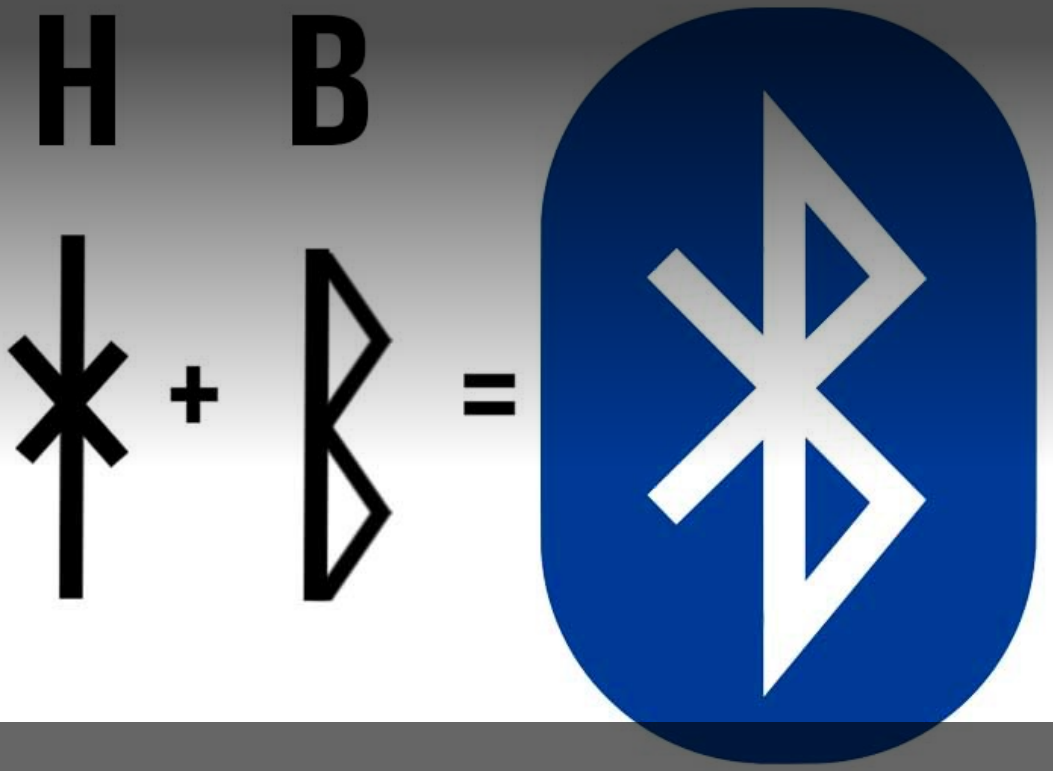
Bluetooth



Geoff Merrett
ELEC3227/6255: Networks

Image: https://mind-blowingfacts.com/wp-content/uploads/2019/03/words_7.jpg

Outline

- Introduction
- Bluetooth
  - (reasonably quickly)

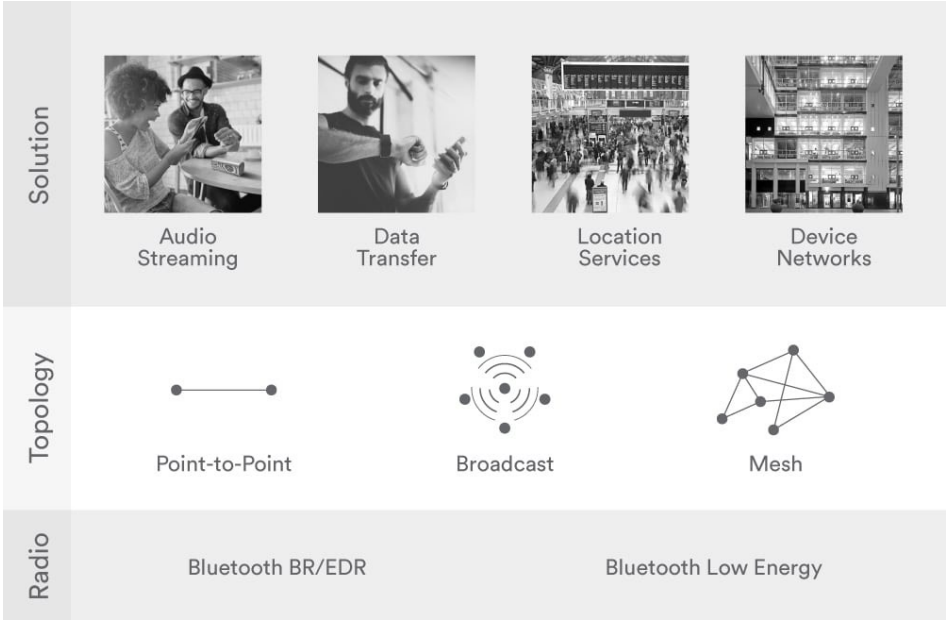
- Bluetooth Low Energy/Bluetooth Smart

Introduction

"The Global Standard for Connection

Bluetooth® technology proves the power of connection. ***4 billion devices will ship this year*** *using Bluetooth to connect. To phones, to tablets, to PCs, or to each other.*

And Bluetooth enables multiple ways to connect. After first demonstrating the power of simple point-to-point connections, Bluetooth broadcasting is now powering the global beacon revolution and accelerating new markets—like smart buildings—through mesh connections."



https://www.bluetooth.com/bluetooth-technology/, December 2019

Introduction

- Designed for Personal Area Networks (PANs), e.g. Bluetooth headsets

- Released in 1998 by Bluetooth SIG
  - Today, the SIG is a consortium of >34,000 companies who manage the standard
  - Originally (v1.1-1.2) standardized by the IEEE as IEEE 802.15.1
  - Newer versions backwards compatible with older ones (*except BLE; more later*)

Electronics and
Computer Science

UNIVERSITY OF
Southampton

Bluetooth

Bluetooth Classic *or*
Bluetooth BR/EDR

Bluetooth Classic (BR/EDR)

"The Bluetooth BR/EDR radio is designed for low power operation. The Bluetooth BR/EDR radio includes multiple PHY options that support data rates from 1 Mb/s to 3 Mb/s, and supports multiple power levels, from 1mW to 100 mW, as well as multiple security options. It supports a point-to-point network topology optimized for audio streaming."

https://www.bluetooth.com/bluetooth-technology/radio-versions/

Bluetooth Physical Layer

- Operates at 2.4 GHz
  - originally used only Gaussian Frequency Shift Keying (GFSK) modulation providing data-rates of 1 Mbps
  - revisions have provided more PHY options and now allow up to 3 Mbps
- 79 Channels, each with a 1 MHz spacing
  - Time is discretized into slots; a single ‘slot’ is 625 us
  - Packets can last 1, 3 or 5 slots
- Frequency Hopping Spread Spectrum (FHSS)

Hedy Lamarr

From Wikipedia, the free encyclopedia

Hedy Lamarr (/ˈhɛdi/), born **Hedwig Eva Maria Kiesler** (November 9, 1914[a] – January 19, 2000), was an Austrian-born American film actress and inventor who in 2014 was posthumously inducted into the National Inventors Hall of Fame. [1]

After a brief early film career in Czechoslovakia, including the controversial *Ecstasy* (1933), she fled from her husband, a wealthy Austrian ammunition manufacturer, and secretly moved to Paris. Traveling to London, she met Louis B. Mayer, head of Metro-Goldwyn-Mayer (MGM) studio, who offered her a movie contract in Hollywood.

She became a star with her performance in *Algiers* (1938), her first film made in the United States.[2] Her MGM films include *Lady of the Tropics* (1939), *Boom Town* (1940), *H.M. Pulham, Esq.* (1941), and *White Cargo* (1942). Her greatest success was as Delilah in Cecil B. DeMille's *Samson and Delilah* (1949).[3] She also acted on television before the release of her final film, *The Female Animal* (1958). She was honored with a star on the Hollywood Walk of Fame in 1960.[4]

At the beginning of World War II, Lamarr and composer George Antheil developed a radio guidance system for Allied torpedoes, intended to use frequency-hopping spread spectrum technology to defeat the threat of jamming by the Axis powers.[5] Although the US Navy did not adopt the technology until the 1960s,[6] various spread-spectrum techniques are incorporated into Bluetooth technology and are similar to methods used in legacy versions of Wi-Fi.[7][8][9] Recognition of the value of this work resulted in the pair being inducted into the National Inventors Hall of Fame in 2014.[5][10]

Contents [hide]

Hedy Lamarr

Publicity photo (c. 1944)

Born	Hedwig Eva Maria Kiesler November 9, 1914 Vienna, Austria-Hungary
Died	January 19, 2000 (aged 85) Casselberry, Florida, U.S.
Citizenship	Austria (1914–1953) United States (1953–2000)
Occupation	Actress, inventor
Spouse(s)	Fritz Mandl (m. 1933; div. 1937) Gene Markey (m. 1939; div. 1941) John Loder (m. 1943; div. 1947) Teddy Stauffer (m. 1951; div. 1952) W. Howard Lee (m. 1953; div. 1960) Lewis J. Boies (m. 1963; div. 1965)
Children	3

UNITED STATES PATENT OFFICE

2,292,387

SECRET COMMUNICATION SYSTEM

Hedy Kiesler Markey, Los Angeles, and George Antheil, Manhattan Beach, Calif.

