Guide to Wireless Communications, 3rd Edition

Chapter 5
Wireless Personal Area Networks

Objectives

- Describe a wireless personal area network (WPAN)
- List the different WPAN standards and their applications
- Explain how Bluetooth and ZigBee work
- Describe the security features of low-rate WPAN technology

© Cengage Learning 2014

What is a WPAN?

- Wireless personal area network (WPAN)
  - Group of technologies that are designed for short-range communications
  - Eliminates the need for wires or cables to interconnect multiple devices
- Applications for WPAN technology include:
  - Home control systems (smart home)
  - Connecting audio and video devices to computers
  - Portable device data exchange
  - Industrial control systems

© Cengage Learning 2014

What is a WPAN?

- Applications for WPAN technology include :
  - Location services — smart tags used to locate people at home or at the office
  - Security systems
  - Interactive toys
  - Inventory tracking
- Advantages
  - WPAN devices use very little power
  - Short range helps maintain security and privacy

© Cengage Learning 2014

Existing and Future Standards

- Institute of Electrical and Electronics Engineers (IEEE)
  - Currently developing various standards for WPANs
  - Covers lower two OSI model layers
    - Physical (PHY)
    - Data link

© Cengage Learning 2014

Existing and Future Standards

- IEEE 802
  - Divides Data link layer into two sublayers:
    - Logical Link Control (LLC)
    - Media Access Control (MAC)
  - Divides PHY layer into two sublayers:
    - Physical Layer Convergence Procedure (PLCP)
    - Physical Medium Dependent (PMD)

© Cengage Learning 2014

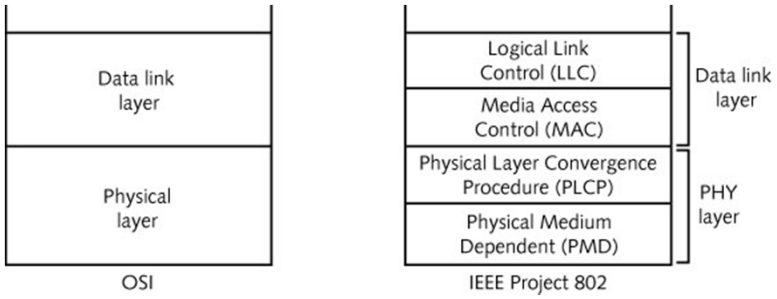

Figure 5-1 OSI model versus IEEE 802

© Cengage Learning 2014

RF WPANs

- Include
  - 802.15.1 and Bluetooth
  - 802.15.4 (ZigBee)

© Cengage Learning 2014

IEEE 802.15.1 and Bluetooth

- Industry specification
  - Bluetooth Special Interest Group (SIG)
- Defines small-form-factor, low-cost wireless radio communications
- IEEE used a portion of the specification as the base material for 802.15.1
  - Ensures interoperability with Wi-Fi using 2.4 GHz frequency band
- 802.15.1 standard
  - Approved in March 2, 2002
  - Compatible with Bluetooth version 1.1 and incorporated into version 1.2

© Cengage Learning 2014

Bluetooth Protocol Stack

- Bluetooth RF layer
  - Defines how the basic hardware that controls the radio transmissions functions
  - Data bits (0 and 1) are converted into radio signals and transmitted
  - Equivalent to OSI Physical layer
- Bluetooth radio module
  - A single radio transmitter/receiver (transceiver)
  - Only hardware required for Bluetooth to function
  - Bluetooth 1.1, 1.2 can transmit at a speed of up to 1 Mbps
  - Bluetooth version 2.1 transmits at 2.1 or 3 Mbps – called **enhanced data rate (EDR)**

