Bluetooth Low Energy (BLE) Communication Process

by Sage Mooneyham

Background

- Relatively new technology (introduced in 2010)
- Digital Radio Protocol
  - Transmits via Radio Waves
- Designed for low power consumption, bandwidth, complexity
- Classic Bluetooth is not directly compatible with BLE

Table 1-1. Specification configurations

Device	BR/EDR (classic Bluetooth) support	BLE (Bluetooth Low Energy) support
Pre-4.0 Bluetooth	Yes	No
4.x Single-Mode (Bluetooth Smart)	No	Yes
4.x Dual-Mode (Bluetooth Smart Ready)	Yes	Yes

BLE and the ISM Radio Band

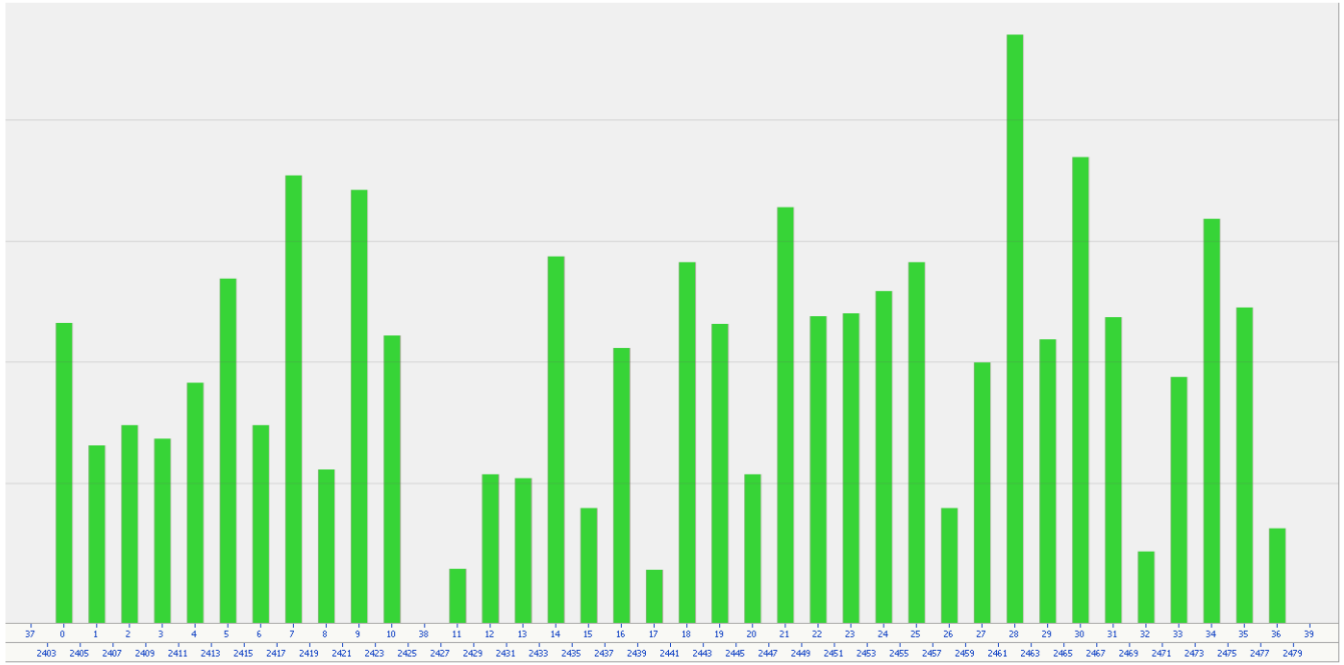
- ISM: Industrial, Scientific, Medical
- Range of frequencies reserved for ISM purposes.
- Frequency ranges must be defined and allotted, as devices operating on the same/similar frequencies can interfere with each other
- BLE operates on the 2.4 GHz ISM band (2.4000 – 2.4835 GHz range)
  - 40 channels of 2 MHz spacing (37 for connection, 3 for advertising)
  - Operates in the same frequency as Bluetooth Classic and Wifi

Frequency Hopping Spread Spectrum (FHSS)

- Method by which the carrier frequency hops to different channels in the range
- BLE uses FHSS to reduce potential interference and eavesdropping
- NextChannel = (CurrentChannel + Hop) % 37
  - Hop is defined randomly at connection time between two devices
- These hops occur multiple times a second, sending data in bursts
- BLE goes a step further, using a variation of FHSS

