Bluetooth and IEEE 802.15

CS-1699 Wireless Networks

Term : Spring 2018

Instructor : Xerandy

Objectives

- Explain the roles of the Bluetooth protocol stack and core protocols
- Describe the enhancement to Bluetooth in Bluetooth 3.0 and 4.0
- Compare the purposes of IEEE 802.15.3 and IEEE 802.15.4

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

Internet of Things

- Key application area for short-range communications
- Future Internet
  - Large numbers of wirelessly connected objects
  - Interactions between the physical world and computing, digital content, analysis, and services.
  - Called the Internet of Things
    - And many other "Internet of …" titles
  - 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 (MTM, M2M, D2D, etc.), also machine-type communications (MTC)
  - Devices working together for data analysis and 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

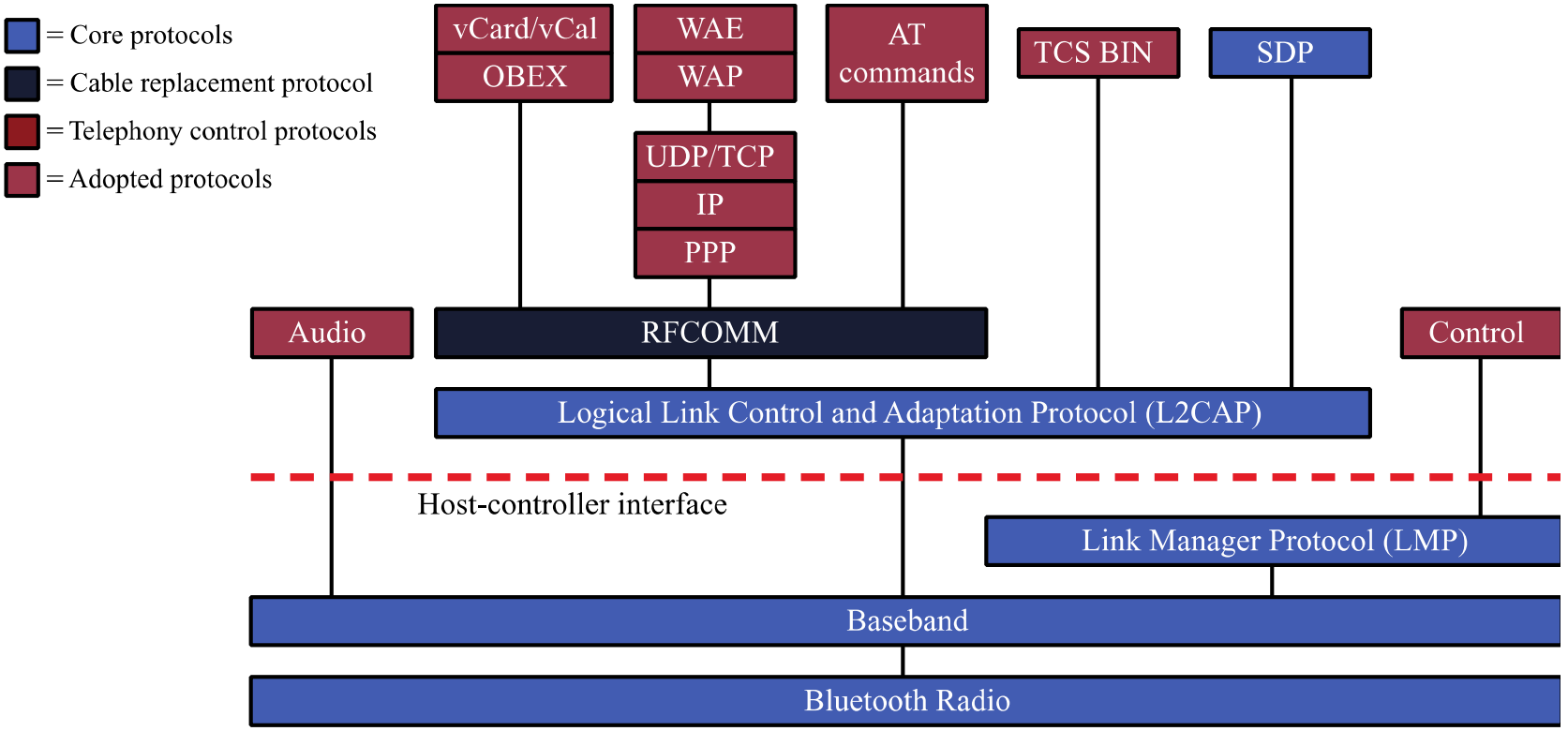
Top uses of Bluetooth

- 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 Standard Documents

- Divided into 2 groups : Core and Profile
  - Core specification :
    - Details of various layers of Bluetooth protocol architecture
  - Profile specifications
    - Use of Bluetooth technology to support various applications
- This class focuses on
  - Bluetooth 2.1 Basic/Enhanced Data Rate (BR/EDR)
  - Enhancements :
    - Bluetooth 3.0 Alternative MAC/PHY (AMP)
    - 4.0 Bluetooth Smart (Bluetooth Low Energy)

Bluetooth Protocol Stack



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			

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

- Cable replacement protocol
  - RFCOMM : Presents a virtual serial port for binary data transfer, emulating EIA-232 standard
- Telephony control protocol
  - Telephony control specification – binary (TCS BIN)
  - Defines the call control signaling for the establishment of speech and data calls between Bluetooth devices
  - Also defines mobility management procedures for handling groups of Bluetooth devices
- Adopted protocols
  - Specification issued by other standard-making organization and being incorporated into Bluetooth architecture
    - PPP (Point to Point Protocol):
      - Internet standard protocol for transporting IP datagrams over a point-to-point link
    - TCP/UDP/IP
    - OBEX (Object Exchange Protocol)
      Session-level protocol developed by Infrared Data Association(IrDA)
    - WAE/WAP

Bluetooth Core Protocol

- Radio
  - Specifies details of the air interface, including frequency and the use of frequency hopping
- Baseband
  - Concerned with connection establishment within a piconet, addressing, packet format, timing, and power control
- Link Manager Protocol
  - Responsible for link set up, including security aspect and packet size
- Logical link control and adaptation protocol (L2CAP)
  - Adapts upper layer protocols to the baseband layer
- Service discovery protocol
  - Inquiries on device information, services, and character of services

