EEEN3008J: Advance wireless communications

Bluetooth and IEEE 802.15

Dr Avishek Nag

(avishek.nag@ucd.ie)

IEEE 802.15

- Wireless Personal Area Networks
  - –Short-range communication
  - –Low-cost, low-energy to provide long battery life
- Several standards have been provided
- We focus on 802.15 technologies
  - –Other viable WPAN alternatives exist

IEEE 802.15.1	Bluetooth certification	active
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	
IEEE 802.15.3	High-Rate wireless PAN (e.g., UWB, etc.)	
IEEE 802.15.4	Low-Rate wireless PAN (e.g., ZigBee, WirelessHART, MiWi, etc.)	active
IEEE 802.15.5	Mesh networking for WPAN	
IEEE 802.15.6	Body area network	active

Source: wikipedia

Internet of Things

- Key application area for short-range communications
- Internet of things
  - Large numbers of wirelessly connected objects
  - Interactions between the physical world and computing, digital content, analysis, and services.
  - Useful for health and fitness, healthcare, home monitoring and automation, energy savings, farming, environmental monitoring, security, surveillance, education, and many others.
- Machine-to-machine communications (M2M), also machine-type communications (MTC)
  - Devices working together for automated control

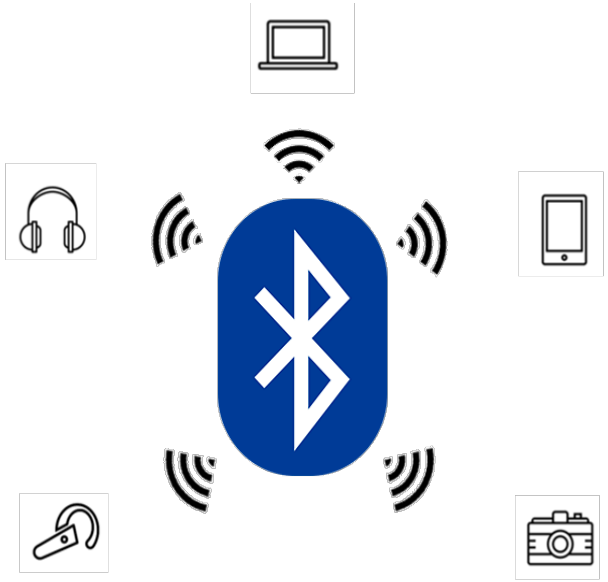
Bluetooth

- Universal short-range wireless capability
- Uses 2.4-GHz band
- Available globally for unlicensed users
- Devices within 10 m can share up to 2.1 Mbps or 24 Mbps of capacity
- Supports open-ended list of applications
  - Data, audio, graphics, video
- Started as IEEE 802.15.1
  - New standards come from the Bluetooth Special Interest Group (Bluetooth SIG) Industry consortium
  - Bluetooth 2.0, 2.1, 3.0, and 4.0

Bluetooth application areas

- Data and voice access points
  - Real-time voice and data transmissions
- Cable replacement
  - Eliminates need for numerous cable attachments for connection
- Ad hoc networking
  - Device with Bluetooth radio can establish connection with another when in range

Top use of Bluetooth



- Mobile handsets
- Voice handsets
- Stereo headsets and speakers
- PCs and tablets
- Human interface devices, such as mice and keyboards
- Wireless controllers for video game consoles
- Cars
- Machine-to-machine applications: credit-card readers, industrial automation, etc.

Bluetooth Standards Documents

- Core specifications
  - Details of various layers of Bluetooth protocol architecture
- Profile specifications
  - Use of Bluetooth technology to support various applications
- We first focus on
  - 2.1 Basic/Enhanced Data Rate (BR/EDR)
- Later standards
  - 3.0 Alternative MAC/PHY (AMP)
  - 4.0 Bluetooth Smart (Bluetooth Low Energy)

Protocol Architecture

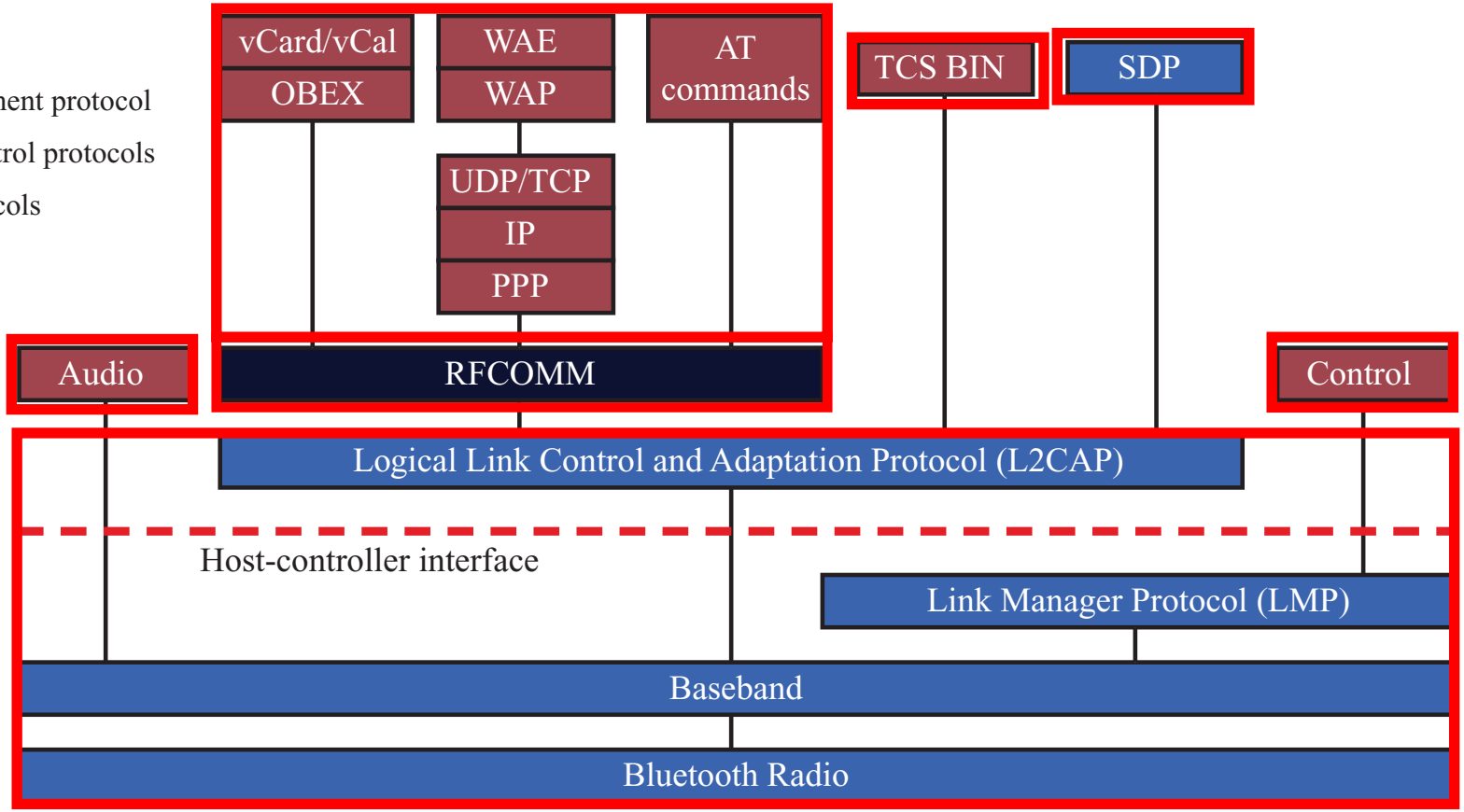
- Bluetooth is a layered protocol architecture
  - Core protocols
  - Cable replacement and telephony control protocols
  - Adopted protocols
- Core protocols
  - Radio
  - Baseband
  - Link manager protocol (LMP)
  - Logical link control and adaptation protocol (L2CAP)
  - Service discovery protocol (SDP)

Protocol architecture II

- Cable replacement protocol
  - RFCOMM
- Telephony control protocol
  - Telephony control specification – binary (TCS BIN)
- Adopted protocols
  - PPP
  - TCP/UDP/IP
  - OBEX
  - WAE/WAP

Bluetooth Protocol Stack

= Core protocols
= Cable replacement protocol
= Telephony control protocols
= Adopted protocols



AT	= Attention sequence (modem prefix)	TCS BIN	= Telephony control specification - binary
IP	= Internet Protocol	UDP	= User Datagram Protocol
OBEX	= Object exchange protocol	vCal	= Virtual calendar
PPP	= Point-to-Point Protocol	vCard	= Virtual card
RFCOMM	= Radio frequency communications	WAE	= Wireless application environment
SDP	= Service discovery protocol	WAP	= Wireless application protocol
TCP	= Transmission control protocol		

