INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

INNOVATIVE SMART SYSTEMS

Communication Protocols for IoT

BLE - Bluetooth Low Energy

Supervisor:
D. Dragomirescu (INSA/LAAS)

Students:
BACLE Lucas, ESTIVAL Emilie,
POTIERS Léo, SERONIE-VIVIEN Paul

2020-2021

Introduction

Bluetooth technology is a wireless networking protocol designed to quickly and remotely connect devices to computers or to each other. It can be used to connect cell phones to each other in order to exchange photos, to connect peripherals to a computer (mouse, keyboard, printer, etc.) or to connect headsets to cell phones to make hands-free calls (Bluetooth car kit). Bluetooth devices automatically detect and connect to each other, making communication much easier.

There are two forms of Bluetooth: Bluetooth Classic and Bluetooth Low Energy, or BLE. Our object of study will be BLE, because it is widely used as a protocol for the IoT. What makes BLE so interesting compared to other wireless protocols is that it's the easiest way to design a product able to communicate with any modern mobile platform (iOS, Android, etc.). Bluetooth Low Energy technology is a very low-power alternative for sensors and accessories. It is ideal for applications that do not require a continuous connection, but require a long life battery. It is not yet compatible with audio broadcasting, but it is compatible with remote controls, for example.

In this report, we will first describe the specificities of BLE on the physical layer and MAC layer. Then we will see what its advantages are in terms of energy consumption, and then we will see what security issues are associated with this technology.

I. Physical layer

When it comes to BLE, the first part of the controller that needs to be described is the physical layer (PHY) since it is the lowest layer of the protocol stack. This layer uses **analog communications circuitry** that will allow the translation of digital symbols over the air. The services provided by this layer go directly to the link layer (LL) that will be treated later.

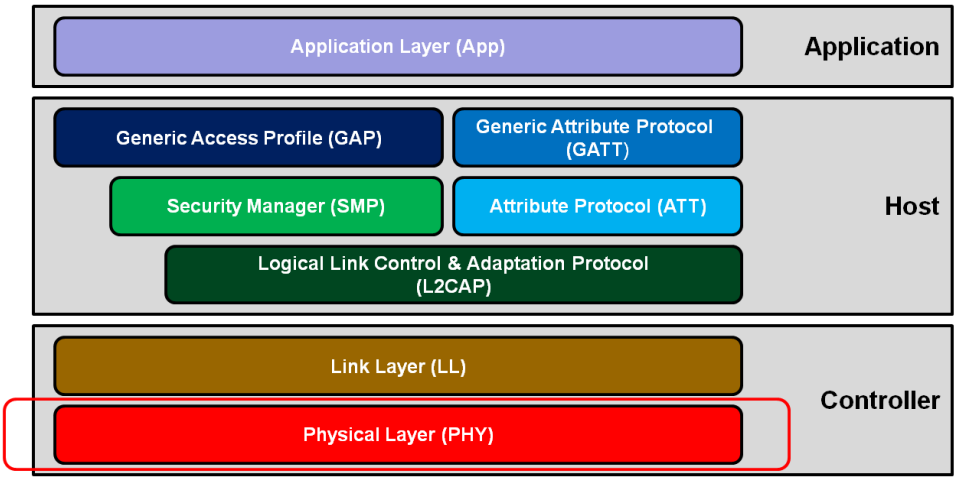

Figure 1 : Protocol stack

BLE uses a Gaussian Frequency Shift Keying (GFSK) modulation in the 2.4 GHz range. This modulation is mostly used to make the changes of frequency smoother. When BLE is transmitting data, one million bits per second are sent with one bit per symbol. The technique to send a binary value is quite simple : a positive frequency deviation is used to send a 1 and, on the opposite, a negative frequency deviation is used to send a 0. BLE has **40 different channels** that are spaced by 2MHz (from 2.4GHz to 2.8GHz). These channels can be of two different types. First, the advertising channels (only 3 out of the 40, channels 37, 38 and 39), that are mostly used for device discovery, establishment of the connection and broadcast transmissions. Then, there are the data channels that represent most of the channels (from channel 0 to 36) and that are mostly used for bidirectional communication, once the connection has been made with another device.

