POLITECNICO DI TORINO

DIPARTIMENTO DI INGEGNERIA MECCANICA E AEROSPAZIALE (DIMEAS)

Master of Science in Biomedical Engineering

Study of low power wireless protocols for event-driven sEMG acquisition systems

Supervisor:

Danilo Demarchi

Paolo Motto Ros

Candidate:

La Piscopia Marika,240118

Academic Year 2018 – 2019

Contents

List of Figures

List of Tables

Abstract

Nowadays smart healthcare constitutes an active field of research that offers the potential of great improvement in the delivery and monitoring of healthcare. The expansion of this sector is supported by the recent development of sensors and embedded systems, wearable and easily integrated into everyday life. New higher performances wireless technologies have empowered the development of Wireless Body Area Networks (WBANs) as the link between different devices placed on the human body offering constant monitoring of relevant parameters without posing constraints on normal daily life activities.

This master thesis project aims to analyse and characterize performances and peculiarity of different wireless protocols to manage the event drive data transfer from an acquisition board to a host station, in which these will be processed. The real-time transmission of digital events generated from the acquisition of biomedical signals like sEMG (surface Electromyography) was investigated with the Average Threshold Crossing (ATC) technique. This methodology allows a low power acquisition due to high reduction in the data size, and to the entire circuitry complexity. The ATC event driven technique in facts registers for a new event each time the signal overcomes a threshold.

The hardware selected for the implementation is a Multi-Protocol System-on-Chip (SoC) with low power consumption to maximize application energy efficiency and battery life. It is a highly flexible single-chip solution for short-range wireless applications adopting one between Bluetooth Low Energy (BLE), ANT, Bluetooth Mesh, Bluetooth 5.0, IEEE 802.15.4, Thread or ZigBee protocol stack to transfer packets among the devices in the network. The setup consists of a specific WBAN composed by one client's and one server's board to test each wireless protocol.

The performances of the network have been assessed in terms of average current consumption, latency and event rate between the delivered and received packet. About current consumption, BLE and Ant showed extremely good results with an average

current peak of about 1mA. Taking into account the latency ANT and Thread have values around 5 ms for the higher data rate even if the second one has a standard deviation of that measure really close to zero. Considering the event data rate transmission promising result have been reached with BLE and Thread with at least 200 events per second. From an overall perspective the most promising protocols for an event driven sEMG acquisition system are BLE for the extremely low energy demand and Thread for the effective latency of few milliseconds at the upper data rate.

Chapter 1

Introduction

The center of this work is the use of the nRF52840 board a fully multi-protocol SoC. It has support for Bluetooth 5, Bluetooth mesh, Thread, Zigbee, 802.15.4, ANT and 2.4 GHz proprietary stacks. This chapter is an overview of all them in order to evaluated the best for performances like the power consumption and latency , as the time slot period between a data from the sensor node on the patient reaches the other node like ad example the pc for the post-processing of the signal. Different bio-applications in fact begin to use wireless transmission for different purposes like the signals acquisition (ECG, EMG and more others), prosthesis and exoskeleton control (for lower and upper extremities) and multiple data management (WBAN system).

Each communication standard was analyzed , coupled with event transmission technique applied to the sEMG signal in order to evaluate pro and cons into wireless transmission application for wearable sensor .

1.1 Biomedical signal

A signal is defined as a quantity of various nature (for example, electrical, mechanical, acoustic) which can vary over time and in space describing a phenomena and carrying information about the source that generated it. In Biomedical application the signal are generated by the human body giving the possibility to understand some complex mechanisms that take place in it. Are examples of biomedical signals the ECG (see Figure 1.1), EMG (see Figure1.2),evocated potentials and so on.

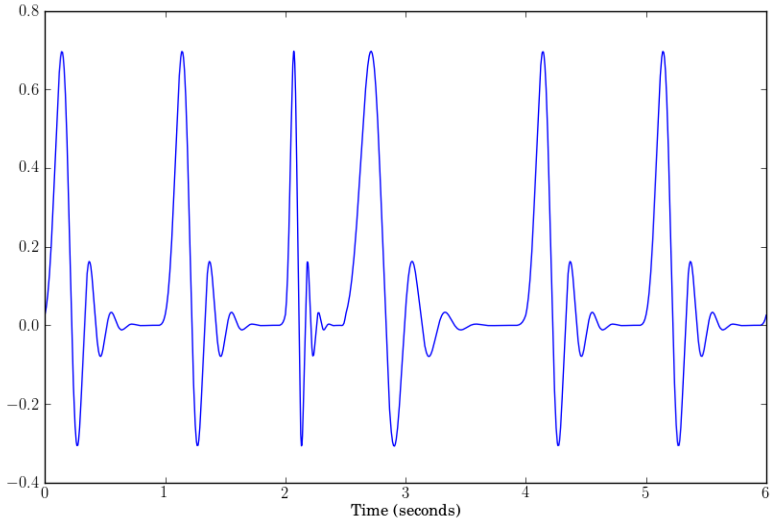

Figure 1.1: ECG signal [2].

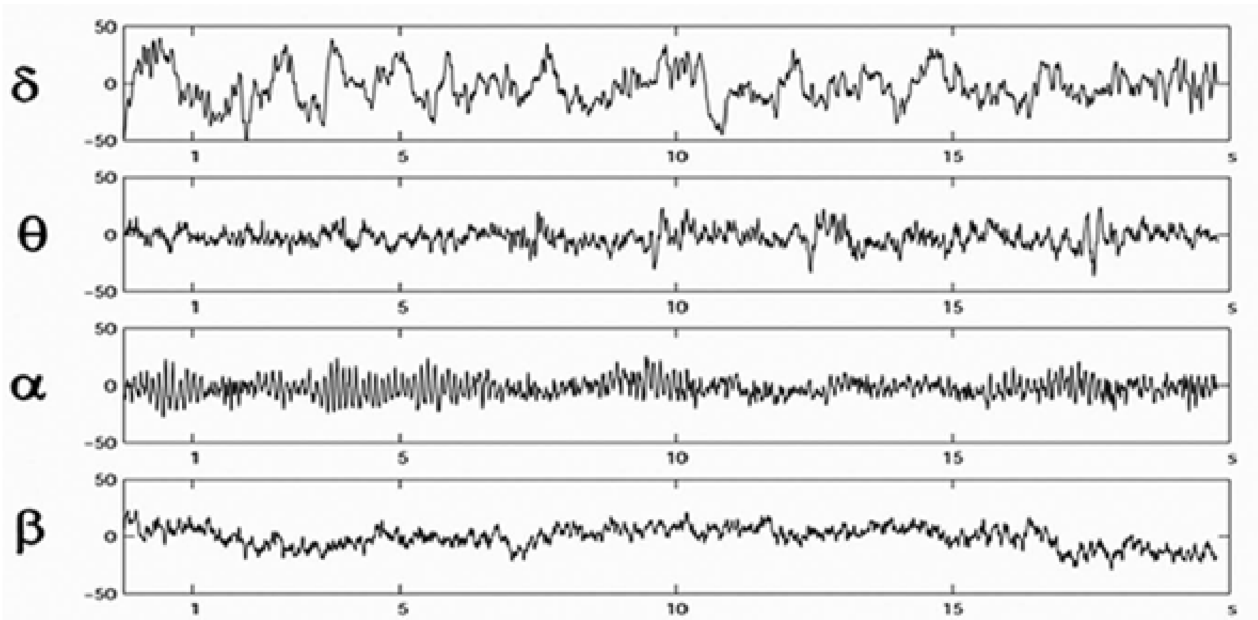

Figure 1.2: EEG signal [3].

A signal can be always represented as function of one or more independent variables. It is a common convention to consider time as the variable independent of the mathematical representation of a one-dimensional signal .The independent variable can be defined in a continuous set (continuous signal) or in a discrete set (discrete signal). The cases in which the independent variable is time we speak of signals continuous over time and discrete signals over time. If, in addition to the independent variable, the signal value is also defined in a discrete set, we say that the signal is numeric. If both are defined in a continuous set, the signal is called analog. Similarly, for systems dedicated to signal processing, they are analog systems and digital systems.

For biomedical signals there are some important steps before we can study it :

- Acquisition : the signal is recorded with a transducer or sensor and opportunely filtered and amplified to reduce the different causes of noises (movement artifacts , 50 Hz interference , ecc.) and set the right amplitude. The signal is now converted from analog to digital form with a dc/dc converter and transferred to a suitable support for subsequent processing, pc.

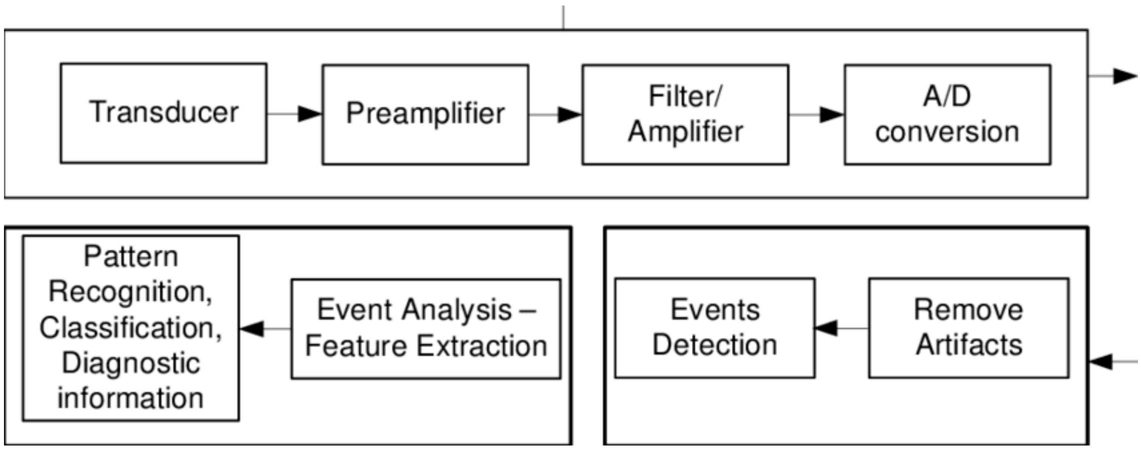

Figure 1.3: Biomedical signal acquisition procedure [4].

- Elaboration : all the techniques useful to extract features from the data. The signals are analyses in different way : time domain analysis ,in frequency or the creation of model to better understand the mechanisms that generated it.

- Interpretation : here there is the interpretation of the previous results to associate them to the real physiological meaning that they assume.

1.2 ATC Technique

The need to manage, transfer and process signals, particularly in biomedical application has as a direct consequence to take account of an increase number of data. The analog signal in fact, as said before is sampled periodically using an analog to digital converter (ADC). However,in the last few years researchers [6, 7] adopted an other kind of approach known as Event Driven sampling. In this case there is a sample every time a specific kind of event occurs for example like a signal overcomes a specif value. Therefore the Average Threshold Crossing technique (ATC) shows a good solution in order to reduce the amount of data to manage and consequently also the circuit complexity and the power consumption. This two aspects are really very important nowadays to implement a new generation of wearable devices for biomedical applications were there is the need to use a low power source and silicon surface for the chip to avoid limiting patient movements.

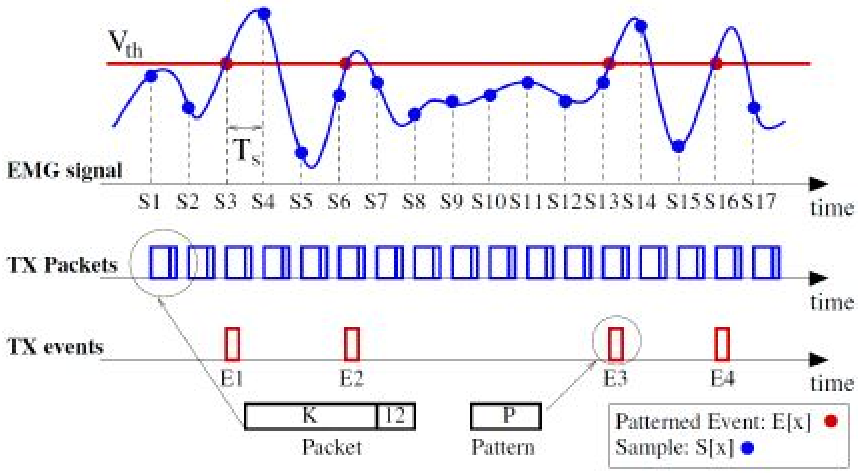

Figure 1.4: Average Threshold Crossing (ATC) technique [5].

In figure 1.4, is represented an overview of this technique applied to the EMG signal;every time it exceeds a fixed threshold the system records an event. As a result from all the events collected the Threshold Crossing (TC) signal is obtained; only time information loosing the real signal amplitude.This technique has some pro and cons. The loos of samples for some applications is not a problem and in this way there is a real reduction in the number of data to compute , the memory of the hardware is smaller and the complex speed of the system is further . All those things give the possibility to have a longer life cycle for the battery. This aspects has stated before is very important for biomedical application; for the patient this means more security to have a reliable life-saving tool and to not repeat the same surgery in a too short period for that sensor have to be implanted in the human body,like for example pacemaker and defibrillator. On the other hand the reduction of information of the real biomedical signal could run into the problem to have no so many features in order to understand the pathology the patient is involved in as so to put in place the correct diagnosis and therapy for him.

1.3 Bluetooth Low Energy

1.3.1 Overview

Bluetooth Low Energy (BLE), usually know also as Bluetooth Smart configures itself as wireless personal area network technology furnished by Bluetooth Special Interest Group (Bluetooth SIG) directed at different kind of applications like health care [9] ,fitness,beacons [8, 10] for the home entertainment industry and for the automotive and automation industries. From the beginning,focusing into design a radio standard with interesting features of low power consumption for low cost, low bandwidth, and low complexity to have a optimal solution available on wearable sensor. As the mater of fact, produce wearable sensors as small as possible and capable to save battery life are the most important features the researches are focusing their attention .

1.3.2 Advantages

What makes BLE so popular are his numerous benefits like following:

- Compatibility: BLE allows you to design viable products today which have the possibility to communicate with so many mobile platform. For example a patient could be able to see itself and understand the data from the sensor he worn reading the data on his mobile phone.
- Flexibility: An other key factors contributing to the success of BLE, very difference towards the classic Bluetooth is that it fits a big set of use cases. Also flexibility

of BLE regards the relatively easy-to-understand stack model allowing anyone to fine-tune his project. In this way researchers of various marketing sectors built their on flexible and relatively low-level APIs [11] to give to future developers to easily program their custom product and to customize the BLE framework for their specific requirements.

- Cost:This standard doesn't need intrusive licensing costs or other fees to access the core specs.

1.3.3 Disadvantages

On the other hand there are also some disadvantages on the use of ble and it is useful to understand which are them and in which way they influence the the application ble is involved in. For ble the main limitation are *Data throughput* and the *Operating Range*.

- Data throughput: From the documentation ble has a modulation rate of a constant 1Mbps. Unfortunately this value is in practical applications much lower for a variety of reasons like bidirectional traffic, protocol overhead, CPU and radio limitations plus other artificial software restrictions. In order to understand that it is described how how the transmission takes place. There is a central(master) which create and established a connection with a peripheral (slave) . The transmission is possible only during a particular connection interval the period between two consecutive connection events that can be set to a value between 7.5 ms and 4 s. For example setting the connection interval to 7.5 ms it corresponds to 1/0.0075 = 133 events/s. This standard previews a maximum of 20 bytes for packet. The data throughput is so calculated as : (133 event/s) $*$ (packets/event $*$ 20 bytes) = max Data Throughput [Mbit/s] In this work it was used the nRF52840 , a multi protocol SoC (system on chip) manufactured by Nordic Semiconductor . Nordic's radio hardware and BLE stack impose at least it can transmit up to six data packets per connection interval and each outgoing data packet can contain up to 20 bytes of user data In that case the new data throughput is: (133 events/s) $*$ (120 bytes) = 15960 bytes/s or $\sim$ 0.125 Mbit/s = 125 kbit/s which is to much lower than the theoretical maximum declared by BLE. Moreover the devise can introduce other constraints that make in practice a potential maximum data throughput in the neighborhood of 5-10 KB per second, depending on the limitations of both peers ,so it's very important to consider in the right way all that variables before design your own application.

- Operating Range: For a wireless device the range value depends on various aspects like the operating environment or the antenna design and device orientation. Bluetooth Low Energy designers are focused on very short-range communication. As a mater of fact transmit power is directly proportional to the reduce the usable lifetime of the battery cell(s). So even if a BLE device can be configured to transmit data 30 meters or more line-of-sight, usually the choice is to have a typical operating range closer to 2 to 5 meters to reduce the range and save battery life without the transmission distance becoming a nuisance to the end user.

1.3.4 Protocol stack

As all the pc application user interfaces himself only with the upper layer of the specific protocol stack. For BLE this is divided in three fundamental part :Application, Host and Controller as is shown in figure 1.5. Moreover, each part is further subdivided in other layer that are the real functional block of the stack providing the functionality needed to operate.

Application:
Strictly connected with the costumers handles the interface and data. The design of application ultimately depends on the specific purpose for which it has been implemented.
Host:
Composed by the following layers:

- Generic Access Profile (GAP)
- Generic Attribute Profile (GATT)
- Logical Link Control and Adaptation Protocol (L2CAP)

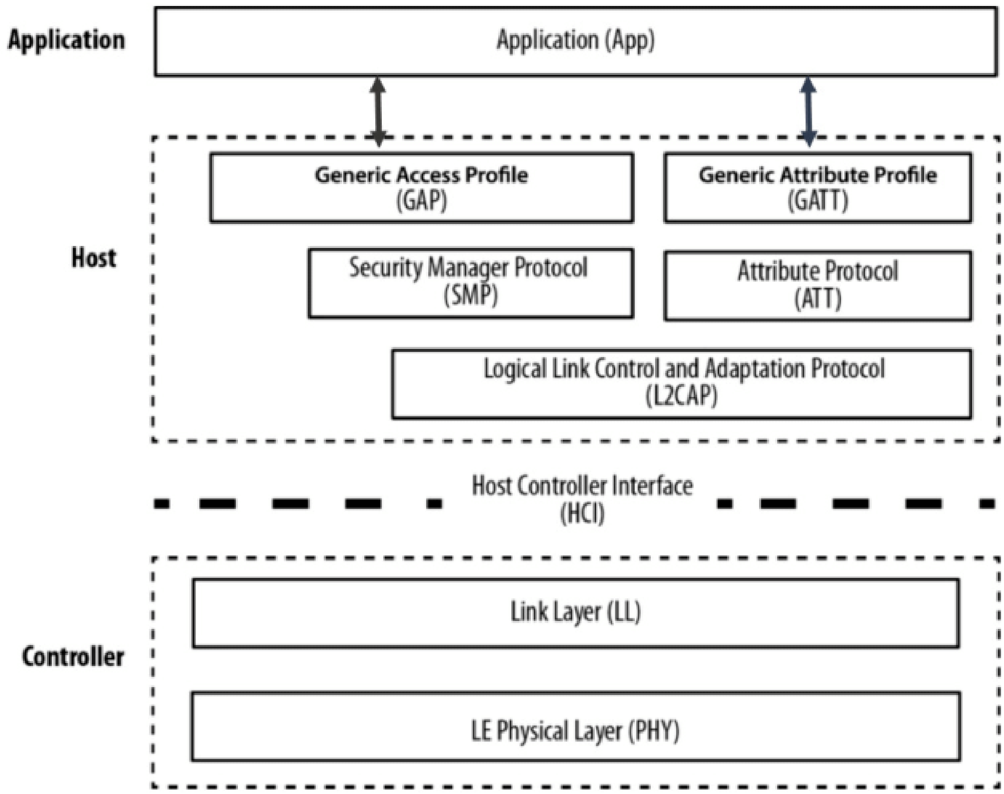

Figure 1.5: The BLE protocol stack [12].

- Attribute Protocol (ATT)
- Security Manager (SM)
- Host Controller Interface (HCI), Host side.

Controller:

Composed by the following layers:

- Host Controller Interface (HCI), Controller side
- Link Layer (LL)
- Physical Layer (PHY)

The next sections will be dedicated to explain how all that layers are organized and how they interact with one each others.

Physical Layer (PHY).

The PHY layer realizes the real modulation and demodulation of analog signals to transform them into digital ones . Ble communication standard uses the 2.4 GHz ISM (Industrial, Scientific, and Medical) band to communicate. This band is divided into 40 channels from 2.4000 GHz to 2.4835 GHz,fig. 1.6.These channels have diversified functions : only 37 menage connection data while the last three (37, 38, and 39) are advertising channels to configure connections and send advertising packets. To encode the bit-stream over the air The modulation adopted is the Gaussian Frequency Shift Keying, GFSK. For Bluetooth Low Energy the modulation is fixed to 1 Mbit/s, which is therefore the upper physical throughput limit for the technology even if is never reached as shown in the last section.