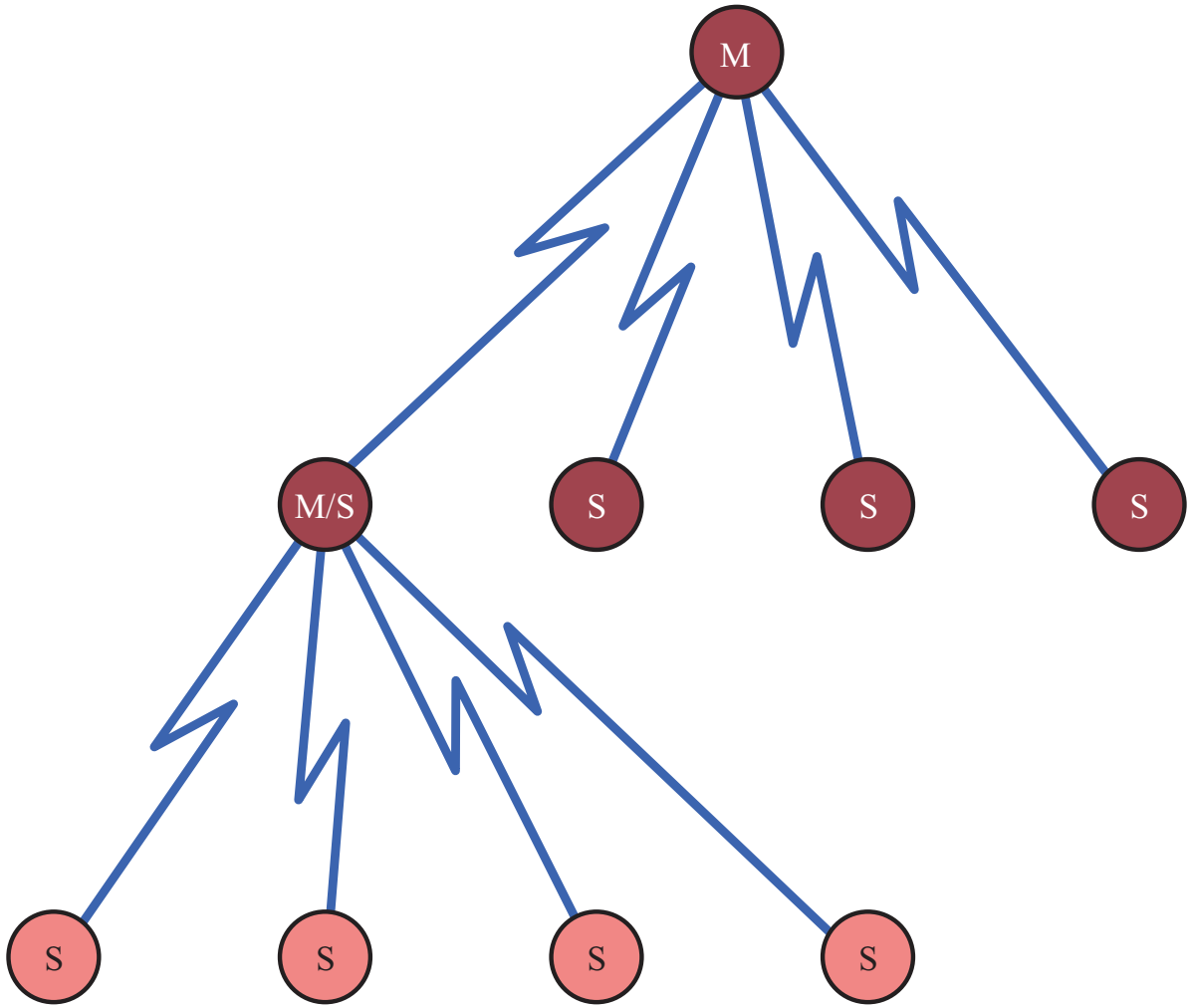
Profiles

- Over 40 different profiles are defined in Bluetooth documents
  - Only subsets of Bluetooth protocols are required
  - Reduces costs of specialized devices
- All Bluetooth nodes support the Generic Access Profile
- Profiles may depend on other profiles
  - Example: File Transfer Profile
    - Transfer of directories, files, documents, images, and streaming media formats
    - Depends on the Generic Object File Exchange, Serial Port, and Generic Access Profiles.
    - Interfaces with L2CAP and RFCOMM protocols

Piconets and Scatternets

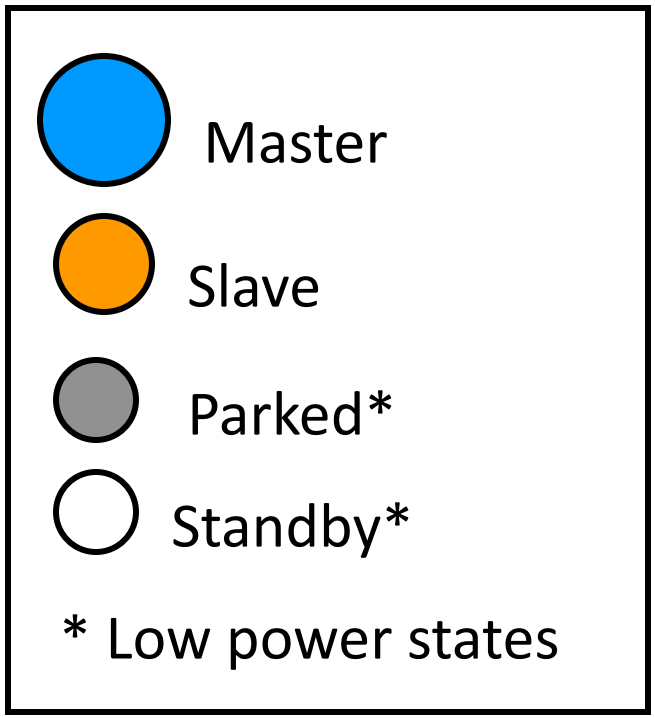
- Piconet
  - Basic unit of Bluetooth networking
  - Master and one to seven slave devices
  - Master determines channel and phase
- Scatternet
  - Device in one piconet may exist as master or slave in another piconet
  - Allows many devices to share same area
  - Makes efficient use of bandwidth

