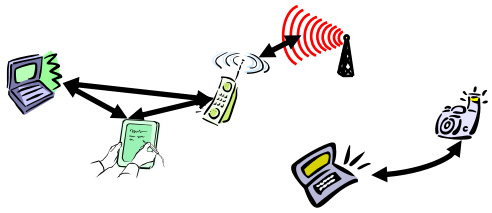
MOBILE COMPUTING

CSE 40814/60814
Spring 2021

Bluetooth

- Basic idea
  - Universal radio interface for ad-hoc wireless connectivity
  - Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
  - Embedded in other devices, very cheap
  - Short range (10m), low power consumption, license-free 2.45 GHz ISM
  - Voice and data transmission, approx. 1 Mbit/s data rate



Bluetooth

- History
  - 1994: Ericsson (Mattison/Haartsen), “MC-link” project
  - Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
  - 1998: foundation of Bluetooth SIG, www.bluetooth.org
  - 2001: first consumer products for mass market, spec. version 1.1 released
  - 2005: 5 million chips/week
- Special Interest Group
  - Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
  - Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
  - > 10000 members
  - Common specification and certification of products

Characteristics

- **2.4 GHz** ISM band, **79 RF channels**, 1 MHz carrier spacing
  - Channel 0: 2402 MHz … channel 78: 2480 MHz
  - GFSK modulation, 1-100 mW transmit power
- FHSS and TDD
  - **Frequency hopping** (spread spectrum) with 1600 hops/s
  - Hopping sequence in a pseudo random fashion, determined by a master
  - Time division duplex for send/receive separation
- **Voice link – SCO** (Synchronous Connection Oriented)
  - **FEC (forward error correction)**, no retransmission, 64 kbit/s duplex, point-to-point, circuit switched
- **Data link – ACL** (Asynchronous Connection Less)
  - Asynchronous, acknowledgments, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched
- Topology
  - Overlapping piconets (stars) forming a scatternet

Bluetooth Piconets

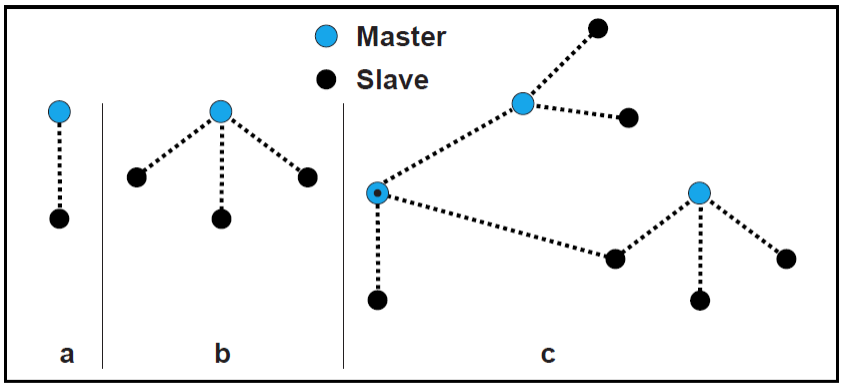
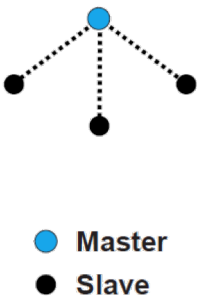


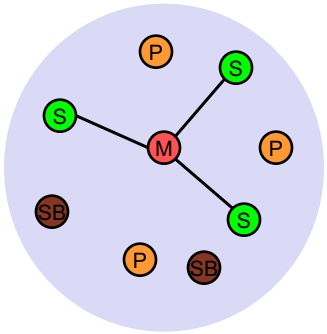
Figure 1.1: Piconets with a single slave operation (a), a multi-slave operation (b) and a scatternet operation (c).

Bluetooth Piconet

- Up to 7 slaves can be active in the piconet; many more slaves can remain connected in a parked state.
- Parked slaves are not active on the channel, but remain synchronized to the master and can become active without using the connection establishment procedure.
- If multiple piconets cover the same area, a device can participate in two or more overlapping piconets via time multiplexing.
- A device can act as a slave in several piconets, but as a master in only one piconet.
- Piconets with the same master are synchronized and use the same hopping sequence and are therefore considered the same piconet.
- A group of piconets in which connections exist between different piconets is called a scatternet.