Application June 10, 1941, Serial No. 397,412

6 Claims. (Cl. 250—2)

This invention relates broadly to secret communication systems involving the use of carrier waves of different frequencies, and is especially useful in the remote control of dirigible craft, such as torpedoes.

An object of the invention is to provide a method of secret communication which is relatively simple and reliable in operation, but at the same time is difficult to discover or decipher.

Briefly, our system as adapted for radio control of a remote craft, employs a pair of synchronous records, one at the transmitting station and one at the receiving station, which change the tuning of the transmitting and receiving apparatus from time to time, so that without knowledge of the records an enemy would be unable to determine at what frequency a controlling impulse would be sent. Furthermore, we contemplate employing records of the type used for many years in player pianos, and which consist of long rolls of paper having perforations variously positioned in a plurality of longitudinal rows along the records. In a conventional player piano record there may be 88 rows of perforations, and in our system such a record would permit the use of 88 different carrier frequencies, from one to another of which both the transmitting and receiving station would be changed at intervals. Furthermore, records of the type described can be made of substantial length and may be driven slow or fast. This makes it possible for a pair of records, one at the transmitting station and one at the receiving station, to run for a length of time ample for the remote control of a device such as a torpedo.

The two records may be synchronized by driv-

Fig. 2 is a schematic diagram of the apparatus at a receiving station;

Fig. 3 is a schematic diagram illustrating a starting circuit for starting the motors at the transmitting and receiving stations simultaneously;

Fig. 4 is a plan view of a section of a record strip that may be employed;

Fig. 5 is a detail cross section through a record-responsive switching mechanism employed in the invention;

Fig. 6 is a sectional view at right angles to the view of Fig. 5 and taken substantially in the plane VI—VI of Fig. 5, but showing the record strip in a different longitudinal position; and

Fig. 7 is a diagram in plan illustrating how the course of a torpedo may be changed in accordance with the invention.

Referring first to Fig. 7, there is disclosed a mother ship 10 which at the beginning of operations occupies the position 10*a* and at the end of the operations occupies the position 10*b*. This mother ship discharges a torpedo 11 that travels successively along different paths 12, 13, 14, 15 and 16 to strike an enemy ship 17, which initially occupies the position 17*a* but which has moved into the position 17*b* at the time it is struck by the torpedo 11. According to its original course, the enemy ship 17 would have reached the position 17*c*, but it changed its course following the firing of the torpedo, in an attempt to evade the torpedo.

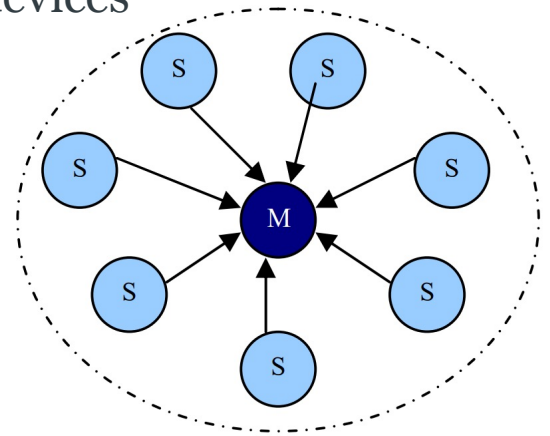
In accordance with the present invention, the torpedo 11 can be steered from the mother ship 10*a* and its course changed from time to time as necessary to cause it to strike its target. In

Bluetooth Physical Layer

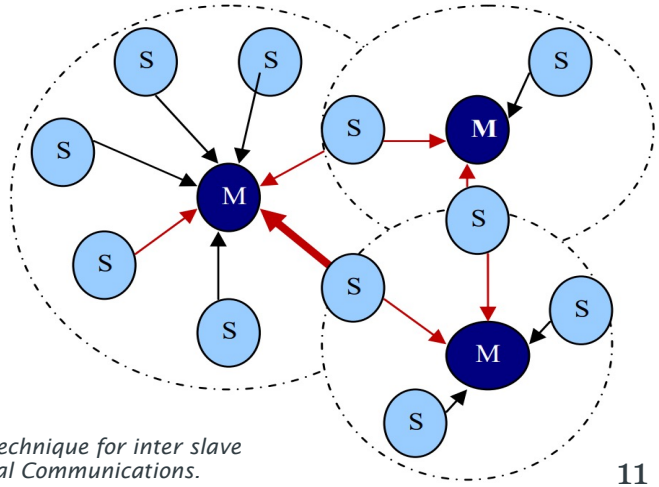
- Operates at 2.4 GHz
  - originally used only Gaussian Frequency Shift Keying (GFSK) modulation providing data-rates of 1 Mbps
  - revisions have provided more PHY options and now allow up to 3 Mbps
- 79 Channels, each with a 1 MHz spacing
  - Time is discretized into slots; a single ‘slot’ is 625 us
  - Packets can last 1, 3 or 5 slots
- Frequency Hopping Spread Spectrum (FHSS)
  - Hops to a different frequency on every packet
  - Pseudorandom hopping sequence determined by the Master’s unique device address
  - Therefore, can hop at up to 1,600 hops/second
- *More on this when we look at BLE*

Piconets and Scatternets

- **Piconet**: a connection between 2 or more Bluetooth devices
  - Always 1 Master and up to 7 Slaves
  - Any Bluetooth device can be a Master or a Slave
  - All devices in the Piconet synchronise with the Master's clock/timing and *f* hopping sequence
  - A device can be a Slave of multiple Piconets, or a Master of one Piconet and a Slave of another…



- **Scatternet**: two or more joined Piconets
  - A Master or Slave of one Piconet acts as a Slave in another
  - No time or frequency synchronisation between Piconets



Images: Chaudhry, Marium & Zahid, Muhammad & Saleemi, Farhat & Chaudhry, Fatima. (2010). Routing technique for inter slave bonding in Bluetooth scatternets formation, Recent Advances in Electronics, Hardware, Wireless and Optical Communications.

Addressing

- **Bluetooth Device Address** (BD_ADDR)
  - The fundamental identifier of a Bluetooth device, similar to an Ethernet or Wi-Fi Media Access Control (MAC) addresses.
  - A 48-bit (6-byte) number uniquely identifies a device among peers (as per MAC addresses, the first 3-bytes of this are regulated and specify the company)
  - Both Public Device Addresses and Random Device Addresses (to allow devices to remain private from being 'tracked')
- **Active Member Address** (AM_ADDR)
  - Each active member in a Piconet is given a 3-bit address by the Master, and acts as a MAC address within the Piconet.
  - There can therefore only be 7 active Slaves in a Piconet at the same time (0x000 is reserved for broadcast packets).
- **Parked Member Address** (PM_ADDR)
  - 'Parked' slaves can remain synchronised, but don't participate in traffic
  - They are allocated an 8-bit address.