Master/Slave relationships

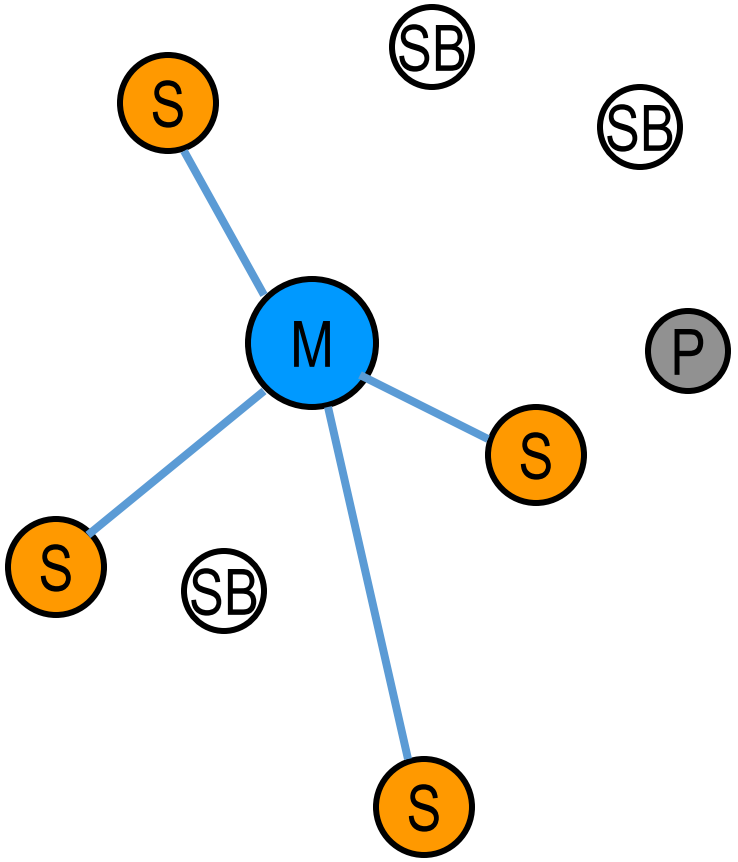


Piconet: Operational States

Operational states

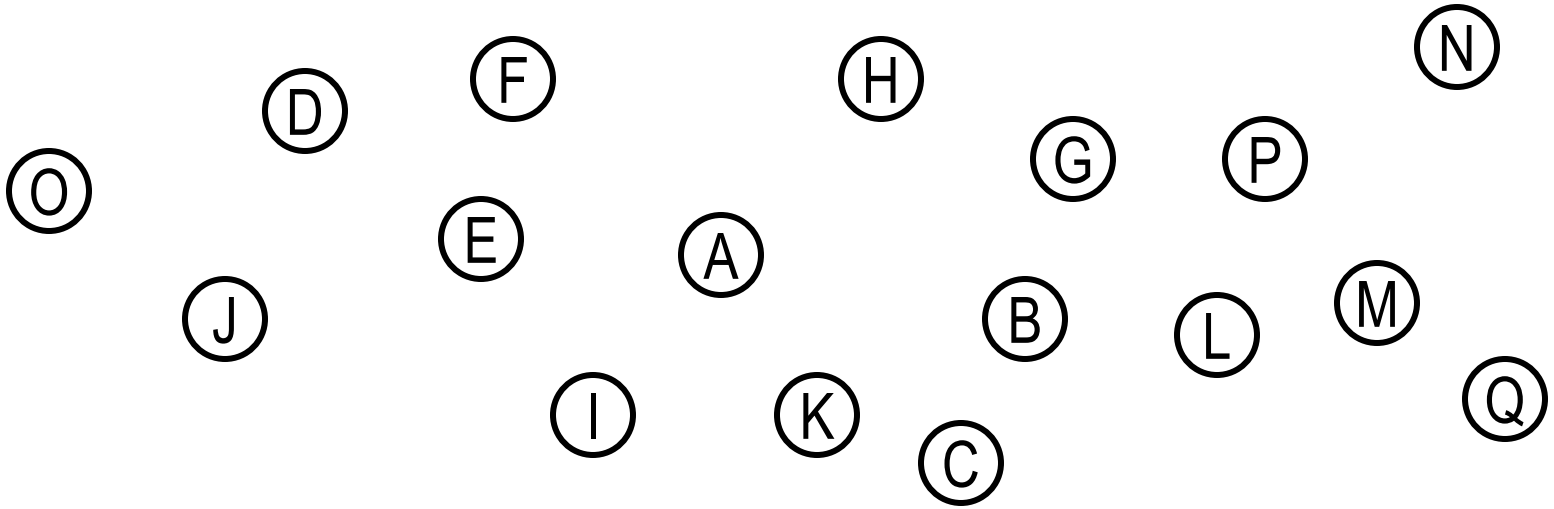


A piconet



Forming a Piconet

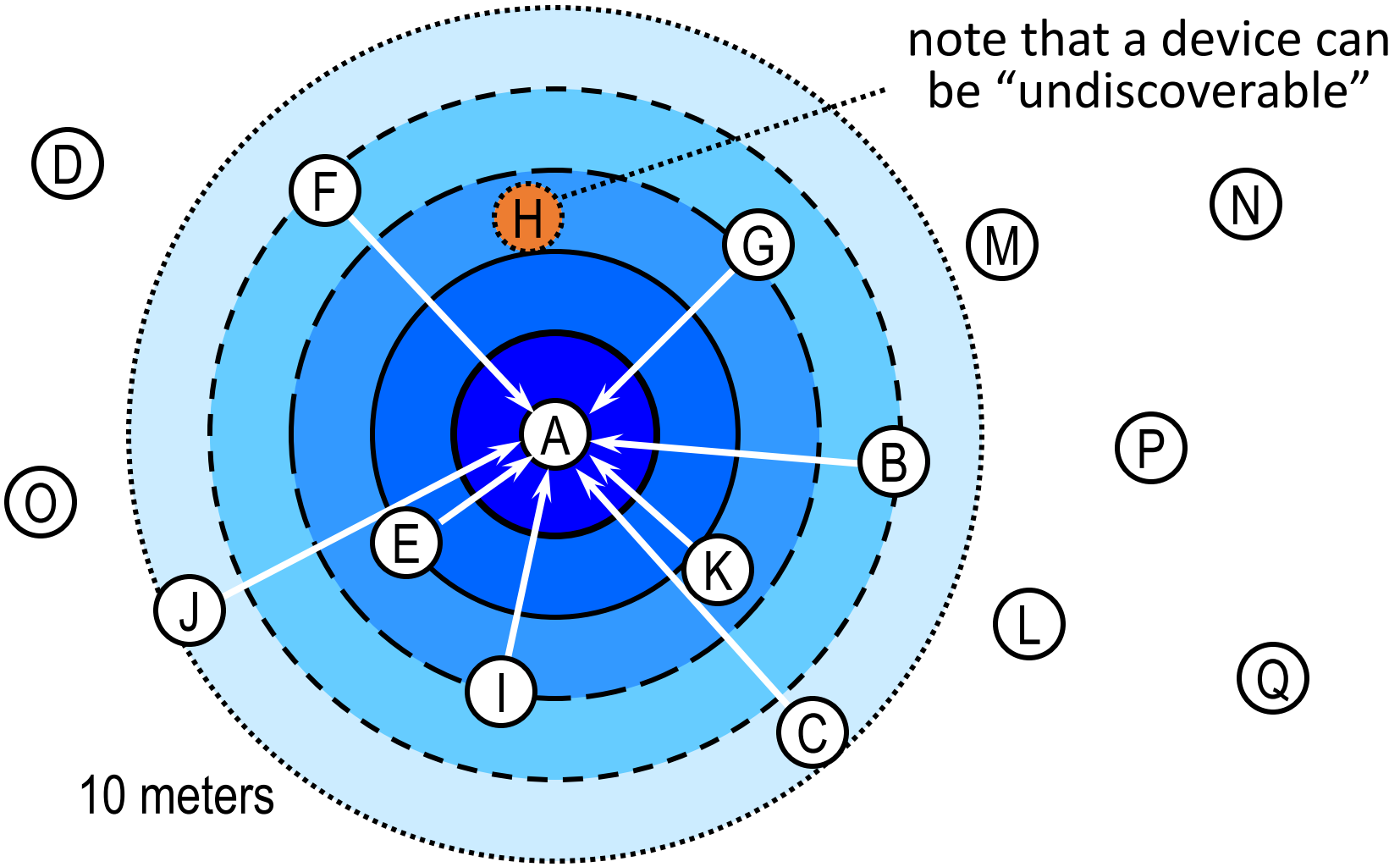
- Initially, devices know only about themselves
  - No synchronization
  - Everyone monitors in standby mode
  - All devices have the capability of serving as master or slave



Forming a Piconet

- Unit establishing the piconet automatically becomes the master
  - It sends an inquiry to discover what other devices are out there
- Addressing
  - Active devices are assigned a 3-bit active member address (AMA)
  - Parked devices are assigned an 8-bit parked member address (PMA)
  - Standby devices do not need an address

Inquiry


note that a device can be “undiscoverable”
D
F
H
G
M
N
A
B
P
O
E
K
J
L
I
C
Q
10 meters

Scatternets

- Piconets with overlapping coverage use different hopping sequences
  - Collisions may occur when multiple piconets use the same carrier frequency at the same time
- Devices can participate in multiple piconets simultaneously, creating a scatternet
  - A device can only be the master of one piconet at a time
  - A device may serve as master in one piconet and slave in another
  - A device may serve as slave in multiple piconets

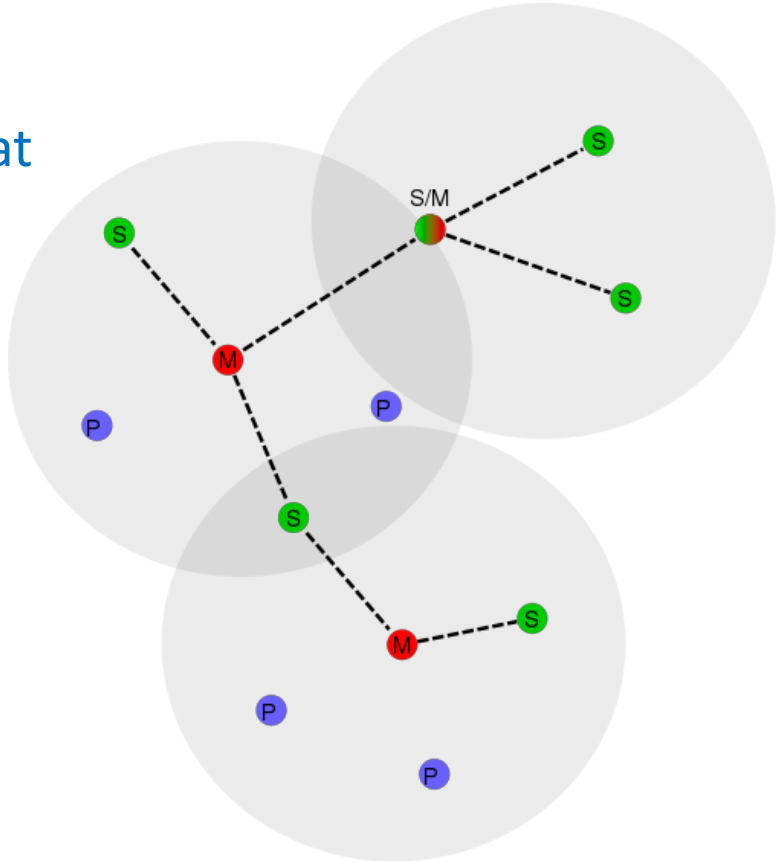
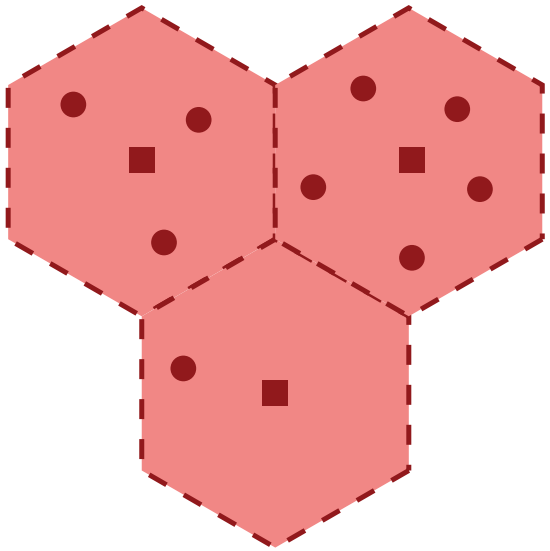
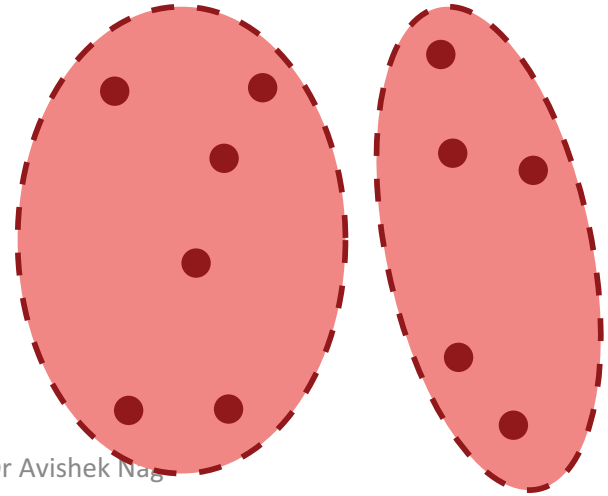


Image source: wikipedia

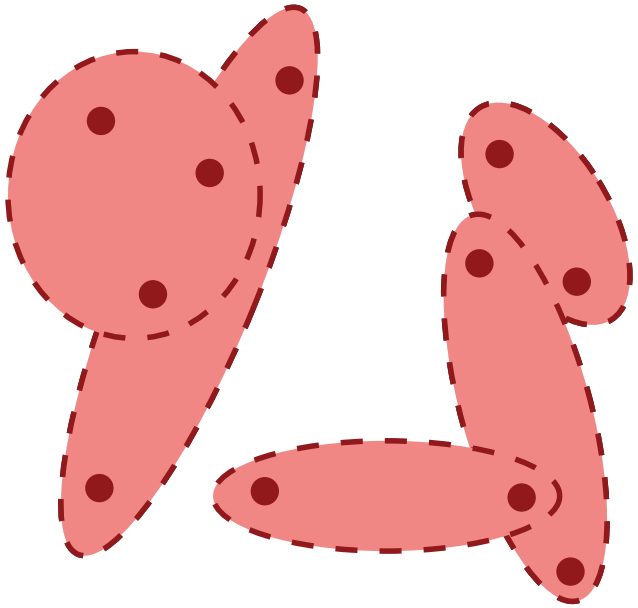
Wireless Network configurations



(a) Cellular system (squares represent stationary base stations)



