Internet of Things: Protocols and Networks

(CSC2106)

Bluetooth Low Energy (BLE)

Recent Protocols for IoT

SINGAPORE INSTITUTE OF TECHNOLOGY

Session	**MQTT**, SMQTT, CoRE, DDS, AMQP , XMPP, **CoAP**, IEC,…	**Security**	**Management**
Network	Encapsulation **6LowPAN**, 6TiSCH, 6Lo, Thread…	IEEE 1888.3, TCG, Oath 2.0, SMACK, SASL, EDSA, ace, DTLS, Dice, …	IEEE 1905, IEEE 1451, IEEE 1377, IEEE P1828, IEEE P1856
	Routing RPL, CORPL, CARP		
Datalink	**WiFi**, **802.11ah**, **Bluetooth Low Energy (BLE)**, **Z-Wave, ZigBee Smart**, DECT/ULE, 3G/LTE, NFC, Weightless, HomePlug GP, 802.15.4e, G.9959, WirelessHART, DASH7, ANT+, LTE-A, **LoRaWAN**, ISA100.11a, DigiMesh, WiMAX, …		

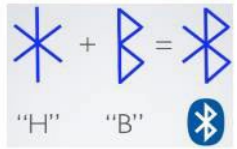
Bluetooth

- Started with Ericsson's Bluetooth Project in 1994 for radio-communication between cell phones over short distances
- Named after Danish king Herald Blatand (AD 940-981)[1]
- Intel, IBM, Nokia, Toshiba, and Ericsson formed Bluetooth SIG in May 1998
- Version 1.0A of the specification came out in late 1999
- IEEE 802.15.1 approved in early 2002 is based on Bluetooth. Later versions handled by Bluetooth SIG directly
- Key Features at **time of launch** in 1999-2000:
  - Lower Power: 10 mA in standby, 50 mA while transmitting
  - Cheap: $5 per device
  - Small: 9 mm2 single chips

1. https://www.bluetooth.com/about-us/bluetooth-origin/#:~:text=Surprisingly%2C%20the%20name%20dates%20back,earned%20him%20the%20nickname%20Bluetooth.

History

ERICSSON intel NOKIA



4.0 Bluetooth®

Bluetooth 5

Go Faster. Go Further.

Bluetooth 5.2

Bluetooth Core Specification v5.1

1994-97 | 2006 | 2010 | 2011-2012 | 2015 | 2016 | 2019 | 2020

TraceTogether

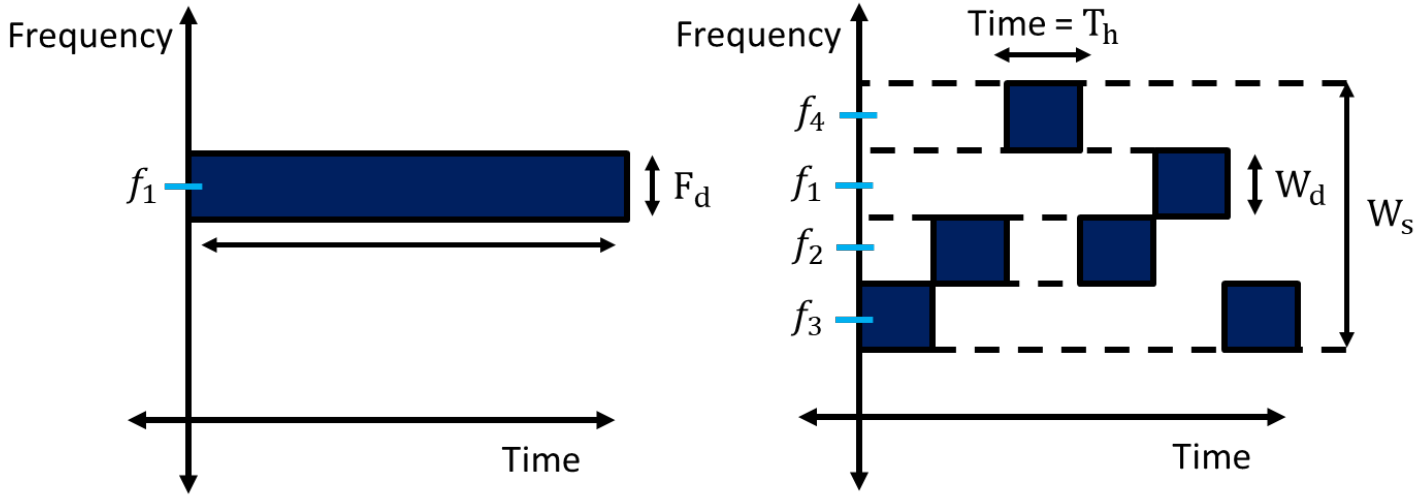
2020

Bluetooth Versions

Bluetooth Versions	Remarks
Bluetooth 1.1	IEEE 802.15.1-2002
Bluetooth 1.2	IEEE 802.15.1-2005. Completed Nov 2003. Extended SCO, Higher variable rate retransmission for SCO + Adaptive frequency hopping (avoid frequencies with interference)
Bluetooth 2.0	+ Enhanced Data Rate (EDR) (Nov 2004): 3 Mbps using DPSK. For video applications. Reduced power due to reduced duty cycle
Bluetooth 2.1	+ EDR (July 2007): Secure Simple Pairing to speed up pairing
Bluetooth 3.0	+ High Speed (HS) (April 2009): 24 Mbps using Wi-Fi PHY + Bluetooth PHY for lower rates
Bluetooth 4.0	(June 2010): Low energy. Smaller devices requiring longer battery life (several years). New incompatible PHY Bluetooth Smart or BLE
Bluetooth 4.1	4.0 + Core Specification Amendments (CSA) 1, 2, 3, 4
Bluetooth 4.2	(Dec 2014): Larger packets, security/privacy, IPv6 profile
Bluetooth 5	(2016): quadruples the wireless range, doubles speed, and broadcasting to two wireless devices at once.

