IEEE 802.15.4
Low Rate Wireless Personal Area Networks (LR-WPAN)

New Trend of wireless technology

- Most Wireless industry focuses on increasing high data throughput
- A set of applications require simple wireless connectivity, relaxed throughput, very low power, short distance and inexpensive hardware:
  - Industrial
  - Agricultural
  - Vehicular
  - Residential
  - Medical

Table 1.2 ISM bands defines by ITU-R

Frequency range		Bandwidth	Center frequency	Availability
00.000 kHz	150 kHz	150 kHz	75 kHz	Region 1 low power, narrow band
6.765 MHz	6.795 MHz	30 kHz	6.780 MHz	Subject to local acceptance
13.553 MHz	13.567 MHz	14 kHz	13.560 MHz	Radio-frequency identification
26.957 MHz	27.283 MHz	326 kHz	27.120 MHz	Citizen Band (CB) radio models
40.660 MHz	40.700 MHz	40 kHz	40.680 MHz	Radio models
433.050 MHz	434.790 MHz	1.74 MHz	433.920 MHz	Region 1 and subject to local acceptance
866.00? MHz	868.000 MHz	2 MHz	867.000 MHz	Region 1. Very narrow band, few channels.
902.000 MHz	928.000 MHz	26 MHz	915.000 MHz	Region 2 only (with some exceptions)
2.400 GHz	2.4835 GHz	83.5 MHz	2.441 GHz	Region 1, Region 2, Region 3
5.725 GHz	5.875 GHz	150 MHz	5.800 GHz	Region 3 has extended the upper range, additional ~ 150 MHz.
24.000 GHz	24.250 GHz	250 MHz	24.125 GHz	
61.000 GHz	61.500 GHz	500 MHz	61.250 GHz	Subject to local acceptance
122.000 GHz	123.000 GHz	1 GHz	122.500 GHz	Subject to local acceptance
244.000 GHz	246.000 GHz	2 GHz	245.000 GHz	Subject to local acceptance

- Region 1 comprises Europe, Africa, the Middle East west of the Arabian Gulf including Iraq, the former Soviet Union and Mongolia
- Region 2 covers the Americas, Greenland and some of the Eastern Pacific Islands
- Region 3 contains most of non-former-Soviet-Union Asia, east of and including Iran, and most of Oceania

IEEE 802 Project:

IEEE 802 Local and Metropolitan Area Networks Standard Committee (LMSC)					
IEEE 802.2 Logical Link Control (LLC)	IEEE 802.3 (Ethernet)	IEEE 802.11 Wireless LANs (WLANs)	IEEE 802.15 Wireless PANs (WPANs)	IEEE 802.16 Broadband wireless access	IEEE 802.20 Mobile broadband wireless access

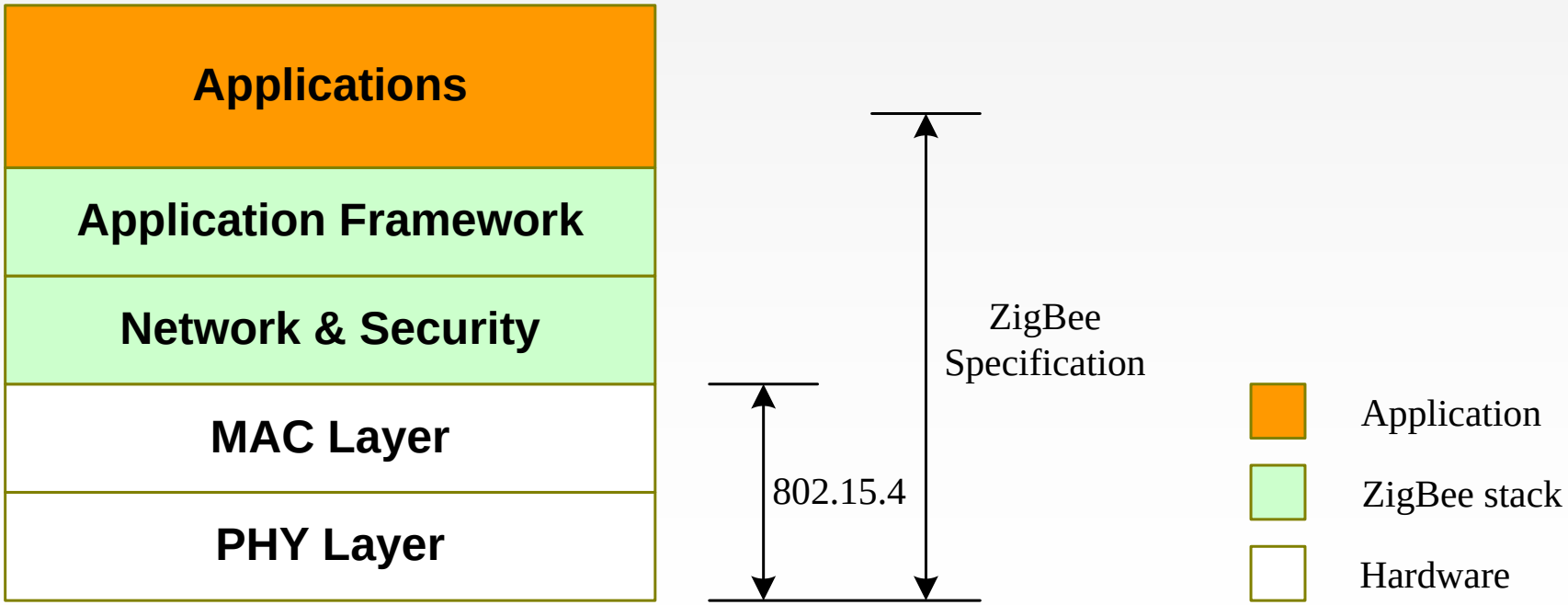
IEEE 802.15.1 (WPAN/Bluetooth)	IEEE 802.15.2 (Coexistence)	IEEE 802.15.3 (High rate WPANs)	IEEE 802.15.4 (Low rate WPANs)	IEEE 802.15.5 (Mesh networking)	IEEE 802.15.6 (BANs)	IEEE 802.15.7 Visible Light Communication (VLC)

Comparison between WPAN

Project	Data Rate	Range	Configuration	Other Features
802.15.1 (Bluetooth)	1 Mbps	10M (class 3) 100M (class 1)	8 active device Piconet/ Scatternet	Authentication, Encryption, Voice
802.15.3 High Rate	22, 33, 44, 55 Mbps	10M	256 active device Piconet/ Scatternet	FCC part 15.249 QoS, Fast Join Multi-Media
802.15.4 Low Rate	up to 250Kbps	10M nominal 1M-100M based on settings	Master/Slave (256 Devices or more) Peer to Peer	Battery Life: multi-month to infinite
802.15.2 Coexistence	Develop a Coexistence Model and Mechanisms Document as a Recommended Practice			