© Cengage Learning 2014

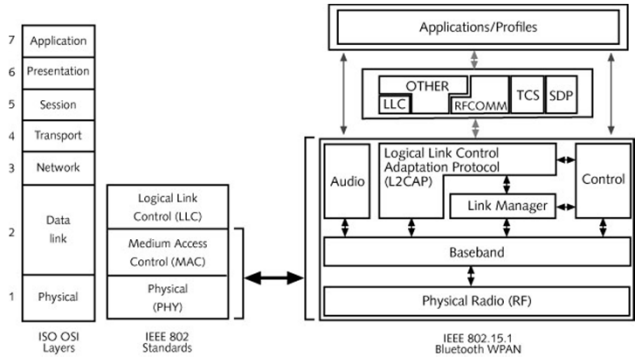

Figure 5-2 Bluetooth protocol stack compared to the OSI protocol model

© Cengage Learning 2014

Bluetooth Protocol Stack

- Bluetooth power classes and ranges
  - Three power classes
  - Determine range between devices
  - Walls and RF interference sources affect the range

Name	Power Level	Distance
Power Class 1	100 mW	330 feet (100 meters)
Power Class 2	2.5 mW	33 feet (10 meters)
Power Class 3	1 mW	3 feet (1 meter)

© Cengage Learning 2014

Table 5-1 Power classes

© Cengage Learning 2014

Bluetooth Protocol Stack

- Modulation techniques
  - Bluetooth 1.x uses a variation of frequency shift keying (FSK)
  - This variation is called **two-level Gaussian frequency shift keying (2-GFSK)**
    - Uses two different frequencies
      - To indicate whether a 1 or a 0 is being transmitted
  - Modulation index
    - Amount that the frequency varies between high and low
    - Between 280 KHz and 350 KHz

© Cengage Learning 2014

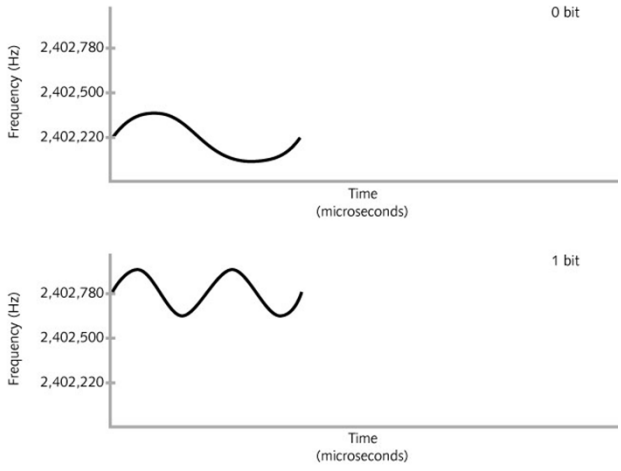

Figure 5-4 Two-level Gaussian frequency shift keying (2-GFSK)

© Cengage Learning 2014

Bluetooth Protocol Stack

- Version 2.x Bluetooth
  - Added two modulations:
    - **Pi/4~DQPSK** (2 Mbps) and **8-DPSK** (3 Mbps)
    - 8-DPSK at 3 Mbps can only be used in ideal conditions
- Version 3.0 Bluetooth
  - Added low power modes
  - 3.0+HS added an **alternate MAC/PHY (AMP)**
  - AMP uses separate radio module for 802.11-like transmissions
- Version 4.0 introduced Bluetooth low energy (BLE)

© Cengage Learning 2014

Bluetooth Protocol Stack

- Bluetooth Baseband layer
  - Lies on top of the RF layer
  - Manages physical channels and links
  - Handles packets, and does paging and inquiry
    - To locate other Bluetooth devices in the area
- Radio frequency
  - 2.4 GHz Industrial, Scientific, and Medical (ISM) band
  - Bluetooth divides frequency into 79 different channels
    - Spaced 1 MHz apart
  - Uses FHSS