Frequency Hoping Spread Spectrum (FHSS)

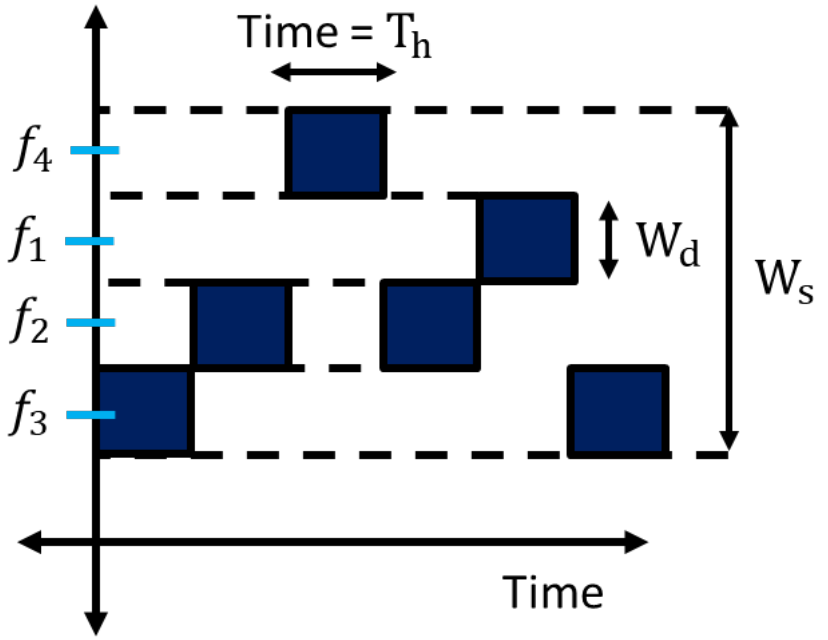
- FHSS: The type of spread spectrum in which carrier hops randomly from one frequency to another.



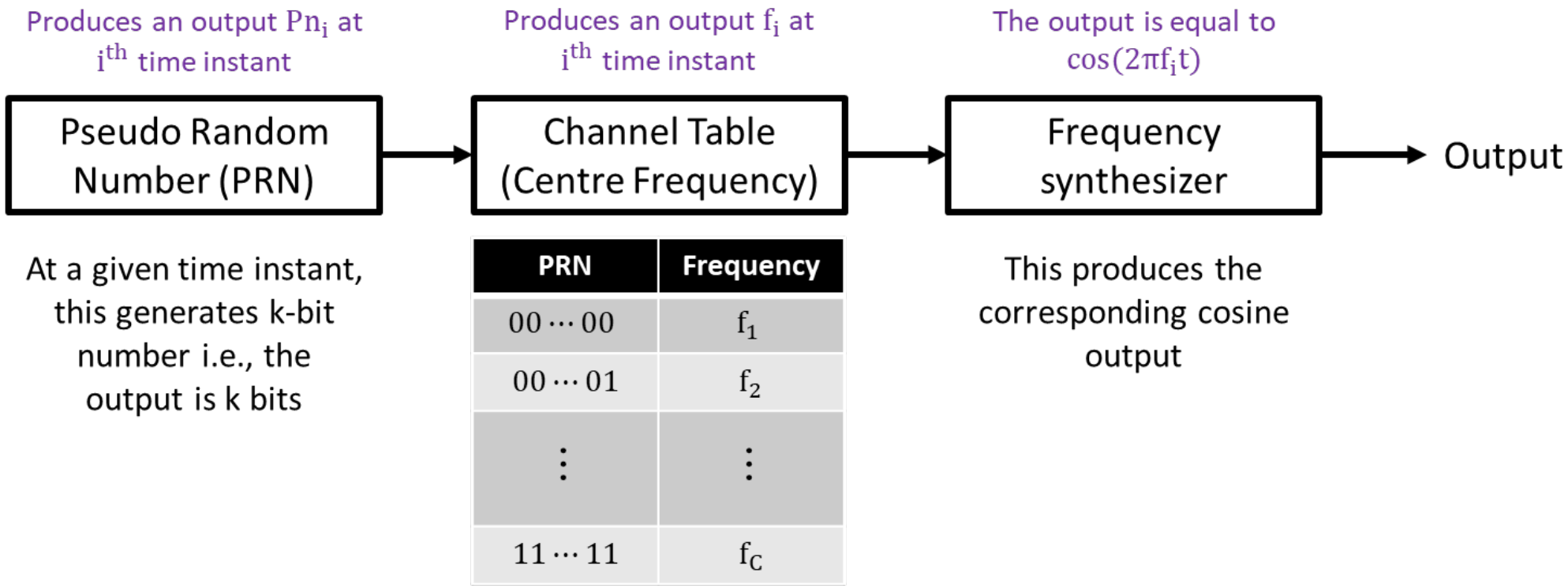
- Symbol definitions:
  - T_h → Hopping Time, W_d → Signal Bandwidth, W_s → Spread Spectrum bandwidth, C → number of carrier frequencies (or channels allocated for the FH signal)
  - Note that $W_s = CW_d$

Frequency Hoping Spread Spectrum (FHSS)

- Channel sequence, $\{f_3, f_2, f_4, f_2, f_1, f_3, \cdots\}$, is a random series of radio frequencies.
- The sequence of channels used is dictated by a spreading code.
- The number of carrier frequencies i.e., C is equal to 4.
- Note that both transmitter and receiver use the same code to tune into a sequence of channels in synchronization.
- The transmitter operates in one channel at a time for a fixed interval
- At each successive interval, a new carrier frequency is selected



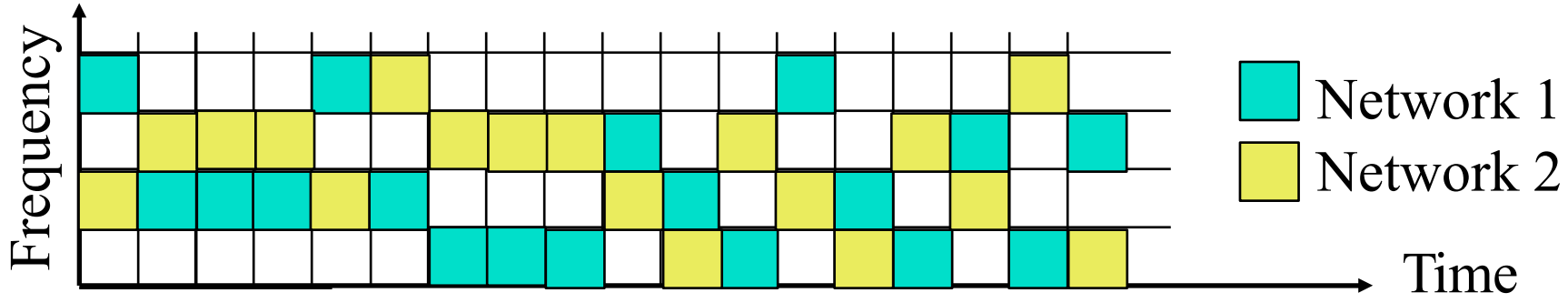
Generating the Frequency Sequence



- Point to be Noted:
  - Using a k-bit PRN generator, we can have a maximum of 2^k carrier frequencies or channels.