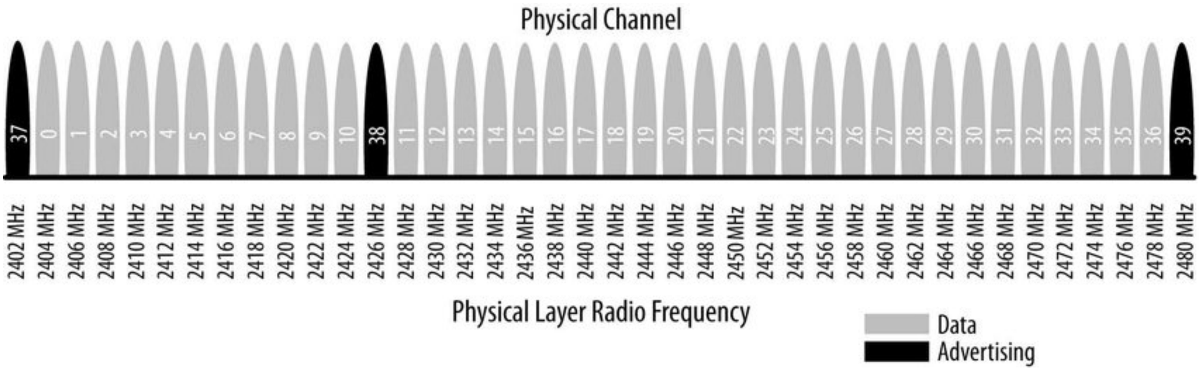

Figure 1.6: Frequency channels. [13]

LINK layer(LL).

The Link Layer (LL) interfaces with the PHY and in the stack it is the only real time constrained layer having as his first purpose to manage the time specifications needed to the protocol. So the HCI interface is a barrier from the upper layers. The LL layer directly sets the radio's state to define the how the devices are connected in the net; so are specified 4 different roles for a peer :

- Advertiser, a device sending advertising packet;
- Scanner, a device scanning for advertising packet;
- Master, a device that initiates and manages the connection and

- Slave, that receive the master connection request and the related time setting.

Each peer is uniquely identified by a Bluetooth Device Address - a 48-bit number that can be a *Public* or *Random Device Adress*.

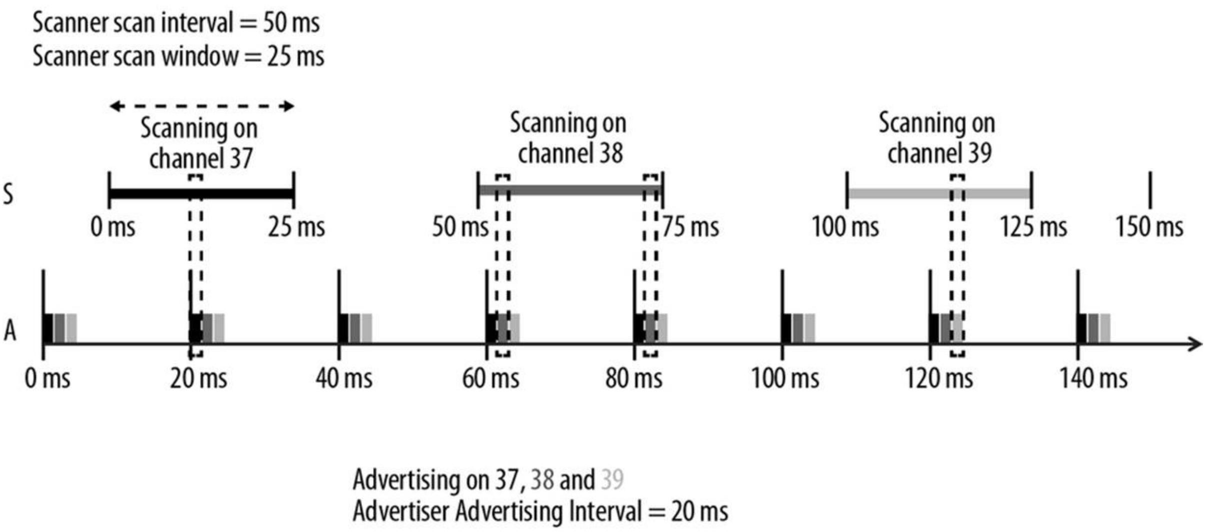

Figure 1.7: Advertising and scanning. [14]

As shown in figure 1.7 to establish a connection it's fundamental the overlapping of the advertising and the scanner period to receive the advertising packet which sets the connection. Nevertheless those periods require the radio turn ON and so a the larger they are, the greater the power consumption. Scanning could be active or passive depending on whether the scanner devise returns or not response back to master.

To establish a connection, there are different steps to executes: a master scans and send his connection request to advertisers. About their Bluetooth Address or the specific advertising information the advertising packets are selected . When the master discover a a slave it again transmits a connection request, to the slave and, provided the slave responds, establishes a connection so a sequence of data exchanges between the slave and the master at predefined times. The link layer also provides for various control processes among which there are the possibility for the master to *Change the connection parameters* depending on the specific connection needs and *Encryption* because it operates actually data encryption and decryption transparently to the upper layers even if the keys are generated and managed by the host.

Host Controller Interface (HCI).

As stated in the introduction BLE can be used to design many application and the Host Controller Interface (HCI) is the central element for this flexibility. The HCI layer makes possible the communication between the host and the controller through a serial interface. So them interact sending each other command, event and data packets.There are cases into which the host and the controller are separated on different chips for the costs to implement the host ,controller and application on a single system-on-chip, or SoC. The producers usually for embedded device solution design an all in one chip, to reduce cost and dimension on the final device; therefore all three layers are implemented on a single low-power CPU.

Logical Link Control and Adaptation Protocol (L2CAP).

The L2CAP performs two key functions :fragmentation and recombination. All packets exchanged between the upper layers are fragmented into the 27-byte maximum payload size of the BLE packets and successively reassembled again to sent upstream the whole message to the appropriate entity in the upper layers of the host. The value of 27-byte maximum payload size is important to note that effectively corresponds to 23 useful bytes because the L2CAP packet header takes up 4 bytes. Finally it is also responsible for the process of routing two main protocols: the Attribute Protocol (ATT) and the Security Manager Protocol (SMP) , described in the sections below.

Attribute Protocol (ATT).

The Attribute Protocol (ATT) is a simple client/server stateless- no state so is a communications protocol in which no information is retained by either sender or receiver- protocol which use attributes that are presented by a device. In BLE each device is a server/clients or both regardless of being a master or slave peer so every time there is a client's request for the server it sends back to the client. An attribute is characterized by these parts:

- a 16-bit attribute handle,identifier to simplify attribute access

- a universally unique identifier (UUID),definining what kind of data contains the attribute
- a set of permissions,
- a value.

All transactions between server and client are clustered into request(always sent by a client) and response(issued by the server as a reply) pairs. Therefore to read/write attribute values from or to a server, the client puts out a read/write request to the server with the handle. For read's operation, the client have to check for the data type based on the UUID of the attribute. On the other hand, for write's operation, the client have to submit data consistently with the attribute type even if the server can reject the operation.

Security Manager (SM).

Each wifi transmission needs to be protect allowing the peers to communicate on an encrypted link.The Security Manager (SM) deals with this aspect of BLE generating security keys. When two devices, want to do something that requires security, they must first *PAIRING*. The Central device trying to access a data value (a "characteristic") on a Peripheral device that requires fist an authenticated access. Pairing it's only a temporary security bond and the key is not stored. To establish a more reliable connection the peers have to *BONDING* : A pairing process followed by the generation and exchange of permanent security keys,therefore creating a permanent bond between two devices. There is also the possibility to select the security level among : Encryption,Privacy,and Signing.

Generic Attribute Profile (GATT).

The Generic Attribute Profile (GATT) defines how data is organized and exchanged between applications. Data are assembled hierarchically in sections called services, organizing user data in characteristics. These contain the user data and other useful information as value, properties,user-visible name, units, and more. GATT makes use of the Attribute Protocol (ATT) as transport protocol to exchange data between devices.

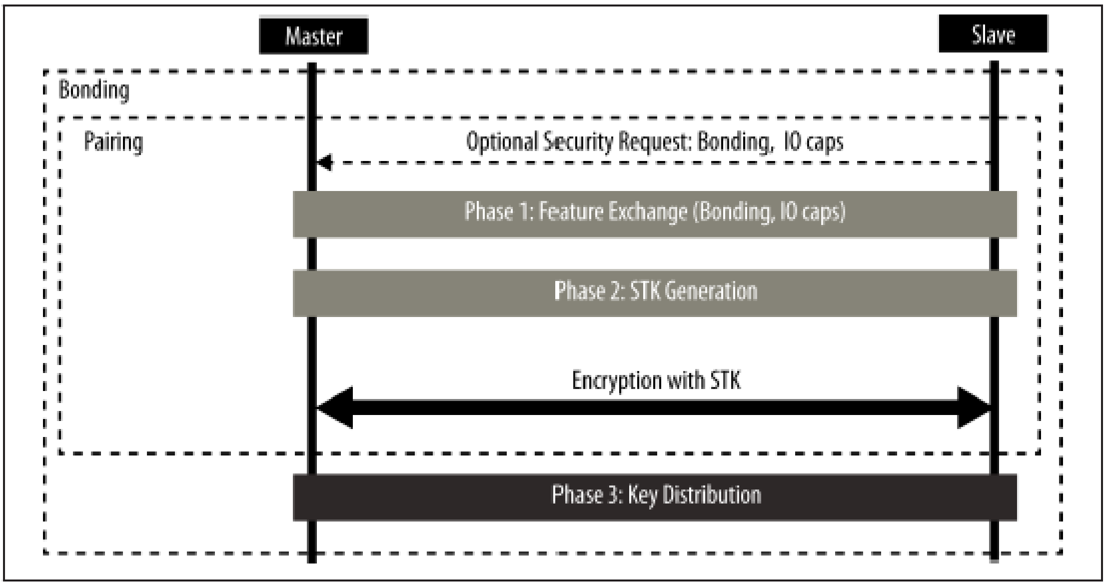

Figure 1.8: Pairing and Bonding sequences [14].

Firstly GATT defines the roles devices can adopt: Client and Server roles. A Client have to send a request and receive a response from it through the services discovering procedure. After that client has permission to read and write attribute found in the server. A Server has the main objective of receiving and sending back answers to a client's requests. It also sends updates started by the server and is responsible for storing and providing the customer with the user's data, organized in the attributes.

A GATT server can have several services each with more than one characteristic. A service could also contain different characteristics. Two definitions have to be underlined: the first is the Declaration, which is the first single cluster attribute, and the second one is Descriptor which is the link of the declaration with the extra attributes to the cluster. There are several types of descriptors, such as user description descriptor, extended properties descriptor or a new one known as Client Characteristic Configuration Descriptor (CCCD). The CCCD works to enable or disable server functions, through which forward characteristics are updates to the client. For example, it enables the transmission of notifications - when a notification is allowed setting in a characteristic property the CCCD to 1- each time the value of the attribute is changed and it is sent to the client.

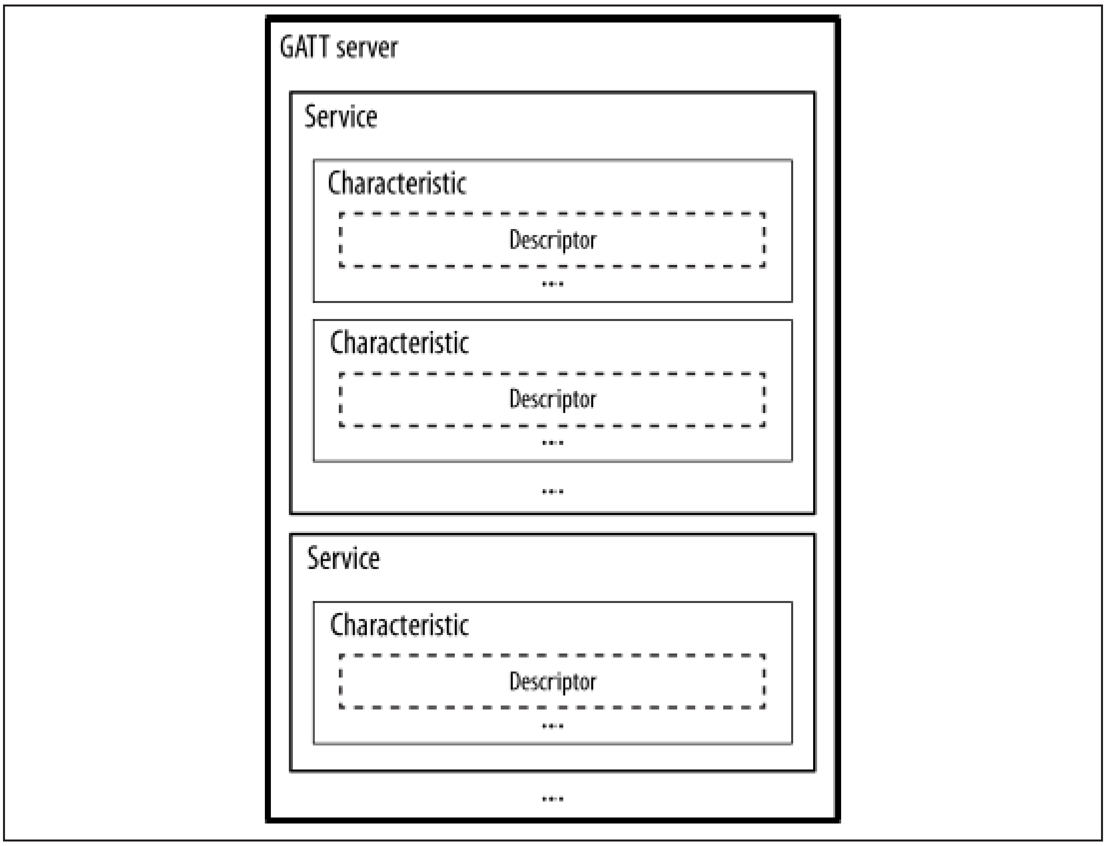

Figure 1.9: 1.19: GATT Server Hierarchy example with three services,each one with his characteristics [14].

Generic Access Profile (GAP).

This layer defines various aspects as : roles, modes, procedures and security needed to establish peers connection and data shearing.

Roles

A device in a BLE network act as one of the following roles:

- Broadcaster: The broadcaster role corresponds to the Link Layer advertiser role. This device is always forwarding data in advertising packets available to all devices that are listening.
- Observer: The observer role corresponds to the Link Layer scanner role. A Observer device is always receiving for advertising packets.
- Central: The central role corresponds to the Link Layer master. It's a device connected to multiple peers,and with the function to add new devices at the network.
- Peripheral: The peripheral role corresponds to the Link Layer slave. This device sending advertising packet to the central peer in order to be recognized and connected to the central device of the network.

Modes and Procedures

The roles operate in different ways achieved through distinct procedures. For example, there are modes of discoverability, which allow the peripheral to be totally or partially invisible to a central device, or the most common, the general detectable mode allowing the peripheral to be found by the central peer. Other modes operate modifying the information of the advertising packets to avoid connection or allow a direct or non-direct connection. Instead, the procedures define the set of actions necessary to implement these modes, such as the general procedure of discovery in a central device, which automatically starts scanning without taking into account the addresses in the folder white list and evaluate each advertising packet found.

Security

The GAP also implements some modes and procedures related to the Security Manager layer. For example, the GAP implements other features that increase the security of the communication, such as address types handling, authentication, among others.

1.4 Bluetooth Mesh

1.4.1 Overview

Bluetooth Mesh (BLE Mesh) introduces a new concept of communication that is no longer point-to-point communication but each device can send messages simultaneously to any other device within its network. This allows extending the range of action of the whole network.In a Bluetooth Mesh network, messages are sent via advertising packages, which means that the forwarding of network messages no longer requires connections to share information. The Ble Mesh assigns each device - the network node - a specific role such as increasing the network's range of action and network coverage. Besides, there is the possibility to remotely manage these nodes through the use of simple smartphone or PC applications.

1.4.2 Device Types

BLE Mesh technology focus on the use of nodes exchange message within the same network.There are various type of nodes to choose the best suits your application and different features to set on these nodes.

- Relay Node: The Relay function corresponds to the possibility of forwarding the message received from another node again. A practical example of this particular functionality is the one used for the light switch as shown in Figure 1.11. Usually, these nodes are directly connected to the power distribution network as they need enough power to receive and redirect network packets.
- Low-Power Node (LPN): A low-power node performs his functions together with another node connecting to it with a friendship feature.The low power node wakes up at specific time intervals only when there is an available message provided by the friend node and then go back to sleep mode to save energy. In this way,

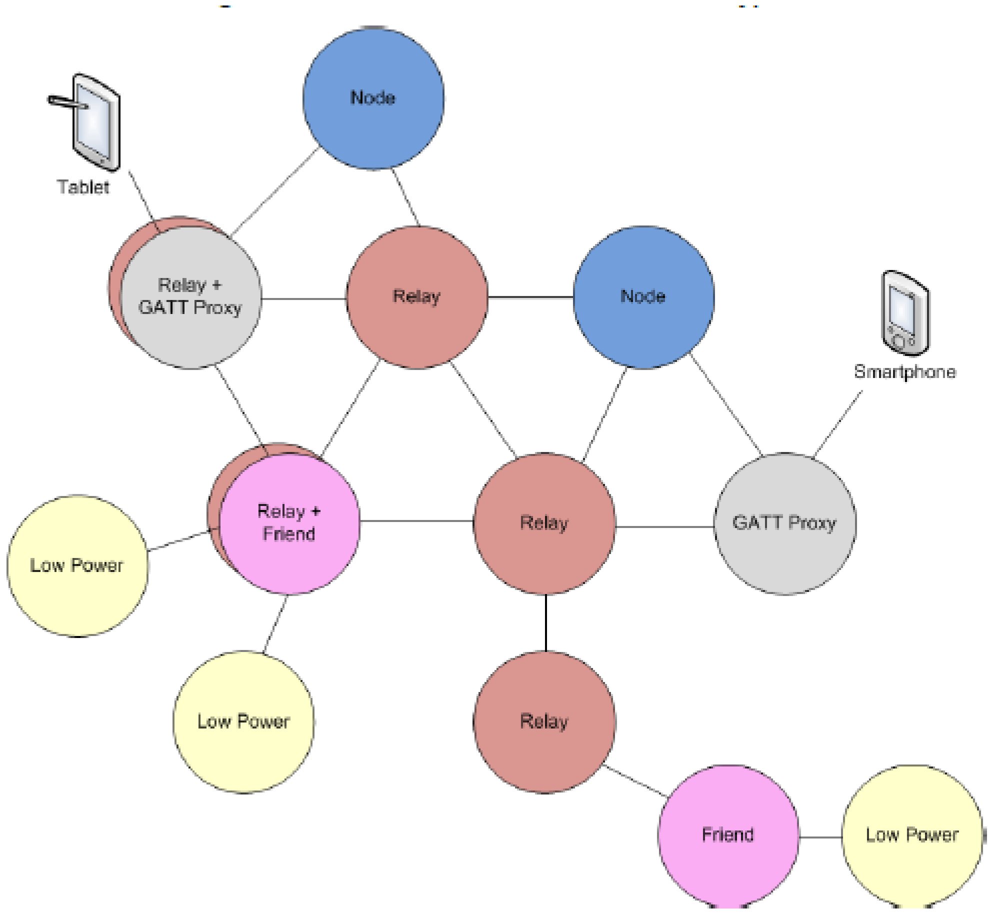

Figure 1.10: Bluetooth Mesh Network Topology. [19]

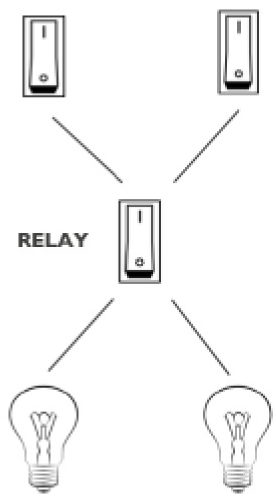

Figure 1.11: Bluetooth Mesh Relay Feature [18]

correctly setting the BLE Mesh low-power function, even a button battery will be enough to power the node at low power for about a year.

- Friend Node: The Friend Node has the goals to receive and store all the messages addressed for his LPN nodes and for this reason, has higher memory requests. The messages will be after re-transmitted to the right LPN thought a polling operation.
- Proxy Node: The Proxy function is the ability of a node to transmit messages between GATT (General ATTribute) and advertisers.The Proxy function is the link between BLE and BLE Mesh as it allows a node configured only for BLE to transmit messages between GATT (General ATTribute) and the advertisers through whom BLE Mesh sends packages. Therefore in this way, a device that only supports BLE can take part in a BLE Mesh Network thanks to a Proxy node that acts as an interface for a smartphone/PC through a GATT connection.
- Provisioner: The Provisioning feature is the process to add a new node and ensures a secure BLE Mesh network. Provisioning requires several steps: an unprovisioned device will send beacons at a specific interval, and the provisioning device will search for it to exchange keys for secure communication.

