CHAPTER 7

Physical Layer

7.1 Introduction

This chapter explains the operation of the physical layer of LE. As shown in Figure 7.1, this is the bottom most layer in the protocol stack. It is responsible for sending and receiving data over the air.

7.2 Frequency Bands

Like BR/EDR, the LE radio also operates in the 2.4 GHz ISM band (ISM stands for Industrial, Scientific and Medical). This frequency band is globally unlicensed and is used by several other devices like remote control toys, cordless telephones, NFC, Wireless LAN, etc. Some microwave ovens also generate interference in this frequency band.

Since this band may be shared by multiple devices, there is a good possibility that there may be interference from the other devices. So, the frequency is continuously changed for subsequent transmissions so that a new frequency is chosen for exchanging the data. The pattern of changing the frequencies is predefined so that the devices that need to exchange data know which frequency to hop to for the next data exchange. This is known as frequency hopping. LE uses frequency hopping technique to combat interference and fading.

The frequency band is divided into 40 channels which are spaced 2 MHz apart. (In contrast BR/EDR uses 79 channels which are spaced 1 MHz apart). The channels are numbered from 0 to 39 starting at 2402 MHz. The frequencies of various channels are derived from the formula:

$$f(k) = 2{,}402 + k * 2 \text{ MHz}, k = 0, \ldots, 39$$

The complete range used by LE is 2.400 to 2.4835 GHz. The frequency bands used by LE are shown in Figure 7.2.

Figure 7.3 shows the sniffer capture of transactions between a mobile phone and an LE device. It shows the transmissions on the 40 channels which include:

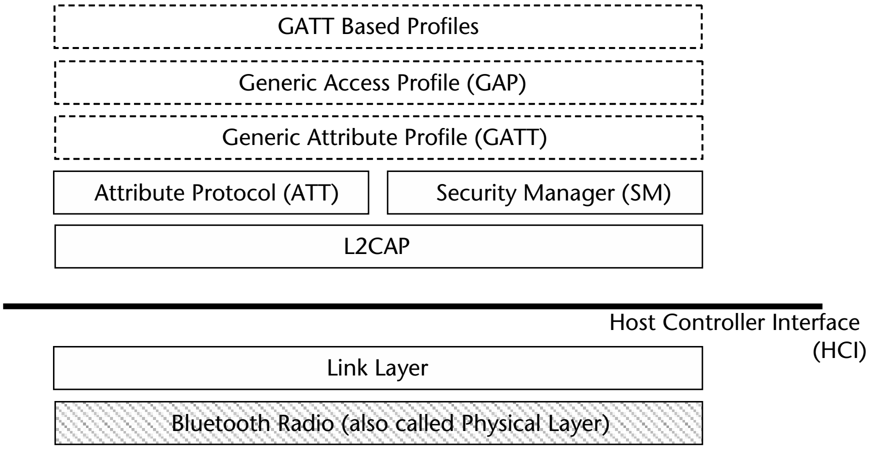

GATT Based Profiles
Generic Access Profile (GAP)
Generic Attribute Profile (GATT)
Attribute Protocol (ATT)
Security Manager (SM)
L2CAP
Host Controller Interface (HCI)
Link Layer
Bluetooth Radio (also called Physical Layer)

Figure 7.1 Bluetooth Radio in LE protocol stack.