© Cengage Learning 2014

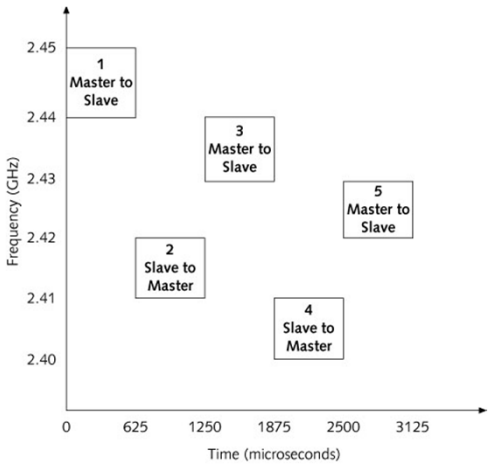

Figure 5-6 Bluetooth FHSS

© Cengage Learning 2014

Bluetooth Protocol Stack

- Radio frequency
  - Bluetooth uses the same frequency as IEEE 802.11b/g/n WLANs
  - Can interfere with 802.11 WLANs and vice versa
  - Bluetooth version 1.2 adds a feature called **adaptive frequency hopping (AFH)**
    - Further improves compatibility with 802.11 WLANs at 2.4 GHz

© Cengage Learning 2014

Bluetooth Protocol Stack

- Network topologies
  - Piconet
    - Bluetooth network that contains one master and at least one slave and that uses the same channel
    - Master and slave devices
    - Master, controls all of the wireless traffic – only 1
    - Slave, takes commands from the master – up to 7
  - Scatternet
    - Two or more linked piconets

© Cengage Learning 2014

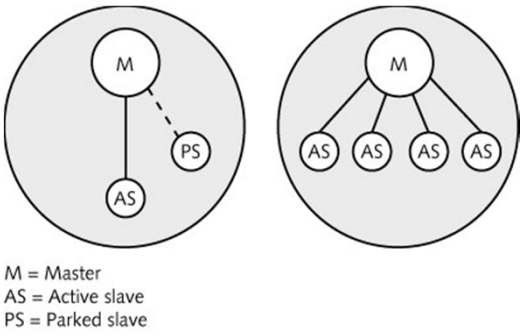

Figure 5-7 Bluetooth piconets

© Cengage Learning 2014

Bluetooth Protocol Stack

- Bluetooth addressing
  - Devices preconfigured with an address
  - Three different types of Bluetooth address

Name	Description
Bluetooth device address	Unique 48-bit number (IEEE 802 hardware or MAC address), which is preconfigured in the hardware
Active member address	3-bit number valid only as long as device is an active slave in a piconet
Parked member address	8-bit number valid only as long as device is a parked slave; a parked device does not retain the 3-bit active member address

© Cengage Learning 2014

Table 5-2 Piconet radio module addresses

 © Cengage Learning 2014

Bluetooth Protocol Stack

- Piconets
  - All devices in a piconet must change frequencies at the same time and in the same sequence
  - Each slave is synchronized with the master's clock
  - Bluetooth connection procedure
    - Called **pairing** – involves two steps
      - **Inquiry procedure**
      - **Paging procedure**
  - Multiple piconets can cover the same area
    - Each can contain up to seven slaves
  - Bluetooth device can be a member of two or more overlapping piconets - a scatternet

 © Cengage Learning 2014

Bluetooth Protocol Stack

- Network topologies
  - Scatternet
    - Group of piconets in which connections exist between different piconets
  - To communicate in each different piconet
    - Device must use the master device address and clock of that specific piconet
  - Bluetooth device can be a slave in several piconets
    - But can be a master in only one piconet
  - A master and slave can switch roles in a piconet

© Cengage Learning 2014

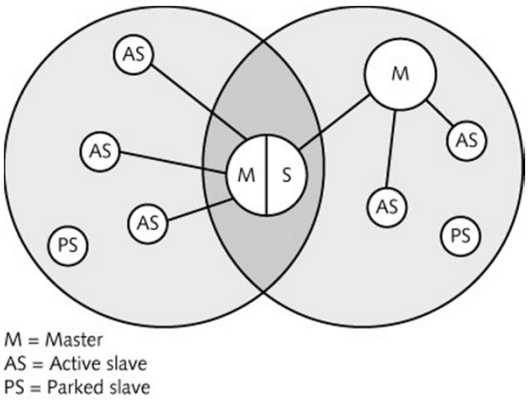

Figure 5-8 Bluetooth scatternet

© Cengage Learning 2014

Bluetooth Protocol Stack

- Bluetooth frames
  - Three parts
    - Access code (72 bits) — timing synchronization, paging, and inquiry
    - Header (54 bits) — packet acknowledgment, packet numbering, the slave address, the type of payload, and error checking
    - Payload (0-2745 bits) — Can contain data, voice, or both

