INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE OCCIDENTE

Reconocimiento de validez oficial de estudios de nivel superior según acuerdo secretarial 15018, publicado en el Diario Oficial de la Federación el 29 de noviembre de 1976.

Departamento de Electrónica, Sistemas e Informática

MAESTRÍA EN DISEÑO ELECTRÓNICO

Guidelines for Building Hybrid Applications Based on Bluetooth Low Energy and IEEE 802.15.4 Protocols

Trabajo recepcional que para obtener el grado de

MAESTRO EN DISEÑO ELECTRÓNICO

Presentan: JOSE MIGUEL REYES CHAIDEZ

Director: JORGE ARTURO PARDIÑAS MIR

San Pedro Tlaquepaque, Jalisco. December of 2016.

Acknowledgments

The completion of this work could not have been possible without the support of my family, my friends and colleagues. It might not be possible to add all the names of the people who always encourage me to continue with this work and don't give up, however, I would like to express my deep sense of gratitude to:

Dr. Jorge Pardiñas for his great support through all the planning and development of this document. Without his excellent guidance and great mentoring, this work would not be possible. Thank you very much Jorge!

NXP Semiconductor staff, thanks to the connectivity team to support me whenever I needed to complete this work. Special thanks to JC Pacheco, Santiago Lopez, Ale Guzman and Carlos Neri for supporting me whenever I disturb them to talk about the topics I planned to talk in this document. I owe you some beers.

My family, I would like to thank my mother and my uncle/father for the support they have gave me all my life with my education, they always encourage me to continue and fight for my dreams and goals. Thanks for teach me that every success requires sacrifices, that you can get what you want, being optimistic and never give up.

Summary

The study case born due to the lack of information provided in the wireless multiprotocol device KW40Z about the recommendation and overview of application involving two wireless protocols: Bluetooth Low Energy and IEEE 802.15.4. This kind of Applications are known as hybrid Applications in this document. This document pertains to provide basic guidelines or recommendations that help wireless applications developers with the design of hybrid applications using Bluetooth Low Energy and non-beacon IEEE 802.15.4 networks. It is divided into five chapters. The introduction begins with the presentation of the case study as well as the issue that is going to be analyzed in this document. Chapter 1 provides an introduction of the Bluetooth Low Energy technology and the basic concepts to understand how it can affect hybrid applications. Chapter 2 gives a short overview of the IEEE 802.15.4 technology with the focus on non-beacon networks. Chapter 3 introduces different schemes of the coexistence of IEEE 802.15.4 and BLE in the 2.4 GHz band. Chapter 4 introduces the hybrid applications and analysis of this kind of applications taking the KW40Z device as an introductory example to analyze hybrid applications. Finally, the document concludes in Chapter 5 with some key recommendations that serves as basic guidelines when designing hybrid applications residing in a multiprotocol device such as the KW40Z from NXP Semiconductors.

Content

Introduction

During the last years, wireless networks has been gaining more attention year over year. As a consequence, different wireless protocols has been introduced to provide ease of use to common activities like turning on/off lights inside of a house as well as monitoring different devices. Although there are different protocols developed for this purpose, there are some protocols that have more popularity, for example, IEEE 802.15.4 and Bluetooth Smart/Bluetooth Low Energy (BLE). IEEE 802.15.4 is widely used on wireless sensor networks while BLE is present in most of the smartphone devices as well as fitness sensors.

Due to the popularity of IEEE 802.15.4 and Bluetooth Low Energy technologies, NXP Semiconductors introduced its KW40 device to the market, a multi-protocol device being able to work in IEEE 802.15.4/BLE networks. KW40 transceiver is a 2.4GHz radio which can operate in IEEE 802.15.4 and BLE applications at the same time. For example, a KW40 device can be configured to be a Heart Rate Sensor in a BLE communication while participating as an IEEE 802.15.4 coordinator inside of an IEEE 802.15.4 network, we can reference to this KW40 applications as a multi-protocol, multi-mode or hybrid applications. Fig. I-1 illustrates an example of a hybrid application using the KW40Z device. The KW40Z device is connected to a smartphone using BLE protocol while it is also sending or receiving packets in an IEEE 802.15.4 network.

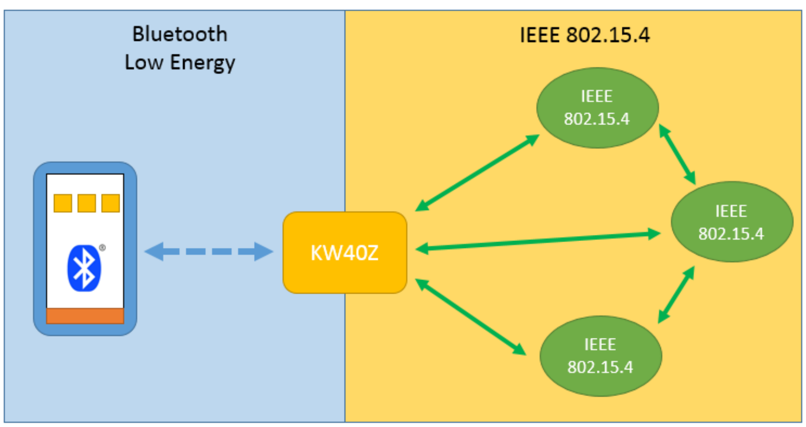

Fig. I-1 KW40Z hybrid application example

It is necessary to have in mind that when talking about a chip introduction, semiconductor companies used to offer all the collaterals needed to create an application using the chip. Hence, when NXP Semiconductor introduced KW40Z device, it designed development boards as well as the software needed to run KW40Z applications. Development boards are FRDM-KW40Z and USB-KW40Z while the software is known as the KW40Z Connectivity Software. This case study will only make use of the FRDM-KW40Z board.

The purpose of the case study is to be able to provide recommendations about multi-protocol or hybrid applications which make use of BLE and IEEE 802.15.4 protocols. This case study will be based on the existing hybrid application on KW40 device which is part of the KW40Z Connectivity Software. It will provide information about how the BLE and IEEE 802.15.4 works and some details about the coexistence of these two protocols working in the 2.4 GHz spectrum. In addition to this, it is the result of the lack of information on the existing documentation which does not provide enough information about how to create and design multi-protocol applications. The main goal is to use the case study as a guideline for customer interested in developing such multiprotocol or hybrid applications. The content of the chapters is summarized in the following paragraphs.

Chapter 1. **Understanding Bluetooth Low Energy Technology.** This chapter will talk about the basics concepts of the BLE technology to understand what roles exist in a BLE connection, what are the parameters that can be configured as well as providing an example of BLE Heart Rate Sensor demo.

Chapter 2. **Understanding IEEE 802.15.4.** It will expose different concepts used on IEEE 802.15.4 technology, explain role types in a non-beacon IEEE 802.14.5 network, the format of the message as well as the parameters that can be configured during a connection. It will also describe the basic communication in a non-beacon network and no security between a coordinator and an end device. This kind of applications are going to be used as part of this case study, which is called "MyWirelessApp Coordinator" and "MyWirelessApp End Device".

Chapter 3. **Coexistence of the IEEE 802.15.4 and Bluetooth Low Energy networks**. This chapter will provide information about the coexistence of these two technologies based on some technical papers already available on the web. It will be of use to explain from the technology point of view that both technologies can work in the same environment and physical space.

Chapter 4. **IEEE 802.15.4/Bluetooth Low Energy Hybrid Applications**. It will provide information about the management of BLE and IEEE 802.15.4 wireless protocols when working together in the same chip as well as explaining one use case which can be of use for future projects. It will also introduce the current KW40Z hybrid application. This application will be analyzed in this chapter in terms of the memory footprints, architecture and information collected through experiments performed when using this application.

Chapter 5. **Conclusions**. This chapter will provide recommendations and possible improvements for the hybrid applications as well as a guideline for developers who are interested on building this type of hybrid applications using BLE/IEEE 802.15.4 protocols.

1. Understanding Bluetooth Low Energy

The purpose of this chapter is to provide a description of the key concepts for the Bluetooth Low Energy (BLE) technology. At the end of this chapter, the reader should be able to understand the roles and the procedure required to have a Bluetooth low energy communication between two BLE devices.

1.1. Background

Bluetooth technology emerged due to the need of having a replacement for cables for data transfer, the concept was to have a point to point communication to send big amount of data. The technology was based on the IEEE 802.15.1 standard, however, after some revisions, the standard was adopted by a Bluetooth Special Interest Group (SIG) which is different from the IEEE. The Bluetooth SIG has been maintaining and updating the protocol by adding features to improve speed as well as security. It was until 2010 when there was a need to have a light protocol under the Bluetooth scheme that would be able to transmit short amount of data with less power consumption as possible, hence, the Bluetooth Low Energy/Bluetooth Smart/Bluetooth Single Mode concept was introduced by the SIG.

Bluetooth Classic is not part of this chapter, however, if the audience has some knowledge of the Bluetooth Classic protocol, it will be noticed that there are a lot of similarities between Bluetooth Classic architecture and the BLE architecture.

A BLE architecture is composed by three main blocks: The controller, the host and the application as shown in Fig. 1-1. The controller is what we used to call the radio part or BLE transceiver of the architecture, then, the host is built purely by software and it is linked with the controller through a host controller interface (HCI) which can be self-descriptive. HCI is the layer that passes messages and events between the controller and the host. Finally, there is the application on top of the host. Across this document, a basic overview would be provided where each layer will be summarized. The details of the protocol can be found in [1]. A good reference for better understanding is [2] and [3].

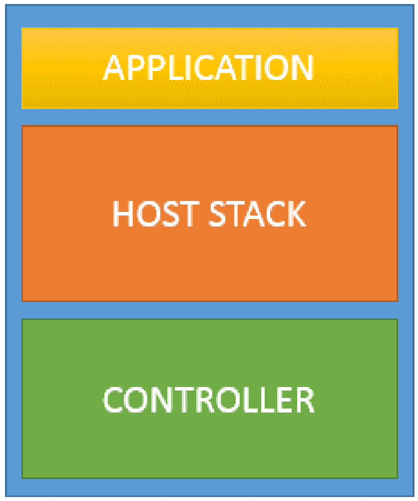

Fig. 1-1 BLE architecture.

1.2. General BLE Example

As an introductory example, the process to exchange data between two BLE devices requires a master and a slave. Hence, thinking in a real application, we are going to make reference to a Heart Rate Sensor (HRS) which will make a connection with a smartphone device. A HRS example was chosen mainly because is the type of application that will be studied in this document. In this scenario, the smartphone is a master or client or central device while the HRS is a slave or sever or peripheral device. The name of the role changes through the BLE layers, this will be explained later in this chapter. However, the HRS starts sending packets known as advertising packets in the three advertising channels in which the smartphone is continuously scanning to look for slave devices to make a connection. Once the smartphone scans and finds the proper HRS, it sends a connection request to perform a connection, hence, at this point devices are considered to have a connection and start communication in the data channels (we have 37 data channels). Then, in order to exchange application data such as a heart rate measurement, the smartphone starts a procedure called service discovery which is used to discover the data available in the heart rate sensor. Once the service discovery is done, the smartphone starts requesting or receiving data from the HRS. Finally, the connection could be terminated by the smartphone or the heart rate sensor at any time.

A more detailed representation of the BLE architecture can be seen in the Fig. 1-2 which shows all the layers of the BLE architecture. These layers will be discussed in the following sections which are required to understand BLE technology but also to know more about the topics that will be used in the current case study where the connection parameters play a key role.

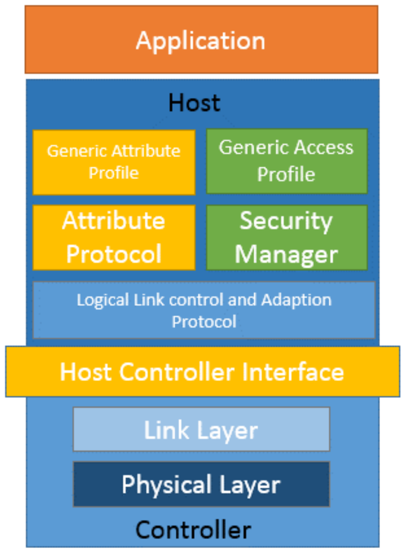

Fig. 1-2 BLE layers.