Bluetooth Piconet

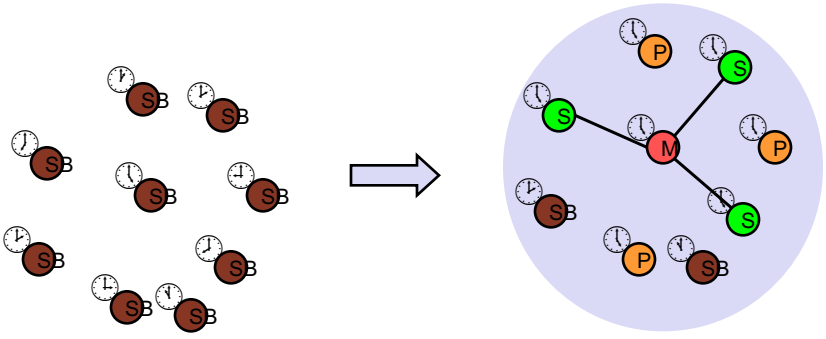


M=Master
S=Slave

P=Parked
SB=Standby

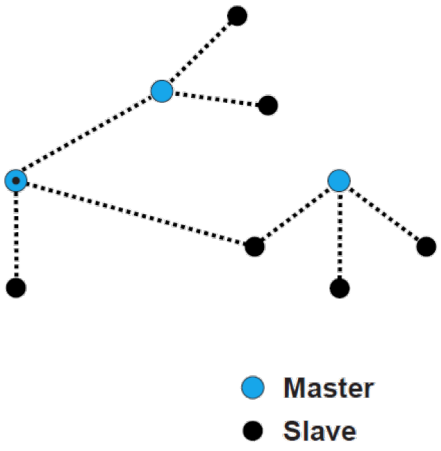
- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
    - Hopping pattern: determined by device ID (48 bit, unique worldwide)
    - Phase in hopping pattern determined by clock
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)

Bluetooth Piconet

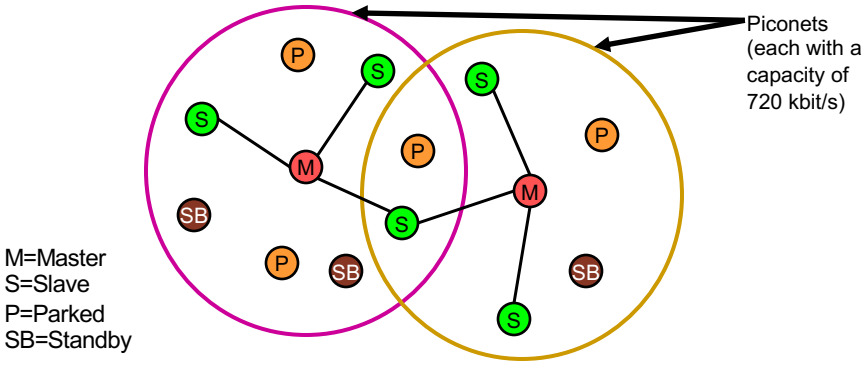


Bluetooth Scatternet

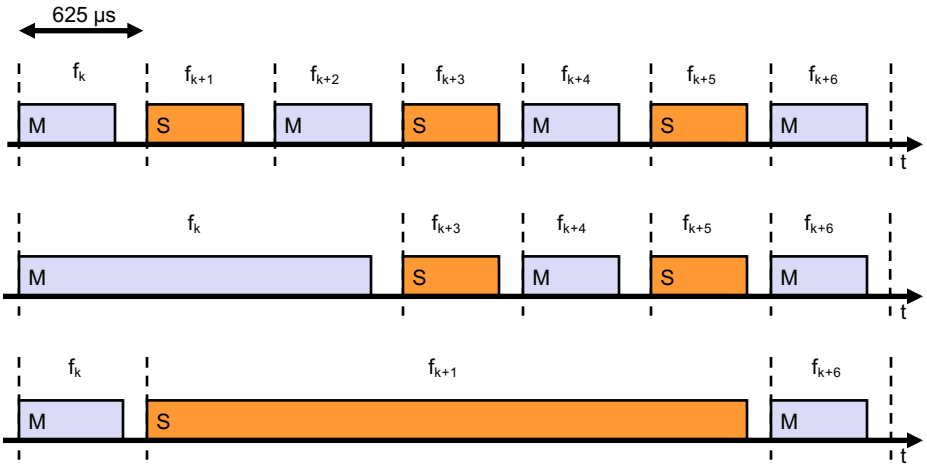
- Piconets that have common devices are called a *scatternet*.
- Each piconet has one master. Slaves can participate in different piconets on a time-division multiplex basis.
- A master in one piconet can be a slave in other piconets.
- Piconets are not frequency synchronized and each piconet has its own hopping sequence.