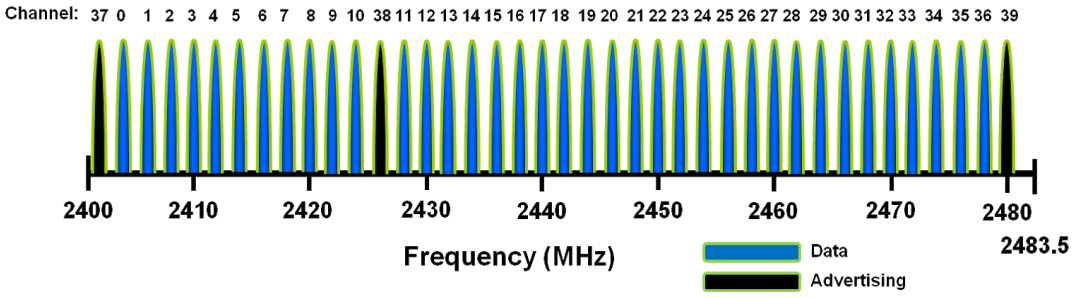

Figure 2 : BLE channels

It is important to note that the range where BLE operates is quite noisy because of WI-FI and others so the advertising channels, the one responsible for finding and getting found by other devices, are placed **outside** of this range, so the link layer can be more robust.

II. Link layer

The BLE Link Layer directly interfaces to the physical layer. It provides the first level of **control** and **data structure** over the radio operations and bit stream transmission and reception. It defines the device address, packet formats and timings, reliability, some security, link layer operations, and BLE state machine.

Two medium access control modes are used : Frequency Division Multiple Access (**FDMA**) and Time Division Multiple Access (**TDMA**). As described earlier in this report, BLE uses 40 frequency channels. The master determines the instants in which slaves are required to listen, and thus coordinates the medium access by using a Time Division Multiple Access (TDMA). A **frequency hopping** scheme is implemented for robust operation. The next channel to use is computed using this basic formula $f_{n+1} = (f_n + hop) \ mod \ 37$, where hop is negotiated at the establishment of a connection. It is important to notice that BLE devices implement a mechanism permitting to remap a given packet from a known bad channel to a known good one at runtime to minimize the interferences influence. This means that two devices communicating must cycle through the channels and remap those to a set of less crowded channels.

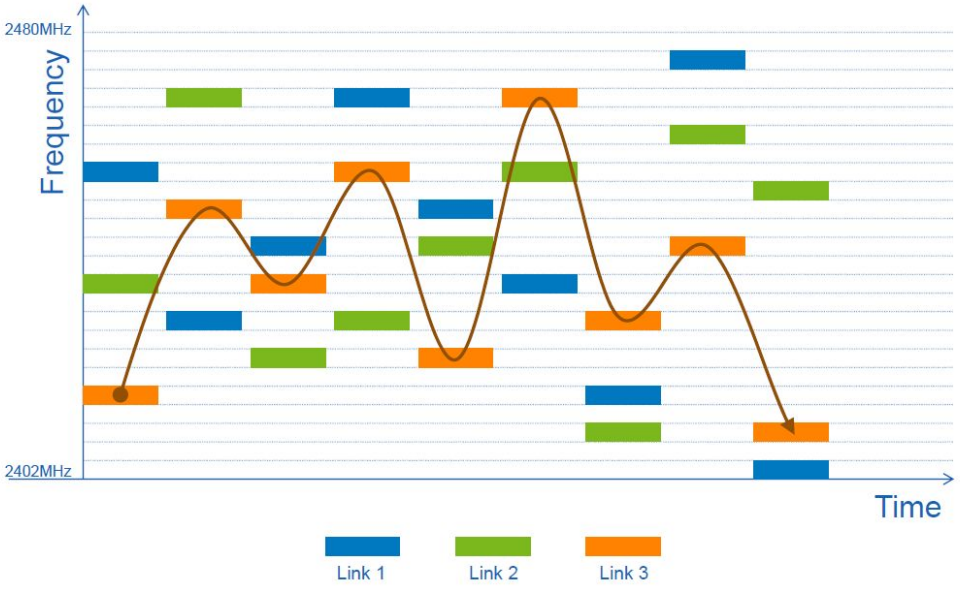

Figure 3 : Example frequency hopping scenario

BLE Link Layer makes three types of network topologies possible. First is the **point-to-point** used for establishing one-to-one (1:1) device communications. As a huge number of slave devices can be connected to a single master, this makes tree (as proposed by Texas Instruments) and star (also called Piconet) network topologies possible. Second is **broadcast**, a network topology used for establishing one-to-many (1:many) device communications. This topology can be used for localized information sharing and is ideal for location-based services such as retail point-of-interest information, indoor navigation and wayfinding, as well as item and asset tracking. Finally, **mesh** is a topology used for establishing many-to-many (m:m) device communications. It enables the creation of large-scale device networks and is ideally suited for control, monitoring, and automation

systems where a maximum of 32,767 devices need to reliably and securely communicate with one another.