1.4.3 Protocol Stack

The BLE Mesh stack is built upon the BLE architecture as show in Figure1.12. The functions of that layers are the following:

- Bluetooth Low Energy Core Specification: all the layer are on the top of BLE standard specification and so uses the two mechanisms of advertising and connection.
- Bearer layer: this level configures an abstraction for the passage of information between the underlying BLE and the higher levels. They are identified as "bearers" and are of two types ADV bearer and GATT bearer. The ADV bearer handles a mechanism for BLE advertising and the GATT bearer the one that for BLE connections.

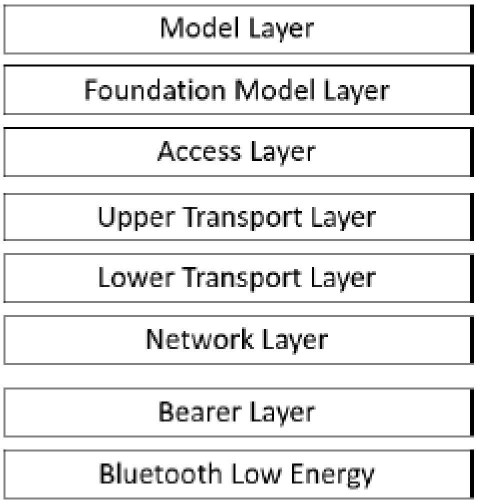

Figure 1.12: Bluetooth Mesh Stack Architecture. [18]

- Network layer: it takes care of forwarding and network security.
- Transport layer: bigger messages are segmented and reassembled in this layer. Also in this layer there is attention of security.
- Access layer: this layer ensures that the packet is clear and well organized to go from the more technical layer to the more application focused layers above.
- (Foundation) model layer: the highest layers are connected to the definition of model ;a particular scenario implemented for the final application . On the top a BLE Mesh device can be seen as a combination of different models that constitute his application layer.

1.4.4 Operation and Key Concepts

- Managed Flood: BLE Mesh uses the managed flood process to transfer messages with sufficient redundancy to have the security that it is received on the other side. However, this mechanism is controlled so that the same packet is re-transmitted only once if it has already been re-transmitted previously. Each message is associated with a TTL (Time to Live) value that limits the number of times a message can be forwarded. The TTL value is decreased by 1 each time a message is received and retransmitted by a node.

- Publish- and Subscription-Based Communication: a Publisher Node sends messages, and only nodes that have subscribed to it can act on these messages.In this way, there can be the coexistence of different products in the network without the specific communications being disturbed and go into error. An example is shown in Figure 1.13 : in a house, we have several rooms and each can subscribe to the switches specific to that room. Besides, messages can be unicast, multicast and/or broadcast, in the sense that it can reach one or more nodes in the network.

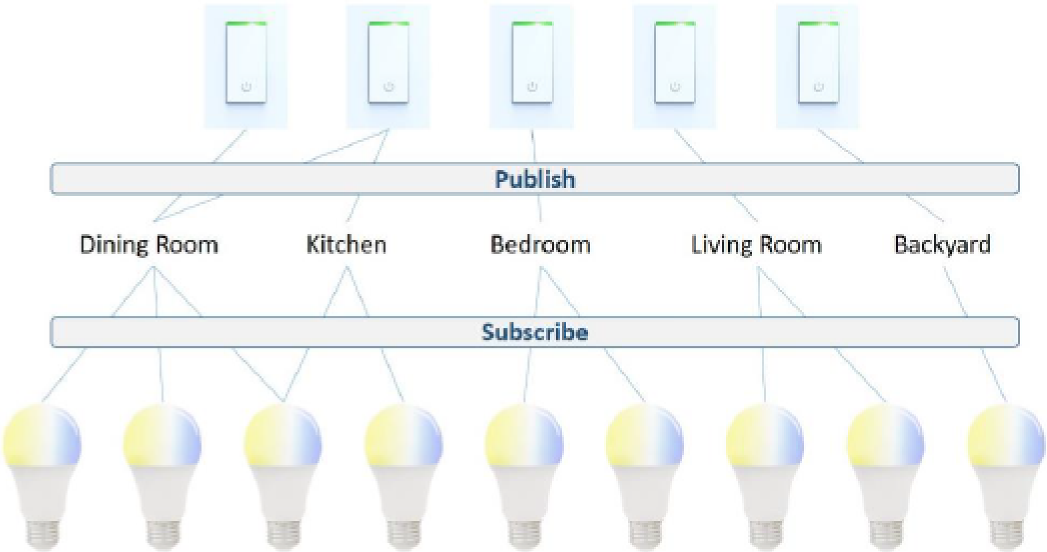

Figure 1.13: Publish and Subscribe Mechanisms. [19]

- Elements: Elements define each one aspects of a node's functionality. Therefore, each node will have at least one element called "Primary Element". In the case of a light bulb, it can have an element that manages its functions such as ON/OFF and control on the level of brightness expressed in the Light Lightness Server Model. Usually, each element is associated with a unique address, known as a unicast address to ensure that there are no errors in the management of multiple elements in the same node.

- Models: Models define the functionality of a node and correspond to the services of Bluetooth devices. There are three types of Mesh Models - Client, Server and Control Models that combine both Client and Server into a single model.

Server Model - The Server Model defines the messages that a model can transmit and receive and the behaviors associated with the messages themselves. on the other hand, server models express the states of the element that can be read or controlled by a Client. Client Model - A client model defines the set of messages needed to change the Server's status. an ON/OFF switch- a client- can send a message to an ON/OFF server to change the status of the device. Control Model - An end application could use server or client models together with control logic. Each combination of server and client models results in a control model.

- Model Hierarchy: Sometimes models can extend functionality to others; so models can be hierarchical. For example, the 'Light Light Lightness' model extends the 'Generic OnOff Server' model and the 'Generic Level Server' model. Models that do not contain other models are known as "root models".

1.5 Ant

1.5.1 Overview

ANT™ is a high-performance wireless sensor network protocol in the 2.4 GHz ISM band. It can handles more types of Network Topologies [1.15], is ultra-low power, efficient ,easy to use and provides reliable data communication.The protocol stack [1.14] is minimal and streamlined so is can run also on simple devices with considerably reduces system costs.The Physical, Network and Transport OSI layers are very smart to use and ANT creates key low-level security features as foundation of further high level and more specific development from the next Applications layers designers.

1.5.2 Node

Each node in an ANT network is made up of two parts: an ANT protocol engine and a host controller. The ANT engine takes care of establishing and maintaining ANT connections and channel operation with the firmware. The host controller instead handles the particulars of an application and initiate an ANT communications to other nodes, through a serial interface between host and ANT engine, as shown in Figure

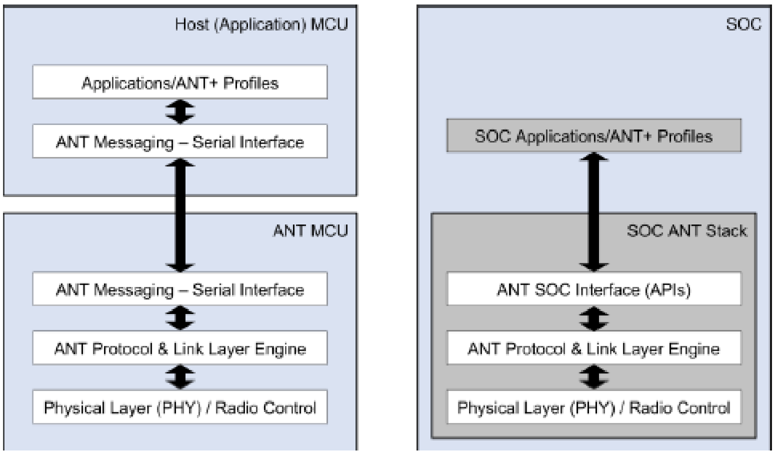

Figure 1.14: Contents of an ANT node. [15]

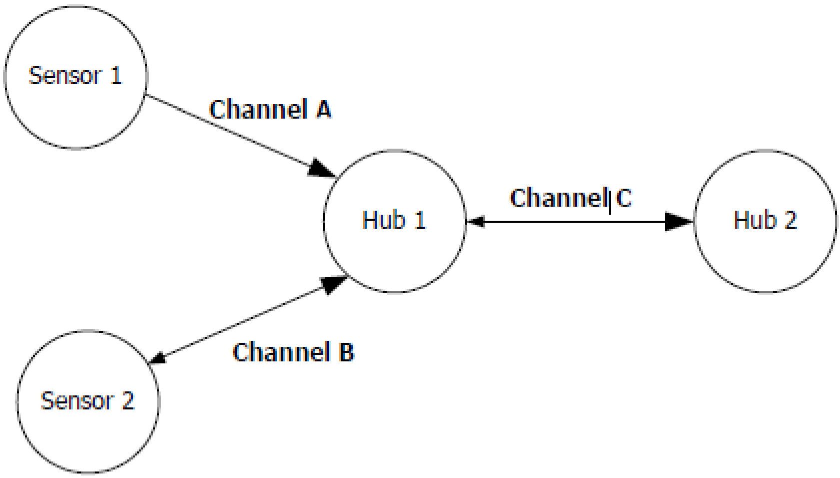

Figure 1.15: A simple ANT network: each ANT node connects to other nodes through sharing channels. Each channel is configured for two nodes but multiple nodes can connect to a single channel. One node is the master-transmitter and the other on is the slave-receiver. Moreover ANT node can be as both a slave and a master simultaneously for different channels. [15]

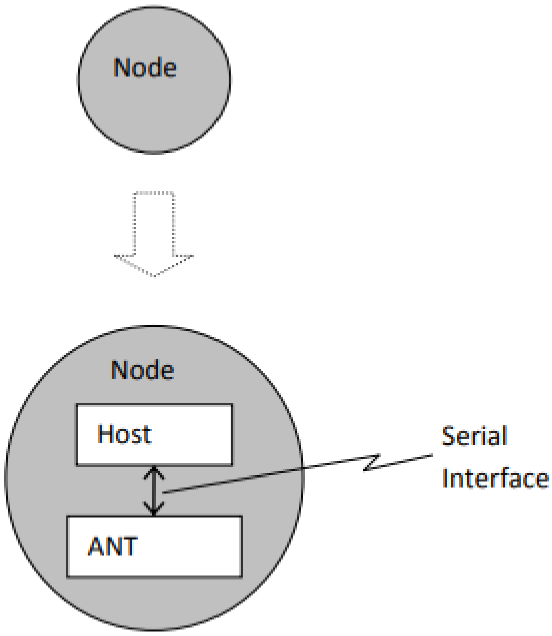

Figure 1.16: Contents of an ANT node. [15]

1.5.3 Channel

ANT usage and configuration is channel-based, so the channel is the ANT protocol's central part. The channel is required every time to two nodes have to exchange data among them.

The smallest channel includes at least a Master and a Slave as shown in Figure1.17.

Channel Communication.

A channel fist of all must to be configured in relation to the data type and direction to sent. There are synchronous, independent, bidirectional channels. When a channel is open the master node searches to avoid interference with other device and starts to transmit message on channel period (Tch) as shown in Figure 1.18. Furthermore, it has to be take care to aspects such as to select the desired channel parameters (e.g. RF frequency, channel period and channel ID) and single channel encryption. There are four data types,each one determines they will be sent among nodes: broadcast, acknowledged, burst and advanced burst message transfers.

Two main directions are used to transfer data :

1. Forward Direction (Master -> Slave) and

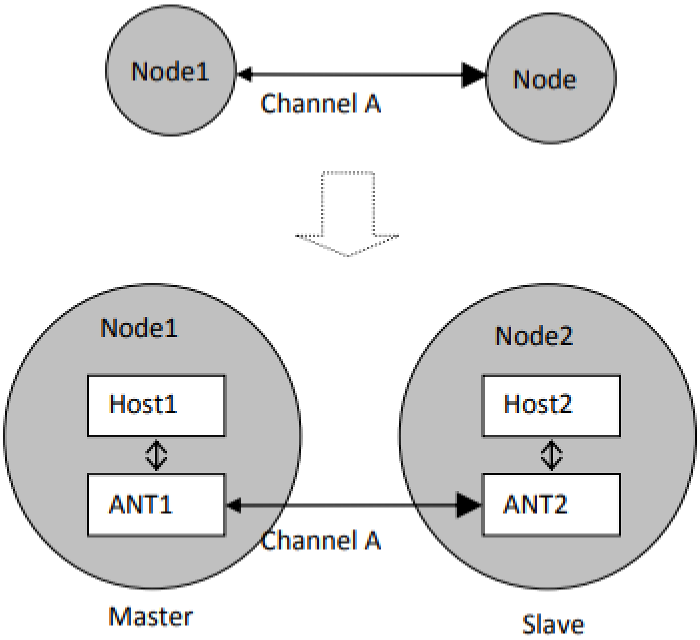

Figure 1.17: Channel communication between two ANT nodes. [15]

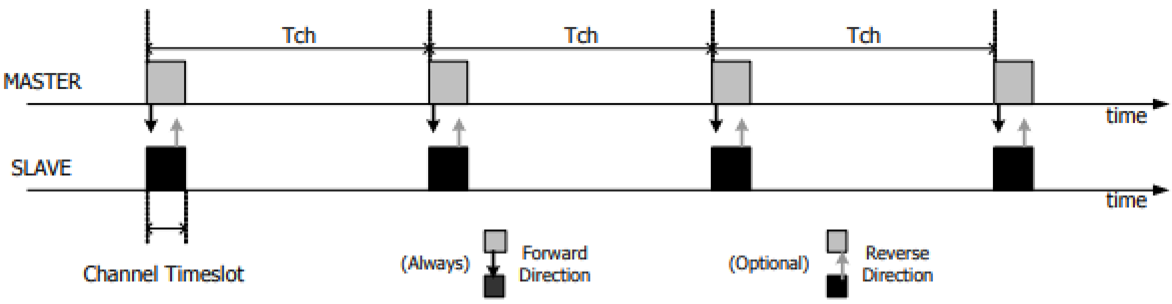

Figure 1.18: Channel communication showing forward and reverse directions. [15]

2. Reverse Direction (Slave -> Master).

Channel Configuration.

The complete channel configuration requires to define the next properties -before the channel will open- in order to correct establish the communication between two nodes as shown in the Table 1.2 where is reported a standard channel configuration for a simple application.

1. Channel Type: The Channel Type is an 8-bit field selecting for the kink of communication will occur on the channel; in the Table 1.1 there are some example codes.

Value	Description
0x00	Bidirectional Slave Channel
0x10	Bidirectional Master Channel
0x20	Shared Bidirectional Slave Channel
0x30	Shared Bidirectional Master Channel
0x40	Slave Receive Only Channel (diagnostic)
0x50	Master Transmit Only Channel (legacy)

Table 1.1: Channel properties. [15]

2. RF Frequency: The RF frequency (1.1) is an 8-bit field obtained thorough the equation:

$$RfFrequencyVal = \frac{DesiredRfFrequency(MHz) - 2400MHz}{1MHz} \tag{1.1}$$

ANT technology provides 125 unique RF operating frequencies even if there is the possibility to use the same RF frequencies for different channels;in fact is the producer's responsibility make reliable the use of the same frequency. Usually the default frequency is set to 66 and corresponds to the network operating frequency of 2466MHz.

3. Channel ID: The Channel ID, crucial in device pairing, it's a 4-byte value decoding for 3 fields – Transmission Type, Device Type and Device Number. The

transmission type is a values looking for the different transmission characteristics of a device. The Device Type indicates the class (or type) of the master device. The Device Number decodes for a specific master device.

4. Channel Period: The channel period (1.2) is the basic message rate of a broadcast data packet sent (master) and received (slave), on every time-slot at this rate. Depending on the specific application the channel message rate can change from 0.5Hz to above 200Hz. Moreover the upper limit is constrained also by the computational capacity of the system. For example,a message rate of 4Hz on a channel is selected with a channel period of 32768 / 4 = 8192. The most performance message rate is 4Hz which gives The default message rate is 4Hz, which gives more readily discoverable networks with good power and latency characteristics. To sum-up this is a very critical aspect and has to be related with the following issues:

    - The message rate has an impact on the power consumption.
    - A small channel period corresponds to an higher data-transfer rates.
    - A small channel period results in faster successful device-search operations.

$$ChannelPeriodVal = \frac{32768}{MesageRate(Hz)} \tag{1.2}$$

5. Network: An ANT network is a set of operating rules for all participating nodes, which have to take part if they want to communicate with the other nodes. There are several kind of Ant network like public and private networks each one labeled with two components : *Network Number* and *Network Key.* Also ANT+ is an example of managed network. The key advantage of this kind of network is devices' interoperability - the possibility of wireless communication with other ANT+ products - for them produced by companies members of the ANT+ Alliance.

Establishing a channel

Therefore to permit a channel creation and start the master and slave have to share common information for the channel configuration as detailed in section 1.5.3. The

Parameter	Value	Description
Network Number	0	Default Public Network
RF Frequency	66	Default Frequency 2466MHz
Device Number	1	Sample Serial Number
Transmission Type	1	Transmission Type (no shared address)
Device Type	1	Sample Device Type
Channel Type	0x10	Bidirectional Transmit Channel
Channel Period	16384	2Hz Message Rate
Data Type	0x4E	Broadcast

Table 1.2: Channel communication between two ANT nodes. [15]

Figure 1.19 explains how to properly establish communication between two ANT nodes. Text within solid lines express channel parameters with no default value you have to set for your own application, while the other ones in dashed lines expresses defaults channel parameters even if you are free to change them.

1.5.4 Data Types

ANT supports four data types as shown in the Table1.3: broadcast, acknowledged, burst and advanced burst data. Data are encapsulated and transmitted over the RF Channel in 8 byte packets. All the data can be transmitted in both forward and reverse direction between two nodes except for unidirectional channels, which have the permission to send broadcast data only in the forward direction.

Data Type	Channel Direction	Description
Broadcast	Forward/Reverse	Default Data Type. Broadcast messages sent every timeslot.
Acknowledged	Forward/Reverse	If requested, sent on the next channel timeslot.
Burst	Forward/Reverse	A burst transfer will commence at start of the next timeslot.
Advanced Burst	Forward/Reverse	An advanced burst transfer will commence at start of the next timeslot. Bursts packets synchronize off each other.

Table 1.3: ANT data types. [15]

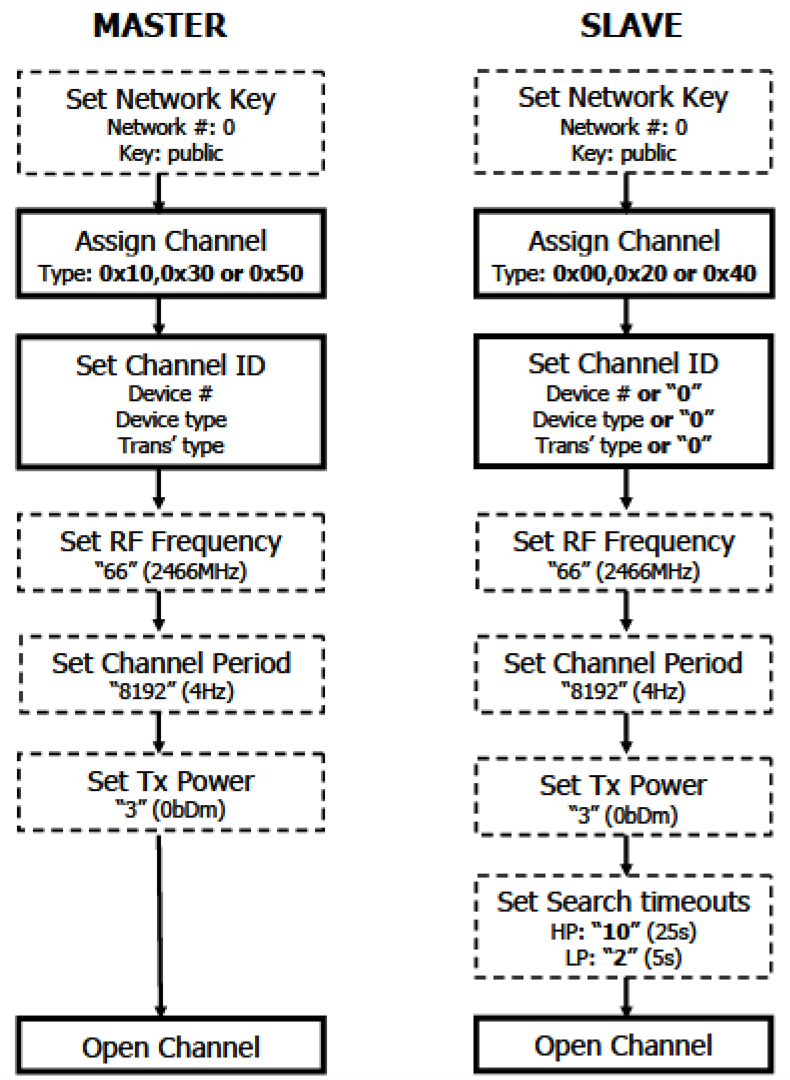

Figure 1.19: Channel routine establishment between master and slave nodes. [15]

1.6 IEEE 802.15.4

1.6.1 Overview

This standard defines the physical layer (PHY) and medium access control (MAC) sublayer requirements for low-data-rate wireless connectivity devices with limited battery consumption requirements operating in about 10 m. Physical layers (PHYs) support different frequency bands such as free 868–868.6 MHz, 902–928 MHz, and 2400–2483.5 MHz bands. The raw data rate is 250 kb/s.