802.15.4 Architecture

- IEEE 802.15.4 Working Group
  - Defining lower layers of protocol stack: MAC and PHY



General characteristics

- Simple lightweight protocol for WPAN
- Data rates upto 250 kbps
- Star or Peer-to-Peer operation
- Support for low latency devices
- CSMA/CA channel access (optionally Slotted CSMA/CA)
- Fully handshaked protocol for transfer reliability
- Low power consumption
- Channels:
  - 16 channels in the 2.4 GHz ISM band,
  - 10 channels in the 915 MHz ISM band
  - 1 channel in the European 868 MHz band.
- Extremely low duty-cycle (<0.1%)

IEEE 802.15.4 Device Types

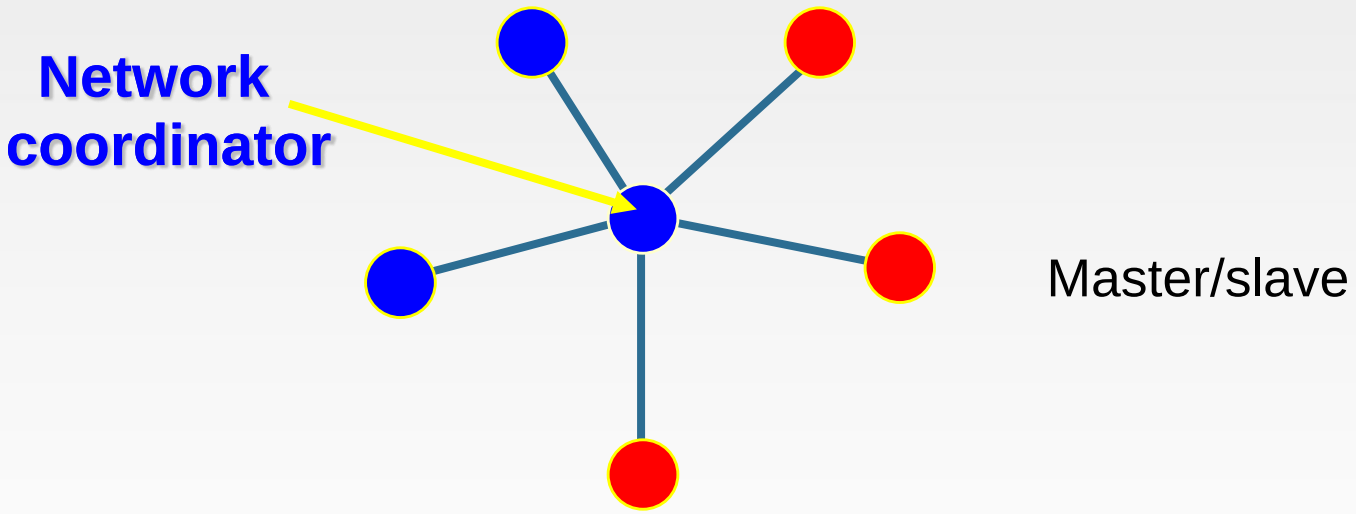
- There are two different device types :
  - A full function device (FFD)
  - A reduced function device (RFD)
- The FFD can operate in three modes by serving as
  - Device
  - Coordinator
  - PAN coordinator
- The RFD can only serve as:
  - Device

FFD vs RFD

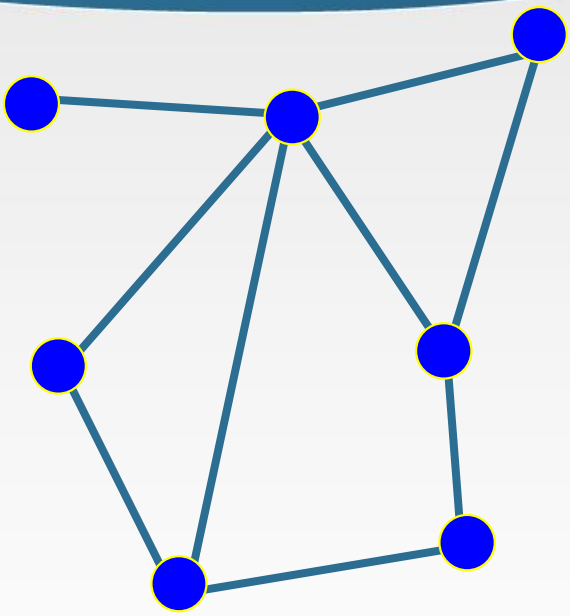
- Full function device (FFD)
  - Any topology
  - Network coordinator capable
  - Talks to any other device

- Reduced function device (RFD)
  - Limited to star topology
  - Cannot become a network coordinator
  - Talks only to a network coordinator
  - Very simple implementation

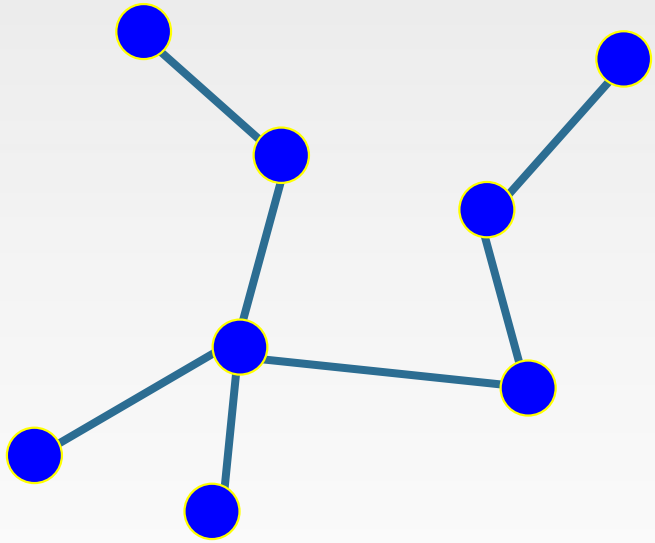
Star topology



Peer to peer topology



Point to point



Tree

Full Function Device (FFD)

Communications Flow

IEEE 802.15.4 PHY

IEEE 802.15.4 PHY overview

- PHY functionalities:
  - Activation and deactivation of the radio transceiver
  - Energy detection within the current channel
  - Link quality indication for received packets
  - Clear channel assessment for CSMA/CA
  - Channel frequency selection
  - Data transmission and reception