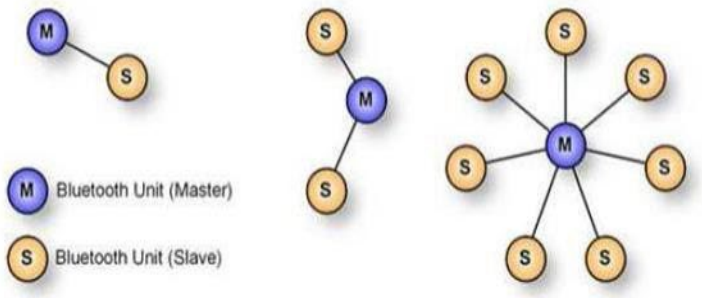
Bluetooth Classic: Details

- **Frequency Range:** 2402 - 2480 MHz
  - Total 79 MHz band
  - 23 MHz in some countries, e.g., Spain, France and Japan
- **Data Rate:** 1 Mbps using 1 MHz (Nominal) 720 kbps (User)
- **Frequency Hopping Spread Spectrum:** 1600 times/s → 625 us/hop (microseconds/hop)
  - Hopping Sequence decided using PRN generator agreed upon between master and slave
- **Security:** Challenge/Response Authentication. 128b Encryption
- **TX Output Power:**
  - Class 1: 20 dBm Max. (0.1W) – 100m
  - Class 2: 4 dBm (2.5 mW)
  - Class 3: 0 dBm (1mW) – 10m



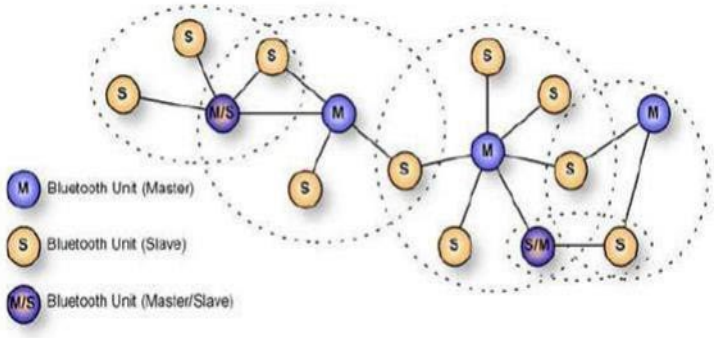
Ref: http://www.bluetooth.com/, http://www.bluetooth.org/, http://grouper.ieee.org/groups/802/15/index.html

Topology



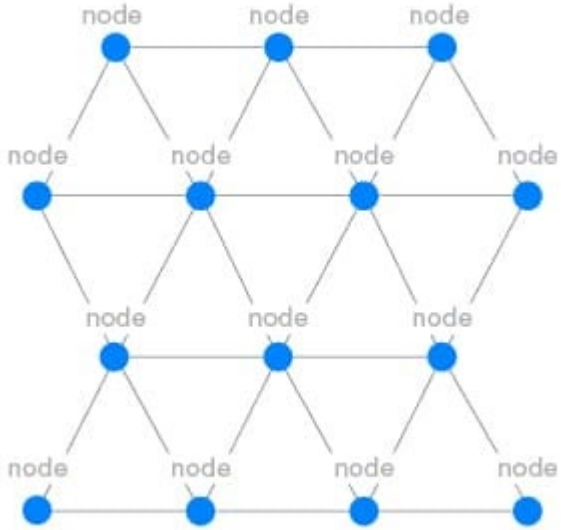
Piconet v4.0

Up to 7 active slave per master..
Up to 255 'parked' slaves per master



Scatter net v4.1

Multiple piconets joined to form Scatternet

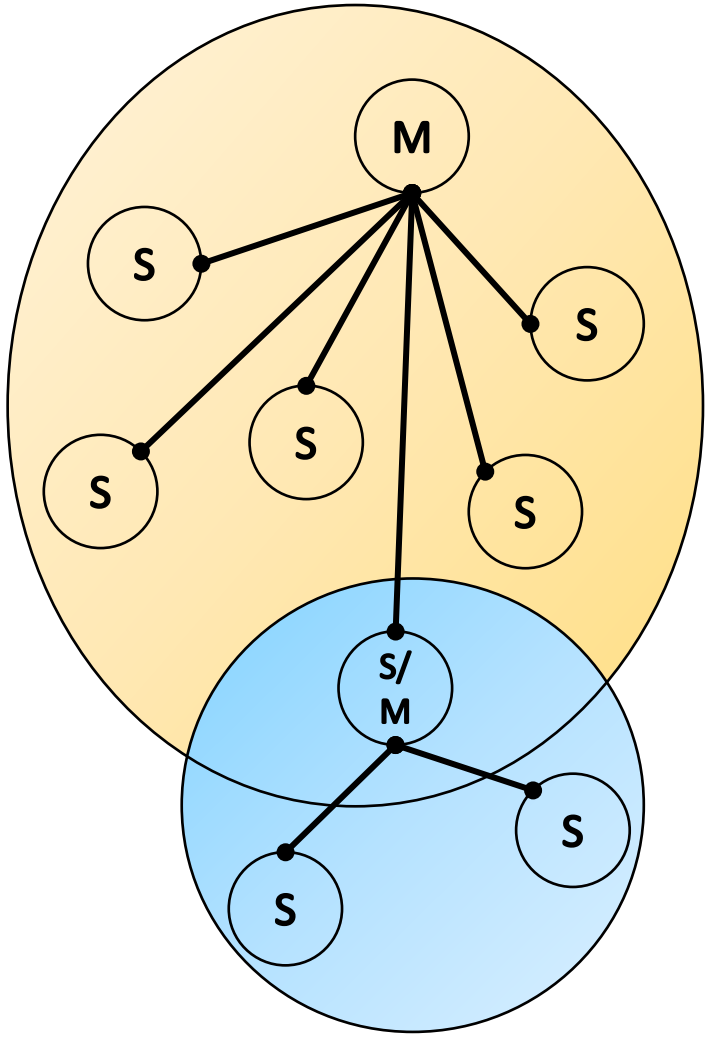


Bluetooth Mesh v5.0

Bluetooth Mesh: https://www.bluetooth.com/blog/the-fundamental-concepts-of-bluetooth-mesh-networking-part-1/

Topology contd …

- Piconet is formed by a master and many slaves
  - Basic unit of Bluetooth networking
  - Up to 7 active slaves and up to 255 Parked slaves.
  - Slaves can only transmit when requested by master
- Active slaves are polled by master for transmission
- Each station gets an 8-bit parked address
  - 255 parked slaves/piconet
- The parked station can join in 2us. Other stations can join in more time.
- Uses FHSS – TDD. Master determines the following:
  - Frequency-hopping sequence
  - Timing offset, i.e., when to transmit
- A Bluetooth node can be both a master in one piconet and slave in another.



