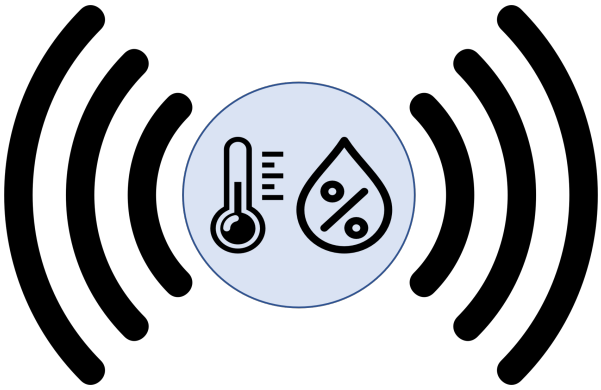
TÉCNICO LISBOA



Wireless Sensor Networks for Environmental Monitoring

Ismael Filipe Maia Gonçalves da Trindade

Thesis to obtain the Master of Science Degree in

Electrical and Computer Engineering

Supervisor(s): Prof. João Manuel Torres Caldinhas Simões Vaz

Examination Committee

Chairperson: Prof. Francisco André Corrêa Alegria
Supervisor: Prof. João Manuel Torres Caldinhas Simões Vaz
Member of the Committee: Prof.Jorge Manuel Dos Santos Ribeiro Fernandes

November 2021

Declaration

I declare that this document is an original work of my own authorship and that it fulfills all the requirements of the Code of Conduct and Good Practices of the Universidade de Lisboa.

Declaração

Declaro que o presente documento é um trabalho original da minha autoria e que cumpre todos os requisitos do Código de Conduta e Boas Práticas da Universidade de Lisboa.

Acknowledgments

First of all, I would like to thank the *Instituto de Telecomunicações* (IT), IT – Lisboa, where this dissertation was conducted. Furthermore, I would like to thank the project ”Wireless Sensor Network for Environmental Monitoring (WSN-EM)”, PTDC/EEI-EEE/30539/2017, financed by *Fundação para a Ciência e Tecnologia (FTC)*.

I am deeply thankful to my supervisor, Prof. João Vaz, for his support, guidance and encouragement. I am grateful for the opportunity of working with him, the experience itself, and the knowledge gained during this dissertation.

To all my friends, particularly to those who shared this journey with me, Lourenço, Tomás, Miguel, Madalena and João. Thank you for your companionship and adventures.

I would like to express my gratitude to my family, especially my parents, brother and grandparents, as well as Carolina, who have always been there for me throughout my academic career and to whom I dedicate my thesis. It would not have been possible for me to reach this milestone without your support.

Resumo

As Redes de Sensores Sem Fio (RSSF) são consideradas uma das tecnologias de informação com maior crescimento, além de terem uma ampla variedade de aplicações com enorme potencial. A capacidade de detecção e transmissão sem recurso a uma infraestrutura física permanente tornam esta tecnologia especialmente apelativa para a utilização em sistemas de monitorização, nomeadamente na monitorização ambiental.

Esta tese irá apresentar alguns conceitos fundamentais, os principais desafios no planeamento e as aplicações das RSSF. Actualmente, embora hajam inúmeros protocolos no mercado, o foco deste estudo será nas mais proeminentes iniciativas de standardização de protocolos abertos para RSSF. Este estudo permitirá desenvolver um documento que auxiliará os investigadores de circuitos eletrónicos na procura de um protocolo. Os protocolos ZigBee e Bluetooth Low Energy serão aprofundados com maior detalhe, de modo a compreender melhor o funcionamento inerente de um protocolo. E, assim, ajudar no desenvolvimento de um protocolo proposto.

Por fim, esta dissertação irá propor um simples protocolo, destinado a fins experimentais, para monitorização ambiental de humidade e temperatura. Uma vez que os sensores são projectados para terem uma autonomia de bateria de vários anos, é fundamental simplificar a gestão da rede e o consumo de energia pelas comunicações. Deste modo, este protocolo visa reduzir o consumo energético da rede. As aplicações deste sistema incluirão monitorização ambiental e agricultura de precisão, bem como a capacidade de detecção de um incêndio, ao detectar um aumento repentino da temperatura acima de um certo limite. Estas aplicações beneficiarão a sociedade de diversas formas.

Palavras-chave: Redes de Sensores Sem Fios, Standards, Monitorização Ambiental, Bluetooth Low Energy, ZigBee.

Abstract

Wireless Sensor Networks (WSNs) are regarded as one of the most rapidly developing information technologies, with a wide variety of potential applications. Their capacity to sense and transmit without a permanent physical infrastructure, makes them an appealing technology for use in monitoring systems, particularly in Environmental Monitoring.

This thesis will introduce some fundamental concepts of WSNs, their design challenges and applications. Moreover, an overview of several prominent standardization initiatives for open standard protocols for Wireless Sensor Networks will be presented. This study provides a document that will help electronic circuit design researchers in their search for a protocol. Currently, there are numerous protocols in the market, however, the focus of this study will be on the open standards. Furthermore, ZigBee and Bluetooth Low Energy protocols will be explained in greater depth to better comprehend the functioning of a protocol and assist in the development of a proposed protocol.

Finally, this dissertation discusses a simple proposed protocol for environmental sensing, which monitors humidity and temperature, and is intended for experimental purposes. Considering that the sensor nodes are projected to have a battery autonomy of several years, it is critical to simplify the network management and the communications energy consumption. Therefore, this protocol aims to reduce network energy consumption and management. Applications of this system will include environmental and precision agriculture monitoring, as well as fire detection capability by tracking a sudden temperature increase over a certain threshold. These applications will benefit society in a variety of ways.

Keywords: Wireless Sensor Networks, WSN Standards, Environment Monitoring, Bluetooth Low Energy , ZigBee.

Contents

List of Tables

List of Figures

List of Acronyms

AA Access Address.

ACL Access Control List.

ADV Advertising.

AES Advanced Encryption Standard.

AHR Application Support Sublayer Header.

AMP Alternate MAC/PHY.

AMR Automatic Meter Reading.

AoA Angle of Arrival.

AoD Angle of Departure.

APL Application Layer.

App BLE's Application Layer.

ATT Attribute Protocol.

BIG Broadcast Isochronous Group.

BLE Bluetooth Low Energy.

BLE5 Bluetooth Low Energy 5 Specification.

BPSK Binary Phase-Shift Keying.

BR Basic Rate.

BS Base Station.

BSN Beacon Sequence Number.

BSN Base Station Network. **CBC-MAC** Cipher Block Chaining - Message Authentication Code.

CCA Clear Channel Assessment.

CLH Cluster Head. **CP** CTEInfo Present.

CRC Cyclic Redundancy Check.

CSA Channel Selection Algorithm.

CSMA-CA Carrier Sense Multiple Access with Collision Avoidance.

CSRK Signature Resolving Key .

CSS Chirp Spread Spectrum.

CTE Constant Tone Extension.

DBPSK Differential Binary Phase-Shift keying.

DSSS Direct Sequence Spread Spectrum.

D7AP DASH7 Alliance Protocol.

ECDH Elliptic Curve Diffie-Hellman.

ED Energy Detection.

ED End-Device.

EDR Enhanced Data Rate.

FCS Frame Check Sequence.

FDMA Frequency Division Multiple Access.

FEC Forward Error Correction.

FFD Full-Function Devices.

FHSS Frequency-Hopping Spread Spectrum.

FSK Frequency Shift Keying.

GAP Generic Access Profile.

GATT Generic Attribute Profile.

GFSK Gaussian Frequency-Shift Keying.

GMSK Gaussian Minimum Shift Keying .

GTS Guaranteed Time Slots.

HCI Host Controller Interface.

ID Identification.

IEEE Institute of Electrical and Electronics Engineers.

IETF Internet Engineering Task Force.

IPv6 Internet Protocol version 6.

IoT Internet of Things.

ISM Industrial, Scientific and Medical.

ITU International Telecommunication Union.

L2CAP Logical Link Control and Adaptation Protocol.

LE Low Energy.

LEACH Low Energy Adaptive Clustering Hierarchy.

LEPC Low Energy Power Control.

LL Link Layer.

LLID Logical Link Identifier.

LoRaWAN Long Range Wide-Area Network.

LPN Low Power Node.

LPWA Low Power Wide Area.

LQI Link Quality Indicator.

LSB Least Significant Bit .

LTE Long Term Evolution.

MAC Medium Access Control.

MD More Data.

MFR Medium Access Control Frame.

MHR Medium Access Control Header.

MIC Message Integrity Code.

MSB Most Significant Bit.

M2M Machine-to-Machine.

NESN Next Expected Sequence Number.

NHR Network Layer Header.

NWK Network Layer.

O-QPSK Offset Quadrature Phase-Shift Keying.

OSI Open System Interconnect.

PAN Personal Area Network.

PDU Personal Area Network.

PHY Physical Layer.

PHR Physical Layer Header .

PN Pseudo-Random Noise.

PPDU Physical Protocol Data Unit.

PSDU Physical Service Data Unit.

P2P Peer-to-Peer.

RF Radio Frequency.

RFD Reduced-Function Devices.

RFID Radio Frequency Identification.

RFU Reserved for Future Use.

RTC Real Time Clock.

SoC System-On-Chip.

SDF Start-of-Frame Delimiter.

SHR Synchronisation Header.

SIG Special Interest Group.

SMP Security Manager Protocol.

SMS Short Message Service.

SN Sensor Node.

SN Sequence Number.

TCXO Temperature Compensated Crystal Oscillator.

TERM Terminator.

TVWS Television White Space.

UWB Ultra-Wide Band.

WAN Wide Area Network.

WebS Web Server.

WSAN Wireless Sensor and Actuator Networks.

WSN Wireless Sensor Network.

Chapter 1

Introduction

1.1 Motivation

Over the past few years, there has been an increase in weather conditions as a consequence of climate change. For this reason, it emphasizes the importance of a thorough understanding of our environment and its development for human beings. Wireless Sensor Networks (WSN) have been used in a variety of industries and can also be used in environmental monitoring applications.

Environmental monitoring using WSN is of most importance to help prevent natural catastrophes and predict climate change. Late detection of a wildfire allows it to grow to larger proportions, making it more difficult to extinguish. WSNs would detect and send a fire alarm as soon as possible, increasing firefighters' performance.

Furthermore, it can be used in a variety of applications, in order to assist people in their work and reduce cost and time. In agriculture, WSNs are capable of measuring the humidity and temperature present in the fields. These sensed measures allow the farmer to determine whether or not it is necessary to irrigate the crops, thereby conserving valuable natural resources such as water, which are becoming increasingly scarce.

Currently, there are many technologies suitable for Wireless Sensor Networks, making the decision of selecting one to be implemented much harder. However, some protocols excel in comparison to others, most notably those that are open protocol standards. These standards are open to the public and are maintained through a collaborative and consensus driven process. Thus, facilitating interoperability, data exchange between devices and they are designed for widespread adoption. Therefore, the initial motivation was to make a study on the available open protocol standards suitable for WSNs, in order to help the electronic design circuit researchers to choose one for their future projects.

Moreover, a protocol is necessary to test in the field the functioning of the electronic circuit, designed by the researchers. Furthermore, the importance of balancing energy consumption with transmission time cannot be ignored. Thus, this thesis proposes a simple protocol for environmental sensing.

1.2 Objectives

The purpose of this thesis is to elaborate a document that would be useful for the electronic circuit design researchers and it is not intended for telecommunications development. The main task is to gather an overview of the predominant open standards for wireless sensor networks, in order to provide a manual that could assist circuit design researchers in developing a radio communication system.

In this particular case, a simple and energy efficient proprietary protocol based on Bluetooth Low Energy will be discussed, not with the objective of competing with industrial networks, but to be used in scientific field experiments. The goal of this proposed protocol is to provide a simple communication protocol that can be used to test and prove that the radio communication system devel oped by the researchers, using the star topology, consumes very little energy.

The work carried out within this thesis was hosted by Instituto de Telecomunicações at Instituto Superior Técnico, University of Lisbon.

1.3 Thesis Outline

This section aims to present a brief description of topics covered in each chapter for a better understanding of the work that follows. This thesis is composed by a total of six chapters.

In Chapter 2 it is introduced the applications of wireless sensor networks and its standardisation initiatives. Firstly, it will be introduced the main concepts of a WSN, its design challenges and its deployment in different use cases. Secondly, an overview of the most popular standardisation initiatives for WSN.

Chapter 3 gives an introduction to the ZigBee standard protocol in further detail, describing its architecture, physical layer, MAC layer and other aspects.

Chapter 4 comprises information about the Bluetooth Low Energy standard protocol in more detail, introducing its architecture, physical layer and link layer.

Chapter 5 details the proposed approach of a simple protocol for environmental sensing.

Finally, Chapter 6 concludes the thesis, summarising the approach and outlining the main limitations to be addressed in future work.

Chapter 2

Applications of WSN and standardization Initiatives

2.1 Introduction to Wireless Sensor Networks

Wireless Sensor Networks (WSNs) are self-configured wireless networks that do not require any infrastructure. They are designed to monitor physical parameters or environmental conditions such as temperature, humidity, sound, vibration, pressure, motion, or pollutants and transmit the sensed data across the network to a centralised location or *sink*, where it can be viewed and analysed [1]. A sink, also referred to as a base station, is a special node responsible for collecting, processing, and controlling data from a group of sensor nodes. One can obtain information from the network by inserting queries and retrieving results from the sink.

A wireless sensor network can be as small as a two-node network or as large as thousands of nodes connected. The actual network size will vary depending on the application and deployment, but it is expected that a WSN will have a significant number of nodes in general.

Sensor nodes are devices that have at least one sensor and may include actuators, as well as processing and networking capabilities for data processing and wireless access. Sensors measure an observation's physical property and quantity, converting the measure into a signal that may be electrical (e.g. current, voltage, power, resistance, etc.), mechanical (e.g. pressure, flow, liquid density, humidity, etc.) chemical (e.g. oxygen, carbon monoxide, etc.), acoustic (e.g. noise, ultrasounds, etc.), or any other signal type. Actuators are devices that can respond to a stimulus(caused by an input signal) by performing an action (e.g. turning on a light, triggering an alarm, turning off an irrigation system, etc).

Radio signals allow the sensor nodes to communicate with each other. Sensing and computing devices, radio transceivers, and power components are all integrated into a wireless sensor node.

The sensor nodes in a WSN possess very limited processing speed, storage capacity, and communication bandwidth due to their design constraints.

After being deployed, the sensor nodes are responsible for self-organising an adequate network infrastructure, which typically includes multi-hop communication. The inbuilt sensors then begin collecting

data of importance. Wireless sensor devices also respond to requests for specific instructions or sensing samples given from a control site. Actuators can be added to wireless sensor devices, in order to perform certain tasks in response to particular situations. This kind of network has a more specific term, which is Wireless Sensor and Actuator Networks (WSAN).

WSNs can be stand-alone networks, although connecting them to other networks (such as the Internet) for remote access and management may be beneficial. In this situation, a Sensor Network Gateway can provide communication between the WSN and another network.

Wireless sensor networks enable innovative applications and require nontraditional protocol design paradigms, due to numerous limitations. An appropriate balance between communication and signal/data processing capabilities must be achieved, because of the demand for minimal device complexity along with low energy consumption. This has motivated a massive effort in research, standardization, and industrial investments in this area [1].

2.2 Applications of WSNs

WSN technology allows a wide range of control and monitoring Sensor Network Applications (or use cases) in a variety of contexts, including environmental monitoring, healthcare and assisted living, sports and fitness, critical infrastructure monitoring, logistics, home automation, industrial monitoring, smart metering and urban monitoring [2].

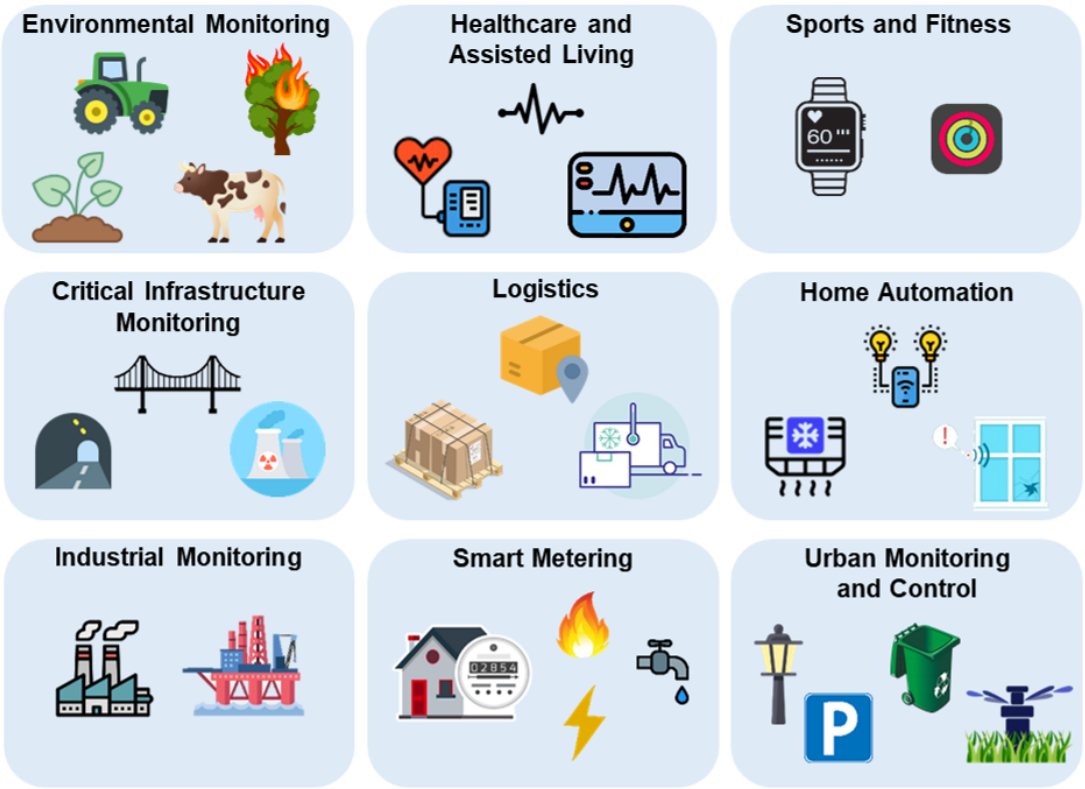


Figure 2.1: Applications of WSN across different sectors (this image was designed using resources from [3–5]).

2.2.1 Environmental Monitoring

In this application, sensor nodes are dispersed across a specific area to monitor factors such as temperature, humidity, pollen concentration, UV radiation, ambient noise, air pollutants and several other parameters. These data allows researchers to investigate the environmental conditions of a certain area and how they affect people, animals or vegetation. Environmental sensor networks have a wide range of WSN applications in earth scientific research, such as sensing volcanoes, oceans, glaciers, and forests.

Moreover, environmental monitoring systems are utilised in a variety of applications to help people in their work and to reduce costs and time. Agricultural monitoring, habitat monitoring, indoor monitoring, greenhouse monitoring, temperature monitoring, and forest monitoring are all examples of environmental monitoring applications that have evolved significantly.

Agricultural monitoring improves productivity, not only in quantity but also also in quality, and the scarcity of water in certain regions justifies the use of sensors that allow to see the degree of humidity of the soil to determine the timing and amount of watering. Also humidity of the leaves can be used to predict the possibility of fungal infections, as well as solar radiation meters, to determine the degree of maturity and therefore the ideal time to harvest.

Forest monitoring includes fire monitoring, which detects fire ignition using sensors deployed strategically and densely in a forest. These sensors will transmit the specific origin of the fire to end users, before it spreads uncontrollably. This sensed data provides valuable information that can help the firefighters to understand the fire behaviour such as point of ignition, the spread speed and the direction of maximum spread [6].Furthermore, because the sensors may be left unchecked for months or years, effective power harvesting techniques, such as solar cells, may be used to power them [7].

2.2.2 Healthcare and Assisted Living

For an accurate diagnosis, wearable wireless sensors can record the levels of many physiological parameters, such as temperature, blood pressure, electrocardiograph, and insulin, on a regular basis.

In the hospital or at home, sensor nodes can be used to locate, monitor, and identify patients. This provides remote care, allowing patients that are disabled or the elderly to get care at home. On the other hand, if critical events are detected, alarms can be set off, for example acceleration sensors may indicate that a person has fallen [1].

2.2.3 Sports and Fitness

Sports and fitness are another application area where wearable sensors can contribute. Heart rate sensors may connect with a watch that displays the outcome of the measurement or with a device that stores the important data of a training session, for example. Furthermore, this data may be transmitted to a remote database using a connection to the Internet, where the recorded data may be processed and evaluated, and a ”virtual trainer” can offer feedback and assistance to the user while the training session is in progress [2].

2.2.4 Critical Infrastructure Monitoring

Periodic architectural health monitoring may help buildings, bridges, tunnels, and other structures. Sensor networks can be employed in infrastructures and mechanical systems to undertake continuous monitoring of parameters to predict the collapse of a bridge or the breakage of a piece. For this purpose, it is mostly used vibration, displacement, and temperature sensors .

On the other hand, when emergency situations (such as seismic testing or structural damage) are detected, the sensor nodes can rapidly report the occurrence, allowing necessary responses to be taken. Internal pipeline corrosion monitoring is another possible use in the petroleum and natural gas industries [8].

2.2.5 Logistics

WSNs can be used in the logistics domain since many logistics systems require real time monitoring of numerous environmental conditions and improved package handling (tracking products, pallets or luggage). These needs can be met by combining logistics and WSNs.

The use of WSNs in Cold Chain Logistics (a supply chain that maintains a constant temperature) can considerably improve chain monitoring and management [8]. WSNs can be used to monitor a variety of environmental conditions in real time and collect reliable data to meet the needs of Cold Chain Logistics, for example the shipping and storage of vaccines to combat the current global pandemic, COVID-19.

2.2.6 Home Automation

WSNs provide a wide range of applications for user comfort and home control in the house, such as: light control, window shades, heat ventilating and air conditioning, glass-break sensors and motion sensors. All of this can be controlled using data obtained by a variety of sensors that monitor characteristics including temperature, humidity, light, and presence [8].

2.2.7 Industrial Monitoring

Critical communications are carried out in industrial contexts utilising cables, which are known to be more reliable than wireless connectivity. Nevertheless, adding wireless sensor nodes for managing devices that are not already connected will benefit these environments. WSNs will enable monitoring operations that are presently performed manually or not at all.

In harsh industrial environments (chemical, energy or water treatment industries), WSN applications could be of great interest. The location of the personnel can be obtained in real time and they can also initiate an emergency request if necessary. Monitoring chemical agents in the environment, as well as the levels of fuels and gas tanks, is an additional important application in these circumstances [8].

2.2.8 Smart Metering

Data collecting from utility meters has traditionally needed human intervention. Companies that provide gas, water, and electricity have attempted to read meters at customers' homes remotely. Wireless sensor Automatic Meter Reading (AMR) systems provide a low-cost method for gathering a home's electric, gas, and water usage and report it to the operator [9].

2.2.9 Urban Monitoring and Control

Wireless sensor networks can be used in an urban environment to monitor and control irrigation of green areas, reduce lighting in areas where people are not present, schedule waste pickup based on container filling, and identify available parking spaces. This applications may result in a reduction in staff and an improvement in the information offered to the community [8].

2.3 Design challenges in Wireless Sensor Networks

The deployment of sensor networks has numerous obstacles. Without any infrastructure, sensor nodes communicate on wireless, lossy lines. Another concern is the sensor nodes' limited, usually non-renewable energy supply. To ensure that the network will last as long as possible, the protocols must be developed from the beginning with the goal of effective energy resource management.

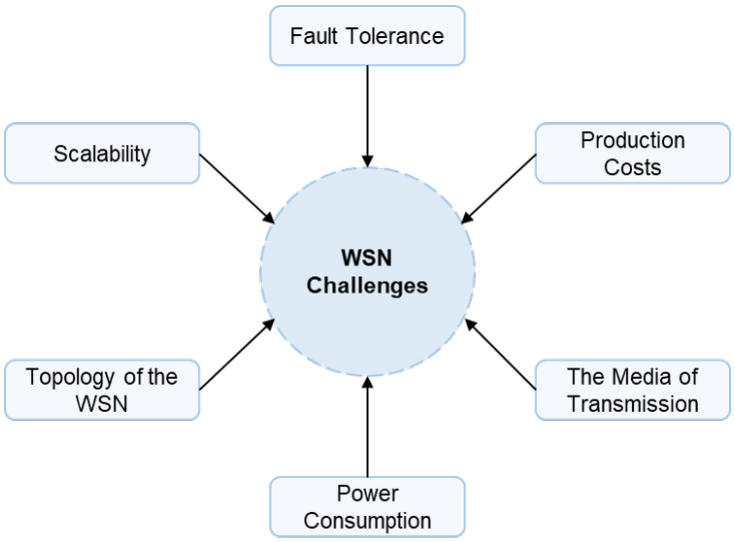


Figure 2.2: Design challenges in WSN.

Many aspects impact sensor network design, including scalability, fault tolerance, manufacturing costs, hardware restrictions, WSN topology, transmission media, and power consumption [1, 10, 11].

2.3.1 Scalability

Wireless sensor networks can differ in scale from a few nodes to several hundreds. Furthermore, the deployment density is variable. The node density for collecting high resolution data could reach the

point where a node's transmission range has numerous neighbors. The protocols used in WSNs should be scalable to these levels and capable of successfully maintaining and preserving performance.