1.3. Physical Layer

The physical layer specifies the frequency spectrum space in which the technology works and how the channels are characterized in conjunction with all the RF parameters required by a radio working on BLE.

BLE operates in the 2.4GHz spectrum using a Gaussian Frequency Shift Keying, modulation index of 0.5, channel spacing of 2MHz and with 1Mbps of data rate. There are 40 channels defined by BLE technology. Channels are classified in two kind of channels: advertising channels and data channels. The advertising channels are the ones in which devices can perform a connection, this means that it is where two BLE devices make a connection. Once the connection is done, the communication between the connected devices are done through the data channels.

There are 3 advertising channels and 37 data channels. Moreover, it is worth to mention that BLE works by frequency hopping mechanism, so, radio is always jumping between channels.

In order to coexist with WiFi technology, the advertising channels are placed in gaps of the 2.4GHz WiFi channels. This makes that BLE devices could be visible when working in a crowd WiFi environment. Fig. 1-3 shows the distribution of the BLE and WiFi channels in the 2.4GHz frequency spectrum.

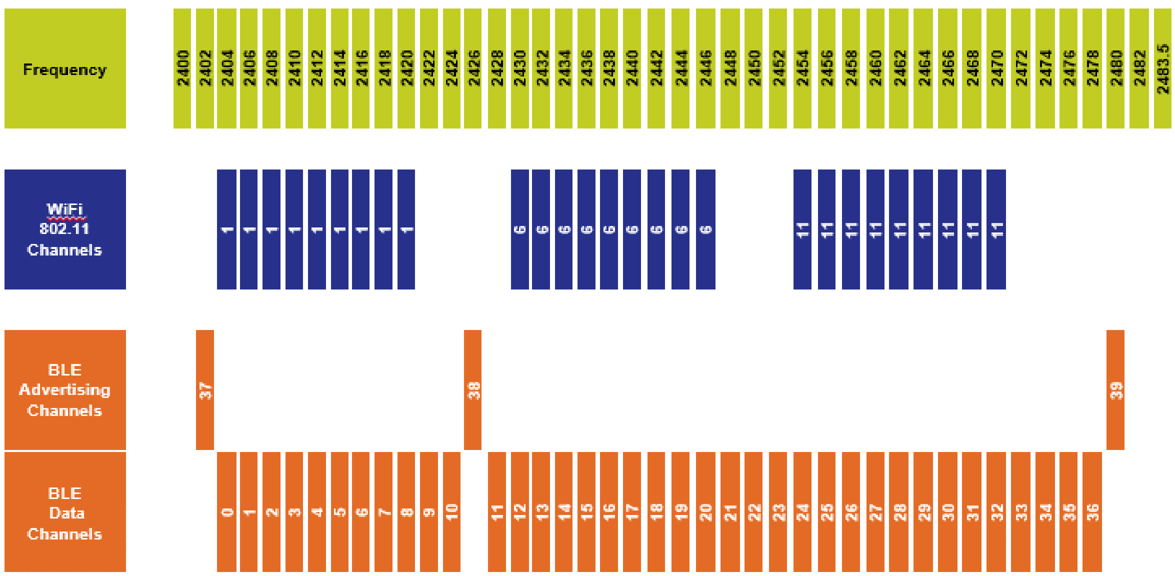

Fig. 1-3 BLE channels distribution.

1.4. Link Layer

The link layer is responsible to define the key parameters for a BLE connection as well as determine how each device can see each other. A simple state machine can be found inside of the Link Layer which is defined as shown in Fig. *1-4*. A short description of each state will be described in this section.

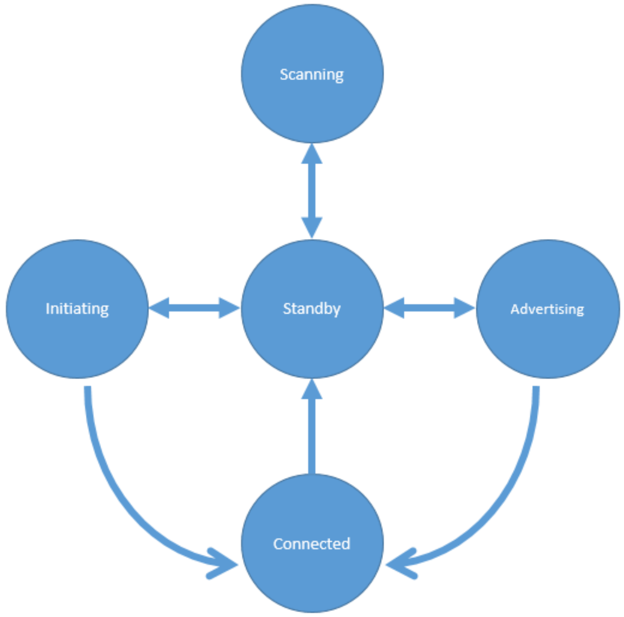

Fig. 1-4 Link layer state machine.

Standby: It is when the radio is in idle mode. It is not transmitting or receiving.

Advertising: It is when device is sending packets in the three advertising channels (37, 38 and 39), so, scanning devices can listen those packets. It is important to understand that advertising packets is like the presentation card of a BLE device since it contains data to identify such device. It is called advertising event when a packet has been sent in each advertising channel. In other words, advertising events are the set of packets sent in each of the advertising channels. A new advertising event will take place after an advertising interval has been reached. The advertising interval shall be an integer multiple of 0.625 milliseconds in the range of 20 milliseconds to 10.24 seconds. Fig. 1-5 illustrates the advertising events and advertising interval. It is important to mention that advertising interval is configured in the link layer, however, an upper layer sets the configuration of the link layer by defining the advertising parameters.

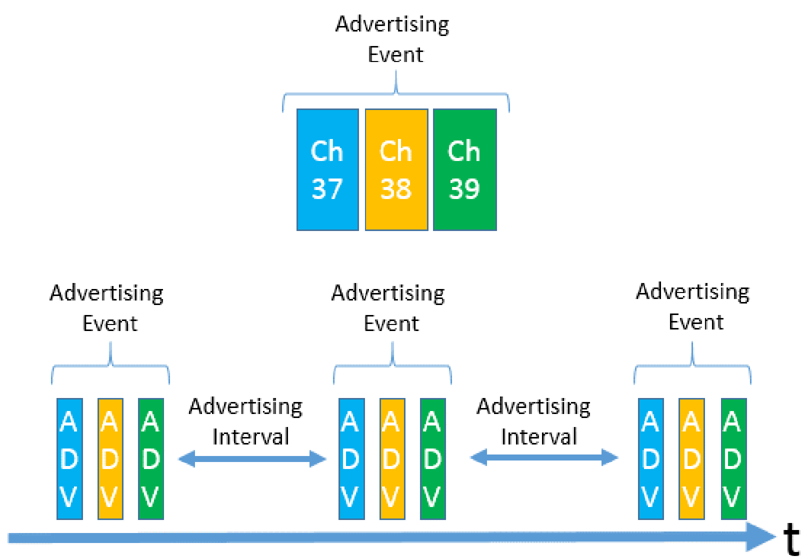

Fig. 1-5 Advertising events and advertising intervals.

Scanning: It is the state in which a device is listening in the advertising channels in order to collect data from an advertiser, if the scanner requires more data, it can send a scan request to ask for more data if available in the advertiser. Advertiser will reply in a scan response, all this procedure runs in the advertising channels. In order to be able to get the advertising packets, the scanning procedure defines a scan interval and a scan window. The scan interval is the time between two scan events, then, the scan windows is how long the scan event will stay in one particular channel. A scan event is performed in one advertising channel to be able to listen one of the packets of the advertising event. The scan interval shall be an integer multiple of 0.625 milliseconds in the range of 2.5 milliseconds to 10.24 seconds. In the same way, the scan window shall be less or equal than the scan interval. Fig. 1-6 illustrates the scan window and the scan interval.

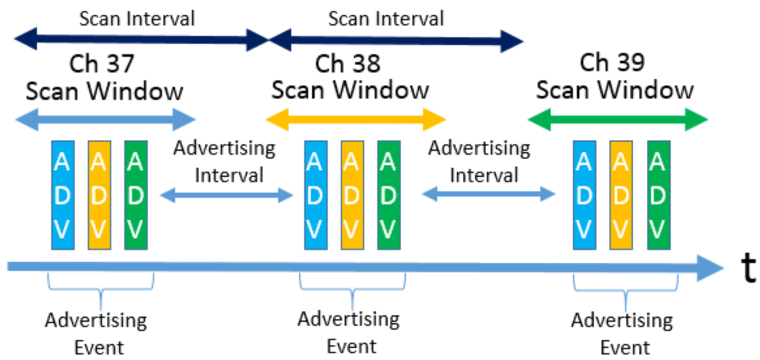

Fig. 1-6 Scan interval and scan window.

Initiating: The initiating state is when a device wants to make a connection with a peer device, hence, once the initiator finds the desired device to make a connection, it sends a connection request in order to enter in the connection state.

Connection: The connection state is entered when the advertiser and the initiator make a connection. In order to enter to the connection state, the initiator shall send a connection request to the desired advertiser.

The link layer introduces two roles: the master and the slave. Master devices are the ones that perform scanning and the only ones to request a connection to a peer device by sending a connection request. On the other hand, slave devices are the ones that perform advertising, which basically means to send packets on the three advertising channels defined by the specification. The advertising packets are the packets in which the devices announce they are there to exchange data or to make a connection. Advertising packets can be seen as broadcast packets since all master devices can listen or scan such packets.

Other important feature defined by the Link Layer is the packet format. There is only one packet format defined in BLE Link Layer, the packet format is shown in Fig. 1-7.

Preamble (1 byte)	Access Address (4 bytes)	Protocol Data Unit (PDU) (2 to 39 bytes)	CRC (3 bytes)

Fig. 1-7 Link layer packet format.

Finally, although the Link Layer defines only one packet format, we can define two different Protocol Data Units (PDU) in BLE, the advertising PDU and the data PDU. Hence, advertising PDU is used when devices are in the advertising and scanning state while the data PDU is used when devices are in the connection state.

1.5. Host Controller Interface (HCI)

The HCI is a layer that serves as interface between the controller and the host. There can be two kind of solutions, one using two integrated circuits, the radio and the microcontroller (MCU) where the host and the application is written and the second solution which include the radio and the MCU in the same die. In both solutions, the HCI acts as the interface between the radio and the MCU, such interface could be UART, USB, among others.

1.6. Logical Link Control Adaption Protocol (L2CAP)

It is known as a multiplexer to the upper layers, it defines internal channels to determine to which upper layer a message would be sent. It is important to notice that this layer is built by software, so, talking about channels, this means a logical channels inside the host and not physical channels. For example, there is a channel defined for the Attribute Protocol layer and one for the Security Manager Layer.

1.7. Security Manager(SM)

The Security Manager is in charge of the security procedures that are defined by the BLE specification. It defines the methods and the different keys that are used to encrypt a connection.

1.8. Attribute Protocol (ATT)

The Attribute Protocol (ATT) is the protocol that BLE uses to communicate between two devices. This layer introduces two roles, client and server, then, it also defines the way in which the two types of roles can communicate between them. Basically, it defines the basic types of messages exchanged between the client and the server, hence, there are client initiated messages and server initiated messages.

There are two client initiated messages: the requests and the commands. Both are sent by the client, however, all requests require a response to be able to send a new request. On the other hand, commands do not demand a response from the server. Client initiated messages are shown in Fig. 1-8.