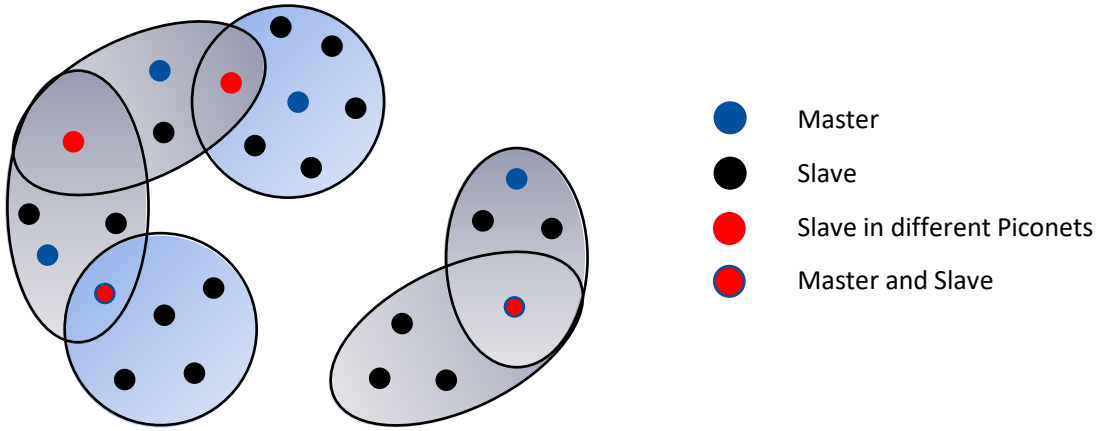
Ref: P. Bhagwat, "Bluetooth Technology for short range wireless Apps," IEEE Internet Computing, May-June 2001, pp. 96-103

Bluetooth – Channel Acess

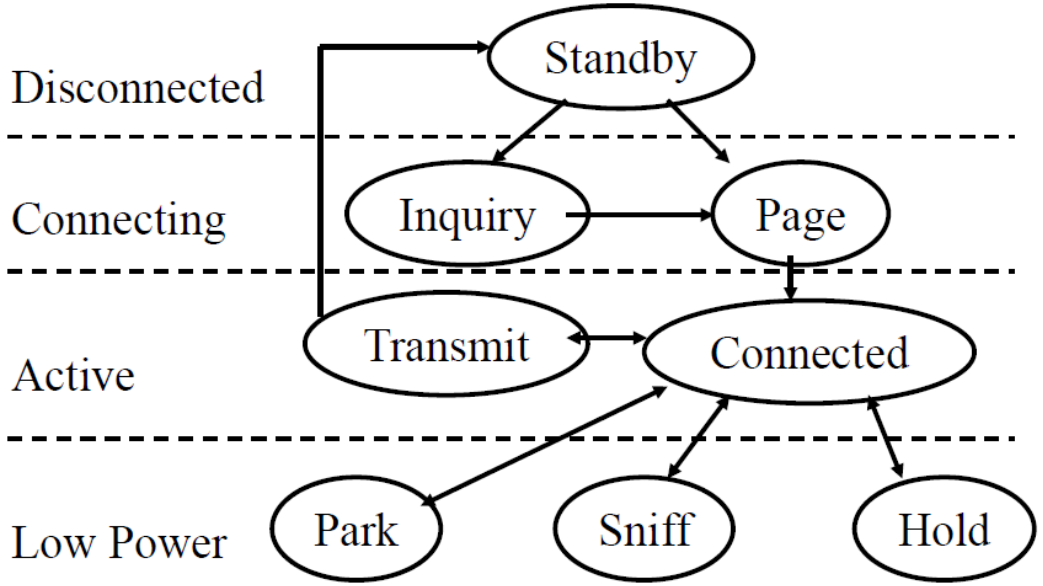
- Frequency Hopping Spread Spectrum
  - Total bandwidth divided into 1MHz physical channels
  - Hopping sequence shared with all devices on piconet
  - Maximum Radio Frequency Hopping:
    - 1600 times per second
    - Minimum Hop Time is equal to 625 microseconds
    - Slot Time is equal to 625 microseconds
  - Packets = 1 slot, 3 slot, or 5 slots long
  - The frequency hop is skipped during a packet.
- TDD:
  - Master starts in even numbered slots only.
  - Slaves start in odd numbered slots only.

Topology contd …

- Scatternet:
  - Device in one piconet can exist as master or slave in another piconet
  - Allows many devices to share same area
  - Makes efficient use of bandwidth
  - Main Disadvantage:
    - Collisions can occur when devices in different piconets use the same Frequency Hopping Sequence



Bluetooth Operational States

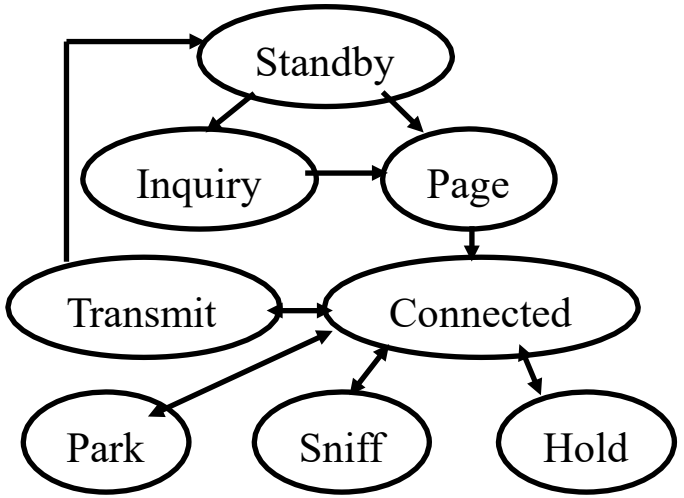


- **Standby**: Initial state
- **Inquiry**: Master sends an inquiry packet. Slaves scan for inquiries and respond with their address and clock after a random delay (CSMA/CA – Carrier Sense Multiple Access/Collision Avoidance)

https://ecee.colorado.edu/~ecen4242/marko/Bluetooth/Bluetooth/SPECIFICATION/Baseband.htm#:~:text=2.3.,-3%20Connection%20Modes&text=A%20Bluetooth%20device%20in%20the,and%20from%20the%20different%20slaves.