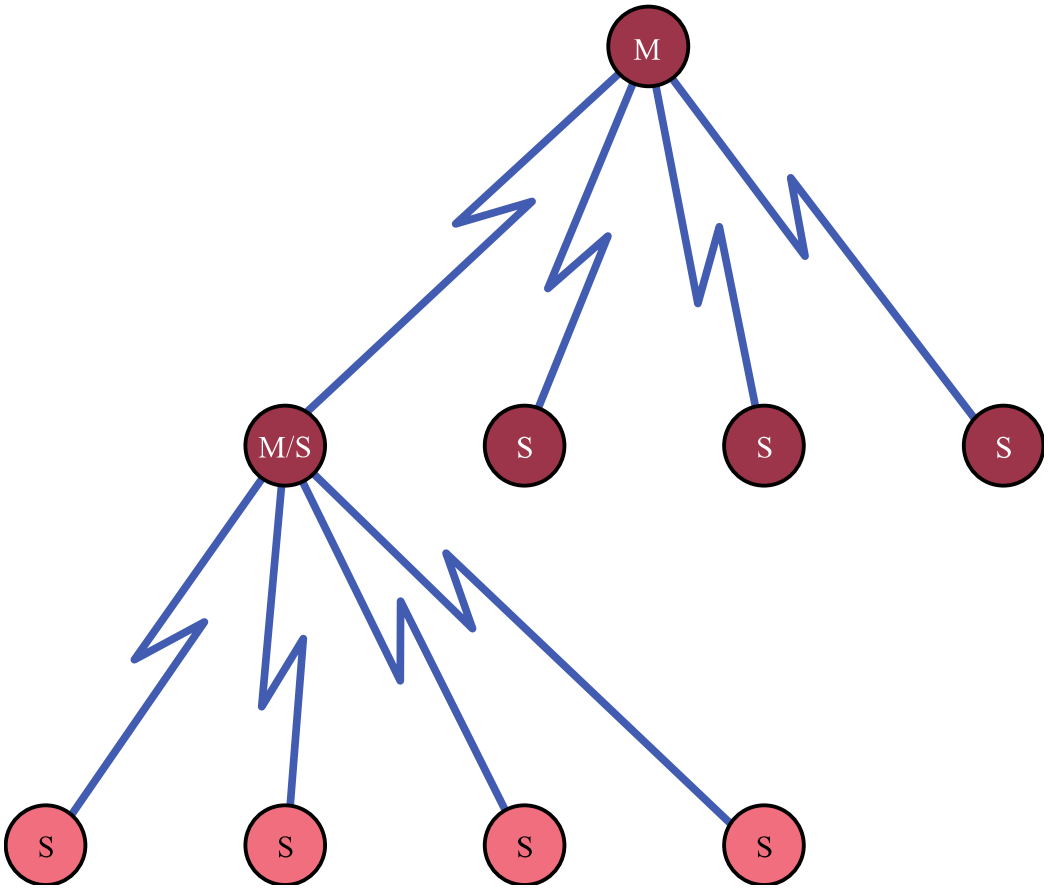
Profiles

- 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

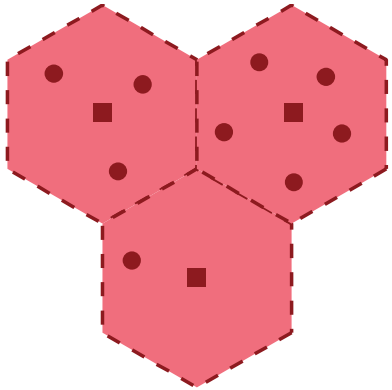
Piconets and Scatternets

- 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

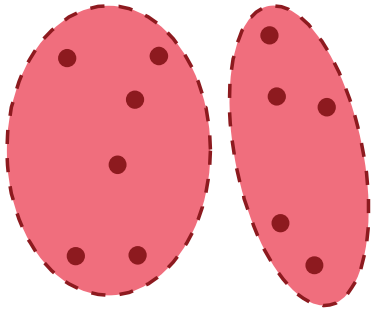
Master/Slave Relationship



Wireless Network Configuration