Scatternet

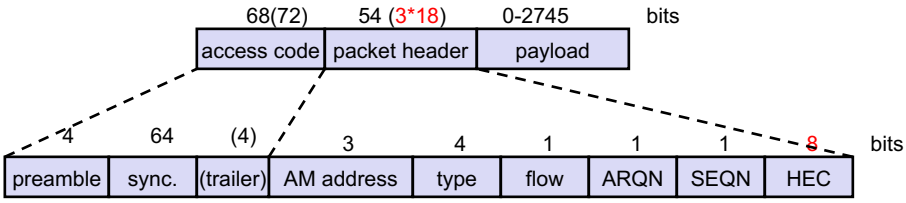


Frequency Selection

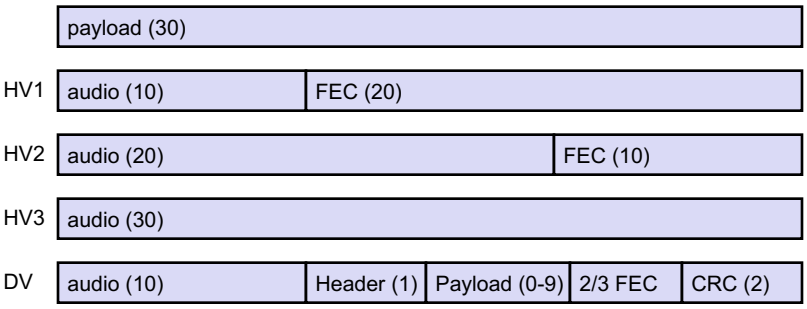


Bluetooth Packets

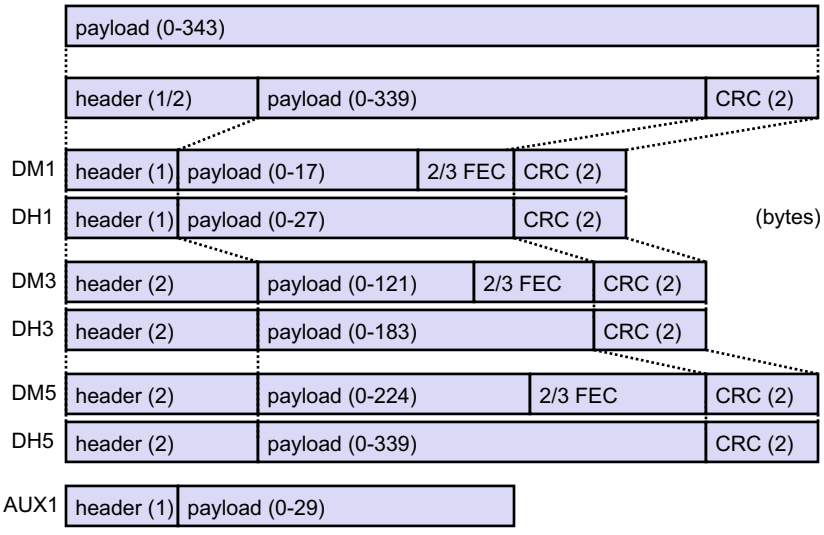
- Packet structure
  - Access code
    - Channel, device access, e.g., derived from master
  - Packet header
    - active member address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum



SCO payload types



ACL Payload types



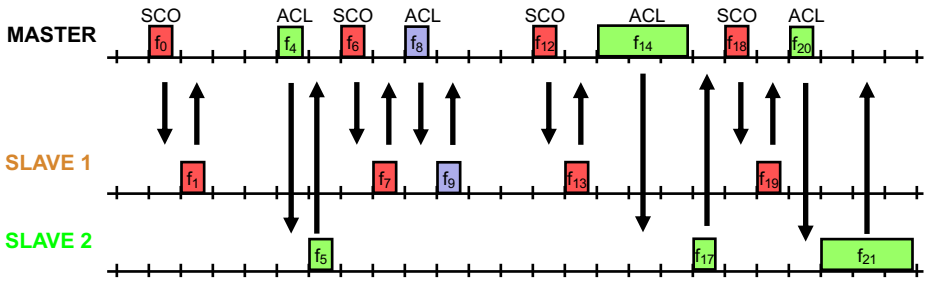
Data rates

	Type	Payload Header [byte]	User Payload [byte]	FEC	CRC	Symmetric max. Rate [kbit/s]	Asymmetric max. Rate [kbit/s] Forward	Reverse
ACL 1 slot	DM1	1	0-17	2/3	yes	108.8	108.8	108.8
	DH1	1	0-27	no	yes	172.8	172.8	172.8
3 slot	DM3	2	0-121	2/3	yes	258.1	387.2	54.4
	DH3	2	0-183	no	yes	390.4	585.6	86.4
5 slot	DM5	2	0-224	2/3	yes	286.7	477.8	36.3
	DH5	2	0-339	no	yes	**433.9**	**723.2**	57.6
	AUX1	1	0-29	no	no	185.6	185.6	185.6
SCO	HV1	na	10	1/3	no	64.0		
	HV2	na	20	2/3	no	64.0		
	HV3	na	30	no	no	64.0		
	DV	1 D	10+(0-9) D	2/3 D	yes D	64.0+57.6 D		