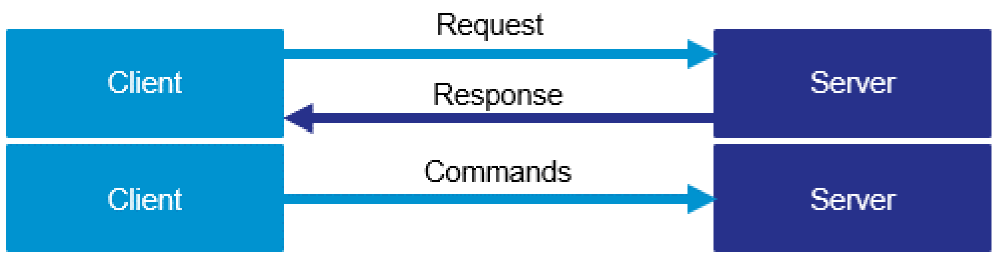

Fig. 1-8 Client initiated messages.

Similar to the client initiated messages, there are server initiated messages: indication and notifications. The indications similar to the request, requires a response from the client, nevertheless, this response is called confirmation. Then, the notifications do not require confirmation from the client. Server initiated messages are shown in Fig. 1-9.

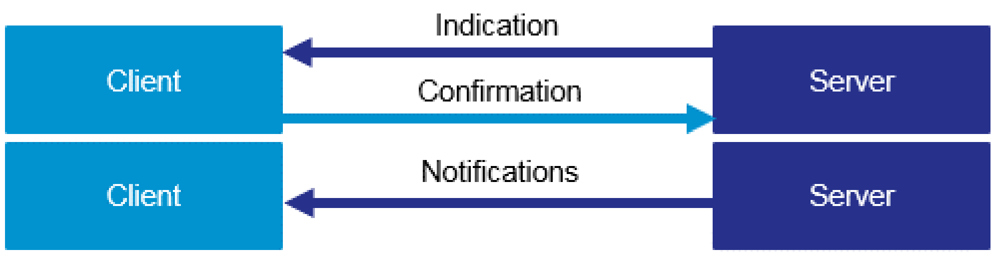

Fig. 1-9 Server initiated messages.

1.9. Generic Attribute Profile (GATT)

This layer follows the roles introduced by the attribute protocol. The GATT defines the database of a server which basically means a collection of data which has a meaning, in other words, this profile is the one that provide a description to the stored data in the server. As defined by the SIG:

"Generic Attribute Profile (GATT) is built on top of the Attribute Protocol (ATT) and establishes common operations and a framework for the data transported and stored by the Attribute Protocol. GATT defines two roles: Server and Client. The GATT roles are not necessarily tied to specific GAP roles and may be specified by higher layer profiles. GATT and ATT are not transport specific and can be used in both BR/EDR and LE. However, GATT and ATT are mandatory to implement in LE since it is used for discovering services."

In the same way, GATT profile defines a hierarchy which is composed by services, characteristics and descriptors. Hence, the GATT based profiles are the ones that provides meaning to BLE devices since most of the BLE profiles are GATT based profiles such as Heart Rate Profile, Glucose Profile, Human Interface Device Profile, among others. All the adopted profiles are public in the SIG web page.

Following the heart rate sensor example cited at the beginning of this chapter, there is the Heart Rate Profile which defines the rules or the specification for a Heart Rate application, hence, it defines a Heart Rate Collector and a Heart Rate Sensor. The Heart Rate Collector does not require a GATT database and plays the client role according to the Heart Rate Profile, i.e. a smartphone device. On the other hand, the Heart Rate Sensor plays the server role and it is composed by different services such the Heart Rate Service and Device Information Service. These services are defined by Heart Rate Profile that is already adopted and they are known as a primary services. However, depending on the implementation of the device, developers might require additional adopted services for other functionalities in their product such as the battery service which might be used in all battery powered devices. There could be also custom profiles developed for custom applications, nevertheless, if a specific application gain popularity, it could be proposed for adoption to the Bluetooth SIG. The process of usual BLE communication between server and client is shown in Fig. 1-10.

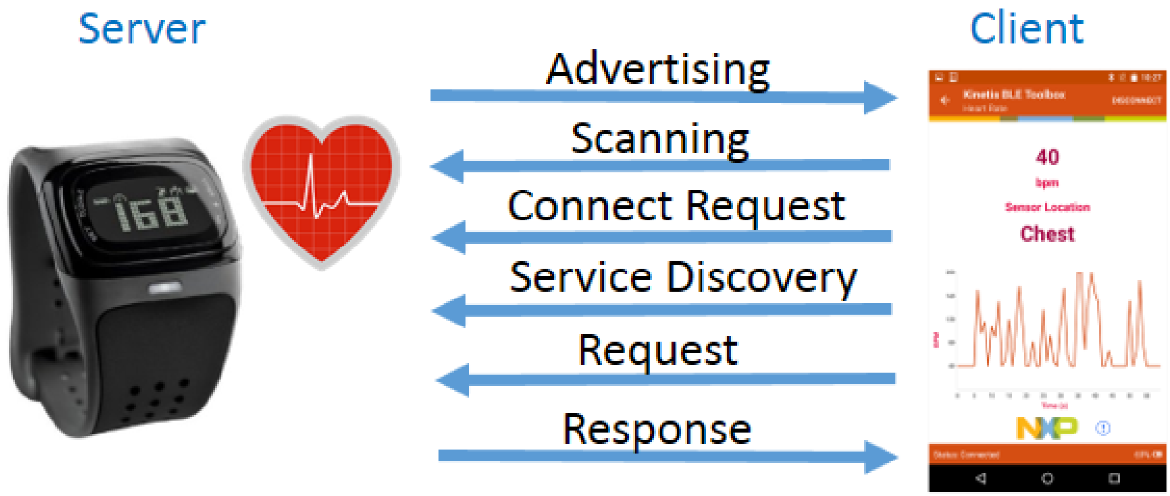

Fig. 1-10 BLE heart rate sensor application flow.

1.10. Generic Access Profile (GAP)

It defines the rules of the connection, the timing to make advertising, scanning parameters, security level and defines if the device can make a connection. Although the Link Layer is the responsible to monitor connection parameters. It is responsibility of the GAP layer to define and set such parameters when sending a connection request. In addition to this, GAP layer also introduce new roles in the BLE communication, these roles are the next:

1. **Central**. The central devices usually are the master devices which are willing to seek peer or peripheral devices to establish a connection.
2. **Peripheral**. This type of devices are slave devices looking for peer or central devices to establish a connection.
3. **Broadcaster**. It only sends advertising packets and it is not willing to perform a connection for peer devices.
4. **Observer**. It only stays listening in the advertising channel, it can be known as a scanner device which only listen in the channels and it is not willing to perform a connection with peer device.

At this point, it might be confusing the roles of the devices across different layers. Nevertheless, the heart rate example can be used to demonstrate common BLE application where the sensor is the peripheral since it is the device that performs advertising while the smartphone is the central device.

Different from the GAP roles, the GAP defines the rules of the connection that are sent in the connection request command, some main parameters that need to be defined when sending this command are:

Connection Interval: how often devices are going to exchange two valid packets during a connection (this is also known as a connection event). It plays a critical role since this is the timing in which the radio could be in sleep or idle mode.

Connection Event: Once the connection interval is reached, it means a connection event has been produced. Basically, the connection event is the event in which the master and the slave device exchange data.

Connection Slave Latency: how many connection events the slave can ignore without affecting the connection.

Supervision Timeout: it is the maximum time that a Link Layer can wait for a valid packet from the peer device before considering the connection lost.

The Fig. 1-11 illustrates some of the parameters discussed above. It shows how the frequency hopping works in BLE. In Fig. 1-11, the hopping pattern is set to 9 and it is assumed the first connection event will take place in channel 9, then, the next connection event will take place in channel 18, then, channel 27 and so on. The time between two connection events is called connection interval and it shall be an integer multiple of 1.25 milliseconds in the range of 7.5 milliseconds to 4 seconds.

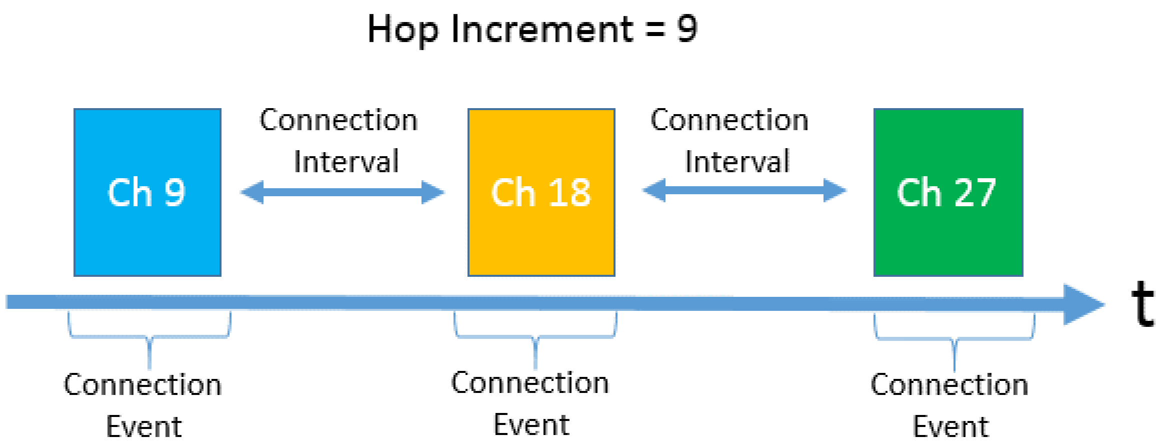

Fig. 1-11 Main connection parameters.

1.11. BLE Packet Format

As discussed in the previous sections, there are two different type of packets. The advertising packets and the data packets. At the end, when two devices are in a connection state, they transfer data using the data format packet. Fig. 1-12 shows the format of the data packets, it can be seen that maximum application data that can be obtained per packet transfer is 20 byte of length.

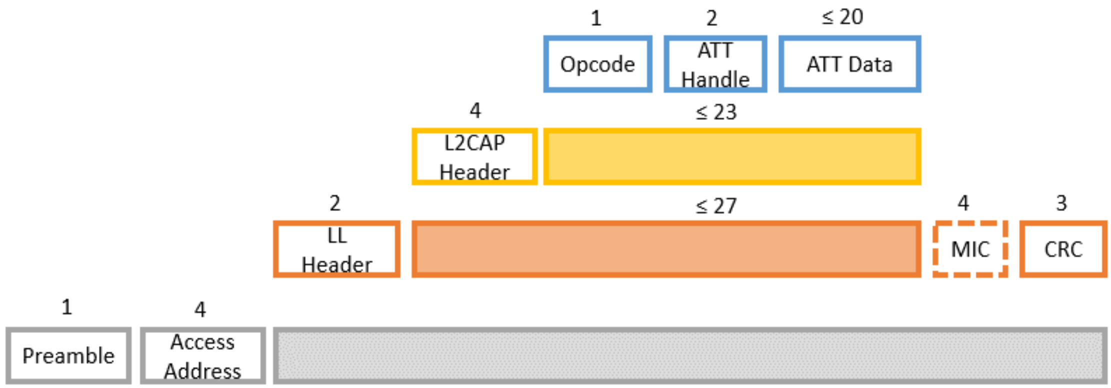

Fig. 1-12 BLE data packet format.

2. Understanding IEEE 802.15.4

The purpose of this chapter is to provide a description of the key concepts for the IEEE 802.15.4 technology. At the end of this chapter, the reader should be able to understand the roles and the procedure required to have a communication between IEEE 802.15.4 based devices.

2.1. Background

The IEEE 802.15.4 is a low power wireless standard maintained by the Institute of Electrical and Electronics Engineer (IEEE) introduced in the early 2003 due to the lack of a standard protocol in the wireless world for low rate, low duty cycle, cost effective and low power technology. Different from other IEEE 802 standards, the IEEE 802.15.4 mission is to create a technology that is able to operate for years in devices powered by commercial primary batteries. This would allow developers interested in radio technology to create sensor networks under a specific protocol that would allow interoperability between many devices using the same standard. Hence, the wireless sensor networks were the central topic of this standard.

