INNOVATIVE SMART SYSTEMS

INSA TOULOUSE, DGEI

TOWARD IINTERNET OF THINGS

Let’s talk about BLE

Authors:
Pierre PRIE
Axel BAYLE

January 22, 2019

Summary

Introduction

The Bluetooth Low Energy (BLE), or Bluetooth Smart is a new standard introduced in 2010 as part of the Bluetooth 4.0 Core Specification. Originally designed by Nokia as Wibree before being adopted by the Bluetooth Special Interest Group (SIG), BLE has an entirely different technology than the classic Bluetooth. BLE is a radio standard design with a focus on lowest possible power consumption, optimized for low cost, low bandwith and complexity. BLE has become more and more popular and is, nowadays, supported on almost all phones, android, IOS, blackberry and windows devices and becomes a standard of communication. With its success and the devellopment of the IOT world, Bluetooth 5.0 specification was realesed in the early 2017 to better meet the needs of IOT developers and consumers.

In this paper we will try to go throught the original BLE protocole and explore it main characteristics. We will first present an overview of the BLE standard. Then we will detail the PHY layer with the access to the channel, following by the security and the routine and finally we will present some usages and application of BLE. In those different parts, we will briefely present the improvment of the 5.0 specification to the 4.0 BLE specification, if it is relevant.

Chapter 1

Overview

As we said, the BLE standard is complitely different from the classical Bluetooth standard. That means that those two wireless communication standards are not directly compatible and old Bluetooth devices cannot communicate directly with new BLE device (single-mode device), that is why Dual-mode devices have been design. Those dual-mode devices implements both standards and can communicate with any Bluetooth device. Phones, Tablets and PCs are the typical existing dual-mode devices.
The Bluetooth 5.0 specification brought to the desgin of new Bluetooth 5.0 cells. Indeed, evenif the "old" BLE cells from the 4.x standards are still workings and can communicate with the "new" cells from the BLE 5.0 standard, they can't be udapted because of the modifications on the physical layer needed with the new BLE 5.0 standard.

BLE devices are devided on three major blocks with various layers for each of them. The picture 1.1 illustrate the strucutre of the BLE device.

- The application is the highest layer, it contain the user interface and all the logic depending on the purpose of the current application.
- The Host is on charge of the highest layers that leads to the application. It control the connexion, data and security managment and also the profils definitions.
- The Controller is on charge of the lowest layers which controll the access to the radio channel with all the requiered adjustments (time and fruency syncronisation) and the transmission and reception of frames.
- The Host Controller Interface (HCI) is a standardized communication protocol between Host and Controller.

BLE devices have two diffrent ways to communicate, by braodcasting or connections. This two communications methodes involved four possible role defines by the Generic Access Profile (GAP) layer and the Link Layer (LL):

- The broadcaster (GAP) or advertiser (LL) : sends advertising packets to anyone who is listenning whitout any security or privacy protocole.

