FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Wireless Solutions for Household Appliances

João Tiago Caetano Águia de Moura

WORKING VERSION

Mestrado Integrado em Engenharia Eletrotécnica e de Computadores

Academic Supervisor: Eng. Pedro Alexandre Rodrigues João

Corporate Supervisor: Eng. Catarina Maria Brito de Noronha Santiago, PhD

June 25, 2017

Resumo

Nas palavras de Eric Schmidt, "No futuro, a Internet desaparecerá. Não a sentirás, pois estarás sempre na sua presença". A presente dissertação aborda o desafio de projetar soluções *wireless*, no contexto da Internet das Coisas, para dispositivos de aquecimento de água da Bosch Termotecnologia S.A. O objetivo principal deste documento é incorporar os esquentadores com conectividade fiável em qualquer ponto da casa, permitindo que os dispositivos sejam controlados remotamente. Dado o contexto empresarial desta dissertação, são também objetivos minimizar o consumo energético e o custo da solução *wireless*. A empresa definiu uma solução base de hardware: um *dongle wireless* que usa o microcontrolador CC2531 da Texas Instruments, deixando para desenvolvimento: 1) uma implementação de software baseada em ZigBee na solução base e 2) a pesquisa de uma solução alternativa que superasse a existente em alcance, custo e consumo energético.

A partir desta dissertação foi possível desenvolver um protótipo que comprovasse o conceito e atendesse aos requisitos de controle remoto em esquentadores Bosch. Após este trabalho, apoiado pelos resultados do teste de desempenho sem fio, o autor observa que a nova solução, o microcontrolador CC1310 da Texas Instruments, supera em todos os requisitos: alcance, custo e consumo energético, quando comparado com a solução base. Em matéria de software, é reconhecida como vantajosa a facilidade de desenvolvimento e a conectividade aprimorada no uso de protocolos padronizados e pertencentes ao domínio público. No entanto, as soluções proprietárias e personalizadas são melhor dimensionadas para os desafios e apresentam melhor segurança nas comunicações, uma vez que as *frames* e as *payloads* não são do conhecimento público. Deste modo, o protocolo é baseado em ZigBee, no entanto adota uma camada aplicacional proprietária, por forma a aproveitar sinergias protocolares nesta aplicação. Finalmente, embora esta dissertação estude um problema específico, o autor considera esta dissertação relevante para indivíduos ou organizações que procurem soluções *wireless* em aparelhos domésticos, no espírito da Internet das Coisas.

Abstract

In the words of Eric Schmidt, "In the future, the Internet will disappear. You won't even sense it, it will be part of your presence all the time.". The present dissertation addresses the challenge of designing wireless solutions within the context of the Internet of Things for Bosch Termotecnologia S.A. water heating devices. The main objective is to embed water heaters with ubiquitous and reliable connectivity within the house, enabling devices to be remotely controlled. Keeping power consumption and cost to a minimum is also an objective of this project, since it was developed in a corporate environment. The company defined a base hardware solution: a wireless dongle using the Texas Instruments microcontroller CC2531, leaving to be developed: 1) a ZigBee based software implementation on the base solution and 2) to research an alternative solution that would surmount the existing one in range, cost and power consumption.

From this dissertation it was possible to develop a prototype proving the concept and meeting the requirements of remotely controlling Bosch gas water heaters. After this work, supported by the wireless performance test results, the author observes that the new solution, Texas Instruments microcontroller CC1310, outperforms in all requirements (range, cost and power consumption) when compared with the base solution. In matters of software, it is recognized as advantageous the ease of development and enhanced connectivity of using standard protocols in the public domain. However, tailored proprietary solutions present an enhanced fit for the challenge and also improved security in communications, since data frames and payloads are not of public knowledge. Therefore, the protocol is based on ZigBee but follows a proprietary high-level for synergy of both solutions. In a closing remark, although this dissertation is aimed at a concrete case, this dissertation is deemed relevant for individuals or organizations that pursue wireless solutions design for household appliances, trending on the Internet of Things.

Acknowledgements

Firstly, I would like to thank my academic supervisor Prof. Pedro João and my corporate supervisor Eng. Catarina Santiago for their relentless guidance and support. Every time I stumbled upon a tougher challenge, their door was always open.

I would also like to express my sincere appreciation to my team leader at Bosch Termotecnologia S.A., Eng. Nuno Silva, for the opportunity of this curricular internship and all precious insights in engineering and leadership I've witnessed during this period.

I would also like to acknowledge my colleages at Bosch Termotecnologia S.A., for their support in this endeavor. A special thanks to my team mates at ENG3.2: Bruno Pereira, Diogo Guimarães, Inês Vaz, Hugo Costa, José Oliveira, Luís Terra, Paulo Lopes, Ricardo Vieira, Sérgio Conceição, Sérgio Ferreira, Rúben Martins and Hugo Lebre. I would also like to acknowledge some particular remarks to André Ribeiro, Simão Ribeiro, Nélson Capela, Fábio Valente, Joaquim Ribeiro and Igor Trindade. It was my pleasure to work alongside you.

On another note, I would like to thank all my academic professors, both in Portugal and Macau, for their guidance and wisdom, in contributing to the engineer I almost am.

Finally, I must express my profound gratitude to my parents, to my girlfriend Joana and my friends António, Francisco and Luís and all other friends, for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this dissertation. This accomplishment would not have been possible without them. Thank you.

J. Tiago Águia de Moura

NANOS GIGANTUM HUMERIS INSIDENTES

* * *

"If I have seen further, it is by standing on the shoulders of giants."

Sir Isaac Newton

Contents

List of Figures

List of Tables

Abbreviations

AES	Advanced Encryption Standard
API	Application Programming Interface
bps	bits per second
dB	decibel
dBm	decibel-milliwatts
GmbH	*Gesellschaft mit beschränkter Haftung* (Company with limited liability)
GWH	Gas Water Heater
Hz	Hertz
IDE	Integrated Development Environment
IEEE	Institute for Electrical and Electronics Engineers
ISM	Industrial, Scientific and Medical (frequency bands)
IoT	Internet of Things
PCB	Printed Circuit Board
RF	Radio Frequency
R&D	Research and Development
S.A.	Sociedade Anónima
SHA	Secure Hash Algorithm
UART	Universal Asyncronous Receiver and Transmitter
WCP	Wireless Communications Protocol
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WHAN	Wireless Home Area Network
WWW	*World Wide Web*

Chapter 1

Introduction

This dissertation follows the research and development of wireless solutions for household appliances, specifically gas water heaters from Bosch Termotecnologia S.A.. This chapter will precipitate a first approach to the challenges facing this dissertation project, the company where it was developed and the market outlooks for the Internet of Things and the gas water heater sectors within this dissertation context.

1.1 About the Dissertation

We're on the brink of an indoor revolution. In a not so distant future, envision all the devices laying around your house, passive and idle, suddenly coming to life, energized by the power of networks and potentiated by adaptive learning capabilities. Not just having hot water and central heating, but also the experience of remotely controlling these devices from your fingertips. This connectivity revolution is called the Internet of Things (IoT) and it's a future already dawning upon us.

The Internet of Things promises to connect structures and equipment, i.e. things, that were previously operating offline, bringing them together in an integrated interface with remote access and control. It offers new ways for previously existing technologies to perform and adapt, suiting an enhanced user experience.

The present work will draw inspiration from the ongoing Internet of Things revolution, synthesizing a concrete application of this technology by developing reliable wireless communications between a gas water heater and remote controller. The main goals for this project demand the designed system to communicate wireless and securely, while keeping low power consumption and being able to accommodate significant communication ranges across different rooms and floors.

This project was developed at Robert Bosch GmbH water heater factory at Aveiro, Portugal integrated in the Electronics Research and Development (R&D) Team lead by Eng. Nuno Silva and supervised by Eng. Catarina Santiago.

This document will cover the efforts undertook on researching and developing wireless solutions for household appliances, specifically the wireless interaction between a Gas Water Heater

(GWH) and a Human-Machine Interface (HMI), remotely located within the same domestic infrastructure. It begins with the Literature Review chapter, revising the current academic literature and industry standards and how this work may draw from what has already been done. Following, it will be discussed the Methodologies and Development employed in this work, assuring rigorous and quality information and how the idealized system became a functional prototype. Finally, the last two chapters will compile the Results Analysis of the developed work and the Conclusions and Future Work will evaluate the achievements and what new goals may lie ahead.

1.2 About the Company

This section incorporates a general descriptions about Robert Bosch GmbH and its subsidiary Bosch Thermotechnik GmbH, of which the Aveiro plant, Bosch Termotecnologia S.A., is part of and serves as corporate headquarters for the Residential Water Heating business unit.

In a top-down approach, the Bosch Group is a leading technology supplier and service provider with over EUR 73 Billion in revenue (2016). It counts with more than 390.000 associates all over the world. The Group is present in different business sectors, such as Mobility Solutions, Industrial Technology, Consumer Goods, and Energy and Building Technology. Recently, the Group defines itself as a leading IoT company, driving innovation and creating top of the line solutions for homes, cities, industries and mobility. The Group's strategic goal is to create solutions that are "Invented for Life". Recently, Bosch has been shifting into an IoT company, investing in sensor technology, software, services and an IoT Cloud. The Bosch Group integrates Robert Bosch GmbH, which counts roughly with 450 subsidiary and regional companies in about 60 countries. [3]

Bosch Thermotechnik GmbH is a subsidiary entirely owned by the Bosch Group. It defines itself as a leading manufacturer in heating and hot water solutions and are committed in providing indoor comfort with energy efficient and environmentally responsible products. Known through brands like Bosch, Buderus, Junkers, Worcester, or in Portugal, Vulcano, the subsidiary manufactures a plethora of products, ranging from boilers and heat pumps to gas and electric water heaters. [4]

Aveiro, Portugal is the location of one of the Bosch Thermotechnik GmbH factories. It was founded in 1977 as Vulcano and to this day, this brand boasts popularity among the Portuguese people. Later adquired by the Bosch Group, Aveiro is nowadays the competence centre for Residential Water Heating worldwide, with a significant investment poured into a new R&D Department.

1.3 Market Overview

This section will contextualize the reader with macroeconomic current and forecast values for two market sectors: the field of study of this dissertation, the Internet of Things; and the field of application of this project, as it was developed in Bosch Termotecnologia S.A., Water Heating solutions, as domestic or commercial gas water heaters.

1.3.1 Internet of Things

The Internet of Things promises to deliver a world with more accessibility and controllability for a plethora of devices that surround us. With applications ranging in industrial, medical, household and urban contexts, it is surprising the power one technology can unleash in transforming the landscape of civilization. The following image illustrates the wide array of application domains [1]:

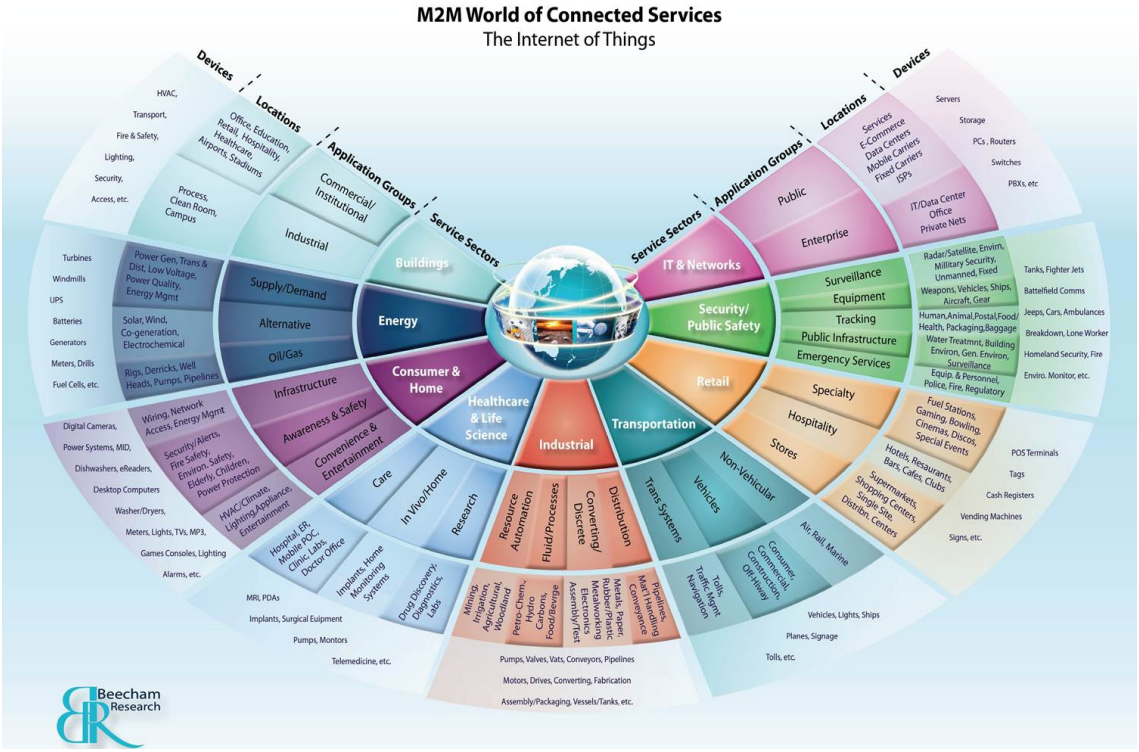


Figure 1.1: IoT Application Domains [1]

The Internet of Things is a trend making a lasting mark in the technology sector. Consumer demand is expected to grow every year, with analysts projecting 20 to 30 billion (short scale) connected devices by the year 2020, adding about 3 billion new devices per year. This market outlook has been confirmed in semiconductor demand, as with companies like AMD and NVIDIA, that have seen a huge revenue growth due to the increasing computational demands from the advent of the Internet of Things, machine learning, blockchain technologies, Industry 4.0 and cloud and fog computing [x]. Improved connectivity and computation are the key words for the near futures, with companies lining up their corporate strategies with this trend. According to Cisco [5], *"Global IP traffic is expected to reach 194.4 exabytes per month by 2020, up from 72.5 exabytes per month in 2015. The global annual run rate will reach 2.3 zettabytes by 2020 - up from 870 exabytes in 2015"*. Furthermore, an Internet of Things development must contain the following characteristics:

- **Distributivity**: Data gathered from different sources and processed by different units.
- **Interoperability**: System infrastructure compatible between institutions.
- **Scalability**: Possibility of working with billions of devices in the same network.
- **Lean**: Capability of operating in scarcity of power and computation resources.
- **Secure**: System and data protection from intrusion.

In 2015, the market size for the Internet of Things was USD$15.41B according to the IHS, and is estimated to reach USD$30.73B in 2020 and USD$75.44B in 2025. McKinsey&Co, in another report [6], claims that *"linking the physical and digital worlds could generate up to $11.1 trillion a year in economic value by 2025"*, this constitutes about 11.6% of World Gross Domestic Product (GDP) forecast by OECD's numbers (USD$ 95.5 trillion forecast) [7]. It is a huge impact in the world economy by one technology with multiple applications, albeit, mostly in industry under the banner of the 4th Industrial Revolution, or Industry 4.0.

