INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
TOULOUSE

Bluetooth Low Energy

Summary:

Group: Aguttes - Hellouin - Kasse - Skiker

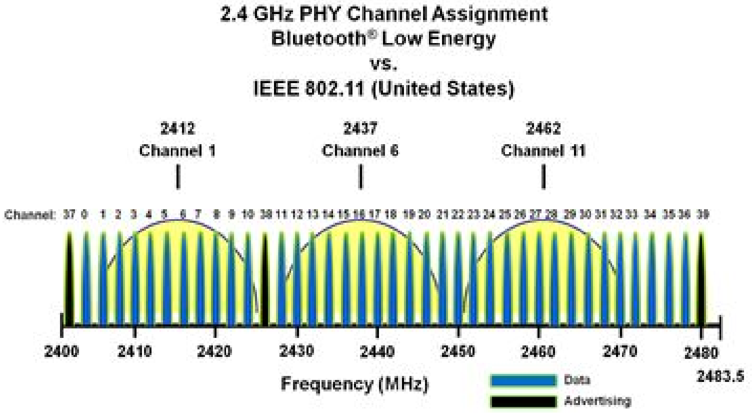
1. Physical Layer

BLE radio uses frequencies between 2402 MHz and 24835 MHz. These frequencies belong to the 2,4 GHz Industrial, Scientific and Medical (ISM) band. This band is license-free.

The BLE protocol divides the 2.4 GHz band into 40 channels.

Three channels (37, 38 and 39) are dedicated to **advertising** and allow **broadcast transmission**, **device discovery** and **connection establishment**. These 3 channels are essential for BLE to work. Since IEEE 802.11 (Wifi) also uses the 2.4 GHz band, the frequencies associated with these vital channels have been fixed in a way that limits interferences with IEEE 802.11 (see fig.1 below).

The other channels (0 to 36) are dedicated to **data transmission**. They are used for bidirectional data exchange between previously connected devices.



In unicast mode, a device can connect to an advertiser. During connection establishment, the initiator device defines a connection interval (time between two data exchanges) and fixes an algorithm called the **frequency hopping sequence**. This algorithm allows two devices to communicate using different data channels over time. Frequency hopping is fixed as follows:

Where is an integer that can range from 5 to 16. This technique is called **Frequency Hopping Spread Spectrum (FHSS)** and enables use of the full bandwidth, consequently avoiding many interferences. This process is especially relevant in this case since, as we said, WiFi uses the same frequencies as BLE.

The Link Layer can also perform **Adaptive Frequency Hopping**, using knowledge of proximity devices generating interferences to mark certain channels as “bad channels”. Then, a remapping of frequency hopping allows “bad channels" avoidance.

During transmission, BLE transmits at 1 Mb/s but this throughput rate is never really attained because of the upper layers of the protocol.

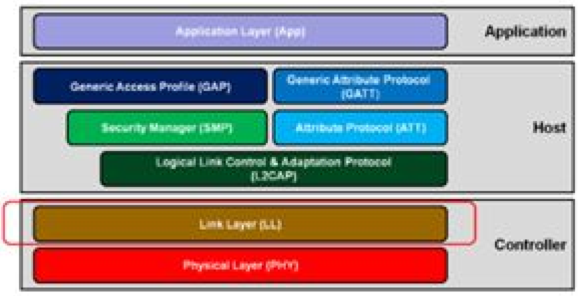
Concerning modulation, **Gaussian Frequency Shift Keying (GFSK)** is used. FSK modulation relies on frequency deviation, coding 1 as $F_{Channel\ n} + \Delta f$ and 0 as $F_{Channel\ n} - \Delta f$ where 140 kHz ≤ Δf ≤ 175 kHz. Moreover, in BLE, a Gaussian filter is applied to the modulator. This filter reduces sideband power, thus decreasing interferences with neighboring channels.

References for this part :

Bluetooth® Low Energy (BLE) Physical Layer, Microchip developer help
https://microchipdeveloper.com/wireless:ble-phy-layer
Getting Started with BLE, Chapter 2
https://learning.oreilly.com/library/view/getting-started-with/9781491900550/ch02.html#BLEProtocolBasics
Bluetooth® Low Energy Channels, Microchip developer help
https://microchipdeveloper.com/wireless:ble-link-layer-channels#adaptivefrequencyhopping
Technologie Bluetooth : Couche physique, Xavier LAGRANGE, Laurence ROUILLÉ, 10 mai 2007
https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/internet-des-objets-42612210/technologie-bluetooth-te7410/couche-physique-te7410niv10003.html