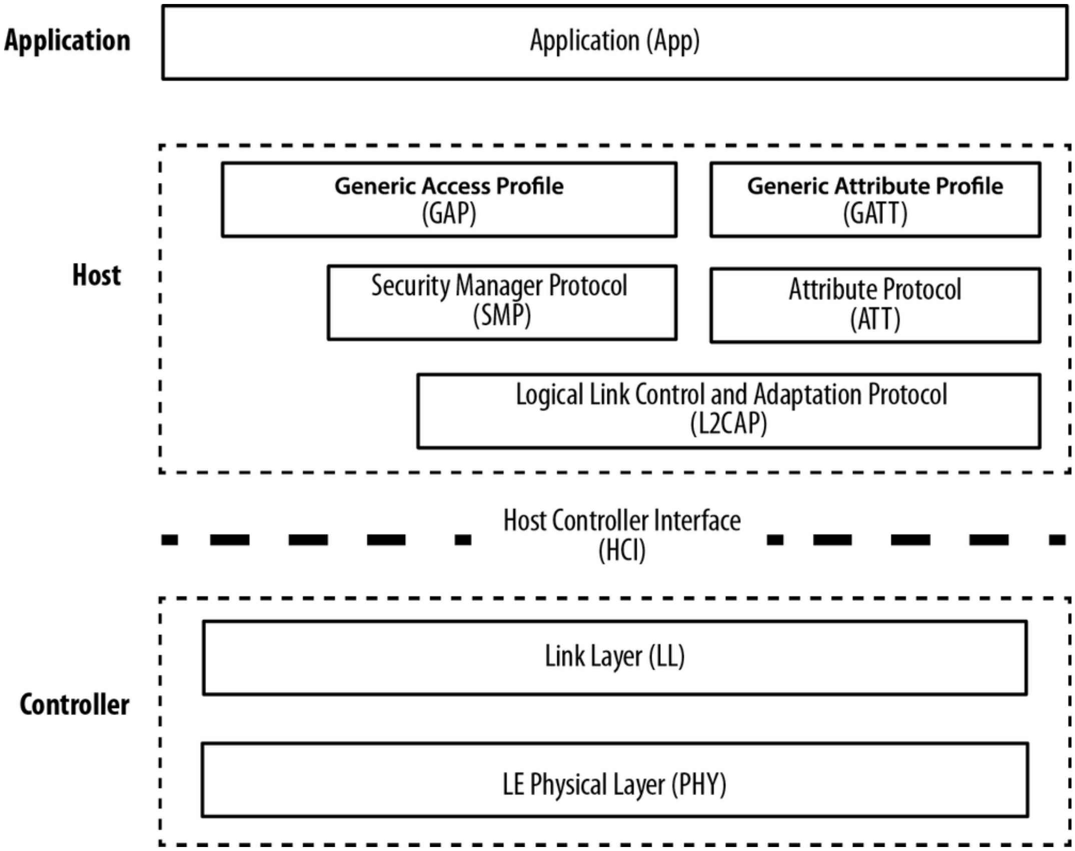

Application
Application (App)
Host
Generic Access Profile (GAP)
Generic Attribute Profile (GATT)
Security Manager Protocol (SMP)
Attribute Protocol (ATT)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Controller
Link Layer (LL)
LE Physical Layer (PHY)

Figure 1.1: Architecture of the BLE protocol stack

- The observer (GAP) or scanner (LL) : scans for broadcasters, listening for advertising data
- The Central (GAP) or master (LL): Can establish and manage a connection with one or more devices
- The Peripheral (GAP) or slave (LL) : can accept or ask for one or more connection with other devices

The Generic Attribute Profile (GATT) layer defines the two data communications role :

- The Server : Contains the data to be monitored. He sends the data in request from a Client. The serveur is typically associated with the Link Layer Slave and the GAP Peripheral device role.
- The Client: Sends request to a Server for datas. The client is typically associated with the Link Layer Master and the GAP Central device role.

With those ways of communication the BLE Network is supossed to have a Star-bus topology. But with the BLEv4.2 and BLEv5.0, a device can be connected to severals others and be at the same time Central and Peripheral or Broadcaser and Observer. So the Network topology tend to evolved to a Mesh topology with a teoretical unlimited number of Nodes.

Let's speak about the energy consumption of a BLE device. The measurement have been made with a Texas Instrument CC2541 chip operating as a GAP "Peripheral" in a BLE connexion[1]. The current consuption vary accordingly to the state of the device, the measure have been made with the longest awake time of the device during the cycle (total of 1 second):