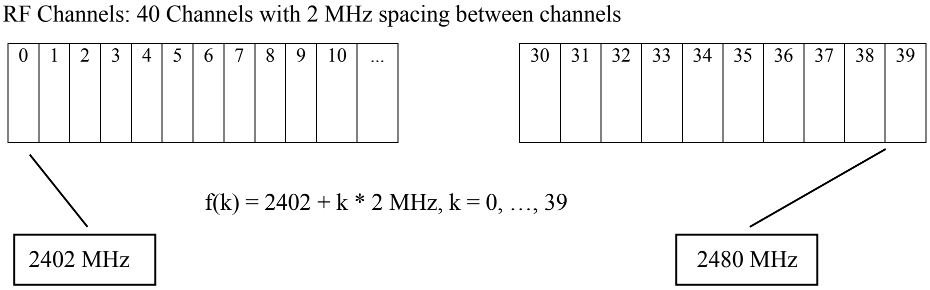

RF Channels: 40 Channels with 2 MHz spacing between channels
0
1
2
3
4
5
6
7
8
9
10
...
30
31
32
33
34
35
36
37
38
39
f(k) = 2402 + k * 2 MHz, k = 0, …, 39
2402 MHz
2480 MHz

Figure 7.2 RF channels used by LE.

1. Data transmissions on channel 0 to 36.
2. Advertisements on channels 37, 38, and 39.

As seen in the figure, the channels are spaced 2 MHz apart.

7.3 Transmitter Only, Receiver Only, or Both

An LE radio may have only a transmitter, only a receiver or both. This is in contrast to BR/EDR specification where it's mandatory for the BR/EDR radio to have both a transmitter and a receiver. This helps in reducing the cost and simplifying the design of devices which only need to transmit or receive data.

An example of this could be an LE based TV remote control. The remote control may need to only transmit the commands based on which buttons the user presses and not receive anything back from the TV. As per the LE specification, such a device is allowed to have only a transmitter.

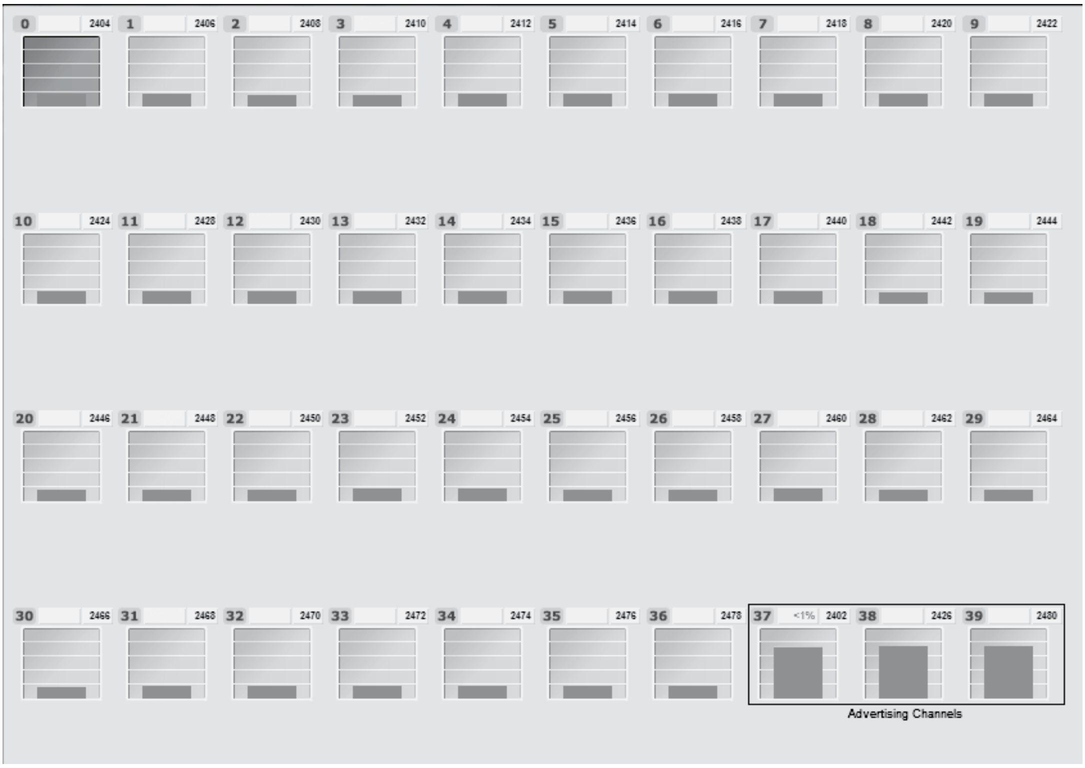


Figure 7.3 Sniffer capture of transmissions on LE channels.