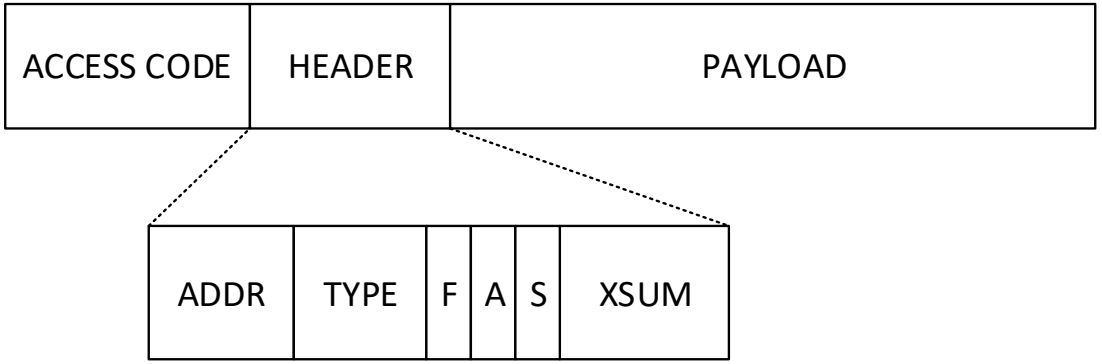
Inquiry (Discovery) and Data Transfer

- Inquiry procedure
  - A device sends out an 'inquire' (on 16 different frequencies), requesting a response from nearby devices (<10m)
  - Devices that are currently set to respond, i.e. are 'discoverable' listen for long enough to hear the 16 channel 'train'
  - This process can take up to >10 seconds

- Data transfer
  - Slaves all share the Master's clock (which ticks at 312.5 us, i.e. half a slot length)
  - The Master transmits in even slots, and receives from Slaves in odd slots
  - The Master chooses which Slave(s) to address, whereas Slaves must listen in every receive slot in case the Master wishes to communicate with it

Piconets

- To communicate on the Piconet, a device needs to know:
  - **The channel hopping sequence:** the Bluetooth Device Address of the Piconet Master is used to derive this
  - **The phase:** the system clock of the Master determines the phase in the hopping sequence
  - **The Channel Access Code:** specific to an individual Piconet, and derived from the Master's Bluetooth Device Address



Link Layer Services

- Bluetooth supports two types of links:
- **Synchronous Connection Oriented (SCO)**
  - Usually used for voice
  - Point-to-point link between a single master and a single slave
  - Reserved slots at a regular interval
  - Can support up to 3 simultaneous SCO links at a time
  - No retransmissions
- **Asynchronous Connection Less (ACL)**
  - Usually used for data transfer
  - Point to multi-point (star) link between master and all slaves in piconet
  - Master can establish ACL link to any slave in any slots not reserved for SCO
  - Retransmissions usually applied

Error Control

Three options:

- 1/3 rate
  - every bit is repeated 3 times for redundancy
- 2/3 rate
  - a generator polynomial encodes a 10 bit code to a 15 bit code
- ARQ (*Automatic Repeat reQuest*)
  - Packets are retransmitted until an acknowledgement is received. Unnumbered acknowledgements, +ve or –ve.

Electronics and
Computer Science

UNIVERSITY OF
Southampton

Bluetooth Low Energy

Bluetooth Smart / Bluetooth 4.0+

Bluetooth Smart

- Bluetooth v4.0 introduced Bluetooth Smart, incorporating both Classic (BR/EDR) and Low Energy (BLE).
  - Single-mode Bluetooth or Bluetooth Smart (either BLE or BR/EDR), or
  - Dual-mode Bluetooth Smart Ready (both BLE and BR/EDR)

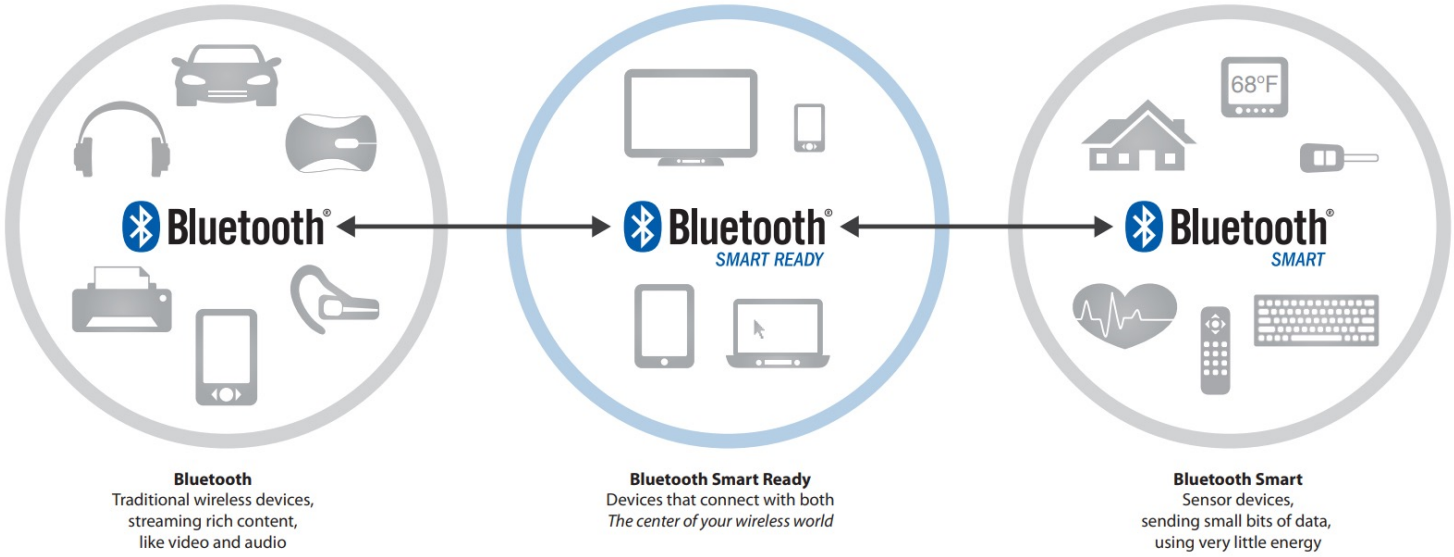


Figure 1. The relationship between Bluetooth Smart and Bluetooth Smart Ready devices (Source: Bluetooth SIG)

Bluetooth Low Energy (BLE)

*"The Bluetooth Low Energy (LE) radio is designed for **very low power** operation. The Bluetooth LE radio provides developers a tremendous amount of flexibility, including multiple PHY options that support **data rates from 125 Kb/s to 2 Mb/s**, multiple power levels, from 1mW to 100 mW, as well as multiple **security options** up to government grade.*

*BLE also supports **multiple network topologies**, including a point-to-point option for data transfer, a broadcast option for location services and a mesh option used for creating large-scale device networks."*

https://www.bluetooth.com/bluetooth-technology/radio-versions/

Bluetooth Low Energy

- BLE designed for IoT devices:
  - Low current consumption
  - Low energy consumption (i.e. small packets, throughput, latencies and duty cycles)
  - Asymmetric devices (server devices much more constrained that clients)
  - IoT data patterns (primarily one-way data transfer, publish and subscribe, etc)
  - 50-150 m ranges
- New stack, designed for operating for years off a coin cell
  - new PHY (though shares parts of PHY to allow hardware duplication with BT Classic)
  - new advertising mechanisms
  - asynchronous connection-less MAC
  - asynchronous client/server data-model
  - ***BLE is not backwards compatible with BT Classic devices***

BLE vs Bluetooth Classic

Technical Specification	Classic Bluetooth	Bluetooth Low Energy
Distance/Range	100 m (330 ft)	50 m (160 ft)
Over the Air Data Rate	1 – 3 Mbit/s	1 Mbit/s
Application Throughput	0.7 – 2.1 Mbit/s	0.27 Mbit/s
Active Slaves	7	Not defined; implementation dependent
Security	56 / 128-bit and application layer user defined	128-bit AES with Counter Mode CBC-MAC and application layer user defined
Robustness	Adaptive fast frequency hopping, FEC, fast ACK	Adaptive frequency hopping, Lazy Acknowledgement, 24-bit CRC, 32-bit Message Integrity Check
Latency (from a non connected state)	Typically 100 ms	6 ms
Total time to send data (depending battery life)	100 ms	3 ms, less than 3 ms
Voice capable	Yes	No
Network topology	Scatternet (See figures above)	Star-bus (See figures above)
Power consumption	1 as the reference	0.01 to 0.5 (depending on the use case)
Peak current consumption	Less than 30 mA	Less than 20 mA
Service discovery	Yes	Yes
Profile concept	Yes	Yes

Source: Laird Technologies, http://www.summitdata.com/blog/ble-overview/

BLE Devices

- Server device
  - IoT devices/end devices/peripherals
  - Low-power, constrained, small
  - Expose their state, and notify client(s) when it updates

- Client device
  - Central device/data sink/base station/phone
  - More capability
  - Can use exposed state, read/write to it

Source: Qualcomm, https://datatracker.ietf.org/meeting/interim-2016-t2trg-02/materials/slides-interim-2016-t2trg-2-7

