INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

Study of physical layer of Bluetooth Low Energy (BLE) protocol

Léo Picou - Mohanprabhu Selvara - Huijie Lin - Zhe Qu - Xuantang Xiong
5 ISS - B1
2019-2020

1. What are the frequency ranges used by BLE (in Europe) ?

Bluetooth Low Energy technology use the same spectrum range (the 2.400–2.4835 GHz ISM band) as classic Bluetooth technology, but uses a different set of channels.

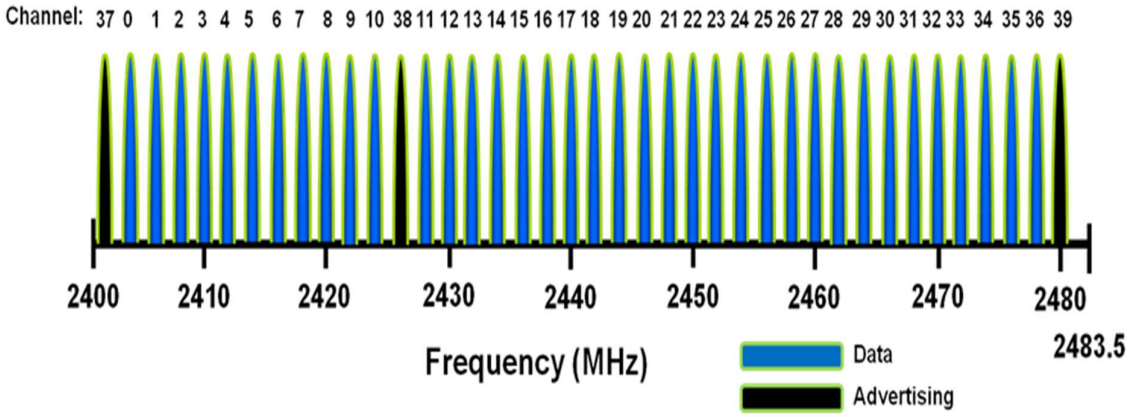
2. What is the modulation used by BLE ? What is the binary data rate ? What is the bandwidth ?

Modulation used by BLE:

Gaussian frequency shift keying (GFSK) is the modulation scheme tradionally used. It operates in the basic rate (BR) mode and ble mode. To increse the datarate, π/4-DPSK or 8DPSK can be used. Indeed the each symbol carry up to 3 bit with 8DPSK, instead of only one for 1GFSK.

Bandwidth:

Instead of the classic Bluetooth 79 x 1-MHz channels, Bluetooth Low Energy can use 40 x 2-MHz channels



Binary data rate:

If we apply the nyquist formula :

$$C = 2B\ log_2\ M$$

With a bandwidth of 2 MHz, and M=2 (1GFSK) the number of level of the signal, we should have a maximum data rate of 4 Mbps. But what we don't understand is that we can't find this value so there must be an error somewhere in our calculation.

	LE 1M	LE Coded S=2	LE Coded S=8	LE 2M
Symbol Rate	1 Ms/s	1 Ms/s	1 Ms/s	2 Ms/s
Data Rate	1 Mbit/s	500 Kbit/s	125 Kbit/s	2 Mbit/s
Error Detection	CRC	CRC	CRC	CRC
Error Correction	NONE	FEC	FEC	NONE
Range Multiplier (approx.)	1	2	4	0.8
Bluetooth 5 Requirement	Mandatory	Optional	Optional	Optional

Taken from [11]

We understand that to increase the datarate, we need either to increase the bandwidth or to increase the number of bit per symbol.
BLE introduce a large number of coding bit, which allow to have a “coding gain” up to 12 dBm with S=8. In this configuration only 1/8 bit is really useful information.

3. Define the packet structure. What is the actual throughput of BLE (precise all the hypothesis for this evaluation) ? What is the time on air ?

The link layer of Bluetooth low energy defines the packet format of the advertising channel and the data channel.
The BLE packet format:

BLE Packet

Preamble	Access Address	Protocol Data Unit (PDU)	CRC
1 Byte	4 Bytes	2-257 Bytes	3 Bytes

Advertising/Data PDU

Advertising Channel PDU

Header	Payload
2 Bytes	0-37 Bytes

Data Channel PDU

Header	Payload	MIC
2 Bytes	up to 255 Bytes (incl. MIC)	4 Bytes

We can see that there are 4 part on the BLE packet, Preamble, Access Address, PDU, and CRC code.