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



(b) Conventional ad hoc systems

(c) Scatternets

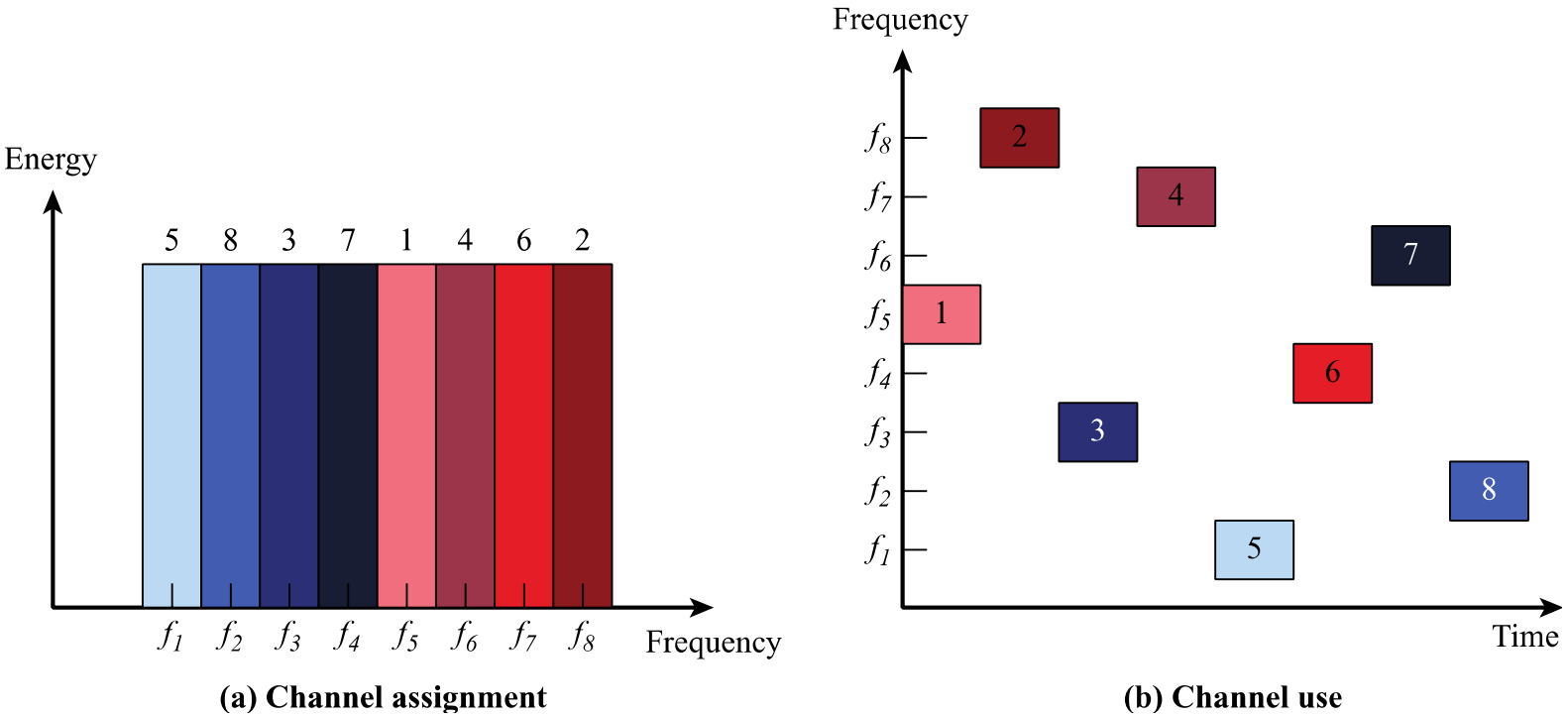
Radio Specification

- 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

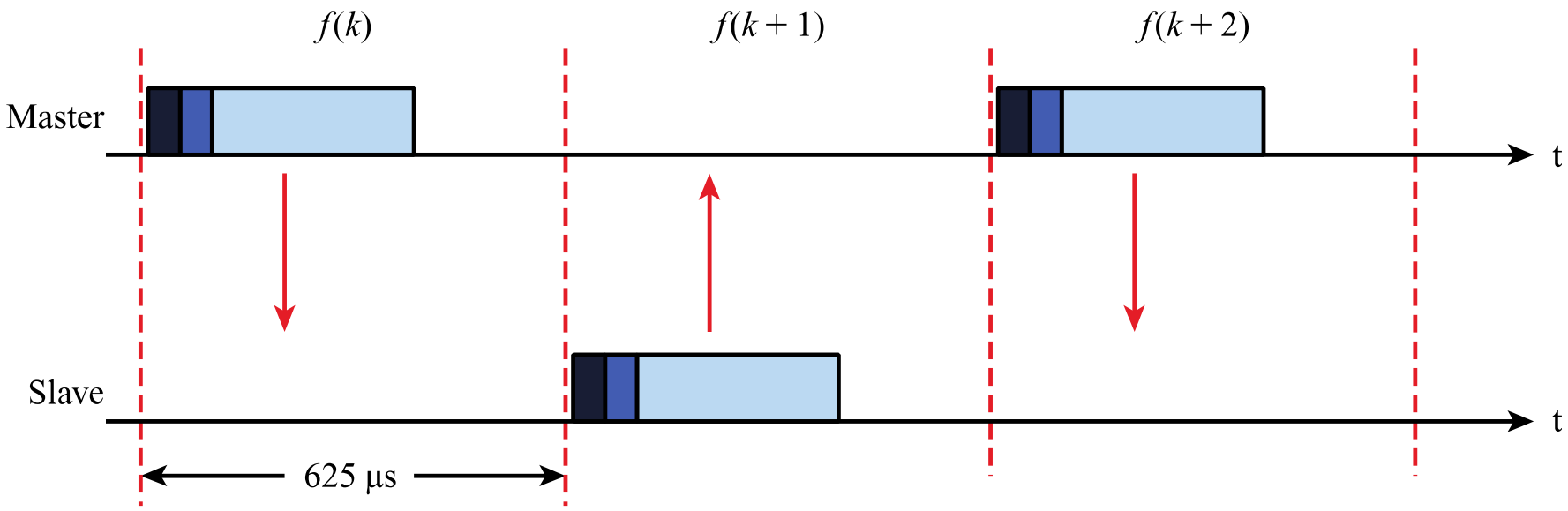
- Provides resistance to interference and multipath effects
- Provides a form of multiple access among co-located devices in different piconets
- Total bandwidth divided into 1MHz physical channels
- FH occurs by jumping from one channel to another in pseudorandom sequence
  - The hop rate is 1600 hops per-second
- 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 in Bluetooth