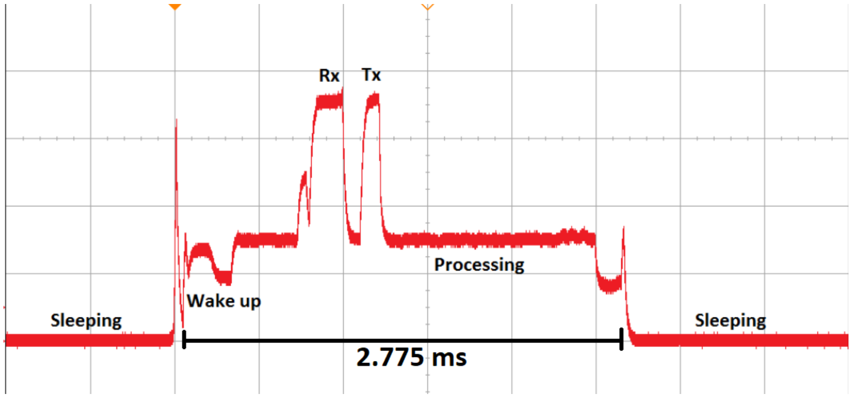


Figure 1.2: Current Consumption versus time during a single connection event for a peripheral device

- State 1, wake-up : 400 µs - 6 mA
- State 2, pre-processing : 315 µs - 7.4 mA
- State 3, pre-Rx : 80 µs - 11 mA
- State 4, Rx : 275 µs - 17.5 mA
- State 5, Rx-to-Tx : 105 µs - 7.4 mA
- State 6, Tx : 115 µs - 17.5 mA
- State 7, post-processing : 1325 µs - 7.4 mA
- State 8, pre-Sleep : 160 µs - 4.1 mA
- State 9, Sleep : 997.225 µs - 0.001 mA

With this table, we found a consumption of 8.5312 mA during the 2.775 ms of wake time using to sent a payload of 255 Bytes. That mean an average current of 0.0247 mA during the whole cycle (1 second).So during 1 cycle of 1second we use 0.0247 mA to send 255 Bytes of data. That mean each Byte needs 97.9 nA to be sent.

[1] Datas from the fallowing article :Measuring Bluetooth Low Energy Power Consumption By Sandeep Kamath and Joakim Lindh, `http://www.ti.com/lit/an/swra347a/swra347a.pdf`

Chapter 2

PHY layer & Access to the channel

The Bluetooth Low Energy operates in the same spectrum range, 2,4–2,4835 GHz ISM band, as the normal Bluetooth. It uses 40 channels, 3 for unidirectional advertising and 37 for bidirictional communication. All the communication are based on frequency hopping and has a bitrate of 1Mbps with 1 bit per symbol. That's why it is a good way to send small datas, or small chunks of data quickly.

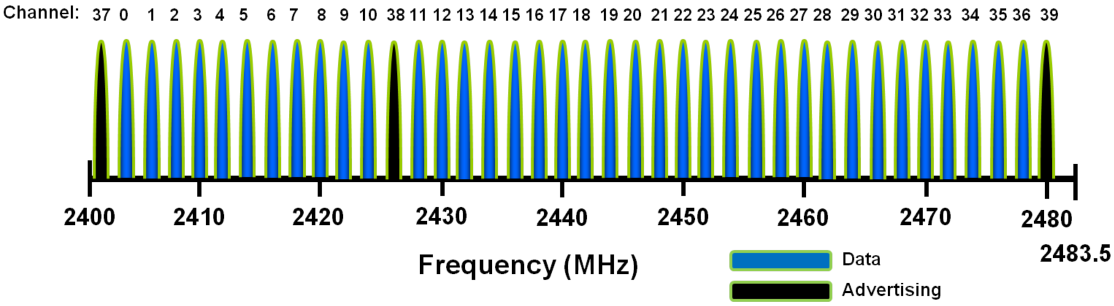


Figure 2.1: BLE channels

To handle several communications at the same time the BLE used both TDMA and FDMA. The TDMA allows to have different time slots for defferent transmitter. The FDMA is used to change the frequency of emmission and by going this to use the whole BLE spectrum.