BLE Stack

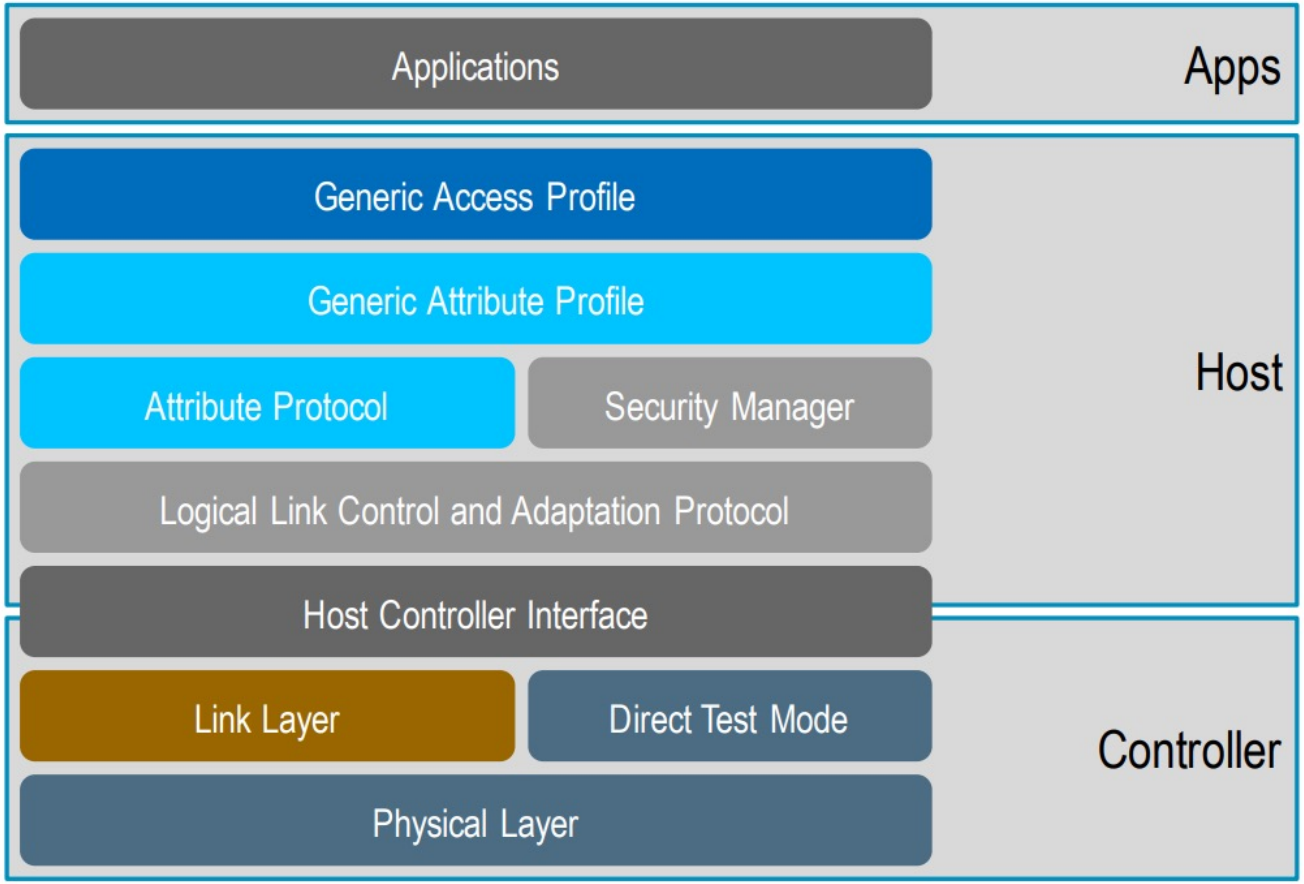


Image: Qualcomm https://datatracker.ietf.org/meeting/interim-2016-t2trg-02/materials/slides-interim-2016-t2trg-2-7

Electronics and
Computer Science

UNIVERSITY OF
Southampton

BLE
PHY Layer

BLE PHY

- 2.4 GHz ISM band
  - GFSK modulation @ up to 1 Mbps
  - Divided into 40 channels with a 2 MHz spacing
  - 37 ***data channels*** (0-36) and 3 ***advertising channels*** (37-39)

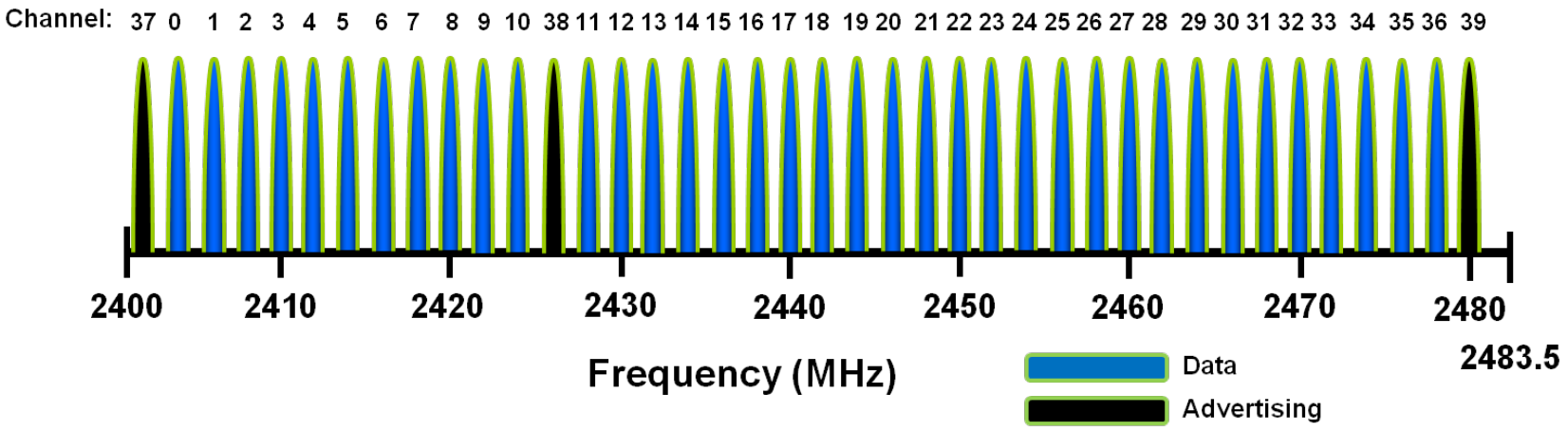


Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

BLE PHY

- Advertising channels arranged to have centre frequencies that don't overlap with common WiFi/802.11 channels, to aid coexistence