Bluetooth Operational States contd …

- **Page**: Master in page state invites devices to join the piconet. Page message is sent in 3 consecutive slots (3 frequencies). Slave enters page response state and sends page response including its device access code.
- Master informs slave about its clock and address so that slave can participate in piconet. Slave computes the clock offset.
- **Connected**: A short 3-bit logical address is assigned
- **Transmit**



Ref: http://www.cse.wustl.edu/~jain/cse574-20/

Energy Management in Bluetooth

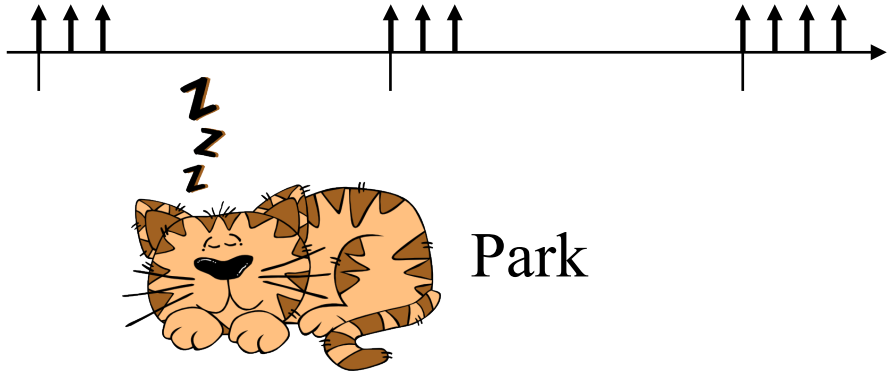
Three inactive states:

1. **Hold**: No Asynchronous Connection List (ACL). Synchronous Connection Oriented (SCO) continues.

   Node can do something else: scan, page, inquire

2. **Sniff**: Low-power mode. Slave listens after fixed sniff intervals.
3. **Park**: Very Low-power mode. Gives up its 3-bit active member address and gets an 8-bit parked member address. Wake up periodically and listen to beacons. Master broadcasts a train of beacons periodically

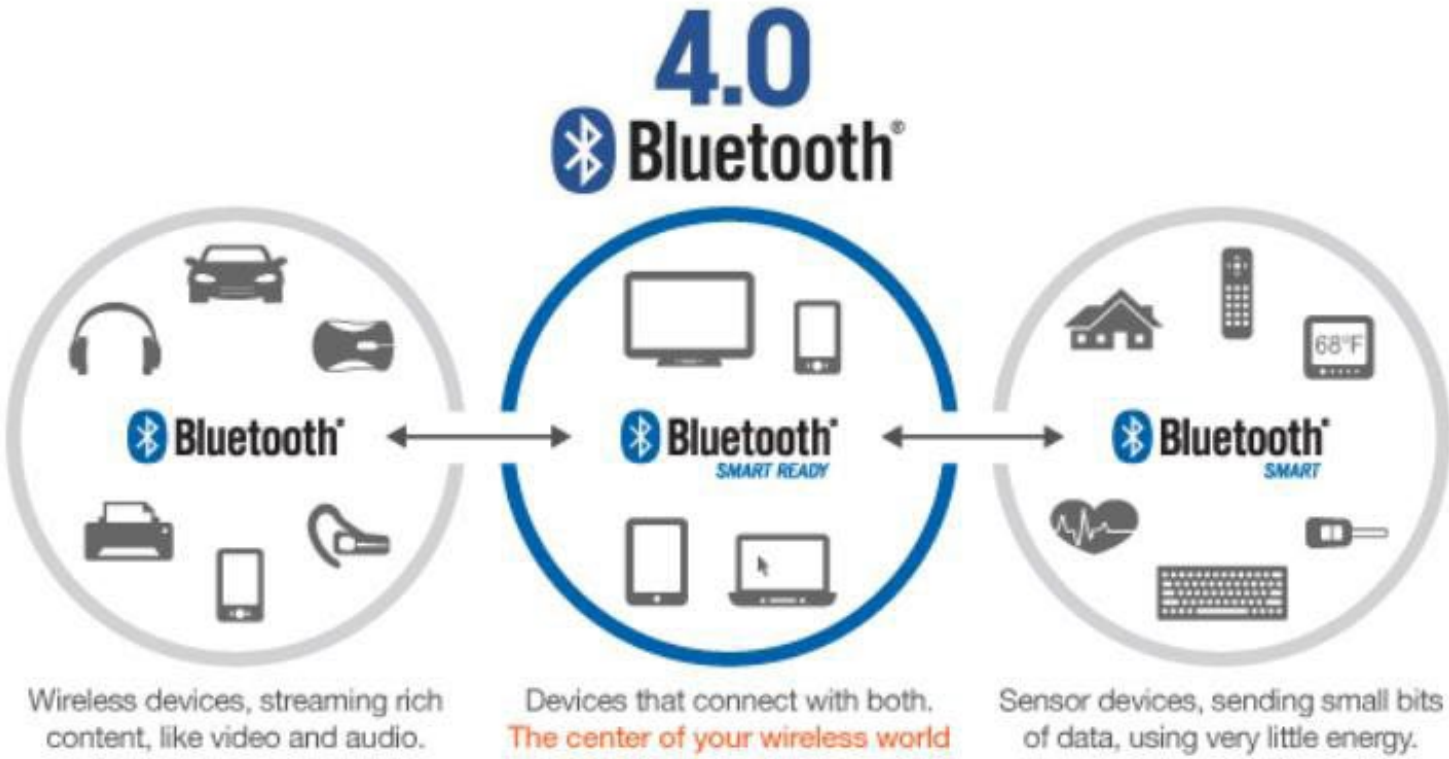
Sniff



Park

Bluetooth 4.x

- Bluetooth 4.0
- Bluetooth Low Energy
  - BLE, BTLE, LE
- SIG Preferred
  - Bluetooth Smart
  - Bluetooth Smart Ready



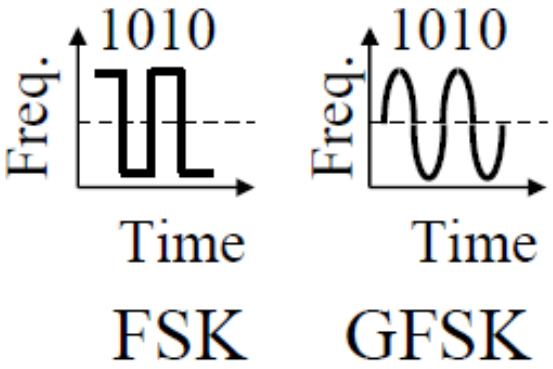
Bluetooth 4.2 ‘Smart’

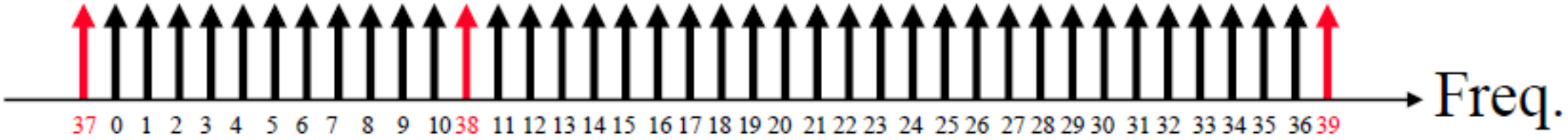
- **Low Energy**: 1% to 50% of Bluetooth classic
- **For short broadcast**: Your body temperature, Heart rate, Wearables, **sensors**, automotive, industrial