7.4 Output Power

LE defines the transmitter output power to be in the range of 0.01 mW (–20 dBm) to 10 mW (+10 dBm). The device can change the output power dynamically to optimize the power consumption and reduce the interference on other equipment.

7.5 Range

Based on the output power defined in the previous section, LE devices support a range of about 30m to 100m.

7.6 Modulation Characteristics

LE uses Gaussian Frequency Shift Keying (GFSK) mechanism.

The bandwidth-bit period product BT=0.5 and the modulation index is between 0.45 to 0.55. A binary one is represented by a positive frequency deviation and a zero is represented by a negative frequency deviation.

The reference signal is defined in Table 7.1.

Some of these terms are beyond the scope of this book and are provided here just for reference. The details can be looked up in the Bluetooth specifications.

Table 7.1 Reference Signal for LE

Modulation	*GFSK (Gaussian Frequency Shift Keying)*
Modulation Index	0.5 +/– 1%
Bandwidth Bit period Product, BT	0.5 +/– 1%
Bit Rate	1 Mbps +/– 1 ppm
Modulation data for wanted signal	PRBS9
Modulation data for interference signal	PRBS15
Frequency accuracy better than	+/– 1 ppm

What is GFSK modulation?

Modulation is the process of mixing one signal with another signal. The signal that contains the information to be transmitted is called the *modulating signal*. It is mixed with a high-frequency signal called the *carrier signal*. Generally the frequency of the carrier signal is much higher than the modulating signals. For example the carrier signal would be in the range of GHz (2.4 GHz for Bluetooth) and the modulating signal would be in the range of MHz.

The three key properties of the carrier signal are: amplitude, phase, and frequency. Any of these can be modified during the process of mixing with the carrier signal. The resulting modulated signal is then transmitted to the remote side where it is demodulated to reconstruct the original signal.

For example, when a binary number (string of 0s and 1s) is to be transmitted over the air, it is mixed with a carrier signal, and then transmitted over the air. If the 0s and 1s were mixed to the amplitude then one level of amplitude would represent a 0 and another level of amplitude would represent a 1 after modulation. This modulated signal is now in a state that can be transmitted over the air. At the receiver side, the receiver would interpret the different amplitude levels as 0 and 1 and reconstruct the binary number.

Frequency Shift Keying (FSK) conveys information by varying the carrier signal frequency to represent a 0 or a 1. So a binary 1 can be represented by increasing the frequency of the carrier signal and 0 can be represented by decreasing the frequency of the carrier signal. One of the reasons for using frequency modulation to encode data compared to amplitude modulation is that generally the noise signals change the amplitude of a signal. So, modulation signals which ignore the amplitude of the signal are relatively more immune to noise.

Gaussian Frequency Shift Keying (GFSK) applies Gaussian filter to the modulating signal before it is mixed with the carrier signal. The Gaussian filter smoothens the shape of the frequency pulse so that high frequencies at the time of switching can be avoided. This helps to reduce the spectral width of the signal and is also called *pulse shaping*.