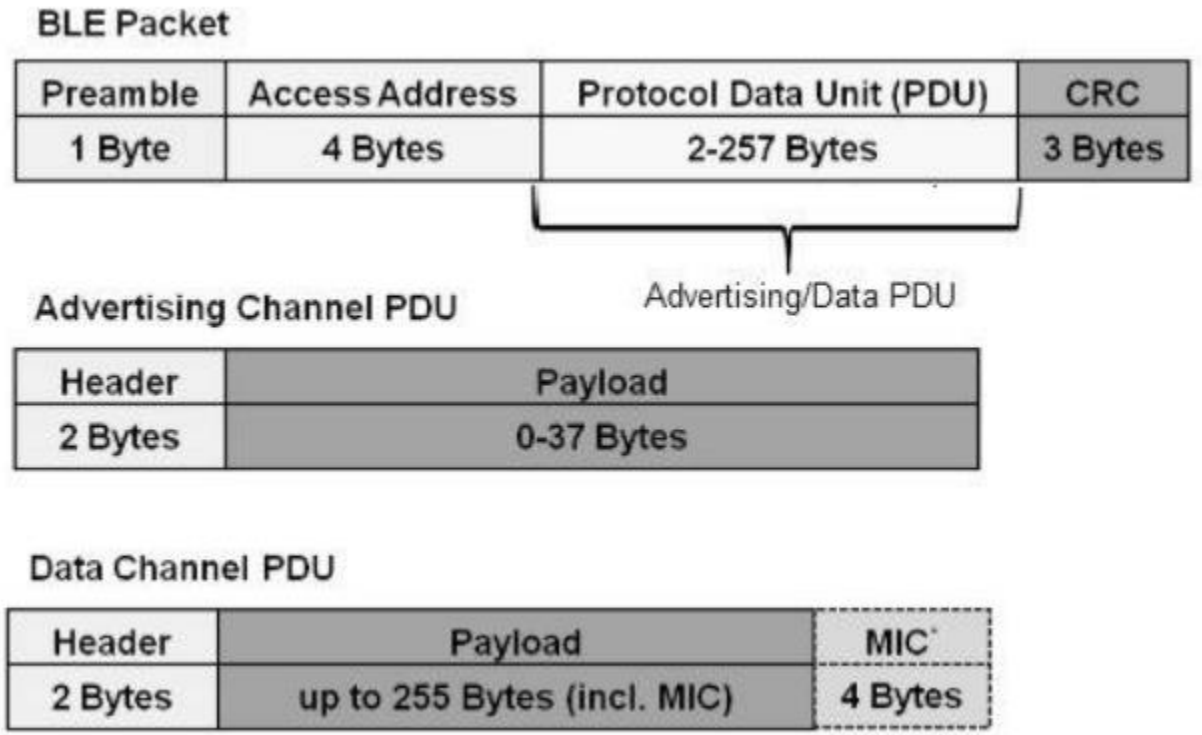
Adaptive Frequency Hopping (AFH)

- Works the same as Frequency Hopping Spread Spectrum
- Main device in connection creates a channel map
- Continuously updates status of channels and shares with connection



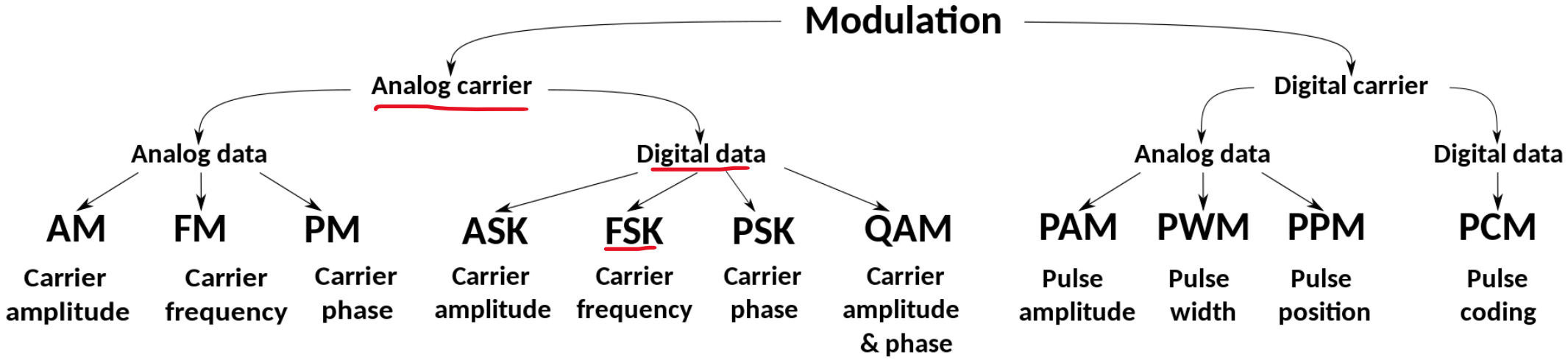
BLE Packet Format (v4.2)

- Preamble: used for synchronization
- Access Address: Random value (distinguishes devices on same channel)
- PDU: Protocol Data Unit
  - Differs based on channel type
    - Header: formatting
    - Payload: message being sent
    - MIC: message integrity check
- CRC: Cyclic Redundancy Check