*D*ata *M*edium/*H*igh rate, *H*igh-quality *V*oice, *D*ata and *V*oice

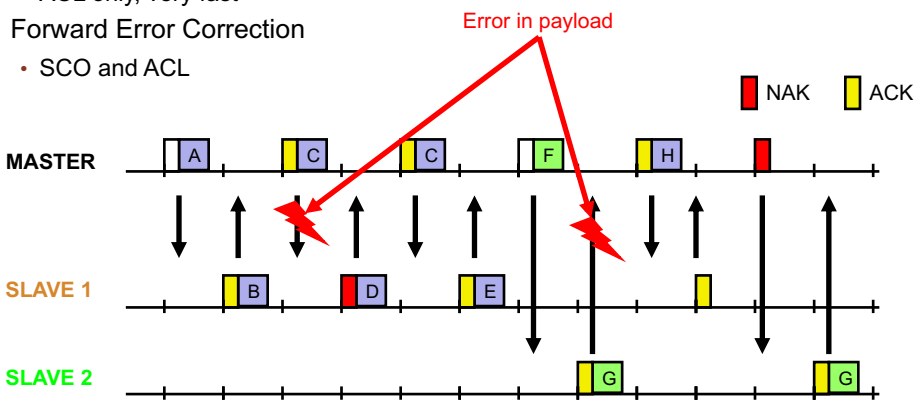
Link Types

- Polling-based TDD packet transmission
  - 625µs slots, master polls slaves
- SCO (Synchronous Connection Oriented) – Voice
  - Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point
- ACL (Asynchronous ConnectionLess) – Data
  - Variable packet size (1, 3, 5 slots), asymmetric bandwidth, point-to-multipoint



Robustness

- Slow frequency hopping with hopping patterns determined by a master
  - Protection from interference on certain frequencies
  - Separation from other piconets
- Retransmission
  - ACL only, very fast
- Forward Error Correction
  - SCO and ACL



Bluetooth Versions

- Bluetooth 1.1
  - also IEEE Standard 802.15.1-2002
  - initial stable commercial standard
- Bluetooth 1.2
  - also IEEE Standard 802.15.1-2005
  - eSCO (extended SCO): higher, variable bitrates, retransmission for SCO
  - AFH (adaptive frequency hopping) to avoid interference
- Bluetooth 2.0 + EDR (2004, no more IEEE)
  - EDR (enhanced date rate) of 3.0 Mbit/s for ACL and eSCO
  - lower power consumption due to shorter duty cycle
- Bluetooth 2.1 + EDR (2007)
  - better pairing support, e.g., using NFC
  - improved security

Bluetooth Versions

- Bluetooth 3.0 + HS (2009)
  - speeds up to 24Mbps (using co-located Wi-Fi link!)
- Bluetooth 4.0
  - Classic Bluetooth
  - Bluetooth High Speed
  - Bluetooth Low Energy
- Bluetooth Low Energy (BLE):
  - Marketed as Smart Bluetooth
  - Lower power, lower cost
  - Use in healthcare, fitness, security, entertainment devices
  - 40 channels
- Bluetooth Profiles (different types of applications)

Energy Consumption in Classic BT

- Traditional Bluetooth is **connection oriented**. When a device is connected, a link is maintained, even if there is no data flowing
- **Sniff modes** allow devices to sleep, reducing power consumption to give months of battery life (e.g., wake up every 100ms)
- Peak transmit current is typically around 25mA
- Even though it has been independently shown to be lower power than other radio standards, it is still not low enough for **coin cells** and energy harvesting applications

Bluetooth Low Energy (BLE)

- Bluetooth low energy is a new, open, short range radio technology
  - Blank sheet of paper design
  - Different to Bluetooth classic (BR/EDR)
  - Optimized for ultra low power
  - Enable coin cell battery use cases
    - < 20mA peak current
    - < 5uA average current

BLE Basic Concepts

- Everything is optimized for lowest power consumption
  - Short packets reduce TX peak current
  - Short packets reduce RX time
  - Fewer RF channels to improve discovery and connection time
  - Simple state machine
  - Single protocol
  - ...

BLE Fact Sheet

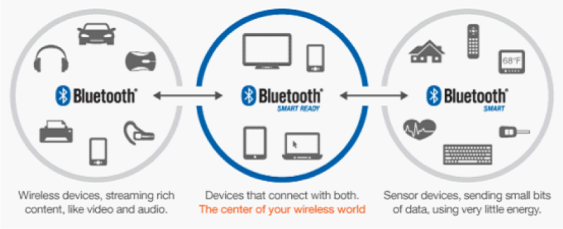
- Data Throughput
  - For Bluetooth low energy, data throughput is not a meaningful parameter. It does not support streaming
  - It has a data rate of 1Mbps, but is not optimized for file transfer
  - It is designed for **sending small chunks of data** (exposing state)

"Exposing State" (Example: IoT)