1.6.2 Device Types

In an IEEE 802.15.4 network, there can be two device types full-function device (FFD) and a reduced-function device (RFD); however, only FFD can be a personal area network (PAN) coordinator or a coordinator. The RFD can have only one FFD at a time and transfers a small amount of data, so have less memory. To have communication, two devices have to be on the same physical channel and constitute together a WPAN. The smaller WPAN is made up of at least one FFD as the PAN coordinator.

1.6.3 Network topologies

An IEEE 802.15.4 LR-WPAN can operate in two different architectures: the star topology or the peer-to-peer topology as shown in Figure 1.20.

- In the star topology, there is a single central node - the PAN coordinator- which manages communication with other devices. The PAN coordinator can have a proper function, however, it has to start, close, and routing data in the network. Each device is characterized by a unique extended address to communicate within the PAN or a short address assigned by the PAN coordinator when the device is associated.
- The peer-to-peer topology permits devices to transfer data to each other without limitations. there is always a PAN coordinator selecting for a unique identifier useful to enable intra-net communication using short address and beyond-net

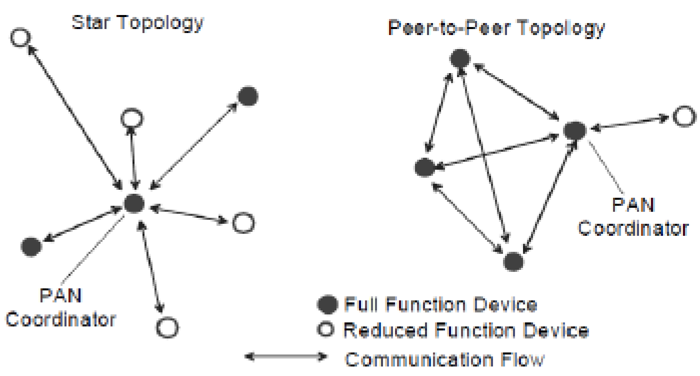

Figure 1.20: IEEE 802.15.4 Network Topology. [21]

communication. Peer-to-peer in this way offers the possibility to implement more articulated networks such as mesh networking topology.

1.6.4 Protocol stack

For the IEEE 802.15.4 standard, there is a very simple protocol stack composed by only two layers plus others on the top to better define the device's application level . In the Figure are underlined the interfaces of the layers,very important to define the logical links. The Physical layer (PHY) contains the radio frequency (RF) transceiver equipped with low-level mechanism of control, and the MAC sublayer to establish the link to the physical channel and various types of transfer.

PHY sublayer

The PHY furnishes two services: the PHY data service and the PHY management service. The PHY data service guarantees the forwarding and validation of PHY protocol data units (PPUDs) through the physical radio channel. Moreover, other important PHY features are radio transceiver management and channel selection, clear channel assessment (CCA), and correct data routing in the physical medium.

MAC sublayer

For the MAC sublayer, there are two services: the MAC data service and the MAC management service. Both interface with the MAC sublayer management entity (MLME) service access point (SAP) (known as MLME-SAP). The MAC data service guarantees the forwarding and validation of MAC protocol data units (MPDUs) across the PHY data service. Moreover, other important MAC features are beacon management, channel access, frame validation, acknowledged frame delivery, association, and disassociation plus some links with security mechanisms.

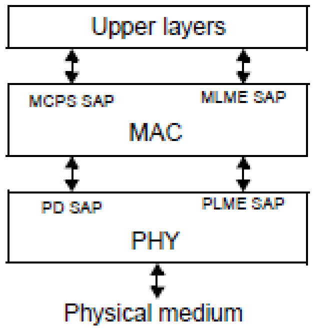

Figure 1.21: IEEE 802.15.4 Stack. [21]

1.6.5 Functional overview

The networks coordinator configures the superframe structure, divided into 16 slots of equal duration each stays for start frame transmission, bounded by network beacons sent by the coordinator, as illustrated in Figure 1.22.a. The superframe has an active and an inactive portion into which the coordinator enters the low power mode, as illustrated in Figure 1.22.b. To avoid using a superframe structure, the beacon transmissions have to be disabled. The beacons have the functions to synchronize connected devices, identify the PAN and describe the superframe 's structure. The contention access period (CAP) between two beacons is a sufficient portion of the CAP remains for contention-based access to other networked devices or new devices wishing to join the network. To ensure low-latency applications, the PAN coordinator dedicates portions of the active superframe called guaranteed time slots (GTSs) (see Figure 1.23) as the contention-free period (CFP) dedicated to devises communications.

1.6.6 Concept of primitives

A service primitive is an abstraction layer to provide the required information by a particular service. Figure 1.24, shows the service hierarchy and the relationship between

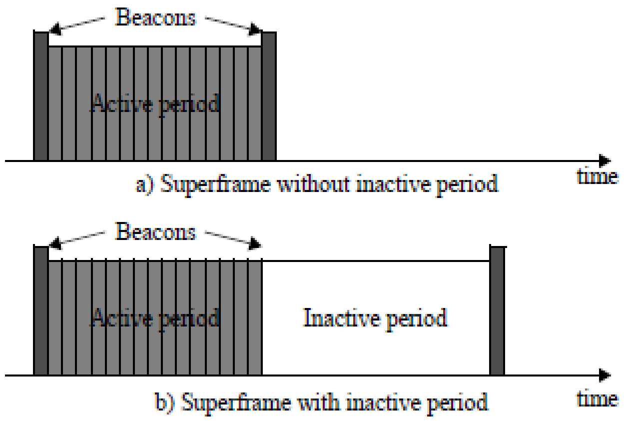

Figure 1.22: IEEE 802.15.4 Superframe Structure. [21]

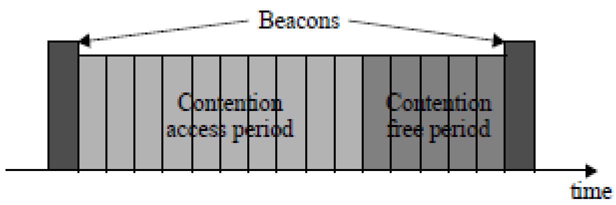

Figure 1.23: Structure of the active periods with GTSs. [21]

the two correspondent users and their associated layer (or sublayer) peer protocol entities. The services are specified through the information flow descriptions between the N-user and the N-layer modeled by discrete events, which characterize the provision of a service. Each event passes a service primitive from one layer to the other through a layer SAP associated with an N-user. There are four primitives types: Request / Indication /Response and Confirm.

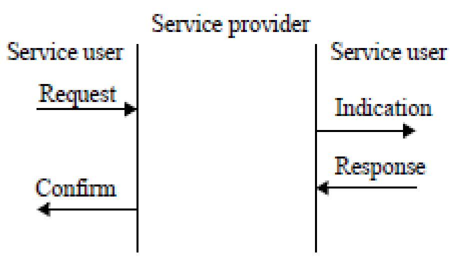

Figure 1.24: IEEE 802.15.4 Service Primitives. [21]

1.7 ZigBee

1.7.1 Overview

ZigBee is standard-based protocol adopted for wireless sensor network applications. Zigbee in particular defines the application layers above the 802.15.4 physical and MAC layers; see Figure 1.25.

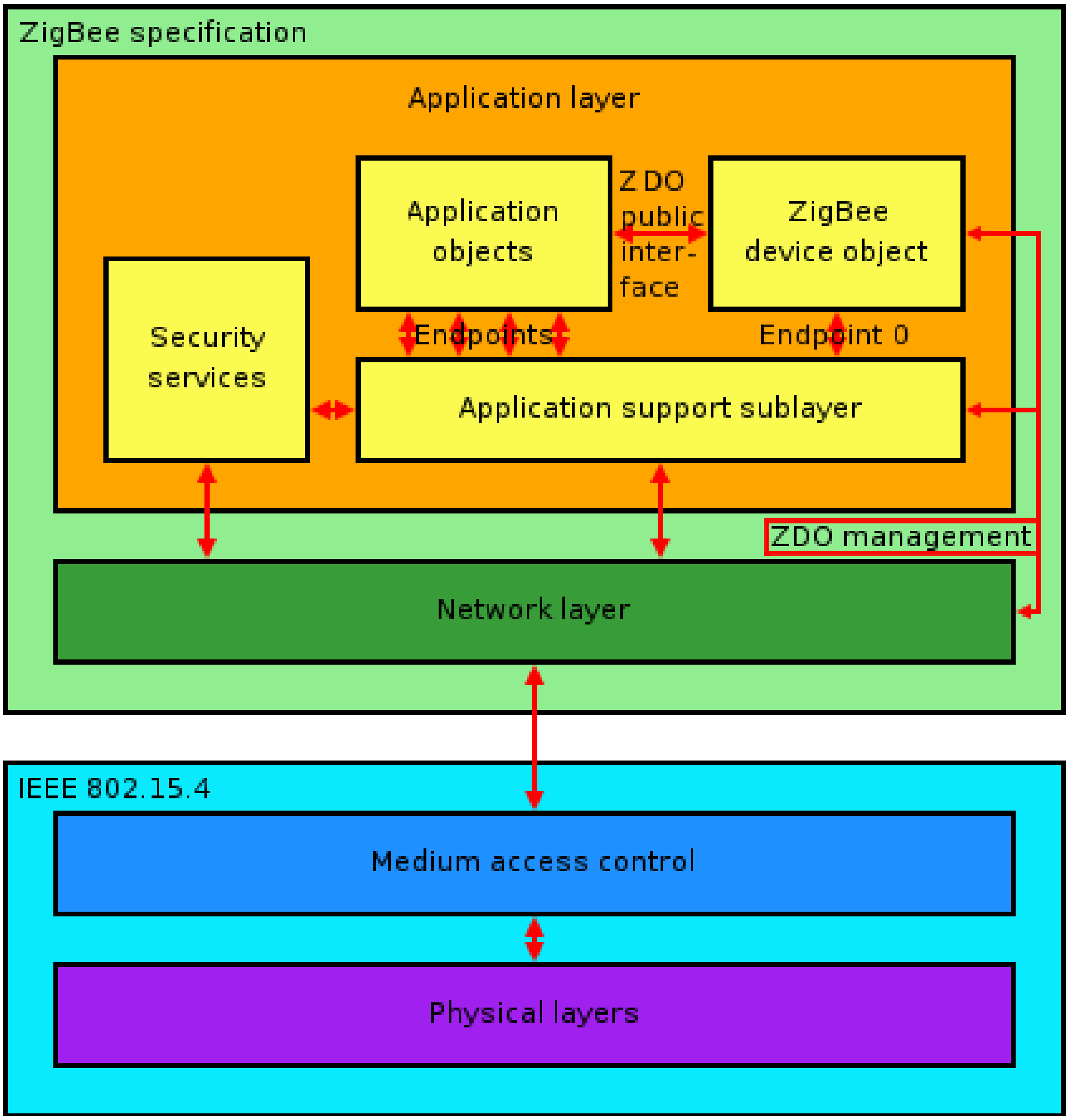

Figure 1.25: ZigBee Protocol Stack. [36]

1.7.2 Protocol Stack

Each level performs the necessary services at the previous level by providing the interfaces through a Service Access Point (SAP).

- Application Layer (APL): top layer made up to the Application Framework, ZigBee Device Object (ZDO), and Application Support Sublayer (APS).
- Application Framework helps to build a correct profile onto the ZigBee stack specifying standard data types for profiles, descriptors useful in service discovery, frame formats to transport data, and a key-value pair construct to develop simple attribute-based profiles.
- Application Objects Software at an endpoint to control a ZigBee device. Each node can supports up to 240 application objects and each application object endpoints from 1 to 240 (with endpoint 0 dedicated ZigBee Device Object).
- ZigBee Device Object Defines whether a device within the network acts as a coordinator, router, or end device by configuring a secure relationship between network devices. It also provides some management commands defined in the ZigBee Device Profile (ZigBee commissioning).
- ZDO Management Plane simplifies communication between APS and NWK layers with the ZDO that has to respond to network access and security requests using the ZigBee Device Profile (ZDP).
- Application Support (APS) Sublayer provides a data service to the application and ZigBee device profiles and saves binding links.
- Security Service Provider (SSP) configures security mechanisms for layers NWK and APS .
- Network (NWK) Layer manages network address and routing gyving instructions to the MAC layer. some goals are starting the network (coordinator), assigning network addresses, adding and removing network devices, routing messages, applying security, and implementing route discovery.

1.7.3 Device Types

In a Zigbee network there are three types of devices such as: Coordinators,Routers and End devices.

1. Coordinators: it has the task to start and control the network by storing the network management information and the security keys.
2. Routers: can connecting directly to the network coordinator , other routers or child device, extend the network coverage area and solve the problems of congestion or malfunctioning devices.
3. End devices: can connecting with the coordinator or other routers. They have the function to transmit and receive messages without routing operation.

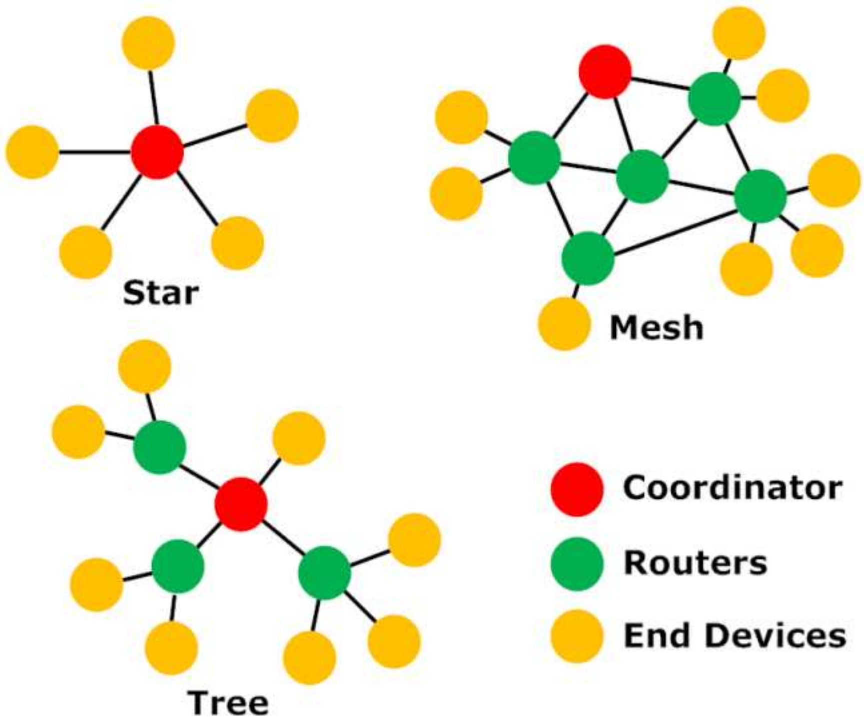

Figure 1.26: ZigBee Devices and Network Topology. [37]

1.7.4 ZigBee Mesh Network Topology

Each Zigbee network as shown in Figure 1.26is composed of the connection of one coordinator, multiple routers and end devices. In particular, the router transmits messages to neighboring devices and therefore must have at least 2 connections. The mesh topology supports the "multi-hop" communication mechanism, i.e. the packages reach their final destination by jumping on the nodes following the most reliable and economical path, avoiding by default the faulty devices. Among the advantages of this kind of topology, there is the possibility of the network to be increased through all intermediate devices, to recover - adding more routers - even weaker signals and to use an infinity of alternative paths.

1.7.5 Joining a ZigBee Network

A ZigBee Network can be established in two approach: through MAC Association or Network Rejoin.

MAC Association

As implemented in MAC layers, the MAC association is supported by each ZigBee device. The ZigBee coordinator for adding other devices outputs a NLME-PERMIT-JOINING.request. On the other hand, the joining device must issue a NLME-JOIN.request with the rejoin flag set to FALSE. In this case, the MAC protocol starts, as shown in the Figure 1.28, where the joining device sends a joining request and the receiving device forwards a message with the new address to be used by the joining device in the network.

Network Rejoin

This is an NWK layer routine (see Figure 1.27) and it's detached from the MAC Association ones. There isn't the need for a router's NLME-PERMIT-JOINING.request and the connection it's secure if the device has the current NWK key even if obtained in different ways.

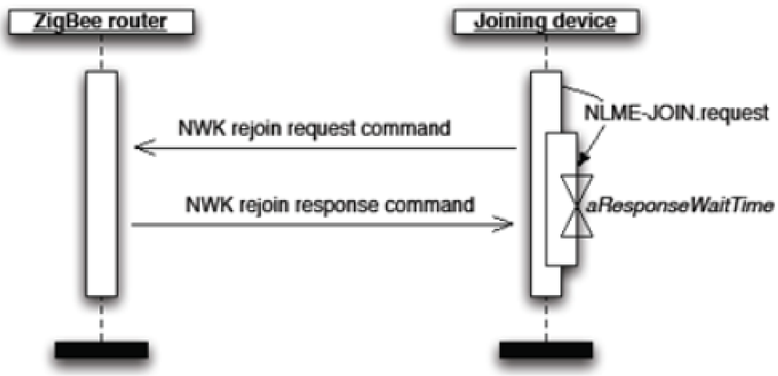

Figure 1.27: ZigBee MAC Network Rejoin approach. [20]

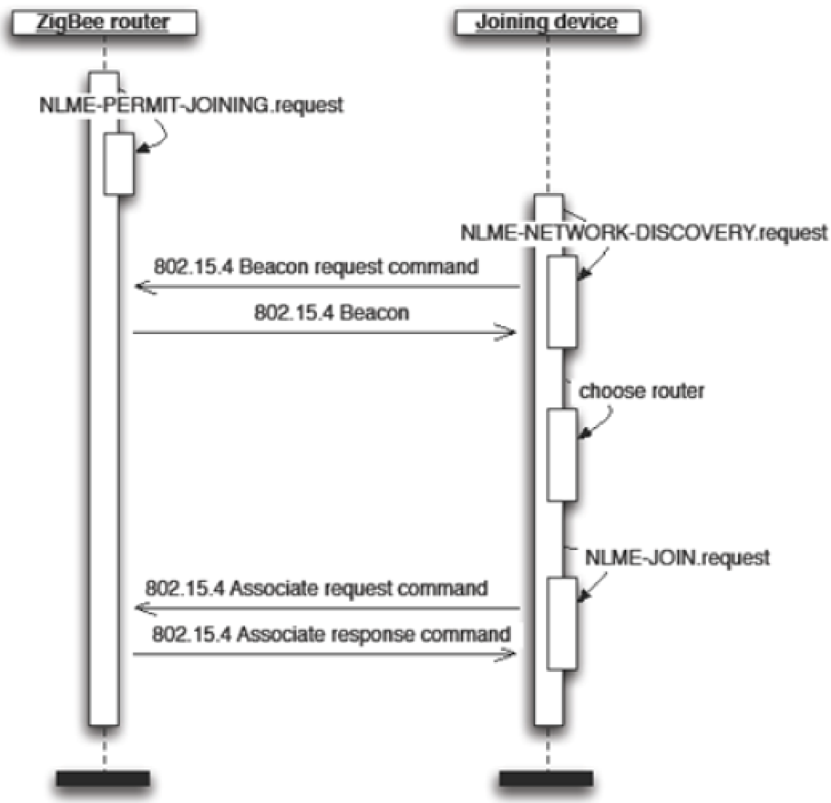

Figure 1.28: ZigBee MAC Association approach. [20]

1.7.6 Application Profiles, Clusters and Endpoints

Application Profiles

An Application Profile it's how different devices are organized in specific application each identified by a profile ID. There are two types of application profiles:

1. Public Application Profiles: Interoperable application software designed for a specific task.

2. Manufacturer-Specific Profiles: Private application profile. In an application profile all the devices share information with each other employing clusters, with the function of inputs or outputs from the device. Each cluster has a Cluster ID that uniquely identifies it in the application.

Endpoints

An endpoint it's a entity designed for a specific communication application and to clarify which packets are intended for each application and device. ZigBee devises could have 240 endpoints with endpoint zero dedicated to the ZigBee Device Object (ZDO), to provide control and management commands.

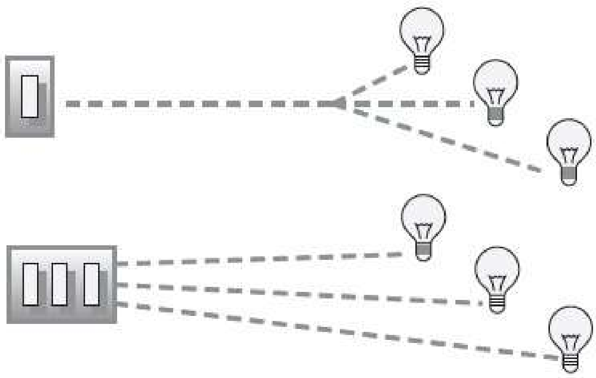

Figure 1.29: Endpoints As Virtual Wires Between Applications. [26]

ZigBee Cluster Library (ZCL)

The ZCL is a library of clusters available for any application. This allows common clusters to be reused: for example, the same lighting clusters can be used for all the application needs lighting controls. Each cluster has two "ends": client and server.