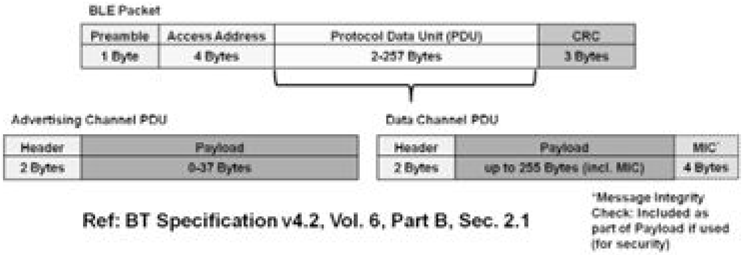
2. MAC

The Link Layer is the layer that deals with addressing and communications between devices.



Devices can play different roles : **advertiser** (A device sending advertising packets), **scanner** (a device scanning for advertising packets), **master** (a device that initiates a connection and manages it later), **slave** (a device that accepts a connection request and follows the master's timing).

Devices exchange data packets bidirectionally at a speed of around 1Mbit/s : advertising channel PDU (before connexion) and Data Channel PDU (after connexion). Advertising packets can be sent without any connection.



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

Every packet is checked in BLE protocol. There is no upper limit for retransmissions; it means that we are sure at 100% that the packet is received.

The identification of every device is possible thanks to the Bluetooth address (equivalent to MAC address). Bluetooth address is a 48 bits number and can be public or random. The master will scan during a scanning interval for the slave(s) to connect after an advertising interval. We distinguish passive scanning, with no acknowledgment to the advertiser, and active scanning, with a Request packet sent to the advertiser.

The Host Controller Interface (HCI) is a standard protocol of communication between a host (transport layer) and a controller (physical layer).

The Logical Link Control and Adaptation Protocol (L2CAP) is in charge of the transport of data in encapsulated packets between ATT and SMP protocol. It deals with fragmentation and recombination. It is possible to create own user-defined channels for high-throughput data transfer.

The Attributes Protocol (ATT) is a simple client/server stateless protocol based on attributes presented by a device. Each server contains data organized in the form of attributes, each of which is assigned a 16-bit attribute handle, a universally unique identifier (UUID), a set of permissions, and finally, of course, a value.

The Generic Attribute Profile (GATT) defines how data is organized and exchanged between applications. It is the main interface to a BLE protocol stack. There are a variety of application profiles that were developed and can be used.

The Generic Access Profile (GAP) defines how devices interact with each other at a lower level, outside of the actual protocol stack.

The Security Manager (SM) allows the generation and exchange of security keys between peers. It is involved in the pairing or bonding operations.

References for this part:

Getting starting with Bluetooth Low Energy
https://learning.oreilly.com/library/view/getting-started-with/9781491900550/ch02.html#BLEProtocolBasics
Bluetooth Low Energy

https://microchipdeveloper.com/wireless:ble-link-layer-overview

3. BLE consumption

It’s not straightforward to predict the exact BLE power consumption in a cyclic sleep scenario from the data sheet alone. Due to his technology, and the difference of hardware/firmware which could be used, lots of parameters affect the BLE Consumption. There is a large amount of power needed between a device that operates on advertised mode and devices which establish connections and engage multiple peripherals. BLE consumption will depend on:

- Chipset/radio
- BLE Stack + version
- BLE parameters
- Firmware efficiency

Let’s focus on the BLE current consumption cycle of Emission/Reception. In the graph below, you can see how different states in a BLE connexion, impact on the current consumption [1].

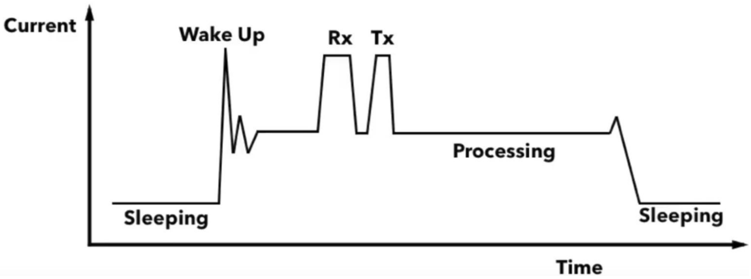


Figure 1 :Current Draw Cycle

Due to the different number of parameters related to the consumption, the easiest way to know how your BLE device consumes for sending your byte packet is to monitor your current consumption on several duty cycle. Major factor which will affect your overall consumption is the duty cycle. We select one study [2] with fixed parameters (transmit power, data to send…) which is using this method, to understand how the duty cycle impacts the overall BLE consumption. Obviously, as a result of this study, we can notify that our BLE consumption will depend mainly on the duty cycle applied due to the gap between the sleeping mode consumption (0.75 µA under 3.3V) and the wake-up state (4.5 mA under the same voltage).