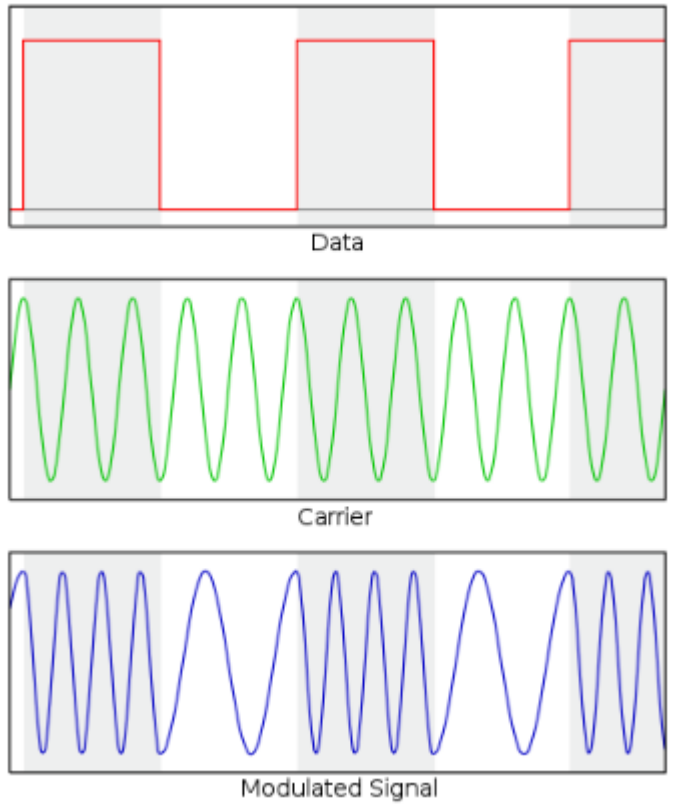
Signal Modulation

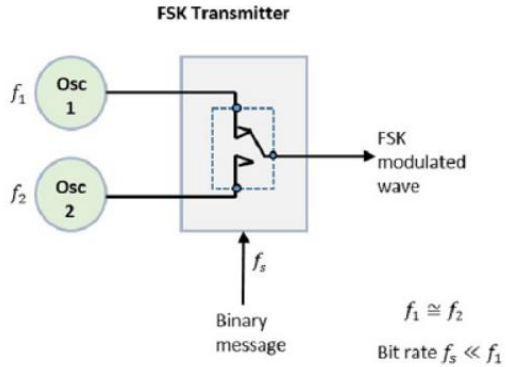
- Generally, signals are low frequency, and need to be modulated (coded/packaged) in order to be properly transmitted.
  - Especially important in long range wireless communication
- Amplitude, Frequency, and Phase Modulation
- BLE uses a variation of Frequency Modulation
  - Gaussian Frequency Shift Keying (GFSK)



Frequency Shift Keying

- In FSK, frequency of the carrier signal is shifted(changed) to multiple discrete frequencies based on the digital signal
- Binary FSK is used (switch between 2 frequencies)
- Gaussian FSK applies Gaussian filter to carrier
  - Reduces sideband power and interference
- Data Throughput: 1 Mbps





Synchronous Demodulation

- Data must be demodulated (unpacked) when at receiver.
- Performed through the use of two bandpass filters and envelope detectors
- Envelope detectors take the shape of the peak of a signal, and return the original shape of the intended message
- From here, a decision circuit compares the inputs, and chooses which input is most likely the original message

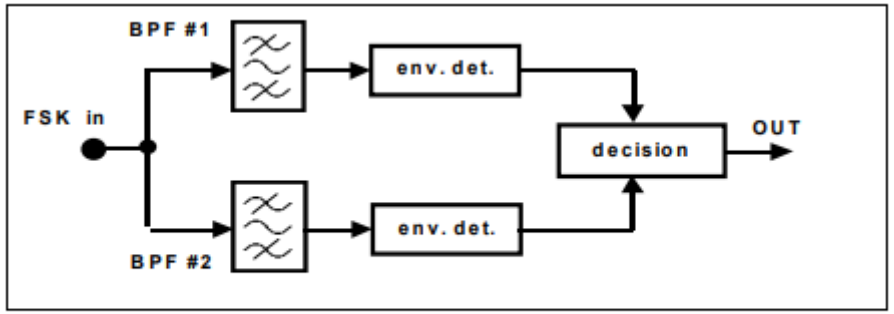


Figure 3: demodulation by conversion-to-ASK

Sources

- https://en.wikipedia.org/wiki/Bluetooth_Low_Energy#:~:text=Bluetooth%20Low%20Energy%20technology%20operates,has%2040%202%2DMHz%20channels.
- https://www.bluetooth.com/blog/how-bluetooth-technology-uses-adaptive-frequency-hopping-to-overcome-packet-interference/
- https://en.wikipedia.org/wiki/Frequency-shift_keying
- https://www.tutorialspoint.com/digital_communication/digital_communication_frequency_shift_keying.htm
- https://www.eng.auburn.edu/~troppel/courses/TIMS-manuals-r5/TIMS%20Experiment%20Manuals/Student_Text/Vol-D1/D1-07.pdf