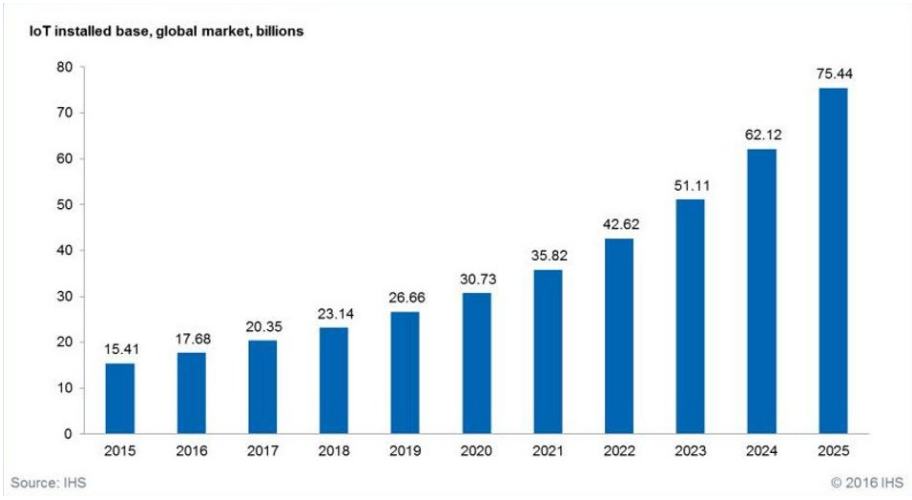


Figure 1.2: IoT Market Growth 2015-2025 in USD$ Billions

1.3.2 Gas and Electrical Heating Solutions

This section will cover the economic frame of Bosch (Aveiro), Portugal and the heating and hot water solutions market. It is having repercussions in every existing platform, even in previously simple and discrete home appliances in electronics matters, as in gas water heaters, with consumers now demanding for wireless accessibility and more sophisticated computing features.

In data from the Observatory for Economic Complexity (OEC), a project by the Massachusetts Institute of Technology (MIT), the home appliances produced at BOSCH Thermotecnologia S.A. are classified according to the Harmonized System (HS):

- **HS841911**: Heaters; instantaneous gas water heaters, for domestic or other purposes
- **HS841919**: Heaters; instantaneous or storage water heaters, non-electric, other than instantaneous gas water heaters
- **HS851610**: Heaters; electric, instantaneous or storage water and immersion heaters

Since this dissertation was developed in Portugal, there is a relevant fact to mention about the previously listed categories. Bosch Termotecnologia S.A. is responsible for producing the majority of instantaneous gas water heaters for the Portuguese market, under the name Vulcano, but also contributes significantly to world trade in this market. The following data visualization was extracted from the OEC website and displays global exports of instantaneous gas water heaters by country in 2015 [2]. Portugal appears not only as the largest instantaneous gas water heater exporter in Europe, but also achieves 3rd place in exports worldwide, following Japan and China respectively.

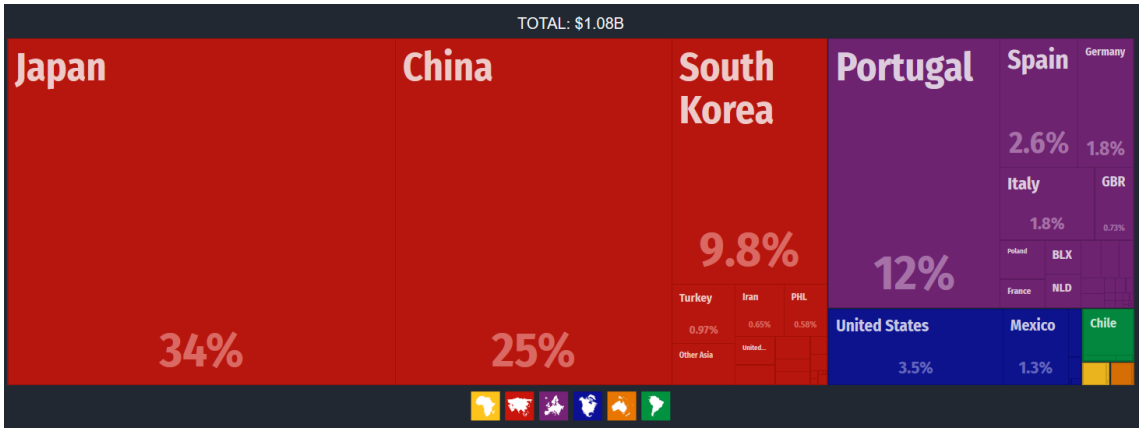


Figure 1.3: Worldwide Exporters - Instantaneous Gas Water Heater Trade (2015) [2]

On a further note, please refer to the Appendix, under Instantaneous Gas Water Heaters Trade, to visualize more related data, such as the worldwide importers trade breakdown and Portuguese export destinations.

Chapter 2

Literature Review

Wireless Radio Frequency Communications have been around for more than a century. Since the invention of the radio , wires became a thing of the past in an increasing number of applications. For many wired systems [8], the advantages of adopting wireless solutions were perceived: the radio, mobile phones, computer networks and cordless electronic peripherals are such examples [9]. Wireless technology promises to solve the physical constraints of having wires, saving resources, increasing portability and delivering reliable communication with an enhanced user experience.

This chapter compiles the recent chronology and comparative analysis of Wireless Communication Protocols (WCP). Furthermore, it is of interest to this project to review the study of Indoor Radio Frequency (RF) Propagation, considering the effects of obstacles and different materials in signal strength and reliable communication. The information and credits presented in this dissertation were researched in online search engines for academic publications (e.g. Google Scholar), institutional websites (e.g. IEEE) and in manufacturers and hardware resellers websites (e.g. Texas Instruments, Farnell, Digikey, Nordic Semiconductors, Silicon Labs and NXP). To note that all the above mentioned organizations did no contribution to this project nor the author, in order to avoid conflicts of interest with pursuing academic and corporate work.

2.1 A Brief Chronology of Wireless Communications

In this section, the literature review will begin by presenting a brief review of the developments in wireless communications. This revision will only encompass recent chronological milestones in wireless communications within consumer households, reviewing mainstream commercial products and technologies.

2.1.1 From Wired to Wireless

Before the XXI century, few economical and efficient wireless communications solutions reached the consumer market. During the XX century, wireless devices or smart household appliances, were too expensive and that kept many consumers at bay. However, market sizes were skyrocketing since earlier in the century. To reinforce this point, the first mobile telephone was priced at

USD$ 9.333,00 (2017 inflation adjusted) when it was released in 1984, while today it is possible to purchase a tremendously more functional device for a few tens or hundreds of USD$. In 1990, with the advent of the World Wide Web, the IEEE 802.11 Working Group came together to start working in defining a standard for Wireless Local Access Networks (WLANs). Later, in 1997, IEEE 802.11 was launched and has been a great contributor to technological democracy and has improved ever since. To exemplify, in 1997, 802.11 delivered a maximum data rate of 2 Mb/s, while with 802.11ac of 2014, communications could reach data rates up to 6,93 Gb/s [10]. Also, internet access began as an expensive and reserved service in its low data rate days in the 1990s, relatively to what it is today, counting more than 3600 Million individuals are connected to the World Wide Web [11].

In the Age of Information, the digital revolution is also accompanied by a wireless one [12]. In the last 20 years, markets have seen a vast number of wireless solutions embedded in consumer goods, alike of telephones, computers, industrial management systems, household, medical and urban appliances. Within Home Automation, where this project takes place, the trend seems towards a profuse use of data and ubiquitous connectivity, from sensors to control and actuators. Both in the case of Heating, Ventilation and Air-Conditioning (HVAC), Light Control, Energy Management or Security Systems, the Internet of Things decidedly affirms itself as the leading movement for innovation in household appliances [13].

2.2 An Overview of Wireless Communication Protocols

Following a brief review of the recent history of wireless communications, it follows a look onto the advent of different wireless communication protocols, that have brought about a standardized approach and, in various use cases, have enabled cordless transmission of information. Be it within a home, an office, a public building or even a city, there are wireless technologies that suit these different applications and allow for enhanced connectivity.

Since this study is focused around household appliances, we will only look at the available frameworks in this context. Within the indoor domestic sphere there are 2 types of radio frequency networks: Wireless Local Access Networks (WLANs) and Wireless Personal Area Networks (WPANs). These two types differ in specifications, as with frequency, modulation, range, security techniques and overall power consumption, hence implying different standards for different applications: 802.11b/g/n/ac for WLANs and 802.15(.1, .3, .4) for WPAN. Although there are several protocols enabled by each standard, some general differences can be listed about WLANs and WPANs, as shown in Table 2.1.

-	**WLAN**	**WPAN**
Standard	IEEE 802.11.x = b, g, a, n, ac	IEEE 802.15.1, 802.15.3, 802.15.4
Definition	A wireless local area network (WLAN) is a wireless computer network that links two or more devices using a wireless distribution method within a limited area such as a home, school, computer laboratory, or office building.	A (WPAN) wireless personal area network is a low range wireless network which covers an area of only a few dozens of meters
Layers	PHY and MAC used with TCP/IP	PHY and MAC + Custom High Level
Frequency Band	2.4 GHz ISM (802.11b/g/n) 5 GHz (802.11a/n/ac)	2.4 GHz ISM (also 868/900 MHz)
Power consumption	Has Low Power mode	Very Low power
Peak current	100-200 mA	<100 mA
Range	30m/300m in/outdoor	20 m indoor
Modulation	OFDM DSSS (802.11b)	DSSS, O-QPSK

Table 2.1: WLAN and WPAN general differences

In a more detailed approach, it will be presented a comparative review of popular protocols, both for WLANs and WPANs in regard to their different characteristics [14] [15] [16] [17] [18] [13] [19]. This thorough comparison was synthesized in table 2.2. Following this table, a summarized review will be assessed textually.

2.2.1 ZigBee

ZigBee is a wireless networking protocol set by ZigBee Alliance in 2003, specialized in low data rates within short to medium ranges. It is divided in several communication layers as can be observed in Figure 2.1. It boasts a physical (PHY) and media access control (MAC) low level layers, as defined by the standard IEEE 802.15.4, followed by a network (NWK) and application (APP) layer at the high level. In frequency ranges, it operates in compliance with regional regulatory bodies, according to public Industrial, Scientific and Medical (ISM) bands, of 2.4 GHz worldwide and for sub 1 GHz, 868 MHz in Europe, 915 MHz in North America and 920 MHz in Japan.

Architecturally, ZigBee defines three roles for devices, which can be visualized in Figure 2.2. A Coordinator sets up a network, a Router specialized in routing messages, and End Devices that pass most time asleep and usually own the incentive of waking up when data transmission is necessary. The ZigBee stack is also equipped with ZigBee Device Objects (ZDOs) for more elegant software design, and application profiles for the areas of Home Automation and Smart Energy Management, which make ZigBee a very interesting solution for Internet of Things applications.

Characteristic	ZigBee	WiFi	6LoWPAN	Z-Wave	Bluetooth	Bluetooth Low Energy
Standard	IEEE 802.15.4	IEEE 802.11a/b/g	IEEE 802.15.4	ITU G.9959	IEEE 802.15.1	IEEE 802.15.1
Classification	WPAN	WLAN	WPAN	WLAN	WPAN	WPAN
Year	2003	1997	2007	2005	1998	2010
Frequency Band	2.4GHz ISM 868MHz ISM	2.4 GHz ISM 5 GHz ISM	2.4GHz ISM 868MHz ISM	2.4GHz ISM 868MHz ISM	2.4GHz ISM	2.4GHz ISM
Throughput	20kbps 250kbps	22Mbps	20kbps 250kbps	9.6kbps 40kbps	768kbps	1Mbps
Nominal Range	MEDIUM	MEDIUM	HIGH	MEDIUM	LOW	LOW
Power	LOW	HIGH	LOW	MEDIUM	MEDIUM	LOW
Latency	<5ms (beaconless @250kbps)	<6ms	<5ms (beaconless @250kbps)	<39ms (@40kbps)	<100ms	<3ms
Modulation	BPSK/O-QPSK	QPSK	BPSK/O-QPSK	BFSK	GFSK	GFSK
Spreading	DSSS	DSSS	DSSS	No	FHSS	FHSS
RX Sensitivity	<-85 dBm @ 2.4GHz <-92 dBm @ 868MHz	<-84 dBm	<-85 dBm @ 2.4GHz <-92 dBm @ 868MHz	<-101 dBm @ 40 kbps	<-70 dBm required <-90 dBm typical	<-70 dBm required <-93 dBm typical
Identifiers	16|64 bit MAC Address 16 bit NWK identifier	16|64 bit MAC Address 128 bit IPv6 Address	16|64 bit MACAddress 128 bit IPv6 Address	32 bit home ID 8 bit node ID	48 bit public device address	48 bit public device address
Device Types	Coordinator, Router and End Device	Host, Router	Mesh node, Edge, Router, Host, Router	Controllers and Slaves	Single Type	Single Type
Network	Mesh, Star	Star	RPL	Star	Scatternet	Star
Encryption	128 bit AES	WPA	128 bit AES	128 bit AES	BR/EDR	BR/EDR
Complexity	HIGH	HIGH	MEDIUM	MEDIUM	MEDIUM	MEDIUM
Implementation	45-128kB (ROM)	24kB (ROM)	24kB (ROM)	32-64kB (Flash)	∼40kB (ROM)	∼100kB (ROM) ∼30kB (RAM)
Size	2.7-12kb (RAM)	3.6kB(RAM)	3.6kB(RAM)	2-16kB (SRAM)	∼2.5kB (RAM)	
Publicly Available	YES	YES	YES	NO	YES	YES

Table 2.2: Wireless Protocol Comparison

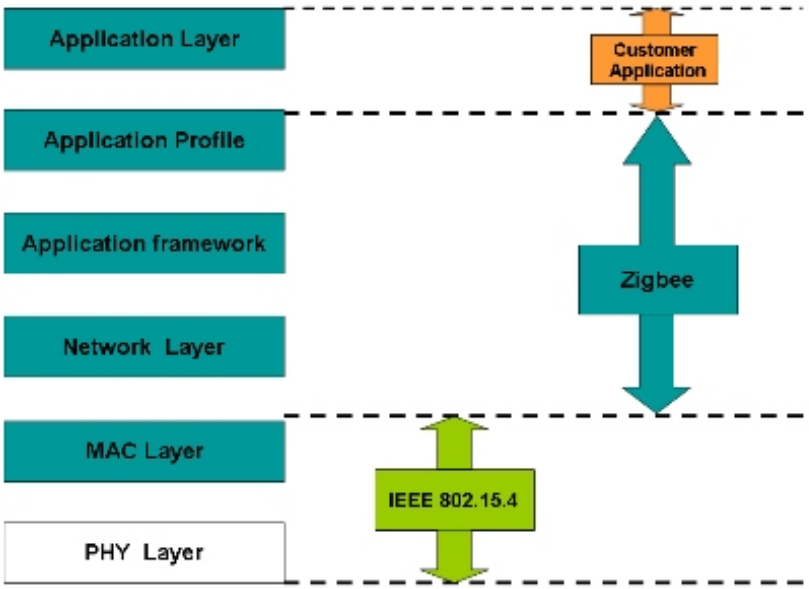


Figure 2.1: ZigBee Stack Layers

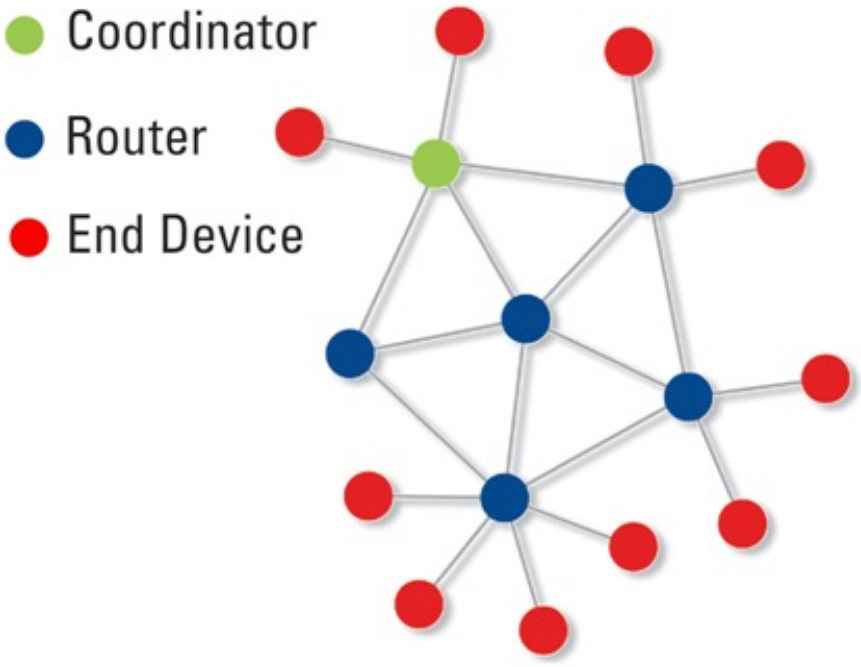


Figure 2.2: ZigBee Device Types

2.2.2 Wi-Fi

Wi-Fi is a wireless protocol developed by the Wi-Fi Alliance in 1999, based on the IEEE 802.11 standard of 1997 and that operates at 2.4 GHz and recently with the option of 5 GHz . The Texas based organization owns the trademark for Wi-Fi and is responsible for certifying devices that claim using Wi-Fi. Wi-Fi Alliance requires that a device must comply with at least one of the following: 802.11a, 802.11b, 802.11g or 802.11n. It features Wireless Protected Access 2 (WPA2) in compliance with IEEE 802.11i as security, based on a 128-bit Advanced Encryption Standard. As mentioned, the latest Wi-FI standard, released in 2013, allows for almost 7 Gb/s and counts presence in more than 25% households worldwide [10].