  Not for voice/video, file transfers, …
- **Small messages**: 1Mbps data rate but throughput not critical
- **Battery life**: In years from coin cells
- **Simple**: Star topology. No scatter nets, mesh, …
- **Lower cost** than Bluetooth classic
- New protocol design based on Nokia’s **WiBree** technology Shares the same 2.4GHz radio as Bluetooth
  - ➢ Dual mode chips
- All new smart phones (iPhone, Android, …) have dual-mode chips

Bluetooth 4.2 ‘Smart’ PHY

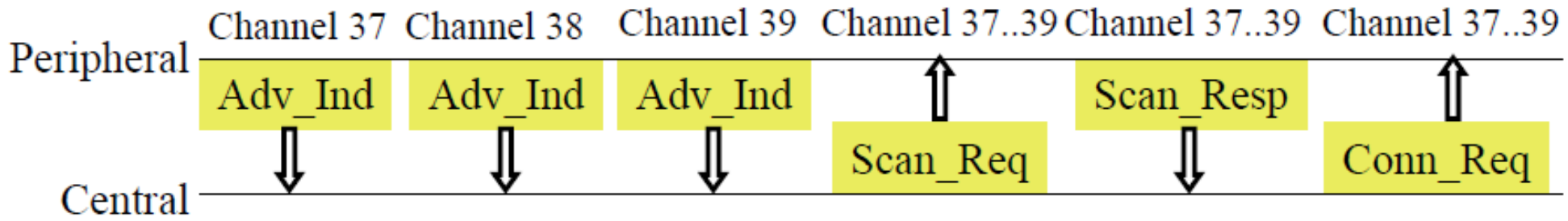
- 2.4 GHz. 150 m open field
- Star topology
- 1 Mbps Gaussian Frequency Shift Keying Better range than Bluetooth classic
- Adaptive Frequency hopping. **40 Channels with 2 MHz** spacing
- 3 channels reserved for advertising and 37 channels for data
- Advertising channels specially selected to avoid interference with Wi-Fi channels





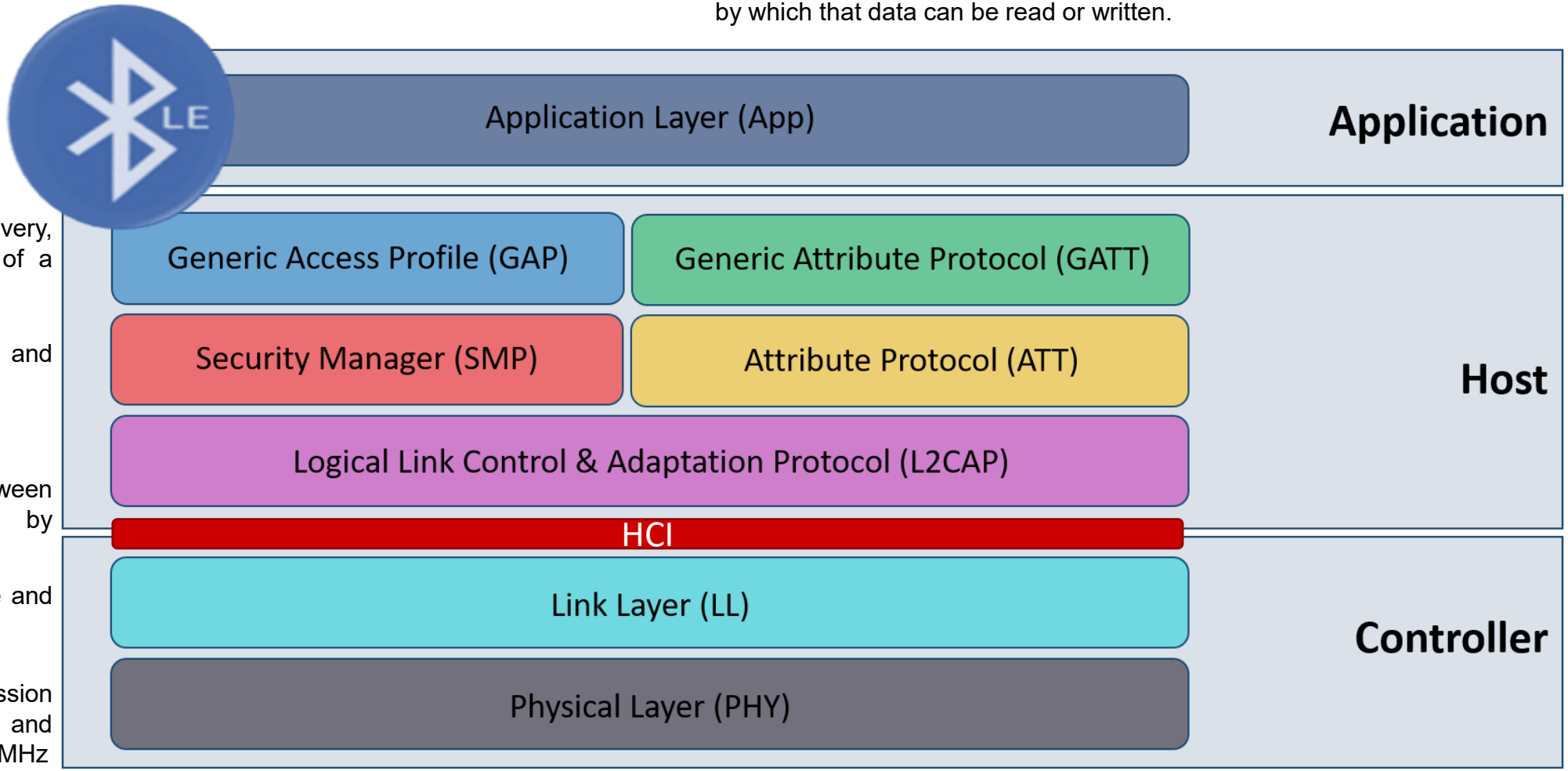
Bluetooth 4.2 'Smart' MAC

- Two Device Types: "**Peripherals**" simpler than "**central**"
- Two PDU Types: Advertising, Data
- **Non-Connectable Advertising**: Broadcast data in clear
- **Discoverable Advertising**: Central may request more information. Peripheral can send data without connection
- **General Advertising**: Broadcast presence wanting to connect. Central may request a short connection.
- **Directed Advertising**: Transmit signed data to a previously connected master



Bluetooth Smart Protocol Stack

ATT: It defines how data is represented in a BLE server database and the methods by which that data can be read or written.