(b) Conventional ad hoc systems



(c) Scatternets

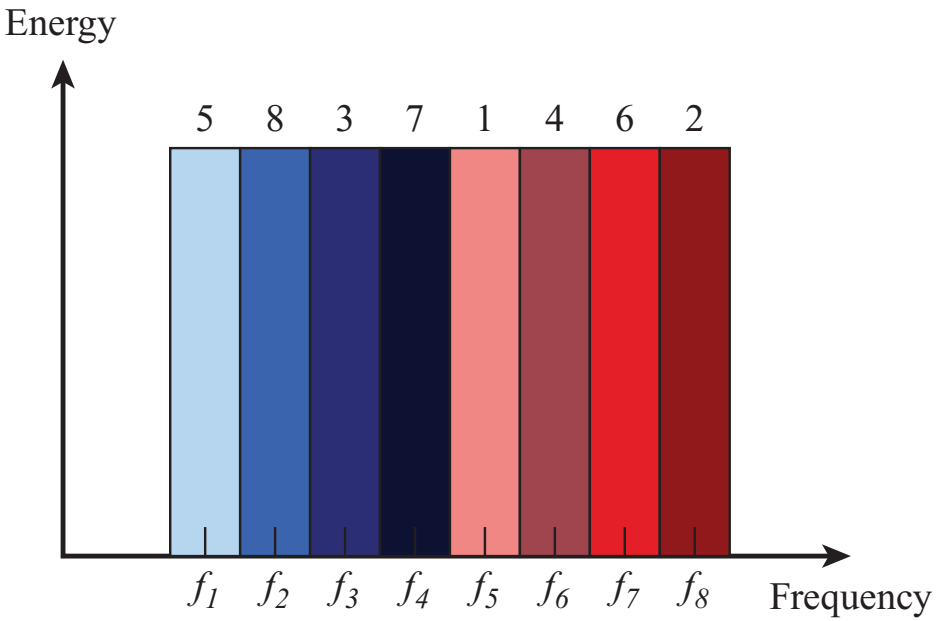
Radio Specification

- Classes of transmitters
  - –Class 1: Outputs 100 mW for maximum range
    - ➢Power control mandatory
    - ➢Provides greatest distance
  - –Class 2: Outputs 2.4 mW at maximum
    - ➢Power control optional
  - –Class 3: Nominal output is 1 mW
    - ➢Lowest power

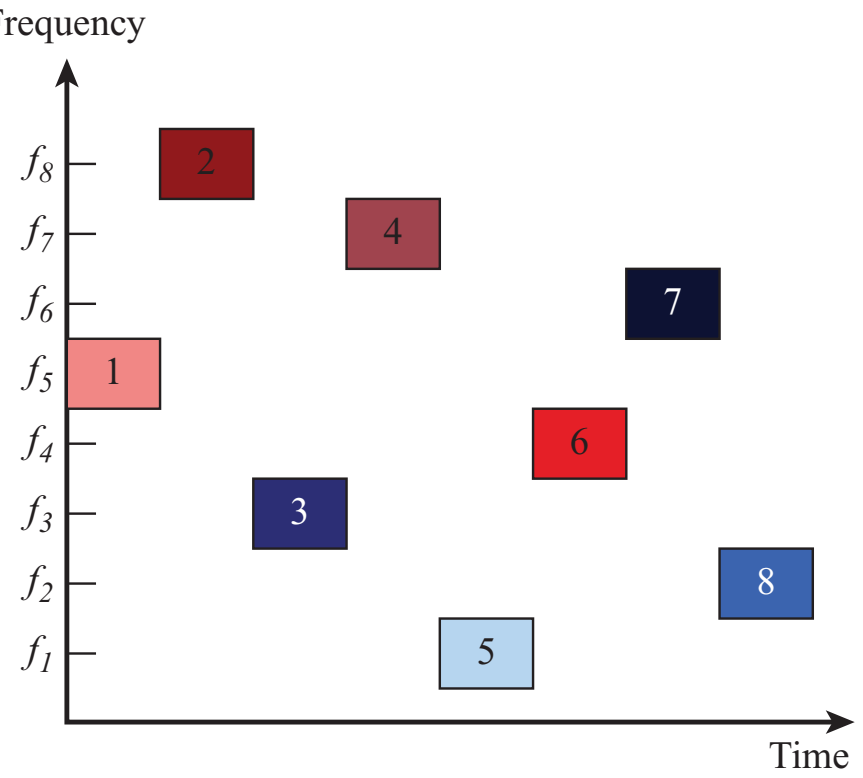
Frequency Hopping in Bluetooth

- Provides resistance to interference and multipath effects
- Provides a form of multiple access among co-located devices in different piconets
- Total bandwidth divided into 1MHz physical channels
- FH occurs by jumping from one channel to another in pseudorandom sequence
- Hopping sequence shared with all devices on piconet
- Piconet access:
  - Bluetooth devices use time division duplex (TDD)
  - Access technique is TDMA
  - FH-TDD-TDMA

Frequency Hopping Example



(a) Channel assignment

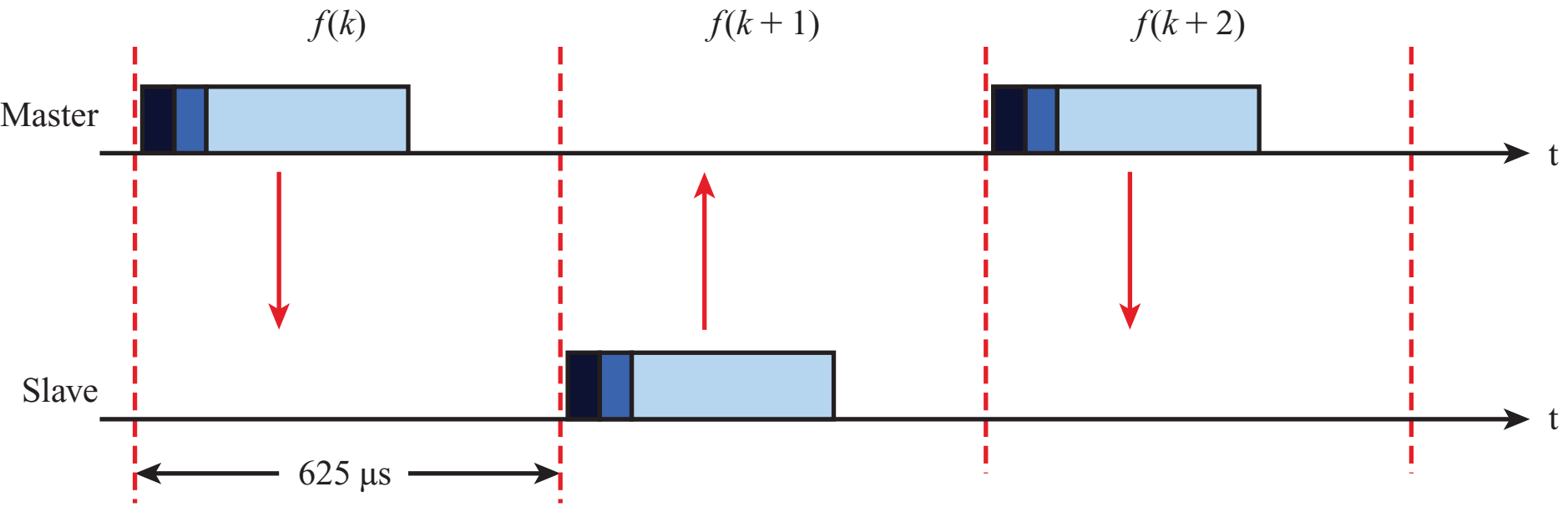


(b) Channel use

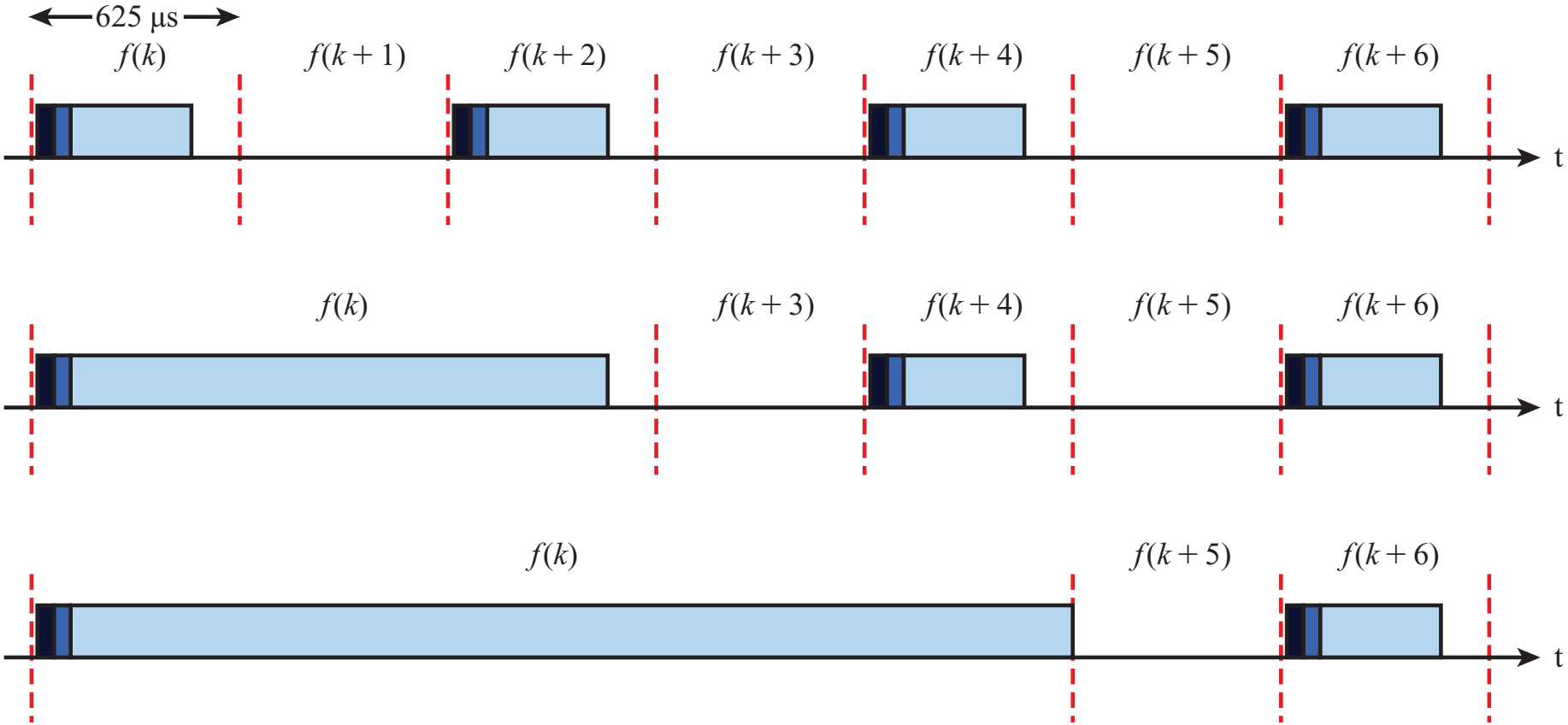
Inventor of Frequency Hopping

Hedy Lamarr (1914 – 2000)