Preamble: The receiver uses it for synchronization (time, frequency) and AGC (automatic gain control). It is a predefined forme known by the receiver that has a size of 1 byte. The advertising package uses "10101010" in binary form. Data packets use "10101010" (if the LSB of the access address is 0) or "01010101" (if the LSB of the access address is 1) in binary form.

Access Address:The size of this champ iss The Acces Address is for identify the destination. For all the advertising packet, it predefined as 0x8E89BED6. And for the data packet, it's a 32 it random value generate by the BLE devices in "initiating state".

PDU:As shown in the figure, it consists of "advertising channel PDU" or "data channel PDU".

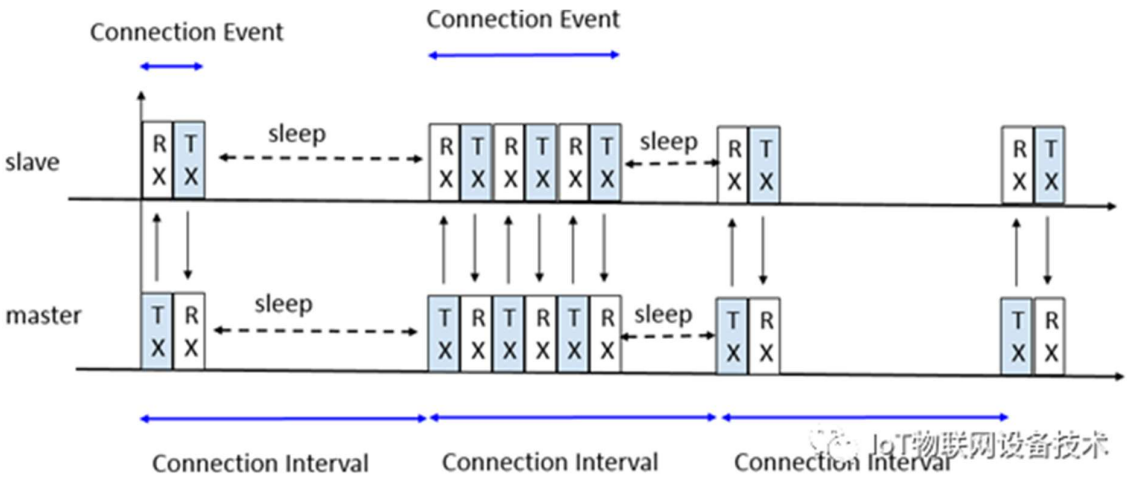
CRC:It is 24 bit in size. It is calculated with the value of PDU.It is used for detect the error in the packet. 24 bit CRC is calculated using polynomial of the form $x^{24} + x^{10} + x^9 + x^6 + x^4 + x^3 + x + 1$.

1.therorical throughput value

In BLE products, a common contradiction is the conflict between the ability and the data rate: in order to transmit fast, we need to increase the transmission rate, but increasing the transmission rate increases the

consumption.

Once a BLE device establishes a connection, the two devices exchange data periodically. The period called Connection Interval, and the interval range is 7.5ms-4s. In addition, the data to be exchanged occurs between Connection Events, and the rest of the time is in the sleep state. Even if there is no data interaction at the application layer, the link layer will exchange data (empty packets) at the Connection Interval. The longer the connection event, the shorter the sleep time.



Therefore, the connection interval determines the transmission rate. The smaller the connection interval, the faster the data is sent, but the more the power consumption.

If the connection interval is 7.5ms and each connection interval can send 125 bytes, then the unidirectional transmission rate is calculated:

1000ms / 7.5ms *125bytes = 16666 bytes/sec = 133328 bps

If there is a response, bidirectional transmission:

1000 ms / (2 * 7.5 ms) * 125 bytes = 8333 bytes/sec =66664 bps

2.PDU

When data is transmitted through BLE, the data is sent and received in the packets. Multiple packets can be sent in a connection interval. Each packet is not necessarily the same size, but the packet has the maximum maximum, so

it needs to be introduced. The concept of a PDU (protocol data unit). The maximum PDU indicates the maximum data capacity that can be transmitted in a connection interval. Different BLE protocol stacks or different chips support different values.