2.3.2 Fault Tolerance

Sensor nodes(SN) are susceptible and are commonly used in hazardous environment. Nodes can fail due to hardware issues, physical damage, or an insufficient supply of energy. Node failures are expected to be much higher than in wired or infrastructure based wireless networks that have been strengthened. The protocols used in an SN should be capable of quickly detecting node failures and of handling a large number of node failures while maintaining and preserving the network's full functionality. This is especially important in the design of routing protocols, which must ensure that alternative paths are available for packet redirection. Fault tolerance criteria vary depending on the deployment environment.

2.3.3 Production Costs

Wireless sensor networks may be able to compete with traditional information gathering methods if individual sensor nodes can be produced economically, as many deployment models regard sensor nodes as disposable equipment. A sensor node's target price should preferably be very low.

2.3.4 Hardware Constraints

Every sensor node must have a sensing unit, a processing unit, a transmission unit, and a power supply at the very least. Optionally, the nodes may contain numerous built-in sensors or external devices such as a localisation system, to allow location aware routing. However, each additional feature comes at a cost and increases the node's power consumption rate and physical dimensions. Thus, additional functionality must be constantly evaluated against cost and power requirements.

2.3.5 Topology of the WSN

Despite the fact that WSNs have progressed in various areas, they continue to have limited resources in terms of energy, computational power, memory, and communications capabilities. Energy consumption is of the utmost importance, as evidenced by the vast number of algorithms, procedures, and protocols created to conserve energy and thereby extend the network's lifetime. One of the most critical challenges that could assist in the decrease of energy consumption in WSN is topology maintenance.

2.3.6 The Media of Transmission

Radio communication over the widespread ISM bands is often used to communicate and interact among the nodes. However, some sensor networks use optical communication or infrared communication, with infrared communication having the benefit of being robust and practically absent of interference.

2.3.7 Power Consumption

As previously mentioned, the majority of the WSNs's challenges revolve around their restricted power resources. The battery's size is limited by the size of the nodes. As a consequence, there is a need to carefully consider concerns of efficient energy consumption while building both software and hardware architecture. Data compression, for example, may lower the amount of energy consumed for radio transmission, but it requires more energy for computation and/or filtering. Furthermore, the energy policy is dependent on the application; for example, in some applications, it may be acceptable to turn off a subset of nodes in order to save and conserve energy, whilst in other cases, all nodes must be active simultaneously.

2.4 WSN standardization Initiatives

The standard specifies the functionalities and protocols that sensor nodes must use to communicate with different networks. There are a variety of standard WSN architectures, each of which is further characterised by amendments and upgrades. True interoperability between devices and applications requires universally accepted specifications and protocols, which can only be achieved through standardization.

This section highlights some of the most prominent WSN standardization initiatives. Several well-known standard developing organisations (SDOs), such as the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), the International Telecommunications Union (ITU), the International Organisation for standardization (ISO) and the International Electro-technical Commission (IEC) are involved in a variety of open standardization projects along with industrial consortia such as, the ZigBee Alliance, the Bluetooth Special Interest Group(SIG), the LoRa Alliance, the Dash7Alliance and Weightless SIG. These SDOs and SIGs have the objective of having these standards adopted, in order to minimise WSN market fragmentation and allowing several competing technologies to coexist.

The importance of Open Standards

In essence, open standards offer greater value to the end-user. Closed standards may be used by product managers and developers who believe that they will provide additional security, guarantee interoperability between their products, or force consumers to purchase more of their own products in order to get the most value out of the products they have already purchased. However, consumers desire alternatives, and the industry is recognising that proprietary ecosystems are no longer feasible. Nowadays, the vast majority of WSN manufacturers use open and standardised networking protocols, allowing the freedom of choice to the consumers [12].

There are protocols that gain market dominance without going through the standardization process. These protocols are referred to as *de facto* standards, which are common in emerging markets or monopolised markets, and are capable of holding a market to deter potential competition. standardization

is as a countermeasure to the negative effects of *de facto* standards. There are positive exceptions, like Linux, operating system, a *de facto standard* operating system, which does not have this negative market grip, because the sources are published and maintained openly, inviting competition.

2.4.1 IEEE

The Institute of Electrical and Electronics Engineers (IEEE) is a not-profit organisation committed to engineering, computing, and technology development [13]. The IEEE supervises several publications, conferences, technical standards, and professional and educational events.

Figure 2.3: The Institute of Electrical and Electronics Engineers (IEEE) logotype (extracted from [13]).

IEEE's major standard for WSNs is *IEEE 802.15.4*, which defines the physical (PHY) and Medium Access Control (MAC) layer functions of a low power radio interface. It was created to optimise battery life in wireless sensor systems used in short-range communication. The physical layer supports low bands of 868/915 MHz and high bands of 2.4 GHz. For managing access to the radio channel, the MAC layer employs CSMA/CA.The IEEE 802.15 Task Group 4 was formed to study a low data rate solution with multi-month to multi-year battery life and very minimal complexity.

Residential, industrial, and environmental monitoring, control, and automation are among the wireless sensor applications that use this standard. IEEE 802.15.4 has essentially become the *de facto* radio interface for WSNs [14].

2.4.2 IETF

The Internet Engineering Task Force (IETF) is an open multinational community of network designers, operators, manufacturers, and academics concerned with the development and efficient operation of the Internet. The IETF designs and updates Internet protocols and architectures [15]. The specifications developed by the IETF are not official standards, but they are *de facto* standards, which means that a wide community accepts and uses their specifications.

Figure 2.4: The Internet Engineering Task Force (IETF) logotype (extracted from [15]).

Working Groups (WGs) of the Internet Engineering Task Force (IETF) develop publications with the purpose of providing solutions and relevant information for specific Internet problems.There are three main IETF WGs relevant to WSNs:

- The IPv6 Low power Wireless Personal Area Network (6LoWPAN) WG has the objective of developing solutions for enabling IPv6 packet transfer on top of IEEE 802.15.4 networks [16].
- The Routing over Low Power and Lossy Networks (ROLL) Working Group was formed with the goal of creating routing solutions for Low Power and Lossy Networks (LLNs), which include WSNs. [17].
- The Constrained RESTful Environments (CoRE) WG has the goal of defining a Constrained network Application Protocol (CoAP) for the manipulation of resources on a device [18].

2.4.3 ITU

The International Telecommunications Union (ITU) is the United Nations organisation responsible for issues related to information and communication technologies. ITU-T is the organisation in charge of telecommunications standards [19].

Figure 2.5: The International Telecommunications Union (ITU) logotype (extracted from [19]).

Ubiquitous Sensor Networks (USNs) were the focus of a ITU-T research aimed at identifying viable technologies for standardization work within the organisation [20]. On the other hand, the ITU released a technical paper on the applications of WSN in next generation networks [21].

2.4.4 ISO and IEC

The International Organisation for standardization (ISO) develops and publishes international standards on a wide range of topics. Organisations from both the public and private sectors are members of ISO [22]. Similarly to ISO, the International Electrotechnical Commission (IEC) is a non-profit global membership organization whose work supports quality infrastructure and international commerce in electrical and electronic products [23].

Figure 2.6: The International Organisation for standardization (ISO) and the International Electrotechnical Commission (IEC) logotypes (extracted from [22, 23]).

The ISO/IEC Joint Technical Committee (JTC) 1 was founded as a result of a merging of ISO and IEC organisations with the objective of focusing on information technology. In 2010, the JTC 1 Work

Group 7 was established to work on standardization in the areas of generic sensor network solutions and application-oriented sensor networks [24].

2.4.5 ETSI

Figure 2.7: The European Telecommunications Standards Institute (ETSI) logotype (extracted from [25]).

The European Telecommunications Standards Institute (ETSI) is one of the founding partners in *oneM2M*, a global standard initiative that covers requirements, architecture, API specifications, security solutions, and interoperability for M2M and IoT technologies. The number of connected devices is rapidly increasing (26 billion end 2020, 900 million five years ago) and it is expected to increase in the following years.

According to ETSI, oneM2M communication is present in eHealth,connected vehicles, home automation and energy management, public safety and industrial process control, and smart cities, which are applications that are commonly related to WSN [25].

2.4.6 Industry alliances efforts for standardization

There are multiple industrial alliances built around individual technologies that encourage the adoption of a certain technology as a *de facto* standard. The ZigBee Alliance, Bluetooth SIG, LoRa Alliance, WEIGHTLESS SIG, DASH7 Alliance are a few examples of such special interest groups (SIGs) or alliances that develop open standards.

2.4.7 LoRa Alliance

LoRa is a proprietary wireless RF technology that is also one of the driving forces behind the LoRa Alliance, which is working on the open LoRaWAN (Long Range Wide-Area Network) protocol and ecosystem. Since its establishment in 2015, the LoRa Alliance has grown to hundreds of members(Cisco, IBM, Actility, Sagemcom, Microchip Technology,Orange, KPN, Swisscom, SingTel, Proximus, and many others) [26].

Figure 2.8: LoRaWAN Alliance logotype (extracted from [26]).

The LoRaWAN open standard architecture was designed by the LoRa Alliance to provide a medium access control mechanism and allow End-Devices(ED) to connect with one or more gateways with the primary goal of enabling mainly uplink communication. As illustrated in Figure 2.9, LoRaWAN specifies

the data link layer protocol on top of the LoRa physical layer protocol. The LoRa protocol specifications are shown in Table 2.1 [27].

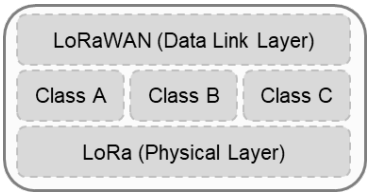


Figure 2.9: LoRaWAN protocol architecture.

LoRa is a physical layer technology that enables wireless communication over long distances with low data rates and low battery consumption. It operates in an unlicensed band technology that uses the spread spectrum approach to modulate signals in the sub-GHz ISM band. LoRa can also be used for peer-to-peer (P2P) communication between nodes [27] .

Table 2.1: LoRa protocol specifications.

Specification	**LoRa Technology Support**
Standard	LoRa Alliance
Operational Frequencies	Unlicensed ISM band 868 MHz, 915 MHz
Modulation	Chirp Spread Spectrum (CSS)
Coverage Range	2 km - 5 km (urban) / 15 km (rural)
Data Rate	0.3 - 50 kbps (EU) / 0.9 - 100 kbps (US)
Topology	Star

LoRa and LoRAWAN, as well as Sigfox, have *de facto* emerged as the primary non-cellular Low Power Wide Area(LPWA) ecosystems and solutions. However, LoRaWAN has the advantage of being an open alliance rather than a proprietary one, such as SigFox's proprietary strategy [9].

The LoRaWAN Alliance employs a star network topology and specifies three types of ED classes (Class A, Class B, Class C). Class A devices have very limited downlink capacity, with only one scheduled window available after each uplink transmission. Class B devices have more time slots for downlink communication, whereas class C devices have a substantially higher power consumption and perform continuous listening. Each class represents a trade off between battery life and downlink communication latency on the network. To authenticate end devices with the network and protect the privacy of application data, the LoRaWAN standard employs symmetric-key cryptography [9].

These classes have different capabilities that allow them to cover a wide range of applications as smart parking, smart waste management, smart metering, applications to remotely control connected devices at home, localisation, logistic applications, farming, and security applications. LoRa's focus on long range communication makes it unsuitable for many interior smart home appliances. It is, however, utilized, and it may be used for some smart home applications that require a distance element. Generally, for smart home applications where distance is less of an issue, it is typical to use other solutions, such as Bluetooth, or short distance home automation solutions such as ZigBee.

In 2021, the municipality of Lisbon will have a LoRa network. It will be an open and free network, accessible to companies and municipal services, but the same applies to the private sector, start-ups and universities. According to the Lisbon City Council, LoRa will be used for environmental monitoring

devices (noise, air, and water quality), intelligent irrigation of green spaces, meteorological data gathering, control of public lighting, parking space occupation on public roads, and waste container filling levels.In addition, LoRa will make it easier to locate civil protection teams, count bicycles, people, or vehicles, and operate security applications like intrusion detection or restricted access to facilities [28].

2.4.8 DASH7 Alliance

The DASH7 Alliance Protocol (D7AP) is an open standard protocol for wireless sensor and actuator communication that operates in the unlicensed SUB-GHz bands. It is developed and maintained by the DASH7 Alliance, an industry consortium established in 2009 [29]. D7AP is based on ISO18000-7, a specification for active radio frequency identification (Active RFID) used by the US Department of Defense. From ISO/IEC 18000-7, D7AP obtains the default settings of 433MHz active air interface connection, an asynchronous Media Access Control (MAC), and a presentation layer that exclusively utilizes highly organised data components. D7AP expands the functionality of the standard from RFID systems to WSN environments by making it a full stack , implementing the complete OSI model, that provides compatibility between different providers from the physical layer to the application layer [30].

Figure 2.10: DASH7 Alliance protocol logotype (extracted from [29]).

D7AP networks are built in a analogous manner to LoRaWAN networks, allowing users to create their own private network. D7AP networks, in addition to end devices and gateways, can include sub-controllers, which are capable of relaying communications between gateways and multiple end devices. Sub-controllers perform the same functions as gateways but use less power and have sleep cycles. Their primary function is to relay data from end devices to gateways. End devices/endpoints can also send and receive data from one another, and gateways can query endpoints' data. Endpoints can transmit data to the gateway at any moment (asynchronously) and must wake up on a regular basis to await downlink transmissions. Endpoints can either deliver data directly to a gateway or subcontroller, or they can transmit an all-cast or any-cast message and wait for acknowledgements from all or at least one gateway. D7AP can implement a tree topology alongside the more common star and star-of-stars topologies, due to the use of sub-controllers. All gateways communicate with a Network Server (NS), which performs administrative tasks such as data aggregation and handling duplicate communications [31] .

D7AP is built on the acronym *BLAST*, which stands for Bursty, Light, Asynchronous, Stealth, and Transitive. Bursty refers to sporadic data sequences with short time-on-air, whereas Light refers to the small data packets with maximum size of 256 bytes. Asynchronous as it is not necessary to synchronise on a regular basis, nor is it necessary for handshaking, devices only communicate when needed. DASH7 devices can choose to only reply to previously configured devices, as suggested by the term Stealth. Any other device's requests will be ignored. Furthermore, the nodes do not require any beaconing or

advertising. Finally, Transitive refers to the high mobility features in which nodes can freely migrate between different areas of the network's coverage(between different gateways) [31].

D7AP acts as an intermediary between the Short and Large Area Networks, thriving in urban and industrial network deployments with ranges up to 500 meters, connecting actuators and messaging applications (sensors, alarms, states) [29].

The D7A protocol is developed for 433 MHz, 868 MHz, and 915 MHz SUB-GHz ISM bands and it employs narrow band modulation scheme using two-level GFSK. Low, normal, or high communication modes are available, with data rates of 9.6 kbps, 55.555 kbps, and 166.667 kbps, respectively [31]. DASH7 can reach distances ranging from a few hundred meters to a few kilometers, depending on the speed and band, and it offers low latency with multiyear battery life. DASH7 establishes distinct channels for each band and it is frequency-agile. Devices can be configured to scan for messages through more than one channel [32]. Forward error correction and symmetric key cryptography are both supported by DASH7 [9]. The DASH7 wireless specifications are described in Table 2.2 [27].

Table 2.2: DASH7 protocol specifications.

Specification	**DASH7 Technology Support**
Standard	Inherited ISO/IEC 18000-7
Operational Frequencies	Unlicensed ISM band 433MHz, 868MHz, 915MHz
Modulation	2-GFSK
Coverage Range	1 km - 2 km (rural/urban)
Data Rate	9.6 kbps(Low), 55.555 kbps(Normal), 166.667 kbps(High)
Topology	Tree, Star

2.4.9 Weightless Special Interest Group

The Weightless Special Interest Group (Weightless SIG), which was established in 2012, is a non-profit organisation that develops and maintains a group of standards that were initially intended to encourage LPWAN communications in TV white space (TVWS) [33]. Among the founding members of the Weightless-SIG are: Accenture, ARM, M2COMM, Sony-Europe, and Telensa [34].

Figure 2.11: Weightless Special Interest Group logotype (extracted from [35]).

Weightless SIG has established three separate open standards, as shown in Table 2.3, each with different technical capabilities [31, 36]:

- *Weightless-W* uses TV white space(TVWS), operating in the 470-790 MHz band, with a variety of different modulation schemes, data rates and bidirectional communication [33]. However, Weightless-W is unavailable in many regions of the world, due to regional regulations and spectrum allocation of TVWS, because of this lack of prospective market share the development of Weightless-W was ceased before 2005. Nevertheless, this standard in the smart oil and gas sector, where TVWS is likely to be available, has a lot of potential [33]. Weightless-W follows a star

Table 2.3: Weightless protocols specifications.

Specification	**Weightless Technology Support**		
Standard	Wheightless-W	Wheightless-N	Wheightless-P
Operational Frequencies	TVWS 470-790 MHz	ISM SUB-GHz EU (868 MHz), US (915 MHz)	SUB-GHz ISM or licensed
Modulation	16-QAM, BPSK, QPSK, DBPSK	UNB DBPSK	GMSK, offset-QPSK
Coverage Range	5 km (urban)	3 km (urban)	2-5 km (urban)
Data Rate	1 kbps-10 Mbps	30 kbps-100 kbps	200 bps-100 kbps
Topology	star	star	star

topology and offers a solution with a very high data rate, if TVWS is available [31].

- *Weightless-N* is the second standard developed, with the majority of the hardware being developed by an organisation named NWave. Weightless-N uses the ISM band rather than the TVWS band and has no downlink capabilities. Weightless-N was ultimately unsuccessful, and ETSI was granted responsibility for the standard [31]. The failure of this standard is largely attributed to an unbalanced link budget and the need for a Temperature Compensated Crystal Oscillator (TCXO) component [33] .

- *Weightless-P* is the most recent standard from Weightless SIG, launched in 2016, it was designed for low data rate networks in the sub 1GHz ISM bands and it fully supports downlink communications [37]. Weightless-P splits the spectrum into 12.5 kHz channels. Flexible channel assignment, adaptive data rates, and time-synchronised base stations provide optimal spectrum use.

  Weightless-P's encryption is performed using AES-128 bits keys, and message integrity is ensured using a 32-bit long Message Integrity Code (MIC) calculated using AES 128 bits keys [38]. Weightless-P topology is a star, constituted of End Devices(EDs) and Base Stations (BSs). End devices are simpler, less costly, and have a lower duty cycle than BSs. To form a cell, all EDs communicate with a single BS, and BSs are connected via a network known as the Base Station Network (BSN) [35]. Resource allocation, scheduling, roaming, and security are all managed by the BSN. The architecture of Weightless-P is significantly influenced by LTE. The mobility feature of Weightless-P is comparable to that of LTE, since it supports handover, roaming, and cell re-selection [31].

  On the physical layer, the use of GMSK modulation in Weightless-P eliminates the need for the problematic TCXO device, resolving one of the main obstacles of Weightless-N. Furthermore, Weighless-P uses GMSK and QPSK modulation, which are superior to Weightless-N's modulation with DBPSK. However, QPSK has a greater error rate and requires more power to reduce it, and using GMSK reduces Weightless-P's effective range, potentially making it less appropriate for usage in WANs [31]. In an urban context, depending on density, Weightless-P has a range of 2-5 km, whereas in a rural area, it has a range of approximately 25 km [31].

  Weightless-P enables organisations to establish private networks while maintaining total ownership of the infrastructure, assuring network exclusivity [33]. This protocol could be applied, for example,

to smart metering, industrial machine monitoring and traffic sensors. Ubiik, a Taiwanese company, has promoted the technology and is now the primary manufacturer and distributor of Weightless-P solutions [39].

2.4.10 ZigBee Alliance

The ZigBee Alliance is a non-profit organisation that manages and develops the ZigBee open standard. The alliance was established in 2002 and is currently formed by more than 450 companies [40].

Figure 2.12: ZigBee Alliance logotype (extracted from [12]).

The ZigBee standard is a set of high level communication protocols that use low power radios based on IEEE 802.15.4 and operates in the unlicensed bands of 2.4 GHz, 900 MHz, and 868 MHz. At 2.4GHz (16 channels), raw data throughput rates of 250Kbs are possible, 10Kbs at 915–921Mhz (27 channels), and 100Kbs at 868Mhz (63 channel). Depending on the power output and environmental conditions, transmission distances range from 10 to 100 meters. The transmission range of sub GHz channels is up to 1km [41]. The ZigBee network can be configured as a tree, star, or mesh topology.

ZigBee is ideal for network RF applications that require low data rates, low power and security. Zigbee is a protocol best known for connecting smart devices such as lights, plugs, and smart locks to a home network. The ZigBee protocol specification is shown in Table 2.4 [41]. In Chapter 3.1, Zigbee will be explained in further detail.

Table 2.4: ZigBee protocol specification.

Specification	**ZigBee Technology Support**
Standard	ZigBee PRO Specification
Operational Frequencies	Unlicensed ISM Band 2.4 GHz, 868(Europe)/915(Americas) MHz
Modulation	BPSK/ O-QPSK
Coverage Range	10 - 100 m
Data Rate	10 kbps - 250 kbps
Topology	Star, Tree, Mesh

2.4.11 Bluetooth Special Interest Group

Bluetooth Special Interest Group (SIG) is a non-profit organisation, established in 1998, which has currently a global community of over 36.000 companies. The Bluetooth SIG's primary responsibilities include the publication of Bluetooth specifications as well as the protection and promotion of Bluetooth technology [42].

Figure 2.13: Bluetooth Special Interest Group logotype (extracted from [42]).

Bluetooth specifications are classified into two types: Bluetooth classic and Bluetooth Low Energy (BLE). The Bluetooth Classic, also known as Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR), is a low power radio that transmits data via 79 channels in the unlicensed 2.4GHz ISM frequency band. Bluetooth Classic is the standard radio protocol used by wireless speakers, headphones, and in-car entertainment systems. It allows for device-to-device communication. [43].

Unlike Bluetooth Classic, BLE is designed for short range wireless communication with a focus on low data rate, energy constrained applications. BLE's purpose, in addition to being low power, is to enable the development of low cost, simplified radio transceivers for applications that are both cost and resource (i.e. memory) constrained.

The BLE, like ZigBee, uses the 2.4 GHz ISM band to transmit. It provides a maximum data throughput of 2 Mbps and it has 40 channels with 2 MHz spacing. To avoid interference from other devices, the BLE employs frequency hopping. Unlike classic Bluetooth, BLE devices, on the other hand, run at the same frequency over longer periods of time to simplify timing requirements [44]. BLE offers a variety of network topologies, including point-to-point, broadcast, and, most recently, mesh, allowing Bluetooth to support the development of reliable, large scale device networks [43].

BLE is suited for several WSN applications, such as building automation, health care, home automation, agriculture and smart cities [42]. BLE can also be used in applications that require direct communication between the device and a smartphone. The Bluetooth protocols specifications are shown in Table 2.5 [43]. In Chapter 4.1, BLE will be discussed in further detail.

Table 2.5: Bluetooth protocols specifications.

Specification	**Bluetooth Technology Support**	
Standard	Bluetooth Low Energy (BLE)	Bluetooth Classic
Operational Frequencies	Unlicensed ISM Band 2.4 GHz	Unlicensed ISM Band 2.4 GHz
Modulation	GFSK	GFSK, $\pi/4$DQPSK, 8DPSK
Coverage Range	10 - 400 m	1 - 100 m
Data Rate	125 kbps - 2 Mbps	1 Mbps - 3 Mbps
Topology	Point-to-Point, Broadcast, Multicast	Point-to-Point(including piconet)

Chapter 3

The Zigbee Standard Protocol

3.1 ZigBee Introduction

ZigBee is an open global standard that defines a set of communication protocols for low power consumption, low cost implementation, short range and low data rate communication, which also supports mesh networking and multihopping [45]. One of the key features of the ZigBee standard is its mesh networking capability, a message is relayed from one device to another until it finally reaches its distant destination. For this reason, this standard gets its name due to the similarity of the specific zigzag dance a bee performs to spread a message to reach its hive. A bee performs a zigzag dance, which is then repeated by the next bee that is slightly closer to the hive, until the message is delivered to the hive. Thus, the metaphor for the way devices on the network find and interact with each other and the name of the standard ZigBee [46].

Figure 3.1: ZigBee's standard protocol logotype (extracted from [40]).

ZigBee is primarily designed for battery powered applications that demand a low data rate, low cost, and long battery life. In certain ZigBee applications, the total time the wireless device is engaged in any type of activity is relatively low. The device spends the majority of its time in a power saving mode referred to as sleep mode.Many ZigBee applications use devices with duty cycles of less than 1% ensuring years of battery life. As a result, ZigBee-enabled devices can run for several years without needing to be replaced.

The ZigBee specification is developed by a consortium of more than 450 companies from the semiconductor industry to software developers (some relevant members are in Figure 3.2, like Google, Huawei, Legrand, Samsung SmartThings, and Amazon) that integrate the ZigBee Alliance, which was established in 2002 as a non-profit organisation [47].

Figure 3.2: Most relevant members of the ZigBee Alliance (extracted from [40]) .

3.2 Architecture

The concept of networking layers is one of the most common techniques to set up a communication network. Each layer oversees a specific function in the network. Data and commands are generally passed exclusively to the layers directly above and below them. There are several advantages to layering a network protocol. For example, if a protocol suffers changes over time, rather than updating the entire protocol, it is simpler to replace or modify the layer that is affected by the change.

The ZigBee stack architecture is based on the Open System Interconnect (OSI) and it is built on top of the IEEE 802.15.4 standard, which defines the two lower layers of the protocol stack, the Physical Layer (PHY) and the Medium Access Control (MAC) protocols. The IEEE 802 standards Committee created this standard, which was first issued in 2003. Therefore, a ZigBee compliant device also complies with the IEEE 802.15.4 standard. In comparison with other standards such as IEEE 802.11, the minimum requirements to fulfil ZigBee and IEEE 802.15.4 specifications are significantly simplified, which minimizes the complexity and expenses of installing ZigBee compliant transceivers.