Frequency-Hop Time-Division Duplex



Examples of Multislot Packets

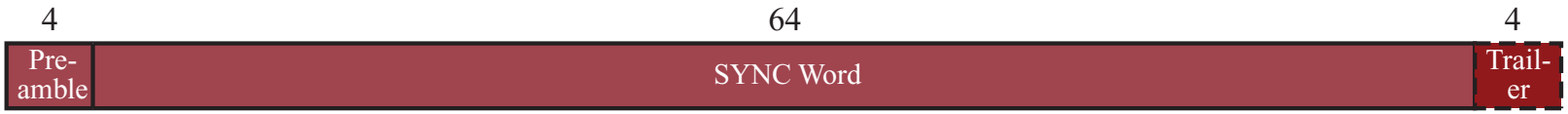


Physical Links between Master and Slave

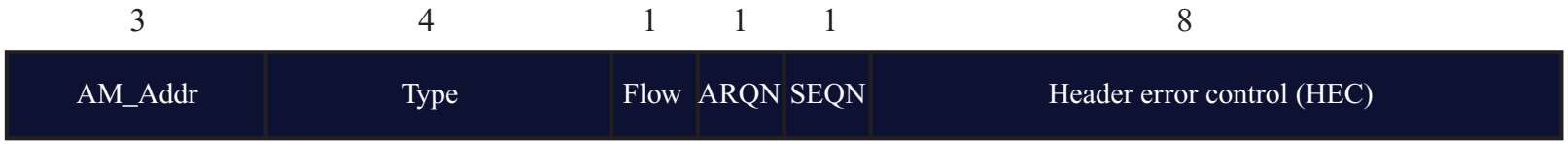
- Synchronous connection oriented (SCO)
  - Allocates fixed bandwidth between point-to-point connection of master and slave
  - Master maintains link using reserved slots
  - Master can support three simultaneous links
  - Retransmissions are never supported
- Asynchronous connectionless (ACL)
  - Point-to-multipoint link between master and all slaves
  - Only single ACL link can exist
- Extended Synchronous connection oriented (eSCO)
  - Reserves slots just like SCO
  - But these can be asymmetric
  - Retransmissions are supported

Bluetooth Baseband Formats

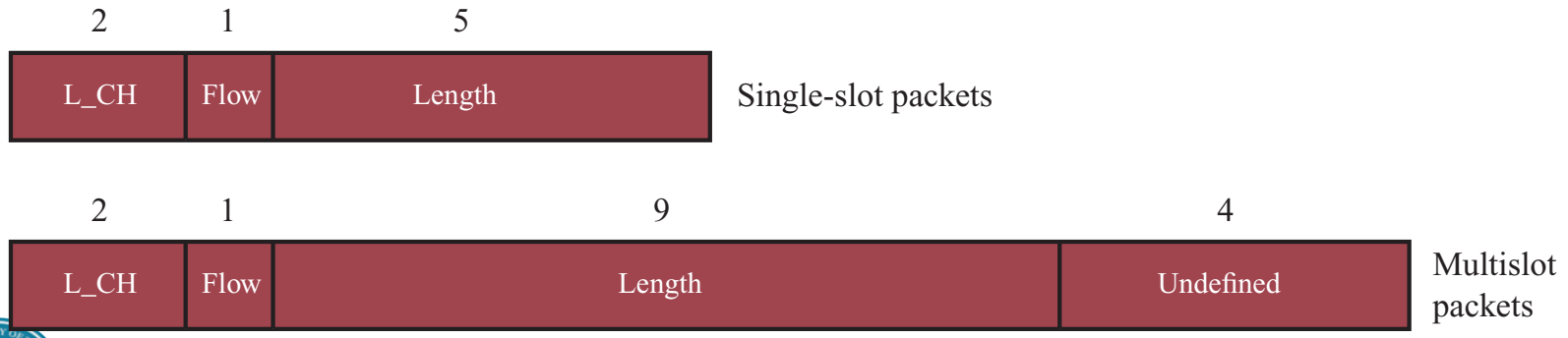
(a) Packet format



(b) Access code format



(c) Header format (prior to coding)



(d) Data payload header format

Bluetooth Packet Fields

- **Access code** – used for timing synchronization, offset compensation, paging, and inquiry
- **Header** – used to identify packet type and carry protocol control information
- **Payload** – contains user voice or data and payload header, if present

Types of Access Codes

- Channel access code (CAC) – identifies a piconet
- Device access code (DAC) – used for paging and subsequent responses
- Inquiry access code (IAC) – used for inquiry purposes

Packet Header Fields

- AM_ADDR – contains “active mode” address of one of the slaves
- Type – identifies type of packet (table in next slide)
- Flow – 1-bit flow control
- ARQN – 1-bit acknowledgment
- SEQN – 1-bit sequential numbering schemes
- Header error control (HEC) – 8-bit error detection code

Type Code	Physical Link	Name	Number of Slots	Description
0000	Common	NULL	1	Has no payload. Used to return link information to the source regarding the success of the previous transmission (ARQN), or the status of the RX buffer (FLOW). Not acknowledged.
0001	Common	POLL	1	Has no payload. Used by master to poll a slave. Acknowledged.
0010	Common	FHS	1	Special control packet for revealing device address and the clock of the sender. Used in page master response, inquiry response, and frequency hop synchronization. 2/3 FEC encoded.
0011	Common	DM1	1	Supports control messages and can also carry user data. 16-bit CRC. 2/3 FEC encoded.
0101	SCO	HV1	1	Carries 10 information bytes; typically used for 64-kbps voice. 1/3 FEC encoded.
0110	SCO	HV2	1	Carries 20 information bytes; typically used for 64-kbps voice. 2/3 FEC encoded.
0111	SCO	HV3	1	Carries 30 information bytes; typically used for 64-kbps voice. Not FEC encoded.
1000	SCO	DV	1	Combined data (150 bits) and voice (50 bits) packet. Data field 2/3 FEC encoded.
0100	ACL	DH1	1	Carries 28 information bytes plus 16-bit CRC. Not FEC encoded. Typically used for high-speed data.
1001	ACL	AUX1	1	Carries 30 information bytes with no CRC or FEC. Typically used for high-speed data.
1010	ACL	DM3	3	Carries 123 information bytes plus 16-bit CRC. 2/3 FEC encoded.
1011	ACL	DH3	3	Carries 185 information bytes plus 16-bit CRC. Not FEC encoded.
1110	ACL	DM5	5	Carries 226 information bytes plus 16-bit CRC. 2/3 FEC encoded.
1111	ACL	DH5	5	Carries 341 information bytes plus 16-bit CRC. Not FEC encoded.

Payload format

- Payload header
  - L_CH field – identifies logical channel
  - Flow field – used to control flow at L2CAP level
  - Length field – number of bytes of data
- Payload body – contains user data
- CRC – 16-bit CRC code

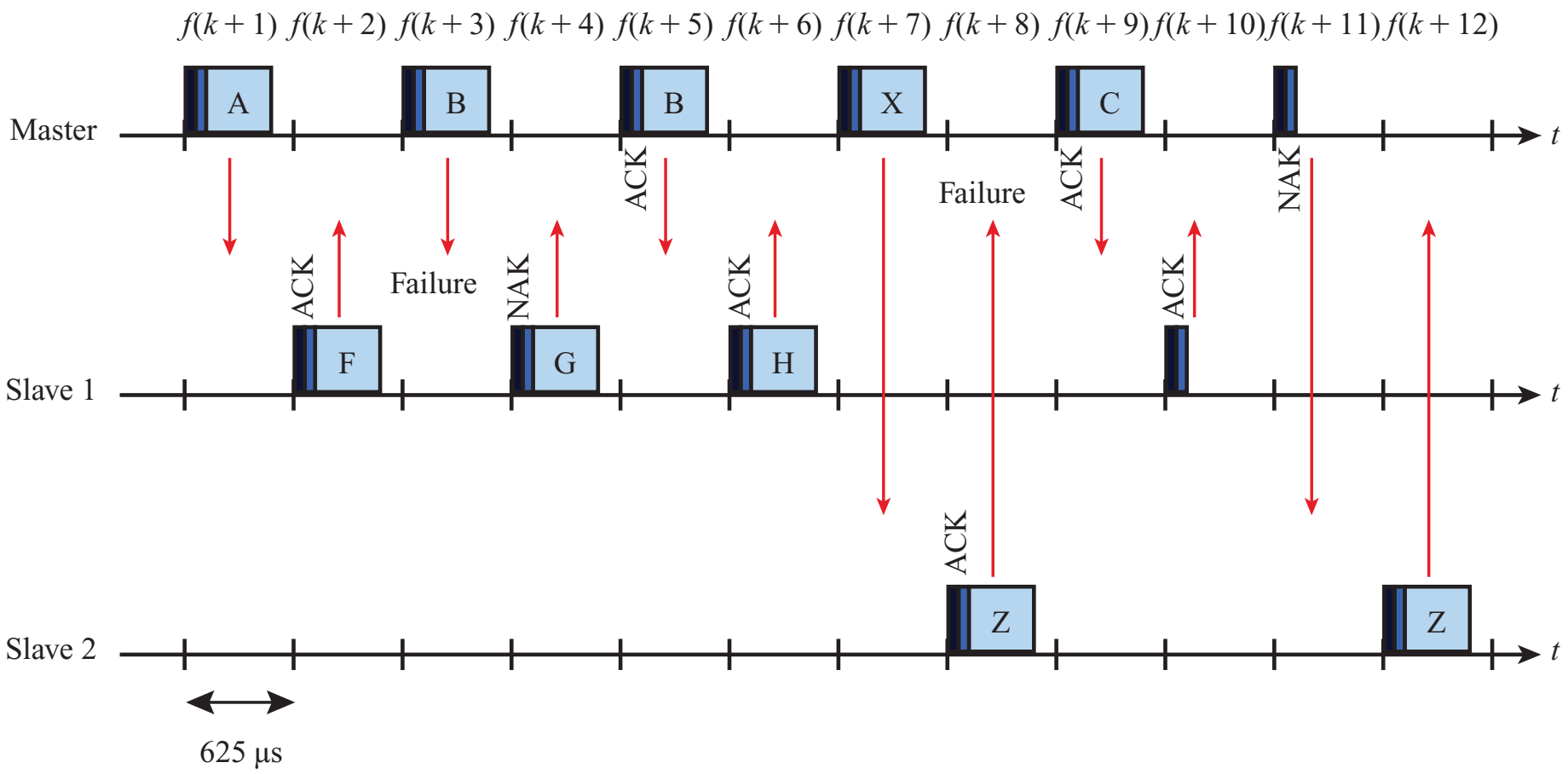
Error Correction Schemes

- 1/3 rate FEC (forward error correction)
  - Used on 18-bit packet header, voice field in HV1 packet
- 2/3 rate FEC
  - Used in DM packets, data fields of DV packet, FHS packet and HV2 packet
- ARQ
  - Used with DM and DH packets