3.ATT MTU

MTU (maximum transfer unit) is similar to the maximum PDU. It is also used to indicate how much data can be sent in a connection interval. The concept is used in GATT interaction.

Calculation of Data Throughput：

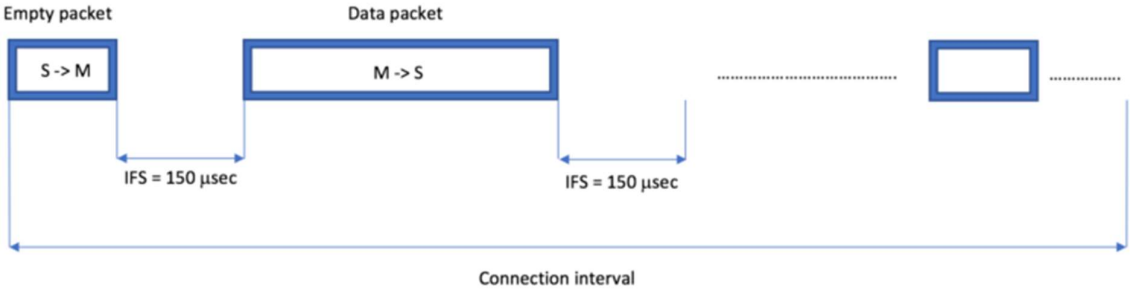
Nordic nRF51822

nRF51822 uses 1Mbps PHY. According to its specifications, a maximum of 120 bytes can be sent within a connection interval. Therefore, when the connection interval is set to 7.5ms, the maximum transmission rate is calculated:

1000ms / 7.5ms * 120 = 15960 bytes / s = 127680 bps

It can be seen that even if calculated according to the shortest connection interval, the rate was originally lower than the theoretical rate of the BLE.

Time for transmit a data packet:



Data_Packet_Time = Time to transmit empty packet + IFS + Time to transmit the actual data packet + IFS.

Time to transmit empty packet can be calculated like this:

Time to transmit empty packet = empty PDU packet size / raw data rate

An empty PDU packet include:Preamble(1 bytes) + Access Address(4bytes) + LL Header(2bytes) + CRC(3bytes) = 10 bytes= 80bits.

So the Time to transmit empty packet = 80bits/1Mbps = 80 us

A data packet include : Preamble(1 bytes) + Access Address(4bytes) + LL Header(2bytes) +PUD(255bytes maximal) +CRC(3bytes) = 265 bytes=2120 bits

Time to transmit data packet = 2120 bits/1 Mbps = 2120 us.

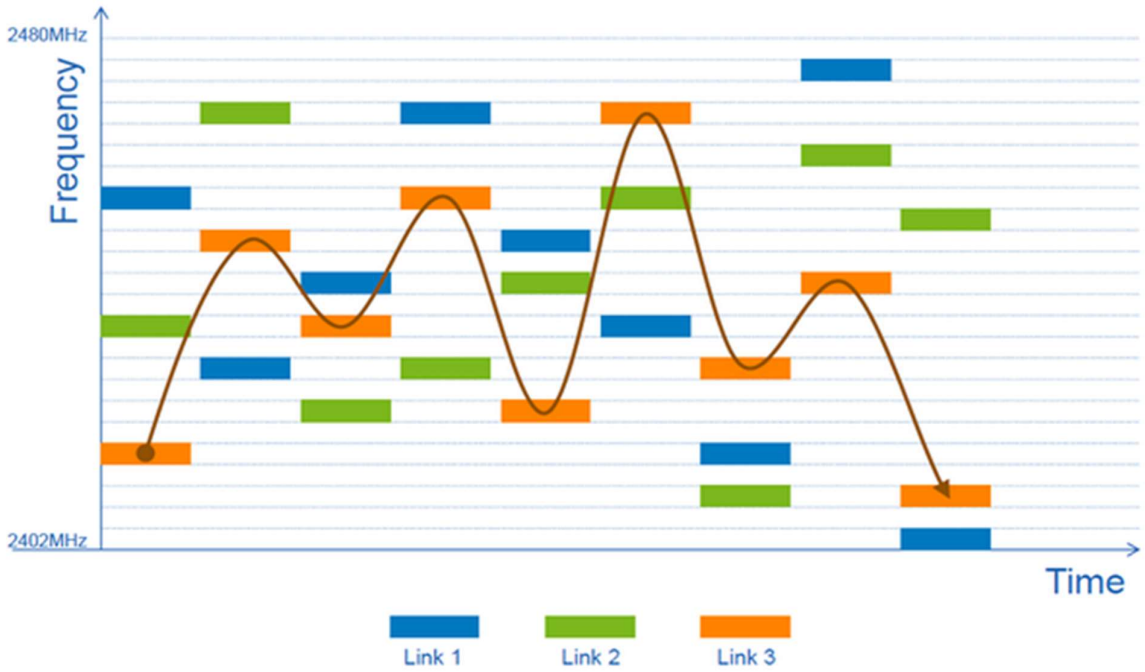
So we have Data_Packet_Time = 80us + 150us + 2120us + 150us = 2500us

