost-efficient decoder was unavailable for most commercial applications. In 1998, a new approach to turbo codes solved both of these problems. Using efficient SISO-decoder algorithm hardware developers recently introduced the first commercially viable turbo decoder based on the iterative decoding of product codes rather than the convolutional codes [4.38]. In the general sense, turbo product, or block turbo, codes are composed of a multidimensional array of block codes, such as Hamming and BCH (Bose–Chaudhuri–Hocquenghem) codes.

REFERENCES

[4.1] T. S. Rappaport, ''An Introduction to Indoor Radio Propagation,'' http://sss-mag.com/indoor.html, 2001.

[4.2] R. H. Katz, ''CS 294-7: Radio Propagation,'' White Paper, University of California–Berkeley, 1996.

[4.3] T. S. Rappaport, *Wireless Communications: Principles and Practice*, IEEE Press, Piscataway, NJ, 1996.

[4.4] B. Peters, ''Sensing Without wires: Wireless Sensing Solves Many Problems, But Introduces a Few of Its Own,'' *Machine Design*, Penton Media, Cleveland, OH, http://www.machinedesign.com/ASP/viewSelectedArticle.asp?strArticleId=57795&str-&strSite=MDSite&Screen = & CURRENTISSUE&CatID=3.

[4.5] T. H. Lin, W. J. Kaiser, G. J. Pottie, ''Integrated Low-Power Communication System Design for Wireless Sensor Networks,'' *IEEE Communications*, Dec. 2004, pp. 142ff.

[4.6] IEEE 802.15 WPAN Task Group 1 (TG1), WPAN, June 20, 2005.

[4.7] Bluetooth SIG, www.bluetooth.com (more information at www.bluetooth.org).

[4.8] G. Fleishman, ''Inside Bluetooth 2.0,'' *Macworld*, Feb. 9, 2005.

[4.9] C. Perkins, ''IP Mobility Support for IPv4,'' RFC 3344, IETF, Sterling, VA, Aug. 2002.

[4.10] http://www.wave-report.com/tutorials/OFDM.htm.

[4.11] ZigBee Alliance, Bishop Ranch, CA, http://www.zigbee.org/.

[4.12] W. C. Craig, ''ZigBee: Wireless Control That Simply Works,'' *ZMD America*, Dec. 8, 2004; ''Open House,'' ZigBee Alliance, Bishop Ranch, CA, http://www.zigbee.org/.

[4.13] IEEE 802.15 WPAN Task Group 4 (TG4), http://grouper.ieee.org/groups/802/15/pub/TG4.html.

[4.14] E. Callaway, P. Gorday, L. Hester, J. A. Gutierrez, M. Neave, B. Heile, V. Bahl, ''Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless

Personal Area Networks,'' *IEEE Communications*, Vol. 40, No. 8, pp. 70–77, Aug. 2002.

[4.15] D. Minoli, *Hotspot Networks: Wi-Fi for Public Access Locations*, McGraw-Hill, New York, 2002.

[4.16] WiMAX Forum, Beaverton, OR, http://www.wimaxforum.org/home.

[4.17] N. Mavrakis, ''3G Wireless Systems: A Comprehensive Study,'' White Paper, Stevens Institute of Technology, Hoboken, NJ, Dec. 15, 2002.

[4.18] G. Patel, S. Dennett, ''The 3GPP and 3GPP2 Movements Toward an All-IP Mobile Network,'' *IEEE Personal Communications*, Aug. 2000.

[4.19] 3GPP, European Telecommunications Standards Institute, http://www.3GPP.org.

[4.20] 3GPP2, European Telecommunications Standards Institute, http://www.3GPP2.org.

[4.21] ITU, ''The IMT-2000 initiative,'' ITU-R Draft Record M; ''Detailed Specifications of the Radio Interfaces of MT-2000,'' Document 8/126; International Telecommunications Union, Geneva, Switzerland, http://www.itu.int/imt.

[4.22] L. Bos, S. Leroy, ''Toward an All-IP-Based UMTS System Architecture,'' *IEEE Network*, Jan. 2001.

[4.23] UMTS TDD Alliance, http://www.umtstdd.org.

[4.24] B. Turner, ''The Impact of VoIP, Wi-Fi and 3G Data on Wireless Telecom: How Fixed-Mobile Convergence Will Reshape the Wireless Industry,'' International Wireless Telecom-Carriers Global Edition, World Media Online Limited, London, info@wirtel.co.uk.