2.2.3 6LoWPAN

6LoWPAN is a hybrid wireless protocol bringing together a low level PHY and MAC layers from IEEE 802.15.4 and Internet Protocol version 6 (IPv6), packet processing and routing on top of that. However, the joint venture of the two protocols leaves some problems in regard to a large difference in packet size, solved with fragmentation (127 byte frame in IEEE 802.15.4 and 1280 byte packet in IPv6); and difference in frame header size, solved with header compression (2 byte header in IEEE 802.15.4 and 40 byte header in IPv6). A 6LoWPAN configuration can operate in mesh under and route over setups. Mesh under, as the name suggests, makes use of the low level PHY and MAC layers, according to IEEE 802.15.4 addresses. Route over, does the opposite, it relies on the high level IPv6 protocols to route packets between points [17].

2.2.4 Z-Wave

Z-Wave is a proprietary wireless protocol developed by ZenSys, currently a division of Sigma Designs. It has the Z-Wave Alliance, a body for promoting Z-Wave in automating domestic and commercial infrastructure. Z-Wave follows an architecture composed by the classical PHY and MAC layers, followed by transfer, routing and application layers. It operates in sub 1 GHz ISM bands, such as 868 MHz in Europe and 900 MHz in North America. For mostly home automation applications, Z-Wave employs a source routed mesh network topology, which provides the possibility of obstacle circumvention in an indoor environment [13].

2.2.5 Bluetooth

Bluetooth is a piconet technology protocol for short range applications, developed and maintained by the Bluetooth Special Interests Group. It is classified as a Wireless Personal Area Network (WPAN) protocol. It follows the standardization by IEEE 802.15.1 and operates in the worldwide unlicensed ISM bands around 2.4 GHz. Recently, it has also been released as Bluetooth Low Energy, featuring a much lower current consumption and a slightly increased range, however it reduces application throughput.

2.3 Wireless Hardware Design

The Internet of Things has brought a big surge in semiconductors demand and, through innovation, higher supply for low cost, low power and reliable wireless solutions. Many companies have developed wireless modules to ensure an easy development and a simple integration processes with other consumer goods. As the main focus point of this work is the research and development of solutions for domestic gas water heaters with connect, it goes without saying, that this literature review wouldn't be complete without a proper hardware review, covering the more academic part, while the technical details will be further covered in the next chapter.

In WPANs, the vogue is comprised of ZigBee and Bluetooth Low Energy (BLE) protocols, sharing the IEEE 802.15 standard in the physical (PHY) and media access control (MAC) layers. However, ZigBee is standardized by 802.15.4 while BLE follows 802.15.1 directives. While BLE modules have lower energy consumption, ZigBee devices have longer range and can even operate at lower frequencies: 868 MHz in Europe; which allows for a range boost from what was discussed in the previous section. In terms of cost, ZigBee modules are in average more expensive than BLE ones, however the least costly modules were the ones with ZigBee. There is also a new range of protocols, comprising what is called the sub 1 GHz frequency range, typically operating in 868 MHz in Europe and 915 MHz in the United States of America, or even at lower frequencies, around 433 MHz.

When discussing system design for indoor wireless communications it is important to observe certain aspects. Signal range can be defined as a function of receiver sensitivity, output transmitter power, antenna performance, frequency and also co-existence and environment. Firstly, for any communication to occur, there must exist a positive link budget between the points. Link budget is the overall sum of every contribution to signal power, and for communications to exist, it must be positive, meaning that power reaches the receiving end. This can be observed in Equation 2.1.

$$L_B = T_x - R_x - (A + F_{PL} + O_{PL}) \tag{2.1}$$

Where L_B is link budget (dB), T_x is transmission power (dB), R_x is receiver sensitivity (dB), A is antenna losses (dB), F_{PL} is free space path loss(dB) and O_{PL} is obstacle path loss (dB).

2.3.1 Output Transmitter (TX) Power

This parameter comes in first place for it is where the signal originates. The transmitter can output at different levels of power, given the higher output power, the higher signal range but also a greater current consumption.

2.3.2 Receiver (RX) Sensitivity

Another key specification in wireless modules is RX Sensitivity. It speaks of the ability of the receiving device to pick up a weak signal and get information out of it. The design approach is more complex as this parameter depends largely on a number of variables: bandwidth, temperature

and carrier to noise ratio, which in turn defines the application maximum communication bit rate. This relationship can be observed in Equation 2.1.

$$S_{RX} = 10.log_{10}(kTB) + F + \frac{C}{N} \tag{2.2}$$

Where S_{RX} is Receiver Sensitivity in dBm, kTB is thermal noise power, composed by k, which is the Stefan-Boltzmann constant ($5.670373 \cdot 10^{-8} \cdot Wm^{-2}K^{-4}$), T representing temperature in kelvin (K) and B for bandwidth in (Hz). F is noise floor in dBm and C/N is carrier to noise ratio in dB.

2.3.3 Antenna Performance

Antenna Performance or Antenna Gain evaluates the broadcast of the signal. It is proportional to the product of Antenna Efficiency and Directivity. It is significant factor in any wireless project. This project will only deal with antennas that are embedded on the Printed Circuit Board (PCB).

2.3.4 Frequency

The frequency chosen for the wireless application will condition many other variables. Firstly, as will be discussed in RF Propagation, Path Loss is proportional to the inverse of both frequency and distance squared, therefore lower frequencies will be more suitable for large distances and have better obstacle penetration and turning corners. Moreover, frequency is also proportional to bit rate, as is bandwidth - another frequency parameter. Higher frequencies and bandwidth will be able to generate higher bit rates, and consequentially higher data transmission.

2.3.5 Co-Existence

Co-existence is an important parameter in wireless communication systems design. It refers to the concentration or rarefaction of wireless communications at a given frequency range. Certain frequency ranges, like 2.4GHz are crowded with communications, since most consumer goods operate at this level. Choosing a more reserved frequency range within the Industrial, Scientific and Medical (ISM) bands, can improve system performance as interference and wave collision is less likely to occur.

2.3.6 Environment

When we refer to environment, we are listing the effects of all other surrounding conditions. Background noise or obstacles are such examples that will affect the performance of a wireless solution. In the next section, the studies on the effects of indoor obstacles will be reviewed in more detail.

Finally, to note, many constraining requirements need to be optimized for its given application, e.g. low current consumption or high bit rate and long communications range. To have the

best of both worlds it is necessary to firstly define the system requirements before starting the compromising task of designing the system.

2.4 A Review of Indoor RF Propagation

In this section will be presented the studies done in Indoor Radio Frequency Propagation and its importance to the project. It is of paramount importance in designing a wireless solution since signal propagation is significantly affected by obstacles such as walls, furniture or people. Firstly, I should start by a review of Path Loss theory in studying wireless communication. The fundamental background to any further study is a description of the key attenuation stages of RF Propagation: Transmitter, Path and Receiver. Starting with the transceivers in both ends, attenuation is due to cable loss of about 4dB in total, being the propagation path in between points the largest attenuation stage. To calculate the attenuation caused by the path, traditional communications theory formulates Equation 2.3, assuming a clear line of sight (LOS):

$$PL_{FS}(dB) = \frac{(4\pi df)^2}{c} \tag{2.3}$$

d = distance (m) f = frequency(Hz) c = light speed (m/s)

The not so trivial part of estimating Path Loss is in not ideal conditions. Within an office or house there can be a multitude of obstacles between the transmitter and receiver, leading to path loss affection and even to interruptions in communication. Therefore it is crucial to a good development of this project to study the effect of objects and barriers, by researching the academic literature on this matter.

Starting with the effect of walls, Kedar Sahu *et al.* wrote a paper [20] showing that the internal profile of a wall can produce different affections to radio signals. If the wall has air gaps then it has less attenuation than in the case of a solid wall. This was demonstrated by using K Rician Factor comparison. Furthermore, effective walls were also studied and have a K Rician Factor 7dB higher than in the case of slab and complex walls, which implies it causes even less attenuation in propagation.

Another study[21], develops a model called Multi-Wall-and Floor, derived from ray tracing simulations that evaluates penetration loss across multiple walls and floors. Moreover, it takes into consideration the different materials present in the structures, like concrete, brick, stone, wood or glass and the obstacle thickness. Another approach was developed just for 2.4GHz signals, i.e. WiFi., describing the fundamental mathematical formulation for path loss prediction based on empirical modelling [22].

There are also some other studies on this matter [23][24][25][26][27][28][29]. The common theme are frequency and obstacle contributions to path loss, ranging from 868 to 5200 MHz, synthesizing similar models regarding obstacle affection to path loss. Regarding all the mentioned approaches to path loss modeling, it serves to mention that all the attempts to mathematically formulate are broad and empirical. This implies that when trying to design a wireless communication

system that is going to be present as a consumer product in a vast range of domestic layouts, it is advisable to take the worst case scenario of the location cases. In a further section of this work, these models will be put together in designing the system besting the specifications.

2.5 Security in Wireless Communications

Security is a critical aspect of any communication link, even more when it comes to wireless ones. To design a secure system, it is imperative to firstly understand the risks. The consequences or impacts of a communication security breach can vary, from simple wiretapping that shares information with unintended receivers or communication hacking, perturbing the system with outside commands, presenting therefore serious human and material risks. This being said, it has become clear that security plays a role of paramount importance in wireless communications, conferring civil responsibility to the system designers, in ensuring human and material preservation.

In Security Techniques, all the mentioned protocols have data encryption in communicating. Discussing this mean, encryption changes data to be transmitted or stored in direct relation to a set of bits, called key. This key holds the property of exclusive and unilaterally decrypting the data, i.e., reverting it to the original, understandable form. Encryption methods have been around for thousands of years, with many interesting stories with secret messages from the Ancient Classical period . Recently, advances in mathematics have enabled the creation of much more secure and robust encryption methods, which are the technological basis for wireless communication, electronic banking, blockchain as in Bitcoin and account security, just to name a few examples.

Modern encryption standards divide in two categories: symmetric and asymmetric cryptography. Symmetric cryptography makes use of one key, shared by the members of the networks. Information is codified using that key, only to be sent and received and finally decoded by the receiver using the same key. Asymmetric cryptography makes use of both a public and a private key per member of the network. The sender requests and obtains the receiver's public key, using it to encrypt the message. After transmission of the encrypted message, the receiver uses its private key to decode the message and access its plaintext content.

2.5.1 Advanced Encryption Standard

Advanced Encryption Standard (AES) is a symmetric cryptographic standard used to secure data in storage or communications. It is the default security method of many of the studied wireless protocols, like ZigBee. It offers various key lengths (128, 196 and 256 bit) and while the larger two are appropriate for Top Secret level information, 128 bit is only sufficient for Secret classification for the U.S. Government, which attests to the robustness of this standard [30].

2.5.2 Secure Hash Algorithm

Secure Hash Algorithms (SHA) are a set of cryptographic hash functions created by the National Institute of Standards and Technology (NIST). It subdivides historically into SHA-0, SHA-1,

SHA-2 and SHA-3, being the incremented number a new release of this standard. The National Security Agency (NSA) created SHA-2[30], a widely used standard, encrypting information with 256-bit or 512-bit keys. It is absent from wireless protocol usage but can be found in Secure Sockets Layer (SSL). SSL encrypts emails, web browsing, voice-over-IP and a vast array of server-client communications. It is also used in the trending cryptocurrency Bitcoin, providing security to blockchain technology and in U.S. Government classified information.

Chapter 3

Methodologies

This chapter will clarify the methodologies employed in developing this project. It will cover what project management and system design methodologies were considered and employed for all the following work. Hence, it will list the system requirements, create a system architecture, document the design choices and cover the implementation

3.1 Project Management

A project is an individual or team enterprise or set of efforts, planned and executed in order to achieve a particular set of goals. At a micro level, a project is composed of tasks and in turn these tasks can be composed of sub-tasks recursively, as long as there is a quantifiable deliverable. In the macro scope, a project may integrate a group of projects, contributing directly to department goals and consequently, departments come together to fulfil the goals of an organization, such as a corporation or government. Indeed, the fractal nature in the concept of project is evident, as all organizational social structures demonstrate this same idea in different magnitudes.

If projects are such a foundational and relevant component of social life, it becomes clear the importance of project management, i.e., the methods for optimized allocation of time, work capacity and resources in delivering goals. Not to stride away too much from this dissertation objectives, but it serves well to mention the observed evolution in project management methodologies, which are very closely linked with organizational development.

Planning is a fundamental aspect when partaking in a complex work. In Project Management, goals together with time are of the essence, hence methodologies need to be selected and implemented to manage these two variables. In the vast list of development methodologies applicable to the present situation, the Waterfall mode was selected, mainly to comply with work dynamics at the company. This model prescribes a linear sequence of tasks: 1) Requirements; 2) Architecture; 3) Design; 4) Implementing; and 5) Testing. However, in adapting this model to the writing of a dissertation, it was decided to add a step 0) Research and a step 6) Documenting.

The work breakdown required for this project will come from requirements declared for this development, followed by architecture and design and finally developing and testing. As time

constraints reinforce the importance of planning, a Gantt chart was developed for time mapping the different tasks in this project. This document can be found in Appendix A.

This project has two main objectives: one, to develop a wireless communication system integrating Bosch water heating appliances; and second, to write this document, compiling all the research and development efforts. This system will be composed of carefully selected wireless modules for indoor domestic communication between a water heater, capable of outputting hot water and central heating temperatures set by a user from a remote HMI. This HMI should also be able to wirelessly control the temperature of an EWS, taking into account the user inputs for the water heater. Figure 3.1 was designed, in order to visually express the concept of this system.