© Cengage Learning 2014

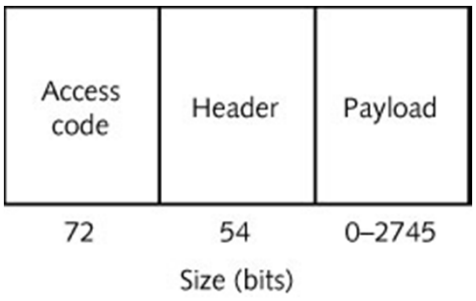

Figure 5-9 Bluetooth PHY frame

© Cengage Learning 2014

Bluetooth Link Manager Layer

- Link Manager layer divided into two functions
  - Piconet management
  - Security
- Managing links between Bluetooth devices
  - **Synchronous connection-oriented (SCO) link**
    - Symmetric point-to-point link between a master and a slave
  - **Asynchronous connectionless (ACL) link**
    - Packet-switched link used for data transmissions

© Cengage Learning 2014

Configuration Options	Maximum Transmission Rate Upstream	Maximum Transmission Rate Downstream
3 simultaneous voice channels (SCO)	64 Kbps × 3 channels	64 Kbps × 3 channels
Symmetric data (SCO)	433.9 Kbps	433.9 Kbps
Asymmetric data (ACL)	723.2 Kbps	57.6 Kbps
Asymmetric data (ACL)	57.6 Kbps	723.2 Kbps

© Cengage Learning 2014

Table 5-3 Supported Bluetooth link configurations

Bluetooth Link Manager Layer

- Error correction
  - 1/3 rate Forward Error Correction (FEC)
  - 2/3 rate FEC
  - Automatic retransmission request (ARQ)

© Cengage Learning 2014

Bluetooth Link Manager Layer

- Bluetooth power usage
  - Once connected to a piconet, a Bluetooth device can be in one of four power modes:
    - Active – actively participates in the channel
    - Sniff – slave listens at a reduced rate
    - Hold – only slave's internal timer is running
    - Park – does not participate in any traffic

© Cengage Learning 2014

Other Layers and Functions

- Logical Link Control Adaptation Protocol (L2CAP)
  - Logical Link Control layer
  - Responsible for segmenting and reassembling data packets
- Radio Frequency Virtual Communications Port Emulation (RFCOMM) data protocol
  - Provides serial port emulation for Bluetooth data
- Link Manager layer
  - Transmits control information

© Cengage Learning 2014

Other Layers and Functions

- Bluetooth profiles
  - Located at the Application layer
  - Determines what functions a device supports
    - AVRCP – remote control
    - A2DP – Bluetooth headset
- Complete list of profiles at http://developer.bluetooth.org/KnowledgeCenter/TechnologyOverview/Pages/Profiles.aspx

© Cengage Learning 2014

IEEE 802.15.4 and ZigBee

- ZigBee standard
  - Provides for the connectivity of simple stationary and mobile devices
    - Low data rates between 20 and 250 Kbps
    - Minimum amount of power
    - Connect at distances of 33 feet (10 meters) to 150 feet (50 meters)
- ZigBee Alliance
  - Formed in 2002

© Cengage Learning 2014

ZigBee Overview

- ZigBee specification
  - Based on the relatively low-level performance requirements of sensors and control systems
- ZigBee devices are designed to remain quiescent for long periods of time – use very little power
- ZigBee transmissions are designed to be short in range
- Spec includes full-mesh networking - some ZigBee devices have the ability to route packets to other devices

© Cengage Learning 2014

ZigBee Overview

- Three basic classes of devices in a ZigBee network
  - Full-function device (FFD)
  - PAN coordinator
  - Reduced-function device (RFD)
- ZigBee protocol stack
  - Based on the OSI seven-layer model
  - Defines only those layers that are relevant to achieving specific functionality