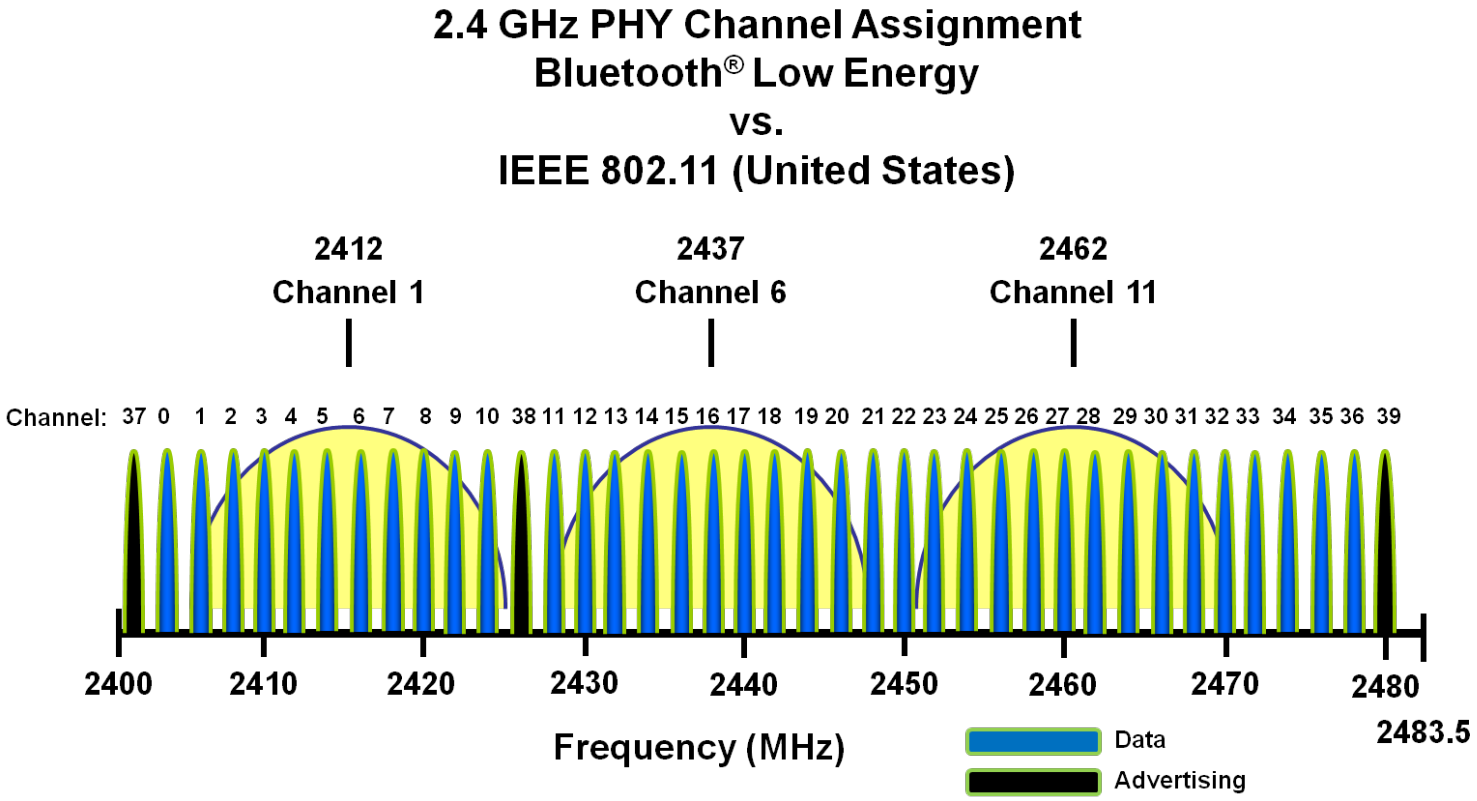


Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

Electronics and
Computer Science

UNIVERSITY OF
Southampton

BLE
Link Layer

BLE Frequency Hopping

- For data connections, frequency hopping is cycles through 37 data channels:

$$f_{n+1}=(f_n + hop) \bmod 37$$

  - f_{n+1} is the channel to use on the next event;
  - *hop* is a value that can range from 5-16 (set when the connection is initialised).

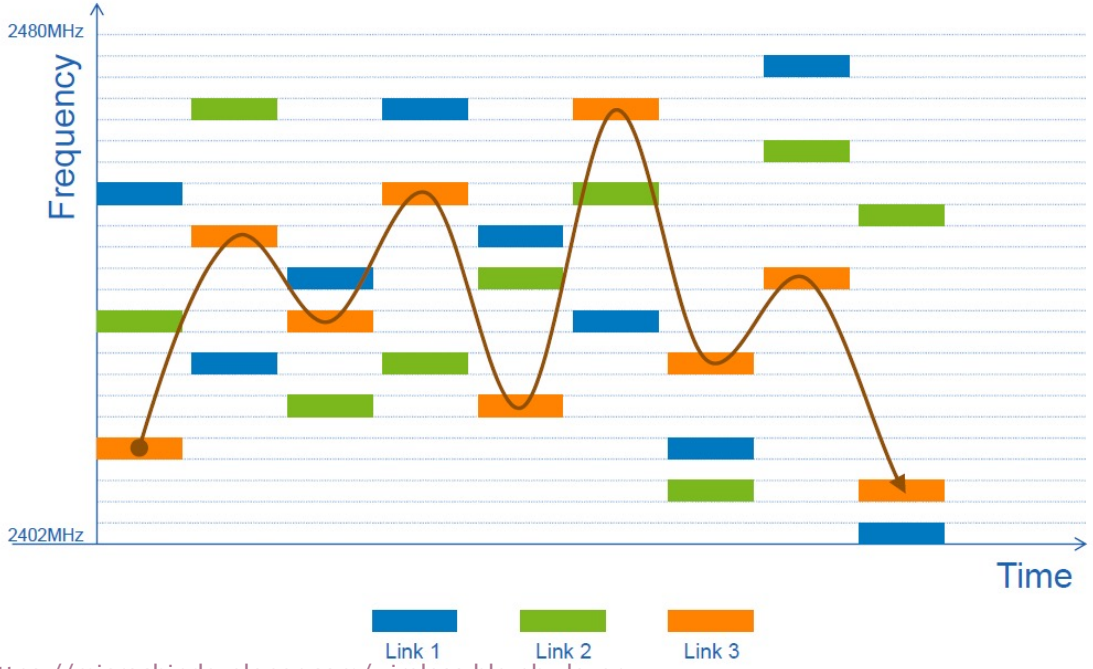


Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

BLE Adaptive Frequency Hopping

- Link layer can remap packets from a known bad channel to a good one
- E.g. BLUE coexisting with WiFi networks using WiFi channels 1, 6, and 11

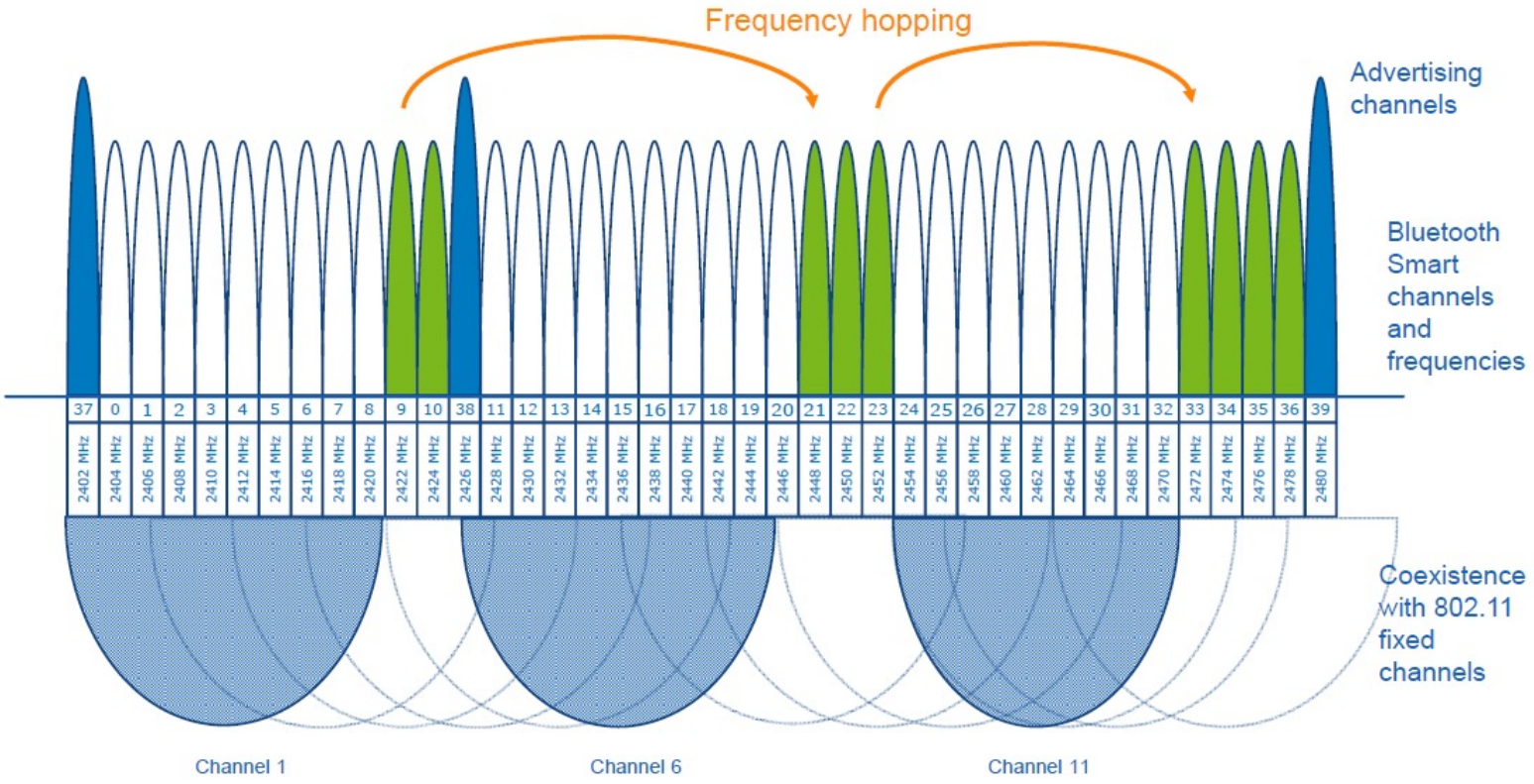
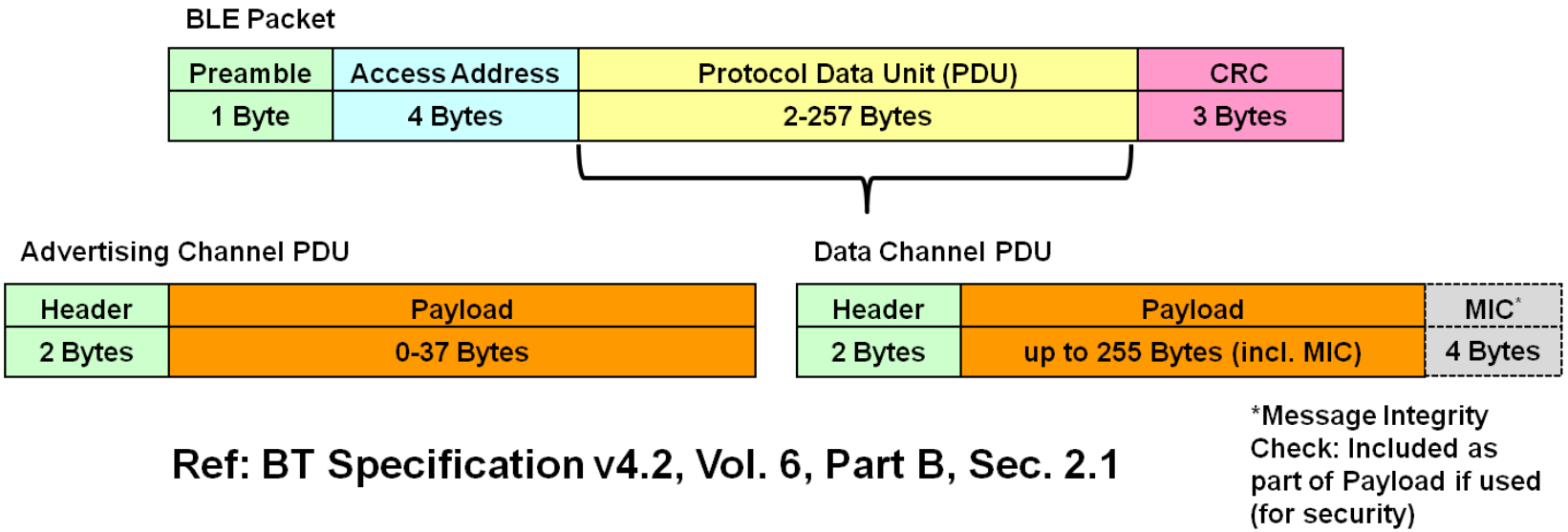


Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

BLE Packet/Frame Types

- BLE has a single packet format for both **advertising channel** and **data channel** packets



Ref: BT Specification v4.2, Vol. 6, Part B, Sec. 2.1

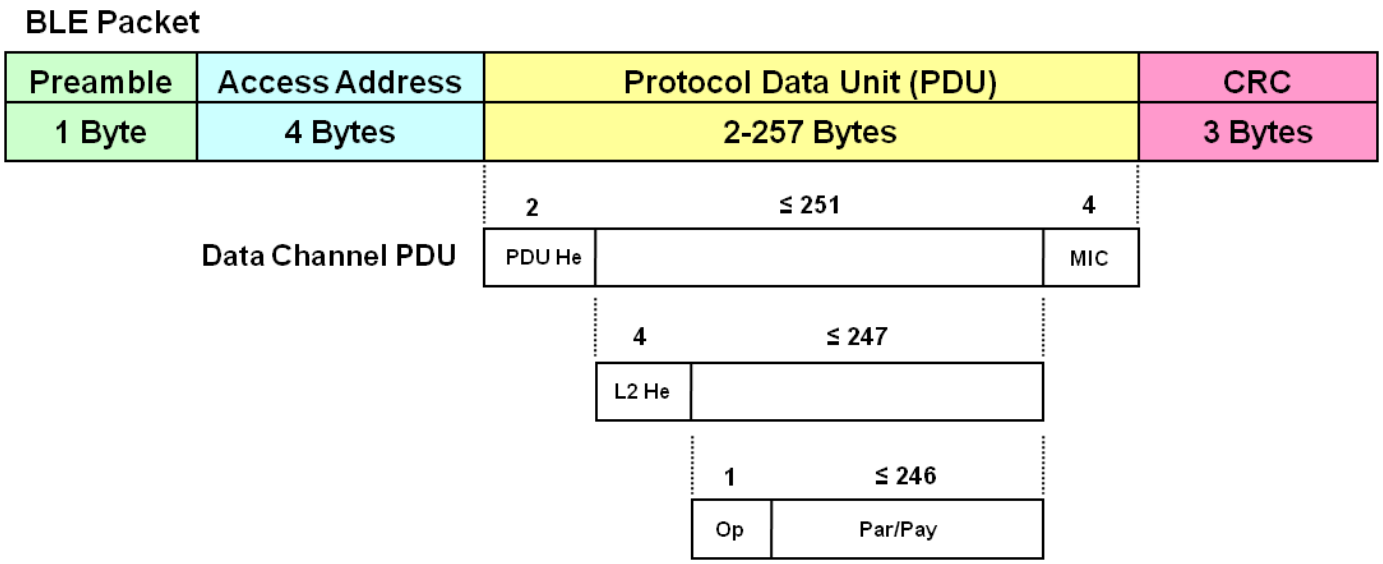
*Message Integrity Check: Included as part of Payload if used (for security)

- Advertising channel PDUs have two purposes
  - Discover Slaves and connect to them
  - Broadcast data for applications that don't require a connection

Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

BLE Packet/Frame Types

- Data Channel PDU:



- 4-byte addresses remove limitation of 7-devices in a single Piconet
  - In reality, there's a practical limitation of 100s of active devices
- 24-bit CRC provides a reliable link layer
  - CRC failures cause re-transmission requests; no limit for re-transmissions

Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

BLE Roles/States

- A BLE can be in one of five states at any time:
  - **Standby**: not transmitting, receiving or connected
  - **Advertising**: periodically broadcasting adverts
  - **Scanning**: actively looking for advertisers
  - **Initiator**: actively trying to initiate connection with another device
  - **Connected**: connected to another device as either Master or Slave

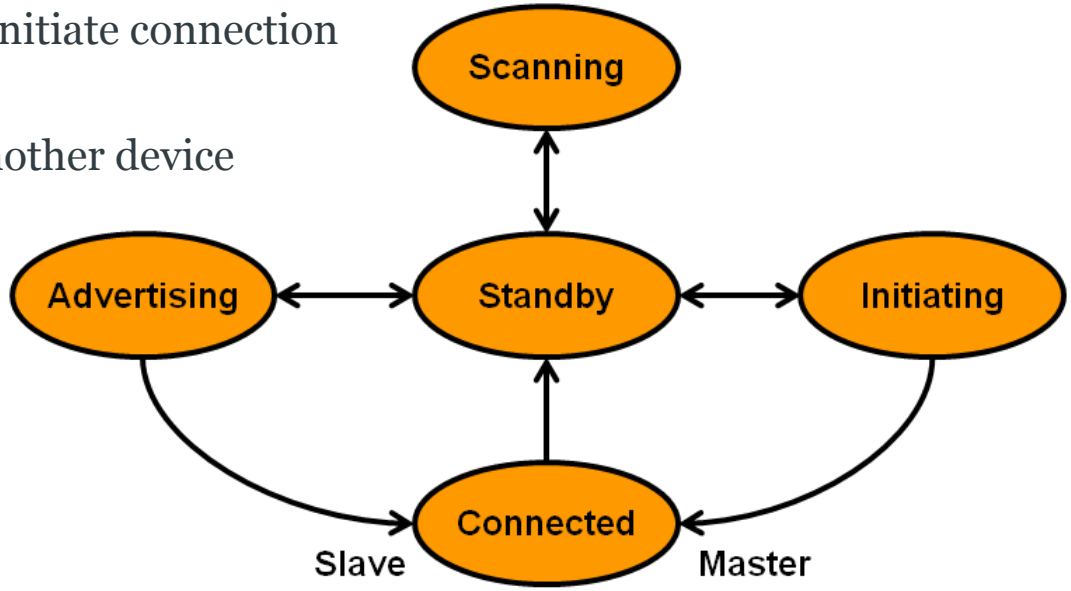


Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

Advertising Packets

- A device in the advertising state transmits advertising packets
  - Advertising packets can contain a data payload
  - Advertising packets can be directed towards a specific scanner device, or undirected
  - Advertisements can be connectable or non-connectable (and therefore just used for broadcast of data)