IEEE 802.15.4 Characteristics

Table 1.3 IEEE 802.15.4 High level characteristics

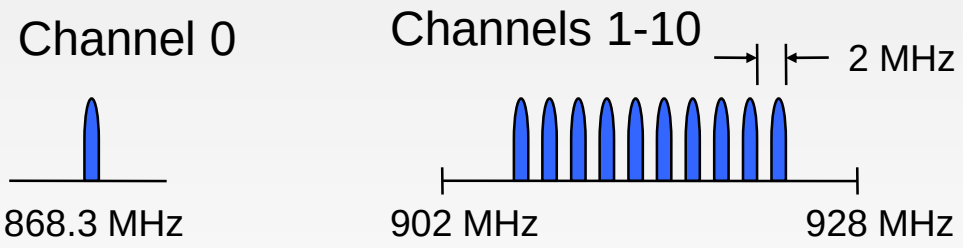
Frequency Band	Two PHYs	Low-Band (BPSK)	868 MHz	1 channel—20 Kbps
			915 MHz	10 channels—40 Kbps
		High-Band (O-QPSK)	2.4 GHz	16 channels—250 Kbps
Channel Access	CSMA/CA and slotted CSMA/CA			
Range	10 to 20 m			
Latency	15 ms			
Addressing	Short 8 bit or 64-bit IEEE			

Acronyms
BPSK (Binary phase shift keying), CSMA/CA (Carrier sense multiple access with collision avoidance), O-QPSK (Offset quadrature phase shift keying)

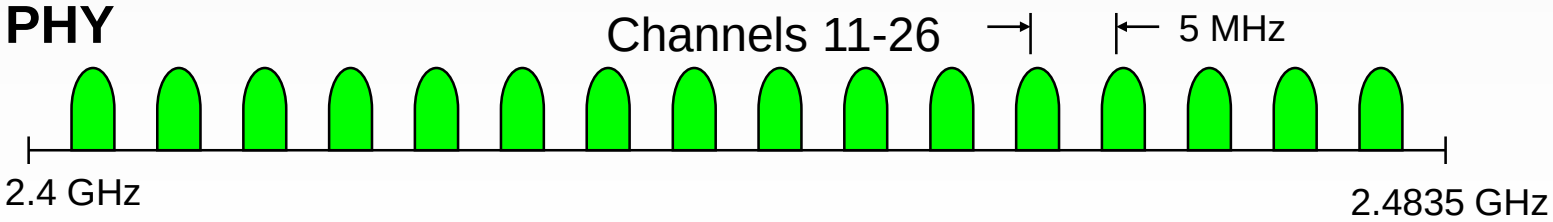
IEEE 802.15.4 PHY Overview

- Operating frequency bands

868MHz/ 915MHz PHY



2.4 GHz PHY

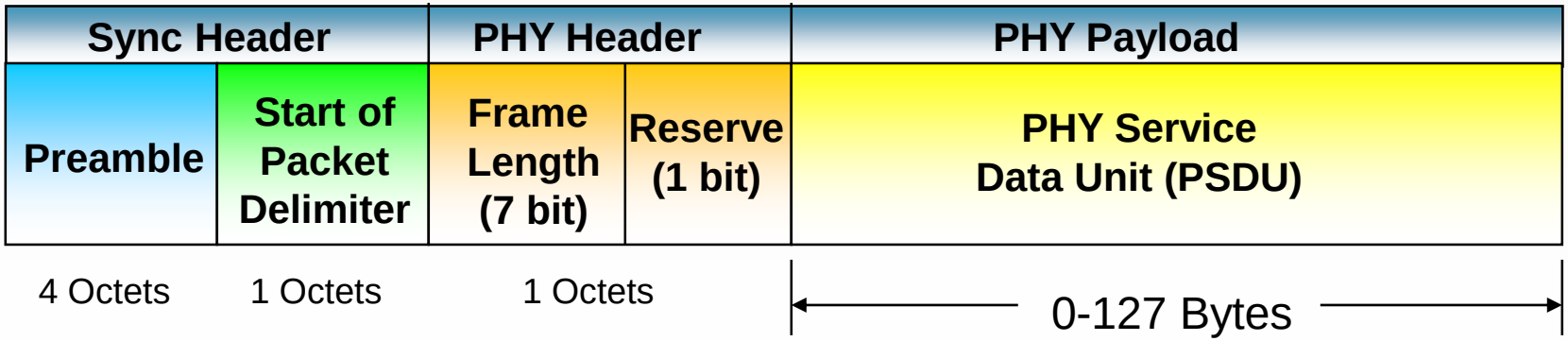


Frequency Bands and Data Rates

- The standard specifies two PHYs :
  - 868 MHz/915 MHz DSSS PHY (11 channels)
    - 1 channel (20Kb/s) in European 868 MHz band
    - 10 channels (40Kb/s) in 915 (902-928) MHz ISM band
  - 2.450 GHz DSSS PHY (16 channels)
    - 16 channels (250Kb/s) in 2.4GHz band