Bindings

Bindings can be defined as the links between two endpoints. A binding can be created between either one or more endpoints, as for lights and switches, that have have the same cluster IDs for input and output clusters.

1.8 Thread

1.8.1 Overview

The thread stack is a very reliable wireless protocol with such good features:

1. Simple network installation start-up and operation: thread networks systems can configure by them-self and when there is the need handle routing problems.

2. Secure: all the devices authorized in the network use an encrypted communication.

3. Small and large networks: for each network, there could be from several devices to hundreds of devices communicating flawlessly.

4. Range: the spread spectrum technology is adopted at the physical layer to reduce interference and cover an area of a standard house.

5. No single point of failure: the design of a Thread network allows each device to be replaced without interfering in the current communication.

6. Low power.

1.8.2 Device Types

1. Border Routers: A Border Router is a specific type of Router that operates as the link from the 802.15.4 network to adjacent networks on other physical layers (for example, Wi-Fi and Ethernet).In a Thread Network, there may be one or more Border Routers.

2. Routers: Routers are projected for routing services to other network devices. Routers are devices established to provide joining and security services that haven't the possibility to enter into sleep mode. sometimes routers can downgrade their functionality and act as REEDs (Router-eligible End Devices).

3. Router-Eligible End Devices: REEDs can become Routers but currently for the net conditions they does not act as Routers. These devices cant not have the function to send messages or provide joining and security services to other devices in the Thread Network. The Thread Network itself in extraordinary case upgrades REEDs to perform as Routers .

4. Sleepy End Devices: This are sleepy end devices or host devices. They share messages with their Parent Router but can not send nothing to other devices.

1.8.3 Protocol Stack

Thread stack shares the lower layers, PHY and MAC layers, with the IEEE 80.15.4-2006 Standard acting in the 2.4 GHz band at 250 kbps. Figure 1.30 illustrates the complete Thread stack. The 802.15.4 MAC layer is responsible for handling messages and routing control. This MAC level includes a CSMA (Carrier Sense Multiple Access) mechanism allowing devices both access to a clear channel and a link-level to ensure reliable communication between neighboring devices.

Adressing

Each device in a Thread network supports IPv6 [1] addressing layout and can creates one or more Unique local Address (ULA) or Global Unicast Address (GUA) addresses. The starter device set the ULA prefix for the Network. Each device has a 16-bit short address and Border Routers can have an additional prefix to generate other GUAs. In a Thread network devices use the Extended MAC Addresses to create their own interface identifier and derive the link local IPv6 address.

[1] IPv6 is version 6 of the Inter-Networking Protocol, classified as the third network level of the ISO/OSI model, created to interconnect heterogeneous networks in terms of technology, performance, management, and therefore implemented over other connection level protocols, such as Ethernet or ATM.

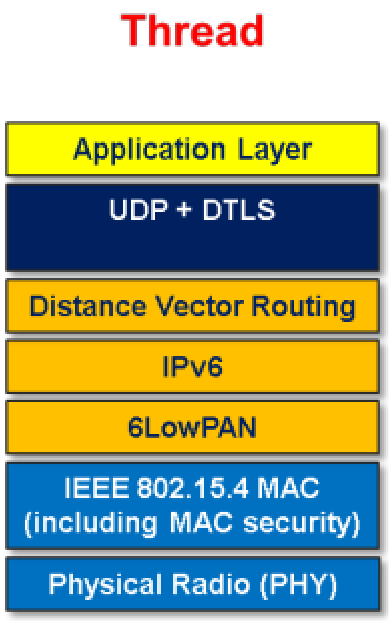

Figure 1.30: Thread Stack [17]

6LoWPAN

All the devices adopt a 6LoWPAN mechanism to reduce the IPv6 header dimension and consequently messages size. Router Parent also allocate short addresses for End Devices and REEDs that will use it to configure the mesh local ULA required for intranet communication.

ICMPv6

Devices support the Internet Control Message Protocol version 6 - ICMPv6 - used to monitor the status of the network and to send management and error packages and thus to report transmission errors. Echo messages typically sent, are used to verify the reachability of a node. These, like the ICMP protocol, can be of two types: request and reply.

UDP

The Thread standard uses the User Datagram Protocol (UDP) a communication protocol able to establish low-latency connections because it only sends packets, which means it has much lower overhead and bandwidth latency. UDP assign each port a numbers to help identify different user request commands and, sometimes a checksum value as receiving data accuracy validation. However, packets from master and them from the slave are identified by different paths and there cold be misunderstanding about their order or about who has send it.

1.8.4 Network Topology

The Thread stack supports full mesh connectivity between all Routers in the Thread Network. The final topology is chosen for the number of Routers because for one's there is a basic star topology otherwise a mesh topology is automatically formed as shown in Figure 1.31.

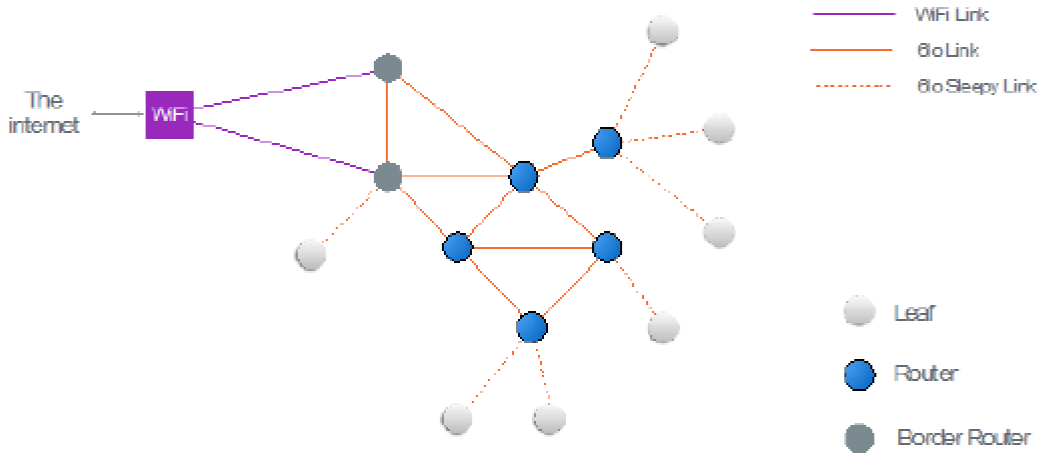

Figure 1.31: Basic Thread Network Topology and Devices [17]

Whit a limit 32 active Routers for Thread Network is built around the concept of No Single Point of Failure so all Router nodes maintain routes and connectivity with the others. Therefore the mesh networks are constantly maintained and connected allowing a more reliable radio system so in case of a busy node the mesh network transmits messages that hop upon multiple intermediary nodes. Usually the sleepy end devices - REEDs - forward directly their messages to a Parent Router Node which handles the routing operations for them.

1.8.5 Joining a Network

To take part in a Thread network and exchange useful application stack information inside and beyond the Thread Network, a device has to get through three different steps:

1. Discovering: Each device to enter the Thread Network needs to establish contact with the Router, then scans and sends on each available channel a beacon request and waits for a response. The beacon contains a payload that includes the network's SSID (Service Set Identifier) and indicates if the Thread Network is accepting new members.The new discovered Thread Network now sends MLE messages to connect to a nearby Router to perform commissioning routine.

2. Commissioning: Thread provides two useful commissioning methods for sharing commissioning information that will allow the joining device to connect to the Thread network once it has taken part. There is the out-of-band method or connect the commissioning session between a connected device and a commissioning application on a smartphone, tablet or web.

3. Attaching: The Parent Router is the connection node for the new joining device with the Thread network in which it is initially configured either as an end device or as a REED. Each new device exchanges MLE link configuration messages [see Figure 1.32] with the Parent Router which will then assign them to a short 16-bit address from the Parent Router.

MLE Messages

For all devices connected to a Thread Network, some important information is needed to keep the network access active. MLE controls all services to distribute network data and exchange connection costs and security counters. MLE messages handle the following informations:

1. 16-bit short and 64-bit EUI addresses 64 long addresses of adjacent devices

2. Device capabilities

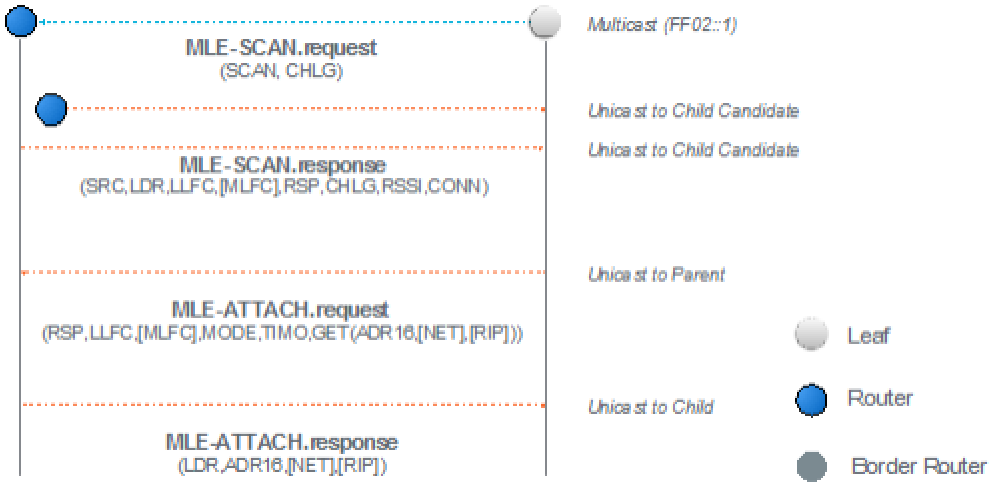

Figure 1.32: Attaching to a Thread Network [17]

3. Proximity connection costs (in the case of a router)

4. Security equipment and frame counters between devices

5. Routing costs to all other routers in the Thread Network

6. Updating network data.

DHCPv6

The DHCPv6, Dynamic Host Configuration Protocol version 6 is a UDP-based client-server protocol for configuring hosts with IP addresses, IP prefixes, and other useful configuration data to operate within an IPv6 network. DHCPv6 uses UDP to request data from a DHCP server. The DHCPv6 service on a In a Border Router The DHCPv6 service sets: - Network Addresses - Multicast addresses required by devices - Hostname Services.

Chapter 2

State of the Art

2.1 Wireless Body Area Network

This thesis project deals with the development of a small basic wireless body area network consisting essentially of two nodes, one capable of transmitting information and the other of collecting it. A wireless body area network (WBANs) consists of the connection of some devices with the task of collecting information - biosignals in case of biomedical applications - and to transfer them between the nodes up to the final one as a PC for data processing [[29], [30]] , features extraction or monitoring of vital parameters [31].

For WBANs, can be defined three levels of connection: Intra-BAN communications, Inter-BAN communications and beyond-BAN communications as shown in Figure 2.1. Intra-BAN communications indicate the exchange of information between wireless body sensors and the master node of the WBAN. The Inter-BAN communications refers to communications between a master node and other personal devices as personal computers and home robots applications. The Beyond-BAN level links personal devices to the Internet.

In this project, the design of an Inter-BAN communication as the server board is an host station connected to the PC was developed. The specific communication between the nodes was implemented through commercial wireless protocols available on the market and the chosen hardware. However, in other studies more channels were used to send messages, increasing the data throghput of the network [33]; the sending of

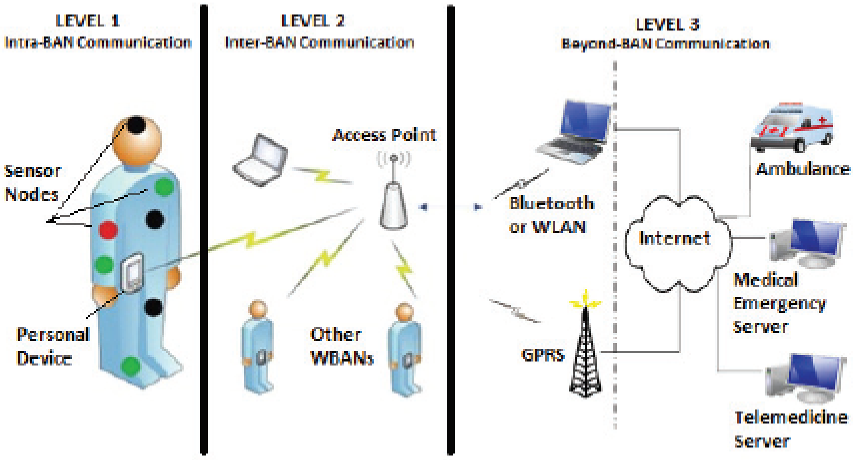

Figure 2.1: Wireless Body Area Networks Architectures. [16]

messages was tested using the human body as a means of transmission /antenna human body communication [32],or different wireless technologies [[34], [16]].

In all these case studies it has been given attention to low power consumption, latency, security and data throughput. For wearable sensors in fact it is to guarantee to function for many hours and the battery sometime can not be replaced. The issue of low power was investigated by [35] into wich researches focus on wireless energy transfer (WET) and wireless information transfer (WIT). The simulations results indicated as the size of data to transmitted is the first target to menage fo a WBANs: decreasing the input data size to transfer will lead to have mainly energy saving as the data size mostly impacts on the sensor consumption. So it's important to reduce the amount of information forwarding by the sensor device to the other one; this is the focus of the ATC technique as tested for this project.

Chapter 3

Materials and Metods

3.1 Acquisition System

This master thesis project aims to analyse and characterize performances and peculiarity of different wireless protocols to manage the event drive data transfer from an acquisition board to a host station, in which these will be processed. The real-time transmission of digital events generated from the acquisition of biomedical signals like sEMG (surface Electromyography) was investigated with the Average Threshold Crossing (ATC) technique. The board chosen to implement the transfer of data is a commercial development kit ;the nRF52840-DK of the Nordic Semiconductor® (Figure 3.1) . The server and the client node are implemented on the same type of board nRF52840-DK for each protocol.

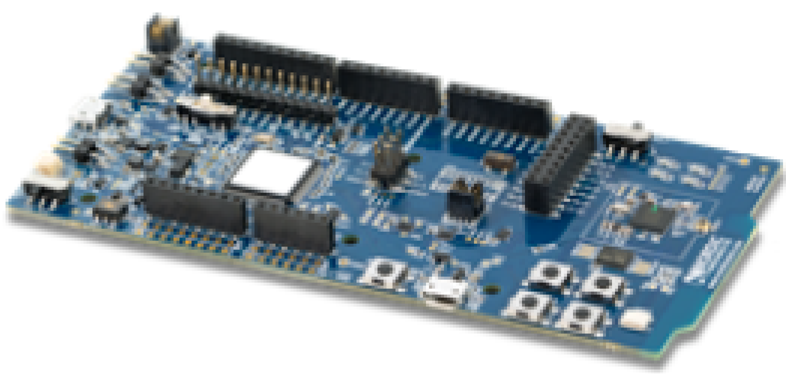

Figure 3.1: nRF52840 Development kit of Nordic Semiconductor®. [22]

The nrf52840-DK was chosen because is a multi-protocol System-on-Chip with very interesting features:

- it's a highly flexible single chip solution for short range wireless applications
- employs power and resource management to maximize application energy efficiency and battery life.
- all the peripherals have their own automated clock and power management to ensure they are powered down when not required to keep power consumption to a minimum.
- it's offered in a compact 7mm x 7mm package with 48 available GPIO.

In some applications like ZigBee and BLE Mesh also was used the nRF52840 Dongle of Nordic Semiconductor® (see Figure3.2) as the coordinator of the Network. The nRF52840 Dongle is a small, low-cost USB dongle with support for BLE, Bluetooth mesh, Thread, ZigBee, IEEE 802.15.4, ANT and 2.4 GHz proprietary protocols. The Dongle is the perfect counterpart hardware for nRF Connect for Desktop and the nrf52840-DK. It was used only as the coordinator role because there is not a debugger integrated and the nrf52840-DK was easier to debug with the Segger Embedded Studio IDE.

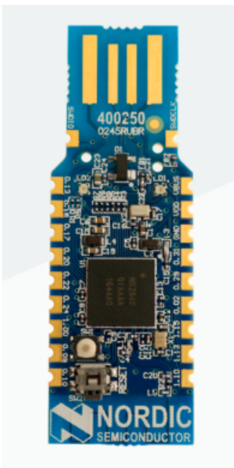

Figure 3.2: nRF52840 Dongle of Nordic Semiconductor®. [22]

Chapter 4

Firmware

The firmware of the NRF52840 is coded in C language with Segger Embedded Studio (SES), an Integrated Development Environment (IDE) that supports Nordic Semiconductor® devices. The real-time transmission of digital events generated from the microcontroller each time the biomedical signal in input overcomes a threshold is the TC value to be sent from the central device to the server device and execute the desired response. The following paragraphs will be dedicated to explaining how the TC signal was processed and sent for each wireless protocol available on the nrf52840-DK. Nordic Semiconductors® provides different software layers that help the developer to create his application more easily. As shown in the Figure 4.1 the Software Development Kit (SDK), Drivers and the SoftDevice interface the application layer on the top with the physical System on Chip (SoC). The SDK is a tool with different pre-compiled examples and firmware modules to assist in the interfacing of the SoftDevice and drivers with the user application, while the SoftDevice, for BLE and ANT protocol, is a group of pre-built binaries in which the Bluetooth and ANT Protocol Stack are already implemented.

4.1 BLE Implementation

For BLE protocol the employed SoftDevice is the s140 for this SoC.

The start point for BLE firmware implementation was the ble-app-hrs example opportunely modified. The initial configurations applied to the SoC are:

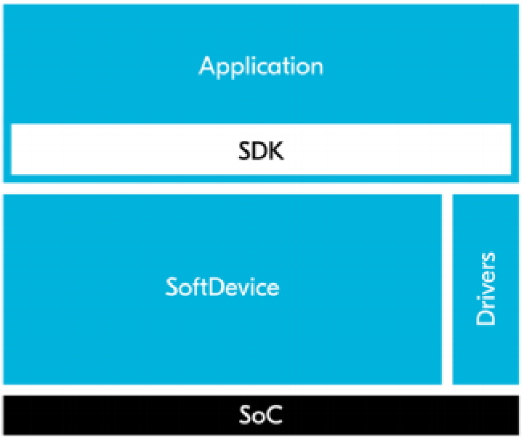

Figure 4.1: Interface between the application and the Nordic microcontroller. [23]

1. Input and Output pin setting: the pin 28 is employed as an input, for receiving the TC signal, the pin 15 performs an output for toggling the led state every time a single threshold crossing event takes place and a new event is forwarding . On the receiver device , the pin 13 performs an output for toggling the led state every time an event is received.

2. BLE stack start: the SoftDevice and the interruption due to a BLE event are enabled. Then, the GAP parameters are configured, such as device name, appearance, among others. Finally, the GATT module is started.

3. BLE min connection interval: this value has been setted to 7.5 ms as the limit value provided by the protocol standard 1.7.

4. Service and Characteristic creation: a service is generated with a characteristic and his attributes for handling the ATC notifying process. The application main service is organized as follow: the first characteristic contains the ATC current value and it possesses a declaration, the actual value and a CCCD descriptor which allows notifying the value. To enable notification this has been set to a two byte hexadecimal number equivalent to 1.

5. Advertising and idle state: the connection parameters are configured and the advertising begins while the main loop enters in an idle state in which it waits for the next event.

After the peripheral device is ready and it begins the advertising, some events have to be triggered by the central peer to accomplish its entire function. A flowchart, describing BLE application actuations and states, is shown in Figure 4.2. It can be observed from the chart that, after the link has been established the channel halts connected for distinct events. In this waiting state, a gpio input event generates the forwarding of a message to the central device.