On the other hand, the ZigBee Alliance develops the upper layers of the protocol stack, by providing the Network layer (NWK) and the framework for the Application layer (APL), that enable interoperable data networking and security services [45]. Figure 3.3 illustrates the layered architecture of the ZigBee protocol stack.

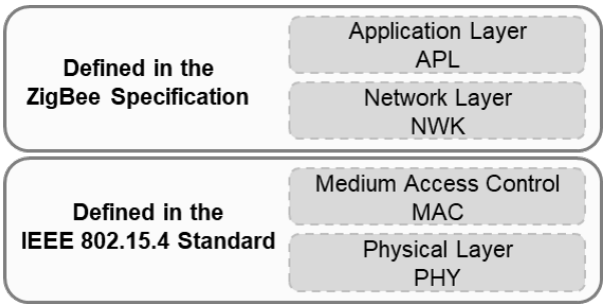


Figure 3.3: Outline of the ZigBee stack architecture.

3.3 Other aspects of ZigBee

3.3.1 The Network Layer

The network layer (NWK), which stands between the MAC and the APL, is responsible for managing the network formation and routing. Routing is the process of selecting the path the message will take to reach its intended recipient. The coordinator and routers of the ZigBee network are in charge of identifying and maintaining the network's routes. Route finding is not possible with a ZigBee end device. The ZigBee coordinator or a router will do route finding on behalf of the end device. A ZigBee coordinator's NWK layer is responsible for constituting a new network and selecting the network topology (Tree, Star, or Mesh). The NWK addresses are also assigned by the ZigBee coordinator to the devices in its network [47].

IEEE 802.15.4 and ZigBee Device Types

According to IEEE 802.15.4 standard, there are two different types of devices [48]: *Full-Function Devices (FFD)* and *Reduced-Function Devices (RFD)*. An FFD is prepared to fulfill all of the functions described in the IEEE 802.15.4 standard and may play any role in the network, it can operate in three different modes:

- A *Personal Area Network (PAN) Coordinator* is the primary controller of a personal area network. This device establishes its own network, which other devices can join.

- A *Coordinator*, which provides synchronisation services through the transmission of beacons. This type of coordinator must be linked to a PAN coordinator and is not capable of creating its own network.

- A simple *Device*: it is simply referred to as a device if it is not operating as a coordinator.

An RFD has limited capabilities, as it only implements the IEEE 802.15.4 protocol in its most basic form. It can only connect with FFD devices, but FFD devices can communicate with any other device on the network. An RFD is intended for fairly simplistic applications, such as a light switch or a passive infrared sensor, that do not require a large quantity of data to be sent. Furthermore, they can only associate with a single FFD at a time. In a network, at least one FFD must serve as a PAN coordinator, providing global synchronisation services to the network and managing potential FFDs and RFDs [49].

A slightly different terminology is applied by the ZigBee standard, as shown in Figure 3.4. A ZigBee coordinator is an IEEE 802.15.4 PAN coordinator. A ZigBee router is a device capable of acting as an IEEE 802.15.4 coordinator. Finally, a ZigBee end device does not serve as a coordinator or router. It is essentially a device with the smallest amount of memory and the fewest processing capabilities and features. Therefore, an end device is often the most affordable device in the network.

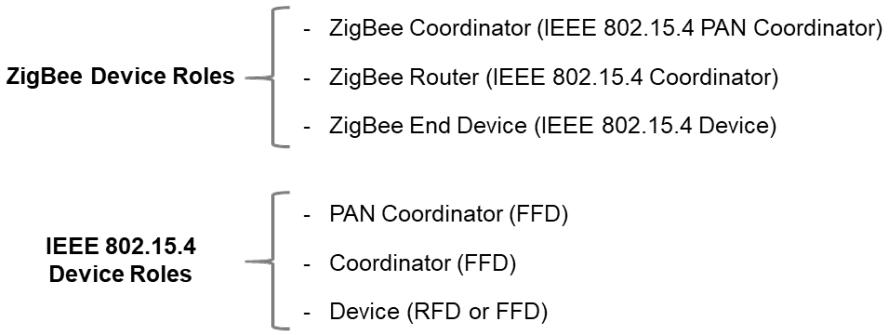


Figure 3.4: IEEE 802.15.4 and ZigBee device types.

3.3.2 Network Topologies

The ZigBee NWK layer is responsible for the network formation. Depending on the networking requirements of the application, the IEEE 802.15.4 standard defines two basic types of network topologies: the *star topology* and the *peer-to-peer topology*. The *cluster-tree topology* is a third form of topology, it may be regarded as a special case of peer-to-peer topology.

3.3.3 The Star Topology

The star network formation is illustrated in Figure 3.5. This topology has a single node that acts as a PAN coordinator. For example, if an FFD is active, it may create its own network and become the PAN coordinator.

The PAN coordinator selects a unique PAN identity that no other network in its radio sphere of influence (the area around the device in which its radio may successfully communicate with other radios) has used [50].

The communication paradigm is the star topology is centralised, which means that each device (FFD or RFD) that joins the network and wishes to communicate with other devices must transmit its data to the PAN coordinator, who will route them to the appropriate destination devices.

The IEEE 802.15.4 standard specifies that the PAN coordinator may be connected to a main supply, whereas other devices are more likely to be battery powered, due to the power-consuming tasks of the PAN coordinator in the star topology.

Consequently, the star topology appears to be insufficient for standard wireless sensor networks, as all sensor nodes are battery powered and hence energy constrained. The battery resources of a sensor node designated as a PAN coordinator would be quickly depleted.

A dynamic PAN coordinator based on the remaining battery supplies in sensor nodes, such as the LEACH protocol [50], could be used to avoid this issue. However, because the dynamic election of a PAN coordinator among a big number of sensor nodes is not practical, this approach appears to be rather difficult [51].

Taking these concerns into account, the IEEE 802.15.4 standard suggests the star topology for applications like home automation, personal computer peripherals, toys, and games [48].

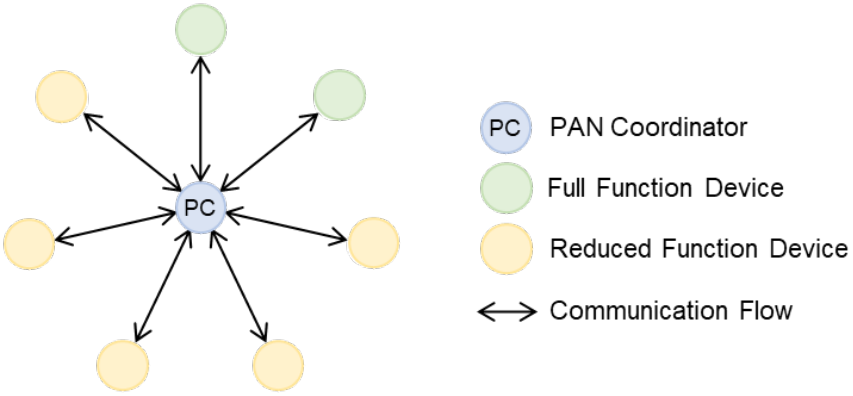


Figure 3.5: Star topology model.

3.3.4 The Peer-to-Peer Topology

The Peer-To-Peer network formation is illustrated in Figure 3.6. Similarly to the star topology, a PAN coordinator is included in the peer-to-peer topology, which is nominated, for example, due to the fact that it was the first FFD device to communicate on the channel.

The communication paradigm in a peer-to-peer topology, on the other hand, is decentralised, where each device can directly communicate with any other device within its radio sphere of influence. A peer-to-peer network can take various shapes depending on the devices that can communicate with each other. A mesh topology refers to a peer-to-peer network that has no restrictions [52].

This mesh topology provides greater networking flexibility. However, it adds more complexity by providing end-to-end connectivity between all devices in the network. Essentially, the peer-to-peer topology operates in an ad hoc wireless network, which allows multiple hops to forward data from any device to any other device on the network. Nonetheless, such functions can be added at the network layer, but they are not part of the IEEE 802.15.4 specification [48].

One of the applications that could benefit from such a topology are wireless sensor networks. The resource usage in the peer-to-peer topology is better distributed than in the star topology because the communication process is not dependent on a single node.

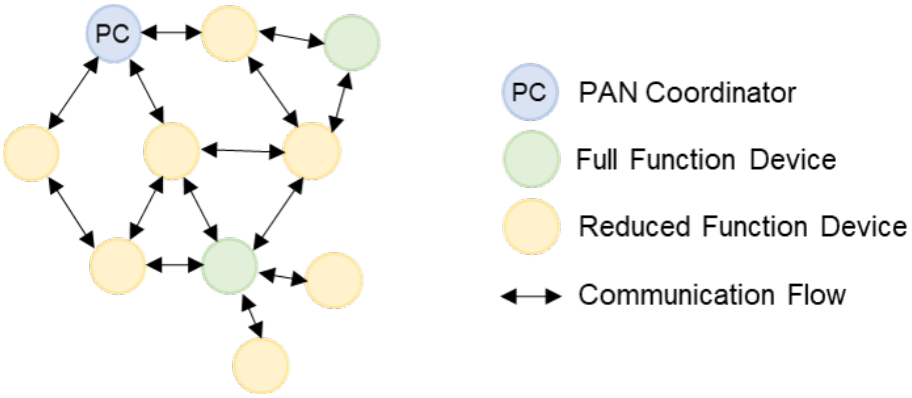


Figure 3.6: Peer-to-Peer topology model.

3.3.5 The Cluster-Tree Topology

The Cluster-Tree network is a type of peer-to-peer network in which most of the devices are FFDs. In this topology, one (and only one) coordinator is selected as the PAN coordinator, which identifies the entire network, potentially because it has greater computational resources than any other device in the PAN. Any FFD can function as a coordinator, synchronising with other devices or coordinators. Since RFDs do not allow other devices to associate with them, they connect to a cluster tree as a leave node at the end of a branch.

The following steps may be performed to build a cluster tree [52]:

- The PAN coordinator forms the first cluster, cluster head (CLH), by selecting an unused PAN identifier and broadcasting beacon frames to the nearby devices. If two or more FFDs attempt to establish themselves as PAN coordinators at the same time, a contention resolution mechanism is required, however, such a mechanism is not defined in IEEE 802.15.4 specification.
- A candidate device that receives a beacon frame may contact the PAN coordinator and request to join the network to the CLH.
  - If the PAN coordinator accepts the device to join the network, the new device is added to the neighbour list as a child device. In turn, the newly joined device then adds the PAN coordinator to its neighbour list as its parent and starts transmitting periodic beacons, allowing other devices to hear these beacons to join the network at this device.
  - If for some reason the original candidate device is unable to join the network at the cluster head, it will search for another parent device.

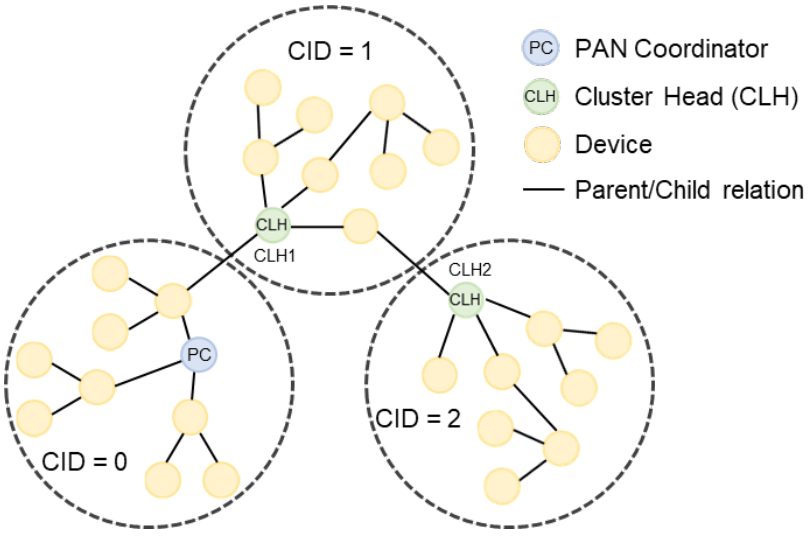


Figure 3.7: Cluster-Tree topology model.

A mesh of multiple neighbouring clusters can be created for a large scale network. In this instance, the PAN coordinator can upgrade a device to serve as the CLH of a new cluster that will be added to the existing one.

For a large scale network, it is possible to form a mesh of multiple neighbouring clusters. In such a situation, the first PAN coordinator instructs a device to become the PAN coordinator of a new cluster, therefore, this device will become the CLH of a new cluster adjacent to the first one. As additional devices join, a multicluster network topology forms, as seen in Figure 3.7. A multicluster structure has the advantage of expanding the coverage area. However, it also increases message latency.

Self-Forming and Self-Healing characteristics of ZigBee

A ZigBee network begins to form as soon as the devices become active, as explained in Section 3.3.3. The first FFD device to connect in a mesh network becomes the ZigBee coordinator, and subsequent devices can join the network by submitting association requests. ZigBee networks are referred to as *self-forming* networks since they do not require any additional supervision to be established.

When a mesh network is formed, on the other hand, there is usually more than one option to transmit a message from one device to another. Normally, the communication is routed in the most efficient manner possible. Nevertheless, the network can choose an alternative way if one of the routers stops working, due to battery exhaustion or if an obstruction interrupts the message route. This is an example of ZigBee mesh networking's self-healing capability [50].

3.3.6 The Application layer

The Application layer (APL) is the top protocol layer in a ZigBee wireless network, where the application objects are hosted. Application objects are developed by manufacturers to customise a device for a variety of uses. A ZigBee device's protocol layers are controlled and managed by application objects.

The ZigBee standard provides the option of using application profiles, which are a set of agreements on application specific message formats and processing actions, to develop an application. The adoption of an application profile allows interoperability across solutions built by different vendors for a specific application. When two vendors use the same application profile to produce their goods, the product from one vendor can interact with the product from the other vendor, as if they were both made by the same vendor. Interoperability is one of the main advantages of the ZigBee protocol stack [50].

3.4 The Physical layer

The first and lowest layer is the Physical layer (PHY). It is responsible for data transmission and reception using a certain radio channel and according to a specific modulation and spreading technique [45].

As mentioned before, ZigBee's PHY is defined in the IEEE 802.15.4 standard. PHY data service and PHY management service are the two services provided by the PHY.

The PHY management service is responsible for the following features [48]:

- The radio transceiver's activation and deactivation

- Within the present channel, energy detection (ED) is used.
- For received packets, the link quality indicator (LQI).
- Clear channel assessment (CCA) for carrier sense multiple access with collision avoidance (CSMA-CA)
- Channel frequency selection
- Data transmission and reception
- Precision ranging for ultra-wide band (UWB) PHYs

The PHY data service is responsible for the transmission and reception of *the physical protocol data units* (PPDUs) across the physical radio channel.

PPDU format

The PHY protocol data unit (PPDU) structure is provided in such a way that the leftmost field is sent or received first, as stated in this standard. The least significant octet of all multiple octet fields must be transmitted or received first and within each octet, the least significant bit (LSB), $b0$, is processed first and the most significant bit (MSB), $b7$, is processed last [48].

In Figure 3.8, it is illustrated the format of the PPDU used in both modulations.

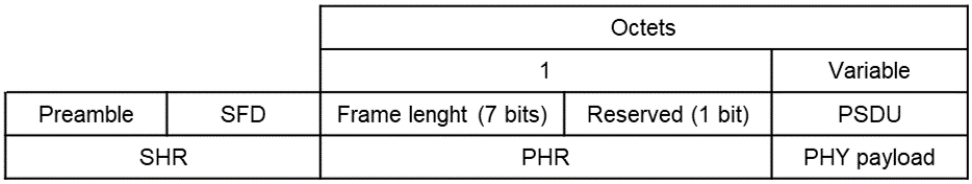


Figure 3.8: Format of the PPDU of IEEE 802.15.4 standard.

Preamble Field

For O-QPSK PHYs, the preamble must be *8 symbols* (i.e., 4 octets), with binary zeros in the Preamble field, while for BPSK PHYs the preamble is *32 symbols* (4 octets).

SFD field

The *Start Frame Delimiter* (SFD field) indicates the end of the *Synchronisation Header* (SHR), and the start of the packet data. The SFD must be formatted as shown in Table 3.1.

Table 3.1: Format of the SFD field of IEEE 802.15.4 standard.

Bits: 0	1	2	3	4	5	6	7
1	1	1	0	0	1	0	1

Frame Length field

Inside the PHY header (PHR), the *Frame Length field* indicates the total number of octets contained in the physical layer service data unit, PSDU, (i.e., PHY payload). It is a value between 0 and 127. Table 3.2 summarises the type of payload versus the frame length value.

Table 3.2: Frame length values of IEEE 802.15.4 standard.

Frame length values	Payload
0-4	Reserved
5	MPDU(Acknowledgment)
6-8	Reserved
9 to aMaxPHYPacketSize	MPDU

3.4.1 Frequency of Operation

This standard specifies operation in the license free spectrum of 2400-2483.5 MHz (2.4 GHz band, used worldwide), 902-928 MHz (915 MHz band, used mainly in North America) and 868-868.6MHz (868 MHz band, covering Europe), which are radio spectrum segments set aside for ISM [53].

The ISM band is an unlicensed spectrum that may be used by virtually any device as long as it conforms to the spectrum restrictions specified by the International Telecommunication Union's Radio Regulations (ITU) [54].

A transceiver that supports the 868 MHz band must also support the 915 MHz band, according to IEEE 802.15.4, and vice versa [48]. As a result, the 868/915 MHz frequency bands of operation are always grouped together.

Furthermore, for channel page zero there is a single channel available between 868-868.6 MHz, 10 channels are available between 902-928 MHz, spaced 2 MHz apart, and 16 channels are available between 2.4-2.4835 GHz, spaced 5 MHz apart, although using only 2 MHz of bandwidth each as shown in Figure 3.9.

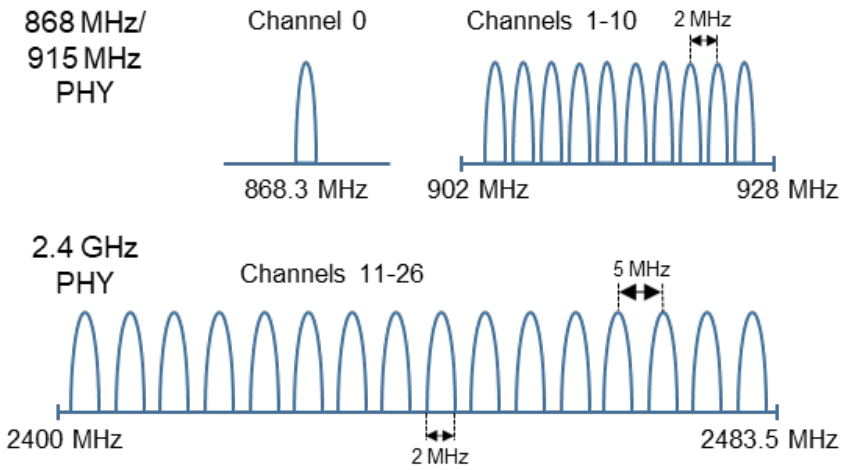


Figure 3.9: ZigBee's operating frequency bands.

The centre frequency of these channels is defined as follows [48]:

F_c = 868.3 in megahertz, for k = 0

F_c = 906 + 2 (k – 1) in megahertz, for k = 1, 2, . . . , 10

F_c = 2405 + 5 (k – 11) in megahertz, for k = 11, 12, . . . , 26

,where k is the channel number

3.4.2 Modulation

O-QPSK PHY

• Operating in the 2450MHz band :

It applies *direct sequence spread spectrum* (DSSS) PHY employing *offset quadrature phase-shift keying* (O-QPSK) modulation. The data rate shall be 250 kb/s and the symbol rate 62.5 ksymbol/s.

This modulation uses a 16-ary quasi-orthogonal modulation technique. For each data symbol period, four information bits are used to choose 1 of 16 nearly orthogonal pseudo-random noise (PN) sequences to be transmitted. The PN sequences for subsequent data symbols are concatenated, and O-QPSK modulates the resultant chip sequence into the carrier.

Figure 3.10 shows a functional block diagram for describing the O-QPSK PHY modulation and spreading functions as a reference.

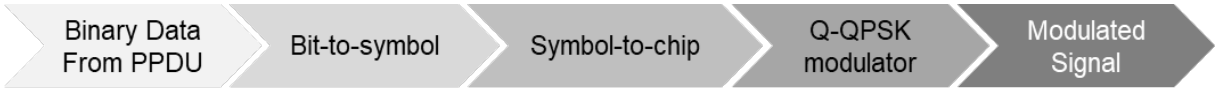


Figure 3.10: O-QPSK PHY modulation and IEEE 802.15.4 standard spreading functionalities.

BPSK PHY

• Working in the 868 MHz, 915 MHz bands:

It employs DSSS in conjunction with binary phase-shift keying (BPSK) for chip modulation and differential encoding for data symbol encoding. For the frequency bands of 868 MHz, 915 MHz the data rate shall be respectively, 20 kb/s and 40 kb/s, and the symbol rate shall be, respectively, 20 ksymbol/s and 40 ksymbol/s.

Each bit in the PPDU must be processed in octet-wise sequence, beginning with the preamble field and finishing with the last octet of the PSDU, using differential encoding, bit-to-chip mapping, and modulation operations. Within each octet, the LSB, b0, is processed first, followed by the MSB, b7.

A functional block diagram is shown in Figure 3.11 as a basis for describing the BPSK PHY modulation and spreading functions.

Figure 3.11: BPSK PHY modulation and spreading functions of IEEE 802.15.4 standard.

The parameters of each frequency band are summarised in Table 3.3.

Table 3.3: Frequency bands and data rates of ZigBee.

PHY [MHz]	Frequency Band [MHz]	Spreading parameteres		Data parameteres		
		Chip rate [kchip/s]	Modulation	Bit rate [kb/s]	Symbol rate [ksymbol/s]	Symbols
868/915	868-868.6	300	BPSK	20	20	Binary
	902-928	600	BPSK	40	40	Binary
2450 DSSS	2400-2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

In general, all of these frequency bands are based on DSSS. DSSS is used to increase the frequency of the signal in order to increase its power and minimise the influence of noise from nearby networks and improve the performance of receivers in a multipath environment. The digital data in BPSK and O-QPSK is in phase with the signal.

The actual data throughput will be less than the maximum specified bit rate due to the packet overhead and processing delays. Additionally, lower frequencies are more appropriate for longer transmission ranges due to lower propagation losses. Furthermore, a higher bit rate allows higher throughput and lower latency, while low rate transmissions provide better sensitivity and a bigger coverage area. Hence, a frequency band might be more appropriate than another depending on the application and the different variables considered.

The PHY packet general structure

Packets are used to communicate data and orders between different devices. Figure 3.12 depicts the overall structure of a packet. The PHY packet is constituted by three components: the Synchronisation header (SHR), the PHY header (PHR), and the PHY payload [50].

The SHR allows the receiver to lock and synchronise with the bit stream. The PHY payload is delivered by the upper layers and it contains data or commands for the recipient device. The PHR

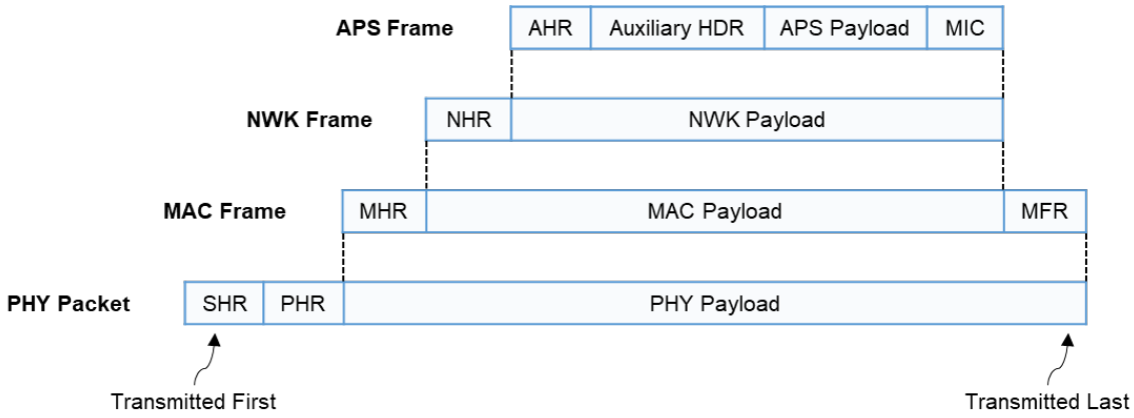


Figure 3.12: ZigBee's packet structure.

provides frame length information.

The MAC frame consists of three components, which are sent to other devices as a PHY payload. The MAC header (MHR) carries addressing and security information. The MAC payload consists of commands or data and has a variable length (including zero length). A 16-bit Frame Check Sequence (FCS) is included in the MAC footer (MFR) for data verification.

The NWK header (NHR) and the NWK payload are the two sections of the NWK frame. The NWK header has network level addressing and control information. The APS sublayer provides the NWK payload.

Application layer control and addressing information are present in the APS header (AHR), in the application support sublayer (APS) frame. The auxiliary frame header (auxiliary HDR) comprises the mechanism and security keys required to add security to the frame. These security keys are exchanged among the associated devices and help in the unlocking of information. Auxiliary headers can be added to the NWK and MAC frames for added security.

In the APS payload, there are data or commands. The Message Integrity Code (MIC) is a security feature of the APS frame that detects any unauthorized changes to the message's content [50].