© Cengage Learning 2014

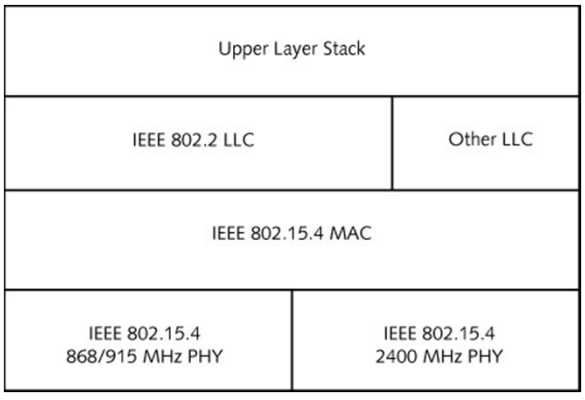

Figure 5-10 ZigBee protocol stack

© Cengage Learning 2014

PHY Layer (MHz)	Frequency Range (MHz)	Chip Rate (kchips/second)	Modulation	Bit Rate (Kbps)
868/915	868–868.6	300	BPSK	20
	902–928	600	BPSK	40
2,450	2,400–2,483.5	2000	O-QPSK	250

© Cengage Learning 2014

Table 5-4 802.15.4 frequency bands and data rates

© Cengage Learning 2014

ZigBee Overview

- ZigBee protocol stack
  - DSSS transmission is used
    - Carrier is modulated with a sequence of 15 chips
    - In both the 868 and 915 MHz bands
  - In the 2.4 GHz band, the technique employs 16 different 32 chip sequences
    - Modulated using offset quadrature phase shift keying (O-QPSK)
      - Uses two carrier waves that are exactly 90 degrees out of phase

© Cengage Learning 2014

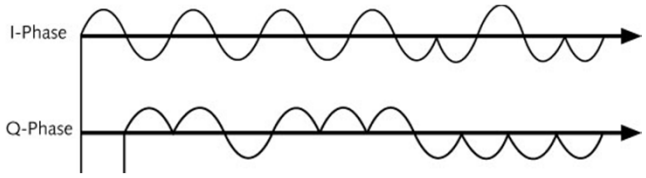

Figure 5-11 Offset quadrature phase shift keying (O-QPSK)

© Cengage Learning 2014

ZigBee Overview

- IEEE 802.15.4 PHY frame format

4 octets	1 octet	7 bits	1 bit	Variable
Preamble	SFD	Frame Length	Reserved	Payload

Figure 5-12 PHY frame format

- 802.15.4 MAC layer
  - Handles all access from the upper layers to the physical radio channel
  - Access to the medium is contention based
    - Uses CSMA/CA

© Cengage Learning 2014

ZigBee Overview

- ZigBee and IEEE Communication Basics
  - Two ways to determine if a channel is clear to transmit:
    - Energy detection
    - Carrier sense
- Beacon-enabled vs. non-beacon communications
  - Contention based – devices use CSMA/CA
  - Contention-free PAN coordinator allocates time slots called guaranteed time slots (GTS)

© Cengage Learning 2014

ZigBee Overview

- Beacon-enabled vs. non-beacon communications
  - In beacon-enabled, PAN coordinator transmits control information to determine which device can transmit
  - Beacon-enabled use a superframe that manages transmission time in a piconet
  - Procedures for associating with and joining a network, routing, and so on, are embedded in the hardware
  - ZigBee devices are engineered to automatically associate with and join the network
  - Device discovery
    - Devices query other devices to identify them
  - Service discovery
    - Identifies the capabilities of specific devices