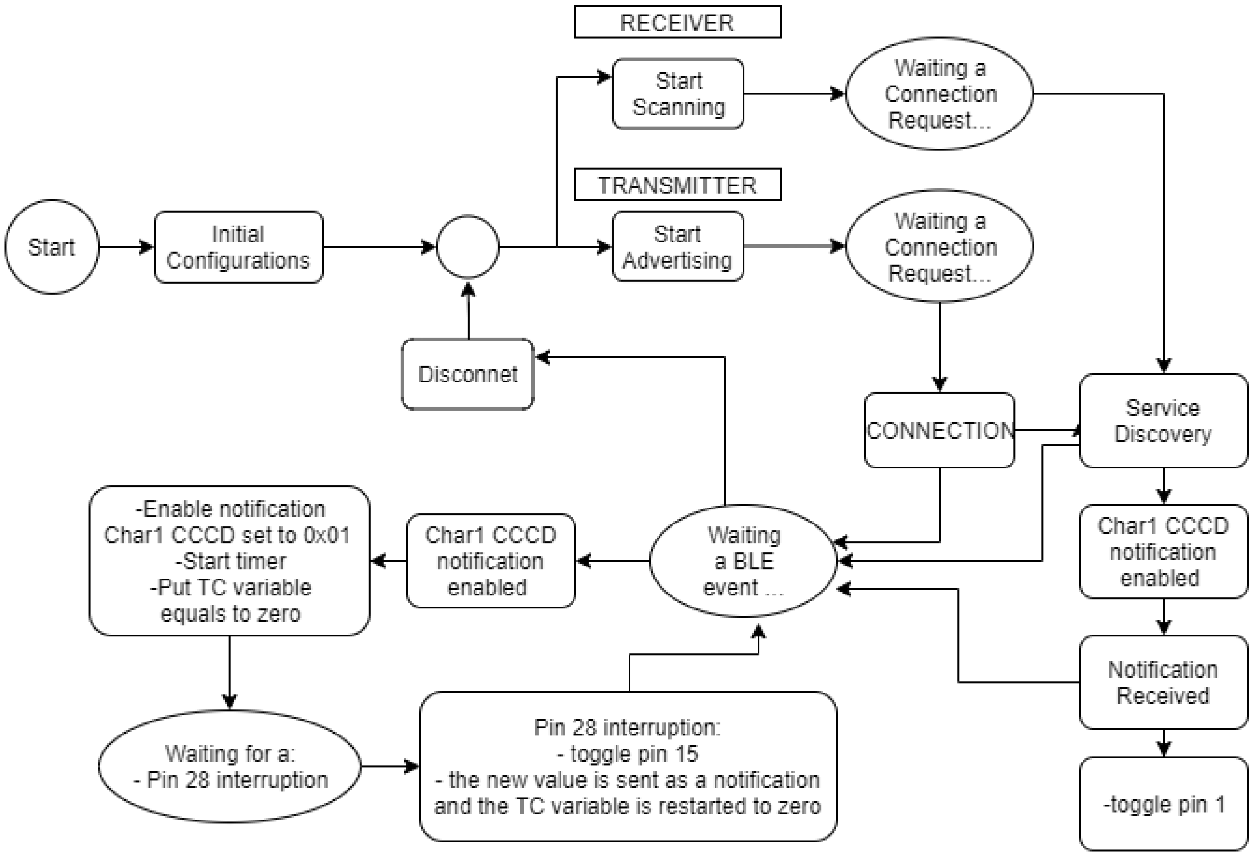

Figure 4.2: BLE Firmware Flowchart

4.2 Bluetooth Mesh Implementation

As the Bluetooth Mesh is based on the Bluetooth low energy part of the Bluetooth 4.0 specification and shares the lowest layers with this protocol also, need to employ a SoftDevice: again the s140 for this SoC. The start point for BLE Mesh firmware implementation was the light-switch example opportunely modified. The initial configurations applied to the SoC are:

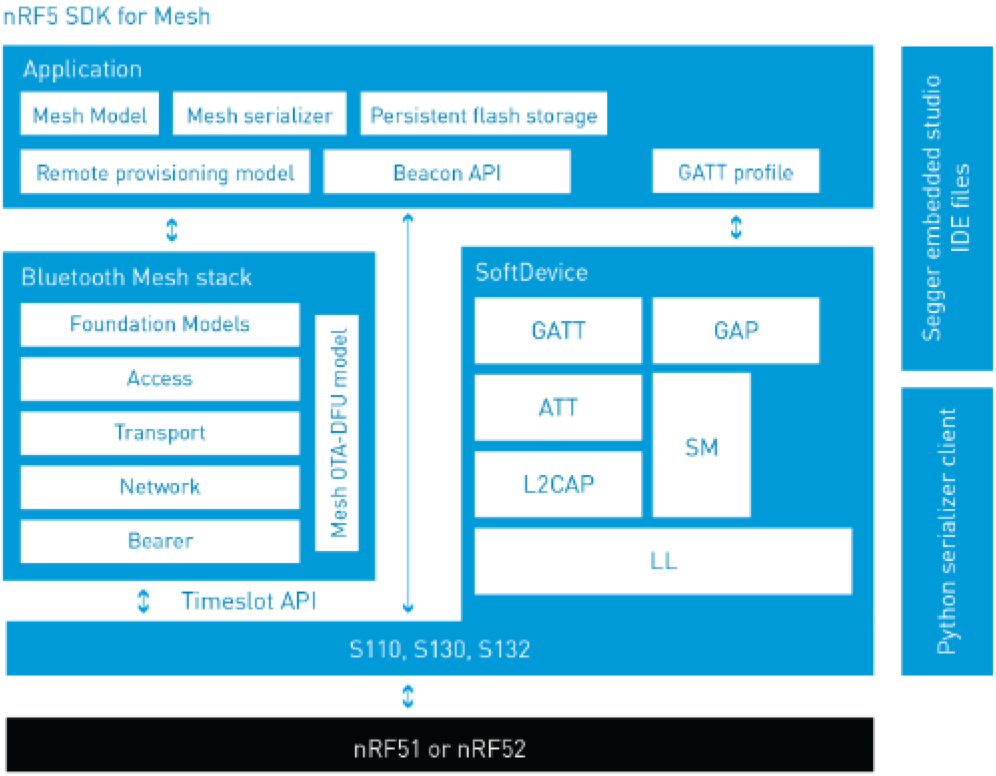

Figure 4.3: Interface between the BLE Mesh application and the Nordic microcontroller. [28]

1. Input and Output pin setting: the pin 28 is employed as an input, for receiving the TC signal, the pin 15 performs an output for toggling the led state every time a single threshold crossing event takes place and a new event is forwarding . On the receiver device , the pin 13 performs an output for toggling the led state every time an event is received.

2. BLE stack start: the SoftDevice and the interruption due to a BLE event are enabled. Then, the GAP parameters are configured, such as device name, appearance, among others. Finally, the GATT module is started.

3. BLE min connection interval: this value has been setted to 7.5 ms as the limit value provided by the protocol standard 1.7.

4. Server Number: the number of server was set to 1 to increase the probability to correct identify the server device and so the application data throughput .

5. Connection and idle state: the connection parameters are configured and the advertising begins while the main loop enters in an idle state in which it waits for

the next event.

After the peripheral device is ready and it begins the advertising, some events have to be triggered by the central peer to accomplish its entire function. The Nrf Mesh mobile App was used as the provisioned of the network. The Generic ON/OFF CLIENT MODEL is set to publish for the ON/OFF SERVER MODEL which in turn is set to subscribe for the first. A flowchart, describing BLE Mesh application trend of states, is shown in Figure 4.2. It can be observed from the chart that, after the link has been established the channel halts connected for distinct events. In this waiting state, a gpio input event generates the forwarding of a message to the central device.

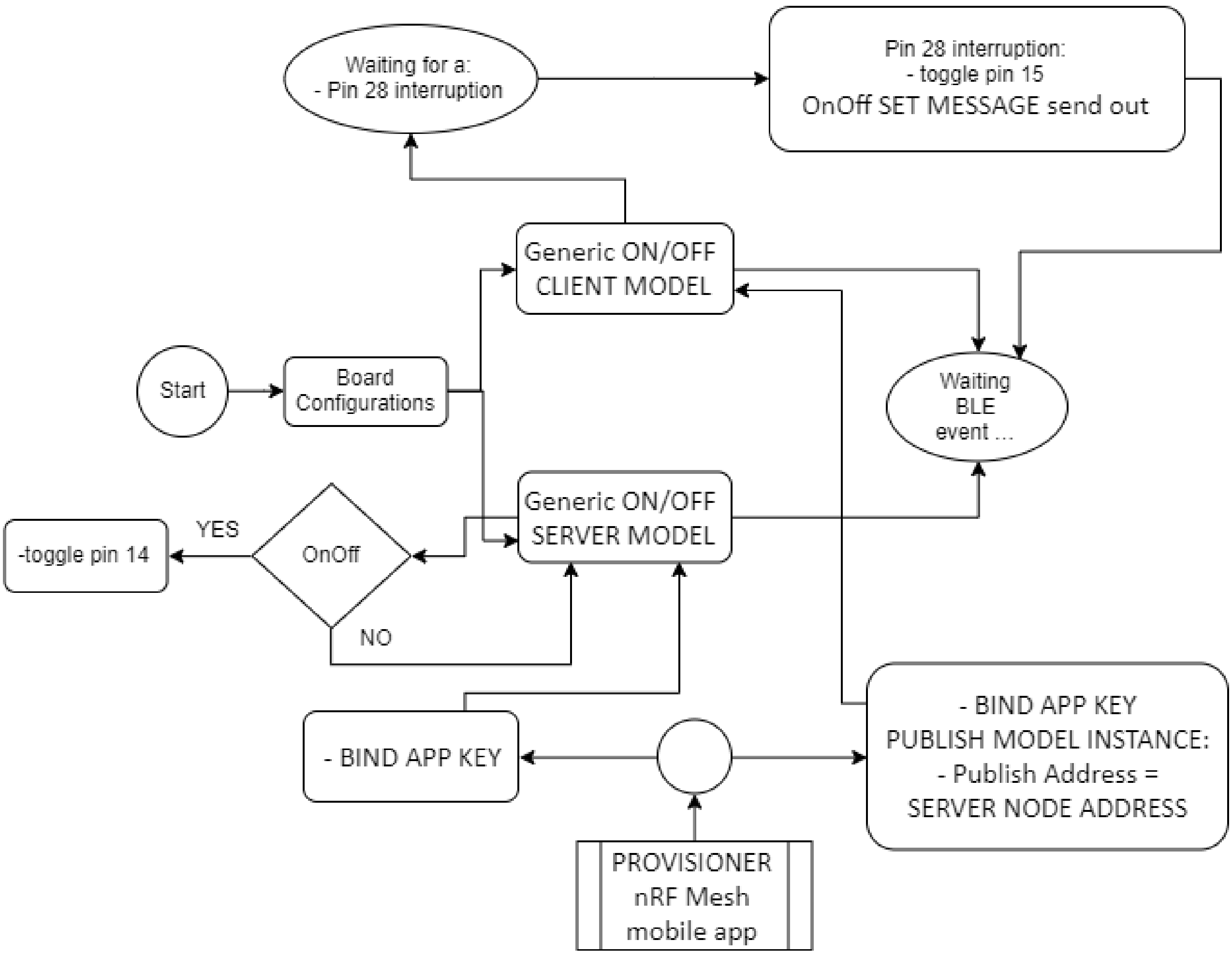

Figure 4.4: BLE Mesh Firmware Flowchart

4.3 ANT Implementation

For ANT protocol the employed SoftDevice is the s340 for this SoC.The start point for ANT implementation was the ant-broadcast example opportunely modified. The initial configurations applied to the SoC are:

1. Input and Output pin setting: the pin 28 is employed as an input, for receiving the TC signal, the pin 15 performs an output for toggling the led state every time a single threshold crossing event takes place and a new event is forwarding . On the receiver device , the pin 14 performs an output for toggling the led state every time an event is received.

2. ANT stack start: the SoftDevice and the interruption due to a ANT event are enabled. Then an NRF-SDH-ANT-OBSERVER is initialized to handle all the ANT events received to the SoftDevice stack event observer.

3. Channel Configuration as shown in Table 4.1

channel_config	TX	RX
.channel_number	0	0
.channel_type	0x10	0x00
.ext_assign	0x10	0x00
.rf_freq	66	66
.transmission_type	1	0
.device_type	2	0
.device_number	2	0
.channel_period	327	327
.network_number	0	0

Table 4.1: Channel configuration of the two ANT nodes.

4. Connection and idle state: the connection parameters are configured while the main loop enters in an idle state in which it waits for the next event.

After both devices are ready and enter in the idle state in order to capture next event. A flowchart, describing ANT application trend of states, is shown in Figure 4.5. It can be observed from the chart that, after the link has been established the channel halts connected for distinct events. In this waiting state, a gpio input event generates the forwarding of a message to the central device.

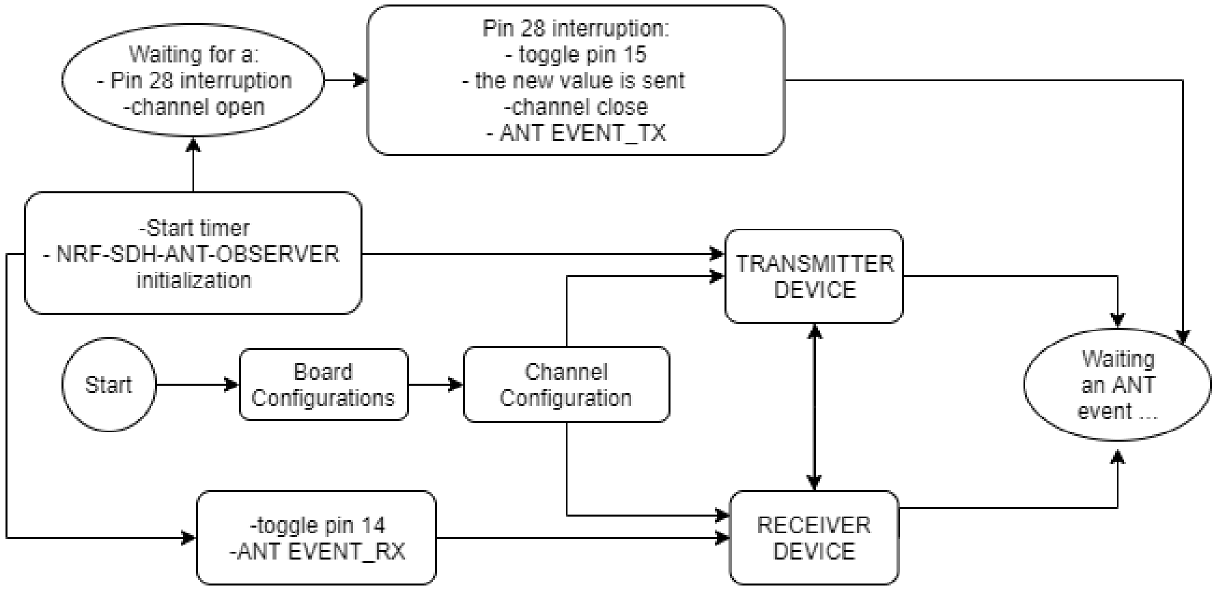

Figure 4.5: ANT Firmware Flowchart

4.4 IEEE 802.15.4 Implementation

For IEEE 802.15.4 protocol there is't to flash a SoftDevice on the SoC. The setup consist of two nRF52840-DK for the role of Router and End Device of the Network . The start point for IEEE 802.15.4 firmware implementation was the wireless-uart example opportunely modified. The initial configurations applied to the SoC are:

1. Input and Output pin setting: the pin 28 is employed as an input, for receiving the TC signal, the pin 15 performs an output for toggling the led state every time a single threshold crossing event takes place and a new event is forwarding . On the receiver device , the pin 13 performs an output for toggling the led state every time an event is received.

2. FSM start: the application task is initialized and the uart from the boards on the original configuration was disabled. The final state machine is launched.

3. Radio: the E-RADIO-TX-DONE and the E-RADIO.RX-DONE events were opportunely recall in the application. IEEE 802.15.4 is set to non-beacon enabled mode.

4. Connection and Idle state: the connection parameters are configured and the devices connect each other while the main loop enters in an idle state in which it

waits for the next event.

A flowchart, describing IEEE 802.15.4 application trend of states, is shown in Figure 4.6. It can be observed from the chart that, after the link has been established the channel halts connected for distinct events. In this waiting state, a gpio input event generates the forwarding of a message to the central device.

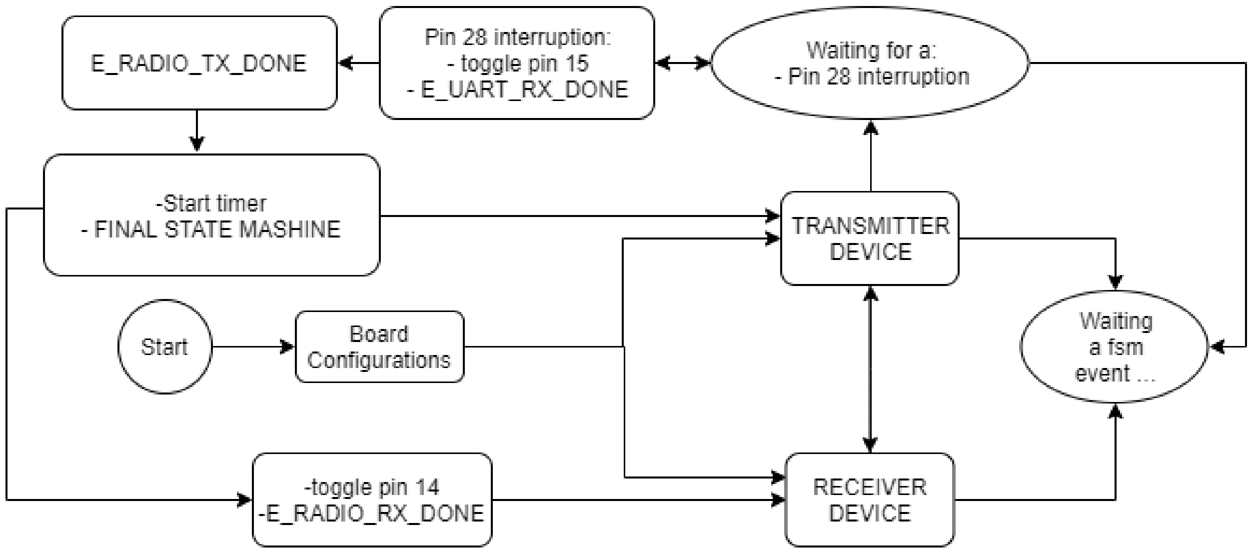

Figure 4.6: IEEE 802.15.4 Firmware Flowchart

4.5 ZigBee Implementation

For ZigBee protocol there is't to flash a SoftDevice on the SoC. The setup consist of two nRF52840-DK for the role of Router and End Device of the Network while a nRF52840 Dongle has been assigned to the role of Network Coordinator. The start point for ZigBee firmware implementation was the light-control example opportunely modified. The initial configurations applied to the SoC are:

1. Input and Output pin setting: the pin 28 is employed as an input, for receiving the TC signal, the pin 15 performs an output for toggling the led state every time a single threshold crossing event takes place and a new event is forwarding . On the receiver device , the pin 14 performs an output for toggling the led state every time an event is received.

2. ZigBee stack initialization and start: Zigbee stack uses ZBOSS a portable, high-performance Zigbee software protocol stack solution.

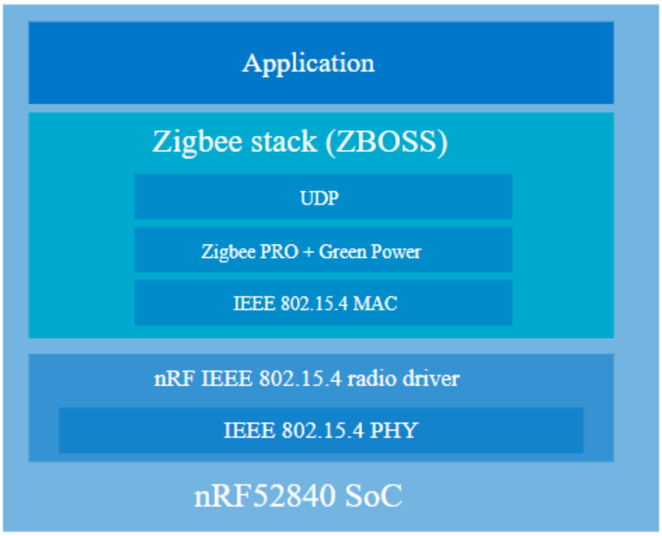

Figure 4.7: Zigbee architecture. [25]

3. Network Organization: Registration of ZCL endpoints and ZCL device context. Besides setting up defaults for the commissioning: network role, stack parameters (64-bit long address, security key, the maximum number of children, etc..).

4. Cluster application definition: On/Off Cluster implemented whit the two On/Off Switch attributes and commands for configuring on/off switching device.

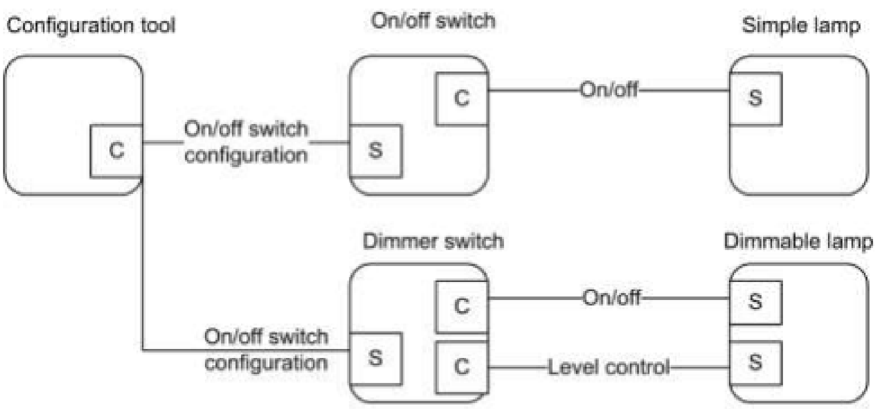

Figure 4.8: Typical Usage of On/Off and Level Control Clusters. [27]

5. Network start-up: the Coordinator performs the events needed to keep active info exchange between the Router and the End Device of the net.