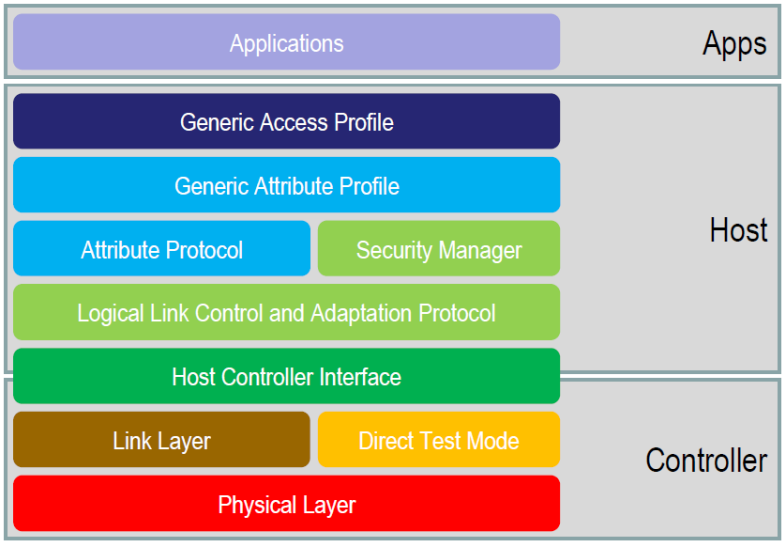
- It's good at small, discrete data transfers
- Data can triggered by local events
- Data can be read at any time by a client
- Interface model is very simple (GATT)

BLE Device Modes

- Dual Mode
  - Bluetooth BR/EDR and LE
  - Used anywhere BR/EDR is used today
- Single Mode
  - Implements only Bluetooth low energy
  - Will be used in new devices / applications

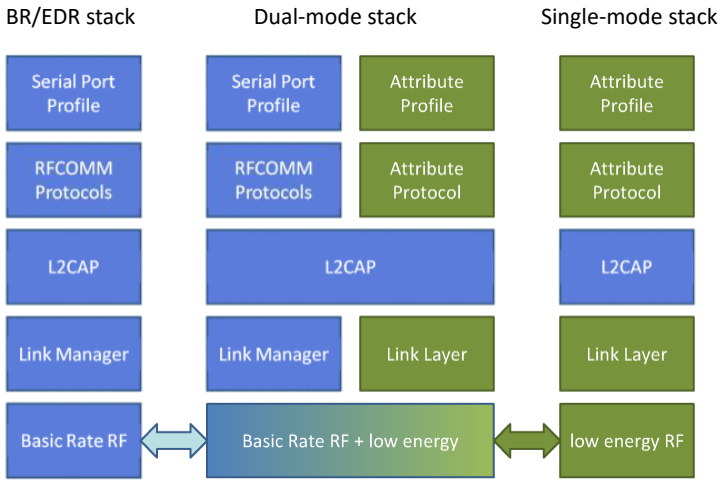


BLE Architecture



BLE Device Modes

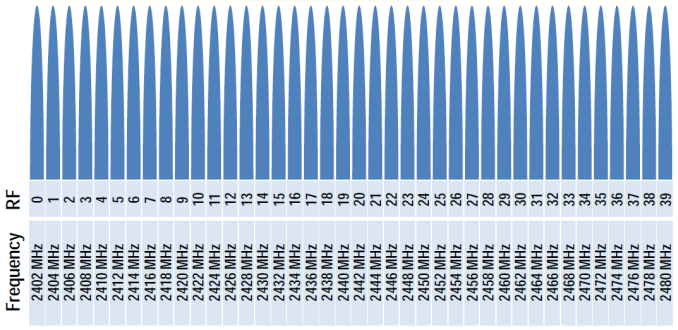
- Dual mode + single modes



BLE Physical Layer

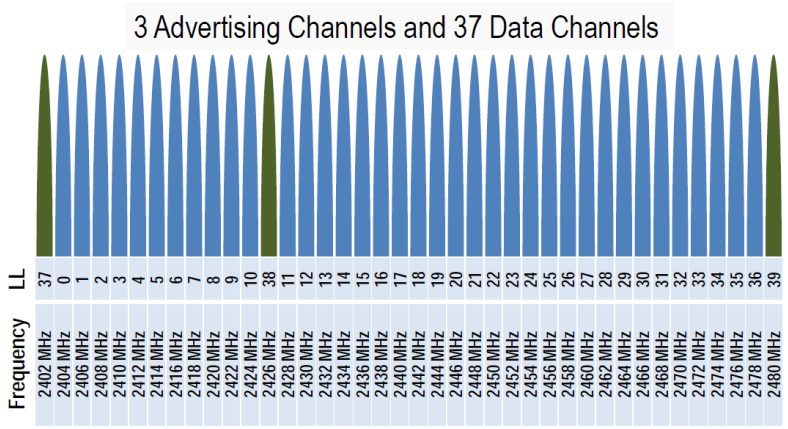
- 2.4 GHz ISM band
- 1Mbps GFSK
  - Larger modulation index than Bluetooth BR (which means better range)
- 40 Channels on 2 MHz spacing