GAP: responsible for device discovery, determines the network topology of a BLE system

SMP: Pairing, Authentication and Encryption

HCI enables interoperability between hosts and controllers produced by different manufacturers

Link Layer defines packet structure and control

PHY Layer takes care of transmission and receiving, modulation and demodulation, etc. 40 channels of 2MHz

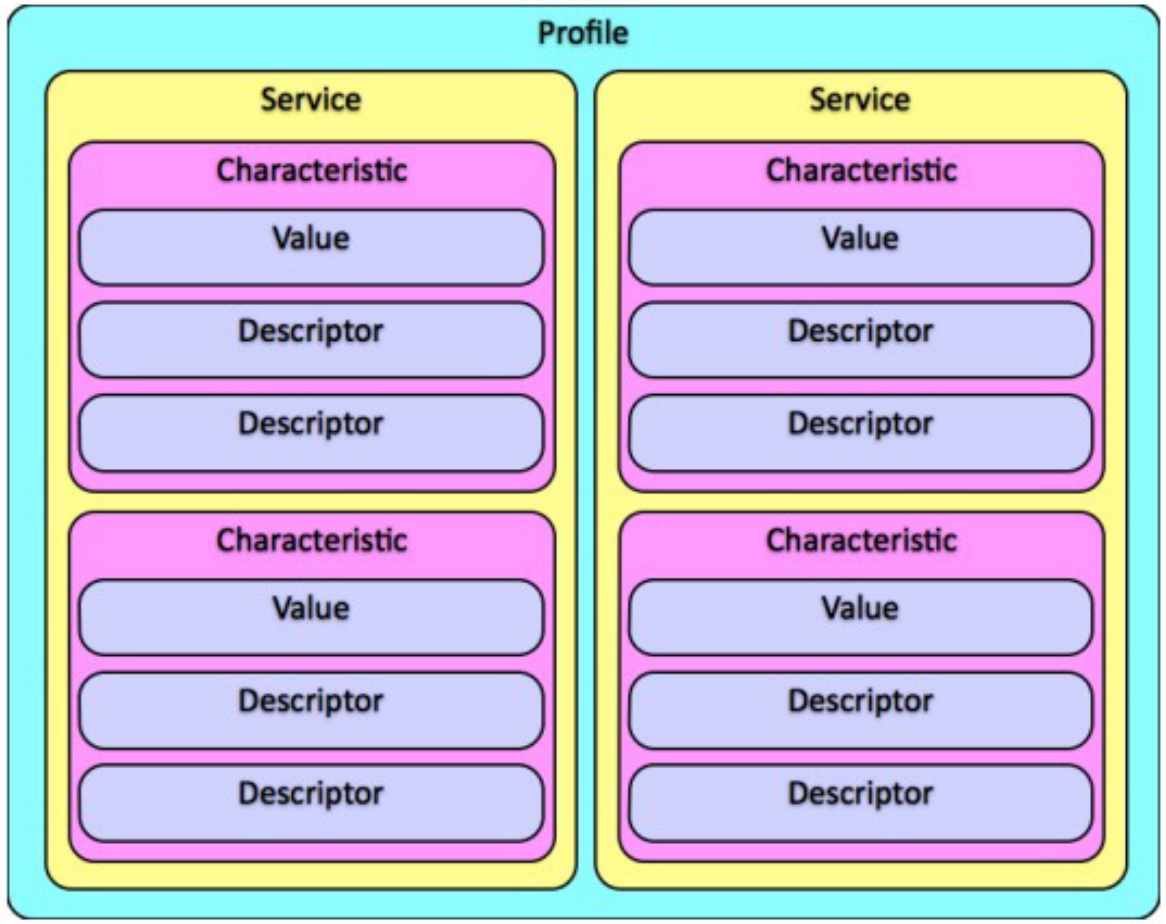
L2CAP: Multiplexing of different application protocols, Segmentation and reassembly of data packets, Controls peak bandwidth, latency, and delay variation

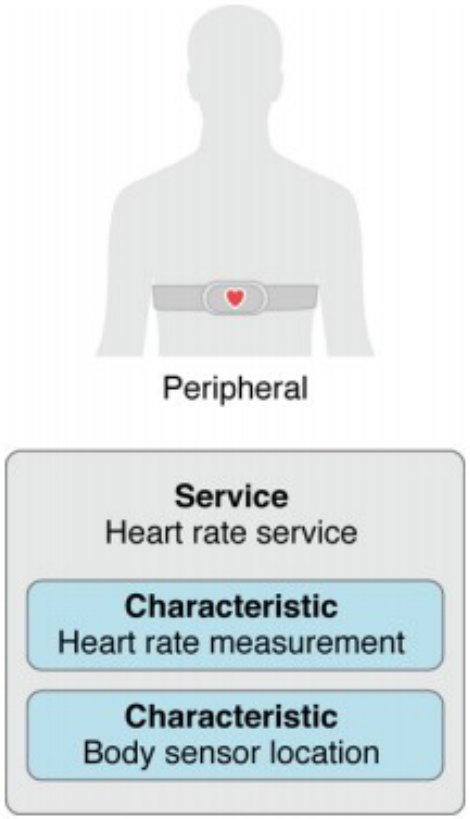
Application Profile Examples

- A2DP Advanced Audio Distribution Profile
- Global Navigation Satellite System Profile
- Hands-Free Profile
- Phone Book Access Profile
- SIM Access Profile
- Synchronization Profile
- Video Distribution Profile
- Blood Pressure Profile
- Cycling Power Profile
- Find Me Profile
- Heart Rate Profile
- Basic Printing Profile
- Dial-Up Networking Profile
- File Transfer Profile

Ref: Bluetooth SIG, "Adopted Bluetooth Profiles, Services, Protocols and Transports," https://www.bluetooth.org/en-us/specification/adopted-specifications

Generic Attribute Profile - GATT





Services, characteristics, and descriptors are collectively referred to as *attributes*, and identified by UUIDs.
16 bits (e.g. "**180A**") or 128 bits (e.g. "**6BCF0ED3-68E3-4804-96D5-5AB8765FB9BC** ")

GATT Operations

- Central can
  - discover Universally Unique IDs (UUIDs) for all primary services
  - Find a service with a given UUID
  - Find secondary services for a given primary service
  - Discover all characteristics for a given service
  - Find characteristics matching a given UUID
  - Read all descriptors for a particular characteristic
  - Can do read, write, long read, long write values etc.
- Peripheral
  - Notify or indicate central of changes

Security

- Encryption (128 bit AES)
- Pairing (Without key, with a shared key, out of band pairing)
- Passive eavesdropping during key exchange (but fixed in Bluetooth 4.2)
- Many products are building their own security on top of BLE

Extra Reading: https://www.digikey.com/eewiki/display/Wireless/A+Basic+Introduction+to+BLE+Security