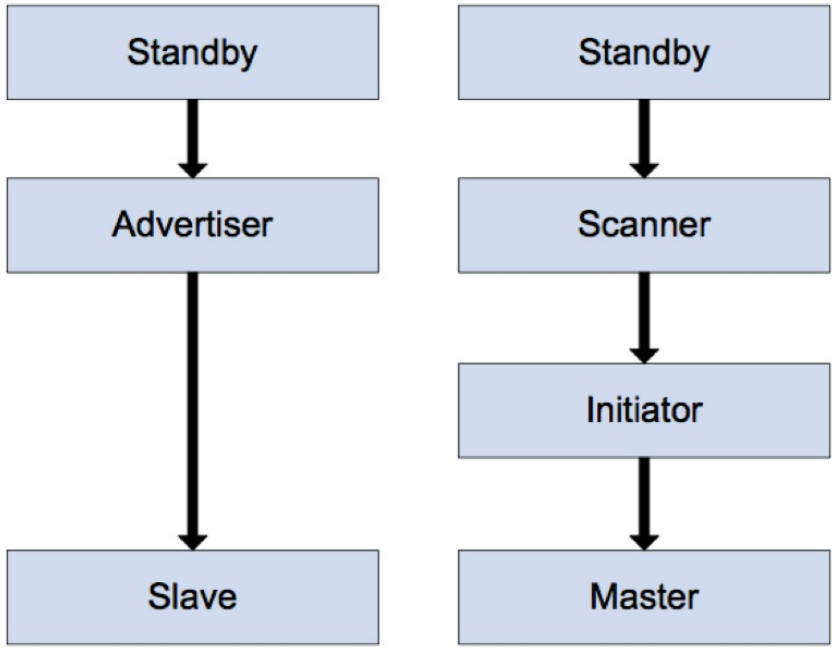


Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

Advertising Packets: Broadcasting Data

- Two roles:
  - **Broadcaster** (the host sending the packets)
  - **Observer** (the host listening for broadcasts)

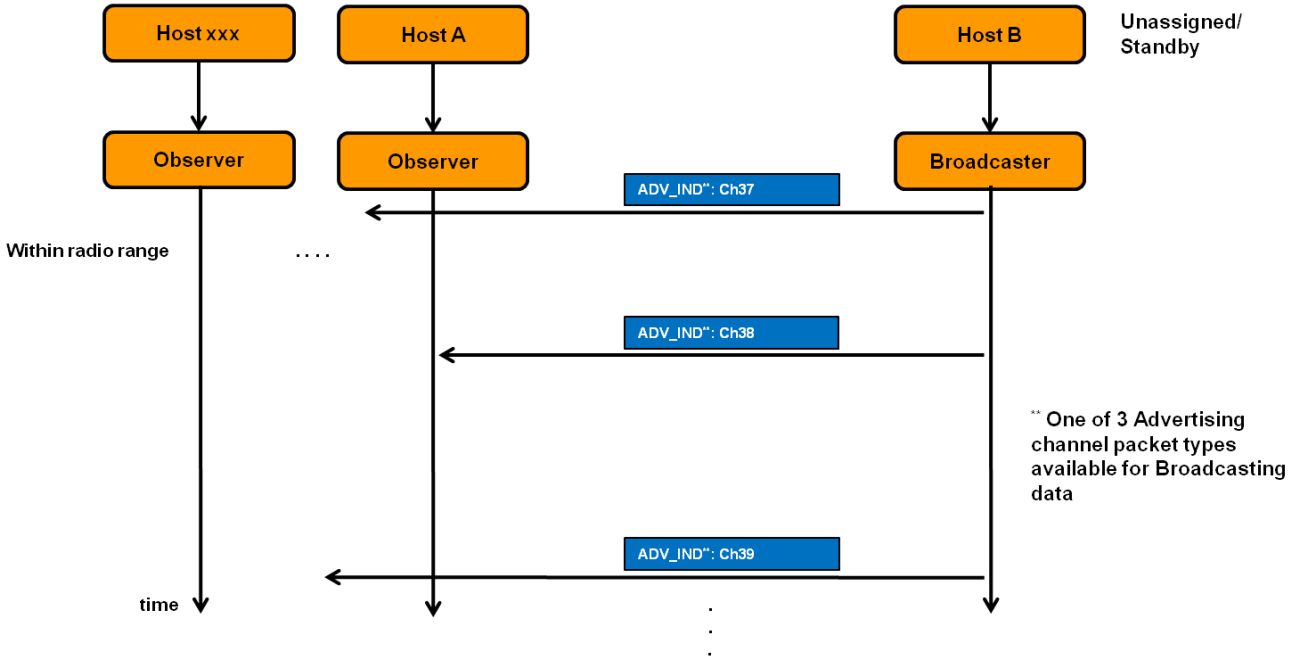


Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

Advertising Packets: Connections

- Servers/Peripherals advertise
  - Advertising interval provides a tradeoff between latency and power consumption
- Advertising event is transmitted on all 3 of advertising channels
- **Passive Scanning:**
  - Host listens for advertising packets; the advertiser doesn't know if they were received

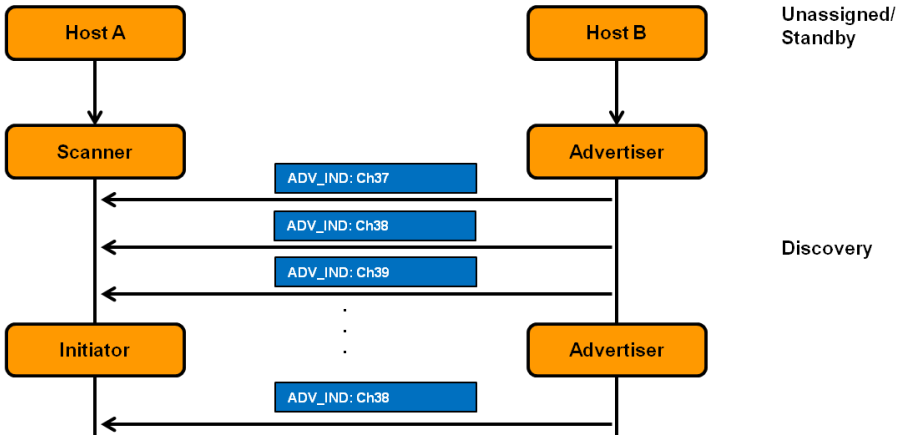


Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

Advertising Packets: Connections

- Servers/Peripherals advertise
  - Advertising interval provides a tradeoff between latency and power consumption
- Advertising event is transmitted on all 3 of advertising channels

- **Active Scanning:**
  - If the host needs more information than can be provided in the advertising packet, the scanner can issue a SCAN_REQ in the interval, and the advertiser responds.

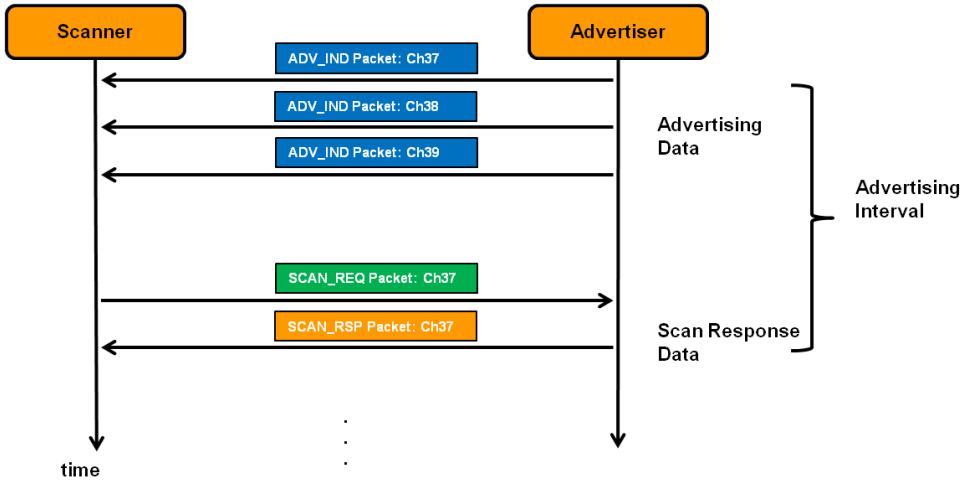


Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

Advertising and Scanning

- Advertising and scanning occur at regular intervals, but they are **not synchronized** so activities **must overlap** for discovery to begin.
- In the example below, only the times indicated by the black dotted rectangles are periods when discovery is possible because advertising and scanning activities overlap.