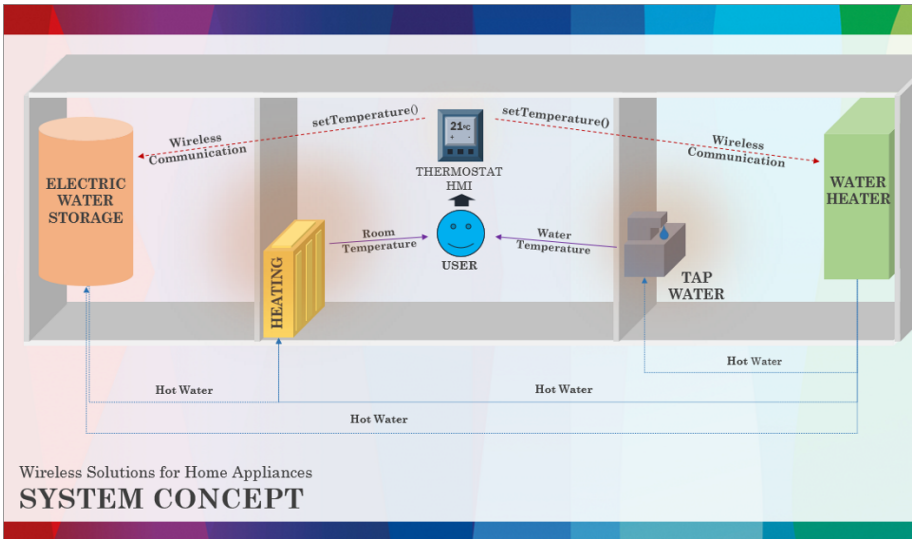


Figure 3.1: System Concept

3.2 System Requirements

The first step in designing a wireless solution is to understand the scope of the problems that this project presents. To understand this scope of constraints, it is customary to draft requirements that define a project's objectives and quality features through functional and non-functional requirements. In functional (Table 3.1) requirements, it is understood to contain the key functionalities that the system should present, on the other hand, on the non-functional side, it was classified in quality (Table 3.2) and legal (Table 3.3) requirements for this project. The following tables list the respective requirements sorted by category, duly tagged with qualitative priority and complexity. Priority defines the importance of that requirement's presence in the final system, while complexity evaluates the relative difficulty of an implementation. On another note, from now on, the EWS concept will merge with the GWH since the resources present at the company already allow the scaling of a wireless solution between a HMI and GWH to a *trio* combination of HMIs, GWHs and EWSs.

Req. ID	Description	Priority	Complexity
FR.01	The system provides wireless communications of instructions between HMI and Water Heater	VERY HIGH	HIGH
FR.02	The system allows user control of Water/Room Temperature	HIGH	VERY HIGH

Table 3.1: Functional Requirements

Req. ID	Description	Priority	Complexity
QR.01	The system shall rely on Low Power Wireless Modules, defined by a TX current of less than 25mA at 0 dBm TX Power.	HIGH	MEDIUM
QR.02	The system shall hold at least 10dB Link Budget at 40 meters without walls between points.	MEDIUM	HIGH
QR.03	The system shall have the lowest cost, without compromising QR.01 and QR.02 quality factors.	HIGH	LOW
QR.04	The system shall be able to have a wireless throughputof at least 100 kbit/s at QR.02 conditions.	LOW	HIGH
QR.05	The system shall have a packet error rate of less than 10% at QR.02 conditions.	VERY HIGH	HIGH
QR.06	The system shall be able to transmit user commands in less than 5 seconds from input.	LOW	MEDIUM
QR.07	The system shall be secured with AES 128-bit encryption or equivalent	MEDIUM	HIGH

Table 3.2: Quality Requirements

Req. ID	Description	Priority	Complexity
LR001	The system must not transmit at frequencies outside ISM bands	VERY HIGH	VERY LOW
LR002	The system must not transmit at powers above 25 dBm	VERY HIGH	LOW

Table 3.3: Legal Requirements

3.3 System Architecture

Architecture is a conceptualization of a system, usually performed aprioristically relative to the development. It prescribes visual and technical guidelines for system design and provides a broad view to the reader of what macrostructures the project has, for its implementation. In terms of applicability in this project, an architecture can be drafted for the software development stage of a wireless solution, given that it is hardware selection, not design and implementation that is required of this project.

Conceptually, the envisioned system consists of a gas water heater (GWH) operated by an internal Electronic Control Unit (ECU) and connected to a Human Machine Interface (HMI) for user input and visualization. There are also at least one Remote HMI, with the function of remotely controlling parameters in water heating units. Also, it is important to mention that all devices do wired communications through a proprietary UART-based protocol. Therefore, it is perceived that command and parameter parsing is the keystone of developing a wireless solution. Therefore, it is inferred that the wireless solution will act primarily as data bridge, routing the UART payload. However, this implementation rises issues concerning scalability and functionalities, since the wireless module will only be routing payloads point-to-point. The wireless module, called "self" in this architecture, is the central structure in connecting two physical layers, the wireless and the wired, hence boast receiving and transmitting functions on both wireless and wired ends as well as internal functions, of optimizing connections and having capacity for scaling data processing if required. This way, the system architecture is dynamic and flexible, contemplating all kinds of device environments as well as future demands on computation features. Figure 3.2 conceptualizes the previously described system architecture.

In system architecture design, if applicable it is also customary to draft a use case diagram as

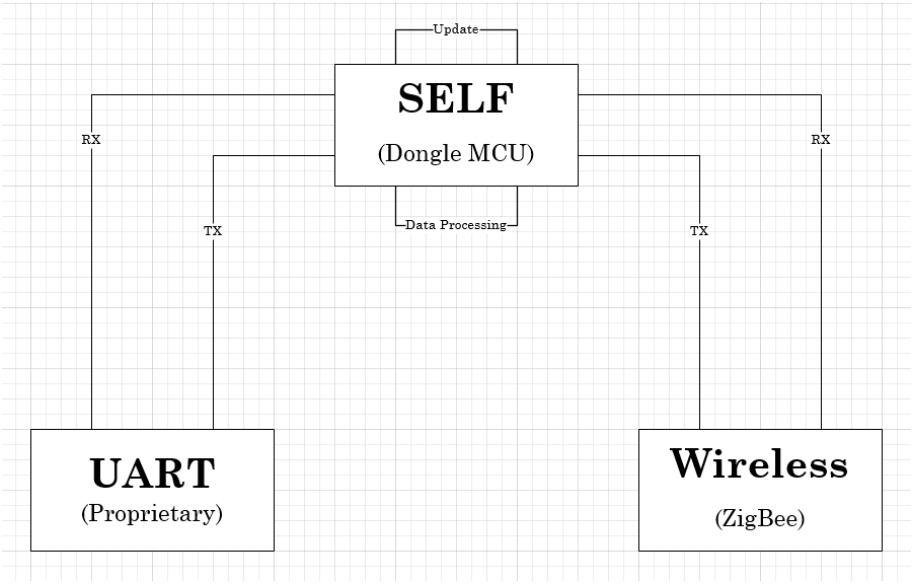


Figure 3.2: System Architecture

presented by Unified Modelling Language (UML), with the purpose of describing the cases of use present in the system, *id est*, the different output behaviors the system can have under user input. Figure 3.3 represents a UML use case diagram, including remote control of tap water temperature, room temperature (through recirculation) and water heater unit's internal variables like mode or errors.

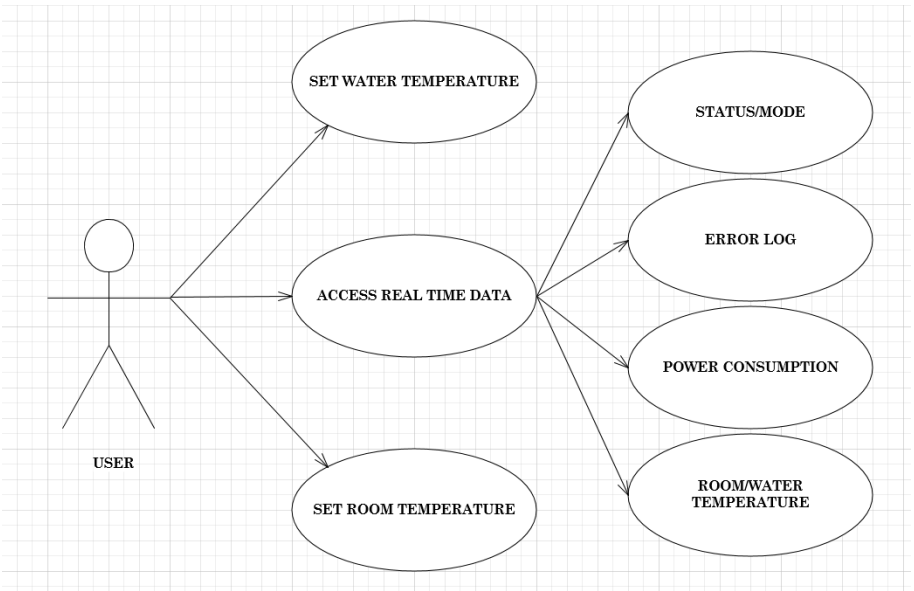


Figure 3.3: Use Case Diagram

When thinking about software implementation, UML also offers sequence diagrams, that describe the logical processing of instruction in several locations. These diagrams can be found in the Appendixes.

3.4 System Design

In this section will be approached the first stage of this development, i.e., the process of researching, evaluating, benchmarking and selecting an appropriate wireless hardware solution according to project functional, quality and legal requirements.

3.4.1 Project Constraints and Analytical Solutions

A list was composed to analytically quantify and model what parameters should be present in the system. The considered parameters in this design are battery life, range coverage and cost. However, within these three variables there are many interrelated factors, as was discussed in chapter 2, but to briefly refresh what was said: battery life i.e. charge duration, is a function of average current (mA); which in turn is composed of TX current, RX current, normal processing current, idle current and sleep current, as present in most datasheets. To simplify and provide an accurate estimate, TX current was used as the key indicator in power consumption metric, as it presents a worst case scenario view on current consumption. It is also a requirement to maximize range, within legal limits and not increasing power consumption through TX current in excess. To maximize range, assuming the same RF path and frequency, according to literature, range is a function of the link budget expressed as the difference between TX power and RX sensitivity. Therefore, to maximize range, the hardware being considered must feature the greatest difference in these two parameters. Finally, cost is required to be minimized, not just because this work is being developed within a corporation, but also because engineering is about optimizing resource allocation. Following on that note, the list counts both with modules and microcontroller units (MCUs), which have an expected price range gap, since MCUs are one of the components in modules. To balance the cost analysis, the internal costs for the printed circuit board (PCB) plus components (but without the MCU) were questioned within the company. Due to the Non-Disclosure Agreement, the author is not allowed to publish the internal cost for this hardware, however it is ensured that a mock-up but reasonable value was accounted for in the models.

3.4.1.1 Hardware Optimization Benchmark for Selection

Following on the parameters of interest to this project (power consumption, range and cost) and to quantitatively look solutions, a spreadsheet model was developed with Microsoft Excel. This model will serve as a benchmark to compare solutions in relation to the parameters and how these weight in the final benchmark result. By inputting to a table the current consumption during transmission and sleep mode, transmission output power, receiver sensitivity and unit cost adjusted to internal costs, together with some equations, a benchmark result was obtained for each model. This result compiled in Table 3.4, tells the normalized (between 0 and 1) score of that module, with tunable weights for these parameters. A fully detailed benchmark table can be found in the Appendixes.

FREQUENCY/PROTOCOL	WIRELESS_MODULE	TYPE	BENCHMARK_SCORE
2.4_GHz_ZigBEE	Texas_Instruments_CC2531_ZigBee	MCU	**0.20**
2.4_GHz_ZigBEE	NXP_JN5169-001_M05_ZigBee	MCU	**0.37**
2.4_GHz_Bluetooth	Texas_Instruments_CC2640_BLE	MCU	**0.37**
sub_1_GHz	Texas_Instruments_CC1310	MCU	**0.89**
sub_1_GHz	On_Semiconductor_AX5043	MCU	**1.00**
sub_1_GHz	NXP_KWOx_M3_ZigBee_868MHz	MCU	**0.83**
sub_1_GHz	ST_S2-LP	MCU	**1.00**
2.4_GHz_ZigBEE	XBEE_Series_1_ZigBee	Module	**0.11**
2.4_GHz_ZigBEE	Telegesis_ETRX357_ZigBee	Module	**0.34**
2.4_GHz_Bluetooth	Panasonic_PAN1740_BLE	Module	**0.34**
2.4_GHz_Bluetooth	Skylab_SKB360_BLE	Module	**0.77**
2.4_GHz_Bluetooth	Silicon Labs_BLE113_BLE	Module	**0.20**
2.4_GHz_Bluetooth	Fanstel_BT832X_BLE	Module	**0.46**
sub_1_GHz	Embit_ZRF212B_ZigBee_868MHz	Module	**0.86**
sub_1_GHz	Atmel_ZigBit_ATZB-RF-212B	Module	**0.49**
sub_1_GHz	MRF89XAM8A-I/RM_boost	Module	**0.69**
sub_1_GHz	ANSolutions_ANY900	Module	**0.37**

Table 3.4: Hardware Selection Benchmark

The following table (Table 3.5) reflects the weights, selected in accordance to perceived importance:

TX Current	Link Budget	Cost
1.00	2.00	2.50

Table 3.5: Benchmark Weights

Furthermore, still on the analytical side, out of curiosity, the same model calculated hardware correlations between parameters, presented in the following table (Table 3.6):

Type	Parameters	Correlation
MCU	Cost to Link Budget	-0.44
MCU	Link Budget to TX Current	-0.22
MCU	TX Current to Cost	0.44
Mods	Cost to Link Budget	-0.28
Mods	Link Budget to TX Current	0.84
Mods	TX Current to Cost	0.14
Cross	MCU to Mods	0.10

Table 3.6: Hardware Specifications Correlation

It is disclaimed scientific relevance or significance in this correlations, since the sample size is negligible and the author does not intend to elaborate causality arguments between observed parameters in hardware. However, the author would like to observe an interesting relationship in selecting optimized hardware. As mentioned before, link budget needs to be maximized while cost and TX current needs to be minimized. Through plain intuition, these constraints appear to

be mutually exclusive, however, when seeking trends in this data, non-intuitive relationships are observed. Within this data, it is expected to observe a linear relation between Link Budget and cost, since this implies farther distances of communication, however probably due to short range protocol certification, as Bluetooth, being a costly endeavor, the cost for short range solutions may be slightly higher in relation to others protocol entities, or even very much the same, however since Bluetooth holds the lowest TX power and RX sensitivity requirements it traduces into a slightly negative correlation in this sample size.

For optimized visualization purposes, the plots of the key hardware parameters are presented in the following figures 3.4, 3.5 and 3.6.