The least significant bit (LSB) of the SHR is the first transmitted bit, and the most significant bit (MSB) of the last octet of the PHY payload is transmitted last, as shown in Figure 3.12.

3.5 The MAC Layer

The Medium Access Control (MAC) layer serves as an interface between the PHY and NWK layers. The IEEE 802.15.4 standard defines the MAC layer, which controls communication channel access and offers flow control via acknowledgements and retransmissions. It controls the access to the radio channel using the CSMA-CA mechanism. If the upper layers detect that the communications throughput has decreased below a specific threshold, the MAC sublayer will be ordered to run an energy detection scan of the available channels. Based on the measured energy, the top layers will change to the channel with the lowest energy. The energy scan is implemented by the IEEE 802.15.4 using a clear channel

assessment procedure. This can be done using a basic in band energy detection exceeding a threshold, IEEE 802.15.4 carrier detection, or a combination of the two.

Moreover, MAC layer is responsible for generating beacons and synchronising the device with beacons (in a beacon-enabled network), controlling the association, administering device security, and designing the guaranteed time slot mechanism, as well as flow control via acknowledged frame delivery and frame validation [55].

The difference between Beacon-Enabled and Nonbeacon Networking

There are two different approaches for channel access: *contention based* or *contention free* [50]. In the *contention based* channel access technique, all devices that wish to transmit in the same frequency channel employ the CSMA-CA mechanism , and the first device that detects that the channel is clear may begin start transmitting. In the contention free approach, the PAN coordinator assigns a specific time slot to each device. This is referred to as a *guaranteed time slot* (GTS). As a result, a device with an assigned GTS will begin transmitting during that GTS, without employing the CSMA-CA mechanism.

The PAN coordinator must guarantee that all devices in the network are synchronised, in order to offer a GTS. The term "*beacon*" refers to a message with a specified format that is used to synchronise the clocks of the network nodes [56]. In section 3.5.2, the format of the beacon frame is described. A coordinator may send beacon signals to synchronise the devices to which it is connected. This process is referred to as a beacon-enabled PAN. The drawback of using beacons is that all devices in the network must periodically wake up, listen for the beacon, synchronise their clocks, and then go back to sleep. This implies that many of the network's devices may only wake up for synchronisation and will not conduct any other tasks while active. Consequently, a device's battery life in a beacon-enabled network is frequently shorter than one that is in a network without beaconing.

A *nonbeacon* network is defined as one in which the PAN coordinator does not broadcast beacons. Owing to the fact that the devices cannot be synchronised with each other, a nonbeacon network cannot have GTSs and hence contention free periods. The battery life in a nonbeacon network can be significantly greater than in a beacon-enabled network, due to the fact that the devices wake up less frequently in a nonbeacon network.

3.5.1 Methods of Data Transfer

In IEEE 802.15.4, there are three methods of data transfer [48, 50]:

- Transfer of data from a Device to a Coordinator.
- Transfer of data from a Coordinator to a Device.
- Transfer of data between two peer Devices.

In a peer-to-peer topology, all three techniques can be employed. Only the first two are utilised in a star topology since no direct peer-to-peer connection is permitted.

A packet is a group of bits that are sent in a specific order, therefore a receiver must have a mechanism to check whether any of the bits received were recovered incorrectly. To identify potential faults in data packets, IEEE 802.15.4 employs a 16-bit Frame Check Sequence (FCS) based on the International Telecommunication Union's (ITU) Cyclic Redundancy Check (CRC).

Transfer of data from a Device to a Coordinator

When a device in a beacon-enabled network wishes to transmit data to the coordinator, it synchronises its clock on a regular basis and uses the CSMA-CA mechanism to transmit data (assuming that the transmission does not occur during a GTS). Only if the data transmitter specifically requests it, the coordinator may acknowledge receipt of the data. Figure 3.13 (a) illustrates the sequence diagram.

Figure 3.13 (b) depicts the data transfer sequence in a network without beacons. In this circumstance, the device transmits data as quickly as the channel is clear. It is optional for the PAN coordinator to send an acknowledgment.

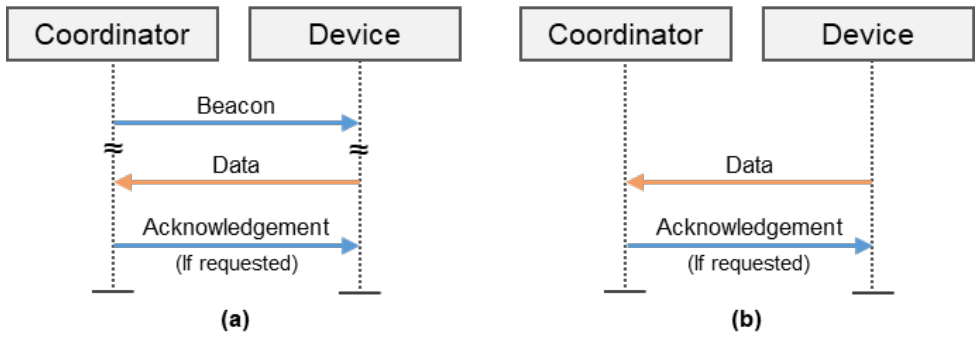


Figure 3.13: Data transfer between a Device to a Coordinator, in IEEE 802.15.4.: **(a)** Beacon Enabled, and **(b)** Nonbeacon Enabled

Transfer of data from a Coordinator to a Device

Figure 3.14 (a) depicts the data transfer steps in a beacon-enabled network from a coordinator to a device. If the coordinator wishes to transfer data to a specific device, it will notify that a data message is pending for that device in its beacon message. Afterwards, the device sends a data request message to the coordinator, stating that it is active and prepared to receive the data. The coordinator confirms that the data request has been received and transmits the data to the device. It is optional for the device to send the acknowledgement.

In the situation of a network without beacons, the coordinator must wait for the device to request data, as illustrated in Figure 3.14 (b). If a device requests data but at that current time there is no data pending for it, the coordinator sends an acknowledgment message with a particular format stating that no data is waiting for that device. As an alternative, the coordinator can transmit a zero-length payload data message.

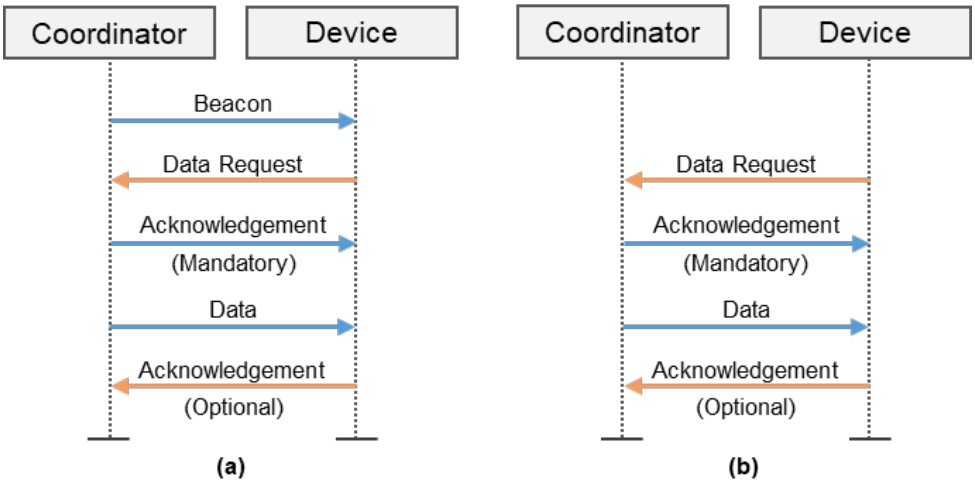


Figure 3.14: Transfer of data from a Coordinator to a Device: **(a)** Beacon Enabled, and **(b)** Nonbeacon Enabled

Transfer of data between two peer Devices

Each device in a peer-to-peer topology may communicate with any other device directly. The devices involved in peer-to-peer data transfers and receptions are often synchronised in various applications.

Addressing in IEEE 802.15.4

In IEEE 802.15.4 there are two different methods of addressing: *16-bit short addressing* or *64-bit extended addressing*. Either 16-bit or 64-bit addressing can be used in a network. Within a single network, the short address facilitates communication. Using the short addressing method reduces the length of messages and reduces the amount of memory space needed.

The possibility of 64-bit addressing, allows a network's maximum number of devices to be 2^{64}, or approximately 1.8×10^{19}. As a result, the number of devices that may join an IEEE 802.15.4 wireless network is essentially limitless.

Additionally to the IEEE address, the ZigBee protocol's Network (NWK) layer allocates a 16-bit NWK address. Each 64-bit IEEE address is mapped to a unique NWK address using a simple lookup table. The NWK address is required for NWK layer transactions. A single IEEE address and a single NWK address can be assigned to every radio inside a network. However, a single radio may support up to 240 devices. The *endpoint* address is a number between 1 and 240 that identifies each of these devices [50].

3.5.2 Frame Structures for MAC

IEEE 802.15.4 defines four MAC frame structures [48, 49] :

- **Beacon frame**: This frame is used by a coordinator to transmit beacons, which are used to synchronise all devices within the same network.

- **Data frame**: This frame is used to transmit data.
- **Acknowledge frame**: This frame is used to acknowledge when a frame is successfully received.
- **MAC command frame**: This frame is used to transmit MAC commands.

Beacon frame

In Figure 3.15 the construction of a beacon frame is depicted. The whole MAC frame is utilized as the payload of a PHY packet. The PHY Service Data Unit (PSDU) is the PHY payload's content.

The receiver uses the preamble field in the PHY packet for synchronisation. The beginning of the frame delimiter (SDF) indicates the transition from SHR to PHR. The frame length specifies the total number of octets in the PHY payload (PSDU).

The MAC header (MHR), the MAC payload, and the MAC footer are the three elements that form the MAC frame (MFR). In the MHR, the frame control field contains information on the frame type, addressing fields, and other control flags. The beacon sequence number (BSN) is specified by the sequence number. The source and destination addresses are provided in the addressing field. The auxiliary security header is optional and contains security processing information.

The NWK layer provides the MAC payload. A superframe is a frame that is bounded on both sides by two beacon frames. In a beacon-enabled network, the superframe is optionally used to help define guaranteed time slots (GTSs). Whether a GTS is utilised to receive or transmit is determined by the GTS field in the MAC payload.

The beacon frame is used by the coordinator to synchronise the devices in a network. Additionally, it is used to notify a specific device in a network that there is data pending for that device in the coordinator. The device will contact the coordinator at its discretion and request that the data be transmitted to it, such process is designated *Indirect transmission*. The address of the devices whose data is waiting at the coordinator is stored in the pending address field of the MAC payload. When a device gets a beacon, it checks the pending address field to determine if it has any data waiting.

The beacon payload field is an optional field that is transmitted with the beacon frame and can be utilised by the NWK layer. The Frame Check Sequence (FCS) field is used by the receiver to verify for any possible errors in the received frame [50].

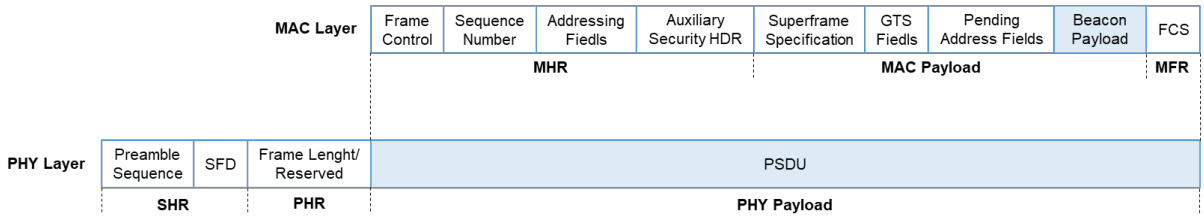


Figure 3.15: ZigBee's MAC beacon frame structure.

Data frame

Figure 3.16 depicts the structure of a data frame. The NWK layer provides the data payload. The data in the MAC payload is designated MAC Service Data Unit (MSDU). The fields in this frame are like those in the beacon frame, with the exception that the MAC data frame lacks the superframe, guaranteed time slot (GTS), and pending address fields. The MAC data frame becomes the PHY payload and it is known as the MAC Protocol Data Unit (MPDU).

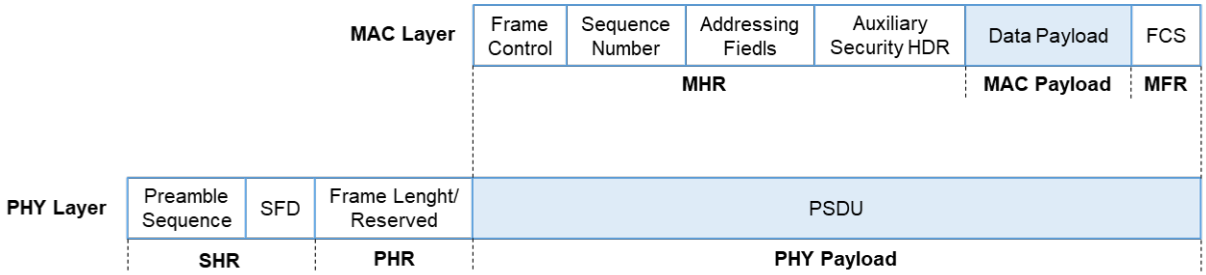


Figure 3.16: ZigBee's MAC data frame structure.

The Acknowledgment frame

Figure 3.17 depicts the structure of an acknowledgment frame. It illustrates the simplest MAC frame format and does not carry any MAC payload. An acknowledgment frame is transmitted from one device to another to confirm that a packet was successfully received.

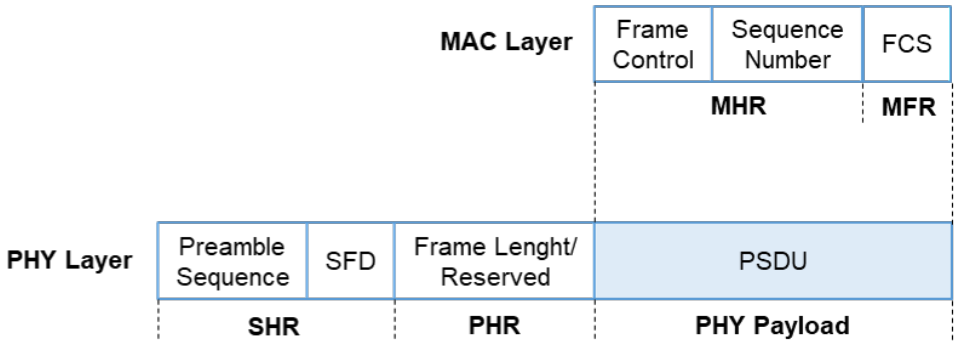


Figure 3.17: ZigBee's MAC acknowledgement frame structure.

The Command frame

Figure 3.18 depicts the structure of a command frame, which is used to transmit MAC commands such as requesting network association or disassociation. The command type field specifies the command's type (for example, association request or data request). The command itself is contained in the command payload. The complete MAC command frame is stored as a PSDU in the PHY payload.

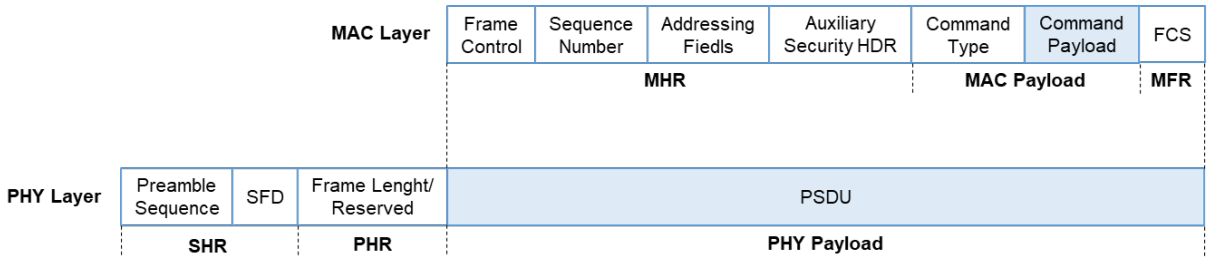


Figure 3.18: ZigBee's MAC command frame structure.

3.5.3 Security in Zigbee

The transmitted communications in a wireless network can be received by any nearby device, including an intruder. In a wireless network, there are two main security vulnerabilities[48, 50]:

- The first vulnerability is *data confidentiality*. The intruder device, by merely listening to the transmitted messages is capable of obtain sensitive information. The confidentiality issue can be solved by encrypting messages prior to transmission. Only the intended receiver will be able to recover the original message, after an encryption algorithm modifies the message with a string of bits known as the security key. The advanced encryption standard (AES) [57] is supported by the IEEE 802.15.4 standard for encrypting outgoing messages.

- The second problem is that, even if the communications are encrypted, the *intruder device may change and resend one of the previous messages*. If a message integrity code (MIC) is included on each outgoing frame, the recipient will be able to detect if the message has been modified in transit. This procedure is known as data authentication.

Methods for key formation, key transfer, frame protection, and device management are among the security services provided by ZigBee. The ZigBee Alliance defines security features for a device based on an open trust concept in which all levels of the communication stack and all applications operating on the same device trust each other [56].

The ZigBee standard offers a variety of options for meeting the following security requirements:

- *Freshness*: To keep data fresh, ZigBee devices keep track of incoming and outgoing freshness counters. When a new key is created, these counters are reset. For the next 136 years, freshness counts on devices that communicate once per second will not overflow.

- *Message Integrity*: For data integrity, the ZigBee standard allows for the transmission of messages of 0-, 32-, 64-, or 128-bit lengths. By default, the integrity level is set to 64 bits.

- *Authentication*: A common network key is used to provide network level authentication. This protects against external threats while consuming very little memory. Unique link keys between pairs of devices are used to establish device level authentication. This protects against both insider and external intrusions, but it comes with a greater memory cost.

- *Encryption*: ZigBee utilises AES encryption with a block size of 128 bits [57] . At the network or device level, encryption protection is available. A common network key is used to encrypt data at the Network level. To achieve device level encryption, distinct link keys between pairs of devices are required. Since certain applications do not require encryption, it may be deactivated without compromising freshness, integrity, or authentication.

Security measures are included into the ZigBee protocol stack at the MAC, NWK, and APS layers. ZigBee will apply the MAC Layer security specified in the IEEE 802.15.4 standard [48] to ensure security for the MAC Layer frames(command, beacon,data and acknowledgement frames). Security MAC Layer data frames only protects communications delivered over a single hop. To offer security for multihop communications, ZigBee would rely on higher layer security, such as NWK Layer security.

The MAC layer defines a number of security suites that employ the Advanced Encryption Standard (AES) as their fundamental cryptographic algorithm. The MAC layer handles security processing, whereas the top layers, which set up the keys, decide on security levels. The MAC Layer includes an auxiliary header to the MAC Layer header for carrying security information, as shown in the Figure 3.12. The message integrity code (MIC) indicates the level of data integrity and it can have values of 0, 32, 64, or 128.

When the MAC layer transmits (receives) a frame with security enabled, it examines the frame's destination (source), obtains the key associated with that destination (source), and then processes the frame according to the security suite defined for the key in use. Each key corresponds to a particular security suite, and the MAC Layer frame header contains a bit that indicates whether security is enabled or deactivated for that frame [56].

The ZigBee Gateway

A ZigBee gateway serves as an interface between a ZigBee network to another network that uses a different standard.

For example, a ZigBee application to be used as an in-home patient monitoring. In this scenario, a wearable device checks a patient's blood pressure and heart rate, and the patient also wears a ZigBee device that communicates with a sensor that collects health-related data, such as blood pressure, on a regular basis. This data is then wirelessly transmitted to a ZigBee gateway, for example, the patient's personal computer, which will send the vital information via the Internet, to the patient's physician for further analysis [58]. The ZigBee gateway in this situation incorporates both the ZigBee and the Internet protocols, allowing the translation of ZigBee packets to Internet protocol packet format, and vice versa.

Chapter 4

The Bluetooth Low Energy Standard Protocol

4.1 Bluetooth Low Energy Introduction

The Bluetooth Low Energy (BLE) technology, also known as Bluetooth Smart, is an open standard wireless technology for short range communications that was developed by the Bluetooth Special Interest Group (SIG) as a complement to traditional Bluetooth. It was released in 2010 as part of the Bluetooth 4.0 core specifications and it constituted a successful step to expand the ecosystem of Bluetooth for IoT [59]. BLE is a technology designed to operate with the lowest possible power consumption, low cost, low bandwidth and complexity. This design goals lead to a low power standard that is capable of running for a long time on a small coin battery [60].

Figure 4.1: Bluetooth logotype (extracted from [59]).

Since the release of Bluetooth 4.0, this technology has been regarded as one of the most promising wireless technologies, with quick adoption of BLE in a wide range of commercial devices. Such growth is closely related to the use of Bluetooth on many mobile devices(smartphones,tablets, laptops, etc.) and wireless smart gadgetry. Furthermore it is compatible with major platforms such as iOS, Android, Microsoft and Linux [61].

BLE devices have an unusually low adoption barrier, due to their ability to communicate with smartphones. Taking into consideration that most people carry a smartphone in their pocket, it is easy for the public to interact with BLE devices using their own smartphone. Furthermore, the Internet Engineering

Task Force (IETF) has developed the adaptation layer to support Internet Protocol version 6 (IPv6) over BLE, thus facilitating the connectivity of BLE devices with the Internet of Things (IoT) [62]. Thus, BLE has a high penetration in current mobile devices and this wide adoption has lead for the adoption of BLE in different IoT use cases.

In 2015, the Bluetooth Special Interest Group (SIG), currently a global community of over 36.000 companies [63], declared the creation of the Bluetooth Smart Mesh working group to define the architecture for standardised mesh networking for BLE [64]. Newer versions of BLE have been standardised since then to accommodate the upcoming wave of IoT use cases. In 2016, version 5.0 was announced, followed by version 5.1 in 2019. More recently, in January 2020, the Bluetooth SIG, introduced the latest version of Bluetooth, version 5.2, which offers new benefits for the next generation of wireless devices and audio technologies [65].

BLE Devices Types

Bluetooth wireless technology systems are divided into two types in the current version of the Bluetooth Core Specification: Classic or Basic Rate (BR) and Low Energy (LE). Device discovery, connection establishment, and connection procedures are all included in both systems. Optional Enhanced Data Rate (EDR) and Alternate MAC and PHY (AMP) layer enhancements are available for the Basic Rate system.

The LE system has characteristics that reduce current consumption, complexity and cost as compared to the BR/EDR system. The LE system is also optimised for applications that require lower data rates and duty cycles. As a result, depending on the application, one system with optional parts may be preferable to the other [2].

While several protocol concepts from previous versions of Bluetooth were reused in BLE, it is nevertheless regarded as a separate technology with distinct design goals and use cases. Thus, BLE is not backward compatible with Bluetooth classic. Any Bluetooth device prior to version 4.0 is unable to communicate with a BLE device in any form, because the upper protocol layers and the applications are incompatible between these two technologies [60].

To face this problem, Bluetooth SIG released in 2013, Bluetooth 4.1, which is the first major update of BLE, to ensure a correct interoperability among devices implementing specification versions of 4.0 and 4.1. Bluetooth SIG introduced *Bluetooth Smart Ready*, a dual-mode wireless standard that allows developers to use both classic Bluetooth and Bluetooth Low Energy in their applications. Therefore there are two types of devices that can implement BLE: *dual-mode* and *single-mode devices*. A dual-mode device can support both Bluetooth classic and BLE, this configuration allows compatibility with billions of existing devices. A single-mode device, on the other hand, is a Bluetooth device that only supports Bluetooth Low Energy [64].

The protocol stacks for conventional Bluetooth, BLE, and Bluetooth Smart Ready are represented in Figure 4.2

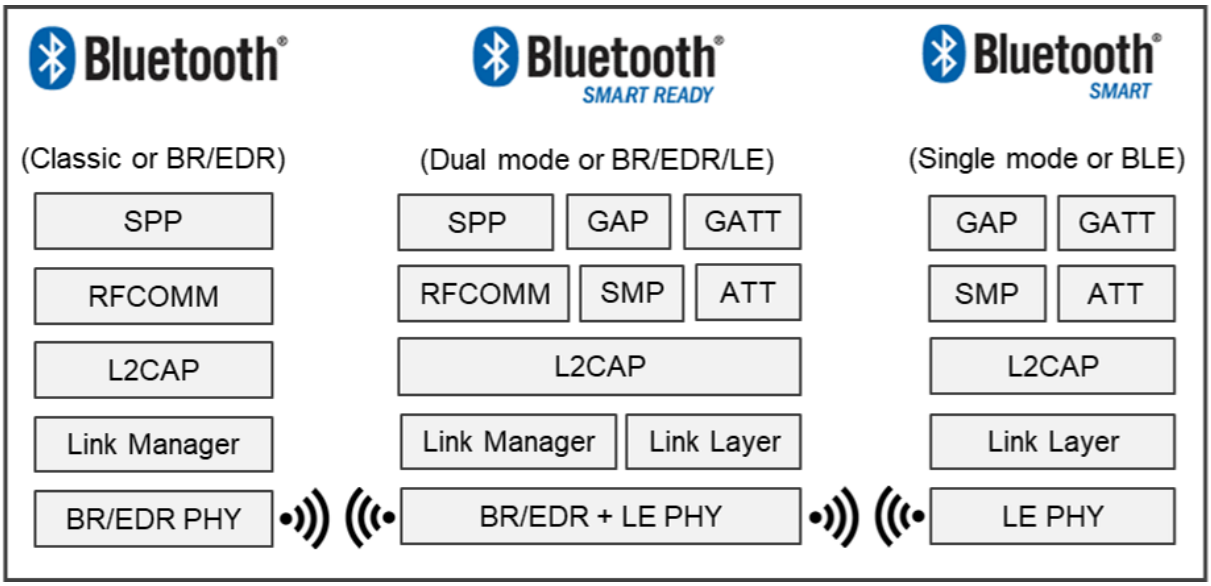


Figure 4.2: Comparison of the protocol stacks of classic Bluetooth, BLE and Bluetooth Smart Ready.