6. Connection Idle state: the main loop enters in an idle state in which it waits for the next event.

After both devices are ready and enter in the idle state in order to capture next event. A flowchart, describing ZigBee application trend of states, is shown in Figure 4.5. It can be observed from the chart that, after the link has been established the system halts connected for distinct events. In this waiting state, a gpio input event generates the updating of the cluster attribute.

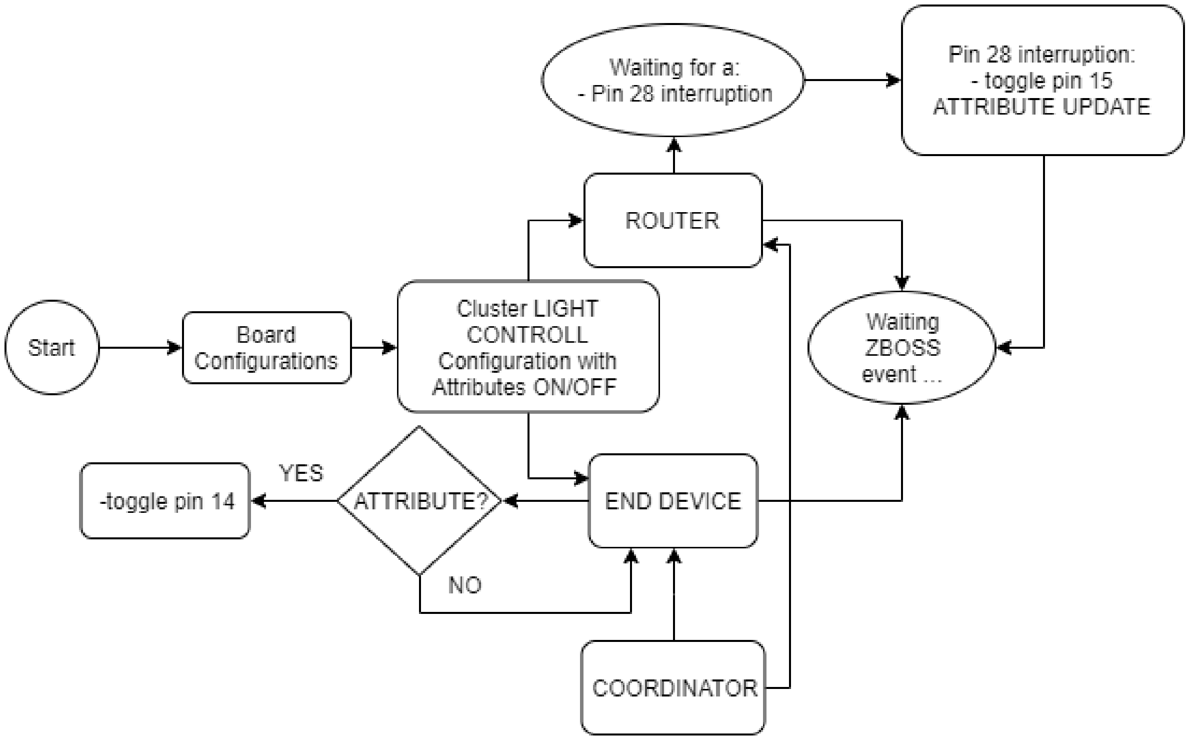

Figure 4.9: ZigBee Firmware Flowchart.

4.6 Thread Implementation

For Thread protocol also there is't to flash a SoftDevice on the SoC. The start point for Thread firmware implementation were the simple-coap-client and server examples opportunely modified. The setup consist of two nRF52840-DK for the role of Client and Server of the Network. The initial configurations applied to the SoC are:

1. Input and Output pin setting: the pin 28 is employed as an input, for receiving the TC signal, the pin 15 performs an output for toggling the led state every time

a single threshold crossing event takes place and a new event is forwarding . On the receiver device , the pin 14 performs an output for toggling the led state every time an event is received.

2. Thread stack initialization and start: The application layer of the example is built on top of the Constrained Application Protocol (CoAP); a specialized Internet Application Protocol for constrained devices.

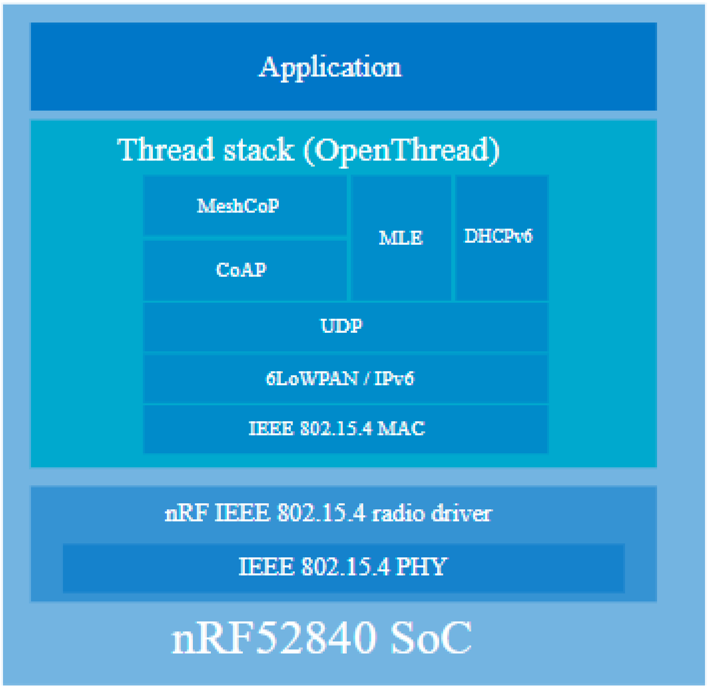

Figure 4.10: Thread Stack Overview.

3. Network start-up: the CoAP Client and the CoAP server of the net on startup, automatically enter the network with the default parameters.

4. Connections Idle state: the main loop enters in an idle state in which it waits for the next event.

After both devices are ready and enter in the idle state in order to capture next event. A flowchart, describing Thread application trend of states, is shown in Figure 4.12. It can be observed from the chart that, after the link has been established the system halts connected for distinct events. In this waiting state, a gpio input event generates the forwarding of the on/off command.

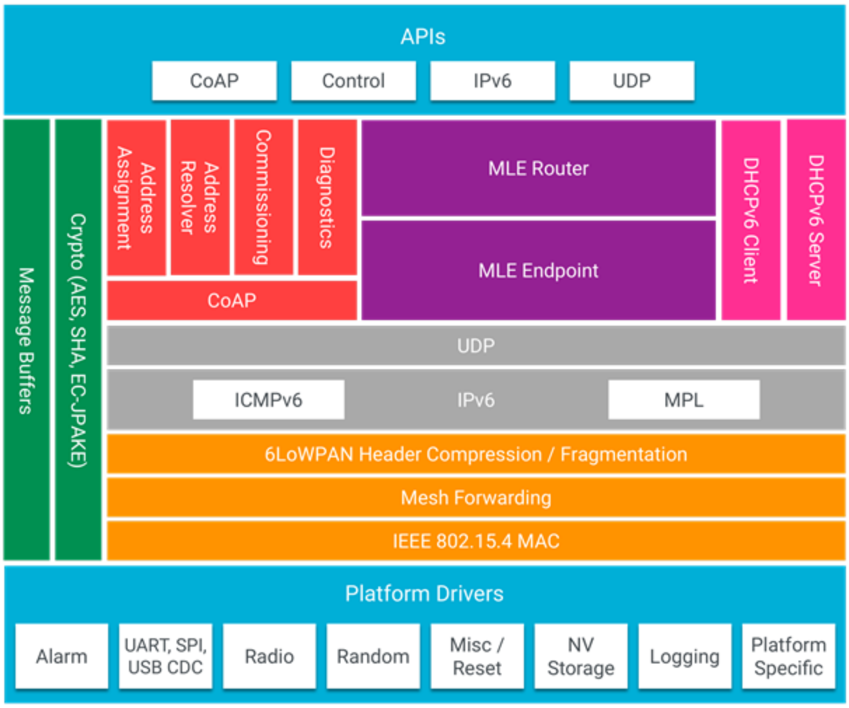

Figure 4.11: Thread Architecture.

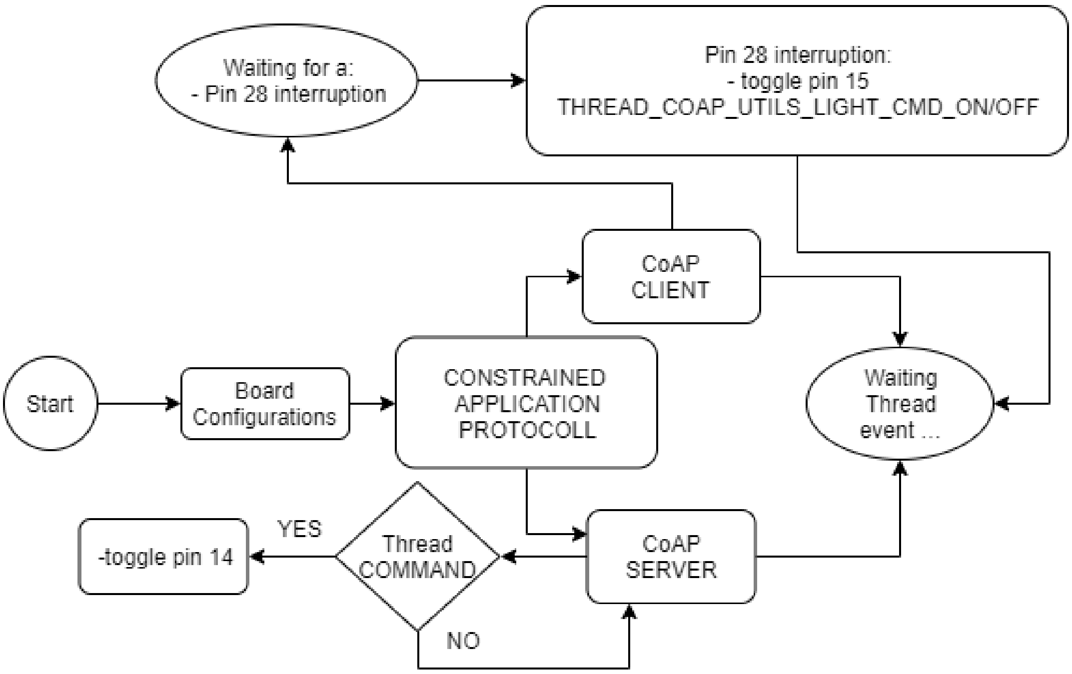

Figure 4.12: Thread Firmware Flowchart.

Chapter 5

Result and Discussion

At the end of the work,the performances were evaluated for each of the wireless standards about latency between transmitted and received event, consumption -measuring current peak on the transmitter node - and maximum events rate. In following all that aspects were analyzed in details.

5.1 Events Data Rate

To test the events data transfer rate, the two output signals -kept out from the nrf52840-DK boards - were connected with two probes connectable to the oscilloscope to analyze the corresponding square waveform frequencies. The sEMG signal was simulated with a square waveform of an appropriate frequency - increased for different test - with amplitude of 3Vpp and 50% of duty cycle. The pin 28 on the transmission node was configured as input port and the corresponding interruption on the rising edge input signal was enabled. As defined before pin 15 on the transmission device was configured as an output port a toggle of his state was effectuate any time an event is received. The correct transfer and receiving packet data were taken into account and BLE , IEEE 802.15.4 and Thread demonstrated to manage like 200 events per second. ANT also reached a 180 events per second.data transfer rate even if the channel period was opportunely set to right send a frequency of 200 Hz; maybe that it's a constrained value closer to the upper limit of the standard. BLE Mesh and ZigBee showed a lower events data rate with about 7 and 40 events per seconds respectively.

5.2 Latency Measurement

The measurement of the time intervals between the transmitted and received signals was obtained with the Universal Counter. The instrumentation was set up with a Labview program. Firstly, the instrument was configured, and the time interval measurement on rising and falling edges was set. The need to read continuously before the interval on the rising edges and then on the falling ones has driven to design a continuous acquisition with two different measurement configurations. It was used a TRUE / FALSE case structure controlled by a two variables equality condition. One is external and the other internal to the case structure and suitably updated at the end of each acquisition. Every 10 samples a statistic has been carried out and reported on a graph (see Figure 5.1) the obtained value, the average value and the standard deviation.

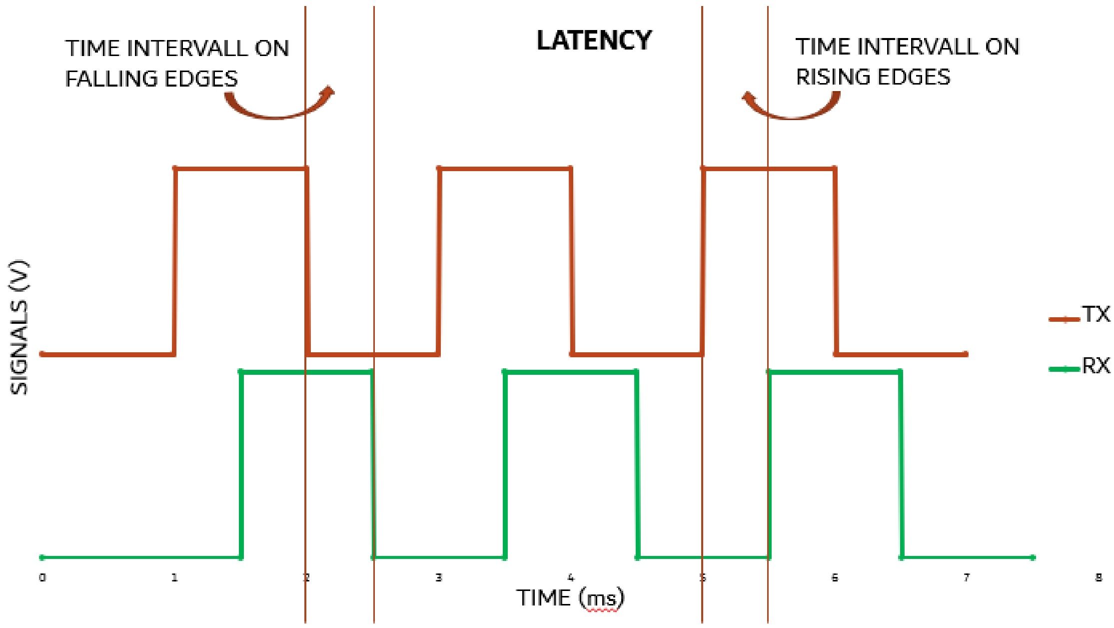

Figure 5.1: Latency Measurement.

5.2.1 Bluetooth Low Energy Latency

About BLE the maximum event data rate is of 200 Hz. In the Figure 5.2 are reported the latency values obtained for 100Hz and 200Hz. It's interesting to note as the the TX and RX signals are out of phase during a period of frequency for both the lower and the higher frequency reported. The signals continuously are out of phase by one period and then return to phase with a time interval varying of 0-20 ms for these reasons. It's important to note about the Figure 5.3 that the standard deviation for those values is really close to zero; an optimal result for biomedical applications.

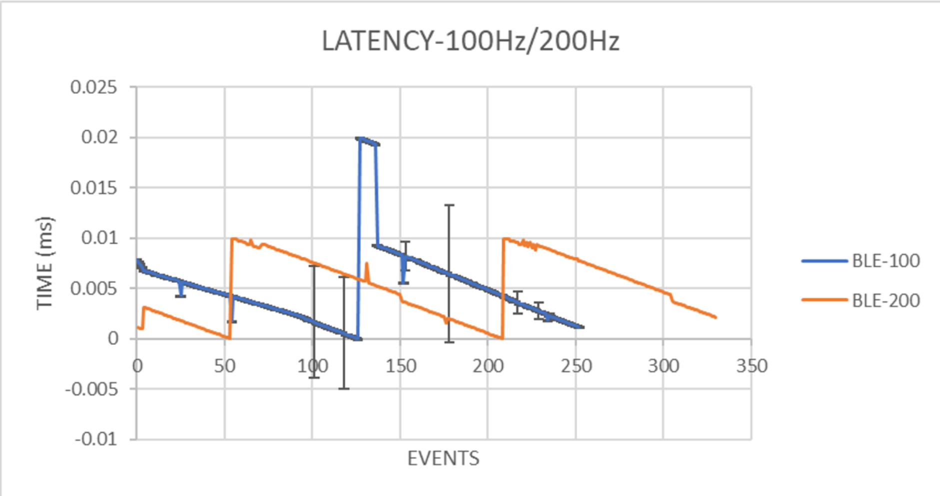

Figure 5.2: BLE Latency Measurement.

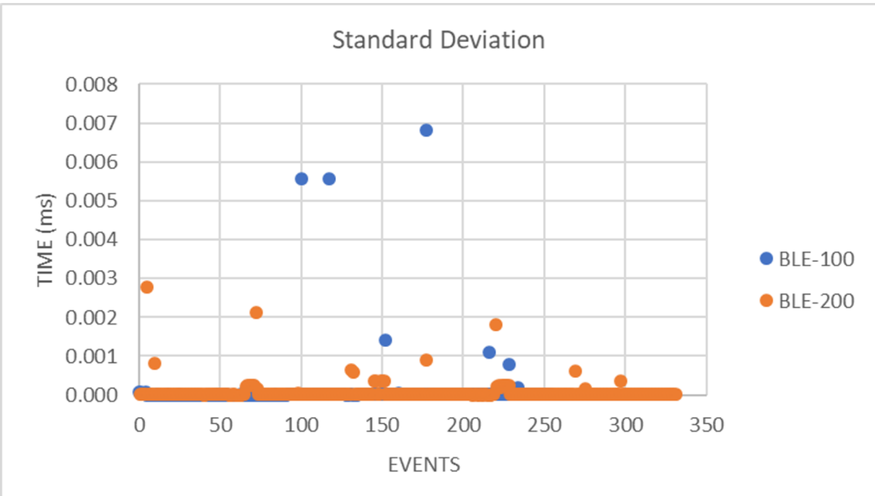

Figure 5.3: BLE Standard Deviation Measurement.

5.2.2 ANT Latency

For the ANT wireless protocol the maximum events data rate reached by the application is 160 Hz . In the Figure 5.4 are reported the latency values obtained for 100Hz and 160Hz. In that case the the TX and RX signals continuously seems to phase out and rephase-in with latency values of about 10/15 ms for 100 Hz and between 0/5 ms for the higher input data transfer. Also the Standard Deviation (Figure 5.5) calculated hop on different values and there is not constant.

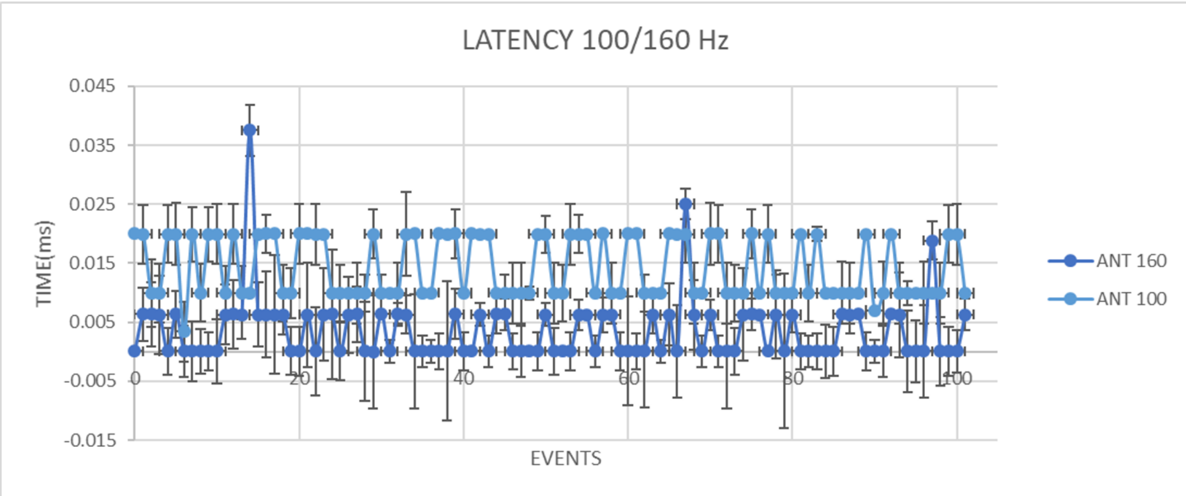

Figure 5.4: ANT Latency Measurement.