The standard follows the Open Systems Interconnections (OSI) Model as most of the others communication protocol. This standard focused in the first two layers of the OSI model, such layers are the Physical layer (PHY) and the Data Link or Medium Access Control (MAC) layer. The rest of the OSI layers are defined by different IEEE 802.15.4 based wireless protocols like ZigBee, Wireless HART, Thread, among others.

Fig. 2-1 shows the OSI Model architecture. This model is not covered in this document; nevertheless, it helps to have a better idea about how the protocol can be expanded adding more layers and complexity to the protocol, one example is the ZigBee protocol, a based IEEE 802.15.4 wireless protocol which is in charge of defining the layers on top of IEEE 802.15.4 to allow interoperability among all ZigBee devices.

2. UNDERSTANDING IEEE 802.15.4

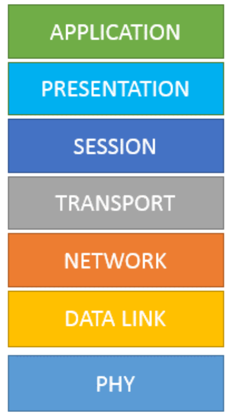

Fig. 2-1 OSI model layers.

Fig. 2-2 shows the IEEE 802.15.4 architecture. As mentioned before, the IEEE 802.15.4 standard only covers the PHY and the IEEE 802.15.4 MAC sublayer. On top of the MAC layer, there could be the final application or more robust protocols that use MAC standard as a baseline.

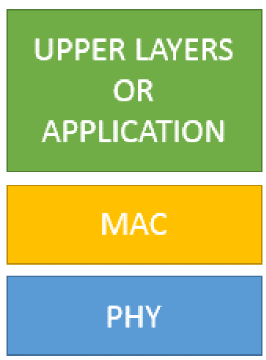

Fig. 2-2 MAC device architecture.

The standard defines frequency operation in the Sub-GHz as well as the 2.4GHz. However, this document is focusing in the 2.4GHz because it is the band where most of the IEEE 802.15.4 applications or devices work and it is the supported band by the KW40Z device, the one to be studied in this work. The standard specifies the use of Direct Sequence Spread Spectrum (DSSS) modulation, which is highly tolerant to the noise and the interference. In addition to this, it uses carrier sense multiple access with collisions avoidance (CSMA-CA) to have access to the channel when transmitting packets.

There are two types of devices defined in the IEEE 802.15.4, a reduced functional device (RFD) and a full functional device (FFD). The RFD usually is a simple device with reduced resources and memory size because it only associates to a coordinator and it does not have a need to send big amount of data continuously, typical application for a RFD device can be a temperature sensor or a switch light. On the other hand, the FFD has more features and capabilities since it is able to act as a coordinator. The coordinator is responsible to create the network and to give access to other devices to join the network. This chapter is going to provide general description of the IEEE 802.15.4 protocol. Nevertheless, the details of the protocol can be found in [4]. A good reference for better understanding is [5] and [6].

2.2. General IEEE 802.15.4 Example

A simple IEEE 802.15.4 application requires at least two devices, a coordinator that will create the network and the end device that will join the network. The coordinator would be a FFD while the end device would be a RFD. In order to create a network, the coordinator has two options, one is to create the network in a pre-configured channel and the second is to start a scanning process in order to identify the IEEE 802.15.4 channel that shows less energy. The network is created using a PAN ID to identify the network as well as a short address to identify the coordinator. Once the coordinator creates the network, it stays in reception mode.

On the other hand, the RFD sends beacon requests in all IEEE 802.15.4 channels to find a network, if a beacon response is received, it means that a network is active in a particular channel. The beacon response includes information about the network such as the association permit bit, if association permit bit is set, this means that end device is able to send the association request to the PAN coordinator to join the network. An association response is sent to the end device with a short address to identify the end device. The association means that both devices are in the same network and they can start to exchange data. The way devices exchange data depends on the type of the network, there are two types of networks: beacon or non-beacon. Data transfer in a non-beacon network is performed at any time while in a beacon network the data transfer is synchronized using beacons sent by the coordinator. This study case is focused on an IEEE 802.15.4 application using non-beacon network. Following sections provide a brief description of the IEEE 802.15.4 architecture as well as of a basic application that will be studied in this document. The application requires a coordinator and an end device in a non-beacon network; both devices transmit any data received through its serial port. Fig. 2-3 illustrates all the flow chart between an end device and a coordinator to exchange data. This process is described in detail in the next sections.

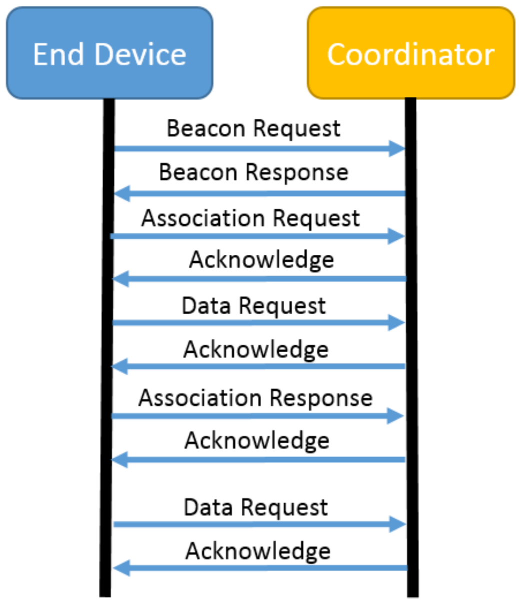

Fig. 2-3 Flow chart of IEEE 802.15.4 communication between end device and coordinator.

2.3. Physical Layer (PHY)

The physical layer is responsible to interface with the transceiver and to define the parameters of the physical medium like the bandwidth of the channel, the supported channels per frequency band and the interface to operate with the upper layer. Some of the functions of the physical layer includes the activation and deactivation of the radio transceiver, Energy Detection (ED), Link Quality Indicator (LQI), channel selection, clear channel assessment (CCA), and transmitting as well as receiving packets across the physical medium. Table I shows the IEEE 802.15.4 supported channels depending on the frequency band and the region.

TABLE I
IEEE 802.15.4 SUPPORTED FREQUENCY BANDS

Regions	Europe	Americas	World
Frequency	868 MHz	902 to 928 MHz	2.4 GHz
Number of channels	1	10	16
Data rate	20kbps	40kbps	250kbps
Modulation	BPSK	BPSK	QPSK

As mentioned before, the focus of the document is in the 2.4 GHz band. The IEEE 802.15.4 defines 16 channels in this band starting at the frequency 2.405 GHz. Then, each subsequent channel is located with an offset of 5 MHz, which mean that channel 12 would be on 2.410 GHz, channel 13 on 2.415 GHz and so on. The defined range of the IEEE 802.15.4 is from channel 11 to channel 26.

Furthermore, the PHY provides the interface between the MAC sublayer and the physical radio channel. It provides two services: the PHY data service and the PHY management service. The PHY data service enables the transmission and reception of PHY protocol data units (PPDUs) across the physical radio channel. The PHY management service offers the interface for upper layers from which the management functions are called, in addition to this, it is responsible to maintain the database of the PHY known as PHY PAN Information Base (PIB). We used to see these references in the architecture as PD-SAP (PHY data service access point) and PLME-SAP (PHY layer management entity service access point). Fig. 2-4 shows a basic MAC architecture and how the PHY interfaces with the upper layers.

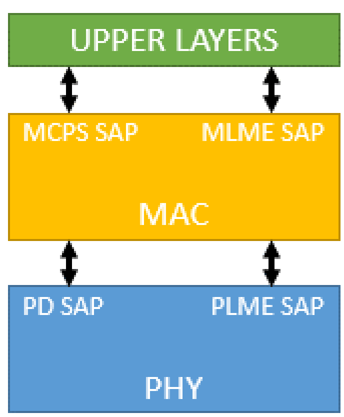

Fig. 2-4 Basic MAC Architecture.

2.4. IEEE 802.15.4 MAC Sub-Layer

This section provides a summary of the key services of the IEEE 802.15.4 sub-layer or MAC sub-sublayer. The MAC sublayer interfaces with the PHY layer and it is responsible to define the types of devices as well as the protocol to allow communication between two devices. Hence, the MAC sublayer manages the beacons, the association, channel access and the data exchange. The MAC sublayer provides the services to allow interface with upper layers or the application, similar to the PHY, the MAC sub-layer defines two services: the MAC data service and the MAC management service. Similar to the PHY, MAC data service is known as MCPS-SAP (MAC common part sublayer service access point) and the MAC management service as a MLME-SAP (MAC sublayer management entity service access point). The following sections will describe the key services of the IEEE 802.15.4 MAC sub-layer.

2.4.1 Type of Devices and Network Topologies

As said before, there are two types of devices defined by the standard, Full Functional Device (FFD) and Reduced Functional Device (RFD). FFD can be a coordinator or an end device. On the other hand, RFD devices can only take the end device role. The protocol defines two network topologies:

1. **Star Topology**. One FFD defined as a coordinator connected to different RFDs or end devices.
2. **Peer to Peer**. It is also called point to point network, it is when two devices talks directly to each other.

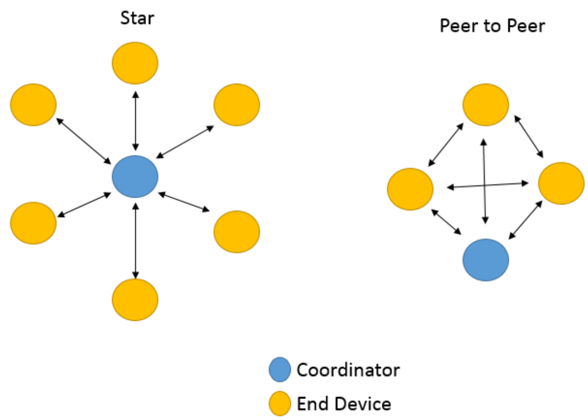

Fig. 2-5 IEEE 802.15.4 Network Topologies.

Although there are two types of network topologies as shown in Fig. 2-5, the standard does not define a network layer that provides rules and algorithms to route packets inside the network. Usually, higher-level MAC based protocols are in charge of the network layer definition.

Coordinator devices are responsible to create the IEEE 802.15.4 network as well as allow access to remote devices. After the network is created, the coordinator can manage the network by implementing beaconed networks or non-beaconed networks. In a beaconed network, the coordinator sends beacon frames to synchronize the network; the interval between two beacons receives the name of superframe. Different from this, nonbeacon networks does not send periodic beacons to avoid traffic overhead in the network. Nonbeacon uses beacon frames to be able to identify an existing network in a physical channel. This way, when end devices find a specific network they want to join, they start the association procedure.

2.4.2 Channel Access

Channel access defines the way that MAC protocol performs operation with peer devices such as packet transfers. MAC uses the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) mechanism to perform any message exchange between two devices. The mechanism ensure that the physical channel is clean to be able to send the packet, if the channel is busy, devices waits for a random back-off period to sense the channel again until the packet is sent. However, there is limitation in which a device can scan the channel, this means that a number of back-off (NB) is defined to determine how many times the device can sense the channel, if the device finds the channel busy NB times, the packet transmission is failed.

2.4.3 Association Procedure

The process to create a link between two devices in IEEE 802.15.4 network is the association. In order to perform an association between two devices, it is required that both devices exist in the same network. Talking about a nonbeacon network, once a coordinator creates a network in a certain channel, the end device can scan the channel by sending beacon requests. The coordinator sends a beacon response whenever there is the reception of a beacon request. The beacon response plays a key role in the communication since it contains the information about the network such as the PAN ID, the coordinator short address and the association permit bit. If the association permit bit is set to TRUE, this means that association is allowed in the network. End devices uses the information contained in the beacon response in order to create the association request command to be able to join the network. The coordinator sends the association response that includes the short address assigned to the end device, if acknowledge is required for the association response, the end device shall send an acknowledge frame to let the coordinator know that the association response was received. At this point, the association was successful and both devices can start to exchange data. All this process is shown in Fig. 2-3.