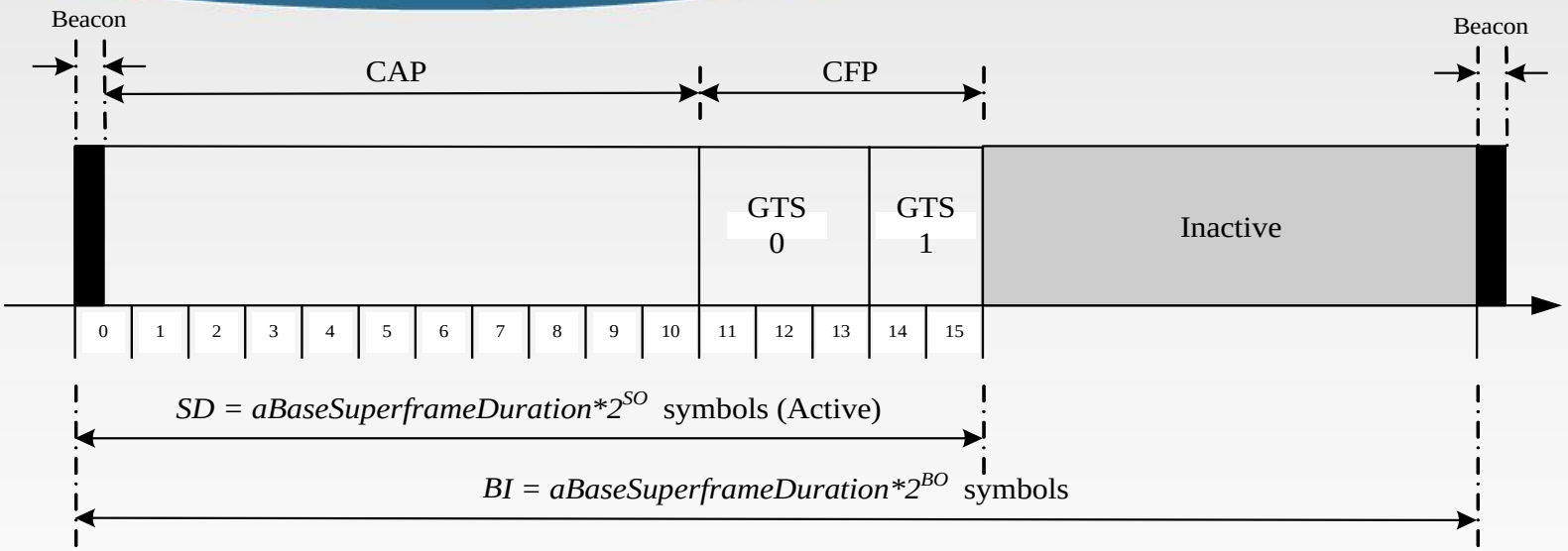
PHY Frame Structure

- PHY Frame Fields
  - Preamble (32 bits) – synchronization
  - Start of packet delimiter (8 bits) – shall be formatted as “11100101”
  - PHY header (8 bits) – PSDU length
  - PSDU (0 to 127 bytes) – data field



IEEE 802.15.4 MAC

Superframe



- A superframe is divided into two parts
  - Inactive: all station sleep
  - Active:
    - Active period will be divided into 16 slots
    - 16 slots can further divided into two parts
      - Contention access period
      - Contention free period

Superframe

- Beacons are used for
  - starting superframes
  - synchronizing with other devices
  - announcing the existence of a PAN
  - informing pending data in coordinators
- In a “beacon-enabled” network,
  - Devices use the slotted CAMA/CA mechanism to contend for the usage of channels
  - FFDs which require fixed rates of transmissions can ask for *guarantee time slots (GTS)* from the coordinator

Channel Access Mechanism

- Two type channel access mechanism:
  - beacon-enabled networks → slotted CSMA/CA channel access mechanism
  - non-beacon-enabled networks → unslotted CSMA/CA channel access mechanism

ZigBee

ZigBee:

- Technological standard designed for control and sensor networks
- Defines higher layer communication protocols built on the IEEE 802.15.4
- Name from the way bees zig and zag while tracking between flowers and relaying information to other bees
- Created by the ZigBee Alliance

ZigBee Alliance:

- An organization with a mission to define reliable, cost effective, low-power, wirelessly networked, monitoring and control products based on an open global standard
- Alliance provides interoperability, certification testing, and branding

ZigBee Promoters:

Important Characteristics

- Low cost
- Low power consumption
- Low data rate
- Relatively short transmission range
- Scalability
- Reliability
- Flexible protocol design suitable for many applications

ZigBee Applications

ZigBee

Wireless Control that Simply Works

BUILDING AUTOMATION

security
HVAC
AMR
lighting control
access control

CONSUMER ELECTRONICS

TV
VCR
DVD/CD
remote

PERSONAL HEALTH CARE

patient monitoring
fitness monitoring

PC & PERIPHERALS

mouse
keyboard
joystick

TELECOM SERVICES

m-commerce
info services
object interaction
(Internet of Things)

INDUSTRIAL CONTROL

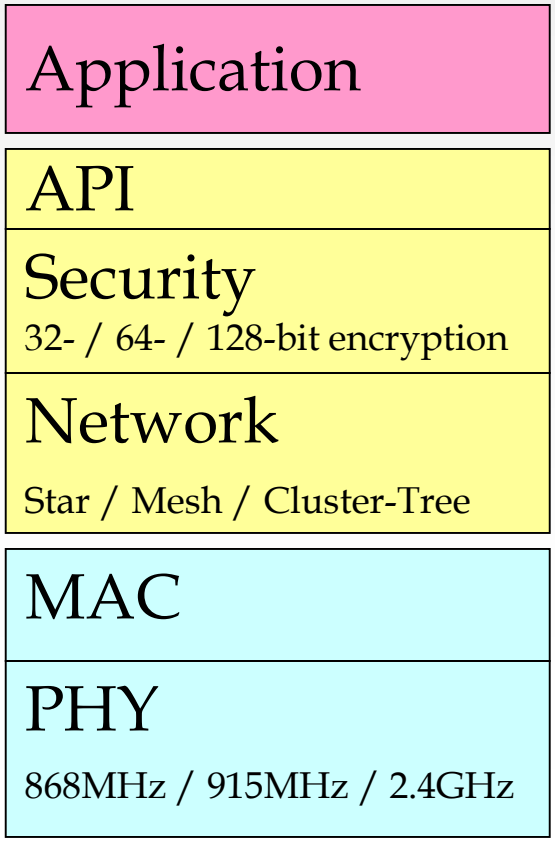
asset mgt
process control
environmental
energy mgt

HOME CONTROL

security
HVAC
lighting control
access control
irrigation

ZigBee/802.15.4 Architecture:

- IEEE 802.15.4 Working Group
  - Defining lower layers of protocol stack: MAC and PHY



Customer

ZigBee Alliance

IEEE 802.15.4

ZigBee Alliance
-"the software"
-Network, Security & Application layers
-Brand management