BLE Gateway

Nowadays, most end-user devices support Bluetooth Smart Ready(dual-mode), whereas sensor infrastructure need to conserve energy and mainly use BLE (single-mode).These Bluetooth Smart Ready devices can use WiFi radios or cellular access to foward data obtained from pure BLE-based sensors to the Internet [60].

4.2 Architecture

As illustrated in Figure 4.3, the protocol stack of BLE is divided into two main parts [64, 66]: a controller part and a host part.

The controller part is responsible for the radio components as well as the hardware to support the reception and transmission of packets. It usually consists of the Physical(PHY) and Link Layer(LL) (implemented in the form of a SoC(System-On-Chip) with an integrated radio).

The host part is responsible for protocols, multiplexing layers, and security. It operates on an application processor and contains upper layer capabilities such as the Logical Link Control and Adaptation Protocol (L2CAP) and the Attribute Protocol (ATT), which specifies a general mechanism for exposing device state data.

On top of the ATT is the Generic Attribute Profile (GATT), which establishes how ATT is used to enable reusable services that expose the standard characteristics of a device, the Security Manager Protocol (SMP) and the Generic Access Profile (GAP), responsible for how the devices find and connect to each other in an interoperable manner.

The Host Controller Interface (HCI) enables the communication between the host part and the controller part via a set of commands and events, along with a data packet format and a set of rules for flow

control. Since the controller part operates with complex real-time requirements and contacts with the Physical Layer, it is beneficial to separate it from the host part.

The Application is responsible for the application logic, user interface and data handling. Nowadays, most BLE chip sets incorporate the controller, the host, and the application into a single chipset, which is referred to as a system-on-chip (SoC). A SoC decreases final equipment costs and size, it is ideal to operate all three layers concurrently on a single chip.

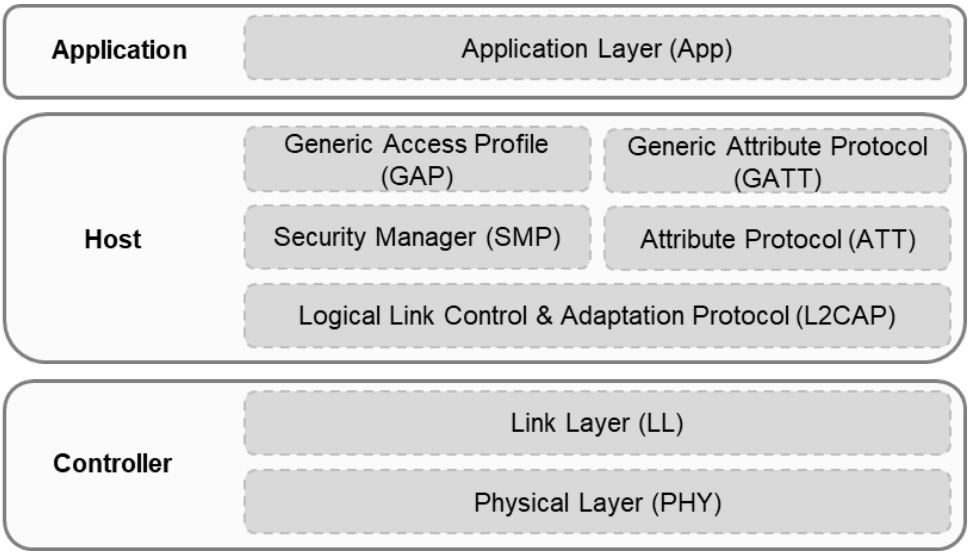


Figure 4.3: The stack of BLE protocol.

4.3 BLE Physical Layer

4.3.1 Frequency of Operation

Bluetooth Low Energy uses the 2.4 GHz Industrial Scientific Medical (ISM) band and has 40 Radio Frequency (RF) channels with a channel spacing of 2 MHz. [64].

The operating frequency bands are according to the formula present in the Table 4.1.

Table 4.1: BLE operating frequency bands.

Regulatory Range	RF Channels
2.400-2.4835 GHz	Fc= 2402 + k*2 in megahertz, for k= 0, ..., 39

This scheme differs from classic Bluetooth (see Table 4.3), which also uses the 2.4 GHz range and defines 79 frequency channels separated by 1 MHz. There are the two types of BLE RF channels available: advertising and data channels. Advertising channels are used for device discovery, connection formation, and broadcast transmission, whilst data channels are utilized for bidirectional communication between connected devices. There are three channels designated as advertising channels,they are defined in Table 4.2. The center frequencies for these channels were chosen to avoid interfering with IEEE 802.11 channels 1, 6, and 11, which are widely utilised in various regions [67].

Bluetooth classic employs 16 to 32 channels for advertising (data broadcasting), while the remaining channels are used for data transfer (used for the transmission of application data). BLE, on the other hand, designates just three channels as advertising channels, while the remaining 37 are designated as data channels, as shown in Figure 4.4. In BLE, the reduced number of advertising channels is the key to a considerable reduction in energy usage [2].

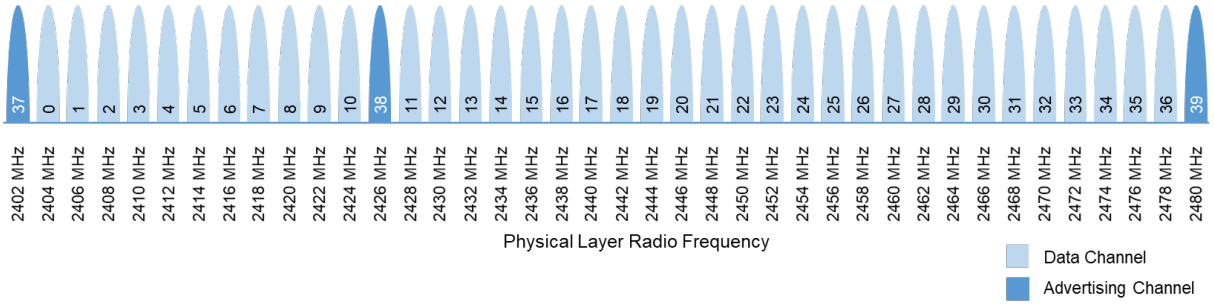


Figure 4.4: Bluetooth Low Energy channels and operating frequency bands.

Table 4.2: Bluetooth Low Energy advertising channels.

BLE Advertising channel number	Frequency value[MHz]
37	2402
38	2426
39	2480

4.3.2 Modulation

BLE employs the Gaussian Frequency Shift Keying (GFSK) modulation, which is an FSK modulation with a Gaussian filter added, just as Bluetooth classic. This filter helps to smooth the transitions between frequencies, which would otherwise result in a significant out-of-band spectrum. However, with BLE, a modulation parameter designated the modulation index is increased. As a result, peak power consumption is reduced, and range and robustness are improved. The modulation index ranges from 0.45 to 0.55, allowing for lower peak power usage [67].

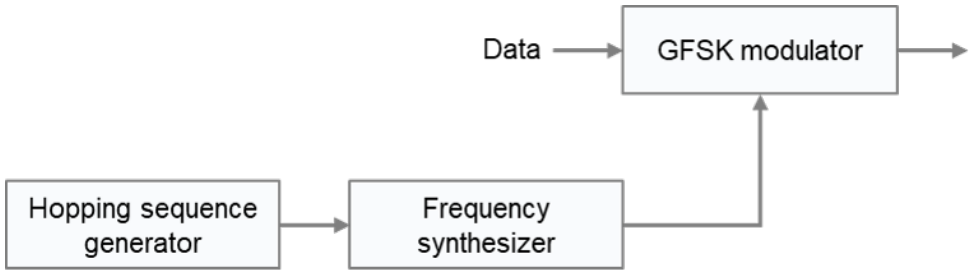


Figure 4.5: Block diagram of the FHSS/GFSK scheme used for the Data channels.

The data channels are dynamic and employ adaptive frequency-hopping spread spectrum(FHSS), which prevents the hopping sequence from using congested frequencies. Each carrier selected by the FHSS method is used as the GFSK modulator's center frequency for these channels (see Figure 4.5).

Advertising channels, on the other hand, are fixed. Considering that BLE uses the same ISM band as WiFi, BLE devices may encounter significant interference if there are WiFi devices nearby with high transmission power. The usage of FHSS can help to reduce the impact of any such interference across any single channel.

Table 4.3: Comparison of the features between BLE and classic Bluetooth (BR/EDR).

	BLE	**BR/EDR**
Data transmission	Short burst data	Continuos data streaming
Frequency band	2.4 GHz ISM Band	2.4 GHz ISM Band
Channels	40 channels with 2 MHz spacing	79 channels with 1 MHz spacing
Channel usage	Frequency Hopping Spread Spectrum (FHSS)	Frequency Hopping Spread Spectrum (FHSS)
Modulation	GFSK	GFSK, $\pi/4$DQPSK,8DPSK
Power Consumption	0.01-0.5 W (depending on use case)	1 W (reference value)
Over the air data rate	LE 2M PHY: 2 Mbps LE 1M PHY: 1 Mpbs LE Coded PHY (S = 2): 500 Kbps LE Coded PHY(S = 8): 125 Kbps	EDR PHY (8DPSK): 3 Mbps EDR PHY ($\pi/4$DQPSK): 2 Mbps BR PHY (GFSK): 1 Mbps
Max Tx Power	Class 1: 100 mW (+20 dBm) Class 1.5: 10 mW (+10 dBm) Class 2: 2.5 mW (+4 dBm) Class 3: 1 mW (0 dBm)	Class 1: 100 mW (+20 dBm) Class 2: 2.5 mW (+4 dBm) Class 3: 1 mW (0 dBm)
Network Topologies	Point-to-point(including piconet) Broadcast Mesh	Point-to-point(including piconet)
Active slaves	Implementation dependent; Not defined	7
Security	128-bit AES in CCM mode and application layer user defined	56/128-bit and application layer user defined
Distance/range (Theoretical max.)	400 m	100 m

4.3.3 BLE Version 4

BLE V4.0/4.1

BLE's versions 4.0/4.1 employ the same low energy packet format and modulation rate of 1Mbps.

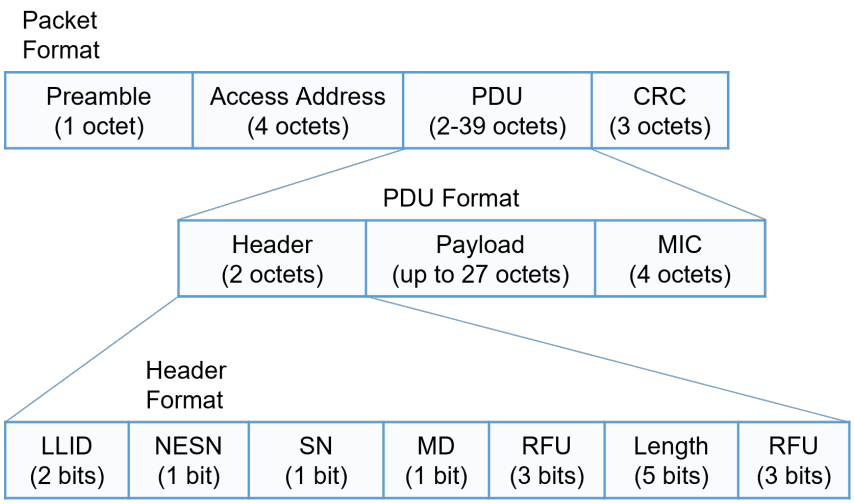


Figure 4.6: BLE's packet format, PDU format and header format of versions 4.0/4.1 link layer data packet.

The frame begins with a one-byte preamble that contains either 01010101 or 10101010, one of two sequences. These sequences enable receivers to perform automatic gain control at the physical layer, increasing the probability of correct frame reception [68].

The next parameter is the destination device's access address, which is a 32-bit identifier. The Access address in the advertising channel is set to a broadcast address, which is a fixed value. The Access address in data channels is a random number selected by the master and sent in the Connect Request message.

The next field is the payload, which has a maximum of 39 bytes wide. The last field contains a 24-bit CRC, which is wider than the 16-bit CRC used in other radio technologies like IEEE 802.15.4. In noisy environments, the usage of a 24-bit CRC provides better robustness.

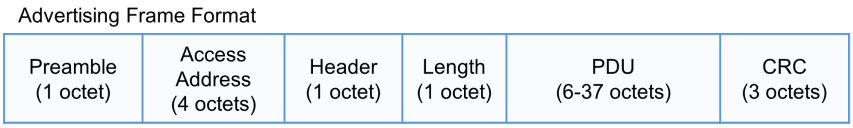


Figure 4.7: BLE's advertising frame format of versions 4.0/4.1.

In an advertisement frame, a header field and a length field are included, as illustrated in Figure 4.7. The header specifies the kind of advertising frame, along with information about the frame's purpose. Since the payload is variable in length, the length field is required.

The data frame is formatted similarly to the advertisement frame. The sequence number and the next expected sequence number are two important bits in the header that are utilized for flow control. Acknowledgements have the same frame format, but they will not have the payload field [2].

BLE V4.2

The modulation rate for Bluetooth v4.2 is the same as it is for Bluetooth 4.0 and 4.1, which is 1 Mbps. The packet format, however, is different as illustrated in Figure 4.8.

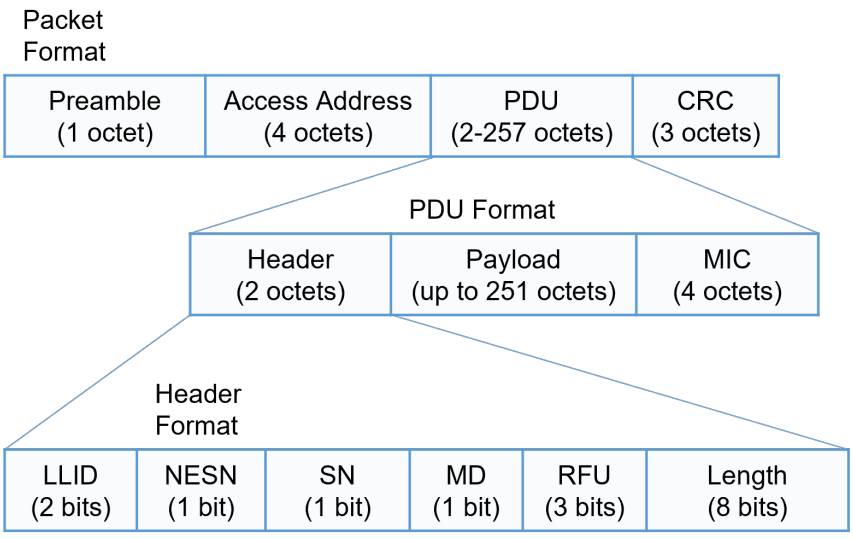


Figure 4.8: BLE's packet format, PDU format and header format of version 4.2 link layer data packet.

Figure 4.8 reveals the difference of the Length field, which is 8 bits long and has a range of 0 to 255 octets, indicating the length of the Payload and, if applicable, the MIC. Considering that the MIC is 4 octets wide, the Payload field must be less than or equal to 251 octets in length [68].

From BLE version 4.2 to BLE version 5.0, the packet format is the same with a payload of 251 octets, as shown in Table 4.4 and in Table 4.5, it will be further studied in section 4.4 [68, 69].

Table 4.4: BLE's packet format and maximum data packet transmission time consumed.

	Preamble	**Access Address**	**Header**	**Payload**	**MIC**	**CRC**
v 4.0/4.1 (328 μs)	1 octet	4 octets	2 octets	27 octets	4 octets	3 octets
v 4.2 (2120 μs)	1 octet	4 octets	2 octets	251 octets	4 octets	3 octets
v 5.0 [1 Mbps] (2120 μs)	1 octet	4 octets	2 octets	251 octets	4 octets	3 octets
v 5.0 [2 Mbps] (1064 μs)	1 octet	4 octets	2 octets	251 octets	4 octets	3 octets

Table 4.5: Comparison of BLE's standards.

	BLE 4.0/4.1	**BLE 4.2**	**BLE 5**			
			LE Coded S=2	**LE Coded S=8**	**LE 1M**	**LE 2M**
Channels	40 (2 MHz)	40 (2 MHz)	40 (2 MHz)	40 (2 MHz)	40 (2 MHz)	40 (2 MHz)
Advertisment Ch.	3	3	3 Primarry 37 Secondary	3 Primarry 37 Secondary	3 Primarry 37 Secondary	3 Primarry 37 Secondary
TX power [dBm]	-20 to 10	-20 to 10	-20 to 20	-20 to 20	-20 to 20	-20 to 20
RX sensitiviy [dBm]	-97	-97	-99	-103	-95	-89
Peak current [mA]	$<$15	$<$15	$<$15	$<$15	$<$15	$<$15
Latency [ms]	$<$6	$<$6	$<$6	$<$6	$<$6	$<$6
Range [m]	10-100	10-100	40-400	20-200	10-100	10-100
Data Rate [Mbps]	1	1	0.5	0.125	1	2
Max Payload [byte]	37	255	255	255	255	255
Max ADV Payload [byte]	37	37	255	255	255	255
Max active nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
PDU format	Single	Single	Single(coded)	Single(coded)	Single	Single

4.3.4 Overview of Bluetooth Low Energy 5 (BLE5)

New PHYs

The Bluetooth Low Energy 5 specification, BLE5, is the most recent version of the BLE standard, and it represents the most significant advancement in Bluetooth technology. BLE5 incorporates two new PHY implementations to the Bluetooth LE 4.0 specification, allowing for better performance. Without raising the transmit power, the two new types allow for enhanced throughput or communication range. The gains are due to enhanced receiver sensitivity and error correction rather than increased transmitting power.

Originally, BLE only supported PHYs with 1 Mbps (so-called LE 1M) modulation and Gaussian Frequency Shift Keying (GFSK). BLE5 has a 2 Mbps PHY (so-called LE 2M) for high throughput, as well as two coded PHYs (named LE Coded) with data rates of 500 kbps and 125 kbps. The rest of the PHYs, including the LE 1M and LE Coded, modulate at 1 mega symbols per second (1 Msps), with the

exception of LE 2M, which modulates at 2 Msps.

Only error detection, not error repair, is performed by Bluetooth low energy version 4. Error correction is now possible with BLE5. Not only can errors at the receiver be detected, but they can also be corrected, up to a certain point, so that the data does not have to be resent to the receiver [70].

Encryption uses the Advanced Encryption Standard - Counter with CBC MAC to encrypt the data (AES-CCM, where CBC-MAC is the initialism for Cipher Block Chaining Message Authentication Code.) Data is sent through a Cyclic Redundancy Check (CRC) algorithm after encryption, followed by a Data Whitening algorithm to prevent long strings of 0s and 1s. The new error correction capabilities in the LE Coded PHY adds two phases to the bit stream processing done by the Link Layer, as shown in Figure 4.9. If using LE coded, data is subsequently passed through a Forward Error Correction (FEC) encoder and a Pattern mapper. The information is then transmitted over the air. The same mechanisms occur to received packets as they do to transmitted packets, but in reverse order.

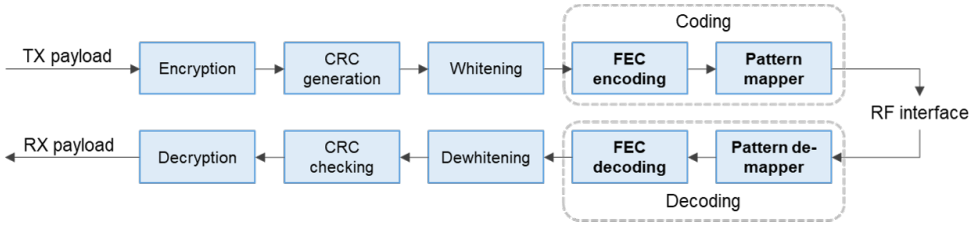


Figure 4.9: BLE5's bit stream processing for LE coded.

Forward Error Correction (FEC) is a method of error correction used by the LE Coded PHY. It works by adding extra, redundant bits to the packets being transmitted. The sole function of those bits is to facilitate the application of the FEC algorithm in order to perform error correction.

FEC Encoding employs a convolutional encoder that generates two bits for each bit of input data using the generator polynomials in equation 4.1.

$$\begin{aligned} G_0(x) &= 1 + x + x^2 + x^3 \\ G_1(x) &= 1 + x^2 + x^3 \end{aligned} \tag{4.1}$$

LE Coded comes with two different coding schemes, S=2 and S=8, from which to choose. Each bit from the convolutional FEC encoder is converted by the Pattern Mapper into P symbols, the value of which is dictated by the coding scheme. When S=2, there is no change (i.e. P=1), but when S=8, each bit from the FEC encoder produces four output bits from the Pattern Mapper (i.e. P=4), as specified in Table 4.6.

With the LE Coded PHY, the choice of coding scheme, S=2 or S=8, has two consequences.With S=2, the range is roughly doubled, and with S=8, the range is roughly quadrupled. However, as can be seen, the need for redundant data to support the FEC algorithm at the receiver has an impact on the number of symbols that must be transmitted, lowering the overall data rate.

The PHYs, their coding schemes, and their data and symbol rates are given in Table 4.7. The designations "LE Coded S = 2" and "LE Coded S = 8" are used to distinguish between the coded PHYs, for simplicity reasons [71, 72].

Table 4.6: BLE's pattern mapper behaviour.

Input (from FEC Encoder)	Output with S = 2 (P =1)	Output with S = 8 (P = 4)
0	0	0011
1	1	1100

- **LE 1M PHY**: 1 Megasymbol / second options:
  - **LE 1M**: Uncoded data is transmitted at 1 Mbps.
  - **LE Coded**: Access Address, Coding Indicator, and TERM1 fields coded at 125 kbps, and payload coded at either (S=8) 125 kbps or (S=2) 500 kbps.
- **LE 2M PHY**: 2 Megasymbols / second option:
  - Uncoded data is transmitted at 2 Mbps

Table 4.7: Features of PHYs in Bluetooth Low Energy 5.

PHY	Coding Scheme		Data rate	Symbol rate
	Header	Payload		
LE 1M	Uncoded	Uncoded	1 Mbps	1 Msps
LE 2M	Uncoded	Uncoded	2 Mbps	2 Msps
LE Coded S =2	S = 8	S = 2	500 kbps	1 Msps
LE Coded S =8	S = 8	S = 8	125 kbps	1 Msps

The PHY used in Bluetooth 4 is LE 1M. It has a symbol rate of 1 Msps and it employs GFSK. Since each symbol translates to one data bit, this corresponds to a bit rate of 1 Mbps. LE 1M is still available for use in Bluetooth 5, and in fact its support is mandatory.

The new LE 2M PHY allows the physical layer to function at a rate of 2 Msps, which is faster than LE 1M and Bluetooth 4. Incorporation in a stack implementation is optional.

When compared to Bluetooth 4, the LE Coded PHY provides for a quadrupling (approximately) of range while requiring no increase in transmission power [70].

Channel Selection Algorithm#2 (CSA#2)

The 2.4 GHz ISM band is used by BLE technology and to coexist with other wireless technologies and minimise interference in this band, BLE uses frequency hopping over 37 available channels .To determine the next hopping channel for the link, previous versions of BLE used a basic channel selection algorithm. The BLE 5 does, however, include a new CSA called CSA#2, which further randomises the channel selection method and improves BLE's compatibility with other technologies while reducing interference.

Extended Advertising

The advertising component of BLE is an important feature that is employed in devices like beacons, which broadcast a small amount of data on a regular basis. Without establishing a connection, this

data can be gathered by nearby smart phones, tablets, and practically any device equipped with BLE technology. Beacons are now widely employed in retail and market advertising, indoor localisation, and other applications as a fast-growing technology on the market [73].

The advertising capability of BLE 5 has been improved, making it more desirable for IoT applications. For advertising reasons, previous versions of BLE only used three frequency channels. Furthermore, the maximum payload size is limited to 31 bytes. For advertising reasons, BLE 5 introduces the term primary channels and secondary channels. Three advertising channels are designated primary channels, whereas the other 37 channels (data channels) are designated secondary channels. The advertisement always appears on three primary channels, for backward compatibility. Extra data can be offloaded onto auxiliary channels as necessary. In comparison to prior BLE versions, it allows for more information to be broadcast. Moreover, the maximum payload has been increased to 255 bytes, thereby increasing the advertising capacity of BLE 5 up to 8 times [71].

Periodic Advertising

Another enhancement in BLE5 is periodic advertising, which allows the transmission of unidirectional data streams to one or more devices without the need for a connection establishment. Data is periodically transmitted at a specified interval from the same advertising set.

The angle of arrival (AoA) and angle of departure (AoD)

In BLE V5.1, the devices' positioning capabilities have been enhanced by enabling AoA and AoD functions. The AoA and AoD techniques can be used by an LE device to assess the direction of transmission or reception. In order to do this, the peer device must have a RF switch and antenna array capable of switching the antenna to receive or transmit the packet. The AoA is calculated using the trigonometry function 4.2, as follows:

$$\theta = \arccos((\psi\lambda)/2\pi d), \tag{4.2}$$

where θ, ψ, λ, and d represent the angle of arrival, phase difference in the signal arriving at the two antennas, signal wavelength, and distance between the two antennas, respectively. The same formula is used to compute AoD, similarly to AoA [71].