[4.25] Staff, ''Broadband Wireless Threatens 3G Voice Ambitions,'' *Wireless Watch*, Oct. 26, 2004.

[4.26] Online Magazine staff, ''Wireless Voice over IP: Technical and Commercial Prospects,'' *3G Online Magazine*, Mar. 22, 2005, http://www.3g.co.uk/PR/March2005/1232.htm.

[4.27] Mobile Pipeline staff, ''Verizon Looking at VoIP over 3G,'' *Mobile Pipeline*, Apr. 1, 2005, http://www.commweb.com/showArticle.jhtml?articleID=160401527.

[4.28] A. J. Viterbi, *Principles of Coherent Communication*, New York, McGraw-Hill, 1966.

[4.29] W. C. Lindsey, M. K. Simon, *Telecommunication Systems Engineering*, Prentice-Hall, Englewood Cliffs, NJ, 1973.

[4.30] W. C. Lindsey, ''Phase-Shift-Keyed Signal Detection with Noisy Reference Signals,'' *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 2, No. 4, July 1966, pp. 393–401.

[4.31] P. C. Jain, ''Detection of a PSK Signal Transmitted Through a Hard-Limited Channel,'' *IEEE Transactions on Information Theory*, Vol. 19, No. 5, Sept. 1973, pp. 623–630.

[4.32] V. K. Prabhu, ''PSK Performance with Imperfect Carrier Phase Recovery,'' *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 12, No. 2, Mar. 1976, pp. 275–285.

[4.33] N. M. Blachman, ''The Effect of Phase Error on DPSK Error Probability,'' *IEEE Transactions on Communications*, Vol. 29, No. 3, Mar. 1981, pp. 364–365.

[4.34] *IEEE Authoritative Dictionary of IEEE Standards Terms*, 7th ed., ANSI/IEEE Std. 100 (formerly called *IEEE Standard Dictionary of Electrical and Electronics Terms*), IEEE Press, Piscataway, NJ, 2001.

[4.35] C. Berrou, A. Glavieux, ''Near Optimum Error-Correcting Coding and Decoding: Turbo Codes,'' *IEEE Transactions on Communications*, Vol. 44, Oct. 1996.

[4.36] C. Berrou, A. Glavieux, P. Thitimajshima, "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes," *Conference Record of the IEEE International Conference on Communications*, 1993.

[4.37] "Communications Blockset," MathWorks, Natick, MA, http://www.mathworks.de/access/helpdesk/help/toolbox/commblks/ref/mpskmodulatorbaseband.shtml#245366.

[4.38] D. Williams, "Turbo-Product Codes Advance ECC Technology," *Advanced Hardware Architectures*, edn, www.ednmag.com, Feb. 3, 2000, pp. 77ff.

[4.39] B. A. Banister, "Using Turbo Product Codes in Client Station Uplink for Reduced Power Consumption," White Paper, Comtech AHA Corporation, Moscow, ID, 2005.

[4.40] G. Karayannis, "Emerging Wireless Standards: Understanding the Role of IEEE 802.15.4 and ZigBee™ in AMR and Submetering—Mapping Your Future: From Data to Value," *AMRA 2003 International Symposium Conference Record*.

[4.41] M. Roberti, "Glossary of RFID Terms," RFID Journal, Inc., Hauppauge, NY, http://www.rfidjournal.com/article/articleview/208.

[4.42] J. Adams, "Designing with 802.15.4 and ZigBee," presented at the Industrial Wireless Applications Summit, San Diego, Ca, Mar. 9, 2004.

[4.43] C. Cordeiro, "Wireless Communication and Networking (WiCAN)," Wireless Communication and Networking (WiCAN) Department, Philips Research, Briarcliff Manor, NY, Carlos.Cordeiro@philips.com; www.ececs.uc.edu/∼cordeicm.

[4.44] IEEE 802 LAN/MAN Standards Committee, "802.22 WG on WRANs (Wireless Regional Area Networks)," www.ieee802.org/22, Oct. 1, 2005.

[4.45] P. Mannion, "Sharing Spectrum the Smarter Way," *EE Times*, Apr. 5, 2004, http://www.commsdesign.com/news/tech_beat/www.eet.com/showArticle.jhtml?articleID=18700443.