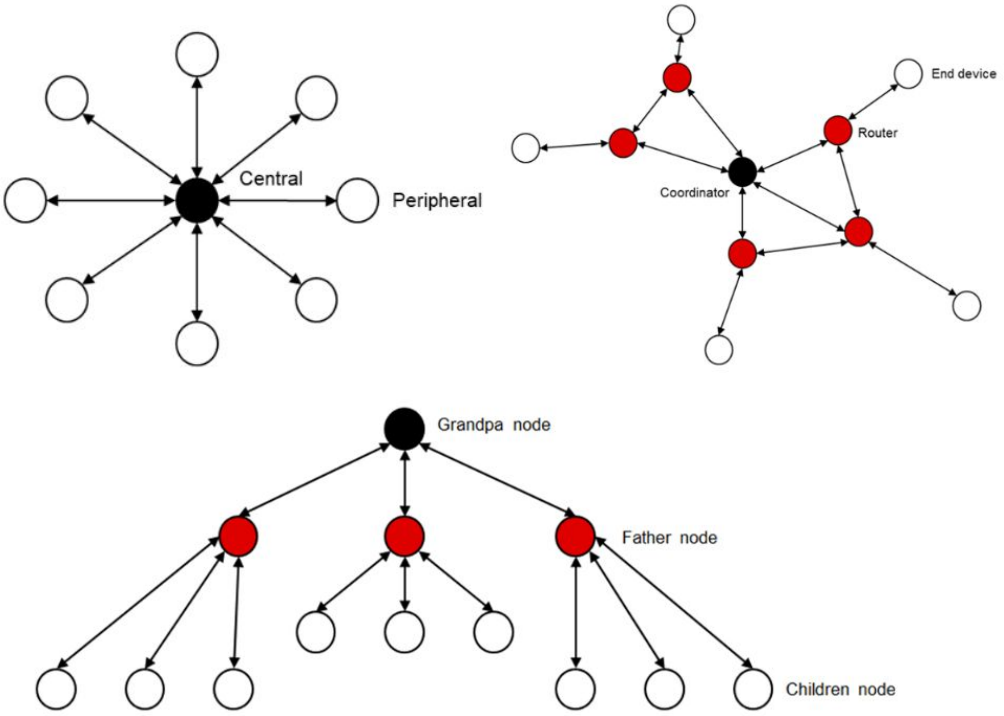

Figure 4 : Star, mesh and tree network topologies

Once connected, the Link Layer acts as a reliable data bearer. All packets received are checked against a **24-bit CRC** and unlimited re-transmissions can be requested until the other devices acknowledge. This happens during the next connection event.

With exception of the broadcast topology, the link layer is also responsible for ensuring **encryption** of the communication if required. Where in a BLE connection data within the payload must be encrypted the BLE Link Layer uses the **AES-128** block cipher for authenticated encryption using Cipher Block Chaining-Message Authentication Code (CCM) mode. Encrypted packets also include a Message Integrity Check (MIC) value to authenticate the validity of a sender, as well as packet counters to prevent replay attacks.

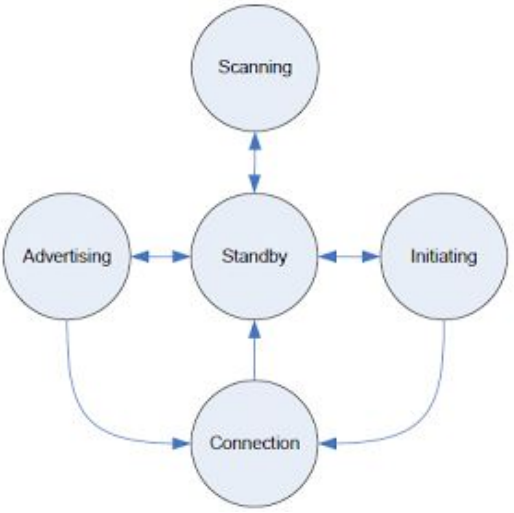

Figure 5 : BLE Link Layer state machine

The BLE Link Layer's behaviour can be represented by a state machine having the following five states : Standby, Advertising, Scanning (Active, Passive), Initiating, Connection (Master, Slave). BLE packets can be divided in two event types : Advertising and Connection events. State transition depends on those, and can trigger the following BLE main operations : advertising, scanning and connection establishment.