2.4.4 Data Transfers

There are two ways to perform data transfers in a network, direct and indirect data transmission. Direct transmission implies that receiver device is in reception state. Different from this, indirect data transmission forces the transmitter device to hold the packet until the remote device polls for the packet.

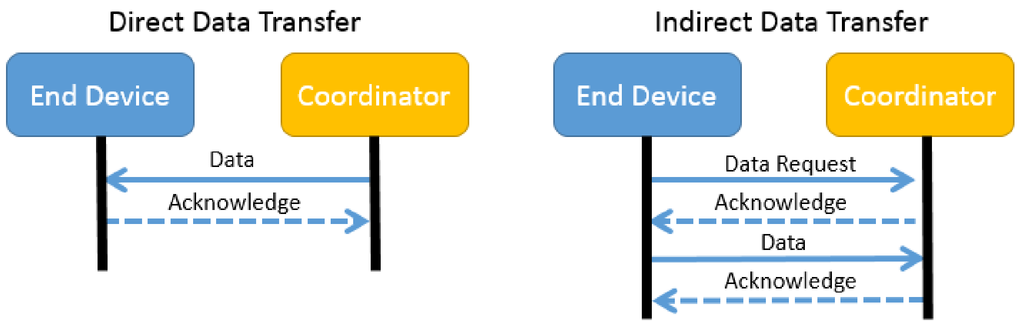

Fig. 2-6 Direct and Indirect Data Transfers.

Fig. 2-6 shows the sequence about using direct and indirect data transfers. In addition to this, there is an acknowledgement feature that is used in an IEEE 802.15.4 network, it depends on the application to enable or disable such feature.

2.4.5 IEEE 802.15.4 Packet Format

The IEEE 802.15.4 packet provides up to 102 bytes of data payload, data sequence number to track the packets and a Frame Check Sequence (FCS) to check errors in the packet. The minimum packet transmitted could be of 16 bytes while the maximum packet can be up to 127 bytes. Fig. 2-7 shows the IEEE 802.15.4 packet format.

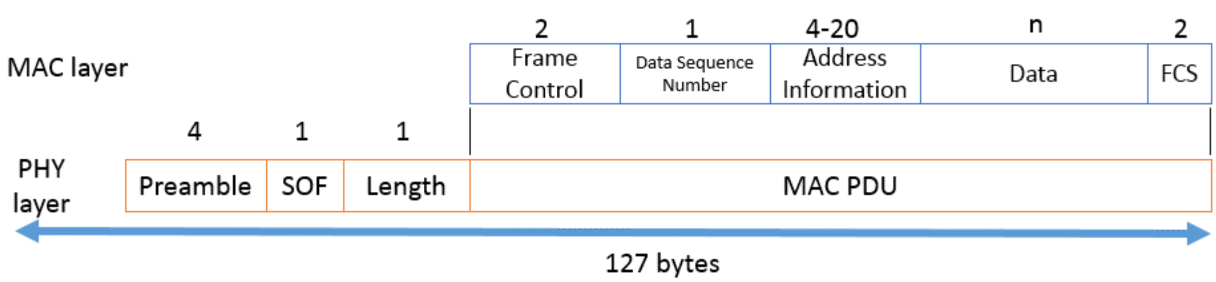

Fig. 2-7 IEEE 802.15.4 Packet Format.

2. UNDERSTANDING IEEE 802.15.4

3. Coexistence of the IEEE 802.15.4 and Bluetooth Low Energy networks

Bluetooth Low Energy and IEEE 802.15.4 are key technologies to create low power sensor devices, there are many companies developing products using these two technologies for the wireless communication. This chapter will provide the description and the results of some reports regarding the coexistence of both technologies using the same space.

3.1. Background

Wireless Sensor Networks (WSNs) are the main topic of the discussions when talking about creating a sustainable city or automated house, basically, when we talk about controlling and monitoring the temperature, humidity, on/off state of a device from our smartphone or wireless controller. Furthermore, not only to have the way to control or monitor any remote device but also to start collecting data which can help us to improve any functionality in the house and to create some profiles that can optimize the power consumption are some of the main use cases that engineers have in mind. All these kind of applications require autonomous and power efficient systems with the feature of being able to work from commercial batteries, here is where the Bluetooth Low Energy and IEEE 802.15.4 based devices play a critical role in such environment mainly because power efficiency is one of the core definitions in their specification. Hence, this is why we focus on these two technologies, as a consequence, it requires a coexistence analysis.

Some investigations around these technologies have shown the importance of analyzing these two technologies working in the 2.4 GHz frequency. There are also papers that includes Wi-Fi networks analysis due to its presence in the 2.4 GHz as BLE and IEEE 802.15.4 do. Fig. 3-1 shows how the three technologies share the physical spectrum space. However, although Wi-Fi networks have shown a big impact in the performance of IEEE 802.15.4 networks, Wi-Fi is not part of this document because of the high power consumption of this technology and it is not supported in the device that we will use for this case study. Thus, there is a need to analyze how

3. Coexistence Of The IEEE 802.15.4 and Bluetooth Low Energy Networks

BLE and IEEE 802.15.4 can coexist to have better performance in the 2.4 GHz. This chapter presents the role of the IEEE 802.15.4 and BLE in the 2.4 GHz spectrum as well as some methods and applications implementing coexistence in different ways. Taking from [7].

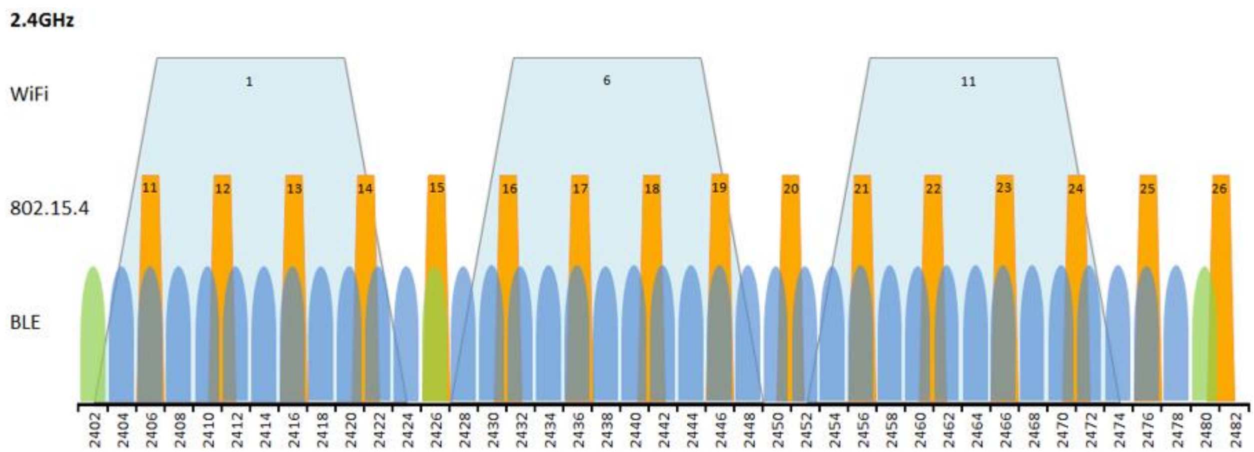

Fig. 3-1 Wi-Fi, IEEE 802.15.4 and BLE in the 2.4 GHz Spectrum.

3.2. Coexistence Methods

The importance of having self-powered devices using batteries and with the feature of communicating wirelessly to report any desired data such as humidity, temperature and other variables of the physical environment, makes IEEE 802.15.4 and BLE the most important protocols to work in an application with the above requirements. In addition to this, there are different research works that talk about the importance and the need of studying these two protocols to have a better performance. In [7], the authors mention the need to integrate these two protocols: IEEE 802.15.4 to collect the data in a mesh network and the BLE device to be the interface with smartphone devices which is the main mobile interface for people.

On the other hand, BLE and IEEE 802.15.4 based protocols have been gaining more space in the mass market. On the BLE side, we can see the increase of the fitness and medical devices such as heart rate monitors, bike sensors and glucometers that make use of this technology. On the IEEE 802.15.4 based protocols side, there are wireless controlled light bulbs and power outlets using ZigBee. Therefore, there are plenty of BLE and IEEE 802.15.4 products that have to coexist in the same physical space as well as in the frequency spectrum.

Due to all the IEEE 802.15.4 and BLE products working in the same area, there are different methods that both technology takes into account to be able to share the same frequency spectrum. There are three coexistence scenarios that will be introduced in this section.

1. BLE an IEEE 802.15.4 in the 2.4GHz Frequency Spectrum. In [8], [9], [10] and [11] it is clearly shown the importance of analyzing the 2.4GHz spectrum. There is a proposal in [9] about the importance of selecting channels that are not affected by Wi-Fi networks, it also shows that Bluetooth devices does not cause a high impact on IEEE 802.15.4 networks.
2. BLE and IEEE 802.15.4 Systems. In [9], as part of the conclusion of this application note, it is presented a signaling mechanism to avoid interference between two radios that are part of the same system. In [12], there is also the same approach offering a custom standard to coexist between a Wi-Fi module with an external IEEE 802.15.4 or BLE radio.
3. BLE and IEEE 802.15.4 Dual Mode Radios. In [7] it is shown the importance of having dual mode radios transmitting Bluetooth and IEEE 802.15.4 protocols, as in the previous scenario, a signaling mechanism should be presented inside of a device that can work in two wireless protocols such BLE and IEEE 802.15.4.

3.3. BLE and IEEE 802.15.4 in the 2.4GHz Frequency Spectrum

The 2.4GHz frequency band is popular since it is license-free frequency band. Technologies like Wi-Fi, IEEE 802.15.4, Bluetooth and Bluetooth Low Energy as well as other proprietary technologies work in this band. Although the main topic on this study case is the coexistence of BLE and IEEE 802.15.4 technologies, it is necessary to mention that there are other wireless technologies using the same frequency spectrum which causes interferences and increases the packet loss rate when there is a lot of activity in a specific range of frequencies in the 2.4GHz band.

IEEE 802.15.4 and BLE technologies define the way they access the channel in their specification. IEEE 802.15.4 uses Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) to access the channel, so it can listen if the channel is idle to transmit a packet. Different from this, BLE implements frequency hopping mechanism which is constantly jumping among BLE channels to transmit data. In this way, if a specific channel presents a lot of noise, data can be exchanged successfully in the next frequency channel. However, a high packet loss data rate is shown when there is a presence of Wi-Fi networks and different IEEE 802.15.4 or BLE active communications sharing the same physical space. The reason of the collisions is due to the big amount of energy present in the 2.4GHz whenever one of the technologies transmit a packet, this causes that the receiver can´t identify incoming packets due to the noisy environment. As shown in Fig. 3-1, all these three technologies use the same frequency space, hence, as specified in [9] there is a need to analyze the network when installing any wireless product. It is mainly to install the network in a channel that shows less energy.

The impact of Wi-Fi networks over Bluetooth and IEEE 802.15.4 is analyzed in [8] and [9], both articles mention that IEEE 802.15.4 is the most affected network when working in channels that shows high Wi-Fi traffic. A possible solution to avoid interference in the channel is the use of software algorithms with the feature of analyzing the network. This is made by performing periodic energy scans in the channel, therefore, when an average of periodic scans results in a noisy channel, the coordinator can decide to switch to a different channel with low noise. In other words, a software algorithm that monitors the energy of the environment periodically can provide meaningful data to the system which could detect when a channel is crowded due to new activity or new devices interfering with the used channel. Hence, the coordinator can choose a different channel to create the network in order to avoid a busy channel.