IEEE 802.15.4
-"the hardware"
-Physical & Media Access Control layers

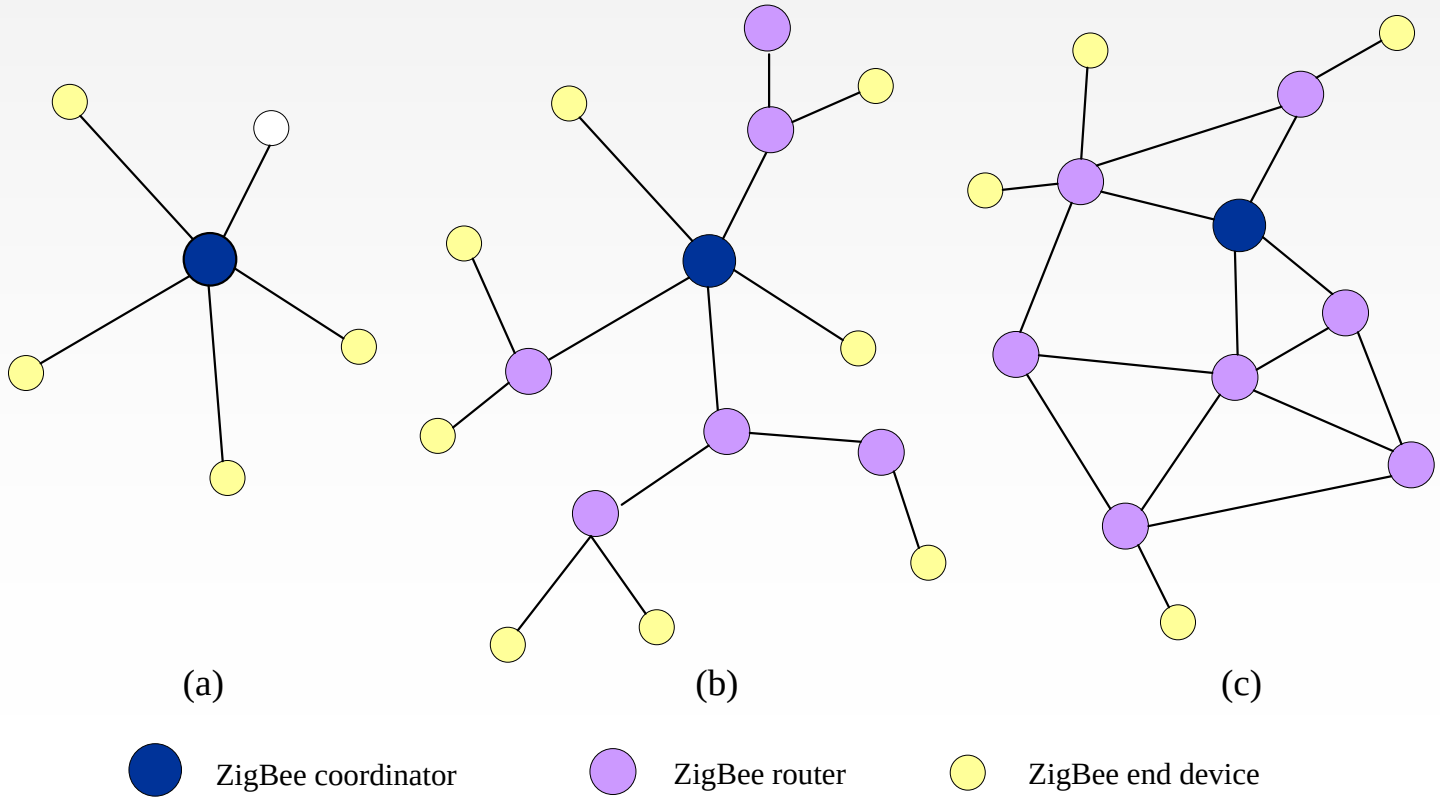
How is ZigBee related to IEEE 802.15.4?

- Takes full advantage of a powerful physical radio specified by IEEE 802.15.4
- Adds logical network, security and application software
- ZigBee Alliance continues to work closely with the IEEE to ensure an integrated and complete solution for the market

ZigBee Network Layer Overview:

- Three kinds of networks supported:

  Star, Tree, and Mesh



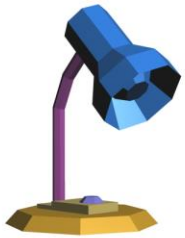
ZigBee Network Layer Overview:

- Three kinds of devices in the network layer
  - ZigBee Coordinator (FFD Device): responsible for initializing, maintaining, and controlling the network
  - ZigBee Router (FFD Device) : form the network backbone
  - ZigBee End Device (RFD Device): must be connected to router/coordinator
- In a tree network, the coordinator and routers can announce beacons.
- In a mesh network, there is no regular beacon.
  - Devices in a mesh network can only communicate with each other in a peer-to-peer manner

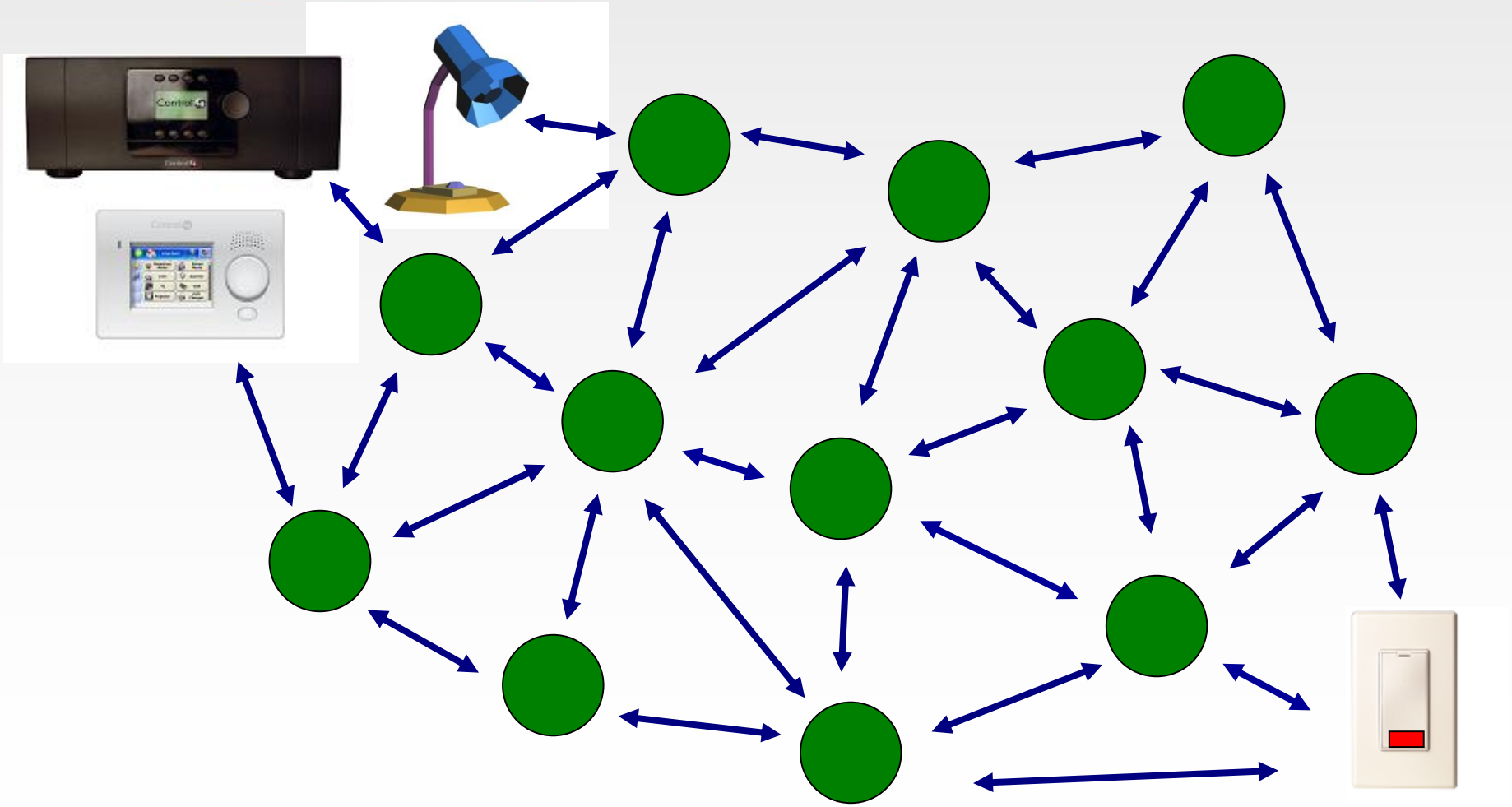
Summary of ZigBee Network Layer:

	Pros	Cons
Star	1. Easy to synchronize 2. Support low power operation 3. Low latency	1. Small scale
Tree	1. Low routing cost 2. Can form superframes to support sleep mode 3. Allow multihop communication	1. Route reconstruction is costly 2. Latency may be quite long
Mesh	1. Robust multihop communication 2. Network is more flexible 3. Lower latency	1. Cannot form superframes (and thus cannot support sleep mode) 2. Route discovery is costly 3. Needs storage for routing table

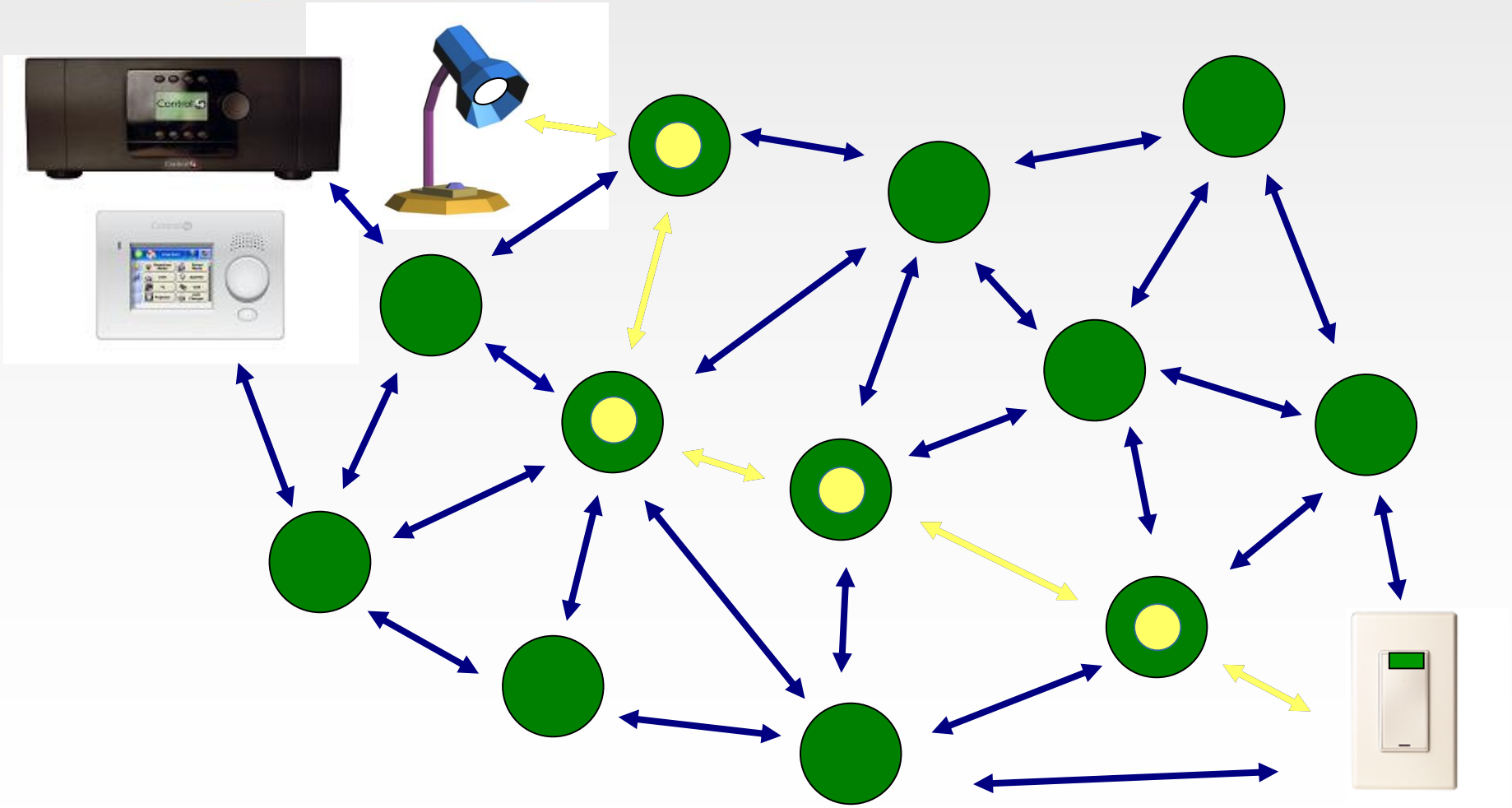
ZigBee Mesh Networking



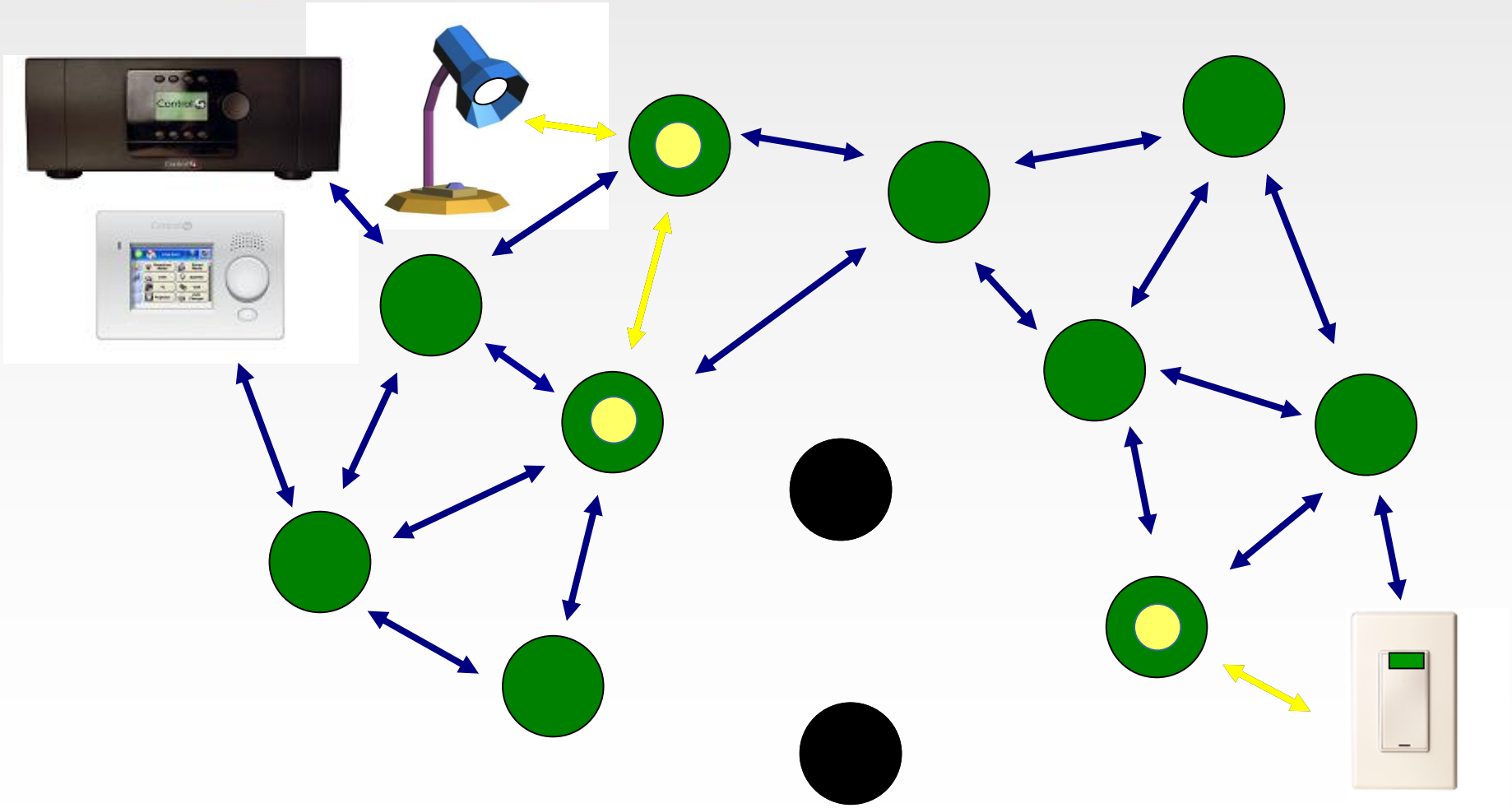
ZigBee Mesh Networking



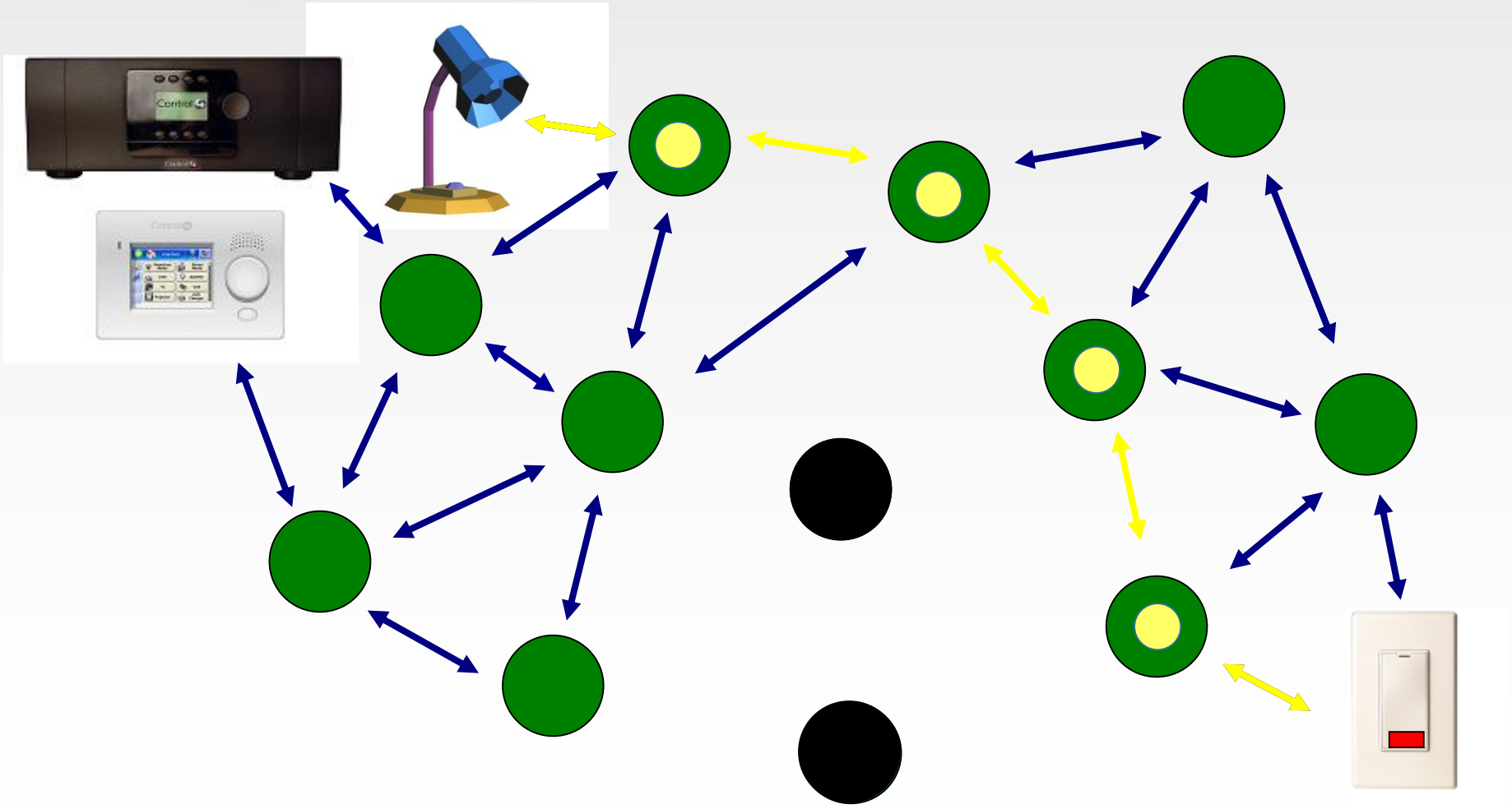
ZigBee Mesh Networking



ZigBee Mesh Networking



ZigBee Mesh Networking

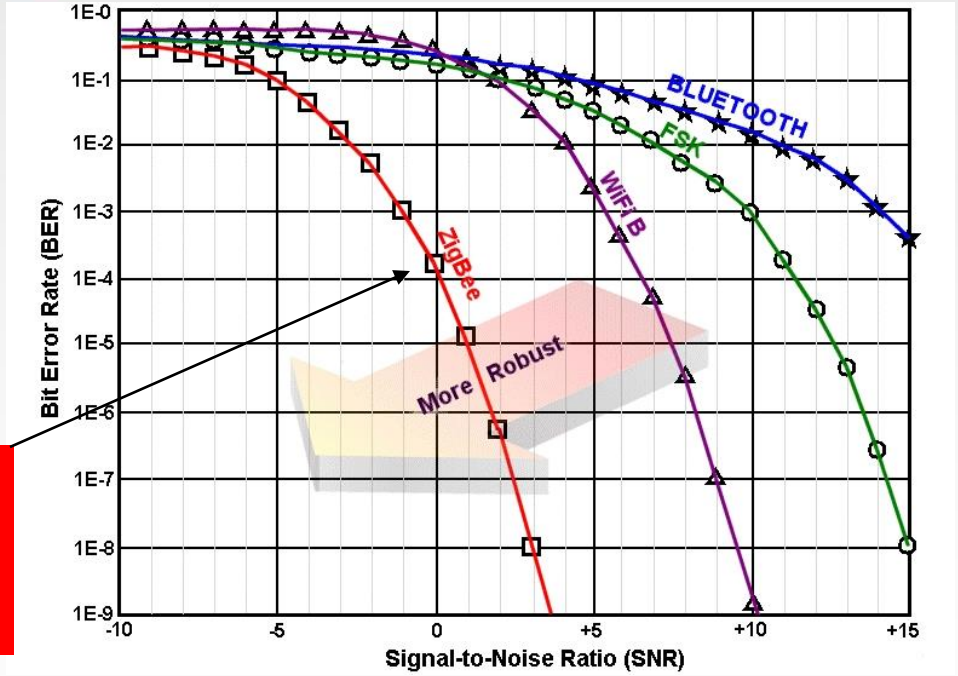


Security

- Encryption specified for MAC, Network and Application Support Sub-Layer (APS)
- Encryption/Authentication mode CCM (CTR +CBC-MAC)
  - CTR is a counter based encryption mode
  - CBC-MAC: Cipher Block Chaining Message Authentication Code provides data integrity
- All security is based on 128 bit key and AES-128 block encryption method

Basic Radio Characteristics

ZigBee technology relies upon IEEE 802.15.4, which has excellent performance in low SNR environments



Frequency Band	License Required?	Geographic Region	Data Rate	Channel Number(s)