4.3.5 BLE Network Topologies

Point-to-point, *Point-to-Multipoint*, and *Mesh* connectivity are among the network topologies supported by Bluetooth, as illustrated in Figure 4.10. For devices that use Bluetooth BR/EDR or BLE, point-to-point connectivity is available. Only BLE devices support the *broadcast* and Mesh connectivity topologies [74].

As illustrated in Figure 4.10, most BLE devices interact with one another using a basic point-to-point (one-to-one) or point-to-multipoint (one-to-many) architecture. For BLE devices, *broadcast* piconets

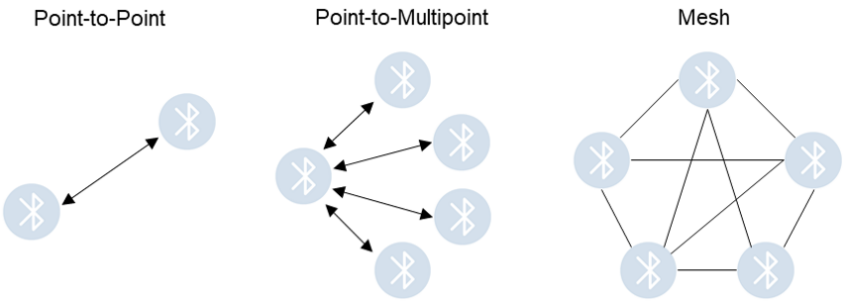


Figure 4.10: Bluetooth Low Energy connection topologies.

provide one-to-many communication links.

A Bluetooth *piconet* connects devices that use one-to-one communication. Each piconet, as illustrated in Figure 4.11, consists of a device that plays the *Master* role, as well as devices that play the *Slave or Advertiser* roles and the *Idle* role.

- The synchronisation reference is provided by the Master device.
- Other devices that synchronise to the master's clock and frequency hopping pattern are designated Slaves.
- Each Slave node is an advertiser before joining the piconet.
- Other Idle devices may exist in a piconet, but they are not active.

In one piconet, a single Bluetooth device can act as a slave, while in another piconet, it can act as a master. A master device per piconet may control up to seven slaves; the slaves interact with the master device but not with one another. A slave device, on the other hand, may be a member of one or more piconets, which are simply groups of Bluetooth-connected devices. In Figure 4.11, it is illustrated an overview of the *scatternet* topology, which is a traditional Bluetooth architecture consisting of two or more piconets.

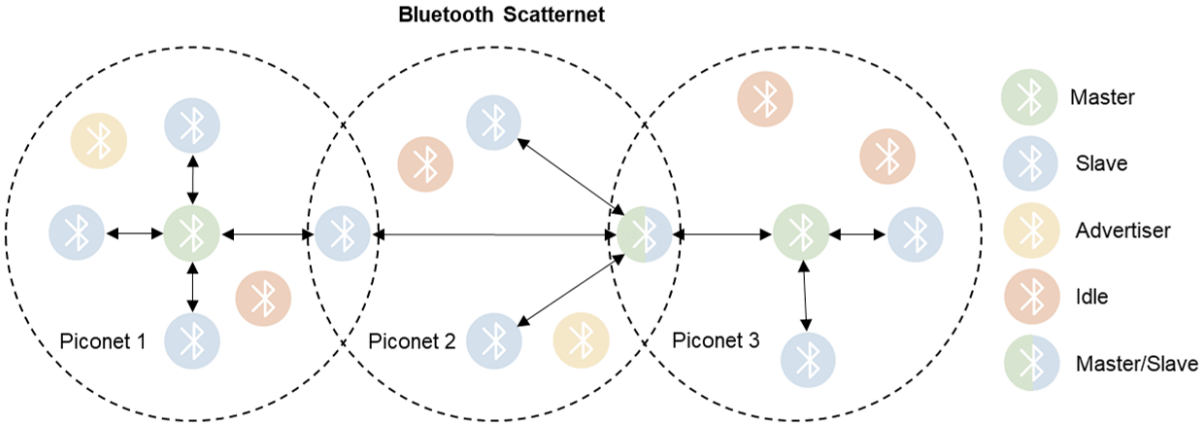


Figure 4.11: Bluetooth Low Energy connection topologies.

In a BLE architecture, the slaves interact with the master on separate physical channels. In contrast to a classic Bluetooth piconet, where all slaves must be on constant standby to listen for incoming connections, a BLE slave invites connections and therefore it has complete control of its power consumption. A BLE master, because it is considered to have less power limitations, will listen for advertisements and establish connections on the back of an advertisement packet, as shown in Figure 4.12.

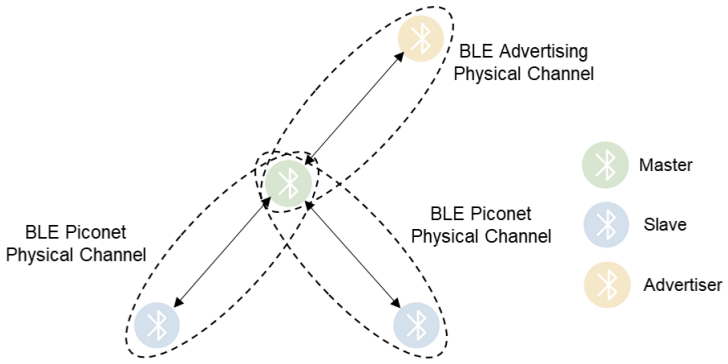


Figure 4.12: BLE the slaves interact with the master on separate physical channels.

While BLE retains the original Bluetooth protocol's operating spectrum and basic communication protocol structure, it also incorporates a new lightweight Link Layer that allows extremely low power idle mode operation, fast device recognition, and reliable and secure point-to-multipoint data transfers. As a consequence, BLE consumes significantly less power in peak, average, and idle modes than classic Bluetooth. BLE utilises just 10% of the power that classic Bluetooth consumes over time(see Table 4.3) [43].

Mesh in BLE

As the Internet of Things (IoT) evolved, the lack of Mesh networking in Bluetooth became a significant disadvantage. On a manufacturing floor, for example, hundreds of wireless enabled sensors may be present, all of which must share data that is later communicated to the outside world and the Internet via wired or wireless means, which Bluetooth was not capable of achieving. In fact, the demand for Mesh networking in Bluetooth was so big that companies like Cambridge Silicon Radio (CSR), which was purchased by Qualcomm in 2015, developed methods for Bluetooth low energy devices to be able to build a Mesh network even though mesh was not yet part of the standard. These companies, along with Nordic Semiconductor and others, collaborated with the Bluetooth Special Interest Group to get mesh functionality into Bluetooth 5. In July 2017, the SIG formally announced that Bluetooth fully supports the Mesh network and built the specific BLE Mesh protocol which is compatible with the BLE 4.0 stack and the upper version.

It is arguable that the fact that Mesh networking is now standardised in BLE makes it a serious competitor for any IoT application. Since Bluetooth is built into every smartphone, tablet, and laptop computer, a BLE network can be configured and reconfigured on the go from an application, whose user may be in the same room or thousands of kilometers away. The cost and complexity of managing a Bluetooth 5 network are both reduced as a result of this, which is a major advantage.

Mesh networking compliments one of Bluetooth 5's other improvements: enhanced range, which is twice that of Bluetooth 4.0, with a theoretical limit of 400 meters [69]. This is accomplished, in BLE5 by raising the maximum output power from 10dBm (10mW) to 20dBm(100mW) [75].

Devices in a Bluetooth mesh can relay data to remote devices that are outside of the source device's direct communication range. This allows a Bluetooth mesh network to expand its radio range and cover a vast geographic area with many devices.The ability to self-heal is another advantage of the Bluetooth mesh over point-to-point and point-to-multipoint topologies. The Bluetooth mesh's self-healing capability means there is no single point of failure in the network. Even if a Bluetooth device disconnects from the mesh network, other devices can still send and receive messages, ensuring that the network remains operational. Mesh networks allow BLE devices to communicate with each other in a many-to-many topology. Mesh is ideal for control, monitoring, and automation systems that need to communicate reliably and securely with thousands of devices.

BLE Mesh devices and nodes

The devices that constitute a Bluetooth mesh network are designated *nodes*. *Unprovisioned* devices are those that are not connected to any Bluetooth mesh network. *Provisioning* refers to the process of converting an unprovisioned Bluetooth device into a node. Each node has the ability to send and receive messages directly or through relaying between nodes.

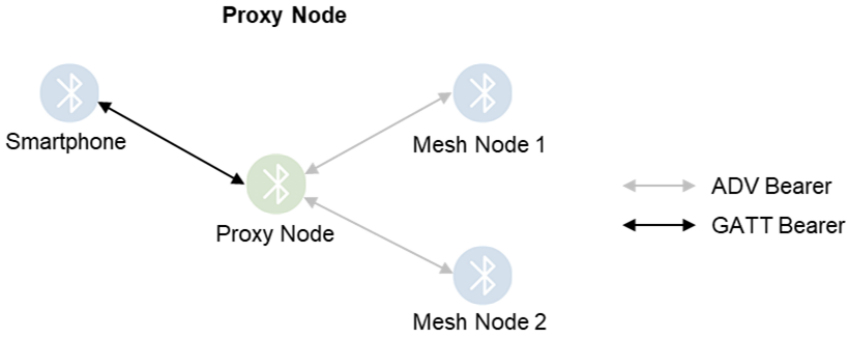


Figure 4.13: Bluetooth Proxy node.

Optional features may be available for each Bluetooth Mesh node, allowing them to gain special features, such as relay, proxy, friend, and low power functions. In Figure 4.14, there are five main types of nodes usually used in a typical structure of BLE Mesh network, which are introduced as below:

- **Relay nodes**: Relay nodes are Bluetooth mesh nodes that provide the Relay function. The relaying method is used by these nodes to retransmit received messages over several hops. A mesh node may become a Relay node depending on the power supply and computational capabilities.
- **Proxy nodes**: Proxy nodes can be used to enable communication between a Bluetooth Low Energy device that lacks a Bluetooth mesh stack and the mesh network nodes. The proxy protocol with generic attribute profile (GATT) operations is used by a proxy node, which operates as an intermediate. A smartphone that does not support the Bluetooth mesh stack, for example, interacts with mesh nodes via GATT operations through a Proxy node, as illustrated in Figure 4.13.

- **Friend node**: Bluetooth mesh nodes with no power limitations are excellent candidates for being Friend nodes. Friend nodes and LPNs cooperate. A Friend node saves messages for an LPN, waiting for the low power node to query. *Friendship* is the relationship between an LPN and a Friend node.
- **Low Power node (LPN)**: Bluetooth mesh nodes with low power can use the Low Power option to minimise radio on time and conserve energy. LPNs are the designation for such nodes. LPNs are mostly concerned with transmitting communications, although they do need to receive messages on occasion. Instead of constantly sending or listening to data packets on the broadcast channel, the low-power node periodically queries its friend node for data, which saves power. For example, when the temperature is above or below the specified threshold values, a temperature monitoring sensor powered by a tiny coin cell battery provides a temperature measurement once every minute. The LPN does not transmit a notification if the temperature remains within the thresholds.
- **End node**: the end node is similar to the end device in Zigbee at the network's edge, without the relay function.

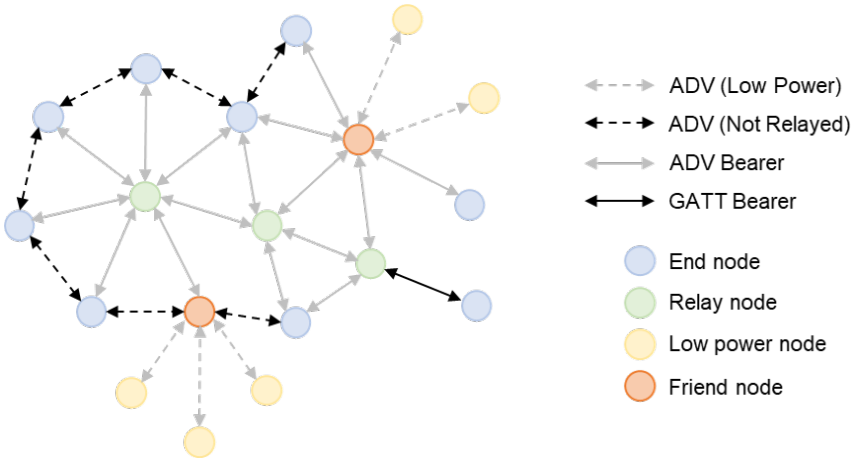


Figure 4.14: Structure of BLE Mesh network.

Apart from nodes, connections also have a variety of types, as shown below:

- **ADV (Not Relayed)**: Two end nodes can transmit and receive broadcast messages to each other, but they cannot relay data packets because they are not relay nodes.
- **ADV (Low power)**: This link is utilised between the low-power node and the friend node, to send and receive data packets. The low-power node will initiate a friendship request and query the friend node for its own data.
- **ADV Bearer**: Broadcast messages can be sent and received between the two nodes using the advertising bearer, and can be forwarded as a relay.
- **GATT Bearer**: Nodes that do not have ADV bearer capability can still participate in the mesh network by sending and receiving proxy PDUs (Protocol Data Units) over the GATT connection with other nodes through a proxy protocol [76].

4.4 BLE Link Layer

The Link Layer (LL) performs tasks that are similar to those performed by the OSI model's medium access control (MAC) layer. In Bluetooth, the LL communicates directly with the BLE PHY and controls the radio's link status to identify whether a device is a master, slave, advertiser, or scanner.

4.4.1 BLE states

The operation of BLE at the Link Layer is based on a low power state machine. The number of states and the number of state transitions are both small, as shown in Figure 4.15.

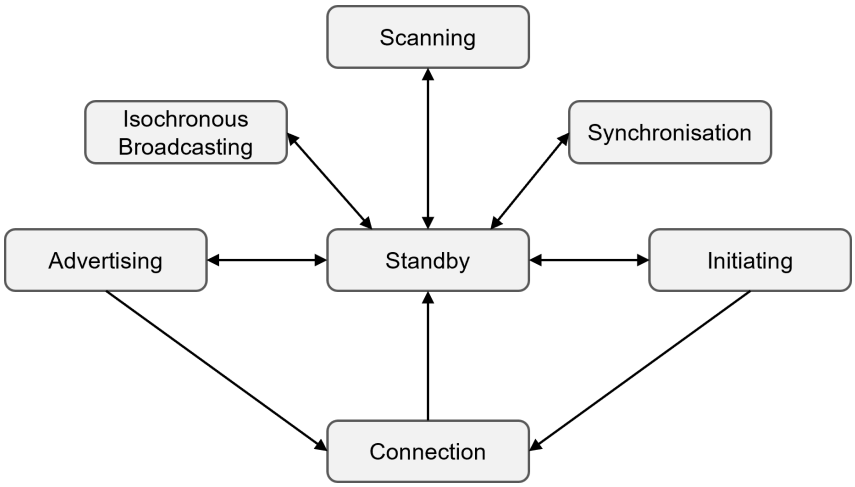


Figure 4.15: BLE's state diagram of the Link Layer state machine.

Only one state can be active at a time in the Link Layer state machine. At least one Link Layer state machine that supports either the Advertising or Scanning states must be present in the Link Layer. The Link Layer state machine can be used by multiple instances of the Link Layer [72].

- **Standby State:** In this state, a device is inactive, no packets are transmitted or received. This state can be entered from any other BLE states.
- **Advertising State:** In this state, a BLE device is known as an "Advertiser." This state is accessed from the "Standby State." The Link Layer is responsible for transmitting advertising physical channel packets and possibly listening to and responding to responses triggered by these advertising physical channel packets.
- **Scanning State:** In this state, Link Layer listens for advertising physical channel packets from other advertising devices.The BLE device in this state is referred to as a "Scanner." This state is accessed from the "Standby State."
- **Initiating State:** The BLE device is known as an initiator in this state. This BLE state may be accessed via "Standby State". The Link Layer will be listening for advertising physical channel packets from a specific BLE device(s) and responding to these packets to initiate a connection with another device.

- **Connection State:** This state can be reached from either the ”Initiating State” or the ”Advertising State”. A device in the Connection State is known as being in a connection. The BLE device can play one of two roles in this connection state: *Master* or *Slave*. It will be in the Master Role once it has entered from the Initiating State. It will be in the Slave Role once it has entered from the Advertising State. The Link Layer in the Master Role communicates with a device in the Slave Role and establishes transmission timings. The Link Layer in the Slave Role will communicate with a single Master Role device.

- **Synchronisation State:** This state can be accessed from ”Standby State”. In this state, the Link Layer listens for periodic physical channel packets from a device that transmits periodic advertising. While in this state, the Host can instruct the Link Layer to listen for isochronous data packets coming from a specific device that is transmitting a Broadcast Isochronous Group (BIG). A ”Synchronised Receiver” is a device that is in the Synchronisation State and receiving isochronous data packets.

- **Isochronous Broadcasting State:** In this state, the Link Layer will send isochronous data packets over an isochronous physical channel. This state can be reached from the Standby State. An ”Isochronous Broadcaster” is a device that is in the Isochronous Broadcasting State.

4.4.2 Frame Structures for BLE

The Link Layer specification uses *little-endian format* for bit ordering when defining fields within packets or Protocol Data Units (PDUs) [72]. The following rules are applied:

- The Least Significant Bit (LSB) corresponds to b_0.

- The LSB is the first bit sent over the air.

- With the exception of the Cyclic Redundancy Check (CRC) and the Message Integrity Check (MIC), multioctet fields must be sent with the least significant octet first.

Packet format for the uncoded and coded PHYs

As shown in Figure 4.16, there are two basic formats: one for the LE Uncoded PHYs and one for the LE Coded PHY.

The packet format for **uncoded PHYs** is defined for LE 1M PHY uncoded and LE 2M PHY uncoded and it is used for packets on all physical channels. There are four mandatory fields and one optional field in each packet. The Preamble, Access Address, PDU, and CRC are all required fields. Constant Tone Extension is an optional field.

The Preamble is used by the receiver to perform frequency synchronisation, symbol timing estimation, and automatic gain control training. It consists of an alternating sequence of 0 and 1 for the uncoded LE 1M and 2M PHYs, with the first bit equal to the LSB of the Access Address.

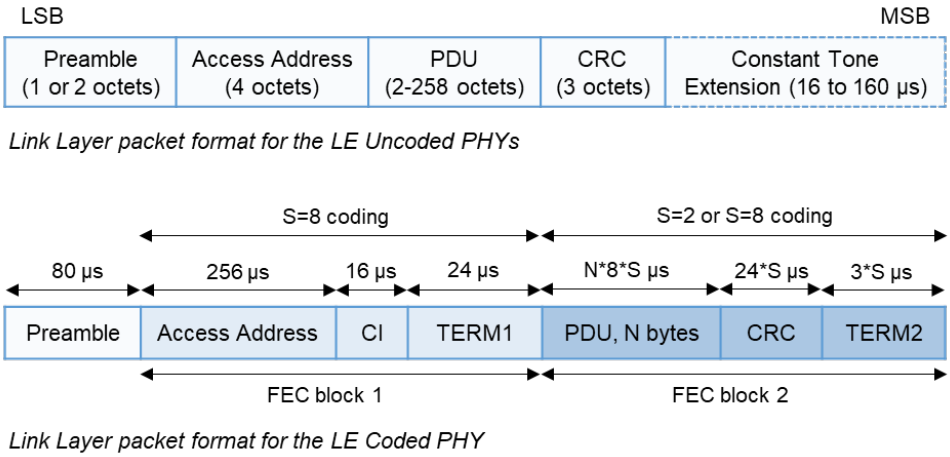


Figure 4.16: BLE's LL packet format for the LE Uncoded and Coded PHYs.

During advertising, the Access Address (AA) value is set to 0x8E89BED6 in the SyncInfo field. Each periodic advertisement and each Link Layer connection between any two devices has a unique Access Address.

Following the Access Address is the Protocol Data Unit (PDU). It will be the Advertising Channel PDU if the packet is on the primary or secondary advertising channel. If the packet is sent via a data channel, the PDU must be a Data Channel PDU. A 24 bit (3 octet) Cyclic Redundancy Check (CRC) is calculated using the bits from the PDU. It is sent at the end of the packet.

In this sequence, the Preamble is sent first, followed by the Access Address, PDU, CRC, and Constant Tone Extension (if present). The whole packet is modulated and sent at the same symbol rate of 1 Msym/s or 2 Msym/s.

The transmission time for the packet (without the Constant Tone Extension) ranges from 44μs to 2128μs. When the Constant Tone Extension is enabled, the duration of the Constant Tone Extension is between 16μs and 160μs.

The packet format for LE **coded PHYs** is used for packets on all physical channels. Each packet consists of the Preamble(is not coded), FEC block 1, and FEC block 2. The LE Coded PHY does not include a Constant Tone Extension.

The uncoded preamble consists of ten repetitions of 0x3C(00111100_2). There are three fields in the FEC block 1: Access Address, Coding Indicator (CI), and TERM1. The S=8 coding scheme, as specified in, shall be used. During advertisement, the access address is set in the SyncInfo field or is set to 0x8E89BED6. Three consecutive zeros in TERM1 signal a termination sequence and reset the FEC encoder (000_2).

Everything in FEC Block 2 is encoded using the Coding Indicator from Block 1. The PDU, CRC, and TERM2 are the three fields that constitute FEC block 2. Depending on the CI value, they shall utilise either the S=2 or S=8 coding scheme. If CI value is 00_2, it indicates that FEC Block 2 is encoded with S=8, and the value 01_2 indicates that FEC Block 2 is encoded with S=2. For every one input bit, the FEC encoder produces two output bits. The pattern encoder generates four output bits for every one input bit when it is used, as shown in equation 4.3. If S=2 it indicates that after exiting the FEC encoder, the

number of bits is doubled.If S=8 it indicates that the input bits are doubled in the FEC encoder, which are subsequently quadrupled by the Pattern Encoder.

$$1\text{bit} \times \frac{2 \text{ bits}}{\underset{\text{FEC}}{1\text{bit}}} \times \frac{4 \text{ bits}}{\underset{\text{Pattern}}{1\text{bit}}} \tag{4.3}$$

The Protocol Date Unit is either the PDU for the Advertising Channel or the PDU for the Data Channel. The data length before encoding ranges from 16 to 2056 bits. The range is either 128-16448 bits (S=8) or 32-4112 bits (S=2) after encoding, as defined in Table 4.8 The bits from the PDU are used to calculate the 24 bit (3 octet) Cyclic Redundancy Check (CRC). In TERM2, three consecutive zeros indicate a termination sequence and reset the FEC encoder(000_2)

The entire packet is transmitted with 1 Msym/s modulation. The transmission time for the packet ranges from 462μs to 17040μs.

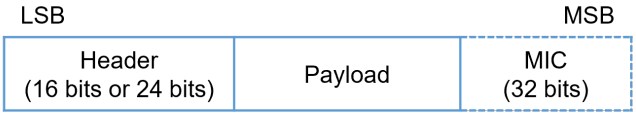
The size and duration of the data packet fields are captured in Table 4.8.

Table 4.8: BLE's LE Coded PHY field sizes and duration.

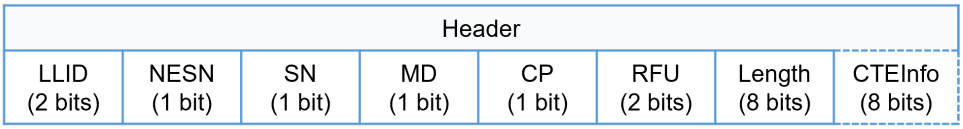
	Fields						
	Preamble	**Access Address**	**CI**	**TERM1**	**PDU**	**CRC**	**TERM2**
Number of Bits	Uncoded	32	2	3	16-2056	24	3
Duration when using S = 8 coding [μs]	80	256	16	24	128-16448	192	24
Duration when using S = 2 coding [μs]	80	256	16	24	32-4112	48	6

BLE'S Advertising Channel packets and Data Channel packets.

The Link Layer uses a single packet structure for both advertising and data channel packets. The



Data Physical Channel PDU



Data Physical Channel PDU header

Figure 4.17: BLE's Data Physical Channel PDU

Data Physical Channel PDU has a 16 or 24 bit header, a configurable size payload, and a Message Integrity Check (MIC) field. An unencrypted ACL connection, or an encrypted ACL connection with a Data Channel PDU with a zero length Payload, shall not include the MIC field. The Data Physical Channel PDU and respective Header field are shown in Figure 4.17.

Table 4.9: BLE's Data Physical Channel PDU header's fields description.

Field name	Description
LLID	The LLID indicates whether the packet is an LL Data PDU or an LL Control PDU. 0b00 = Reserved for future use 0b01 = LL Data PDU: Continuation fragment of an L2CAP message, or an unused PDU. 0b10 = LL Data PDU: Beginning of an L2CAP message or a fully L2CAP message with no fragmentation. 0b11 = LL Control PDU
NESN	Next Expected Sequence Number
SN	Sequence Number
MD	More Data
CP	CTEInfo Present
Length	The Length field specifies the size of the Payload and MIC, if included, in octets.
CTEInfo	The CTEInfo field specifies the Constant Tone Extension's type and length.

Table 4.9 specifies the 6 or 7 fields that form the 16 or 24 bit Header field.

The **Advertising Physical Channel PDU** is also used on the periodic physical channel, despite its name. It is defined by a 16 bit header and a variable size payload, as illustrated in Figure 4.18.