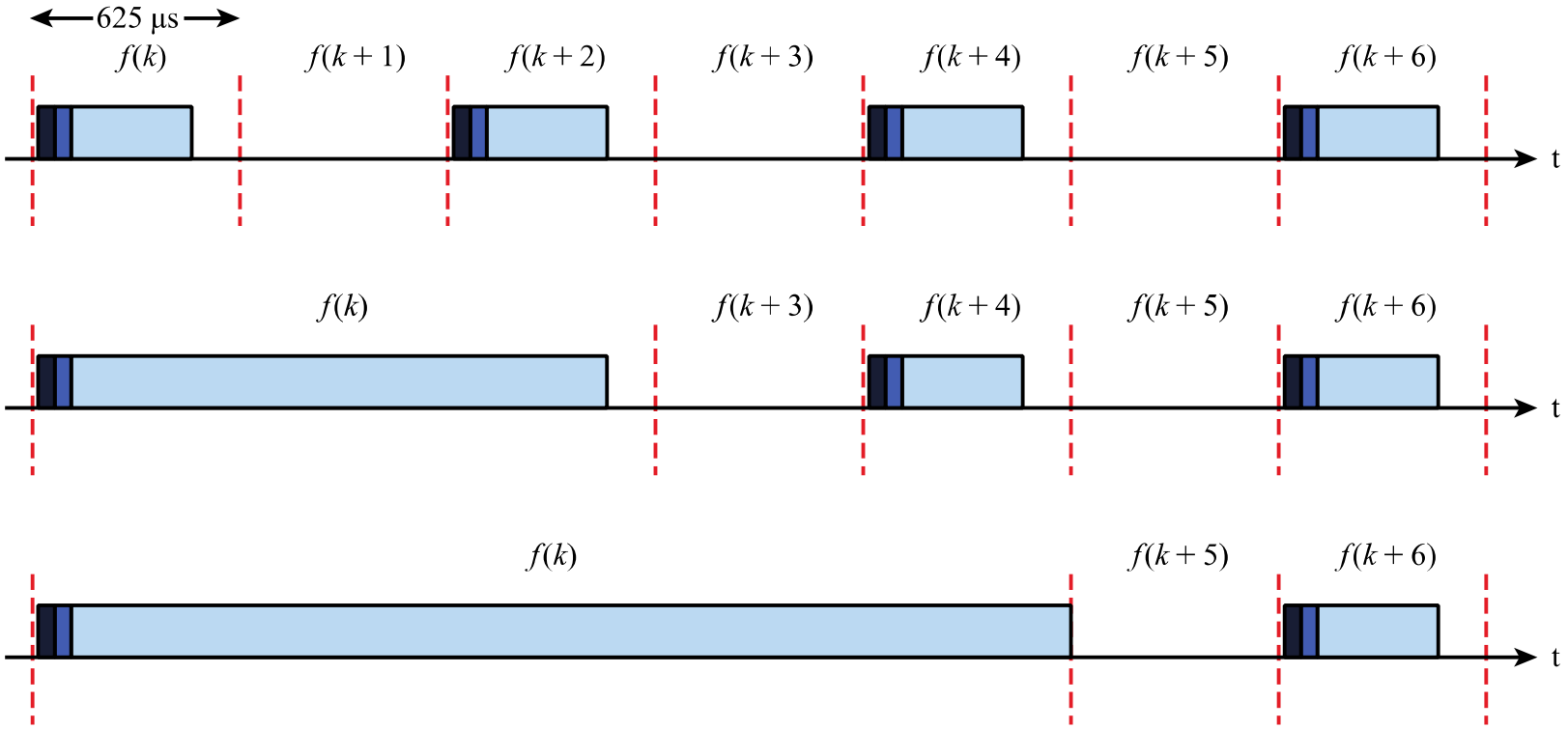


(a) Channel assignment **(b) Channel use**

Frequency Hopping in Bluetooth



Frequency Hopping in Bluetooth



Bluetooth Specification

	Basic Rate	Enhanced Data Rate
Topology	7 simultaneous links in logical star	7 simultaneous links in logical star
Modulation	GFSK	$\pi/4$ –DQPSK and 8DPSK
Peak data rate	1 Mbps	2 Mbps and 3 Mbps
RF Bandwidth	220 KHz (-3 dB), 1 MHz (-20 dB)	220 KHz (-3 dB), 1 MHz (-20 dB)
RF Band	2.4 GHz ISM band	2.4 GHz ISM band
Carrier spacing	1 MHz	1 MHz
RF Carriers	23/79	23/79
Transmit power	0.1 Watt	0.1 Watt
Frequency hop rate	1600 hop/s	1600 hop/s