4. What are the features used by BLE to reduce the effect of interferences ?

Bluetooth uses adaptive frequency hopping technology to adapt to the FM sequence to eliminate radio frequency channels that have interference, a frequency hopping algorithm is used to cycle through the 37 data channels:

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

In this equation f_{n+1} is the frequency(channel) will used for the next event. f_n is the frequency(channel) currently used, and the coefficient hop change between 5 and 16, this coefficient is created when the connection is established. It is added onto the last frequency modulo 37.



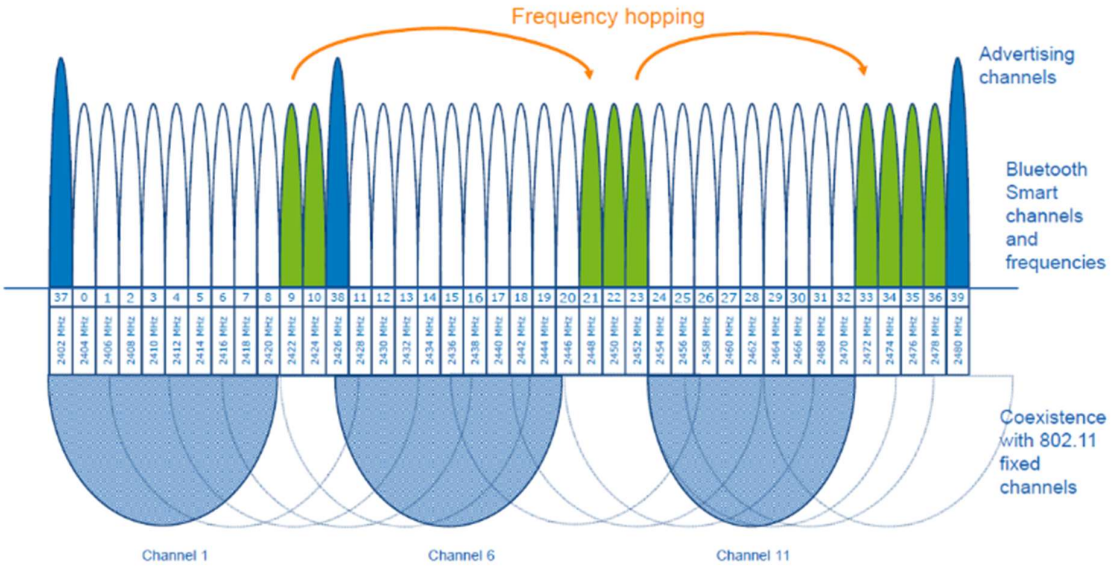
Figure：3 active BLE connections

This figure shows the performance of adaptive frequency hopping technology.

Exemple:

There is a BLE device in the same area as several WiFi networks on channels 1, 6, and 11(the area marked with blue ellipse). The BLE device would mark channels 0-8, 11-20, 24-32 as bad channels. So when the BLE device and the WiFi device are communicating in the same time, the BLE device will cycle through the channel 9,10,21,22,23,33,34,35,36 and remap

them into a good set of channels.



5. What is the maximum transmitted power ? What should be the theoretical sensitivity of a BLE receiver? What is the typical sensitivity of a BLE receiver ?