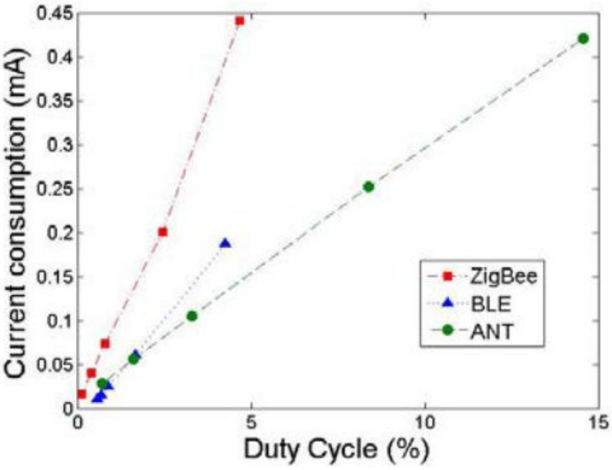
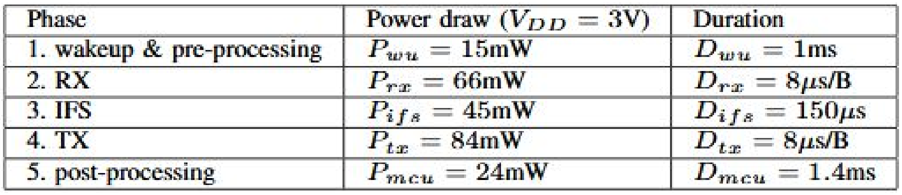


Figure 2: Mean current consumption related to the duty cycle

As you have seen previously, the sleeping mode has a low power consumption (average of 2.5 µW). Let’s focus on the awaking mode. We determine the overall energy consumption of an awaking mode as the sum of the energy consumption of each state. As you have seen in Figure 1, you have four main states (wake-up, RX, TX, processing), where we could also add an IFS state, which is a short delay between TX and RX called inter-frame (IFS). So, the final energy consumption equation during an awaking mode is set as below:

Each energy value will depend on several parameters which is hard to determine in advance, as the transmit power used, the time of processing (depends on the application), number of bytes to send/receive… However, another study [3] shows you an approach of a consumption model if you know these values. In the same study, they measured power consumption for each connection state with a monitoring experience too. You can find these values in the table below:



Phase	Power draw ($V_{DD} = 3$V)	Duration
1. wakeup & pre-processing	$P_{wu} = 15$mW	$D_{wu} = 1$ms
2. RX	$P_{rx} = 66$mW	$D_{rx} = 8\mu$s/B
3. IFS	$P_{ifs} = 45$mW	$D_{ifs} = 150\mu$s
4. TX	$P_{tx} = 84$mW	$D_{tx} = 8\mu$s/B
5. post-processing	$P_{mcu} = 24$mW	$D_{mcu} = 1.4$ms

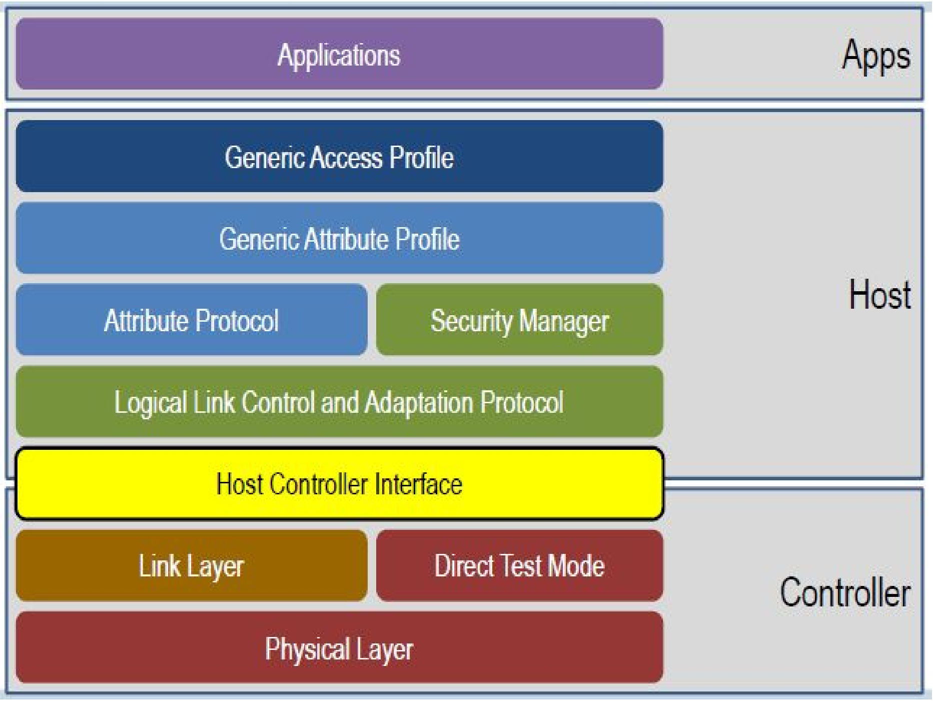
Table 1: General consumption of each state