3.4. BLE and IEEE 802.15.4 Systems

There are other practices pursuing the coexistence between wireless technologies. In [12], a proposal using 3 wire coexistence interface is presented to be able to coexist between a Wi-Fi chip and Bluetooth or IEEE 802.15.4. The same approach could be used in a system that integrates BLE and IEEE 802.15.4 radios, this kind of systems implements coexistence algorithms that provides a priority scheduling. For example, assume that there is a system with a main processor and it contains two radios, one for BLE and one for IEEE 802.15.4, both are interconnected between them using control signals. The main processor collects information or run different tasks, one of the tasks is to send packets to the IEEE 802.15.4 or the BLE radios. Then, the control signals allow the BLE radio to tell the IEEE 802.15.4 when BLE radio is idle, so, the IEEE 802.15.4 can transmit. The IEEE 802.15.4 radio monitors the BLE control signal to know when it is ready to transmit. In this approach, the BLE transmission has higher priority mainly because the advertising interval and connection interval defined in the protocol. Hence, these intervals allow the IEEE 802.15.4 radio to transmit or receive because the BLE Link Layer will be in idle state in between the intervals. Fig. 3-2 shows this type of architectures where an IEEE 802.15.4 radio and a BLE radio share control signals to know when each of them can be active, at the same time, a main processor is connected to the radios to send them the information to be transmitted over the air.

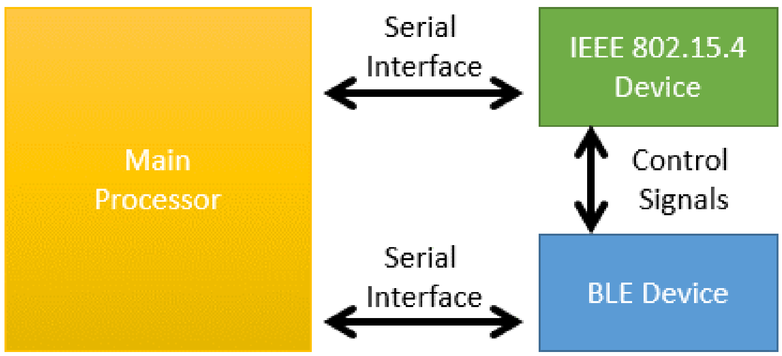

Fig. 3-2 IEEE 802.15.4 and BLE System.

3.5. BLE and IEEE 802.15.4 Dual Mode Radios

Nowadays, due to the high integration of 2.4GHz radios in the consumer market, some semiconductor manufacturers have designed devices which integrates two different link layers in the same die that shares the same physical radio. In other words, semiconductors companies merged two protocols in one radio, meaning that developers can find devices which can transmit BLE packets as well as IEEE 802.15.4 packets using the same transceiver. Developers can create dual mode or hybrid applications with the advantage of monitoring an IEEE 802.15.4 mesh network while having communication through BLE with a smartphone using a single chip. Fig. 3-3 shows a system integrating two different protocols like IEEE 802.15.4 and BLE.

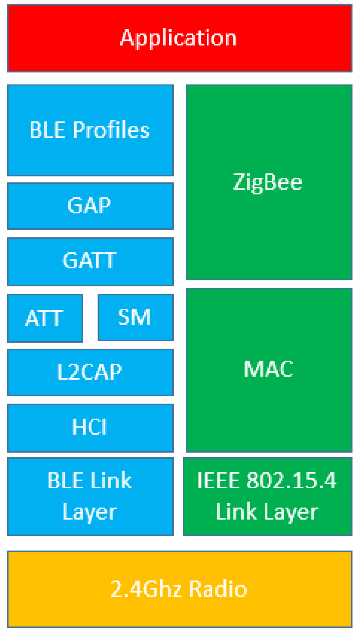

Fig. 3-3 Dual Mode Radio System.

There are different semiconductors companies that are offering this kind of solution for the "Internet Of Things" trend which requires devices talking different legacy protocols like BLE and ZigBee. The KW40Z developed by NXP semiconductors implements the architecture shown in Fig. 3-3. The next chapter will discuss about how BLE and IEEE 802.15.4 can coexist in a single chip.

4. IEEE 802.15.4/Bluetooth Low Energy Hybrid Applications

Hybrid applications are known as an application that integrate two or more technologies. This chapter will provide the description of hybrid applications using IEEE 802.15.4 and BLE technology and the results of some experiments regarding the coexistence of both technologies using the same space. Main focus of the chapter is to analyze how IEEE 802.15.4 and BLE protocols can exist in one single device sharing same physical radio that operates in the 2.4GHz.

4.1. Background

As discussed in previous chapters, there has been a need to integrate IEEE 802.15.4 and Bluetooth Low Energy protocols in one single device due to its popular use in products working in the 2.4GHz and their low power features. In fact, some semiconductor companies already offer products that are able to operate in both protocols, this has brought a new concept in wireless applications known as Hybrid or Multi-protocol applications. The main challenge of such applications is to find a way to integrate two protocols in the same silicon using one single radio. This should support a mechanism to allow intercommunications inside the chip, so, both protocols can share same resources. In this chapter, the KW40Z (first multi-protocol radio from NXP Semiconductor) device will be analyzed, thus it will discuss the architecture of the device as well as review a demonstration application showing the hybrid feature working in the IEEE 802.15.4 and BLE at the same time. The goal is to provide an analysis about the operation of both protocols using the same device and provide some recommendations about how it could be improved if possible.

4.2. The Kinetis W Series KW40Z

The KW40Z device is a System on Chip (SoC) supporting different communication interfaces as well as the first NXP Semiconductor 2.4GHz multi-protocol radio supporting IEEE 802.15.4 and

BLE. It includes the ARM® Cortex®-M0+ CPU with 160KB of flash and 20KB of RAM as well as the hardware security required by the supported protocols. The KW40Z´s radio is compliant with Bluetooth Low Energy version 4.1 and IEEE 802.15.4-2011 standard. Fig. 4-1 shows the block diagram of the KW40Z architecture where the different modules like the power management, the core peripherals, the multiprotocol radio transceiver and the supported communication interfaces are shown.

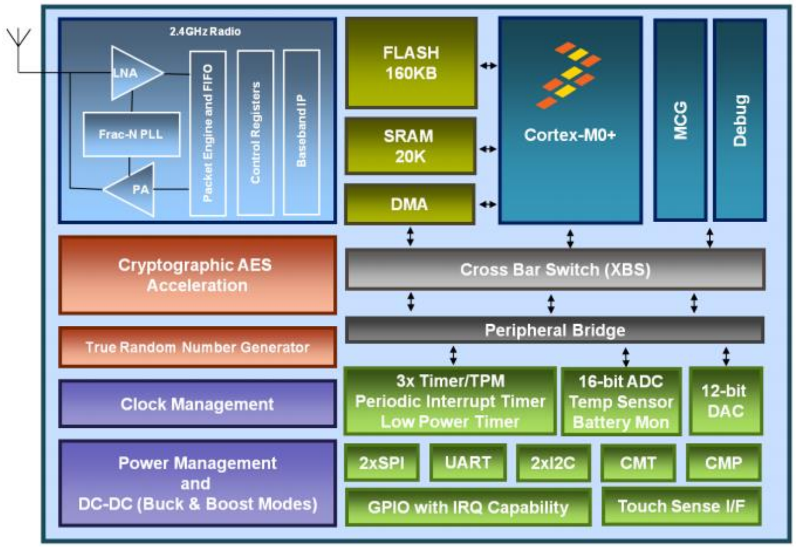

Fig. 4-1 KW40Z block diagram. Taken from [13]

Fig. 4-2 shows the radio block diagram, which basically illustrates how the transceiver or radio is integrated. It contains a Multi-standard PHY that is shared by the BLE and the IEEE 802.15.4 link layers to be able to transmit BLE and IEEE 802.15.4 packets. As it can be noticed, both link layers share one PHY, hence, there is a need of a mechanism to allow the two protocols to work together.

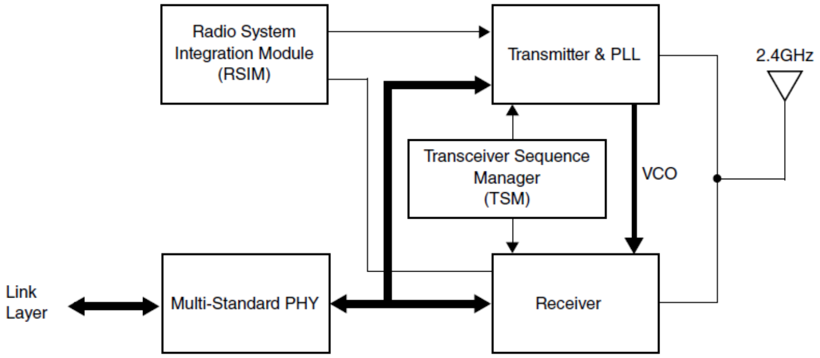

Fig. 4-2 KW40Z radio block diagram. Taken from [14].

NXP Semiconductors offers a hardware development platform “FRDM-KW40Z” or “Freedom KW40Z” to show the features of the KW40Z device such its included DC-DC converter, 16 bit ADC, touch sensing buttons, communication interfaces and its main feature which is dual protocol or multi-protocol radio. In order to demonstrate its different features, the FRDM-KW40Z platform includes the next features:

- NXP ultra-low-power MKW40Z SoC BLE/IEEE Std. 802.15.4 device.
- Integrated PCB inverted F-type antenna and SMA RF port.
- External serial flash memory for Over-the-Air Programming (OTAP) support.
- External serial NXP combo sensor FXOS8700CQ.
- Integrated Open-Standard Serial and Debug Adapter (OpenSDA).
- DC-DC converter with Buck, Boost, and Bypass operation modes through jumper configuration.
- Potentiometer.
- Two push buttons.
- Two touch sensing interface buttons.
- Four red LEDs indicators.
- One blue LED indicator.

Complete design and description of the FRDM-KW40Z platform can be consulted in [15]. The FRDM-KW40Z is supported through the NXP Semiconductor software that is called KW40Z Connectivity Software. It contains IEEE 802.15.4 and BLE software stacks to create applications supporting one of the two protocols but also it offers examples showing dual mode or hybrid application which demonstrate the feature of the device to participate in a IEEE 802.15.4 network as well as a BLE connection at the same time. This kind of application will be reviewed and discussed in the next sections.

4.3. IEEE 802.15.4 and Bluetooth Low Energy Hybrid Application

As explained in previous chapters, it is clear that BLE and IEEE 802.15.4 are two of the most popular wireless technologies. In [7], the authors clarify that there is a need to create a heterogeneous sensor network that integrates wireless sensor networks and personal area networks. In other words, it explains that there is a need to be able to access to the WSNs which support mesh IEEE 802.15.4 based products. The most appropriate device to access such WSNs is through the mobile devices like smartphones. In addition to this, in [16] it is mentioned the importance of having these two protocol in the Internet of Things trend where BLE and IEEE 802.15.4 play a key role. Thus, having applications combining BLE and IEEE 802.15.4 protocols are key interfaces to allow heterogeneous networks, in this document, these kind of applications are called hybrid applications. Hence, here is where the KW40Z device plays an important role due to its feature to operate in both protocols as mentioned in [16]. In this way, developers can save one radio in a hybrid wireless system which makes it less expensive by saving cost and space in the product design. The KW40Z Connectivity Software package includes hybrid demonstration applications that shows the feature to operate in both protocols. This section is going to describe the "ble_802_15_4_dual_mode_demo" example included in the KW40Z Connectivity Software to show the hybrid feature of KW40Z device.

The hybrid or dual mode demo example integrates the BLE Heart Rate Sensor (HRS) and the non-beacon 802.15.4 coordinator demonstration applications into a single hybrid application running on the FRDM-KW40Z platform. Basically, the BLE HRS application can have a connection with a BLE mobile application while running the IEEE 802.15.4 coordinator application that is able to get connected with IEEE 802.15.4 end devices. The BLE HRS can send notifications to the BLE mobile application while receiving or sending data to the IEEE 802.15.4 end device. The IEEE 802.15.4 data is displayed in a serial terminal while the BLE HRS data is displayed in the BLE mobile application. Fig. 4-3 illustrates the hybrid demonstration example included in the KW40Z Connectivity Software.