© Cengage Learning 2014

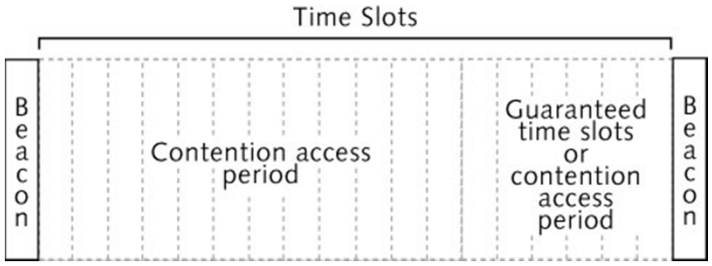

Figure 5-13 802.15.4 superframe

© Cengage Learning 2014

ZigBee Overview

- Coexistence with other standards
  - Relatively wideband interference, such as that generated by IEEE 802.11b networks
    - Appears like white noise to an IEEE 802.15.4 receiver
  - Impact of interference from Bluetooth (802.15.1) devices should be minimal
- Network addressing
  - The ZigBee specification defines several different levels of addresses
    - For identifying devices within a PAN

© Cengage Learning 2014

ZigBee Overview

- Network addressing
  - Levels of addresses
    - IEEE address
    - Network (PAN) address
    - Node address
    - Endpoint address
- ZigBee network topologies
  - Basic topologies
    - Star, tree, and mesh

© Cengage Learning 2014

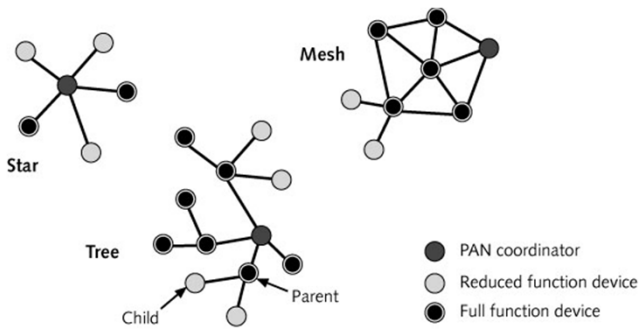

Figure 5-15 Topologies supported bin ZigBee networks

© Cengage Learning 2014

ZigBee Overview

- ZigBee network topologies
  - In both tree and mesh topologies
    - Alternate paths may be available for packets
  - In tree and cluster tree networks
    - Alternate paths are available
      - If another full-function device is within its radio range
  - In a star topology
    - Network is controlled by the PAN coordinator
  - Cluster tree topologies
    - Two or more tree topology networks that are interconnected by full-function devices

© Cengage Learning 2014

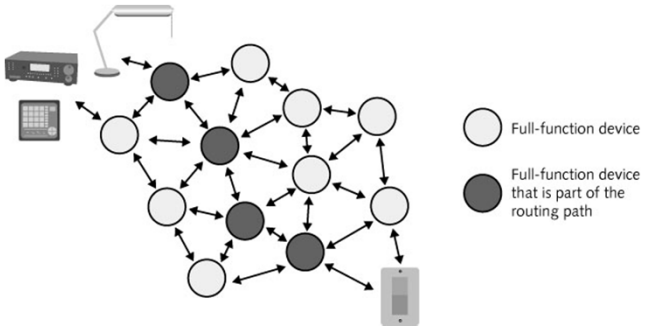

Figure 5-16 Routing of data packets in a ZigBee mesh network

© Cengage Learning 2014

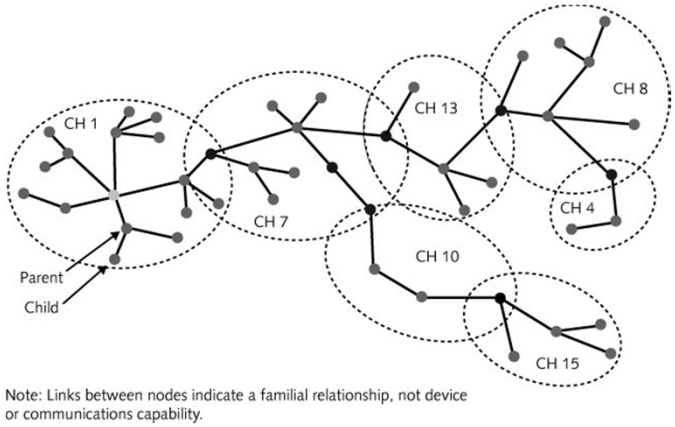

Figure 5-17 ZigBee cluster tree network

© Cengage Learning 2014

ZigBee Overview

- Power management in ZigBee networks
  - Packet routing requires a lot of processing overhead
  - ZigBee devices are designed to be very small
    - Equipped with low-speed, power-efficient CPUs
  - In a ZigBee PAN, only the devices that perform routing or are coordinators incur overhead
  - 802.15.4 standard favors battery-powered devices
    - Does not prevent devices from being connected to another power source
  - ZigBee must maintain certain parameter values
    - In case of a power failure