As a result of the emission measuring, they found an energy consumption of 672 nJ per Bytes. During the reception, the energy consumption calculated is a little bit lower than the previous one, with an average of 528 nJ/B. This energy consumption range is a good estimation of what you will obtain in your common devices using this protocol.

In conclusion of this part, and in order to maximize the energy utility for a given data rate, the BLE device should transmit as many frames as possible within a single connection event and use a longer connection interval, reducing by the way the duty cycle.

4. Security

In the Bluetooth Core specification, there are three main architectural layers: controller, host, and application. Security Manager (SM) at the host layer consists of defining the methods and protocols for pairing and distributing keys, the corresponding security toolkit and the Security Manager protocol (SMP).



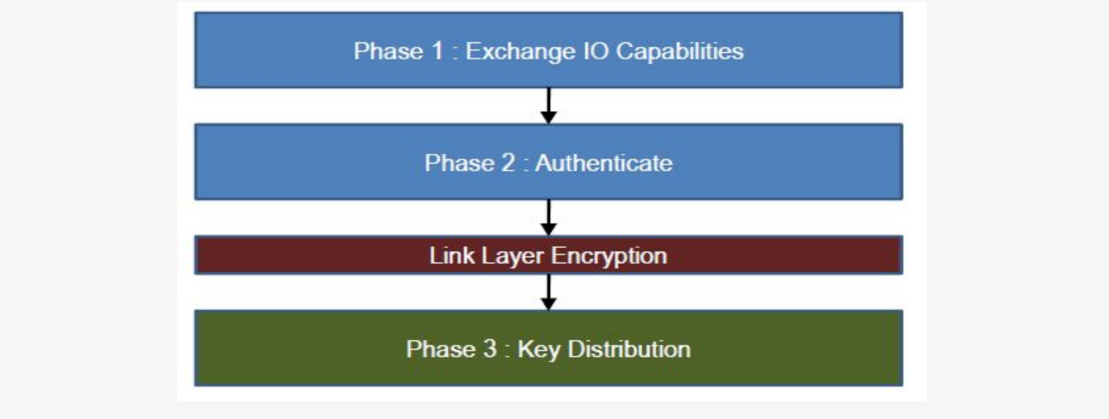
Keys can be used to encrypt a link on future reconnects, verify signed data, or perform random address resolution. In general, there are 3 phases for coupling.

Phase 1: exchange of coupling functions .

Phase 2 (LE legacy pairing): short term key generation (STK)

Phase 2 (LE secure connections): long-term key generation (LTK)

Phase 3: Distribution of transport-specific keys


Phase 1 : Exchange IO Capabilities
Phase 2 : Authenticate
Link Layer Encryption
Phase 3 : Key Distribution

Conclusion

In summary, the level of security of our object depends initially on the version of Bluetooth that we are using

It should be noted that Bluetooth Mesh now makes it possible to increase user security thanks to encryption and authentication at the network and transport layers.

Good practices :

To guard against attacks on your Bluetooth device, several solutions must be implemented. First of all, from a user's point of view, it is important not to use their device anywhere and anyhow. You must turn off your device when it is not in use, and make it non-detectable by surrounding devices except when desired. You should not accept all connections, and type your password away from prying eyes. Passwords should be long enough and random enough not to be guessed

Annexe

[1] *Introduction to Bluetooth Power Consumption*, Bluetooth Consortium Resources

[2] *Power Consumption Analysis of Bluetooth Low Energy, ZigBee and ANT Sensor Nodes in a Cyclic Sleep Scenario*, Artem Dementyev, Steve Hodges, Stuart Taylor2 and Joshua Smith, Wireless Symposium (IWS), 2013 IEEE International

[3] *How Low Energy is Bluetooth Low Energy?*, Matti Siekkinen, Markus Hiienkari, Jukka K. Nurminen, Johanna Nieminen, WCNC 2012

Article By Mark Loveless https://duo.com/decipher/understanding-bluetooth-security