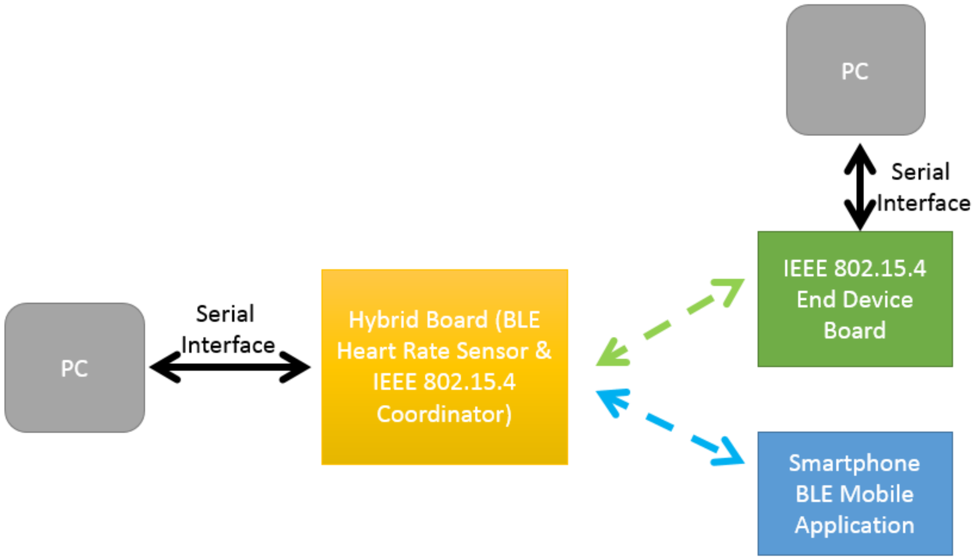

Fig. 4-3 Hybrid BLE and IEEE 802.15.4 application illustration

In order to illustrate a hybrid application, different applications are needed to cover IEEE 802.15.4 and BLE protocols functionality. The system configuration to show a hybrid scenario is built by three different demonstration applications, which are described next.

1. IEEE 802.15.4/BLE Hybrid demo. This demo is included in KW40 Connectivity Software package; it is capable of acting as a coordinator in one IEEE 802.15.4 network while acting as HRS in a BLE network at the same time. In this case, KW40 would be acting as a multiprotocol radio with the capability of monitoring both networks simultaneously.
2. IEEE 802.15.4 MyWirelessApp End Device application is used to act as an IEEE 802.15.4 end device in the network. The acknowledge mechanism is activated. This application can be also found as part of the KW40Z Connectivity Software package.
3. Kinetis BLE Toolbox mobile application. It is a smartphone application which can connect with different BLE applications such blood pressure sensor, heart rate sensor, glucose sensor, among others. In this particular case, it will be used to connect to the HRS part of the Hybrid Demo.

A smartphone, two FRDM-KW40Z boards and two personal computers (PC) are required to illustrate the hybrid demonstration application.

- A FRDM-KW40Z, known as "hybrid board", programmed with the hybrid demonstration application.

- A FRDM-KW40Z, known as "End Device (ED) board", programmed with the IEEE 802.15.4 MyWirelessApp ED.
- A smartphone supporting the Kinetis BLE Toolbox mobile application.

The hybrid board is connected to a PC via serial terminal application (i.e. Teraterm) which will display information received from the ED board as part of the IEEE 802.15.4 network, at the same time, the hybrid board is working as a BLE HRS. It is important to mention that the hybrid board is working as the coordinator of the IEEE 802.15.4 network.

The ED board is connected to the hybrid board in order to share information. For this particular demo, the information exchanged between both devices is introduced through UART interface, each board is connected to a PC through a serial terminal that is used to introduce such information. Hence, the information sent to the ED board through serial terminal is sent over the air to the coordinator, which will display the information in the peer PC serial terminal. In addition to this, the ED board sends a data request message every 820 milliseconds to ask the coordinator if there is any data available to be exchanged.

A smartphone with the Kinetis BLE Toolbox mobile application is connected to the hybrid board. Basically, the smartphone will make a connection with the HRS side of the hybrid application. Once connected, the hybrid board sends notifications every second to the smartphone at the same time it receives or sends packets to the ED board.

Although the demo shows the hybrid functionality in the KW40Z device, there is a lack of information in the KW40Z Connectivity Software package to explain how the hybrid functionality is allowed in this device. Hence, one of the research topics reported in this chapter is the description of such functionality. As mentioned before, the multiprotocol radio has to be shared between the IEEE 802.15.4 and the BLE link layers. Thus, an easy mechanism to be able to create a hybrid application is to transmit IEEE 802.15.4 packets during the idle time of the BLE link layer. As explained in previous chapters, the BLE operates using a frequency hopping mechanism, this means that it is jumping across different channels and there are idle times between each jump. These idle times are the advertising intervals and the connection intervals depending if there is a BLE connection. These intervals would be also named as BLE intervals in this document, hence, there could be a plenty of time to use the physical layer for IEEE 802.15.4 packet exchanges. BLE intervals length would depend on the BLE application configuration. However, if the connection interval is set to 45 milliseconds, there are 45 milliseconds in which the IEEE 802.15.4 link layer can transmit or receive packets when there is an active BLE connection. If the BLE sensor is in advertising mode, the advertising interval is configurable in the sensor, by default, this hybrid application configures it to be about 1.25 seconds. At the end, it is important to understand that there are windows of time in which the IEEE 802.15.4 link layer can operate, these windows are the BLE intervals. Finally, there is also some latency added due to the switching mechanism from BLE link layer to the IEEE 802.15.4 link layer, this latency is ignored in this chapter and it is transparent for the application developer. Fig. 4-4 shows an illustration about how IEEE 802.15.4 and BLE operation takes place in the KW40Z device.

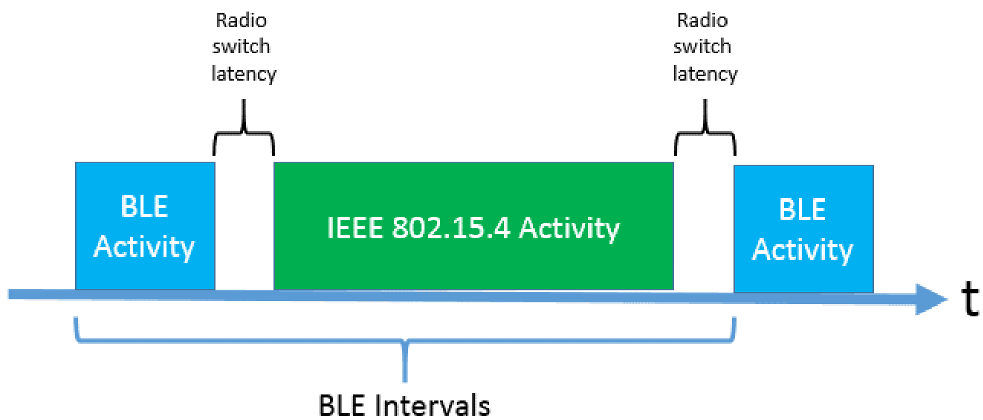

Fig. 4-4 BLE and IEEE 802.15.4 activity in the hybrid application.

In order to implement the operation shown in Fig. 4-4. The hybrid software stack offers a Wireless Mobile Standard (WMS) module to allow the BLE and IEEE 802.15.4 coexistence in the KW40Z device. The WMS is a software module which provides different functions to manage protocol communication and the switching capability between BLE and IEEE 802.15.4 modes of the KW40Z radio. It offers the feature to set priorities and determine when the radio is busy performing some BLE or IEEE 802.15.4 operation. One of the features of the WMS is to calculate the BLE idle or inactivity time, then, if there is enough time to send an IEEE 802.15.4 frame, the IEEE 802.15.4 frame is sent, the radio switches to BLE mode otherwise. This is so because the BLE mode has higher priority due to its frequency hopping mechanism. This way, the WMS module manage BLE and IEEE 802.15.4 protocols to coexist using the same system. Finally, one of the main benefits of the WMS module is that it makes transparent to the application developer to handle radio operations. The WMS implementation is embedded in the low level software layers taking care of the radio switching between IEEE 802.15.4 and BLE protocols. This makes the application developers only care about the application design. At the end, it is responsibility of the WMS to handle radio sequence accordingly.

However, there could be scenarios in which the IEEE 802.15.4 end device will send a packet and the hybrid application could be attending a BLE connection event. This would not allow the hybrid application to receive the packet from the end device, however, since there is acknowledgement support, the missing acknowledge from the hybrid application will cause the end device to retransmit the packet in a random time as specified in the IEEE 802.15.4 standard. In the KW40Z Connectivity Software default implementation, this would be in the range of 1 to 10 milliseconds. Thus, after the BLE connection event is closed, radio will switch to IEEE 802.15.4 mode to be able to receive the retransmitted packet from the end device. Hence, it is recommended that the acknowledge feature be activated when working with Hybrid applications, otherwise, some packets would be missed. Fig. 4-5 shows the scenario in which an upcoming message from the end device is retransmitted at the hybrid application due to a missing acknowledge from the coordinator that is part of the hybrid application.

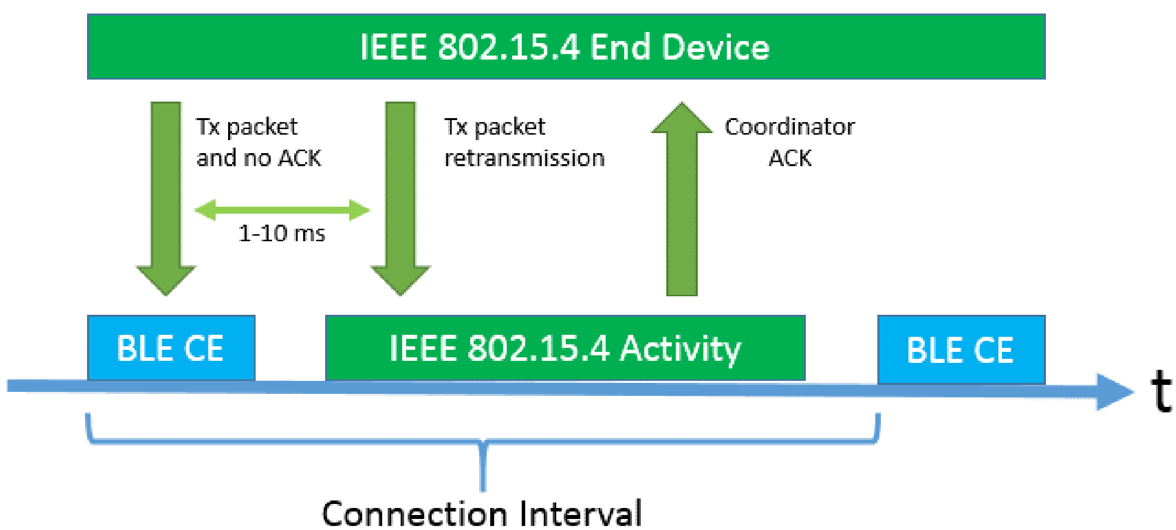

Fig. 4-5 IEEE 802.15.4 packet retransmission on hybrid application

These methods can result reliable because there is always a time frame in which the radio can attend IEEE 802.15.4 or BLE messages. For example, let's assume that there are BLE and IEEE 802.15.4 active connections using the KW40Z Hybrid application. The hybrid BLE Heart Rate Sensor would be connected to the smartphone with a connection interval of 45 milliseconds while the IEEE 802.15.4 end device would be polling the hybrid coordinator every 820 milliseconds. A formula can be deduced showing data exchange between BLE and IEEE 802.15.4 communication when polling time is bigger than the connection interval.

$$\sum_{n=1}^{\infty} \frac{(IEEE802.15.4polling * n)}{Conn_{Interval} - ConnEvtDuration} \quad (4\text{-}1)$$

From (4-1), the “IEEE802.15.4polling” is the time in milliseconds that the ED will wait to send a data request to know if there is data available, “n” represents the number of events of the data requests or polling message event, “ConnInterval” is the connection interval time in milliseconds and the “ConnEvtDuration” is the duration of the connection event in milliseconds.