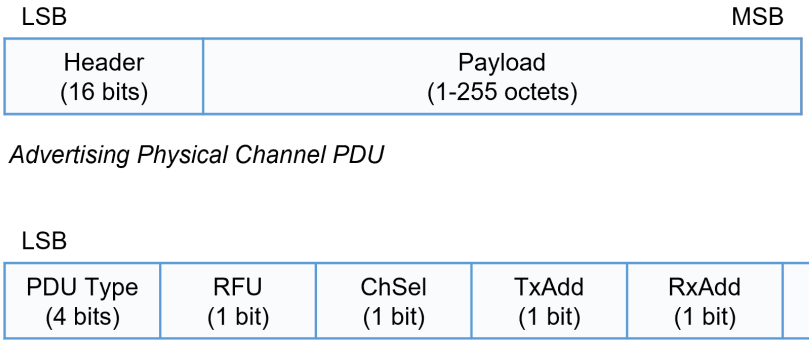


Figure 4.18: BLE's advertising channel PDU

The Advertising Physical Channel PDU header's ChSel, TxAdd, and RxAdd fields include information related to the PDU type defined for each Advertising Physical Channel PDU separately. The ChSel field in the advertising physical channel PDU header must be coded as 1 if the advertiser utilizes the LE Channel Selection Algorithm #2 feature. The TxAdd bit specifies if the advertiser's or initiator's (depending on the kind of advertisement packet) address is public (0x00) or random (0x01). For example, for ADV_IND, ADV_DIRECT_IND, ADV_NONCONN_IND, SCAN_RSP, and ADV_SCAN_IND it refers to the advertiser's address whereas it to refers to the initiator's address in the case of SCAN_REQ and CONNECT_REQ. Depending on the kind of advertisement packet, the RxAdd bit specifies whether the address is public (0x00) or random (0x01). Similar to TxAdd, but the opposite. It only occurs for the forms ADV_DIRECT_IND, SCAN_REQ, and CONNECT_REQ since the Initiator role does not apply to the other kinds.

If the ChSel, TxAdd, or RxAdd fields are not defined as being used in a particular PDU, they are

considered reserved for future use (RFU). The length of the payload in octets is indicated in the Length field of the advertising physical channel PDU header. The Length field must have a valid range of 1 to 255 octets.

The PDU Type field in the header of the advertising physical channel PDU indicates the PDU type as defined in Table 4.10, as well as which channel and PHYs the packet may appear on.

Table 4.10: BLE's Advertising Physical Channel PDU header's PDU Type field encoding.

PDU Type	PDU Name	Physical Channel	Permitted PHYs		
			LE 1M	LE 2M	LE Coded
0b0000	ADV_IND	Primary Advertising	X		
0b0001	ADV_DIRECT_IND	Primary Advertising	X		
0b0010	ADV_NONCONN_IND	Primary Advertising	X		
0b0011	SCAN_REQ	Primary Advertising	X		
	AUX_SCAN_REQ	Secondary Advertising	X	X	X
0b0100	SCAN_RSP	Primary Advertising	X		
0b0101	CONNECT_IND	Primary Advertising	X		
	AUX_CONNECT_REQ	Secondary Advertising	X	X	X
0b0110	ADV_SCAN_IND	Primary Advertising	X		
0b0111	ADV_EXT_IND	Primary Advertising	X		X
	AUX_ADV_IND	Secondary Advertising	X	X	X
	AUX_SCAN_RSP	Secondary Advertising	X	X	X
	AUX_SYNC_IND	Periodic	X	X	X
	AUX_CHAIN_IND	Secondary Advertising and Periodic	X	X	X
0b1000	AUX_CONNECT_RSP	Secondary Advertising	X	X	X
All other values	Reserved for future use				

4.4.3 BLE Security modes

Encryption and Authentication

Bluetooth LE uses the 128-bit Advanced Encryption Standard — Counter with CBC-MAC encryption standard (AES-CCM). Long-Term Keys (LTK) are used in this algorithm to produce a 128-bit "shared secret" key.

Bluetooth (LE) authentication is achieved by digitally signing data with the connection Signature Resolving Key (CSRK). After the Data PDU, the sending device inserts a signature. The CSRK is used by the recipient to verify the signature.

The Generic Access Protocol (GAP) defines two security mechanisms for BLE connections, each with many security levels.

Security Mode 1

Security Mode 1 has four layers and enforces security through encryption:

- **Security Level 1**: There is no security (no authentication and no encryption).

- **Security Level 2**: There is no authentication pairing with encryption.
- **Security Level 3**: There is authenticated pairing with AES-CCM encryption.
- **Security Level 4**: There is authenticated LE Secure Connections pairing with encryption. Elliptic Curve Diffie-Hellman P-256 (ECDH) and AES-CCM encryption are used at Level 4.

Each security level satisfies the standards of the ones below it (e.g. LE Security Mode 1 Level 4 satisfies the requirements for levels 1, 2, and 3.)

Security Mode 2

Data signing is used to enforce security in Security Mode 2, which has two levels:

- **Security Level 1**: There is no authentication pairing with data signing.
- **Security Level 2**: There is authenticated pairing with data signing.

Mixed Security Mode

Mixed Security Mode is used when a device must handle both Security Modes 1 and 2, i.e., signed and unsigned data. Secure Connection Only Mode is Secure Mode 1 with Security Level 4, which implies that all incoming and outgoing Bluetooth device traffic is encrypted and includes authorised connections.

Pairing Modes

Pairing requires verifying the identification of the two devices to be paired, which is usually achieved by sharing a secret. The link is encrypted after authentication, and keys are distributed to allow security to be reestablished considerably more quickly on a reconnection. The devices are considered to be *Bonded* if these keys are saved for a future use [77].

Chapter 5

Discussion of a Simple Proposed Protocol for Environment Sensing

5.1 General Aspects

A simple proprietary protocol will be discussed with the goal of reducing network energy consumption and management, for experimental use. This protocol will be developed into a wide range wireless sensor network for temperature and humidity monitoring in the environment. Applications of this system will include environmental and precision agriculture monitoring, as well as fire detection capability by tracking a sudden temperature increase over a certain threshold.

Network Topology

The main aim of this proposed protocol is to be capable of establishing communications between the sensor nodes (SNs) and base stations (BSs) in the most possible simplified network management, in order to reduce the communication overall energy consumption. The SNs will be powered by a button cell battery, which is intended to have a battery autonomy of 5 to 7 years. The addition of a mesh type (such as BLE mesh) would require data retransmission by sensor nodes, consuming more energy and demanding a more complex network management.

Therefore, there is a trade-off, and the one-to-many (1:m) star type network topology will be used, which means that each sensor node communicates only with the base station, as illustrated in Figure 5.1. Furthermore, communication is always initiated by the sensor node, never by the base station, which is always listening for SNs communications, since it is not so energy constrained. The SN measures temperature and humidity and stores the measurements in its internal memory. When the SN connects to the BS, it sends its stored measurements and clears its memory.

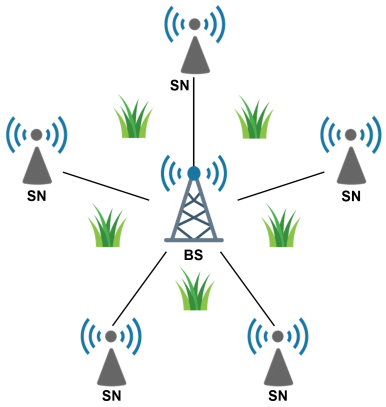


Figure 5.1: The one-to-many (1:m) star network topology to be used in the proposed protocol (this image was designed using resources from [3–5]).

Link Layer

The proprietary communication protocol will take into account the recommendations of Bluetooth Low Energy (BLE) standard version 4.0, due to its simplicity. Nevertheless, it will be further simplified and optimised for this specific WSN application, temperature and humidity environmental monitoring. The Link Layer has a simple packet format as illustrated in Figure 5.2. Its values are merely suggestions considering the values used in BLE. The Link layer has been greatly simplified for experimental purposes. However, because the radio is programmable, larger packages can be built if necessary.

Preamble (1 octet)	Access Address (4 octets)	Packet Payload (27 octets)	CRC (3 octets)

Figure 5.2: The packet format to be used in the Link Layer of the proposed protocol.

The first field is the Preamble, which is one octet long and is used by the demodulator to detect the beginning of a packet. The second field is the Access Address (AA), which is four octets long and is used to identify radio communications node on the physical link. The third field is the Packet Payload, which contains the payload, with a value of 27 octets. The last field of the transmitted packet is the Cyclic Redundancy Check (CRC), which is an error detection code used to detect unwanted changes in a packet. It ensures data integrity for all packets sent over the air.

Physical Layer

The SN's integrated circuit is constituted by a radio transceiver that operates in the 2.4 GHz Industrial Scientific Medical (ISM) band, and it employs ultra low power circuits with low leakage technology to achieve a greater autonomy. In addition, in terms of Physical Layer, the radio transceiver is compliant with BLE's specifications.

BLE was adopted because the modulation is simple to implement and it was possible to develop a demodulator that consumes very low energy, which only operates with GFSK modulation. Therefore,

in terms of hardware energy consumption, it was decided that BLE with this modulation and frequency would be most desirable.

For WSN communications, a subset of three BLE channels (Ch1, Low Frequency; Ch2, Mid Frequency; Ch3, High Frequency) will be used. The main objective of using three channels is not to communicate with multiple SNs at the same time, but to select the best propagation conditions for a particular communication. Table 5.1 contains an overview of the proposed protocol specifications.

Table 5.1: Specifications for the Simple Proposed Protocol.

Proposed Protocol	
Modulation	GFSK
Frequency	2.4 GHz ISM Band
Subset of Channels	Ch1: Low Frequency Ch2: Mid Frequency Ch3: High Frequency
Topology	Star (1:m)

5.2 First time installation of a Sensor Node

The first time a sensor node is installed, it must be rebooted in order to connect to the base station for the first time. The BS will recognise a new SN's first time communication since all SNs will have the same initial ID. Subsequently, the BS will provide and store a unique ID in the SN, which will be selected from a previously stored list. This ID might probably be the Access Address of the BLE protocol.

Furthermore, the BS will configure the SN's Real-Time Clock (RTC), establish a daily schedule for temperature and humidity measurements, as well as predefined time slots for transmitting the sensed data to the BS. Regular communications between each SN and BS occurs at a predefined and unique time slot.

Finally, once all SNs have been installed by the operator, the BS's list with the GPS coordinates of all SNs must be updated. This will be accomplished through the use of the BS's direct cable connection. The configuration of the BS requires a direct cable (USB type) connection. This method may be used to reconfigure the configuration parameters of SNs and BSs. Figure 5.3 shows the steps involved in setting up a sensor node for the first time.

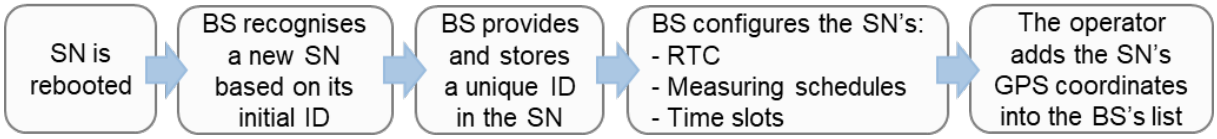


Figure 5.3: The procedures for the first time installation of a sensor node.

5.3 Regular communications

When an SN wishes to communicate, it shall first check the three predefined channels for the lack of communications. Although each SN has a predefined time slot, collisions may occur due to SN's RTC delays or advances, or radiation perturbations from other communication services.

In the event that the SN connects successfully with the BS, the SN shall restart its RTC, allowing it to schedule future time slots and compensate for the time difference. Additionally, after delivering its measurements, the SN shall clear its stored measurements.

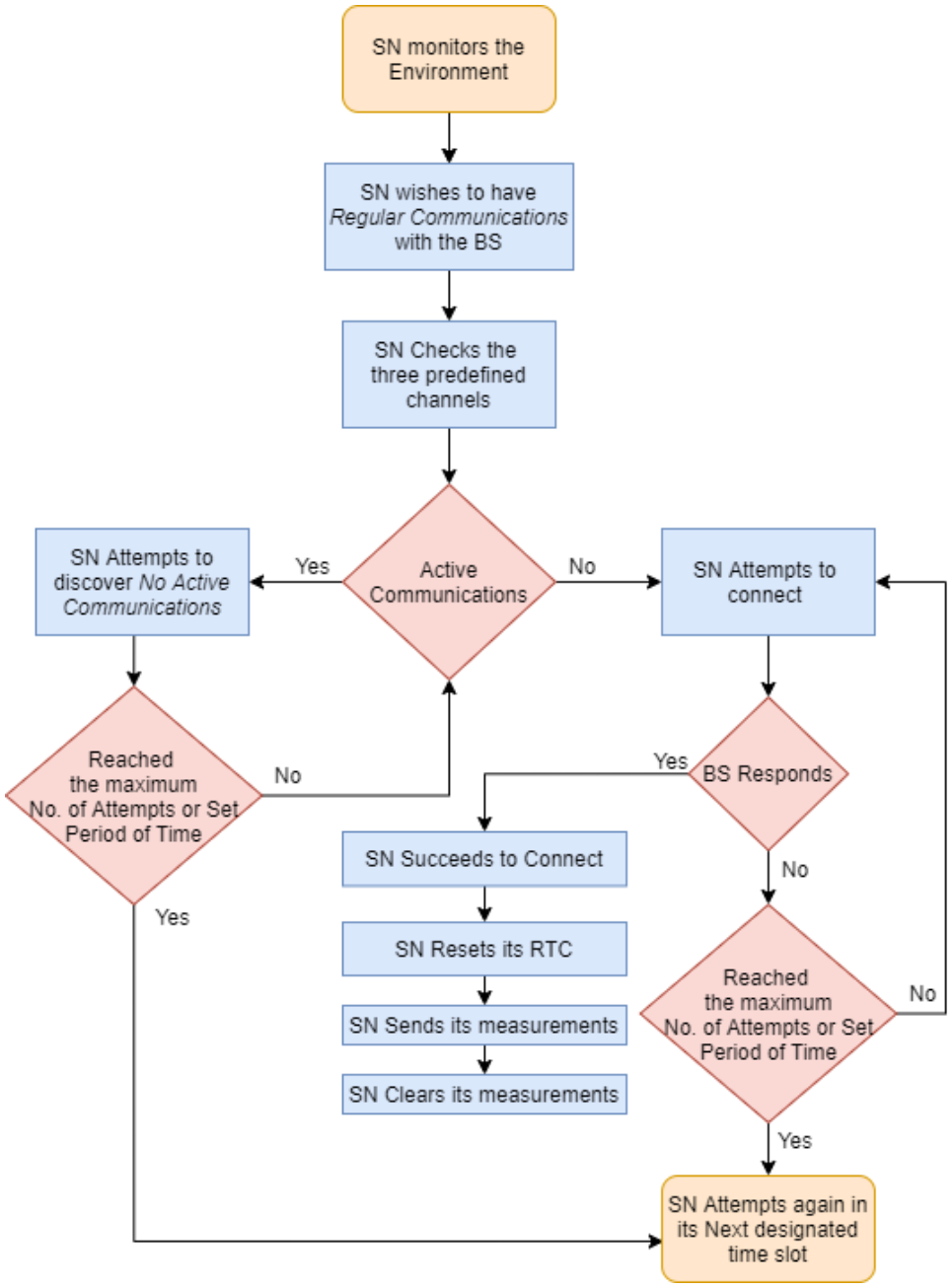


Figure 5.4: Flowchart describing the SN's decision process to establish regular communications with the BS.

Figure 5.4 represents a flowchart depicting the decision process that a SN must execute in order to

initiate regular communications with the BS.

No Active Communications

If there are *No Active Communications*, the SN attempts to contact the BS in the following order: Ch1, Ch2, and Ch3. The BS determines which channel to use based on the highest received power signal. The selected communication channel will be the one in which the BS replies.

- If the *BS does Not Respond*, a maximum predefined number of attempts will be performed by the SN over a set period of time.
- If the *SN Succeeds*, the previous description applies; if it does not, it will attempt again in its next available time slot.

Other Communications are Active

If *Other Communications are Active*, a maximum predefined number of attempts will be performed by the SN over a set period of time, in order to discover *No Active Communications*.

- In *case of Success*, the previous point applies.
- In *case of Lack of Success*, the SN will try again at its next available time slot.

Observations

- When communication efforts fail, there should be enough temporal separation (a short delay) between the time slots of surrounding sensors to prevent communication attempts from overlapping, so that the SNs communicate roughly at the same time, but not simultaneously. Figure 5.5 illustrates this observation. This spacing will also be determined by the number of sensors and the time it takes each one to transmit a signal.

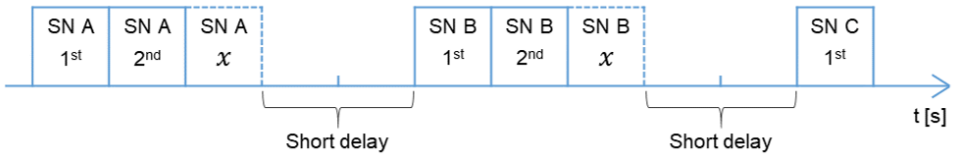


Figure 5.5: Representation of a short delay between the time slots of SNs to ensure that there is no overlapping between them in case of x attempted failed communications, x being the maximum number of attempts within a set period of time.

- If Low Energy Power Control (LEPC) is used, it will provide a method for SNs and BSs to alert each other when received signal strength is too high or too low, and request that the other adjust transmission power accordingly. This implies that a connection can be optimised, decreasing the need for retransmissions, reducing overall power consumption, and allowing applications to function more smoothly. This benefits both the involved SNs and BSs, as well as general 2.4 GHz

coexistence because by not over transmitting, there is less risk of interfering with other 2.4 GHz protocols, such as Wi-Fi.

5.4 Dealing with lost measurements

Depending on the SN's memory storage capacity there are two possible scenarios for lost measurements:

Accept Lost Measurements

In one scenario, if it is acceptable to lose measurements in the event of a failed attempt to connect with the BS, it is unnecessary for the SN to store them, as illustrated in Figure 5.6. Therefore, the SN will erase the old measurements and will only transmit the current ones in its next available time slot.

Under these circumstances, past measurements are lost and do not have a second chance to be delivered. Furthermore, there is no need for the SN's internal memory to be increased.

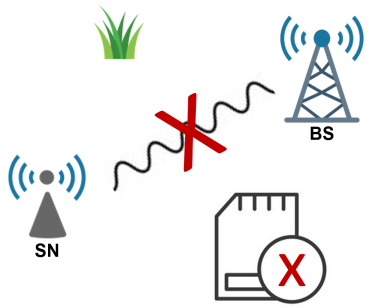


Figure 5.6: In case a SN is unable to connect to a BS, the measure it attempted to communicate will not be stored (this image was designed using resources from [3–5]).

Attempt to Recover Lost Measurements

In another scenario, in the case of a communication failure, the SN should store the failed transmitted measurements in its internal memory and attempt to send them along with the future ones in its next scheduled time slot, Figure 5.7 illustrates this scenario.

When it succeeds to connect with the BS, it should send the most recent measurements first, followed by the older ones. Since the SN missed its previous designated time slot, the base station will be able to analyse its data base and verify that this extra information is related to the previous observation that failed to communicate. This simple procedure would allow us to recover some old measurements that would be lost otherwise. However, it creates the necessity of storing more information in the SN, as well as increased transmission time and energy consumption. Moreover, in this scenario, the SN should have

a predetermined maximum number of previous measurements that it can store in its internal memory without compromising its memory space; otherwise, it would erase them.

Additionally, if the SN is capable of keeping a reference of the specific time slot that failed to transmit the measurements, it would be capable of storing multiple failed communications' measurements and send them to the BS. Furthermore, the BS would not have to determine whether or not the measurement is a previous lost measurement, because it had already been identified as such.

However, the possibility of failed delivered measurements still exists, and there should be a margin of error for missing measurements.

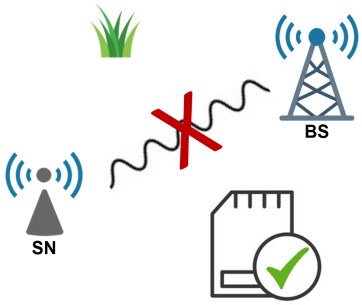


Figure 5.7: In case a SN is unable to connect to a BS, the measure it attempted to communicate will be stored (this image was designed using resources from [3–5]).

There should be a balance between memory and energy usage, for example, a SN may store several measurements and transmit them collectively at the end of the day. This procedure saves energy and requires more memory since it only transmits once rather than transmitting each measurement individually, during the day.

5.5 Sensor node failure or malfunctioning detection

Considering that the communication initiative always starts from the sensor node towards the base station, if a SN fails to communicate with the BS, after a significant period of time without communications or with failed communications, it is possible for the BS to detect a SN malfunction. The BS should then send an alert to the operator reporting this malfunction. Malfunctioning or communication failure can be caused by a variety of factors:

- One possible situation is radio interference, which is noise caused by other wireless transmissions on the same channel or on nearby channels, as illustrated in Figure 5.8. This interference may occur, but it will usually fade away quickly. However, if it persists for a long enough period of time, a failure alert can be triggered.
- Another possible scenario, would be an unexpected obstacle in the radio path, which blocks the communication signal for long enough to trigger a failure alert. For example, a vehicle in between

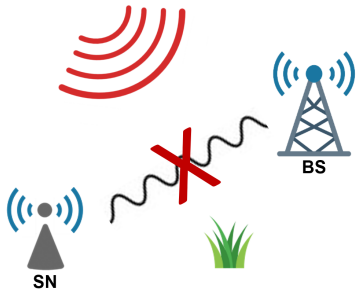


Figure 5.8: Other wireless communications on the same or nearby channels cause radio interference (this image was designed using resources from [3–5]).

the radio path, as depicted in Figure 5.9

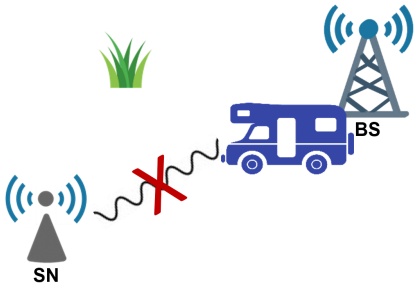


Figure 5.9: Unexpected obstacle in the sensor node's radio path to the base station, which blocks the communication signal (this image was designed using resources from [3–5]).

- Moreover, as seen in Figure 5.10, a hardware problem could disable communications, resulting in a malfunctioning alert.

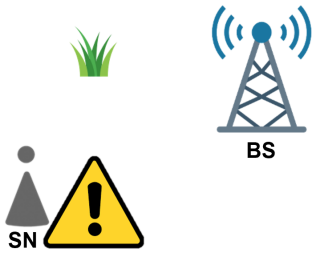


Figure 5.10: The sensor node has a hardware problem that prevents communications (this image was designed using resources from [3–5]).

- Ultimately, as shown in Figure 5.11, the SN will eventually run out of power and, as a result, it will be unable to communicate, resulting in a malfunctioning alert.

In the event that a SN's battery dies, an operator must be dispatched to the terrain to replace it with a new one. When the SN is again reactivated, its ID and location will remain the same, as it is stored both in the SN and the BS's data base.

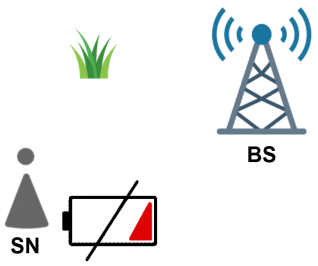


Figure 5.11: The sensor node does not have enough energy to transmit (this image was designed using resources from [3–5]).

In case a defective SN needs to be replaced due to a malfunctioning, there are specific requisites that must be addressed in order to replace it correctly:

- Firstly, removing the damaged SN does not delete its Access Address (AA) from the BS's data base. This could lead to false malfunctioning alerts as well as the waste of memory and available Access Addresses. If the faulty SN's AA remains in the BS, the BS would eventually detect that this AA has not established communication for a certain length of time, triggering an alert. Therefore, when removing the damaged SN, the operator must free its respective AA from the BS's data base.
- Secondly, a new SN is installed in the place of the defective SN. The BS will recognise this SN as a new one and assign it with a new AA, as explained in section 5.2. Nonetheless, the coordinates of this new SN must be provided to the BS.

5.6 Types of Data and information

After monitoring humidity and temperature, the SNs should communicate with the BS as soon as possible. This prevents storing and allows more free usage of the SN's internal memory. Furthermore, in the event of failed communications between the SN and the BS, it offers more time for future attempts of connecting. Additionally, it provides the operator with more up-to-date information about the environment.

Table 5.2 lists the different types of data and information that should be stored in a sensor node and a base station. If there is an effort to recover lost measurements, as discussed in section 5.4, two additional stored fields in the SN are used to store the humidity and temperature readings that failed to be transmitted.

Table 5.2: SN's and BS's stored data and information.

SN's Stored Data	BS's Stored Data
SN's ID	SNs' ID and GPS coordinates
Schedule for Temperature Measurement	Schedules and Data for SNs measurements
Schedule for Humidity Measurement	Schedules for SNs communications
Schedule for SN communication with BS schedule	Schedules for BS to WebS communications
Failed Temperature Measurement (if applied)	No. of a mobile phone for emergency SMSs
Failed Humidity Measurement (if applied)	

5.7 Software development and Web Server database

Software Development

The developed system must be able to receive messages containing sensed data, store them, and display the data via a web user interface.

Web Server database

There are primarily two scenarios in which the BS interacts with its Web Server database:

- **Normal conditions**

  Under normal circumstances, the BS shall send all new data from the SNs, along with the parameters and list of the SNs and BS, to the Web Server (WebS). This can be executed according to a daily schedule, which is configured in the BS. To save energy, it may, for example, communicate only once at the end of the day.

- **Emergency events**

  In the event of an emergency, the BS will send a short message service (SMS) to the operator and immediately transfer the reported alarm data to the WebS, where the operator may examine and further evaluate it. This emergency event procedure is illustrated in Figure 5.14.