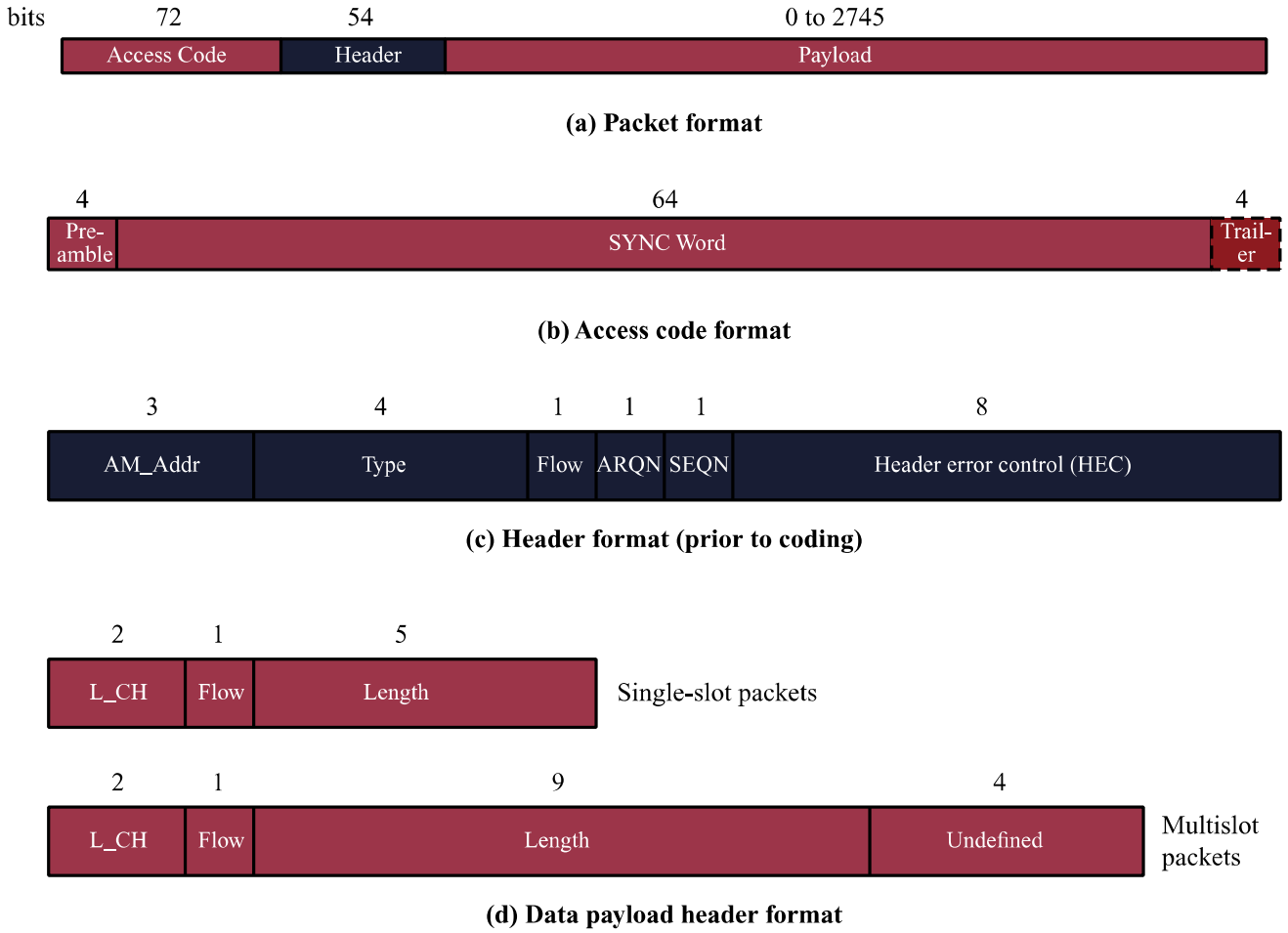
Bluetooth Frequency Allocation

Area	Regulatory Range	RF Channels
US most of Europe and other countries	2.4 to 2.4835 GHz	f= 2.402 + n MHz, n=0,1,…78
Japan	2.471 to 2.497 GHz	f=2.473 + + n MHz, n=0,1,…22
Spain	2.445 to 2.475 GHz	f=2.449 + + n MHz, n=0,1,…22
France	2.4465 to 2.4835 GHz	f=2.454 + + n MHz, n=0,1,…22

Physical Links

- 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
  - Considered as symmetric connection
- Asynchronous connectionless (ACL)
  - Only single ACL link can exist
  - ACL link can be used for broadcasting packet
  - Most ACL packet applies retransmission to assure data integrity
- Extended Synchronous connection oriented (eSCO)
  - Reserves slots just like SCO, but these can be asymmetric connection
  - Retransmissions are supported

Bluetooth Baseband format



Bluetooth Packet Field

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

Bluetooth Packet Header Field

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

Bluetooth Packet Type

Segment	TYPE code $b_3b_2b_1b_0$	Slot occupancy	SCO link	ACL link
1	0000	1	NULL	NULL
	0001	1	POLL	POLL
	0010	1	FHS	FHS
	0011	1	DM1	DM1
2	0100	1	undefined	DH1
	0101	1	HV1	undefined
	0110	1	HV2	undefined
	0111	1	HV3	undefined
	1000	1	DV	undefined
	1001	1	undefined	AUX1
3	1010	3	undefined	DM3
	1011	3	undefined	DH3
	1100	3	undefined	undefined
	1101	3	undefined	undefined
4	1110	5	undefined	DM5
	1111	5	undefined	DH5

Bluetooth Packet Header Field

- Payload header
  - L_CH field – identifies logical channel
    - LMP Message
    - Un-fragmented L2CAP
    - Continuation of fragmented L2CAP
    - Other
  - 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

Bluetooth Error Correction Scheme

- 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

Example of Retransmission Operation