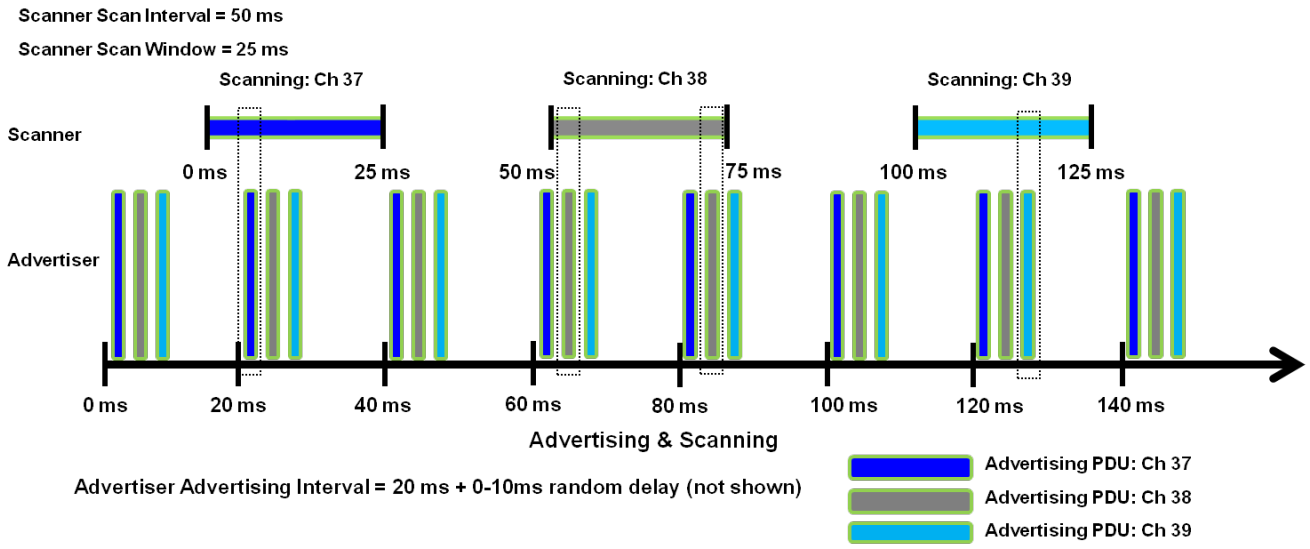
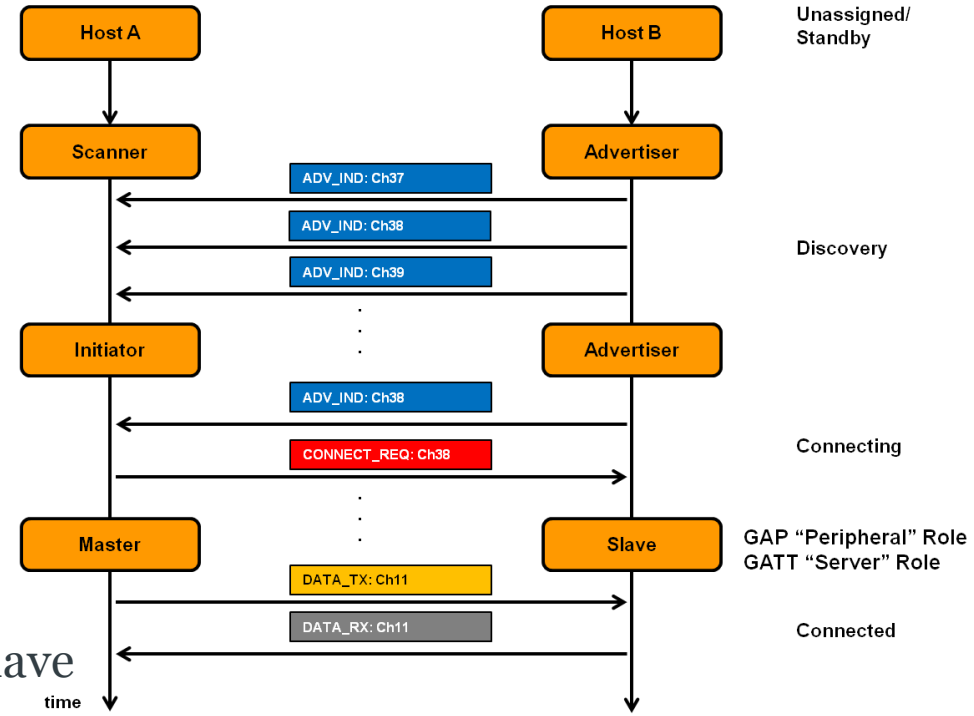


Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

Creating a Connection

- Once a Scanner decides which Advertiser to connect to, it becomes an Initiator, initiating a BLE Link Layer connection process.
- The Initiator responds to an advertising packet with CONNECT_REQ, defining:
  - Frequency hopping sequence
  - Connection Interval (PTO)
  - Slave Latency (PTO).
  - Supervision Timeout (the maximum time between two received packets before a connection is "lost").
- Once the CONNECT_REQ packet is received, data can be exchanged.
- The Initiator becomes the Link Layer Master, while the Advertiser becomes the Link Layer Slave



Source: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

Data Transfer

- Once connected, the Master and Slave exchange data packets at regular intervals, called "connection events".
  - The connection interval is between 7.5 ms to 4 s (step size: 1.25 ms). This is the *master latency*, i.e. how often the master will transmit to the slave
  - The Slave must listen to the Master at an interval defined by the *connection interval* * *slave latency* – the slave latency hence defines the maximum number of connection intervals it can skip if doesn't have any data to send
  - 0-byte data packets are exchanged if there is no other data to exchange

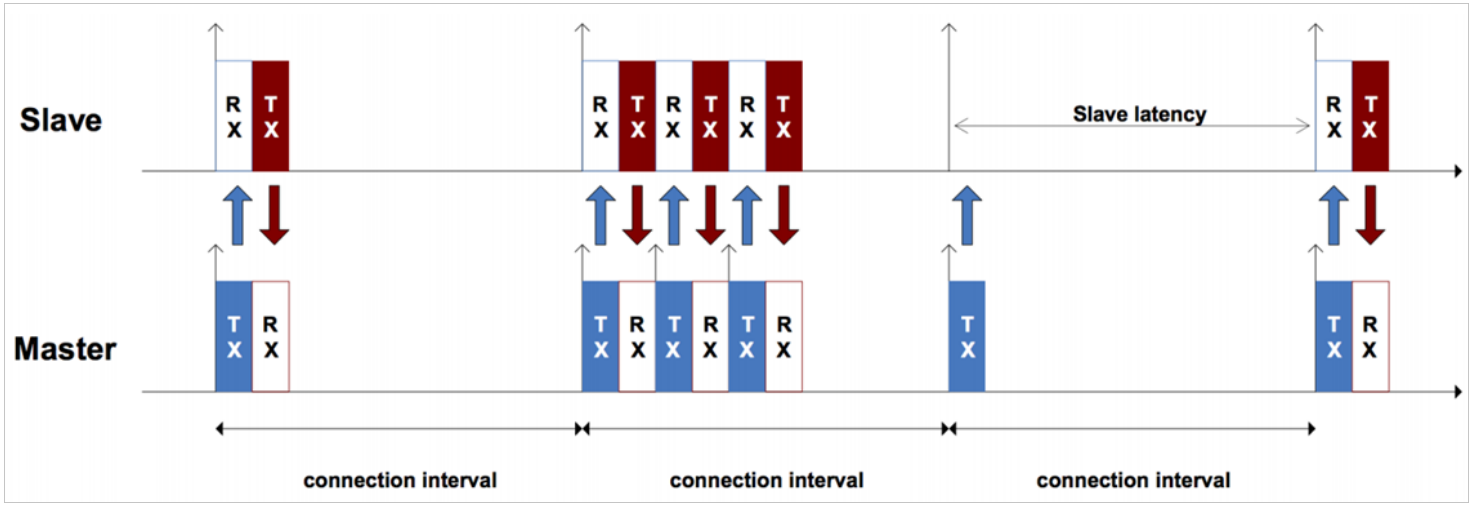


Image: Microchip, https://microchipdeveloper.com/wireless:ble-phy-layer

Questions?