5.8 Precision Agriculture

In order to apply this protocol to a WSN for precision agriculture, sensor nodes must be strategically deployed over a field to monitor humidity and temperature. Based on the sensed information provided by the SNs, farmers will be able to evaluate and determine how to manage their crops, such as the optimal time of day to irrigate the fields. Furthermore, this collected data helps to analyse and have a better understanding of the impact of climate change in this area. Figure 5.12 depicts the two previously discussed advantages.

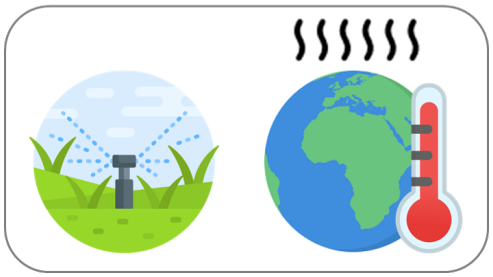


Figure 5.12: The data from the sensor nodes allows researchers to estimate the best time to irrigate fields and the influence of climate change in the area (this image was designed using resources from [3–5]).

Depending on the type of crop and the climate of the region in which it is deployed, a sensor node could monitor humidity and temperature more or less frequently, as illustrated in Figure 5.13. It might also be worthwhile to reconfigure the SNs for a specific time of year in order to extend the device's lifetime by measuring more or less frequently. In Portugal, for example, monitoring humidity and temperature more often throughout the summer is particularly important, due to the shortage of water resources and the increased risk of fire. On the other hand, it would not be necessary to monitor as often during the winter season.

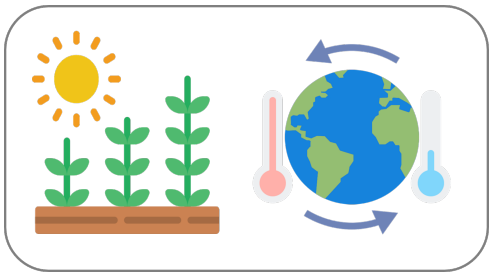


Figure 5.13: Depending on the crops and the seasons, the sensor nodes could be programmed to monitor more or less frequently (this image was designed using resources from [3–5]).

5.9 Fire Detection and Emergency Communications

To implement this proposed protocol in a WSN for fire detection, sensor nodes must be strategically placed throughout the forest to detect fires efficiently. The SNs must constantly monitor the temperature, and if it exceeds a certain temperature threshold, it is an indicator that a fire is starting. This temperature threshold should be high enough to prevent false detection, such as the SN overheating due to the UV radiation from the Sun. Therefore, the SN should be strategically placed, for example on a tree's trunk, where it will be covered by the tree canopy and thus avoid the problem of overheating.

If a sensor node detects a temperature above the predefined threshold, it must promptly establish an *Emergency Communication* with the base station to report it, as explained in the flowchart depicted in Figure 5.15. The respective emergency communication package will include a *flag* to differentiate between an emergency event and a regular communication, so that the BS can prioritise and manage it immediately. Furthermore, in order to help confirm the emergency event, the SN must measure an additional maximum number of consecutive readings and transmit the results to the BS.

On the other hand, the base station must then send an SMS message to a predefined mobile phone informing the Operator of the alert, and transfer the data that triggered the emergency event to the Web Servers. This allows the operator to be quickly notified of an alert and to have an up-to-date information to further analyse and evaluate the emergency situation.

If a different SN also detects this fire alert, there are less doubts that there is a fire. Given the position of the SNs, it will be possible to predict where the fire is spreading. Additionally, by taking into account the time delay between the SNs' alerts and their respective coordinates, it is possible to estimate the distance the fire has spread and its propagation velocity, as portrayed in Figure 5.14.

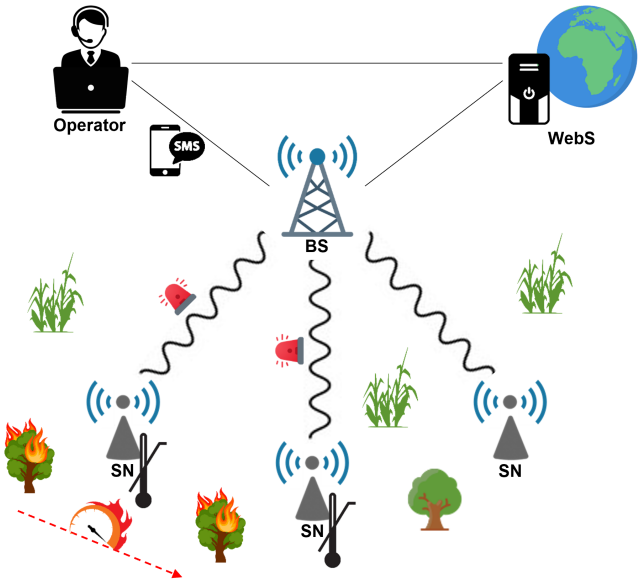


Figure 5.14: In case a sensor node detects an above threshold temperature, the Emergency Communications procedure will be adopted. If another sensor node reports the fire, it is possible to estimate the fire spread and its propagation velocity (this image was designed using resources from [3–5]).

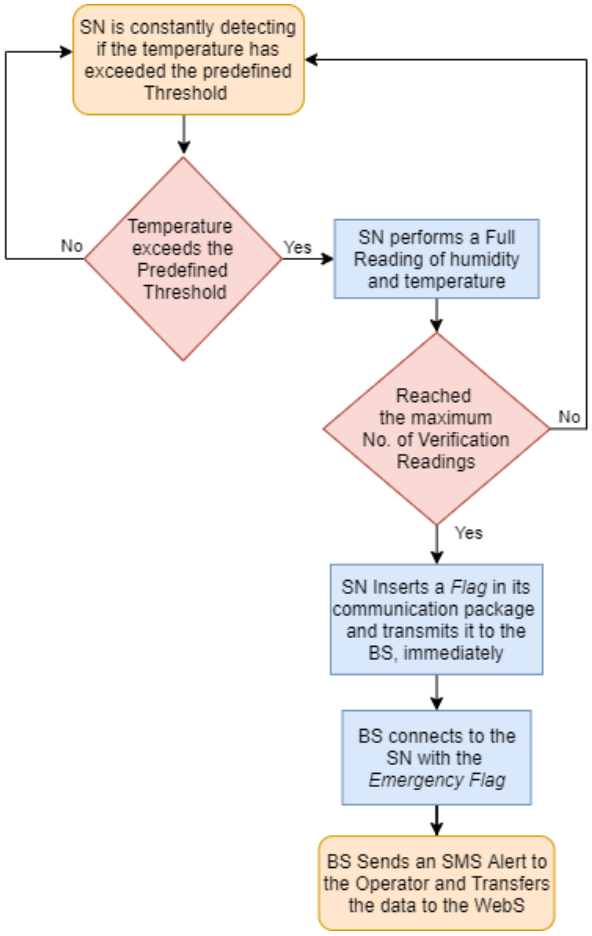


Figure 5.15: Flowchart describing the SN's decision process to establish Emergency Communications with the BS.

Although all developed sensor nodes are identical and continuously measure temperature, the ability to configure two classes of SN would allow the device to save energy and extend its life:

- *Precision Agriculture SN*: The SN is constantly detecting if the temperature has exceeded the predefined threshold, allowing it to detect a fire. Furthermore, it conducts several predefined daily temperature and humidity measurements, which are then communicated to the base station within its designated time slots.
- *Fire Detection SN*: The SN is constantly detecting if the temperature has exceeded the predefined threshold, allowing it to detect a fire. However, in contrast to the previous SN class, it will not conduct multiple daily temperature and humidity measurements and transmissions. It will perform a few daily temperature and humidity readings that will be transmitted to the base station within its designated time slots, merely to indicate that it is active and functioning properly. This will allow the SN to save more energy and extend its life.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

The first objective of this thesis was to conduct a study of open standards for wireless sensor networks in order to help electronic circuit design researches. Chapter 2 introduces the realm of wireless sensor networks, including design challenges and applications. Furthermore, it contains a comprehensive description of each technology, resulting in a document that provides an overview of the most well known open standards for WSN, thus the first objective of the thesis was achieved.

The final goal is to discuss a simple protocol to be applied in a wireless sensor network with a star topology for environmental monitoring. This proposed protocol should be energy efficient, easy to implement and manage, with the objective of being used to test in the field the sensor nodes and the base station developed by the researchers. Their aim is to demonstrate that the radio communication system they designed consumes very little energy.

To accomplish this, the ZigBee and Bluetooth Low Energy protocols were studied in further depth in Chapter 3 and Chapter 4, respectively. In order to better comprehend the functioning of these successful and similar protocols.

Through this approach, it became clear that BLE provided a better solution for the devices developed by the research team, because BLE's modulation allows the radio architecture and the demodulator developed by the researchers to consume less energy. Therefore, in light of this conclusion, the proposed protocol would be based on Bluetooth Low Energy standard version 4.0, due to its simplicity.

Finally, a simple proprietary protocol for experimental use was discussed with the goal of reducing network energy consumption and simplify management. The discussion focused in being applied to monitor temperature and humidity in order to be used for precision agriculture, as well as being capable of fire detection by reporting a temperature above a certain threshold.

After an overview and in depth study of open standards for wireless sensor networks, it was possible to develop a manual to assist researchers and provide contributions for an efficient and simple proprietary protocol for wireless sensor networks for environmental monitoring. Overall, the project was concluded with its main objectives fulfilled.

6.2 Future Work

This thesis took place within an ongoing project. As such, the previously mentioned suggestions, and possible other advances, are expected to be implemented in order to improve the protocol and the devices that researchers are currently developing.

The proposed protocol should also be revised and refined in future studies, searching for a better solution to manage the sensor nodes' RTC.

Finally, future work should include further investigation in energy saving methods to maximise the battery life of sensor nodes. It might be of particular interest to investigate other typologies and algorithms that enhance coverage and provide greater network flexibility, security and reliability to the wireless sensor networks.

Bibliography

[1] M. A. Matin and M. M. Islam. Overview of Wireless Sensor Network Security Technology. pages 3–24, 2012. doi: 10.25236/iceeecs.2018.096.

[2] C. Gomez, J. Paradells, and J. E. Caballero. *Sensors Everywhere: Wireless Network Technologies and Solutions*. Number January 2010. 2010. ISBN 9788493474058. URL `http://www.fundacion.vodafone.es/PortalVodafone/static/fichero/pre_ucm_mgmt_002618.pdf`.

[3] Icons8. Icons, illustrations, photos, music, and design tools. `https://icons8.com/`, September 2021. This image has been designed using resources from icon8.com.

[4] Flaticon. Access +5.6m vector icons and stickers. `https://www.flaticon.com/`, September 2021. This image has been designed using resources from Flaticon.com.

[5] Clipartmax. Millions of clipart image, unlimited download for free! `https://www.clipartmax.com/`, September 2021. This image has been designed using resources from Clipartmax.com.

[6] M. F. Othman and K. Shazali. Wireless sensor network applications: A study in environment monitoring system. *Procedia Engineering*, 41:1204–1210, 2012. ISSN 18777058. doi: 10.1016/j.proeng.2012.07.302.

[7] A. Chandrakasan, R. Amirtharajah, S. H. Cho, J. Goodman, G. Konduri, J. Kulik, W. Rabiner, and A. Wang. Design considerations for distributed microsensor systems. *Proceedings of the Custom Integrated Circuits Conference*, pages 279–286, 1999. ISSN 08865930. doi: 10.1109/cicc.1999.777291.

[8] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras. Applications of wireless sensor networks: An up-to-date survey. *Applied System Innovation*, 3(1):1–24, 2020. ISSN 25715577. doi: 10.3390/asi3010014.

[9] U. Raza, P. Kulkarni, and M. Sooriyabandara. Low Power Wide Area Networks: An Overview. *IEEE Communications Surveys and Tutorials*, 19(2):855–873, 2017. ISSN 1553877X. doi: 10.1109/COMST.2017.2652320.

[10] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. *Computer Networks*, 38(4):393–422, 2002. ISSN 13891286. doi: 10.1016/S1389-1286(01)00302-4.

[11] K. Eghonghon Ukhurebor, I. Odesanya, S. Soo Tyokighir, R. George Kerry, A. Samson Olayinka, and A. Oluwafemi Bobadoye. *Wireless Sensor Networks: Applications and Challenges*. IntechOpen, London, UK, 2020. doi: 10.5772/intechopen.93660.

[12] C. S. Alliance. Why standards. https://zigbeealliance.org/why-standards/, May 2021. Consulted in May 2021.

[13] IEEE. About ieee. https://www.ieee.org/about/index.html, April 2021. Consulted in April 2021.

[14] A. S. Bhosle and L. M. Gavhane. Forest disaster management with wireless sensor network. *International Conference on Electrical, Electronics, and Optimization Techniques, ICEEOT 2016*, pages 287–289, 2016. doi: 10.1109/ICEEOT.2016.7755194.

[15] IETF. About. https://www.ietf.org/about/, April 2021. Consulted in April 2021.

[16] IETF. Ipv6 over low power wpan (6lowpan). https://datatracker.ietf.org/wg/6lowpan/charter/, April 2021. Consulted in April 2021.

[17] IETF. Routing over low power and lossy networks (roll). https://datatracker.ietf.org/wg/roll/charter/, April 2021. Consulted in April 2021.

[18] IETF. Constrained restful environments (core). https://datatracker.ietf.org/wg/core/about/, April 2021. Consulted in April 2021.

[19] ITU. About international telecommunication union (itu). https://www.itu.int/en/about/Pages/default.aspx, March 2021. Consulted in March 2021.

[20] Z. Tafa. Ubiquitous Sensor Networks. 4(4):267–268, 2011. doi: 10.1007/978-1-84996-510-1_13.

[21] ITU-T. Applications of Wireless Sensor Networks in Next Generation Networks. *Series T.2000: Next Generation Networks*, pages 1–94, 2014.

[22] ISO. Iso. https://www.iso.org/the-iso-story.html, April 2021. Consulted in April 2021.

[23] IEC. What we do. https://www.iec.ch/what-we-do, March 2021. Consulted in March 2021.

[24] I. J. W. 7. Liaison statement from jtc 1/wg 7 to other organizations. https://www.ietf.org/lib/dt/documents/LIAISON/file971.pdf, April 2021. Consulted in April 2021.

[25] ETSI. Internet of things (iot). https://www.etsi.org/technologies/internet-of-things, March 2021. Consulted in March 2021.

[26] T. M. Workgroup. A technical overview of LoRa ® and LoRaWAN ™ What is it? 2015. URL https://lora-alliance.org/resource-hub/what-lorawantm.

[27] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J. C. Prévotet. Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility. *IEEE*

Communications Surveys and Tutorials, 21(2):1561–1581, 2019. ISSN 1553877X. doi: 10.1109/COMST.2018.2877382.

[28] L. Inteligente. Lora - a nova rede de lisboa. https://lisboainteligente.cm-lisboa.pt/lxi-noticias/lora-a-nova-rede-de-lisboa/, Dezembro 2020. Consulted in March 2021.

[29] D. ALLIANCE. Dash7 alliance protocol. https://dash7-alliance.org/, March 2021. Consulted in March 2021.

[30] M. Weyn, G. Ergeerts, R. Berkvens, B. Wojciechowski, and Y. Tabakov. DASH7 alliance protocol 1.0: Low-power, mid-range sensor and actuator communication. *2015 IEEE Conference on Standards for Communications and Networking, CSCN 2015*, pages 54–59, 2016. doi: 10.1109/CSCN.2015.7390420.

[31] B. Buurman, J. Kamruzzaman, G. Karmakar, and S. Islam. Low-Power Wide-Area Networks: Design Goals, Architecture, Suitability to Use Cases and Research Challenges. *IEEE Access*, 8: 17179–17220, 2020. ISSN 21693536. doi: 10.1109/ACCESS.2020.2968057.

[32] W. Ayoub, F. Nouvel, A. E. Samhat, W. Ayoub, F. Nouvel, A. E. Samhat, J.-c. Prévotet, M. Mroue, W. Ayoub, F. Nouvel, A. E. Samhat, and J.-c. Pr. Overview and Measurement of Mobility in DASH7 To cite this version : HAL Id : hal-01991725 Overview and Measurement of Mobility in DASH7. Technical report, 2018.

[33] B. Ray. What is weightless? https://www.link-labs.com/blog/what-is-weightles, November 2015. Consulted in April 2021.

[34] J. Finnegan and S. Brown. A Comparative Survey of LPWA Networking. 2018. URL http://arxiv.org/abs/1802.04222.

[35] O. C.I.C. Weightless specification. https://www.openweightless.org/, April 2021. Consulted in April 2021.

[36] U. Raza, P. Kulkarni, and M. Sooriyabandara. Low Power Wide Area Networks: An Overview. *IEEE Communications Surveys and Tutorials*, 19(2):855–873, 2017. ISSN 1553877X. doi: 10.1109/COMST.2017.2652320.

[37] I. Blair, A. Fell, Z. Fu, P. Amyas, F. Petitgrand, D. Smith, P. Smith, K. Wang, W. Webb, S. Wenham, and Farsite. Weightless-P System specification, 2017. URL https://pro-bee-user-content-eu-west-1.s3.amazonaws.com/public/users/Integrators/929cb090-e779-401a-b06c-c629ff6b0fea/ap-cambridgestartuplimi/Weightless-P_v1.03.pdf.

[38] E. Kail, A. Banati, E. Laszlo, and M. Kozlovszky. Security survey of dedicated iot networks in the unlicensed ISM bands. *SACI 2018 - IEEE 12th International Symposium on Applied Computational Intelligence and Informatics, Proceedings*, pages 449–453, 2018. doi: 10.1109/SACI.2018.8440945.

[39] O. C.I.C. Weightless tech now shipping to customers in 20 countries. https://www.businessweekly.co.uk/news/hi-tech/weightless-tech-now-shipping-customers-20-countries, September 2017. Consulted in April 2021.

[40] C. S. Alliance. Our members. https://zigbeealliance.org/members/, March 2020. Consulted in June 2021.

[41] C. S. Alliance. Zigbee faq. https://zigbeealliance.org/zigbee-faq/, May 2021. Consulted in May 2021.

[42] I. Bluetooth SIG. Learn about the history of and people behind the bluetooth sig. https://www.bluetooth.com/about-us/, June 2021. Consulted in June 2021.

[43] I. Bluetooth SIG. Bluetooth technology overview. https://www.bluetooth.com/learn-about-bluetooth/tech-overview/, June 2021. Consulted in June 2021.

[44] K. Shahzad and B. Oelmann. A comparative study of in-sensor processing vs. raw data transmission using ZigBee, BLE and Wi-Fi for data intensive monitoring applications. *2014 11th International Symposium on Wireless Communications Systems, ISWCS 2014 - Proceedings*, pages 519–524, 2014. doi: 10.1109/ISWCS.2014.6933409.

[45] S. Maurya and N. Barwar. Performance Evaluation of AODV and DSDV Routing Protocols over Zigbee Network for Different Topologies under CBR Traffic Pattern. *International Journal of Computer Applications*, 124(11):5–12, 2015. doi: 10.5120/ijca2015905640.

[46] J. Adams and B. Heile. Busy as a zigbee. https://spectrum.ieee.org/computing/networks/busy-as-a-zigbee, October 2006. Consulted in May 2021.

[47] A. Chaudhary, J. Rusia, K. Gourav, P. Tripathi, J. Pandey, S. Majumdar, A. Naugarhiya, B. Acharya, S. Majumder, and S. Verma. Design and simulation of physical layer blocks of ZigBee transmitter. *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017*, pages 347–351, 2017. doi: 10.1109/I-SMAC.2017.8058369.

[48] IEEE Computer Society. IEEE Std 802.15.4-2015 - IEEE standard for low-rate wireless networks (Revision of IEEE Std 802.15.4-2011). *IEEE Standards Associations*, 2015:1–708, 2015.

[49] K. Javed. ZigBee suitability for Wireless Sensor Networks in Logistic Telemetry Applications. Master's thesis, School of Information Science, Halmstad University, 2006.

[50] S. Farahani. *ZigBee Basics*. ELSEVIER SCIENCE & TECHNOLOGY, 2008. ISBN 9780750683937.

[51] A. Cunha, A. Koubâa, R. Severino, and M. Alves. Open-ZB: An open-source implementation of the IEEE 802.15.4/ZigBee protocol stack on TinyOS. *2007 IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems, MASS*, (1), 2007. doi: 10.1109/MOBHOC.2007.4428602.

[52] M. Properties and H. O. Mucosa. Technical Report : Technical Report :. (July):2–3, 2015.

[53] Z. Alliance. ZigBee Specificarion. *Standard, Oct*, 2015. ISSN 0040-8905. URL http://ieeexplore.ieee.org/document/6264290/.

[54] ITU. Impact of industrial, scientific and medical (ism) equipment on radiocommunication services. https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-SM.2180-2010-PDF-E.pdf, May 2010. Consulted in May 2021.

[55] N. S. Bhat. Design and Implementation of IEEE 802.15.4 Mac Protocol on FPGA. pages 4–8, 2012. URL http://arxiv.org/abs/1203.2167.

[56] Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. *Computer Communications*, 30(7):1655–1695, 2007. ISSN 01403664.

[57] B. Rothke. A look at the Advanced Encryption Standard (AES). *Information Security Management Handbook, Sixth Edition*, pages 1151–1158, 2007. doi: 10.1201/9781439833032.ch89.

[58] S. Dağtaş, G. Pekhteryev, Z. Şahinoğlu, H. Çam, and N. Challa. Real-time and secure wireless health monitoring. *International Journal of Telemedicine and Applications*, 2008, 2008. ISSN 16876415. doi: 10.1155/2008/135808.

[59] B. S. I. G. (SIG). Bluetooth Core Specification Addendum. *Bluetooth SIG*, (July), 2012.

[60] O. Pc. The basic concepts of bluetooth low energy (ble) for beginner. https://pcng.medium.com/the-basic-concepts-of-bluetooth-low-energy-ble-for-beginner-c0fe062190c5, September 2019. Consulted in June 2021.

[61] E. L. S.A.U. Ble. https://www.elt.es/en/ble, March 2021. Consulted in June 2021.

[62] J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby, and C. Gomez. IPv6 over BLUETOOTH(R) Low Energy. *Request for Comments*, pages 1–21, 2015. URL http://www.rfc-editor.org/info/rfc7668.txt.pdf.

[63] I. Bluetooth SIG. About us. https://www.novelbits.io/bluetooth-version-5-2-le-audio/, April 2021. Consulted in June 2021.

[64] P. Di Marco, R. Chirikov, P. Amin, and F. Militano. Coverage analysis of Bluetooth low energy and IEEE 802.11ah for office scenario. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, 2015-Decem:2283–2287, 2015. doi: 10.1109/PIMRC.2015.7343678.

[65] M. Afaneh. The ultimate guide to what's new in bluetooth version 5.2. https://www.novelbits.io/bluetooth-version-5-2-le-audio/, March 2020. Consulted in June 2021.

[66] R. Tabish, A. Ben Mnaouer, F. Touati, and A. M. Ghaleb. A comparative analysis of BLE and 6LoWPAN for U-HealthCare applications. *2013 7th IEEE GCC Conference and Exhibition, GCC 2013*, pages 286–291, 2013. doi: 10.1109/IEEEGCC.2013.6705791.

[67] C. Gomez, J. Oller, and J. Paradells. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors (Switzerland)*, 12(9):11734–11753, 2012. ISSN 14248220. doi: 10.3390/s120911734.

[68] B. SIG. Higher speed how fast can it be? https://www.bluetooth.com/blog/exploring-bluetooth-5-how-fast-can-it-be/, July 2021. Consulted in July 2021.

[69] A. Nikoukar, S. Raza, A. Poole, M. Gunes, and B. Dezfouli. Low-power wireless for the internet of things: Standards and applications. *IEEE Access*, 6:67893–67926, 2018. ISSN 21693536. doi: 10.1109/ACCESS.2018.2879189.

[70] I. Bluetooth SIG. Exploring bluetooth 5 – going the distance. https://www.bluetooth.com/blog/exploring-bluetooth-5-going-the-distance/, June 2021. Consulted in June 2021.

[71] B. Badihi, M. U. Sheikh, K. Ruttik, and R. Jantti. On performance evaluation of BLE 5 in indoor environment: An experimental study. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, 2020-August:3–7, 2020. doi: 10.1109/PIMRC48278.2020.9217132.

[72] S. I. G. Bluetooth. Bluetooth Core Specification Version 5.2. *Specification of the Bluetooth System*, 0(December), 2019.

[73] K. E. Jeon, J. She, P. Soonsawad, and P. C. Ng. BLE Beacons for Internet of Things Applications: Survey, Challenges, and Opportunities. *IEEE Internet of Things Journal*, 5(2):811–828, 2018. ISSN 23274662. doi: 10.1109/JIOT.2017.2788449.

[74] MathWorks. What is bluetooth? https://fr.mathworks.com/help/comm/ug/what-is-bluetooth.html#mw_c69b719e-7a55-4680-b0b9-6b251a0d981c, June 2021. Consulted in June 2021.

[75] M. Electronics. Bluetooth 5: Mesh networking, greater range, and ability to coexist offer potential for iot and iiot applications. https://pt.mouser.com/applications/bluetooth-5-mesh-networking-standard/, June 2021. Consulted in June 2021.

[76] S. M. Song and W. J. Yao. Research on the Application Value of Wireless Mesh Network in Power Equipment of the UPIOT. *Journal of Physics: Conference Series*, 1346(1):0–8, 2019. ISSN 17426596. doi: 10.1088/1742-6596/1346/1/012046.

[77] A. Duque. Deep dive into bluetooth le security. https://medium.com/rtone-iot-security/deep-dive-into-bluetooth-le-security-d2301d640bfc, June 2021. Consulted in June 2021.