The transmitted power depends on the class of the device.
There are four classes [7] :

- Class 1: 100 mW (+20 dBm)
- Class 1.5: 10 mW (+10 dbm)
- Class 2: 2.5 mW (+4 dBm)
- Class 3: 1 mW (0 dBm)

We know that the emission power is regulated, a device can't emit too much power in the ISM band. Furthermore, battery life constraints even more the transmission power.

The receiver sensitivity is defined in BLE as the signal level at the receiver for which a Bit Error Rate (BER) of 10^{-3} is achieved. The BLE specification mandates a sensitivity better than or equal to −70 dBm. The coverage range is typically over various tens of meters.However, Bluetooth implementations typically achieve much higher receiver sensitivity levels of -95 dBm or better [2] (until -105 dBm [1]).

6. if a free space environment is considered, what is the radio range of BLE

Considering a perfect free space environment (No multipath, same polarization of the antennas..), we can use the Friis formula to compute the free-space path loss (FSPL) [6].
A convenient way to express this formula is as follow :

$$\mathrm{FSPL(dB)} = 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right)$$

For a simple link budget we got :

$$P_r = P_e - L_e + G_e + G_r - L_r - L_p$$

We can take a Class 3 device (nRF51822), Pe = 1 mW (0 dBm)
According to various specifications of common BLE chip (nRF8001, CC2564), we can take Le=Lr=2 dB
We can also choose Ge=Gr=0 dBm for the sake of simplicity.
The path loss Lp is given by the Friss formula.
The frequency is 2.4 GHz.
Sensitivity = Pr = -96 dBm

We now have only one unknown variable, the distance d. We have :

$$L_p = P_e - L_e + G_e + G_r - L_r - P_r$$

Thanks to the Friis model, we know that :

$$20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right) = P_e - L_e + G_e + G_r - L_r - P_r$$

We isolate d :

$$d = 10^{\frac{P_e - L_e + G_e + G_r - L_r - P_r - 20\log_{10}(f) - 20\log_{10}\left(\frac{4\pi}{c}\right)}{20}}$$

By putting all the numerical values, we got d = 314 m.

$$d = 10^{\frac{-6 + 96 - 20\log_{10}(2.4\cdot 10^9) - 20\log_{10}\left(\frac{4\pi}{3\cdot 10^8}\right)}{20}} = 314$$

This range seems unbelievable, and it is because of the hypothetical free space environment. Indeed such an environment is really rare in our urban areas where we use bluetooth technologies.

7. For an indoor application, evaluate the radio range of BLE. The model IEEE P802.11 will be used for this purpose (see next slide).

We have the same equation as before, but now we replace the FSPL by the equation derived from the IEEE P802.11 model.
The path loss is expressed as follow :

$$L(dB) = L_0(d_{BP}) + 35log(\frac{d}{d_{BP}})$$

We can take a typical office, with a breakdown distance of Dbp = 10m
Therefore, we got :

$$d = 10 * 10^{\frac{P_e - L_e + G_e + G_r - L_r - P_r - L_0(d_{BP})}{35}}$$

For 10meters, we got FSPL = 60 dB. Therefore we have :

$$d = 10 * 10^{\frac{-4-60+96}{35}} = 82$$

This is a much smaller value, but we understand that the attenuation due to multipath, obstacles and reflections is important in an indoor environment.

References :

[1] https://circuitcellar.com/cc-blog/ble-ics-boast-105-dbm-sensitivity/

[2] Gomez, C.; Oller, J.; Paradells, J. Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology. *Sensors* **2012**, *12*, 11734-11753. Disponible sur https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3478807/#!po=79.1667

[3]https://www.rfwireless-world.com/Terminology/BLE-Advertising-and-Data-Packet-Format.html

[4]https://microchipdeveloper.com/wireless:ble-link-layer-channels

[5]https://www.electronics-notes.com/articles/connectivity/bluetooth/radio-interface-modulation-channels.php

[6] "A Note on a Simple Transmission Formula". *IRE Proc.*: 254–256
[7] https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/radio-versions/
[8]https://www.bluetooth.com/blog/exploring-bluetooth-5-how-fast-can-it-be/

[9]https://www.nordicsemi.com/Products/Low-power-short-range-wireless/nRF52840

[10]https://www.novelbits.io/bluetooth-5-speed-maximum-throughput/

[11] https://www.bluetooth.com/wp-content/uploads/2019/03/Bluetooth_5-FINAL.pdf