ARQ Scheme Elements

- Error detection – destination detects errors, discards packets
- Positive acknowledgment – destination returns positive acknowledgment
- Retransmission after timeout – source retransmits if packet unacknowledged
- Negative acknowledgment and retransmission – destination returns negative acknowledgement for packets with errors, source retransmits

An Example of Retransmission Operation



Logical Channels

- Link control (LC)
- Link manager (LM)
- User asynchronous (UA)
- User isochronous (UI)
- User synchronous (US)

Link manager

- Manages various aspects of the radio link between a master and a slave
- Involves the exchange LMP PDUs (protocol data units)
- Procedures defined for LMP are grouped into 24 functional areas, which include
  - Authentication
  - Pairing
  - Encryption
  - Clock offset request
  - Switch master/slave
  - Name request
  - Hold or park or sniff mode

Logical link control and adaptation protocol (L2CAP)

- Provides a link-layer protocol between entities with a number of services
- Relies on lower layer for flow and error control
- Makes use of ACL links, does not support SCO links
- Provides two alternative services to upper-layer protocols
  - Connection service
  - Connection-mode service

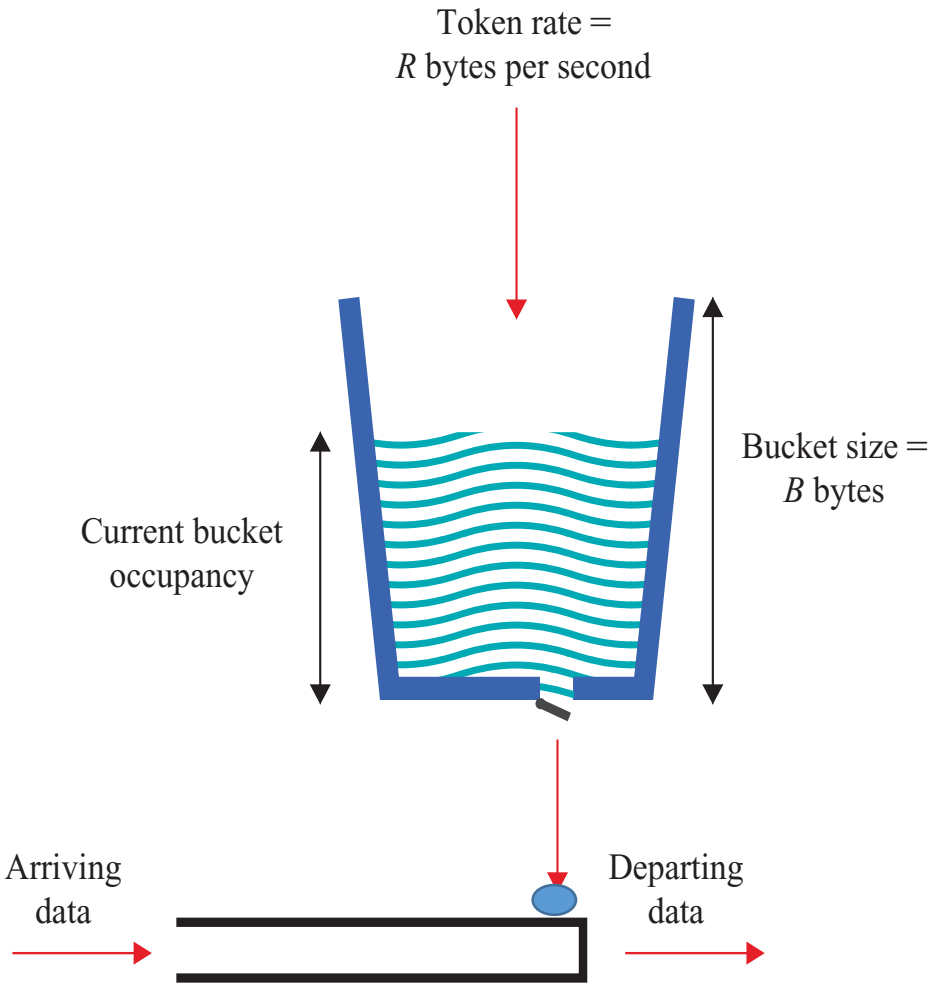
L2CAP Logical Channels

- Connectionless
  - Supports connectionless service
  - Each channel is unidirectional
  - Used from master to multiple slaves
- Connection-oriented
  - Supports connection-oriented service
  - Each channel is bidirectional
- Signaling
  - Provides for exchange of signaling messages between L2CAP entities

Flow Specification Parameters

- Service type
- Token rate (bytes/second)
- Token bucket size (bytes)
- Peak bandwidth (bytes/second)
- Latency (microseconds)
- Delay variation (microseconds)

Token Bucket Scheme



- **Consider sending a packet of size $b < B$**
  - If bucket is full → packet is sent, *b* tokens removed
  - If bucket is empty → packet is queued until *b* tokens arrive
  - If bucket is partially full:
    - No of tokens in bucket > *b*: packet sent immediately
    - No of tokens in bucket < *b*: packet should wait

Bluetooth high speed

- Bluetooth 3.0+HS
- Up to 24 Mbps
- New controller compliant with 2007 version of IEEE 802.11
- Known as Alternative MAC/PHY (AMP)
  - Optional capability
- Bluetooth radio still used for device discovery, association, setup, etc.
- Allows more power efficient Bluetooth modes to be used, except when higher data rates are needed

Bluetooth Smart

- Bluetooth 4.0
- Previously known as Bluetooth Low Energy
- An intelligent, power-friendly version of Bluetooth
- Can run long periods of time on a single battery
  - Or scavenge for energy
- Also communicates with other Bluetooth-enabled devices
  - Legacy Bluetooth devices or Bluetooth-enabled smartphones
  - Great feature
- Possible successful technology for the Internet of Things
  - For example, health monitoring devices can easily integrate with existing smartphones

Bluetooth Smart II

- Same 2.4 GHz ISM bands as Bluetooth BR/EDR
  - But uses 40 channels spaced 2 MHz apart instead of 79 channels spaced 1 MHz apart
- Devices can implement a transmitter, a receiver, or both
- Implementation
  - Single-mode Bluetooth Smart functionality
    - Reduced cost chips that can be integrated into compact devices.
  - Dual-mode functionality to also have the Bluetooth BR/EDR capability
- 10 mW output power
- 150 m range in an open field

Bluetooth Summary

- Bluetooth **1.x** -> Nearly extinct; *if at all* you find a device which is advertised as 1.x - **don't** buy that relic, unless of course you want it as a collectors item.
  Capabilities - **Basic rate** bluetooth (that would be about a *theoretical* maximum of 1 Mbps data rate)

- Bluetooth **2.x** -> The most popular variant, especially 2.1. The 2.1 version makes it easier to pair with different devices (even from different manufacturers) and also increases the reliability per se of the pairing process. Introduced the **Enhanced Data Rate (EDR)** capability (optional).
  Capabilities - **Basic rate** + **EDR** (that would be about a *theoretical* maximum of 3 Mbps data rate; optional)

- Bluetooth **3.x** -> Introduces support for an alternate lower layer, i.e. all the applications that were available with Bluetooth radio earlier can be run over an alternate radio, say like the 802.11 one. This feature is called **High Speed (HS)**, and as the name suggests that was the intent and purpose. The HS feature is optional too.
  Capabilities - **Basic rate** + **EDR** (optional) + **HS** (optional)