If the above data is introduced in (4-1), 45 milliseconds for “Conn_Interval” and 1 millisecond of “ConnEvtDuration”, it will be noticed that every 11th polling message event, there is a collision with a connection event, this means that every 11th polling from the IEEE 802.15.4 end device, the radio would be attending a BLE connection event. However, due to IEEE 802.15.4 specification, the IEEE 802.15.4 End device will retransmit the packet at a random period from 1 to 10 milliseconds as shown in Fig. 4-5.

Nevertheless, there could be a different scenario in which some developers would like to know how many IEEE 802.15.4 packets can be send during the BLE connection intervals. This would need to be calculated based on the end device polling time as well as the connection interval. This case is shown in Fig. 4-6. Ideally in this scenario, the End Device would be sending packets just after the BLE connection event is closed and the IEEE 802.15.4 link layer is already active. Then, a latency of about 1.2 milliseconds for the acknowledgement packet is shown, this value was obtained from a sniffer capture. Hence, the number of IEEE 802.15.4 packets per connection interval would be obtained by (4-2).

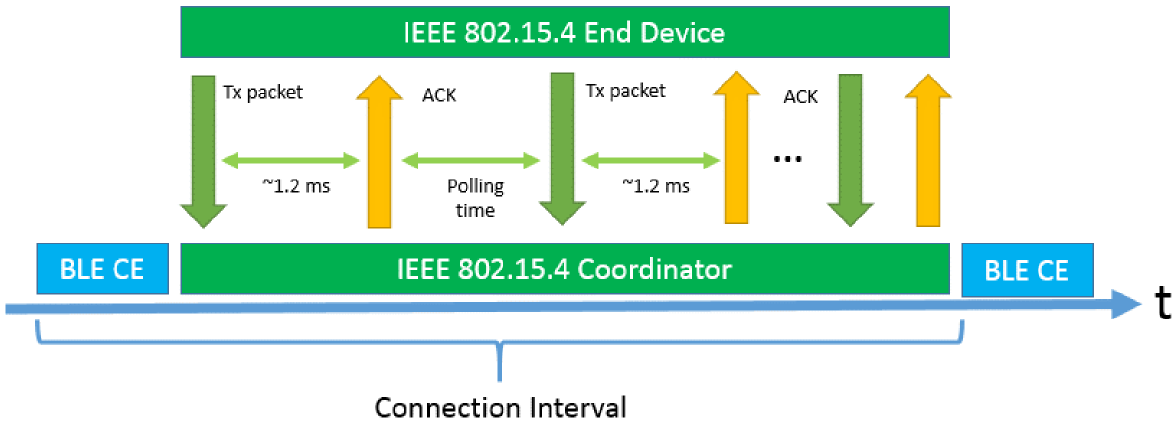

Fig. 4-6 IEEE 802.15.4 multi packet scenario

$$n = \frac{conn_{interval} - ConnEvtDuration}{poll_{time} + 1.2 + (0.032 * nbytes)} \tag{4-2}$$

From (4-2), “polltime” ” is the time in milliseconds that the ED will wait to send a data request to know if there is data available, “nbytes” is the number of bytes contained in the IEEE 802.15.4 message, “ConnInterval” is the connection interval time in milliseconds and the “ConnEvtDuration” is the duration of the connection event in milliseconds.

Hence, assuming a connection interval of 1 second and a polling time of 82 milliseconds, there could be a maximum of 11 packets of max payload (127 bytes) transmitted during the connection interval. It is worth to mention that all the values in the formula should be in milliseconds. However, it is recommended to properly design hybrid applications performing connections with the trade-off between BLE connection intervals and the IEEE 802.15.4, in other words, if a big amount of IEEE 802.15.4 packets needs to be exchanged during an active BLE connection, a bigger BLE connection interval should be negotiated to be able to exchange such data. On the other hand, if there is the need of sending a big amount of data through the BLE connection, the IEEE 802.15.4 packets exchange might be affected since connection events can get longer. The length of the connection event depends of the maximum amount of packets that can be sent during a connection event, this depends on the BLE link layer implementation and it would decrease the idle time of the BLE link layer. This last scenario is shown in Fig. 4-7.

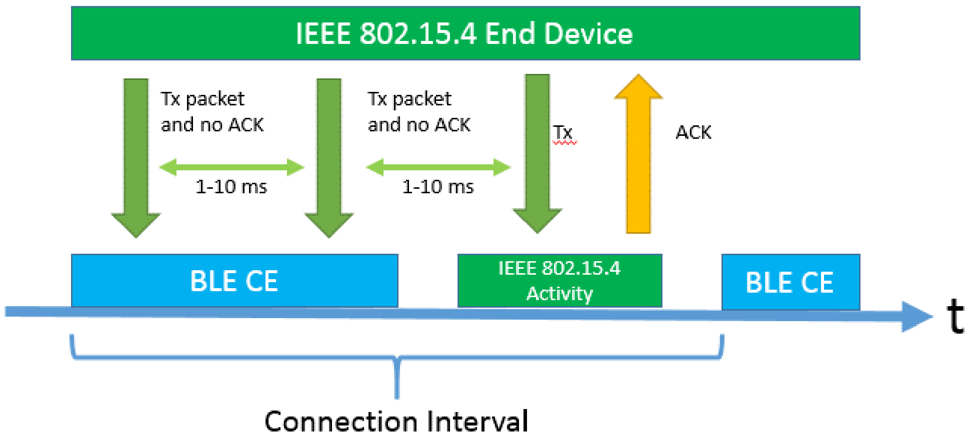

Fig. 4-7 Illustration of a longer BLE connection event.

Finally, one aspect to mention is about the memory footprint that takes to build a hybrid application shown in this chapter. Memory footprint can be consulted in the release notes of the KW40Z Connectivity Software package, it takes about 12.5KB of RAM and about 127.5KB of FLASH, so, the remaining memory for application development is 7.5KB of RAM plus 32.5KB of FLASH, this could result in a minimum space for application development, so, more memory would be desired to build more robust protocol such ZigBee or Thread.

Conclusions

This document provides an overview of the Bluetooth Low Energy and IEEE 802.15.4 protocols as well as the importance of having hybrid applications in wireless sensor networks, the main topic of this document was the coexistence of both technologies using the same frequency spectrum space as well as provide recommendations to design hybrid applications using IEEE 802.15.4 and BLE protocols. The KW40Z device was introduced as the first multiprotocol radio from NXP semiconductor which was used to run some experiments for hybrid applications and explore different recommendation when designing hybrid applications. The next conclusions were obtained from this study case.

1. Frequency spectrum analysis. First recommendation when designing and installing BLE and IEEE 802.15.4 products is to analyze the frequency spectrum to identify what channels are suitable for the application. WiFi channels are one of the biggest interferences in the 2.4GHz band, hence, it is strongly recommended to avoid WiFi channels because of its big impact on IEEE 802.15.4 and BLE networks. Moreover, different from the CSMA-CA mechanism, a software algorithm scanning the environment in a periodic way is recommended to identify if there are channels which can present high energy that can cause higher power consumption as well as high packet loss rate in the network.
2. Use acknowledgement when working with hybrid devices. The use of the acknowledgements is critical to have good IEEE 802.15.4 communications when working in hybrid devices. This is required since hybrid devices share one radio for both protocols, then, there could be incoming IEEE 802.15.4 packets when radio is attending BLE packets in a BLE connection event. Hence, since the IEEE 802.15.4 acknowledge is not received on peer device, it will send the packet again in a random range from 1 to 10 ms with a high confidence that the packet will be received since most of the BLE connection event don’t last more than 2 milliseconds. Moreover, IEEE 802.15.4 retries are configurable and there can be a value that can guarantee IEEE 802.15.4 packet reception.

3. Hybrid applications shall be studied to decide proper BLE intervals as well as IEEE 802.15.4 activity. If there is a need to transmit high amount of IEEE 802.15.4 packets, BLE intervals should be large enough to allow desired IEEE 802.15.4 packets exchange. On the other hand, if there is a need to exchange big amount of data through BLE protocol, IEEE 802.15.4 activity might be affected due to bigger connection event durations. Connection event duration depends on the allowed packets exchange on BLE link layer design.

This case study helped to understand the implications when building IEEE 802.15.4 and BLE hybrid applications on a KW40Z device, it provides description about how the hybrid applications works in the KW40Z device. This information is important to understand since there is not enough documentation in the KW40Z Connectivity Software package. It was found that there is a WMS software module which helps with the hybrid application development by just let the developer worry about the application, in other words, the WMS is in charge of switching the radio to the proper protocol mode, so the application does not need to indicate when it should be in BLE or IEEE 802.15.4 to transmit a packet.

Finally, it was found that the memory footprint of KW40Z might not be useful to build IEEE 802.15.4 based protocol stacks like ZigBee or Thread due to small remaining memory available in the hybrid application. A device with more memory footprint would be convenient for more robust hybrid applications using BLE and robust IEEE 802.15.4 based protocols. However, current KW40Z is suitable for IEEE 802.15.4 and BLE applications.

References

[1] Bluetooth SIG, “Bluetooth Core Specification Version 4.1,” 03 December, 2013.

[2] Kevin Townsend, Carles Cufi, Akiba and Robert Davidson, *Getting Started with Bluetooth Low Energy*. Sebastopol, CA: O’Reilly, May 2014.

[3] Robin Heydon, *Bluetooth Low Energy: The developer’s Handbook*. Crawfordsville, IN: Pearson Education, October 2012.

[4] *IEEE Standard for Local and metropolitan area networks, Specific Requirements Part 15.4: Low Rate Personal Area Networks (LR-PANs)*, IEEE Standard 802.15.4-2011.

[5] Sajid M. Sheikh, Riaan Wolhuter and Herman A. Engelbrecht, “A Random Priority based Scheduling Strategy for Wireless Sensor Networks using Contiki,” *International Conference on Wireless Networks and Mobile Systems*, Lisbon, Portugal, Jan. 2016, pp. 121-128.

[6] Jon T. Adams, “An Introduction to IEEE STD 802.15.4,” in *IEEE Aerospace Conference*, Montana, United States, Mar. 2006.

[7] J. Eliasson, C. Zhong, and J. Delsing. “Heterogeneous Sensor Network Architecture for Highly Mobile Users” in *Wireless Communication and Sensor Networks, 6th International Conference*, Uttar Pradesh, India, Dec. 2010.

[8] S. Zacharias, T. Newe, S. O’Keeffe, E. Lewis. “Coexistence Measurements and Analysis of IEEE 802.15.4 with Wi-Fi and Bluetooth for Vehicle Networks” in *ITS Telecommunications*, Taipei City, Taiwan, Nov. 2012.

[9] A. Sikora, and V. Groza. “Coexistence of IEEE802.15.4 with other Systems in the 2.4 GHz-ISM-Band” in *Instrumentation and Measurement Technology Conference*, Ottawa, Canada. May 2005, pp. 1786-1791.

[10] *Co-existence of IEEE 802.15.4 at 2.4 GHz Application Note*, NXP Semiconductors, UK, 2013.

[11] *Wireless Coexistence in the 2.4 GHz Band Application Note*, NXP Semiconductors, Austin, TX, 2015.

[12] *Collaborative Coexistence Interface Between Broadcom-to-Broadcom Solutions and Broadcom- to-third-party Chips Application Note*, Cypress Semiconductors Corp, 2016.

[13] *MKW40Z/30Z/20Z Data Sheet*, NXP Semiconductors, US, 2015.

[14] *MKW40Z/30Z/20Z Reference Manual*, NXP Semiconductors, US, 2015.

[15] *FRDM-KW40Z Freescale Freedom Development Board User’s Guide*, NXP Semiconductors, US, 2015.

[16] P. Narendra, S. Duquennoy and T. Voigt. “BLE and IEEE 802.15.4 in the IoT: Evaluation and Interoperability Considerations” in *International Conference on Interoperability in IoT (EAI InterIoT 2015)*, Roma, Italy, Oct. 2015.