868.3 MHz	No	Europe	20kbps	0
902-928 MHz	No	Americas	40kbps	1-10
2405-2480 MHz	No	Worldwide	250kbps	11-26

Comparison with Other Technologies:

Table 1.5 ZigBee compared with wireless standards

	Bluetooth	UWB	ZigBee	Wi-Fi
IEEE specification	802.15.1	802.15.3a* (Kim et al. 2008)	802.15.4	802.11a/b/g
ISM frequency band	2.4 GHz	3.1–10.6 GHz	868/915 MHz, 2.4 GHz	2.4 GHz, 5 GHz
Application	Wireless connectivity between devices such as phones, PDA, laptops, headsets	Real-time video and music, multimedia wireless network, WPAN	Industrial control and monitoring, sensor networks, building automation, home control and automation, toys, games	Wireless LAN connectivity, broadband Internet access
Max signal rate	1 Mbps	110 Mbps	250 Kbps	54 Mbps
Nominal range	10 m	10 m	10–100 m	100 m
Transmission power	0–10 dBm	−41.3 dBm/MHz	(−25)–0 dBm	15−20 dBm

Comparison with Other Technologies:

	Bluetooth	UWB	ZigBee	Wi-Fi
Channel bandwidth	1 Mbps	500–7.5 GHz	0.3/0.6; 2 MHz	22 MHz
Modulation type	GFSK	BPSK, QPSK	BPSK (+ASK), O-QPSK	BPSK, QPSK COFDM, CCK, M-QAM
Basic cell	Piconet	Piconet	Star	BSS
Extension of the basic cell	Scatternet	Peer-to-peer	Cluster tree, Mesh	ESS
Max number of cell nodes	8 active devices, 255 in park mode	8	>65,000	Unlimited in ad hoc networks (IBSS), up to 2007 devices in infrastructure networks