$$f = 2402 + 2 \cdot k \text{ MHz}$$



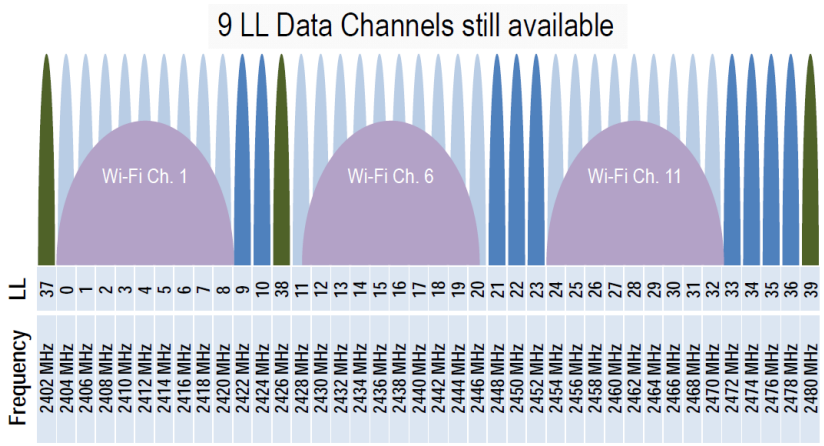
BLE Physical Layer

- Two types of channels



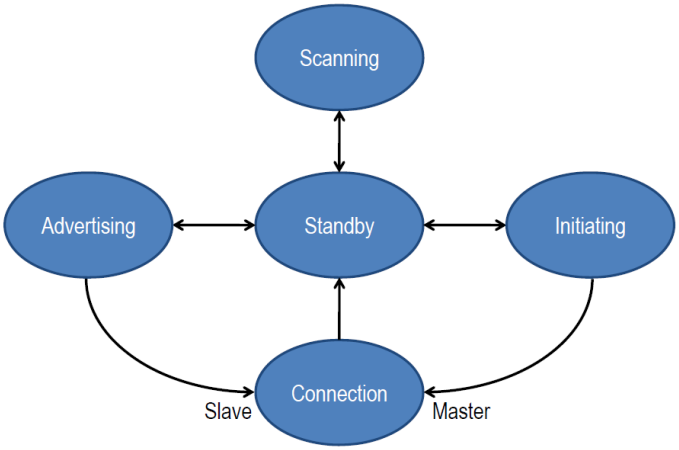
BLE Physical Layer

- Advertising channels avoid 802.11

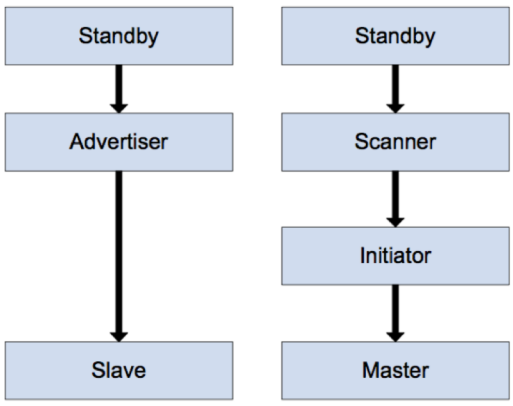


BLE Link Layer

- Link Layer state machine



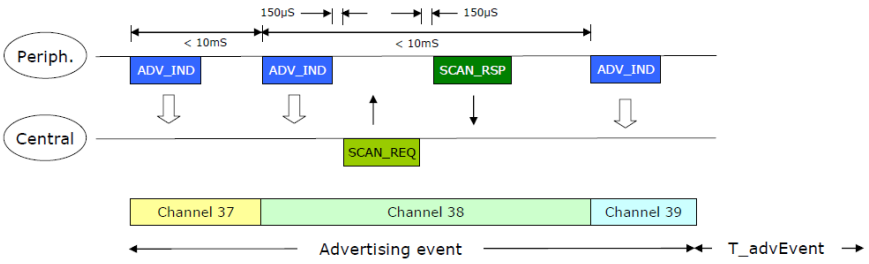
BLE Link Layer



BLE Link Layer

- Possible states:
  - **Standby**: not transmitting or receiving any data, and is not connected to any other device
  - **Advertiser**: periodically broadcasting advertisements
  - **Scanner**: actively looking for advertisers
  - **Initiator**: actively trying to initiate a connection with another device
  - **Master**: connected to another device as a master
  - **Slave**: connected to another device as a slave

BLE Advertising

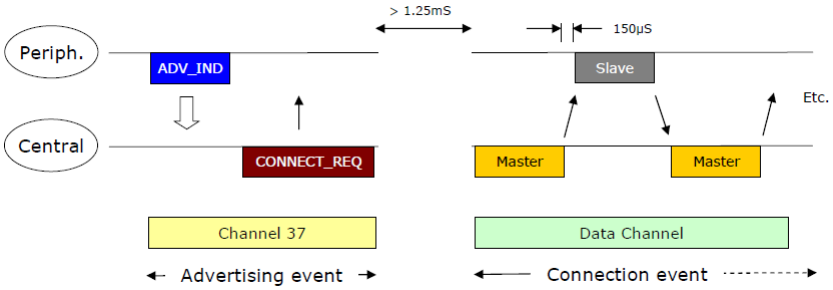


- Devices can advertise for a variety of reasons:
  - To broadcast promiscuously
  - To transmit signed data to a previously bonded device
  - To advertise their presence to a device wanting to connect
  - To reconnect asynchronously due to a local event