To manage the FDMA during a data communication there is an algorithm to calculate the frequency hopping throught the channels. The fomula is :

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

That allow to know the frequency to use during the next connection event. The hop variable is a value in the range 5-16 and it is at the creation of the connection. The figure belows show examples of three simultaneous communications and the frequency hopping associated.

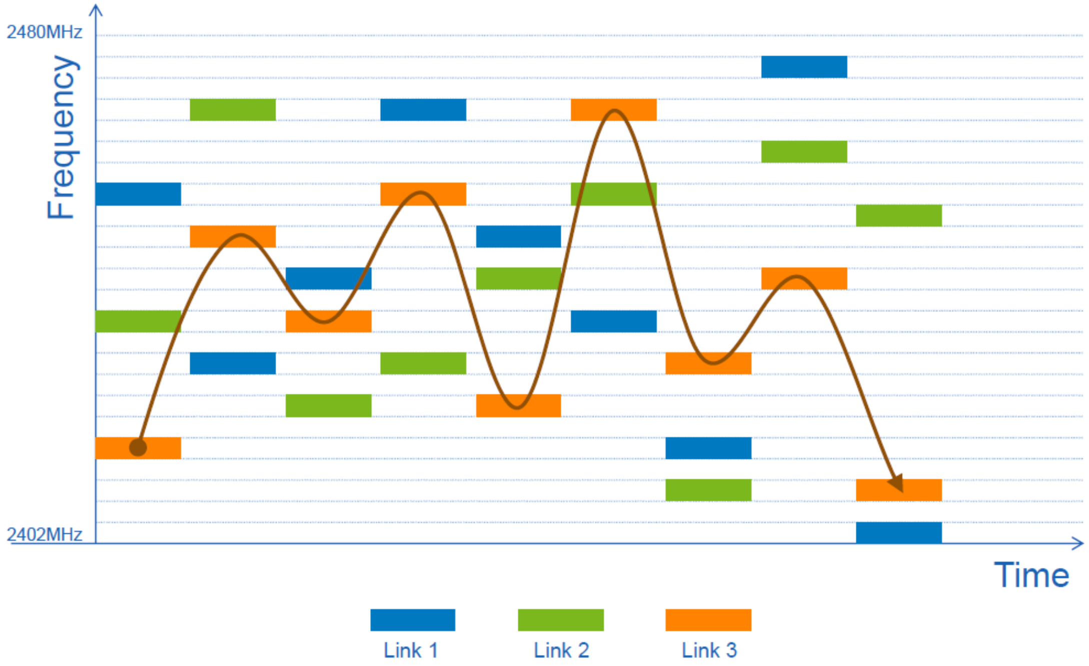
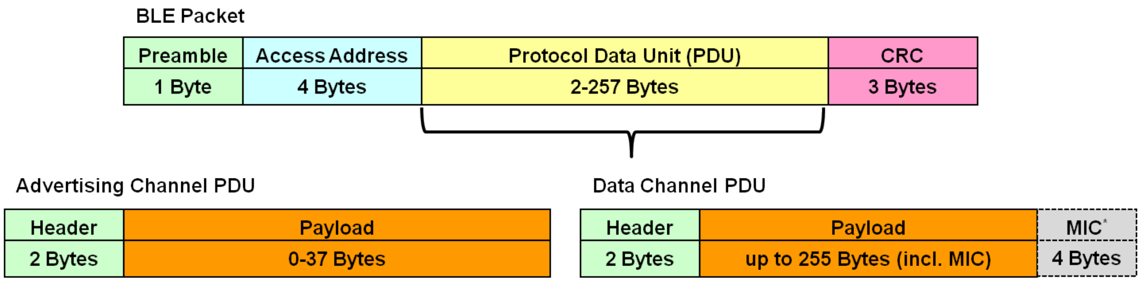