Advertising Channel Usage

- Device discovery
- Connection establishment
- Broadcast transmissions

Data Channel Usage

- Bidirectional communication between connected devices
- Adaptive frequency hopping used for subsequent connection events

According to the states of its link layer, a BLE device can have one of the following fives roles as described by Silabs :

- Advertiser: A device that broadcasts advertisement packets, but is not able to receive them. It can allow or disallow connections.
- Scanner: A device that only listens for advertisements. It can connect to an advertiser.
- Slave: A device connected to a single master (BT 4.0) or multiple masters (BT 4.1 and newer).
- Master: A device that is connected to one or more slaves. Theoretically a master can have an unlimited number of slave devices connected to it, but in practice the master can connect 4-20 slaves at a time.
- Hybrid: It is possible for a device to advertise and scan at the same time or be connected to a master and advertise or scan simulta-neously. This is, however, vendor-specific, and the exact features that are supported should be checked with the vendor.

III. Power consumption

The Bluetooth Low Energy standard was developed with long battery life in mind, allowing for devices that can last anywhere from several months to several years while operating on a single coin-cell battery. This is possible thanks to the power efficiency of Bluetooth Low Energy protocol, which only transmits **small packets** as compared to Bluetooth Classic.

Technical specification	**Bluetooth Basic Rate/Enhanced Data Rate technology**	**Bluetooth Low Energy technology**
Power consumption	1 W as the reference	0.01–0.50 W (depending on use case)
Peak **current consumption**	<30 mA	<15 mA

Figure 6: Table comparing the characteristics between Bluetooth classic and BLE

In Figure 5, we can see that peak current for BLE is two times lower than for Bluetooth Classic. Attention must be paid when it comes to power metrics in BLE. Devices are often rated according to their peak current, but in the case of BLE the device will only be consuming current at the peak level while it is transmitting (connection event) as it is shown below.

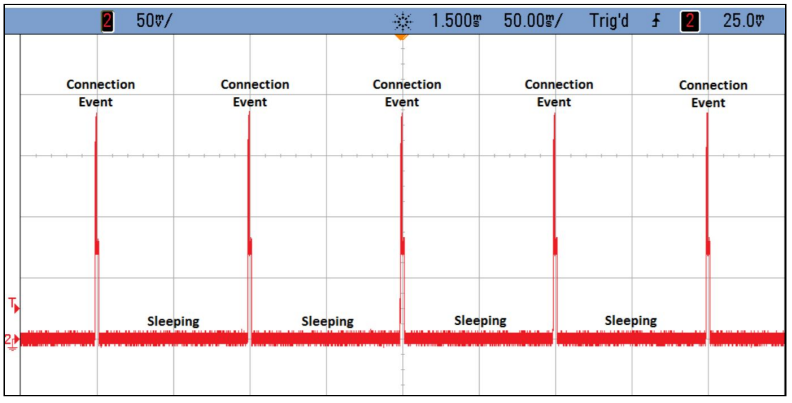

Figure 7 : Current Consumption versus Time during a BLE Connection

A particularity of BLE devices is to transmit only for a small percentage of the total time that the device is connected. When not transmitting, the device is in sleep mode. So the best way to evaluate the consumption of a BLE device is to measure its **average current**. This value can be used to determine the battery life of a device running the BLE stack. But average current is highly dependent on the connection parameters used, so it can't be specified in a datasheet for example. Every time an "average current" specification is given, it is very important to understand the exact **use-case** under which the measurement was made. Figure 5 specifies a wide scale of power consumption for BLE from 2 to 100 times lower than Bluetooth Classic. The width of this range can be explained as we just said by the fact that BLE power consumption is very dependent on the use case.

Current consumption is a major concern in battery-powered products. Optimizing current consumption extends battery life and, as a result, makes better products. Bluetooth Low Energy is basically designed to enable devices to have very low power consumption. It allows it to have a low impact on the batteries, thus increasing their life span. This is a significant advantage for systems where batteries cannot be changed frequently for example. A study[1] by beacon software company *Aislelabs* reported that peripherals such as proximity beacons[2] usually function for 1–2 years, and even 3 to 4 years in best cases, powered by a 1,000mAh coin cell battery. In contrast, a continuous scan for the same beacons in the central role can consume 1,000 mAh in a few hours.

But what can really affect power consumption in BLE ? The two main factors affecting current consumption in a Bluetooth Low Energy device are the **amount of power** transmitted and the total **amount of time** that the radio is active (TX and RX). The amount of transmit power required depends on the range required between master and slave. Range is greatly affected by the environment such as obstacles and the amount of 2.4 GHz (BLE range) traffic present. The amount of time that a radio is active is determined by how often the radio must transmit or receive and the length of time required to transmit or receive. So we can deduce that a longer connection interval will help improve battery life but will also reduce throughput and may result in an unreliable or unstable connection. A lot of parameters can be adjusted in order to find the best ratio.