BLE Advertising

- Four types of advertisements:
  - **Connectable undirected**: any scanner device can initiate a connection with this advertiser
  - **Connectable directed**: only one specific device can initiate a connection with this advertiser
  - **Non-connectable undirected**: no devices can initiate a connection with this advertiser; primarily used for general broadcast of data (up to 31 bytes of payload)
  - **Discoverable undirected**: any scanner device can request more information from the advertising device, but no devices can initiate a connection with it

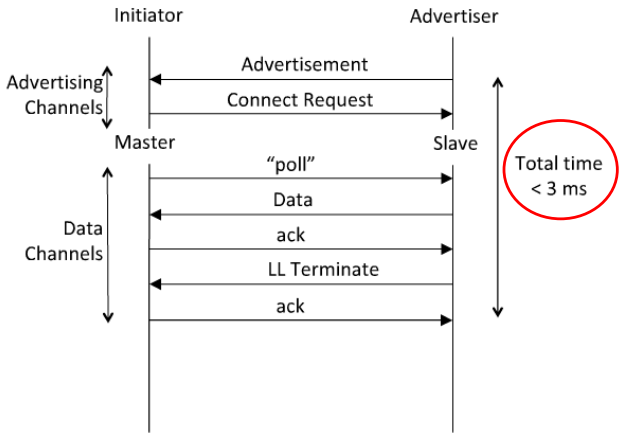
BLE Data Transfer



- Once a connection is made:
  - Master informs slave of hopping sequence and when to wake up
  - All subsequent transactions are performed on the 37 data channels
  - Transactions can be encrypted
  - Both devices can go into deep sleep between transactions

Link Layer Connections

- Very low latency connection



ZigBee

ZigBee™ Alliance
Wireless Control That Simply Works

- IEEE 802.15.4 (similar to Bluetooth and IEEE 802.15.1)
- Pushed by Chipcon (now TI), Ember, Freescale (Motorola), Honeywell, Mitsubishi, Motorola, Philips, Samsung…
- More than 260 members
  - about 15 promoters, 133 participants, 111 adopters
  - must be member to commercially use ZigBee spec
- ZigBee platforms comprise
  - IEEE 802.15.4 for layers 1 and 2
  - ZigBee protocol stack up to the applications

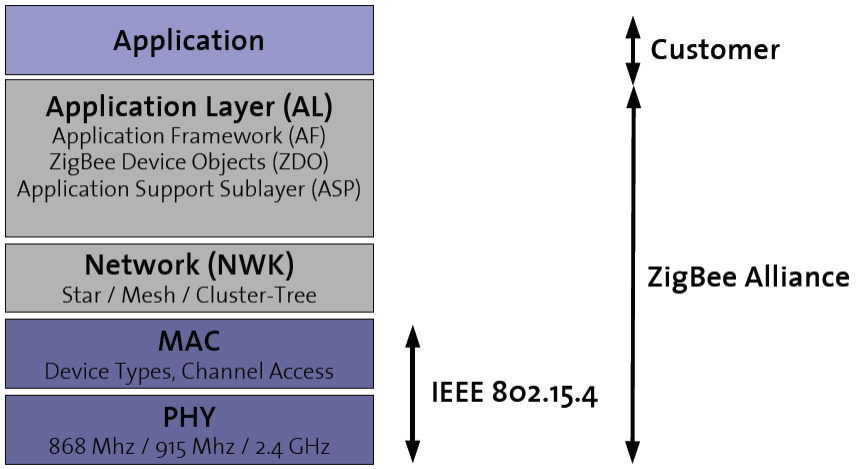
ZigBee

- Design goal
  - Low power consumption
  - Simple Design
  - Few costs
- History
  - ZigBee-style networks began ~1998
  - IEEE 802.15.4 was first completed in 2003
  - ZigBee Alliance was established in 2002

ZigBee Core Market

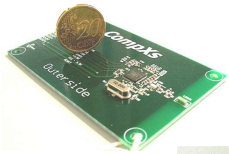
- **Industrial and Commercial**
  - Monitors
  - Movement Sensors
  - Automation
- **Personal Healthcare**
  - Patient monitors
  - Remote Diagnosis
  - Data loggers
- **Building Automation**
  - Security
  - Lighting
  - Fire and Safety systems
- **Automotive**
  - Service controls
  - Inventory tracking

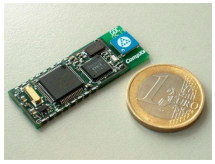
ZigBee Protocol Stack



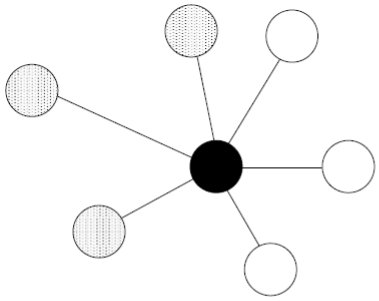
Device Type

- **Full Function Device (FFD)**
  - Network router function
  - Any Topology
- **Reduced Function Device (RFD)**
  - Easy and cheap to implement
  - Limited to star topology
- **Personal Area Network (PAN) Coordinator**
  - Maintains overall network knowledge
  - Needs most memory and computing power