Figure 2.2: BLE frequency hopping illustration

The BLE frames are almost the same for both advertising and data channel. They both had 1 byte for the preamble, 4 bytes for the adress of the master (access adress), then the Protocol Data Unit (PDU). That is the field that change between data and advertising. In the case of data message, the PDU were 2-39 Bytes with BLE 4.0 and BLE 4.1 and it is 2-257 Bytes since BLE 4.2. For the advetising message, the PDU size change with BLE 5 and became 2-257 Bytes just as the data message. This increase of the size of the broadcast message is a big step to better beacons with BLE devices. Finally, the CRC field is the result of a calculus to avoid redundancy. They are several length of CRC but BLE uses the 24 bytes version.



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

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

Figure 2.3: BLEv4.2 frame composition

The most important changes introduced by the new 5.0 BLE specifications are related to the PHY layers. The BLE 5.0 devices now have tree PHY layers : LE 1M, LE 2M and LE Coded. The LE 1M layer is basicly the "old" PHY layer from the BLEv4.x specification, with a 1Mbps bitrate.

The new LE 2M allows to send 2Mbps which is 1.7 times faster than the LE 1M traditionnal layer (counting the interval between packet who remain the same). With this new layer, the radio will take less time to sent the same amount of data than usual, providing a further benefit of reducing power consumption that results in increasing battery life.

The new LE Coded uses a combination of lower data rates of 125kbps or 500kbps. That allows to have a S = symbol/bitrate higher than with the LE 1M, LE 2M where S=1 and then increase the sensitivity and then the range. S = 2 for 500kbps ans S = 8 for 125kbps which brings to increase the communication range by 2 for 500kbps data rates and by 4 for 500kbps data rates.

Finaly, the use of one or an other PHY layer is define by software and can then be modified "on the fly", by the application via the HCI, regarding to the needs of the application or the situation.

Chapter 3

Routine & Security

3.1 Connection Routine

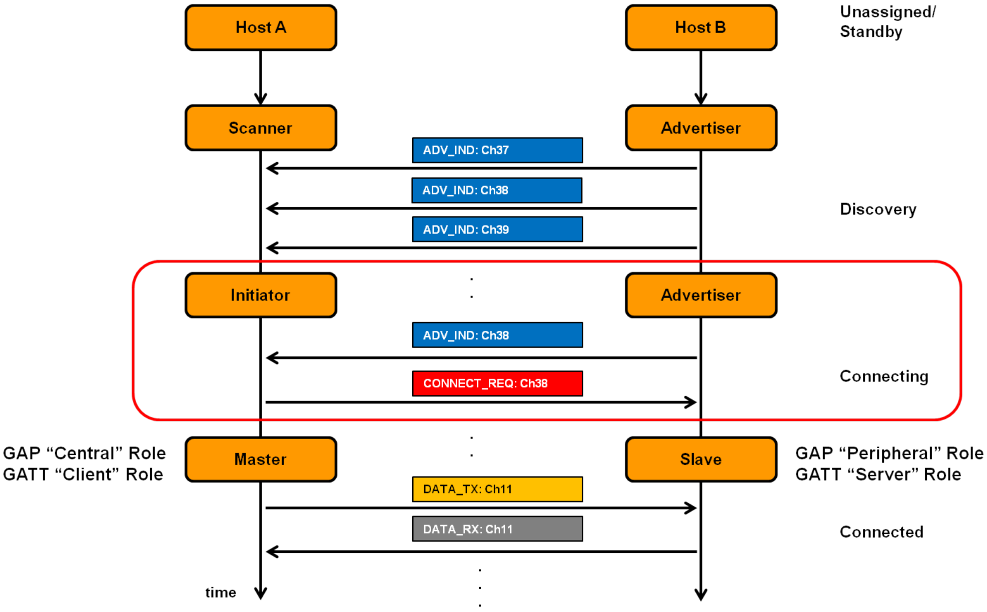


Figure 3.1: BLE connection routine

The BLE connection routine is quiet simple, an host start advertising, called the Advertiser, and another one is listenning, called the Scanner, when the scanner find a suitable advertiser, depending on the PDU’s payload. Then it will start the communication, it become the Initiator, and send a connection request to the Advertiser, this request include, frequency hopping, connection interval, latency,timeout... After this exchange, the connection is done and the data communication can start, the Initiator become the Master, and the advertiser the Slave.