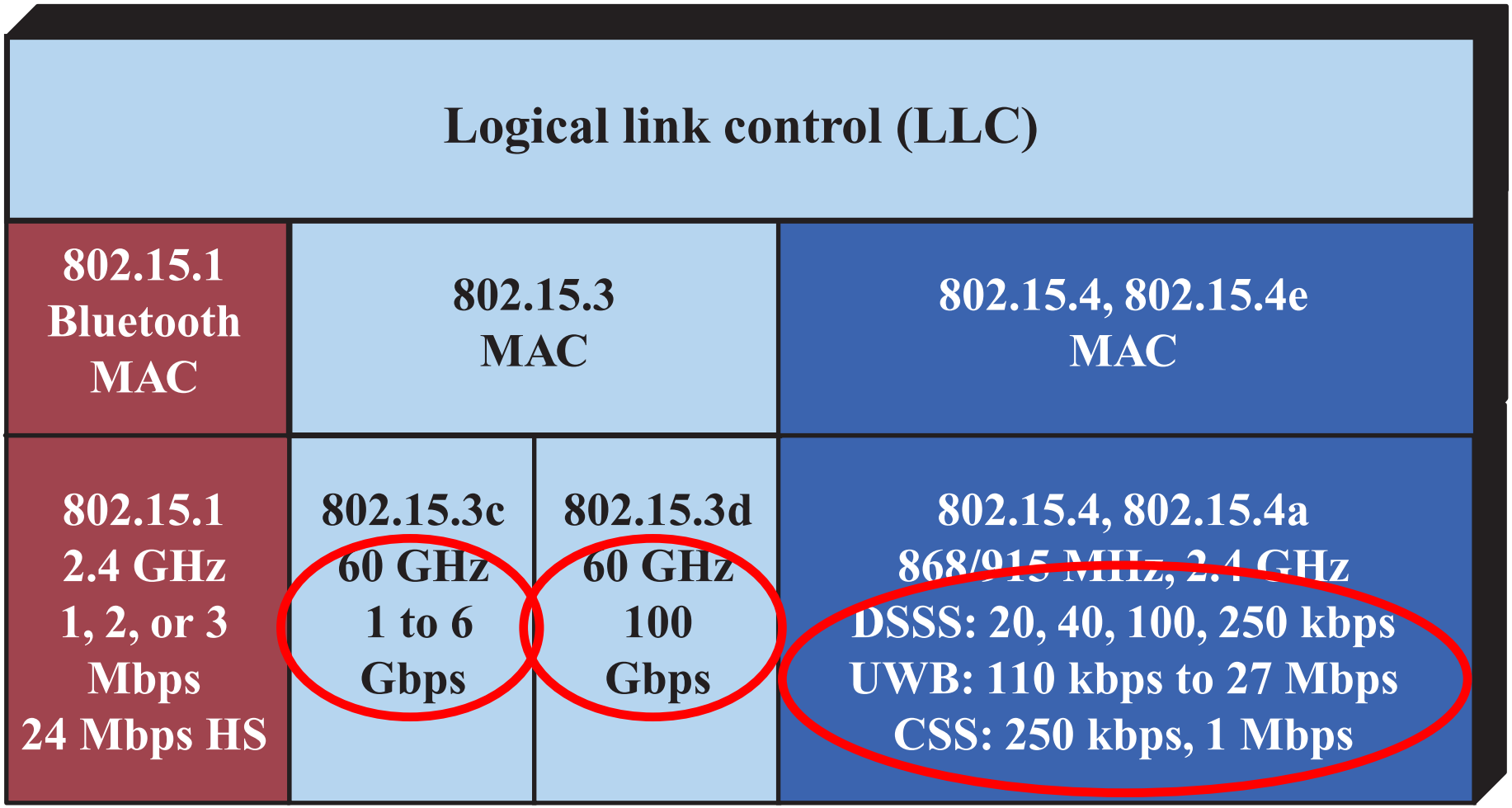
- Bluetooth **4.x** -> Introduces support for collecting data from devices which generate data at a very low rate. The main intent of this feature, called Low Energy (LE), is to aggregate data from various sensors, like heart rate monitors, thermometers etc.

Source: https://www.quora.com/What-is-the-difference-between-Bluetooth-4-0-3-0-and-2-0

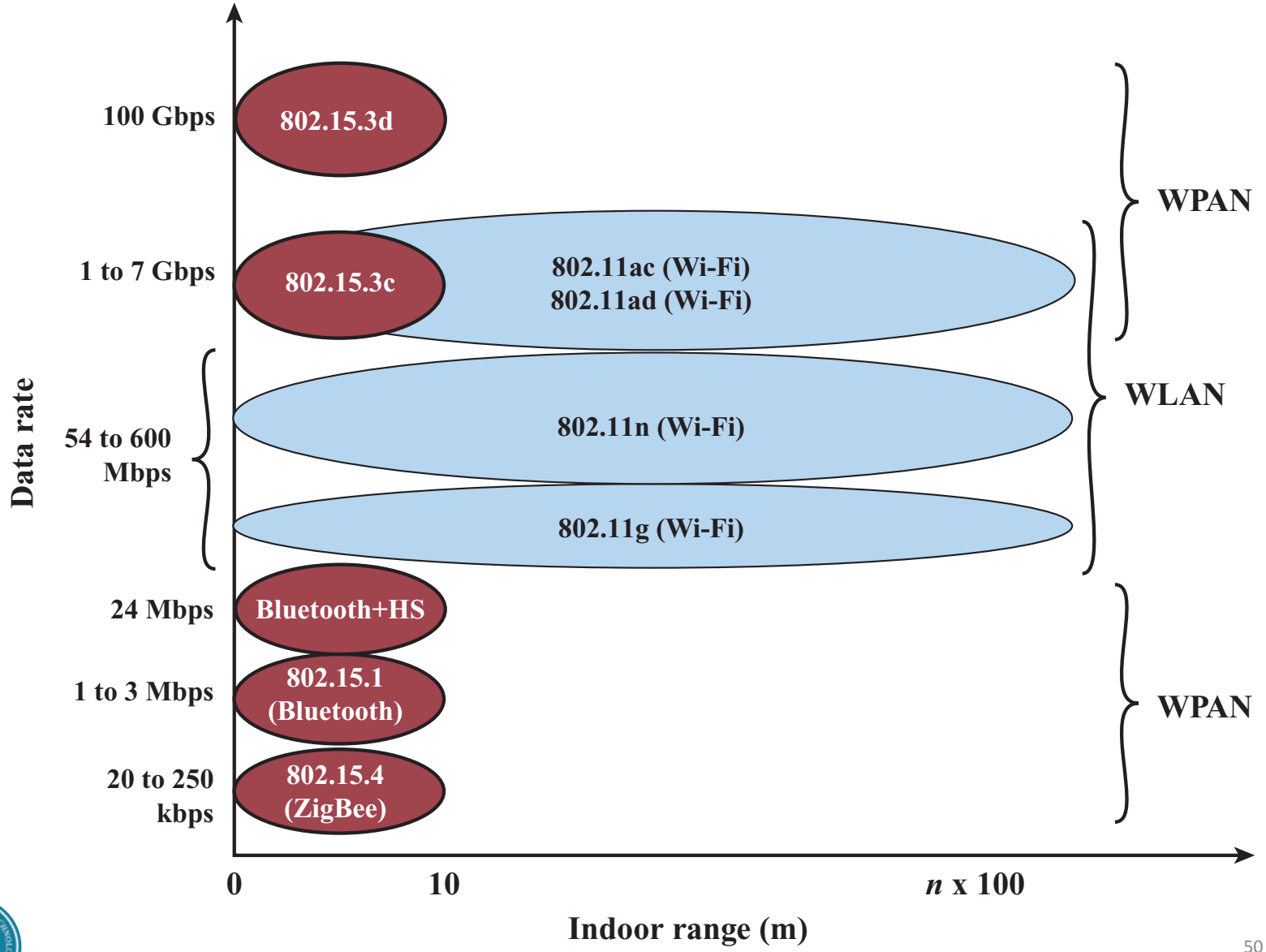
IEEE 802.15

- After 802.15.1, work went two directions
- 802.15.3
  - Higher data rates than 802.15.1
  - But still low cost, low power compared to 802.11
- 802.15.4
  - Very low cost, very low power compared to 802.15.1

IEEE 802.15 Protocol Architecture

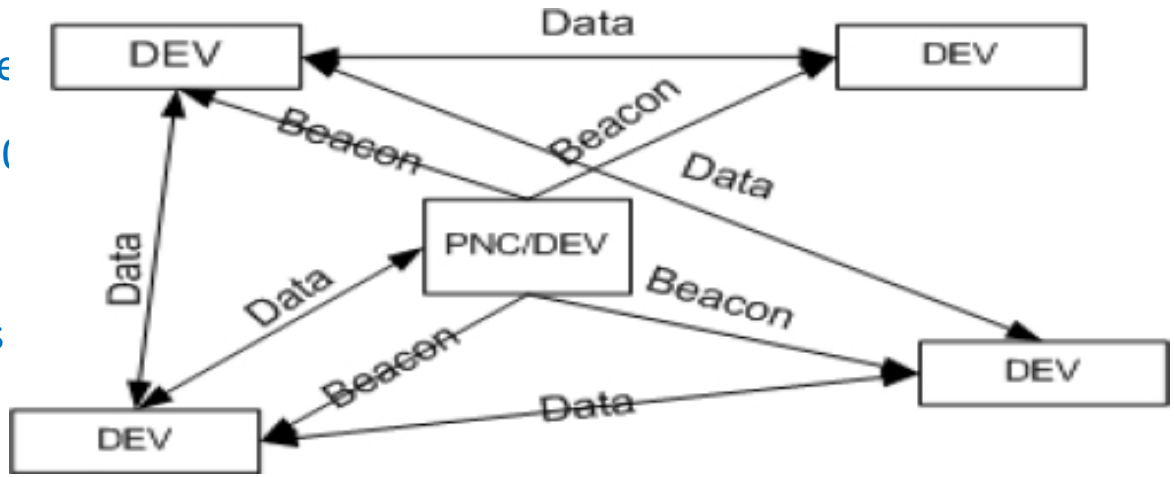


Wireless Local Networks



IEEE 802.15.3

- High data rate WPANs
  - Digital cameras, speakers, video, music
- Piconet coordinator (PNC)
  - Sends beacons to device
  - Uses superframes like 8(
  - QoS based on TDMA
  - Controls time resources
- 802.15.3c
  - Latest standard
  - Uses 60 GHz band, with same benefits as 802.11ad
  - Single-carrier and OFDM PHY modes



IEEE 802.15.4

- Low data rate, low complexity
  - Competitor to Bluetooth Smart
- PHY options in 802.15.4 and 802.15.4a
  - 868/915 MHz for 20, 40, 100, and 250 kbps
  - 2.4 GHz for 250 kbps
  - Ultrawideband (UWB)
    - Uses very short pulses with wide bandwidth
      - Low energy density for low interference with others
    - 851 kbps and optionally 110 kbps, 6.81 Mbps, or 27.234 Mbps
  - 2.4 GHz chirped spread spectrum for 1 Mbps and optionally 250 kbps
    - Sinusoidal signals that change frequency with time identical to Frequency Hopping

IEEE 802.15.4 II

- Many other creative and practical activities
- IEEE 802.15.4f – Active Radio Frequency Identification Tags (RFIDs)
  - Attached to an asset or person with a unique identification
  - An Active RFID tag must employ some source of power
- IEEE 802.15.4g – Smart Utility Networks (SUN)
  - Facilitates very large scale process control applications such as the utility smart-grid network
- IEEE 802.15.4j – Medical Body Area Networks
- EEE 802.15.4k – Low Energy Critical Infrastructure Networks (LECIM)
  - To facilitate point to multi-thousands of points communications for critical infrastructure monitoring devices with multi-year battery life.
- IEEE 802.15.4p – Positive Train Control
  - Sensor, control and information transfer applications for rail transit