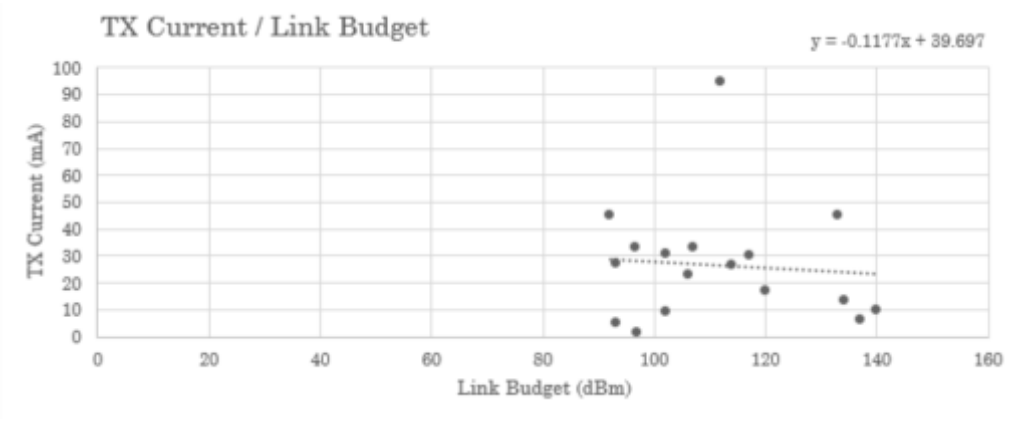


Figure 3.4: TX Current to Link Budget

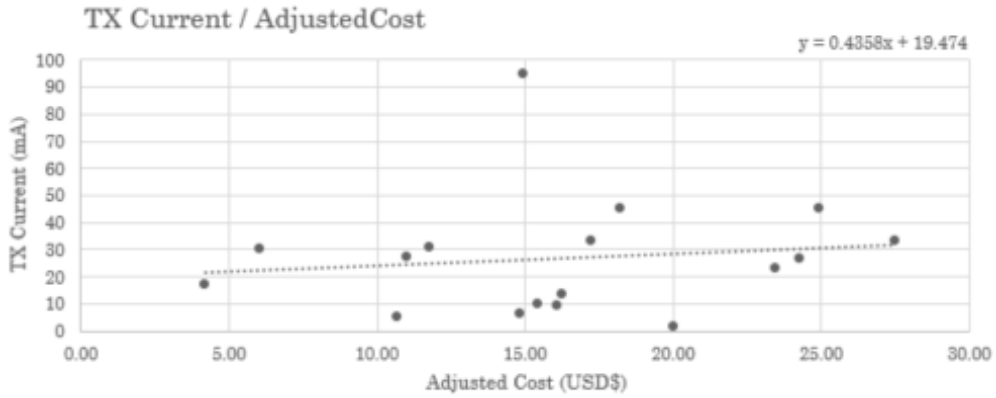


Figure 3.5: TX Current to Adjusted Cost

3.4.1.2 Radio Frequency Transmission Models

Another spreadsheet model was developed to look for answers regarding System Design. Following from the research review on Indoor RF Propagation, a comparative model using several cited approaches for Path Loss was composed. It averages out 3 models present in the academic literature for dealing with frequency, TX power, RX sensitivity, distance and number of walls and

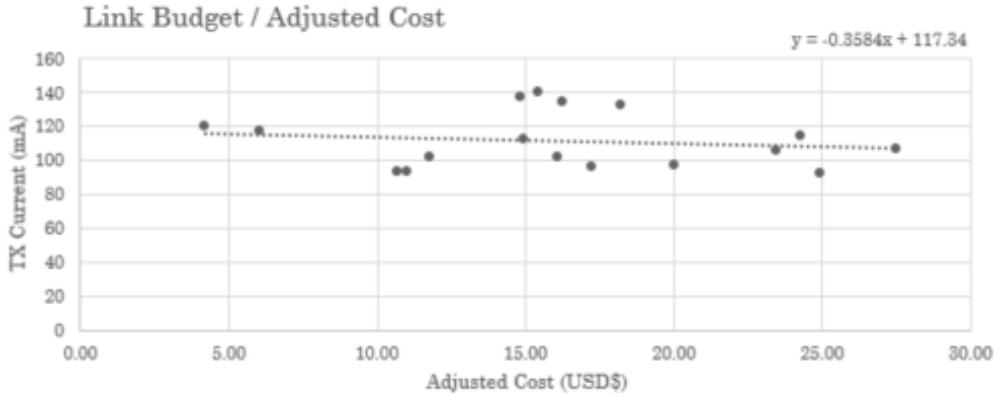


Figure 3.6: Link Budget to Adjusted Cost

floors between transmitter and receiver. The inputs with the greatest variability and nonlinearities are the number of walls and floors, since according to literature, the RF path loss or penetration capability depends on the material, thickness, presence of air gaps, angle of incidence, presence of shielding elements, among other minor causes. Therefore, a fixed over averaged value was used to estimate a propagation range.

Inputting frequency, distance, TX power, RX sensitivity, number of walls and number of floors crossed by the communication and the model returns the remaining link budget, i.e., if positive with some safety margin, e.g., at least 10 or 20 dB, the designer shall be confident that the system will communicate reliably in such conditions. In figure 3.7, a plot shows the budget margin of the link, assuming losses only in the free space between communicating points, and frequency. As can be observed in Figure 3. the margin decays with an increase in frequency, e.g., it decays four times from around 868 MHz to 2400 MHz.

3.4.2 Security Analysis

Security is an essential feature of any wireless communications system, since it protects data, users and system integrity. It was researched what types of attack a wireless solution as this one can be a target of. The potential threats were compiled all this information into a table in the Appendixes. This table also offers a brief description of the attack strategy, qualitative measure for impact of attack and risk, i.e., probability of attack and the ways it is intended to shield this system against each type of attack.

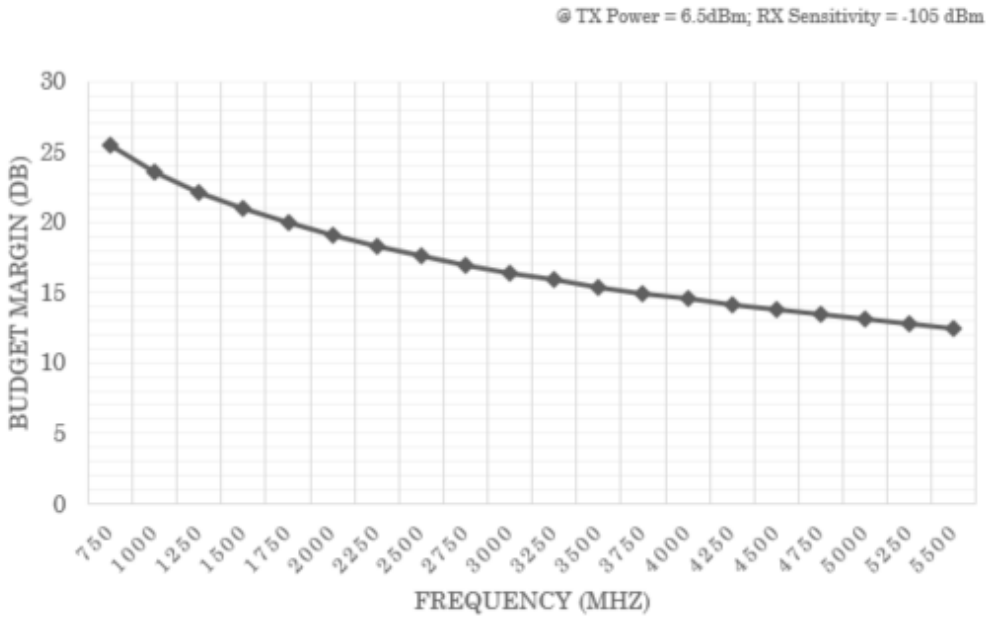
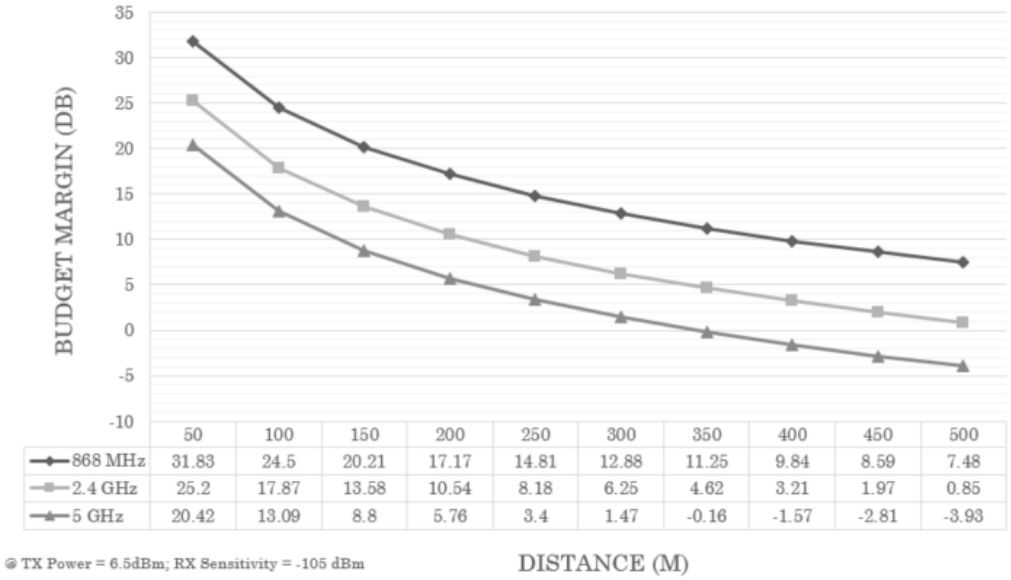


Figure 3.7: Link Margin to Frequency (at 100 meters)



	50	100	150	200	250	300	350	400	450	500
868 MHz	31.83	24.5	20.21	17.17	14.81	12.88	11.25	9.84	8.59	7.48
2.4 GHz	25.2	17.87	13.58	10.54	8.18	6.25	4.62	3.21	1.97	0.85
5 GHz	20.42	13.09	8.8	5.76	3.4	1.47	-0.16	-1.57	-2.81	-3.93

Figure 3.8: Link Budget to Distance

Chapter 4

Results

This chapter will document the outcomes from the development stage in this project. It will cover three main deliverables proposed for this project, alternative hardware selection through a benchmark, the software implementation in the base solution and proof of work and a wireless range benchmark in an indoor environment. In this chapter will also be compared the base solution using Texas Instruments CC2531 running on a proprietary printed circuit board (PCB) and the selected solution in the previous chapter, Texas Instruments CC1310 Launchpad, which is an evaluation module.

Following what was reported on the previous chapter, there were five stages of results in this project. Firstly, to research, evaluate, benchmark and select an appropriate wireless hardware solution for performance comparison with an existing solution at the company: Texas Instruments CC2531 microcontroller. Secondly, to develop software for wireless communications using ZigBee protocol under Z-Stack, demonstrating proof of concept and features. Thirdly, to perform wireless range tests on the existing solution with the purpose of meeting project requirements. Finally, following the procurement of a new solution in the first step, to set up a wireless range test in the same conditions as with the existing solution.

4.1 Hardware Benchmark Results

The selected solution was the Texas Instruments CC1310 with a score of 0.89, it achieves third place on this list of 16 (Table 3.4). Although not presenting the best benchmark result, Texas Instruments offers more tools and resources than the other companies regarding this range of products, together with a larger online community, it increases support in debugging and testing. Texas Instruments CC1310 also gets extra credit for its compatibility with already existing tools at the company, and therefore, the chosen hardware solution for this endeavor.

4.2 System Development

The development of this work begins with the due diligence being made in regard to hardware, software, protocol selection and other requirements. From here on, this section will cover the more experimental and practical side of the project with the development of a base solution: the ZigBee-based Dongle with CC2531; and a sub 1 GHz wireless solution selected sample that in theoretical modelling revealed an enhanced performance in the key parameters. The objective of this part is to setup and evaluate performance between the two systems to later be discussed in this document.

4.2.1 Base Solution: ZigBee Dongle

Considering both strengths and weaknesses of the several connectivity protocols, ZigBee was selected in implementing this system. This choice was due to compatibility with quality hardware in the intended metrics (power consumption, range and cost), a good security standard covering wireless data and risk isolation from World Wide Web cyberattacks, in opposition to Wi-Fi (IEEE 802.11). ZigBee is a communications protocol built upon the IEEE 802.15.4 standard, covering Wireless Personal Area Networks (WPANs). It shares the lower level base of the usual PHY and MAC layer and allows for low cost and low power solutions for connectivity. Within this protocol, devices can be classified in 3 categories: Coordinator, Router and End Device. ZigBee also has the aptitude for operating in mesh network topology, defining a coordinator for network setup and having routers that process and/or redirect (route) messages across the network. Finally, there are end devices, specialized in sleeping for most of the time, and only periodically or by internal event, waking up and sharing some data with the network. This configuration is ideal for sensors in the operational area. This ZigBee device architecture can be exemplified through the following figure: For the ZigBee Dongle, the microcontroller that integrated that project was the Texas Instruments CC2531. Following the 8051 architecture, it can be programmed using IAR Embedded Workbench as the IDE and Z-Stack as the code foundation. Z-Stack is a communications architecture that allows developing mesh networks according to the ZigBee protocol. It presents a physical (PHY) layer, media access control (MAC), network (NWK) and application (APS) layers as other communications protocols, although with different implementations. It also boasts an operating system (OSAL) for vertical stack control. For the ZigBee Dongle, the microcontroller that integrated that project was the Texas Instruments CC2531. Following the 8051 architecture, it can be programmed using IAR Embedded Workbench as the IDE and Z-Stack as the code foundation. Z-Stack is a communications architecture that allows developing mesh networks according to the ZigBee protocol. It presents a physical (PHY) layer, media access control (MAC), network (NWK) and application (APS) layers as other communications protocols, although with different implementations. It also boasts an operating system (OSAL) for vertical stack control.

4.2.1.1 CC2531

Texas Instruments CC2531 [31] is a wireless microcontroller unit (MCU) designed for embedded, ZigBee enabled, RF transceiver applications operating in the 2.4 GHz ISM band. It boasts a low power, 8051 architecture central processing unit (CPU), a AES security coprocessor, a TX Power of 1dBm @ 29mA with idle CPU and a RX sensitivity of -92 dBm. As referenced it allows ZigBee powered application, or any other IEEE 802.15.4 based protocols, like TIMAC - Texas Instruments lightweight PHY+MAC protocol. It also features UART serial communication for compatibility with the BOSCH Termotecnologia S.A. appliance electronics. Currently, the team employs several dongles for the purpose of wireless applications between devices. To provide a comparative reference for this solution optimization problem, a ZigBee based application was developed for a network of thermotechnology devices as referenced in the system concept. It is the purpose of this development to implement the parsing and correct broadcasting of device attributes and commands, such as current room temperature, room temperature setpoint, current water temperature, water temperature setpoint, system mode and error report.

4.2.1.2 IAR Embedded Workbench

The system software architecture consists in developing the application layer of Z-Stack[32] to allow for variable transmission from the thermotechnology devices. The dongle has a serial port connection with the appliance ECU through a proprietary UART protocol, while on the wireless side, dongles can communicate within the ISM 2.4 GHz frequency range. In this development, there was the choice of creating a simple data bridge, by broadcasting the UART messages wirelessly, or conceiving a more complex architecture that allows for data processing and storage within the wireless MCU. The author chose the latter, given the positive optionality of future data processing implementations. As mentioned before, the development environment chosen for the ZigBee Dongle Solution was IAR Embedded Workbench for 8051 (Figure 4.1), which requires a paid license. It has full compatibility with Z-Stack 3.0 (most recent version).

To provide a proof of the designed concept a setup was developed. This setup consists of a gas water heater and remote HMI, featuring a wireless, ZigBee based capability of communicating parameters for integrated connectivity. As a demonstrative case, the temperature setpoint can be defined remotely, offering increased comfort to the end user.