Encryption	E0 stream cipher	AES block cipher (CTR, counter mode)	AES block cipher (CTR, counter mode)	RC4 stream cipher (WEP), AES block cipher
Authentication	Shared secret	CBC-MAC (CCM)	CBC-MAC (ext. of CCM)	WPA2 (802.11i)
Data protection	16-bit CRC	32-bit CRC	16-bit CRC	32-bit CRC

Comparison with Other Technologies:

	Bluetooth	UWB	ZigBee	Wi-Fi
Properties	Cost, easy setup, low interference, device connection requires up to 10 s	Low power, high throughput, low interference, wall penetration	Reliability, very low power, low cost, security, devices can join an existing network in under 30 ms	Speed, flexibility, device connection requires 3–5 s

Acronyms

AES (advanced encryption standard), ASK (amplitude shift keying), BPSK/QPSK (binary/quadrature phase SK), BSS/IBSS/ESS (basic/independent basic/extended service set), CBC-MAC (cipher block chaining message authentication code), CCK (complementary code keying), CCM (CTR with CBC-MAC), COFDM (coded OFDM), CRC (cyclic redundancy check), FHSS/DSSS (frequency hopping/direct sequence spread spectrum), GFSK (Gaussian frequency SK), M-QAM (M-ary quadrature amplitude modulation), MB-OFDM (multiband OFDM), O-QPSK (offset-QPSK), OFDM (orthogonal frequency division multiplexing), WEP (wired equivalent privacy), WPA (Wi-Fi protected access)