3.2 Security

An important point it's that only the data exchange can be secure, by the way, the discovery and the connectiong stage are un-encrypted. When some devices want to have a secure exchange they have to pair themself and exchanging their keys. The security of the communication is ensure by the encryption of the payload. In that case the payload include 4 bytes of MIC, the aim of the MIC is to ensure the secutity. Indeed it allows to identifiate the emitter of the message and prevent replay attack by integrating a packets counter.

But the BLE, as the classic Blueetooth, remain weak and there are a lot of exemple of hacking or security breach on the internet.

Chapter 4

Usages & Applications

Because of its simplicity and its rapidity, the BLE is a good option for IoT solutions. Moreover, the low energy consumption allows it to be embeded in self-power application. For example, there a lot of smart home objects using BLE because they don't need a high range. You can also find BLE include on some fitness monitoring bracelet.

According to the Bluetooth SIG article posted on July10,2018, the BLE market increase each year.and represent 550 million shipment in 2018, and they are planing around 700 million shipment in 2020.

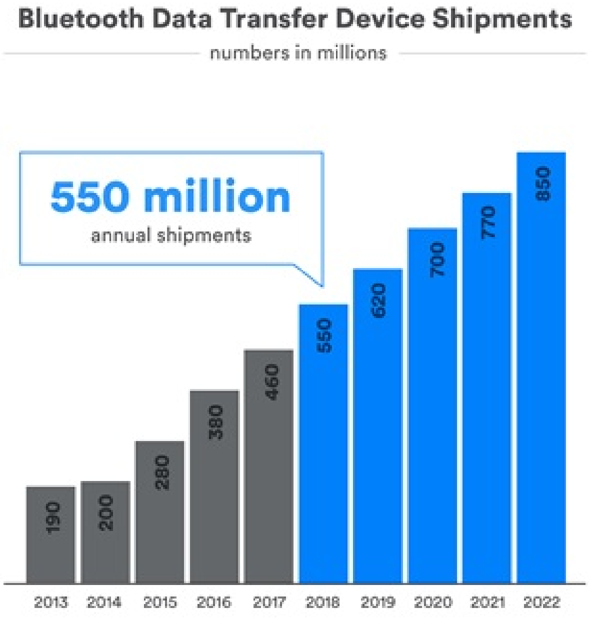


Figure 4.1: BLE Market growth

Conclusion

The BLE is one of the preferred protocol for IOT as ubiquitous on equipment such as smartphonse, computers and connected cars. The Bluetooth Smart or Low Energy has been design to be efficient with a low power consumption and a little security. The last bluetooth standard released, bluetooth 5.0 aims to offer significant performance regarding the speed, range and broadcasting capacity of the devices to better adress the needs of the IOT market.

Sources

- Getting Started with Bluetooth Low Energy by Carles Cufí; Akiba;Robert Davidson; Kevin Townsend Published by O'Reilly Media, Inc., 2014
- Bluetooth 5: a concrete step forward towards the IoT by Mario Collotta, Member, IEEE, Giovanni Pau, Member, IEEE, Timothy Talty, Senior Member, IEEE and Ozan K. Tonguz, Senior Member, IEEE, 2017
- Measuring Bluetooth Low Energy Power Consumption By Sandeep Kamath and Joakim Lindh
- BLE WEBSITES : http://microchipdeveloper.com/wireless:ble-introduction and http://www.summitdata.com/blog/whats-new-with-bluetooth-5-0/
- Bluetooth 5 Go Faster. Go Further. SIG pdf