4.2.1.3 Base Solution Implementation and Results

The base solution suggested by the company for development was a proprietary dongle PCB armed with a Texas Instruments microcontroller CC2531. In matter of communication protocols, ZigBee was selected since it enables a mesh network topology, useful to an application with several devices and decentralized communication. In software development, there was a learning process on how to work with Z-Stack, ZigBee's programming stack, and developed what was proposed in the architecture. Within this development, it was adopted an incremental programming methodology. Firstly, a code sample was compiled for the purpose of understanding the basics about

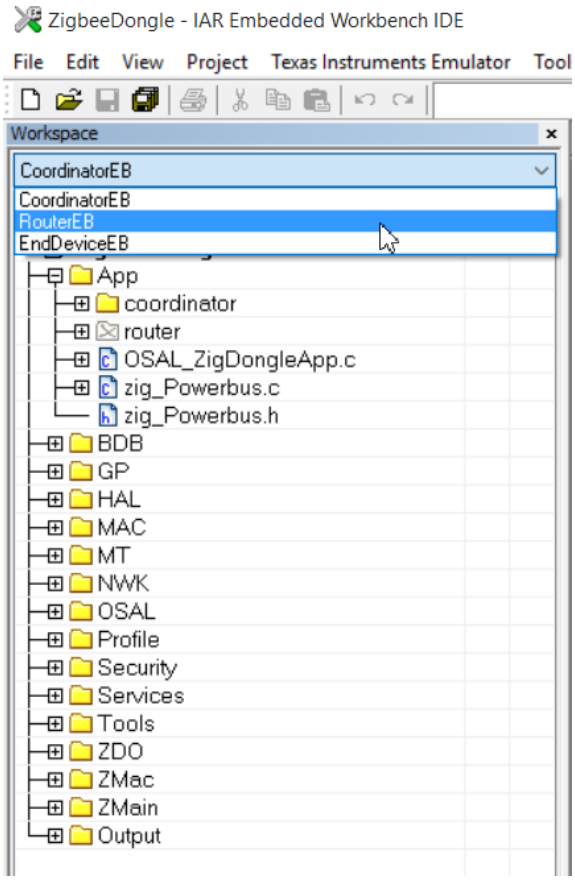
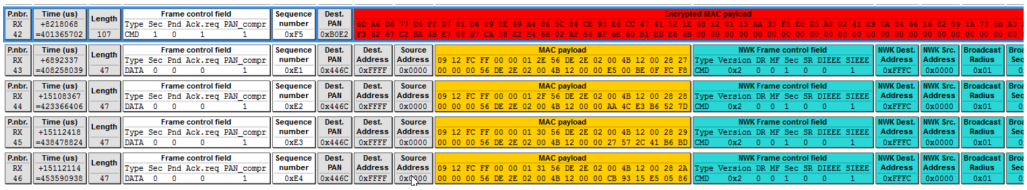


Figure 4.1: IAR Embedded Workbench

Z-Stack and, through sniffing, learning through example the data frames present in a ZigBee communication. Secondly, the code sample was improved to feature a proprietary wireless payload in ZigBee, suited to the variables of Bosch water heaters. This improvement was tested and validated. Thirdly, the code got another increment, this time with the implementation of wired communication through a Bosch UART protocol, tested and validated, creating a full data bridge between devices. Finally, tests were made to the entire system, checking for range and quality of communications around the office. A more detailed breakdown of the incremental software development process follows:

- **1**: Learning to work with Z-Stack, IAR Embedded Workbench and USB packet sniffer;
- **2**: Packet sniffing for coordinator network creation and router joint;
- **3**: Development of a structure for data processing, conceptually a bridge with a toll booth in the middle, i.e. a data link with processing capabilities;
- **4**: Software implementation of a tailored wireless payload solution for Bosch Termotecnologia S.A. requirements;
  - **a**: Test for correct wireless payload transmission and respective wireless payload reception;
  - **b**: Test for correct UART proprietary protocol transmission and reception;
- **5**: Test for end-to-end command transmission and remote device action (e.g. set temperature);

This setup is composed by two HMIs, respectively connected with a ZigBee Dongle, a Texas Instruments CC Debugger and a Zigbee Packet Sniffer for Wireless Communications analysis using Texas Instruments Packet Sniffer. This sniffer captures the raw form of all layers of communication, as exemplified in Figure 4.2. The purpose of this development is to establish a link between HMIs and ECUs. In a network of devices there will be another protocol at play, besides the wireless one. Bosch has a proprietary protocol, using UART, that does wired communication between the HMI and ECU within a gas water heater. It then becomes required for the project, after parsing wireless data in the dongle, to convert and encapsulate it and send it to another device, using the proprietary BOSCH protocol. The final result of this section can be visualized in Figure 4.3, with a demonstrative example of setpoint parsing



P.nbr.	Time (us)	Length	Frame control field	Sequence number	Dest. PAN	Encrypted MAC payload
RX 42	+8218068 =401365702	107	Type Sec Pnd Ack.req PAN_compr CMD 1 0 1 1	0xF5	0xB0E2	6D A6 D6 77 D6 FF D7 81 B6 89 8E 69 A4 B6 5C 84 CE 93 E6 CC 47 41 52 1E 60 12 01 13 AA 33 F8 E0 D5 A8 02 41 E9 0A B4 66 16 82 59 1A 73 5B A3 E0 62 67 C2 BA 4B E7 08 B7 CA 38 E2 E4 66 02 AF 56 BF 6E 60 B1 ED E6 4B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

P.nbr.	Time (us)	Length	Frame control field	Sequence number	Dest. PAN	Dest. Address	Source Address	MAC payload	NWK Frame control field	NWK Dest. Address	NWK Src. Address	Broadcast Radius	Bro Sec
RX 43	+6892337 =408258039	47	Type Sec Pnd Ack.req PAN_compr DATA 0 0 0 1	0xE1	0x446C	0xFFFF	0x0000	09 12 FC FF 00 00 01 2E 56 DE 2E 02 00 4B 12 00 28 27 00 00 00 56 DE 2E 02 00 4B 12 00 00 E5 00 BE 0F FC F8	Type Version DR MF Sec SR DIEEE SIEEE CMD 0x2 0 0 1 0 0 1	0xFFFC	0x0000	0x01	0
RX 44	+15108367 =423366406	47	Type Sec Pnd Ack.req PAN_compr DATA 0 0 0 1	0xE2	0x446C	0xFFFF	0x0000	09 12 FC FF 00 00 01 2F 56 DE 2E 02 00 4B 12 00 00 28 00 00 00 56 DE 2E 02 00 4B 12 00 00 AA 4C E3 B6 52 7D	Type Version DR MF Sec SR DIEEE SIEEE CMD 0x2 0 0 1 0 0 1	0xFFFC	0x0000	0x01	0
RX 45	+15112418 =438478824	47	Type Sec Pnd Ack.req PAN_compr DATA 0 0 0 1	0xE3	0x446C	0xFFFF	0x0000	09 12 FC FF 00 00 01 30 56 DE 2E 02 00 4B 12 00 28 29 00 00 00 56 DE 2E 02 00 4B 12 00 00 27 57 2C 41 B6 BD	Type Version DR MF Sec SR DIEEE SIEEE CMD 0x2 0 0 1 0 0 1	0xFFFC	0x0000	0x01	0
RX 46	+15112114 =453590938	47	Type Sec Pnd Ack.req PAN_compr DATA 0 0 0 1	0xE4	0x446C	0xFFFF	0x0000	09 12 FC FF 00 00 01 31 56 DE 2E 02 00 4B 12 00 28 2A 00 00 00 56 DE 2E 02 00 4B 12 00 00 CB 93 15 E5 05 86	Type Version DR MF Sec SR DIEEE SIEEE CMD 0x2 0 0 1 0 0 1	0xFFFC	0x0000	0x01	0

Figure 4.2: ZigBee Frames Sniffing using CC2531 USB Sniffer

Figure 4.3: Final Setup and Proof of Concept

4.2.2 New Solution: Sub 1 GHz Dongle

The new solution resulted from the hardware benchmark results. The selected alternative solution is the Texas Instruments CC1310 microcontroller. With a score of 0.89/1.00, it achieves third place on this list of 16 (Table 3.4). Although not presenting the best benchmark result, Texas Instruments offers more tools and resources than the other companies regarding this range of products, together with a larger online community, it increases support in debugging and testing. Texas Instruments CC1310 also gets extra credit for its compatibility with already existing tools at the company, and therefore, the chosen hardware solution for this endeavor. The alternative operates below 1 GHz in a band called sub 1 GHz. Although this device came third place in the benchmark, it presents better programming support infrastructure than the top 2 and simulated results fit the requirements. Later in the project, this solution will serve as the alternative for the base solution in wireless performance. its compatibility with already existing tools at the company, and therefore, the chosen hardware solution for this endeavor.

4.2.2.1 CC1310

Texas Instruments CC1310 [33] is a microcontroller unit (MCU) for wireless applications operating in ISM bands bellow 1 GHz, e.g. 433 and 868 MHz in Europe. It embeds a IEEE 802.15.4 based stack for protocol implementation developed by Texas Instruments, called TIMAC, in reference to the MAC protocol layer. It features a ARM Cortex-M3 Processor, tailored for fast data processing and low power consumption, AES security coprocessor, a TX power of 10 dBm @ 13.4 mA and a regular mode RX sensitivity of -124 dBm. On a compatibility note, it also allows for UART serial communication, fitting in communication with the HMI/GWH/EWS home appliances from BOSCH Thermotechnology. This microcontroller can be programmed and debugged with Texas Instruments Code Composer Studio and IAR Embedded Workbench for ARM. Further information can be found in the product datasheet.

4.2.2.2 SUB-1GHz

In contrast with the base solution presented above, powered by the microchip TI CC2531 and ZigBee protocol, a hardware benchmark was developed, as mentioned before, to evaluate new solutions for the power, range and cost constraints. The selected hardware was in the Sub 1-GHz group, due to better radio frequency propagation in domestic environments, low current consumption and a comparatively reduced cost. Within this group, the microchip TI CC1310 from Texas Instruments was the selected hardware for performance comparison with the TI CC2531.

4.2.2.3 SmartRF Studio 7 and Code Composer Studio 7

Smart RF Studio 7 (Figure 4.4) is a computer application by Texas Instruments that allows to evaluate and configure some RF devices from the brand, which the CC1310 is included. Following

the delivery of 2x TI CC1310 Launchpad, which are in other words evaluation kits, a setup was devised to test for range and signal quality.

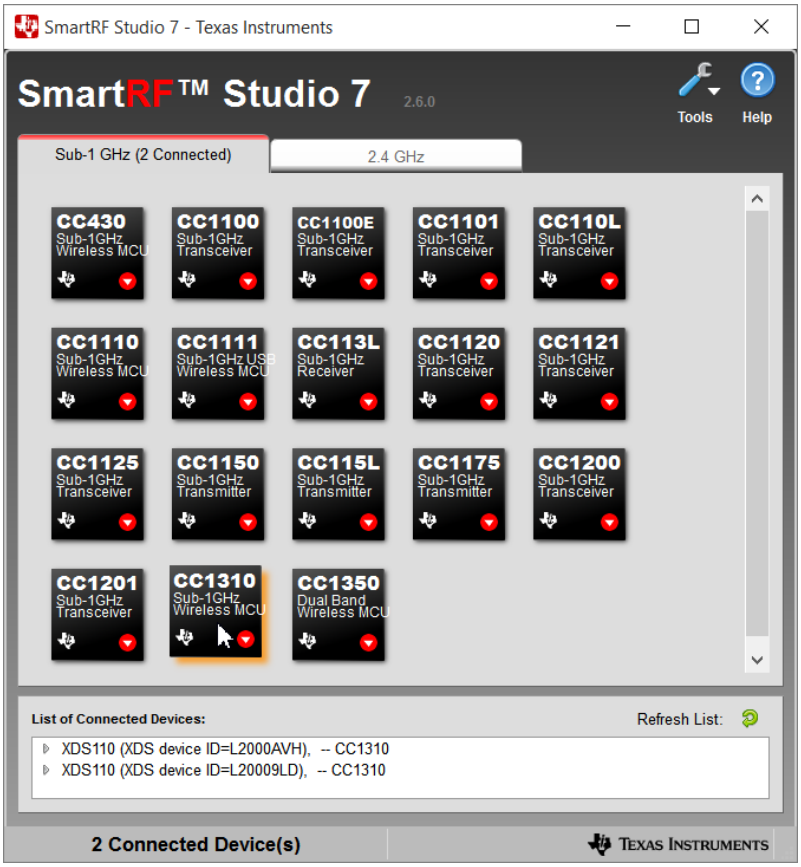


Figure 4.4: SmartRF Studio 7

Code Composer Studio is an Integrated Development Environment (IDE) by Texas Instruments, capable of programming their microcontrollers. It is referred here because it would be the tool of choice to implement a new wireless solution on the TI CC1310, based on what was done with the TI CC2531.

4.3 Wireless Solutions Performance Tests

To evaluate the wireless performance of the two solutions, a test was devised based on quality requirements. Both this test and the following tests took place at Bosch Termotecnologia S.A. research and development department. In matter of requirements, according to QR.02, QR.04 and QR.05, the system shall hold a packet error rate less than 10%, at 40 meters in visual line of sight (VLOS) with a throughput greater than 100 kbps and a frequency of 2.4GHz. Since the CC2531 solution is running on ZigBee protocol, it operates between 20 and 250 kbps throughput. The system was tested and the results were compiled in the following table.

Scenario	Walls	Packets	Errors	%
Office, 2m	0	20	0	<5%
Office, 4m	0	20	0	<5%
Office, 6m	0	20	0	<5%
Office, 8m	0	20	0	<5%
Office, 10m	0	20	0	<5%
Office, 12m	0	20	0	<5%
Office, 14m	0	20	1	5%
Office, 16m	0	20	2	10%
Office, 18m	0	20	3	15%
Office, 20m	0	20	2	10%
Office, 22m	0	20	2	10%
Office, 24m	0	20	2	10%
Office, 26m	0	20	1	5%
Office, 28m	0	20	2	10%
Office, 30m	0	20	1	5%
Office, 32m	0	20	5	25%
Office, 34m	0	20	3	15%
Office, 36m	0	20	9	45%
Office, 38m	0	20	9	45%
Office, 40m	0	20	10	50%

Table 4.1: Base Solution (TI CC2531) Wireless Performance Test Results

Similarly to the previous stage, the same test was applied to the CC1310 microcontroller solution. The chosen data rate was 200 kbps and a frequency of 868 MHz to make an accurate comparison with ZigBee's rates. As noted in the following table, this solution fulfilled quality requirements, holding a 200 kbps link at 40 meters in visual line of sight (VLOS) with less than 10% packet error rate. It revealed better results, as was expected from the RF propagation models. This is because Sub 1 GHz frequencies offer a enhanced penetration ability both in free space and obstacles.

On a further note, a new test was developed, keeping the throughput of 200kbps and 40 meters distance, but this time with 4 walls (50 centimeters thick), and still the device held a packet error rate of less than 5%. The most significant observation from these tests is that, as predicted in theory, frequency and co-existence play a major role in determining wireless performance.

In summary, under the same test, the CC2531 and CC1310 microcontrollers produced very different results. Results are quite negative compared to what the RF propagation models predicted, at the end of Chapter 3. It is speculated that this is due to environmental factors, as the waves can encounter solid metal, shielding its passage in certain points. If the signal is not affected, then obstacles around the office, from desks to chairs can produce a negative effect in RF propagation. Finally, analyzing both tests results, and given that the antenna in the TI CC1310 LaunchPad is wider and larger than the base counterpart, results may be exaggerated. However, it is to be argued that the almost 10dB (one order of magnitude) link budget advantage the new solution has versus

Scenario	**Walls**	**Packets**	**Errors**	**%**
Office, 2m	0	20	0	<5%
Office, 4m	0	20	0	<5%
Office, 6m	0	20	0	<5%
Office, 8m	0	20	0	<5%
Office, 10m	0	20	0	<5%
Office, 12m	0	20	0	<5%
Office, 14m	0	20	0	<5%
Office, 16m	0	20	0	<5%
Office, 18m	0	20	0	<5%
Office, 20m	0	20	0	<5%
Office, 22m	0	20	0	<5%
Office, 24m	0	20	0	<5%
Office, 26m	0	20	0	<5%
Office, 28m	0	20	0	<5%
Office, 30m	0	20	0	<5%
Office, 32m	0	20	0	<5%
Office, 34m	0	20	0	<5%
Office, 36m	0	20	0	<5%
Office, 38m	0	20	0	<5%
Office, 40m	0	20	0	<5%

Table 4.2: New Solution (TI CC1310) Wireless Performance Test Results

the base one corrects the significance of antenna difference for results.