7.7 LE Timeline

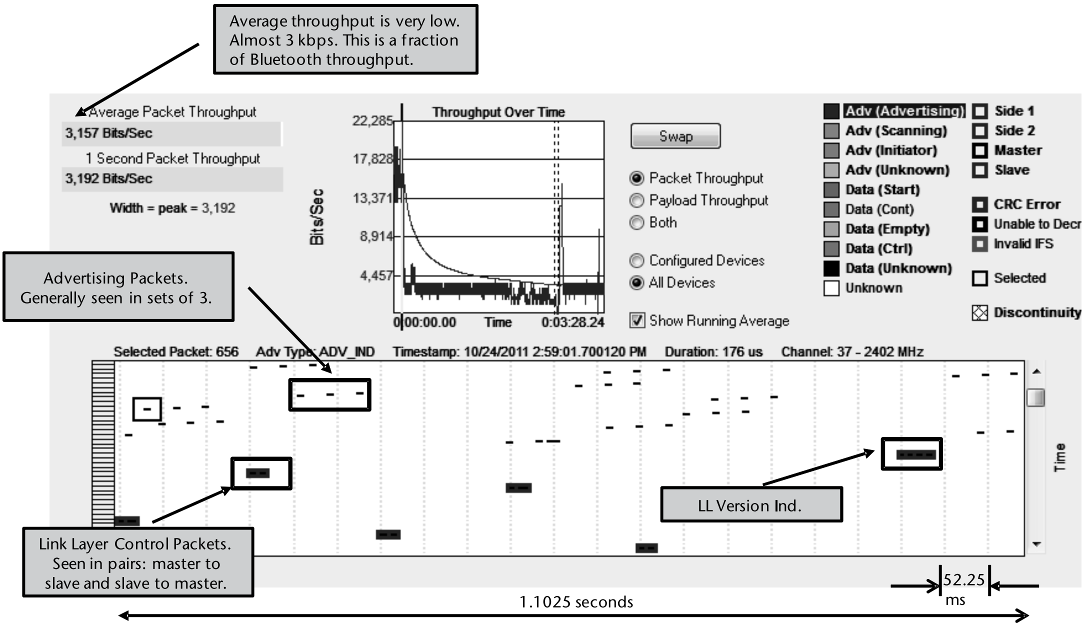
Figure 7.4 shows a typical timeline of transactions happening on the air for LE. The air captures have been taken for one of the GATT profiles where initially the LE device is advertising. Then later on a dual mode device tries to discover the services and creates a connection to this device.

Some of the interesting points to note are:

1. The advertising packets are generally seen in sets of 3 packets. This is because the devices generally advertise consecutively on the three advertisement channels and then wait for some time to restart the advertisement.
2. Most of the space is empty space. This means that for most of the time, there are no transmissions happening. This confirms the statement in the previous chapter that LE is a “mostly off” technology.
3. The average throughput is very low. For this particular capture, this is in the range of 3 kbps. This is much lower than the average throughput seen in classic Bluetooth systems.
4. There could be some instances where lot of data is exchanged. During that time the throughput may go up, but even then it is peaking to a maximum of 17 kbps in this particular example. This is still quite low.

7.8 Summary

This chapter explained the physical layer which is the bottom layer of the LE protocol stack and is responsible for sending and receiving data over the air. Like the BR/



Average throughput is very low. Almost 3 kbps. This is a fraction of Bluetooth throughput.

Average Packet Throughput: 3,157 Bits/Sec

1 Second Packet Throughput: 3,192 Bits/Sec

Width = peak = 3,192

● Packet Throughput
○ Payload Throughput
○ Both

○ Configured Devices
● All Devices

☑ Show Running Average

Selected Packet: 656 Adv Type: ADV_IND Timestamp: 10/24/2011 2:59:01.700120 PM Duration: 176 us Channel: 37 - 2402 MHz

Advertising Packets. Generally seen in sets of 3.

Link Layer Control Packets. Seen in pairs: master to slave and slave to master.

LL Version Ind.

Figure 7.4 LE timeline.

EDR radio, it operates in the 2.4 GHz ISM band though it uses only 40 channels as compared to 79 channels in the case of Bluetooth.

The next chapter will focus on the link layer which is responsible for controlling, negotiating, and establishing the links. The link layer uses the services of the physical layer to send and receive packets. It provides the packets to the physical layer for transmission on the sender side and processes the received packets from the physical layer on the receiver side.

Bibliography

Bluetooth Core Specification 4.0 http://www.bluetooth.org.