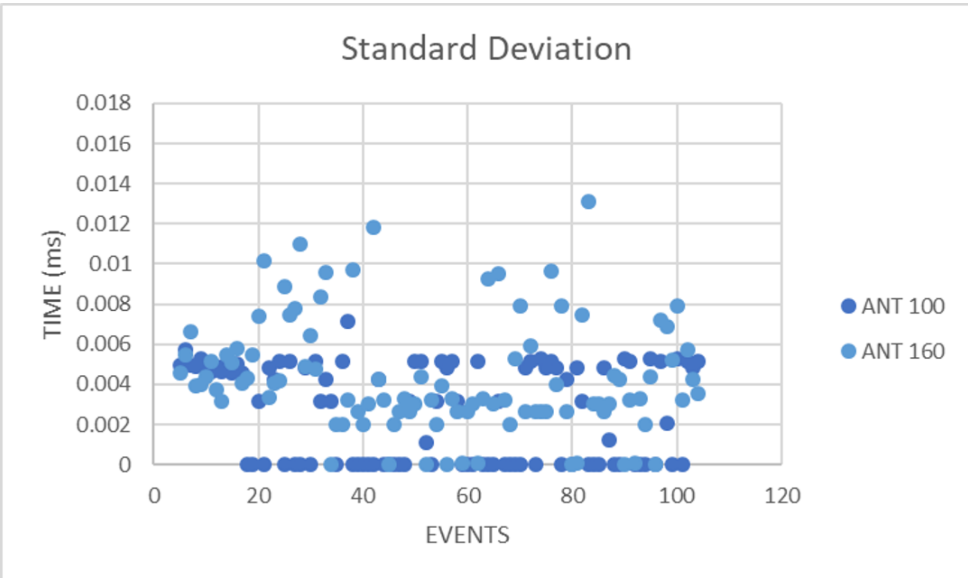

Figure 5.5: ANT Standard Deviation Measurement.

5.2.3 IEEE 802.15.4 Latency

For IEEE 802.15.4 wireless protocol the maximum events data rate correctly reached by the application is 200 Hz . In the Figure 5.6 are reported the latency values obtained for 100Hz and 200Hz. In that case the the TX and RX signals have a more constant behavior: for the 100 Hz the time interval from transmitted/received packets is about 16 ms while for the 200 Hz there are about 7 ms as the input signal frequency has a shorter period. About the standard deviation (Figure 5.7) is also for IEEE 802.15.4 constant with about 1/2 ms mismatch .

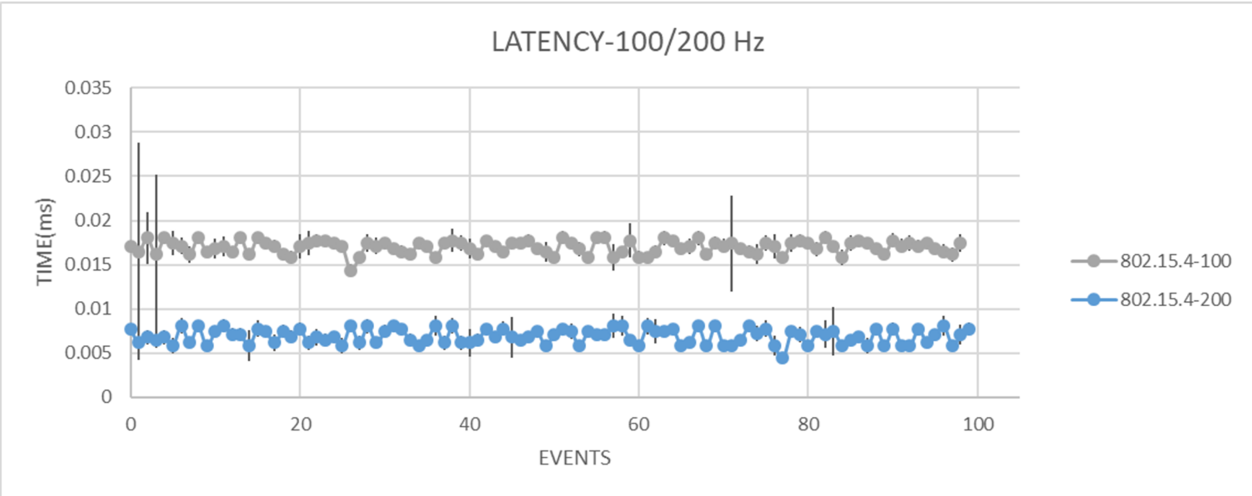

Figure 5.6: IEEE 802.15.4 Latency Measurement.

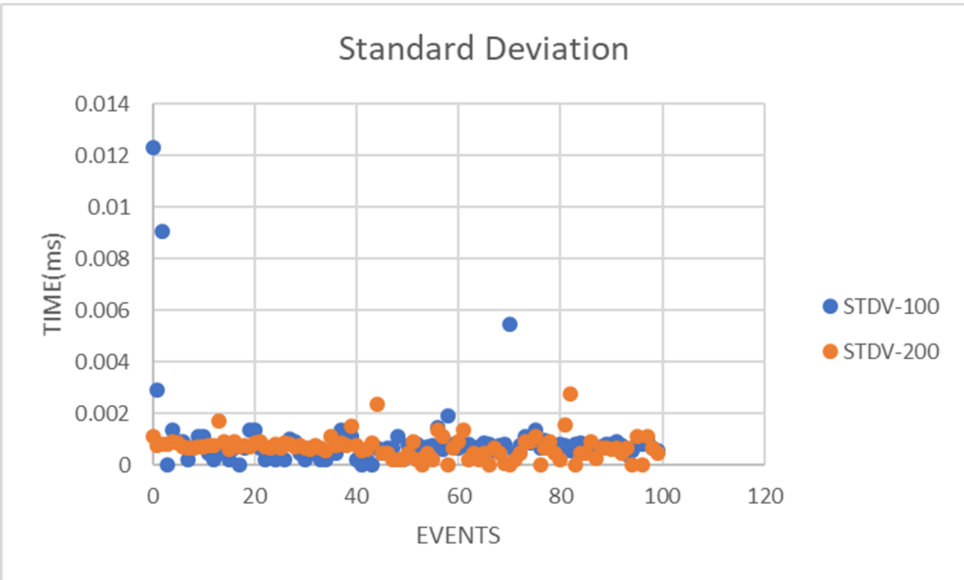

Figure 5.7: IEEE 802.15.4 Standard Deviation Measurement.

5.2.4 Thread Latency

About the Thread wireless protocol the maximum events data rate correctly reached by the application is 200 Hz . In the Figure 5.8 are reported the latency values obtained for 100Hz and 200Hz. For Thread as IEEE 802.15.4 as the TX and RX signals have a more constant behavior: for the 100 Hz the time interval from transmitted/received packets is about 15 ms while for the 200 Hz there are about 6 ms as the input signal frequency has a shorter period. About the standard deviation (Figure 5.9) Thread as the lowest values of about 1ms.

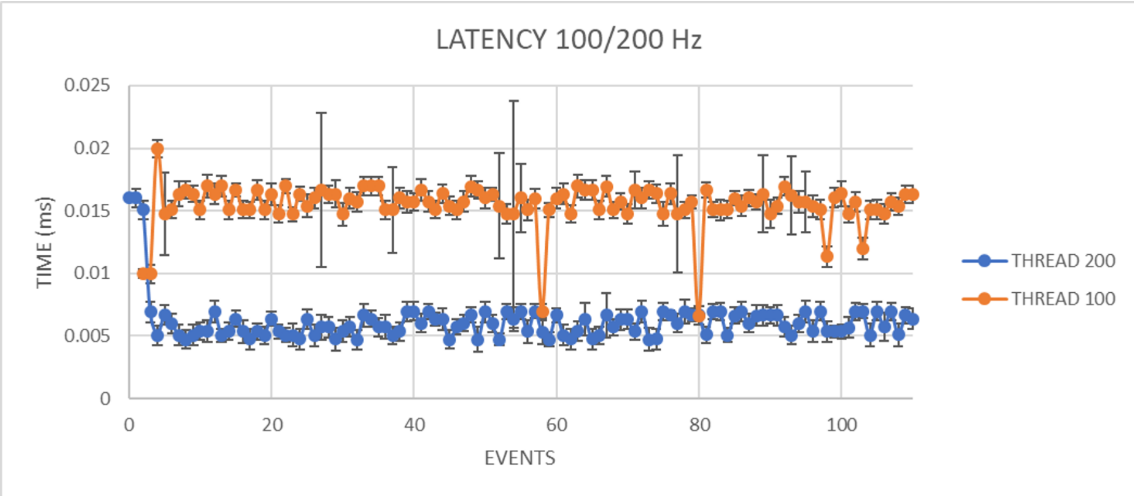

Figure 5.8: Thread Latency Measurement.

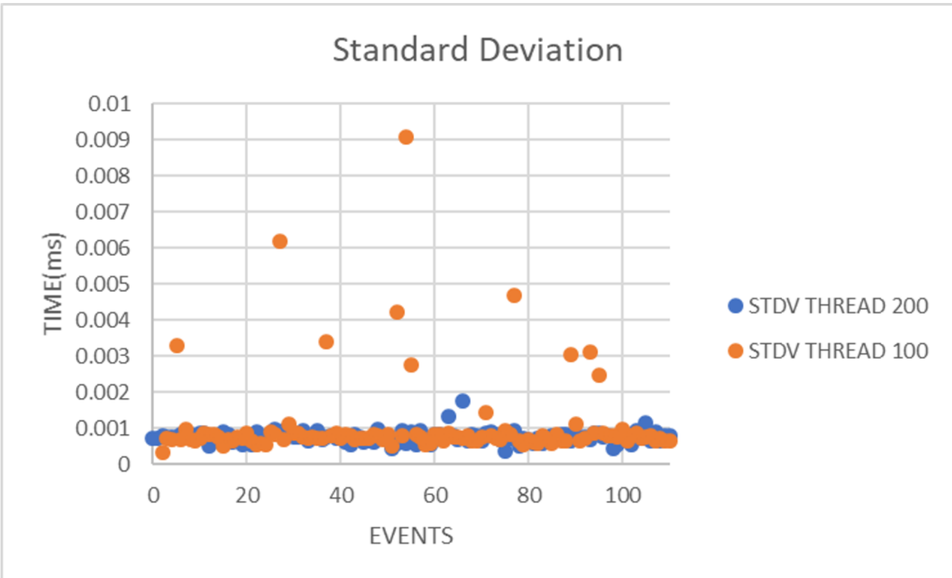

Figure 5.9: Thread Standard Deviation Measurement.

5.2.5 BLE Mesh and ZigBee

As stated before the events data rate obtained for BLE Mesh and ZigBee were not so satisfying. Values of only 40Hz for ZigBee and 7Hz for BLE Mesh are too far from satisfy the minimum requirements especially for biomedical applications. Also, the consumption relative to those standard has led not to conduct further tests.

5.3 Average Current Consumption

The average current consumption analysis has been performed using external equipment. The measurement has been made cutting a soldered bridge on the board to furnish power supply and applying an instrument on its extremities. In the beginning, an active current probe has been chosen to perform the measurement. The probe is connectable to the oscilloscope and provides on the output a voltage ten times greater than the related current one (1 mA -> 10 mV). Even if the generic waveform behavior was respected the results were not satisfying for that range of current (mA), having a lot of noise and sometimes even a negative average value. Considering those issues another instrument has been taken into account and the final measurements have been made using an INA126P. The measure is made taking the loss of voltage on a 10 Ω resistance and configuring the INA to amplify by a value of 5. In the Figure 5.10 are reported the values calculated for different frequencies.

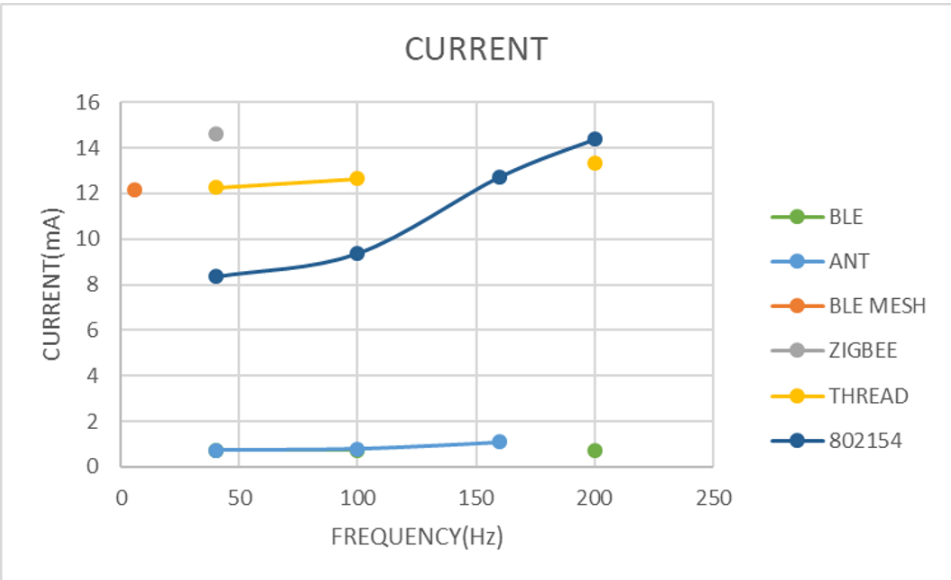

Figure 5.10: Average Current Peak consumption on Transmission Board.

BLE and ANT shown the lowest current consumption with values of about 1 mA for all the range frequency. Only for BLE, the graph (Figure 5.10) line slightly increases proportionately to the events data rate transmission. All other protocols are located at the top of the graph with average current consumption in a range from 12-16 mA. For BLE Mesh it is due to the need to be always in the scanning mode for the transmitter node. Besides it's really important to consider that only for BLE the transmission frequency does not influence the period and frequency of the current peak which occurs at regular intervals of about 1 ms. All the other standard has the current peak in correspondence of the packet transmission and for the higher frequency it occurs more times, increasing the overall consumption of the board.

Chapter 6

Conclusion

A small wireless body area network has been developed in this master thesis project. First of all, the most appropriate hardware has been chosen and an application has been designed to transfer digital events generated by a micro-controller through various wireless protocols available on the market and on the chosen board.

The biological input signal - sEMG for the specific final application - has been processed using the ATC technique, able to reduce the number of events to be transmitted, and for this reason also the consumption on the transmission sensor, the costs and the size of the devices required to manage and transfer a smaller amount of data.

Like other studies in the literature, to evaluate the performance of the wireless protocols available on the market were calculated the maximum events data rate, the average peak current in terms of consumption, and finally latency. In biomedical applications, it is necessary to pay attention to reduce consumption for the development of low power and wearable devices able to manage long hours of autonomy. Moreover must to be reduced latency as the time interval between transmitted and received signal as the response of the system must be as short as possible and so the signal has to arrive in real-time to the other peer of the network. Finally, we tried to increase the maximum data throughput as the maximum number of events transmitted by the client and correctly detected by the receiver device per second.

The communication has been managed one-by-one between a sensor device and a host station connected to a PC for the post-processing of the received data. The wireless protocols BLE, BLE Mesh, ANT, IEEE 802.15.4, Thread and ZigBee - available on nrf52840-DK as hardware setup for the central and server devices - have been reviewed and tested for the forwarding of a packet each time the input signal overcome a fixed threshold.

The tests carried out on two signals output by both nrf52840-DKs have shown that BLE and ANT are the two standards that best hit the target of a low power data transfer with an average current consumption of just 1mA and a good events data transfer of 200 events per second. Otherwise they both show values regarding latency that is not constant and for ANT the standard deviation is too variable. Instead, BLE Mesh and ZigBee, given the recorded results have the lowest data throughput and instead too high current consumption, so were neglected. Moreover, both manage a type of mesh network with different kinds of nodes, each with its specific network function, while in this specific application communication has been designed between two nodes: one transmitter and the other receiver of the biological signal of interest.

On the contrary for IEEE 802.15.4 and Thread have been recorded numbers of correct current consumption and latency bigger but too much more stable than the other ones, and regarding to Thread it has a standard deviation on only 1ms; a very good result for this kind of applications considering up to 200 events per second of correct data transfer between devices.

Therefore, refer to the final reader to choose according to his goals, whether to transfer the data from the sensor to the PC favoring low consumption by choosing the BLE or to bet on higher data throughput and lower and stable latency values with higher current consumption, choosing to use Thread wireless standard.

Bibliography

[1] An IoT Real-Time Biometric Authentication System Based on ECG Fiducial Extracted Features Using Discrete Cosine Transform - Scientific Figure on ResearchGate.

[2] https://i.stack.imgur.com/9vwcE.png

[3] American Journal of Computing Research Repository. 2014, 2(4), 66-70 doi:10.12691/ajcrr-2-4-3.

[4] Biomedical Time Series Processing and Analysis Methods: The Case of Empirical Mode Decomposition - Scientific Figure on ResearchGate.

[5] S. Sapienza, M. Crepaldi, P. Motto Ros, A. Bonanno, and D. Demarchi, On Integration and Validation of a Very Low Complexity ATC UWB System for Muscle Force Transmission, IEEE Transactions on Biomedical Circuits and Systems.

[6] Yan Liu et al 2018 J. Neural Eng.15 016016

[7] Neftci E., Das S., Pedroni B., Kreutz-Delgado K., Cauwenberghs G. (2014). Event-driven contrastive divergence for spiking neuromorphic systems. Front. Neurosci. 7:272. 10.3389/fnins.2013.00272

[8] Ramezani R, Zhang W, Xie Z, et al. A Combination of Indoor Localization and Wearable Sensor-Based Physical Activity Recognition to Assess Older Patients Undergoing Subacute Rehabilitation: Baseline Study Results. JMIR Mhealth Uhealth. 2019;7(7):e14090. Published 2019 Jul 10. doi:10.2196/14090

[9] Alfian G, Syafrudin M, Ijaz MF, Syaekhoni MA, Fitriyani NL, Rhee J. A Personalized Healthcare Monitoring System for Diabetic Patients by Utilizing BLE-Based Sensors

and Real-Time Data Processing. Sensors (Basel). 2018;18(7):2183. Published 2018 Jul 6. doi:10.3390/s18072183

[10] Lin YW, Lin CY. An Interactive Real-Time Locating System Based on Bluetooth Low-Energy Beacon Network †. Sensors (Basel). 2018;18(5):1637. Published 2018 May 21. doi:10.3390/s18051637

[11] nordicsemi.com/Products/Low-power-short-range-wireless/Bluetooth-low-energy

[12] Multi-hop Real-time Communications over Bluetooth Low Energy Industrial Wireless Mesh Networks - Scientific Figure on ResearchGate

[13] Radio Beacons in Indoor Navigation - Scientific Figure on ResearchGate.

[14] Townsend, Kevin, Carles Cufí, and Robert Davidson. Getting started with Bluetooth low energy: tools and techniques for low-power networking. " O'Reilly Media, Inc.", 2014.

[15] This is ANT Ant Message Protocol and Usage.

[16] Negra, Rim, et al. "Wireless Body Area Networks: Applications and Technologies" Procedia Computer Science, vol. 83, 2016, pp. 1274–1281.

[17] Fundamentals, Thread Stack. "Thread Group." White Paper, July (2015).

[18] Baert, Mathias, et al. "The Bluetooth mesh standard: An overview and experimental evaluation." Sensors 18.8 (2018): 2409.

[19] Solda,Vojjala, "Getting Started with Bluetooth Mesh".

[20] "Getting Started with ZigBee and IEEE 802.15.4"

[21] J. A. Gutierrez, et al, "IEEE Standard for Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPAN) - Draft D16", IEEE - 2002.

[22] "nrf52840"https://www.nordicsemi.com/Products/Low-power-short-range-wireless/nRF52840.

[23] "Nordic Semiconductor, Software and Tools" from https://www.nordicsemi.com/Software-and-Tools/Software, Accessed: 1 May 2019.

[24] "nrf52840 Dongle" https://www.nordicsemi.com/Software-and-tools/Development-Kits/nRF52840-Dongle/GetStarted

[25] "Zigbee platform designs" https://infocenter.nordicsemi.com/index.jsp

[26] "ZigBee applications - Part 5: Addressing within the node" https://www.eetimes.com/document.asp

[27] 07-5123-06-zigbee-cluster-library-specification.pdf.

[28] https://infocenter.nordicsemi.com/index.jsp?topic=

[29] Manoni, Lorenzo, et al. "A Comparative Study of Computational Methods for Compressed Sensing Reconstruction of EMG Signal." Sensors 19.16 (2019): 3531.

[30] Teng, Xiao-Fei, et al. "Wearable medical systems for p-health." IEEE reviews in Biomedical engineering 1 (2008): 62-74.

[31] Li, Rui, Daniel TH Lai, and WeeSit Lee. "A survey on biofeedback and actuation in wireless body area networks (WBANs)." IEEE reviews in biomedical engineering 10 (2017): 162-173.

[32] Das, Debayan, et al. "Enabling covert body area network using electro-quasistatic human body communication." Scientific reports 9.1 (2019): 4160.

[33] Januszkiewicz, Łukasz, Paolo Di Barba, and Sławomir Hausman. "Multi-Objective Optimization of a Wireless Body Area Network for Varying Body Positions." Sensors 18.10 (2018): 3406.

[34] Adibi, Sasan. "Link technologies and BlackBerry mobile health (mHealth) solutions: a review." IEEE Transactions on Information Technology in Biomedicine 16.4 (2012): 586-597.

[35] Hao, Yixue, et al. "Energy harvesting based body area networks for smart health." Sensors 17.7 (2017): 1602.

[36] https://commons.wikimedia.org/wiki

[37] Abdala, Mohammed and Salih, Alaa. (2012). Design and Performance Analysis of Building Monitoring System with Wireless Sensor Networks. Iraqi Journal of Science. 53. 1097-1102.