Chapter 5

Conclusion and Future Work

This chapter wraps this dissertation, by listing and reviewing the key findings and achievements this work has enabled. After going through the literature, design and implementation of the system, testing and analyzing results; the author will now assess the illations that arise from this project, *id est*, the importance of this research for academic, corporate or discretionary pursuers of wireless solutions design and recommendations for future research and developments.

5.1 Main Achievements

This work accompanies the current revolution of the Internet of Things (IoT). It has three main deliverables, this document, which thoroughly reviews literature and logs the activities undertook during the project's research and development stages; a solution, implemented in prototype, tested and demonstrative of the concepts of cordless connectivity; and recommendations on cost and performance optimization for wireless solution design.

From the literary scrutiny, a trend is noted in semiconductor manufacturers for the next 10 years, for more competitive solutions, driving the price down and improving specifications, like what happened in the past five years with Microelectromechanical Sensors (MEMS), which have seen their cost reduced from 30-70%. Also, due to current and projected market sizes for the IoT business, the process of selecting or developing solutions for real world implementations will have a major economic impact in determining organizations that survive the battle for the ubiquitous connectivity sector. Although Industry 4.0 occupies the relative majority of the IoT market size, the minor sphere of household applications is not to be unvalued. since it encompasses $USD 200 Billion to $USD 300 Billion projected impact in 2025 [6], about 3-5% of total.

From the academic work cited, a plethora of protocols is available for multiple types of wireless applications. These technologies enable a customizable approach in designing a solution for connectivity challenges, enabling low powered applications as with Bluetooth Low Energy, long range with sub 1 GHz protocols or high data rates with WiFi 802.11ac. As of today, there are physical limits to the real, that lay two features in mutual exclusive conflicts, as between data rate, hence frequency bound by modulation, and signal range. For now, technology has only enabled

us to produce an optimized solution within constraints of two or more variables when designing a wireless solution.

From the prototyping endeavor, after the project management workflow, a solution was devised and implemented, resulting in a system that could communicate wirelessly without flaws up to 30 meters and traded instructions and parameters between Bosch devices. The solution, in the hardware layer consists of a proprietary PCB dongle with a Texas Instruments CC2531, while the software layer is based on ZigBee, firstly because of compatibility with the microcontroller and secondly because of matching application specifications for household devices. However, the software implementation is a proprietary tailored solution which happens to be based on ZigBee. As a conclusive assessment of the software stage, it is recognized as advantageous the ease in development and enhanced connectivity for using standardized protocols in the public domain, however tailored proprietary solutions can present an improved fit for the challenge and often present enhanced security, since data frames are not of public knowledge.

From the hardware optimization models, the microcontroller from Texas Instruments CC1310 was selected. This MCU operates below 1 GHz, which grants better obstacle penetration capability and less path loss while keeping a low data rate that is more than sufficient for the desired application. Moreover, it is mostly ready for proprietary software implementations and it has a lower cost than the currently employed CC2531 microcontroller. Therefore, it is this dissertation's verdict, supported by the wireless performance test results, that the CC1310 presents itself as a better solution in all requirements compared with the present one.

5.2 Future Work

This work wouldn't be complete without a forward look to what could be further developed if the project continued. A system that wirelessly communicates was developed, but now, further improvements should be made, following the trend of data processing, machine learning for an enhanced user experience. User Experience comprises the qualitative, soft data metrics of end user appreciation for the way it interacts with technology. It has always been one of the engineer's main focus when developing a system. Now the same question poses for this wireless solution, how can this system provide an enhanced User Experience? Within the Internet of Things trending expressively, connectivity has gained quite the status as a core user experience parameter, unlocking other data processing opportunities, that in turn, provide an even better user experience is the way many companies are pursuing. Also, in the topic of data processing, data mining and data analytics have been recently criticized across media channels and many elements from the public, for posing a threat to user privacy. It is not the objective of this project, to trade off user privacy for user experience using remote cloud connectivity. Therefore, data processing should be kept for user's use only. How could this be achieved? Firstly, by isolating the network from out-of-home communication channels with the choice of a home access network protocol with military grade security, such as ZigBee: and secondly, by focusing on the impact that engineering can have in

adding value to human life, through implemented heuristics for predictive and adaptive device control.

5.2.0.1 Fuzzy Seasons and Green Home

Fuzzy Seasons was the given name to a simple data processing heuristic evaluated during this project. It consists in using Fuzzy Logic for seasonal adaptive temperature control, combined with a timestamp for time tracking. It also makes use of average local temperature programmed from production for the geography of the end user. Realized, it would be a passive system that would take care of defining water or room temperature in absence of user interaction for energy and comfort optimization.

Firstly, four membership functions representing seasons are created with 52 samples, equivalent to the number of weeks in a year. Then the average temperature for the device region is added to each week. The idle temperature setpoint is defined by the software, taking into account the preferential room or water temperature for each season (e.g. 21^{o}C for Spring, 20^{o}C for Summer, 21^{o}C for Fall and 22^{o}C for Winter). This value will now change for each season, given the weighted average of the user's last ten inputs, weighted a second time, with what the user has done in homologous timestamps from previous years.

A further use for water heating devices data is the opportunity for saving energy during the time the residents are out of home. By asking to input leave and arrival hours for workdays in device setup and configuration, the GWH/EWS will turn off energy use for those hours and turn it back on a sufficient time before arrival for the home to be at the desired temperature. According to a spreadsheet estimationl, it can achieve savings up to 25%, however this outcome may vary, according to the infrastructure heat dissipation.

There are currently other companies in the market that already sell Smart Thermostats, with adaptive control given user inputs and user home leave or arrival, given smartphone presence in the home Wi-Fi network, such as NEFIT, NEST, Ecobee or Honeywell. Such products are aligned with the Internet of Things revolution in home appliances, enhancing the user experience and that should be the way for this project's future improvements.

5.3 Closing Remarks

Finally, this dissertation is deemed relevant for individuals or organizations that pursue wireless solutions design for household appliances, trending on the Internet of Things. A technological breakthrough is disclaimed during this project, claiming that only already existing solutions, methodologies and heuristics from various fields of thought were combined to produce a wireless implementation for Bosch Thermotecnologia S.A.'s home appliances. In a closing remark, it is noted that technological breakthrough is not equivalent to innovation. A breakthrough is a discrete event where a new tool that was deemed out of grasp in physical or logical limits is achieved,

while innovation is a continuous dynamic process that adds or subtracts concepts from multidisciplinary fields and fuses them into a new concept. Therefore this dissertation is written in the spirit of innovation, looking for ways to synergize already existing technologies into a new ones.

Appendix A

Appendix

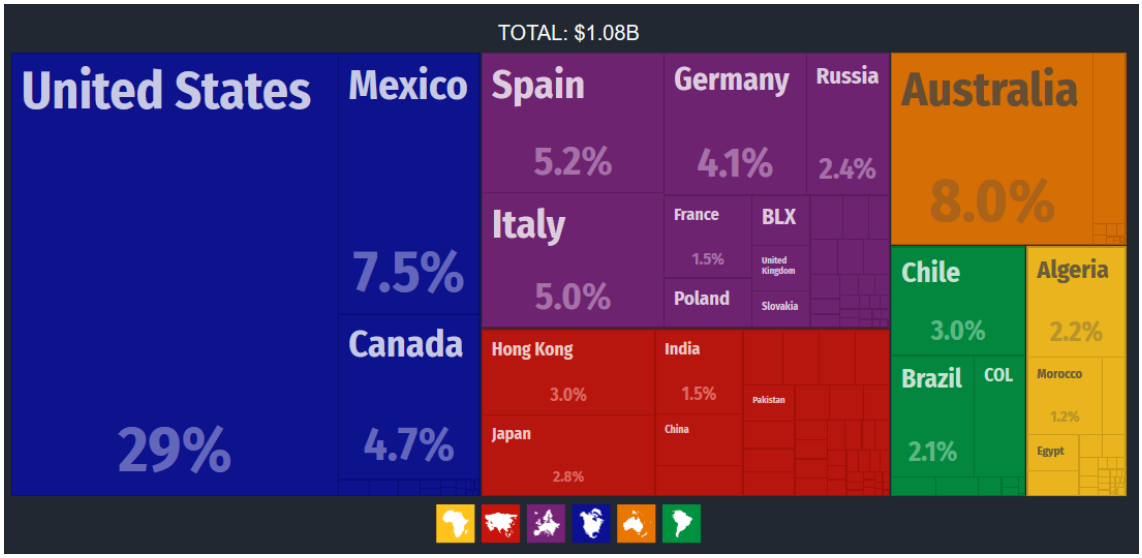


Figure A.1: Worldwide Importers - Instantaneous Gas Water Heater Trade (2015) [2]

Table A.1: Expanded Hardware Selection Benchmark

FREQUENCY/PROTOCOL	COMPONENT	TYPE	BATTERY	CHARGE_(mAh)	TX_CURRENT_(mA)	SLEEP_CURRENT_(mA)	BATTERY_LIFE_(hours)	BATTERY_LIFE_(months)	SIGNAL_POWER_(dBm)	SENSITIVITY_(dBm)	RANGE_(m)	UNIT_COST_($USD)	STORE	BENCHMARK_SCORE
2.4_GHz_ZigBEE	Texas_Instruments_CC2531_ZigBee	MCU	4x_Alkaline_AAA	4000	33.5	0.1	1581.92	2.2	4.5	-92	300	3.20	Texas Inst.	0.21
2.4_GHz_ZigBEE	NXP_JN5169-001_M00_ZigBee	MCU	4x_Alkaline_AAA	4000	23	0.001	2432.77	3.38	10	-96	2000	9.45	Farnell	0.36
2.4_GHz_Bluetooth	Texas_Instruments_CC2640_BLE	MCU	4x_Alkaline_AAA	4000	9.1	0.002	6128.26	8.51	5	-97	140	2.10	Farnsel	0.32
sub_1_GHz	Texas_Instruments_CC1310	MCU	4x_Alkaline_AAA	4000	13.4	0.001	4173.19	5.8	10	-124	2000	2.27	Texas Inst.	0.89
sub_1_GHz	On_Semiconductor_AX5043	MCU	4x_Alkaline_AAA	4000	6.5	0.001	8590.27	11.93	0	-137	1000	0.85	On Semi	0.96
sub_1_GHz	NXP_KW02x_M3_ZigBee_868MHz	MCU	4x_Alkaline_AAA	4000	45	0.001	1243.92	1.73	13	-120	1500	4.19	NXP	0.85
sub_1_GHz	ST_S2-LP	MCU	4x_Alkaline_AAA	4000	10	0.001	5593.38	7.76	10	-130	1500	1.44	ST	1.00
2.4_GHz_ZigBEE	XBEE_Series_1_ZigBee	Module	4x_Alkaline_AAA	4000	45	0.05	1218.72	1.69	0	-92	130	24.95	SparkFun	0.11
2.4_GHz_ZigBEE	Telegesis_ETRX357_ZigBee	Module	4x_Alkaline_AAA	4000	31	0.001	1805.35	2.51	3	-99	1000	11.75	Farnell	0.35
2.4_GHz_Bluetooth	Panasonic_PAN1740_BLE	Module	4x_Alkaline_AAA	4000	5	0.001	11157.6	15.5	0	-93	150	10.66	Mouser	0.22
2.4_GHz_Bluetooth	Skylab_SKB360_BLE	Module	4x_Alkaline_AAA	4000	1.3	0.003	41267.5	57.32	4	-93	300	19.99	Skylab	0.29
2.4_GHz_Bluetooth	Silicon Labs_BLE113_BLE	Module	4x_Alkaline_AAA	4000	27	0.002	2071.16	2.88	0	-93	100	11.02	Digi-Key	0.20
2.4_GHz_Bluetooth	Fansel_BT832X_BLE	Module	4x_Alkaline_AAA	4000	95	0.002	589.24	0.82	20	-92	1500	14.96	Farnsel	0.50
sub_1_GHz	Embit_ZRF212B_ZigBee_868MHz	Module	4x_Alkaline_AAA	4000	17	0.001	3390.44	4.57	10	-110	1000	4.19	Embit	0.88
sub_1_GHz	Atmel_ZigBit_ATZB-RF-212B	Module	4x_Alkaline_AAA	4000	26.9	0.001	2080.32	2.89	11	-103	440	24.25	Atmel	0.50
sub_1_GHz	MRF89XAMA-IRM_boost	Module	4x_Alkaline_AAA	4000	30	0.002	1864.31	2.59	10	-107	1000	6.04	Mouser	0.72
sub_1_GHz	ANSolutions_ANY900	Module	4x_Alkaline_AAA	4000	33	0.006	1691.13	2.35	-3	-110	500	27.50	ANS	0.37

ID / Acronym	Name	Description	Risk	Impact	Scenario	Prevention	Defense Complexity
COA	Ciphertext Only Attack	Attacker has access to a set of ciphertext.	HIGH	VERY LOW	The encryption key may bedetermined by the attacker.	Modern Cryptosystem areguarded against this type of attack.	VERY LOW
KPA	Known PlaintextAttack	Attacker knows the plaintextfor some parts of the ciphertext.	MEDIUM	HIGH	Attempts to decrypt the restfrom the given pair.	Not using linear block cyphers.	MEDIUM
CPA	Chosen PlaintextAttack	The attacker has the text of hischoice encrypted.	HIGH	VERY HIGH	Easy determination of encryption keythrough differential cryptanalysis.	Changing keys frequently.Not having predictable messages in communications.	VERY HIGH
DiA	Dictionary Attack	The attacker tries to obtain the key through a dictionary of popular keys.	MEDIUM	VERY LOW	The encryption key is determinedbecause it is a weak one.	Using random and complex keys.	LOW
BFA	Brute ForceAttack	The attacker exaustively tries allpossible combinations to obtain the key.	LOW	LOW	The encryption key is determined bythe attacker over time.	Using long and complex keys only,	VERY LOW
BiA	BirthdayAttack	The attacker targets the hashfunction to reduce possibelcombinations for the key.	MEDIUM	MEDIUM	The encryption key is determined ina collision: two different inputs produce the same hash value.	Increasing the number of bits inthe encryption key and changing keys oftenly.	MEDIUM
MiM	Man in MiddleAttack	The attacker intercepts a public keyrequest and sends his instead.	HIGH	HIGH	The attacker will decrypt all sentmessages,	Not using asymmetric cryptography.	MEDIUM
TmA	TimingAttack	The attacker reduces bruteforce time by infering the key through processing time between requests.	LOW	LOW	The attacker is able to count time between requests.	Always taking the same time toprocess requests,	MEDIUM
PAA	Power AnalysisAttack	The attacker reduces bruteforce time by infering the key through power consumption between requests.	VERY LOW	LOW	The attacker is able to accesspower consumption levels.	Being able to secure access tothe hardware.	HIGH
FAA	Fault AnalysisAttack	The attacker reduces bruteforce time by infering the key through induced errors.	MEDIUM	HIGH	The attacker is able to input errorsin messages.	Having na alarm system forunexpected communications.	HIGH