© Cengage Learning 2014

Other Technologies Using IEEE 802.15.4

- 6LoWPAN
  - Implements IPv6 on WPANs
  - Makes Internet connection easier
  - Supports mesh networking
- Wireless HART
  - Highway Addressable Remote Transducer (HART) protocol designed for industrial-automation
  - Supports a bus topology and point-to-point; allows digital and analog signals over same cable

© Cengage Learning 2014

Low Rate WPAN Security

- Security should be of little concern with WPANs
- One of the most serious concerns is social engineering
- Designing security in WPANs
  - Much more difficult task than in other networking technologies
- Banking and electronic funds transactions use Public key infrastructure (PKI)
  - Unique security code, or key, provided by a certificate authority
- Certificate authority
  - Private company that verifies the authenticity of users

© Cengage Learning 2014

Security in Bluetooth WPANs

- Bluetooth provides security through authentication or encryption
- **Authentication** is based on identifying the device itself
  - Uses a **challenge-response strategy**
- **Encryption** is the process of scrambling data using math algorithms
  - And ensures that the transmissions cannot be easily intercepted and decoded

© Cengage Learning 2014

Security in Bluetooth WPANs

- Bluetooth encryption modes
  - Encryption Mode 1 — Nothing is encrypted
  - Encryption Mode 2 — Traffic from the master to one slave is encrypted
    - But traffic from the master to multiple slaves is not encrypted
  - Encryption Mode 3 — All traffic is encrypted
- Levels of Bluetooth security
  - Level 1 — No security
  - Level 2 — Service-level security
  - Level 3 — Link-level security

© Cengage Learning 2014

Security in ZigBee and IEEE 802.15.4 WPANs

- ZigBee WPANs use symmetric keys for authentication and encryption
- IEEE 802.15.4 standard provides in addition:
  - Frame integrity, access control, and sequential freshness security services
- Frame integrity uses a message integrity code (MIC)
- Access control is based on **access control list (ACL)**
- Sequential freshness
  - Security service used by the receiving device
  - Ensures that the same frames will not be transmitted more than once

© Cengage Learning 2014

Security in ZigBee and IEEE 802.15.4 WPANs

- Security modes in the 802.15.4 standard
  - Unsecured mode
  - ACL mode (which uses access control)
  - Secured mode (which uses full authentication and encryption)

© Cengage Learning 2014

Summary

- Network protocol is the set of rules for messages exchanged between communication devices
- Bluetooth is a wireless technology that uses short-range radio frequency (RF) transmissions
  - Supported by over 2,500 hardware and software vendors
- Bluetooth stack divided into lower and upper levels
  - Lower levels are hardware

© Cengage Learning 2014

Summary

- Up to Bluetooth 1.2 uses two-level Gaussian frequency shift keying (2-GFSK) modulation
- Version 2 added modulation method to allow 2 and 3 Mbps transmission speeds; uses FHSS
- Error correction schemes used in Bluetooth
  - 1/3 rate Forward Error Correction (FEC), 2/3 rate FEC, and the automatic retransmission request (ARQ)
- ZigBee is a specification for low rate WPANs created by the ZigBee alliance
  - Includes full mesh networking capability
- ZigBee network topologies: star, tree, and mesh

© Cengage Learning 2014

Summary

- IEEE 802.15.4 standard frequency bands: 868 MHz,915 MHz, and the 2.4 GHz-ISM band
- 802.15.4 is designed to coexist easily with other WPAN and WLAN technologies
- Security in Bluetooth supports only device authentication and limited encryption
- ZigBee supports message integrity at the MAC layer
  - Can also check for the freshness of the message

© Cengage Learning 2014