Basic Topology



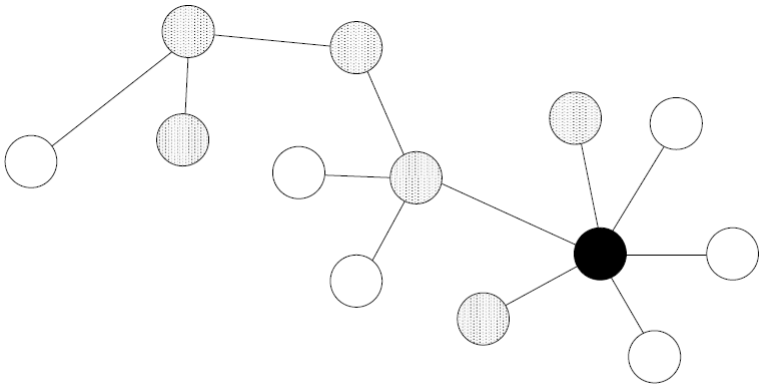
RFD / EndPoint

FFD / Router

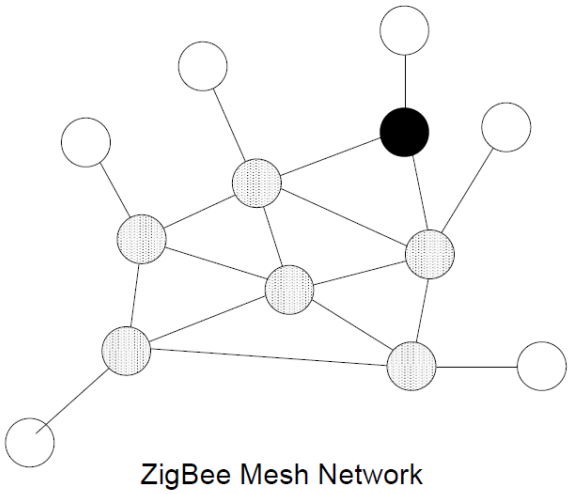
Coordinator

Star Network

Cluster Tree Network



ZigBee PRO: Mesh Network



ZigBee Mesh Network

Bluetooth vs. ZigBee

	Bluetooth (v1)	ZigBee
Protocol Stack	250 kb	< 32 kb (4kb)
Range	10 - 100 meters	30 - 100 meters
Link Rate	1 Mbps	250 kbps
Battery	rechargeable	non-rechargeable
Devices	8	2^16
Air Interface	FHSS	DSSS
Usage	frequently	infrequently
Network Join Time	long	short
Extendibility	no	yes
Security	PIN, 64 bit, 128 Bit	128 bit, AES

Comparison

Technology	Classic *Bluetooth* technology (BR/EDR)[1]	*Bluetooth* low energy technology[2]	ZigBee
Radio Frequency	2.4 GHz	2.4 GHz	2.4 GHz
Distance / Range	10 to 100 meters[3]	10 to 100 meters[3]	10 to 200 meters[4]
Over the air Data Rate	1-3Mbps	1Mbps	250kbps at 2.4 GHz.
Application Throughput	0.7-2.1 Mbps	0.2 Mbps	<0.1 Mbps
Nodes/Active Slaves	7 / 16777184[5]	Unlimited[6]	65535[7]
Security	64b/128b and applications layer user defined	128b AES and application layer user defined	128b AES and application layer user defined
Robustness	Adaptive fast frequency hopping, FEC, fast ACK	Adaptive fast frequency hopping	DSSS, Uses only 16 ch. in ISM band, optional mesh topology has long recovery time
Latency (from a non connected state)			
Total time to send data (det.battery life)[8]	100ms	<3ms	<10ms
Government Regulation	Worldwide	Worldwide	Worldwide
Certification Body	Bluetooth SIG	Bluetooth SIG	ZigBee Alliance
Voice capable	Yes	No	No
Network topology	Scatternet	Star-bus	Star or Mesh
Power Consumption	1 as the reference	0.01 to 0.5(depending on use-case)	2 (router) / 0.1 (end point)
Peak current consumption (max 15 mA to run on coin cell battery)	<30 mA	<15 mA	<15 mA
Service discovery	Yes	Yes	No
Profile concept	Yes	Yes	Yes
Primary Use Cases	Mobile phones, gaming, headsets, stereo audio streaming, automotive, PCs, consumer electronics, etc.	Mobile phones, gaming, PCs, watches, sports & fitness, healthcare, automotive, consumer electronics, automation, industrial, etc.	Fixed location industrial, building & home automation, AMI/SmartEnergy