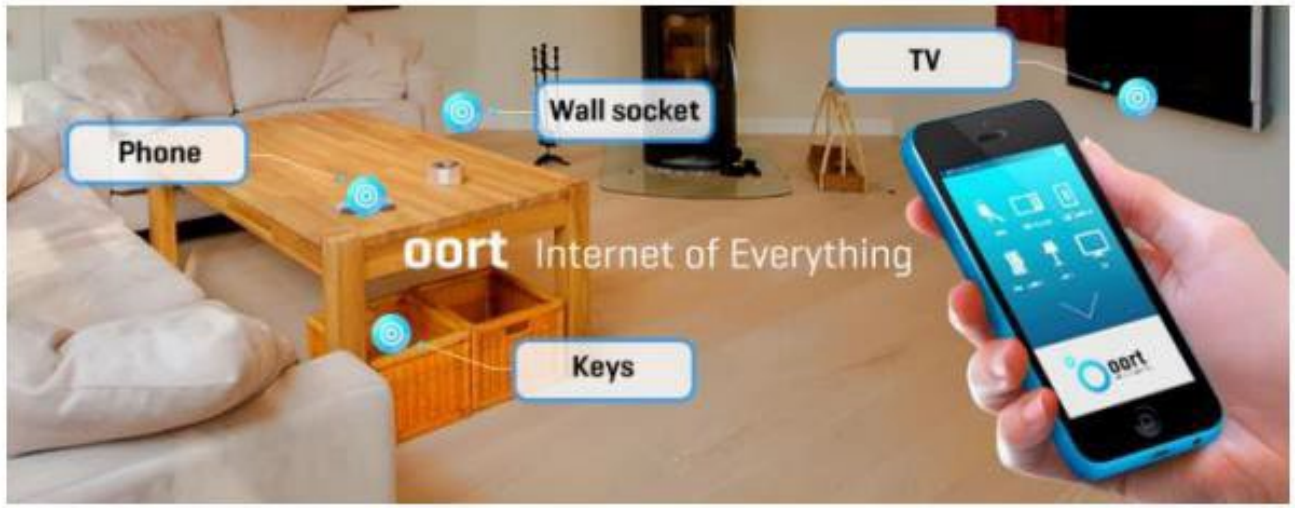
Bluetooth Smart Applications

- Proximity: In car, In room SR6A, In SIT
- Locator: Keys, watches, Animals
- Health devices: Heart rate monitor, physical activities monitors, thermometer
- Sensors: Temperature, Battery Status, tire pressure
- Remote control: Open/close locks, turn on lights

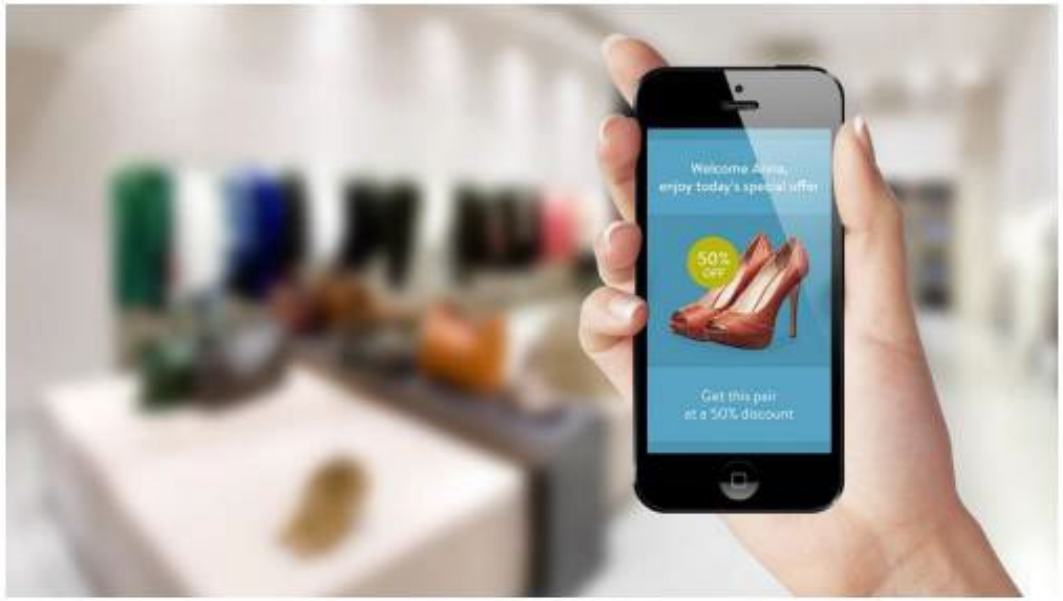
Bluetooth Device Roles

Use Cases – Physical Security

Use Cases – Home Automation



Use Cases – Geo-fencing/ Positioning



Bluetooth 5

- June/December 2016
- Enhanced Bluetooth low energy
- Supports many more devices at low energy, e.g., headphones,
- Dual-audio: two headphones playing two streams
- 2X Data rate using a new modulation → 2 Mbps
- Or 4X range 800 ft using a special coding (Good for beacons) → Long-Range mode allows 1.6 km at 125 kbps
- 8X broadcast capacity by changing the advertising procedure. 255B instead of 31B with v4.2
- aptX compression allows CD quality audio over 1 Mbps. Bluetooth 5.0 allows better quality using 2Mbps.
- +20 dBm (100 mW) transmit power in LE mode → Good for bursts
- Both ends must be Bluetooth 5 to benefit.
  - Backward compatible with older devices using older modes

Ref: Madhur Bhargava, " IoT Projects with Bluetooth Low Energy," Packt Publishing, August 2017, 278 pp., ISBN:978-1-78839-683-7 (Safari Book).

Changes to PHY layer in Bluetooth 5 to support Mesh

SINGAPORE INSTITUTE OF TECHNOLOGY

- **Introduction of new PHY layers**: Includes two new PHY layers, the 2Mbps PHY and the Coded PHY, that provide faster data transfer rates and improved robustness.
- **Wider frequency band**: Uses a broader frequency band of 2 MHz (compared to 1 Mhz in traditional Bluetooth). This allows for more efficient use of the available spectrum and improves the overall performance of the network.
- **Directional communication**: Includes support for directional communication, which allows devices to communicate with each other while maintaining a low power consumption; beamforming techniques.
- **Enhanced mesh networking protocol**: Utilises an enhanced version of the mesh networking protocol, which enables it to support a more significant number of devices in a network and improves its reliability.
- **IPv6 support**: Supports IPv6 that allows for more efficient and secure communication between devices and enables more advanced IoT (Internet of Things) applications.

Summary

1. Bluetooth basic rate uses frequency hoping over 79 1-MHz channels.
2. Three inactive states: hold, sniff, park.
3. Has a fixed set of applications called "Profiles"
4. Bluetooth and Wi-Fi co-exist by time-sharing or adaptive frequency notching
5. Bluetooth Smart is designed for short broadcasts by sensors. 40 2-MHz channels with 3 channels reserved for advertising. One or two-message exchanges
6. Generic attribute profile allows new applications using UUID for data types

SINGAPORE INSTITUTE OF TECHNOLOGY

END