[1] https://www.aislelabs.com/reports/beacon-guide/

[2] **Bluetooth beacons** are hardware transmitters - a class of BLE devices that broadcast their identifier to nearby portable electronic devices. The technology enables smartphones, tablets and other devices to perform actions when in close proximity to a beacon.

IV. Security

Nowadays, because Bluetooth Low Energy is becoming one of the most common wireless standards in use, it is also becoming more commonly used in applications where sensitive information is being transferred. Thus, security should be one of the first priorities of connected objects designers in order to protect the privacy and the security of consumers.

However, the main security issues with the pairing process and BLE in general are passive eavesdropping, man in the middle (MITM) attacks and identity tracking.

Passive eavesdropping is the process by which a third device listens in to the data being exchanged between the two paired devices. The way that BLE overcomes this is by encrypting the data being transferred using AES-CCM cryptography, as explained in previous pages. While AES encryption is considered to be very secure, the key exchange protocols that BLE uses can introduce some severe security vulnerabilities which would allow an attacker to decrypt the data. Thus, the method by which the keys are exchanged, referred to as the "pairing method" or "association model", has a great effect on the security of the connection.

MITM attacks are when a third and malicious device, impersonates the other two legitimate devices, in order to fool these devices into connecting to it. In this scenario, both the central and peripheral devices will connect to the malicious device which redirects the communication route of the two other devices to himself. This gives the legitimate devices the illusion that they are directly connected to each other when in fact their connection has been compromised. As well as enable the malicious device to intercept all the data being sent, this set up also allows it to inject false data into the communication or remove data before it reaches its intended device. As with passive eavesdropping, the pairing method used determines how resilient the BLE connection will be to MITM attacks.

Identity tracking is when a malicious entity is able to associate the address of a BLE device with a specific user and then physically track that user based on the presence of the BLE device. The way BLE overcomes this is by periodically changing the device address. But in fact, it happens that many devices do not change their address, or keep a part of the address similar after the randomization process so they still can be tracked.

But we can remember that at its beginning, classical Bluetooth was not very secured either, and it is much more so now. BLE architects and connected objects designers wishing to use BLE will improve the security process release after release and it will become safer. In the earlier versions of BLE (4.0 and 4.1), the encryption was vulnerable to a brute-force attack so the connection was very vulnerable to passing eavesdropping attacks. But even the updated version called BLE Secure Connection is still vulnerable to MITM attacks, some work still needs to be done on that point.

Conclusion

In this study, we first explained how the physical layer enables data transmission thanks to its multi-frequency channels. Secondly we presented the MAC layer and the way this layer enables data encryption. In a third time, we tackled the main advantage of BLE which is its low energy consumption and how the size of transmitted packets, the peak current consumption and its dependency with the use-case. Finally we tackled the security aspect of this communication protocol and we figured out a few lacks of security.

However, Bluetooth Low Energy is more and more used in many IoT objects of our ordinary life and it enables an efficient communication between devices. Sales of BLE devices are forecast to triple by 2023 to 1.6 billion annual shipments. Therefore, we can imagine that this protocol will be frequently used to carry our personal data transmitting from our connected devices. Hopefully, the next versions of this protocol will increase its security in order to protect even more the consumer's data.

Bibliography

Physical layer

- https://microchipdeveloper.com/wireless:ble-phy-layer

Mac layer

- https://blog.groupe-sii.com/le-ble-bluetooth-low-energy/
- https://microchipdeveloper.com/wireless:ble-link-layer-overview
- https://www.silabs.com/documents/public/user-guides/ug103-14-fundamentals-ble.pdf
- https://www.ti.com/lit/an/swra648/swra648.pdf?ts=1608038366880&ref_url=https%253A%252F%252Fwww.ti.com%252Ftool%252FLAUNCHXL-CC26X2R1

Power consumption

- https://en.wikipedia.org/wiki/Bluetooth_Low_Energy
- https://discourse-production.oss-cn-shanghai.aliyuncs.com/original/3X/7/c/7c84d1dc683e86d61f4db95f90223453fc25861f.pdf
- https://learn.adafruit.com/introduction-to-bluetooth-low-energy/introduction
- https://docs.silabs.com/bluetooth/2.13/general/system-and-performance/optimizing-current-consumption-in-bluetooth-low-energy-devices

Security

- https://www.researchgate.net/publication/336360887_B_Bluetooth_Low_Energy_BLE_Security_and_Privacy