Other IEEE 802.15 standards

- 802.15.2 – Coexistence between 802.11 and 802.15
- 802.15.5 – Mesh networks
  - Multihop networking
- 802.15.6 – Body area networks
- 802.15.7 – Visible light communication

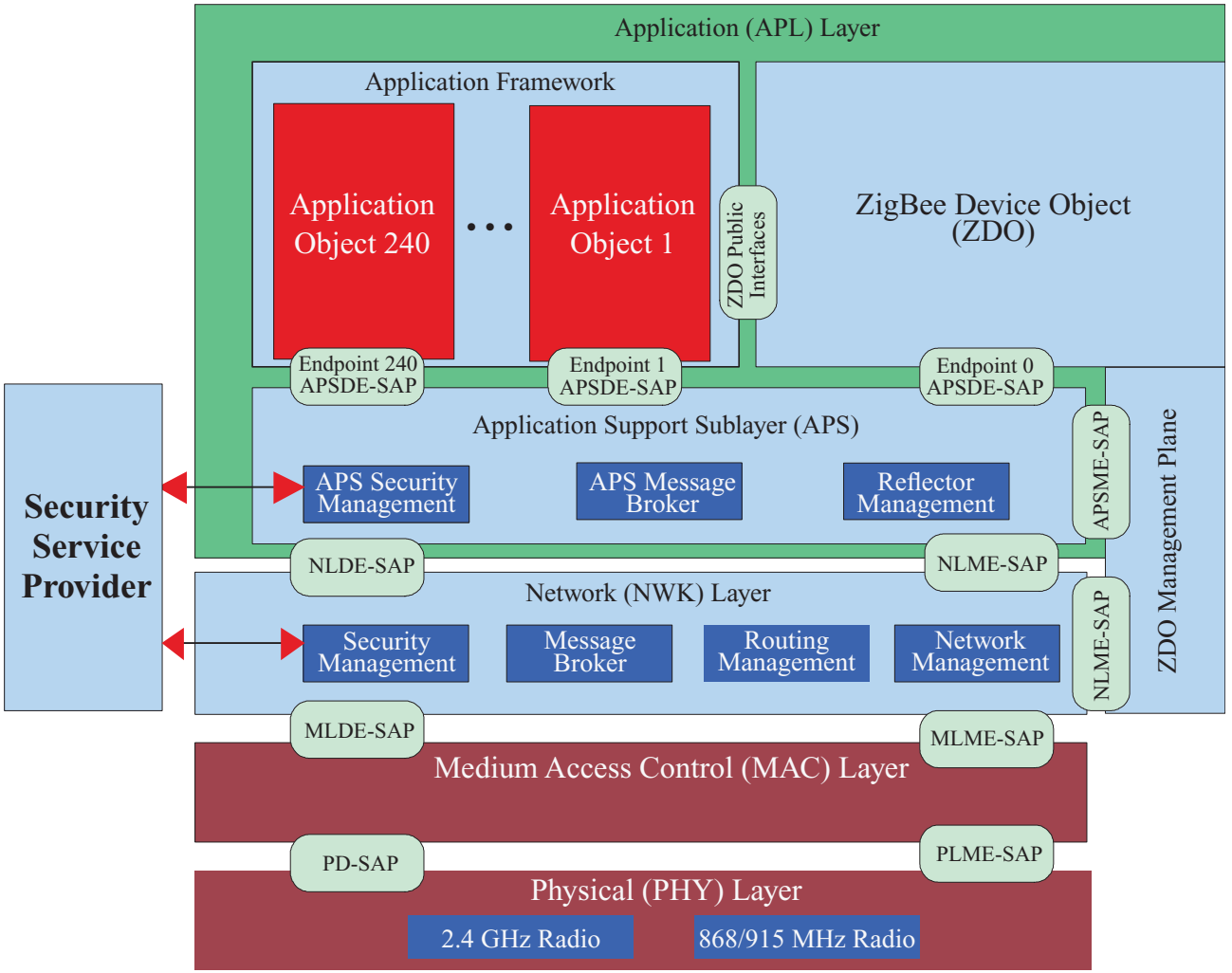
ZigBee

- Extends IEEE 802.15.4 standards
- Low data rate, long battery life, secure networking
- Data rates 20 to 250 kbps
- Operates in ISM bands
  - 868 MHz (Europe), 915 MHz (USA and Australia), 2.4 GHz (worldwide)
- Quick wake from sleep
  - 30 ms or less compared to Bluetooth which can be up to 3 sec.
  - ZigBee nodes can sleep most of the time

ZigBee

- ZigBee complements the IEEE 802.15.4 standard by adding four main components
  - Network layer provides routing
  - Application support sublayer supports specialized services.
  - ZigBee device objects (ZDOs) are the most significant improvement
    - Keep device roles, manage requests to join the network, discover devices, and manage security.
  - Manufacturer-defined application objects allow customization.

ZigBee Architecture

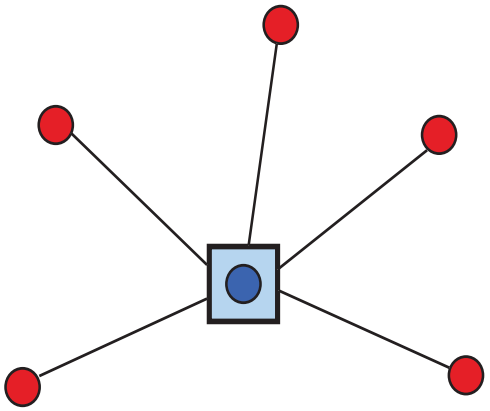


- IEEE 802.15.4 defined
- ZigBee™ Alliance defined
- End manufacturer defined
- Layer function
- Layer interface

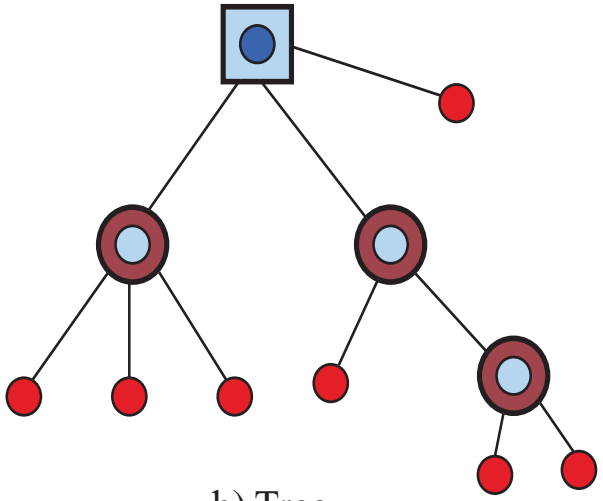
ZigBee

- Star, tree, or general mesh network structures
- ZigBee Coordinator
  - Creates, controls, and maintains the network
  - Only one coordinator in the network
  - Maintains network information, such as security keys
- ZigBee Router
  - Can pass data to other ZigBee devices
- ZigBee End Device
  - Only enough functionality to talk to a router or coordinator
  - Cannot relay information
  - Sleeps most of the time
  - Less expensive to manufacture

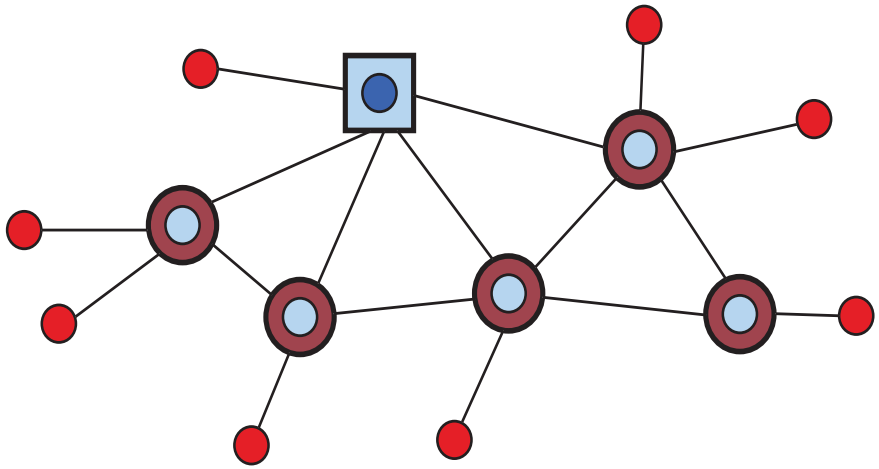
ZigBee Network



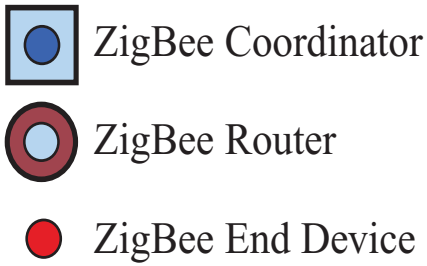
a) Star



b) Tree



c) Mesh



ZigBee alliance

- Industry consortium
- Maintains and publishes the ZigBee standard
  - ZigBee specifications in 2004
  - ZigBee PRO completed in 2007
    - Enhanced ZigBee
    - Profile 1 – home and light commercial use
    - Profile 2 – more features such as multicasting and higher security
- Application profiles
  - Allow vendors to create interoperable products if they implement the same profile

ZigBee application profiles

- ZigBee Building Automation (Efficient commercial spaces)
- ZigBee Health Care (Health and fitness monitoring)
- ZigBee Home Automation (Smart homes)
- ZigBee Input Device (Easy-to-use touchpads, mice, keyboards, wands)
- ZigBee Light Link (LED lighting control)
- ZigBee Network Devices (Assist and expand ZigBee networks)
- ZigBee Retail Services (Smarter shopping)
- ZigBee Remote Control (Advanced remote controls)
- ZigBee Smart Energy 1.1 (Home energy savings)
- ZigBee Smart Energy Profile 2 (IP-based home energy management)
- ZigBee Telecom Services (Value-added services)