Table A.2: Security Risks Analysis

Season	**Membership Function**				**Avg. Temperature(°C)**
	Winter%	Spring%	Summer%	Fall%	Stuttgart, GER
Winter	90.00%	0.00%	0.00%	10.00%	0
Winter	100.00%	0.00%	0.00%	0.00%	0
Winter	100.00%	0.00%	0.00%	0.00%	0
Winter	100.00%	0.00%	0.00%	0.00%	0
Winter	90.00%	0.00%	0.00%	0.00%	2
Winter	80.00%	0.00%	0.00%	0.00%	2
Winter	70.00%	10.00%	0.00%	0.00%	2
Winter	60.00%	20.00%	0.00%	0.00%	2
Winter	50.00%	30.00%	0.00%	0.00%	6
Winter	40.00%	40.00%	0.00%	0.00%	6
Winter	30.00%	50.00%	0.00%	0.00%	6
Spring	20.00%	60.00%	0.00%	0.00%	6
Spring	10.00%	70.00%	0.00%	0.00%	9
Spring	20.00%	80.00%	0.00%	0.00%	9
Spring	10.00%	90.00%	0.00%	0.00%	9
Spring	0.00%	100.00%	0.00%	0.00%	9
Spring	0.00%	100.00%	0.00%	0.00%	14
Spring	0.00%	100.00%	0.00%	0.00%	14
Spring	0.00%	90.00%	0.00%	0.00%	14
Spring	0.00%	80.00%	10.00%	0.00%	14
Spring	0.00%	70.00%	20.00%	0.00%	17
Spring	0.00%	60.00%	30.00%	0.00%	17
Spring	0.00%	50.00%	40.00%	0.00%	17
Spring	0.00%	40.00%	50.00%	0.00%	17
Summer	0.00%	30.00%	60.00%	0.00%	19
Summer	0.00%	20.00%	70.00%	0.00%	19
Summer	0.00%	10.00%	80.00%	0.00%	19
Summer	0.00%	20.00%	90.00%	0.00%	19
Summer	0.00%	10.00%	100.00%	0.00%	19
Summer	0.00%	0.00%	100.00%	0.00%	18
Summer	0.00%	0.00%	100.00%	0.00%	18
Summer	0.00%	0.00%	90.00%	0.00%	18
Summer	0.00%	0.00%	80.00%	10.00%	18
Summer	0.00%	0.00%	70.00%	20.00%	18
Summer	0.00%	0.00%	60.00%	30.00%	15
Summer	0.00%	0.00%	50.00%	40.00%	15
Summer	0.00%	0.00%	40.00%	50.00%	15
Fall	0.00%	0.00%	30.00%	60.00%	15
Fall	0.00%	0.00%	20.00%	70.00%	15
Fall	0.00%	0.00%	10.00%	80.00%	10
Fall	0.00%	0.00%	20.00%	90.00%	10
Fall	0.00%	0.00%	10.00%	100.00%	10
Fall	0.00%	0.00%	0.00%	100.00%	10
Fall	0.00%	0.00%	0.00%	100.00%	10
Fall	10.00%	0.00%	0.00%	90.00%	5
Fall	20.00%	0.00%	0.00%	80.00%	5
Fall	30.00%	0.00%	0.00%	70.00%	5
Fall	40.00%	0.00%	0.00%	60.00%	5
Fall	50.00%	0.00%	0.00%	50.00%	2
Fall	60.00%	0.00%	0.00%	40.00%	2
Winter	70.00%	0.00%	0.00%	30.00%	2
Winter	80.00%	0.00%	0.00%	20.00%	2

Table A.3: Fuzzy Seasons Membership Functions

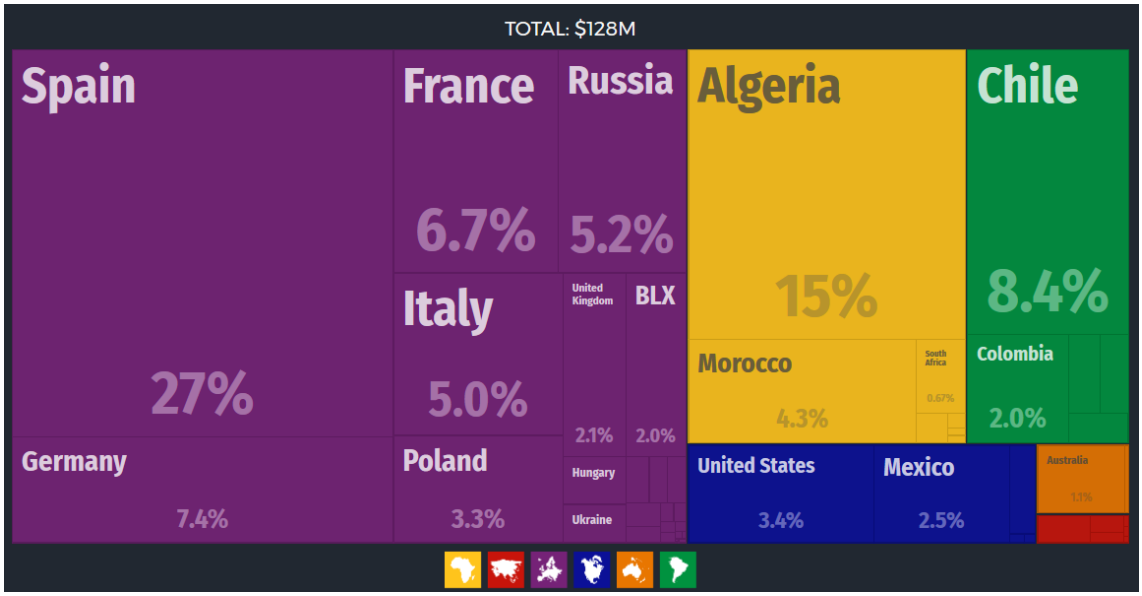


Figure A.2: Portuguese Export Destinations - Instantaneous Gas Water Heater Trade (2015) [2]

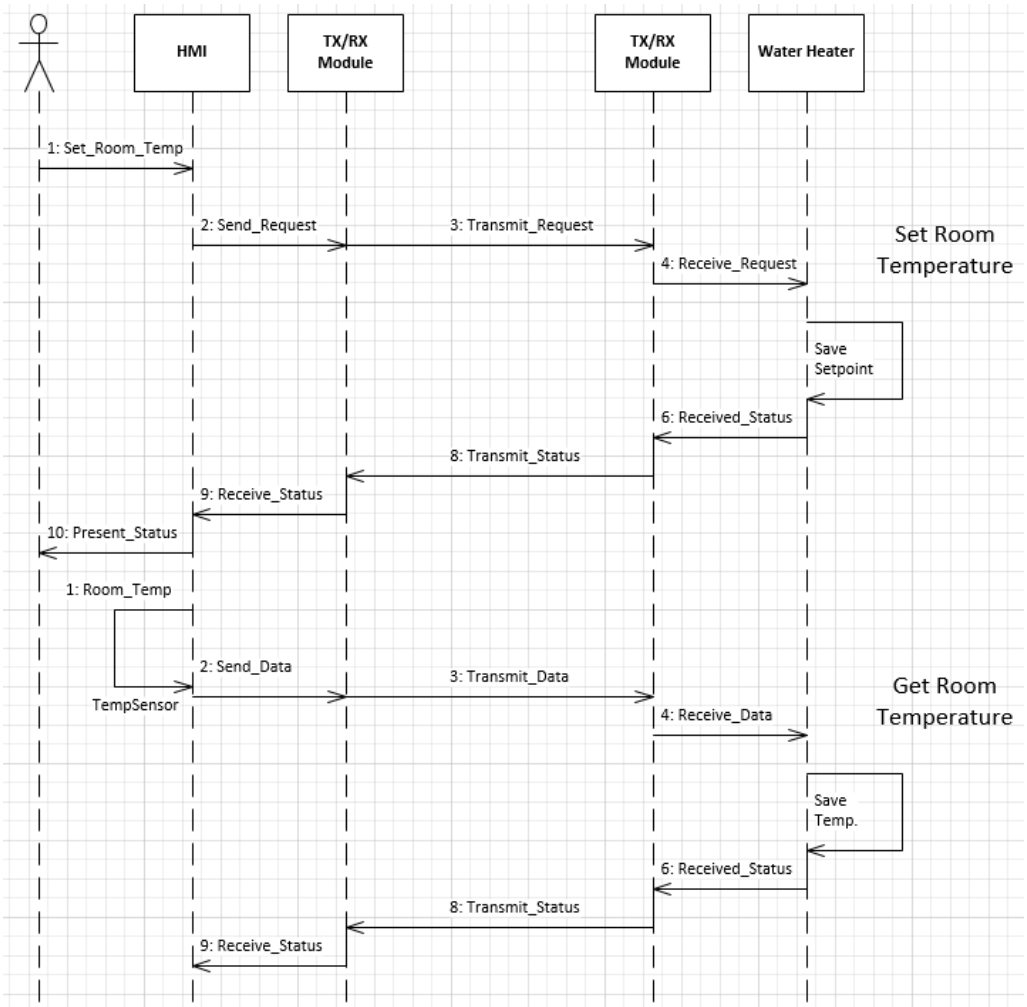


Figure A.3: Sequence Diagram I

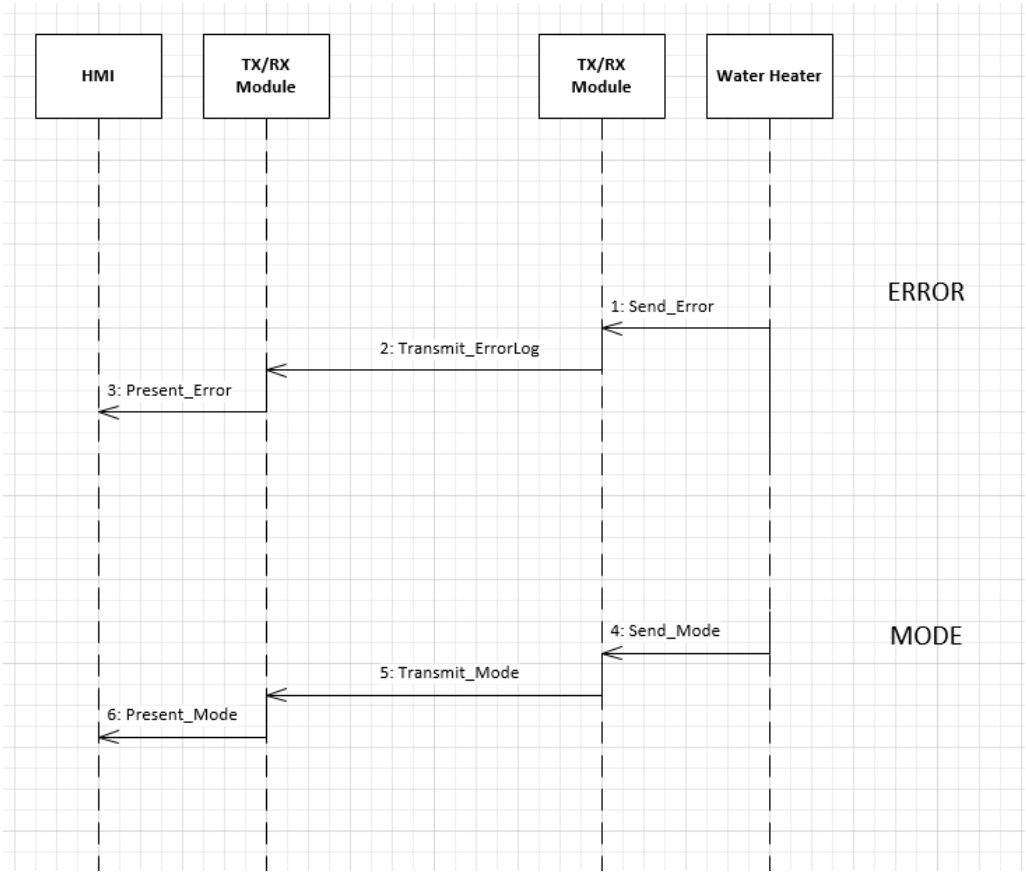


Figure A.4: Sequence Diagram II

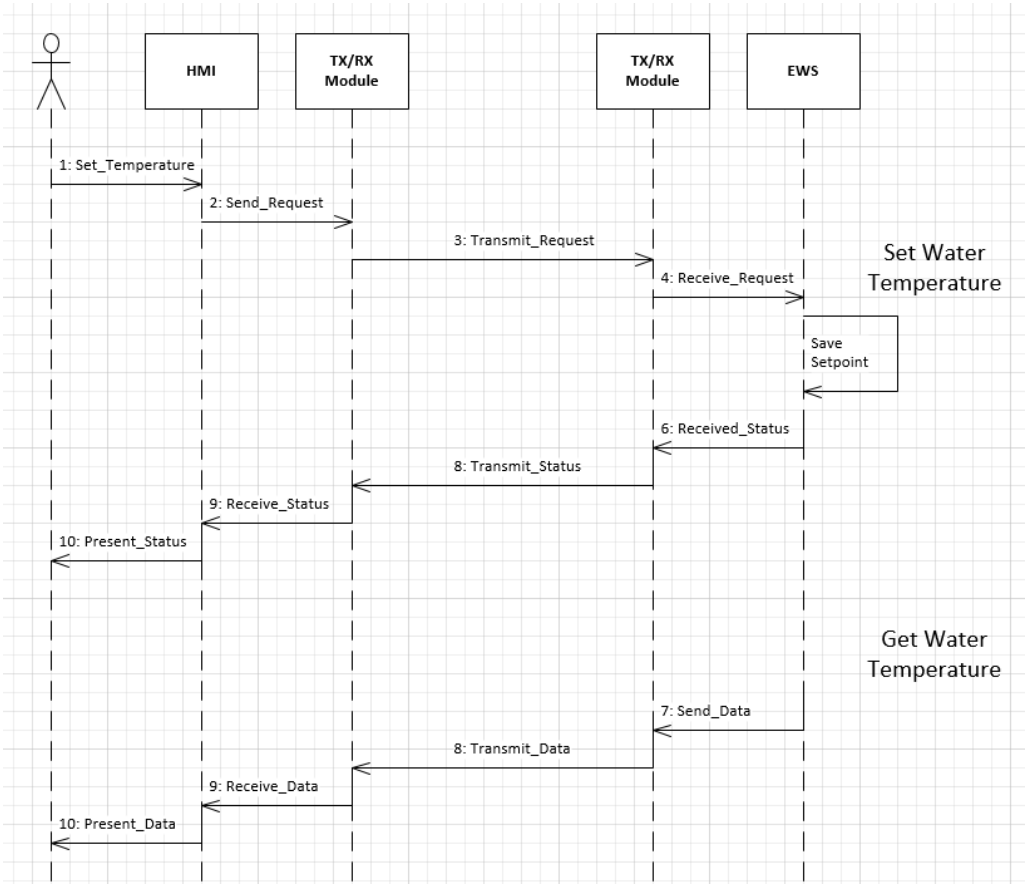


Figure A.5: Sequence Diagram III

Figure A.6: Gantt Chart

References

[1] Breecham Research. M2m world of connected devices - internet of things, 2014. Available at https://evothings.com/how-open-source-initiatives-can-influence-the-internet-of-things//, accessed last time June 8, 2017.

[2] Observatory for Economic Complexity. Exporters: Instantaneous gas water heater trade, 2015. Available at http://atlas.media.mit.edu/en/profile/hs92/841911///, accessed last time June 8, 2017.

[3] Breecham Research. Bosch group, 2017. Available at http://www.bosch.de/en/de/our_company_1/our-company-lp.html, accessed last time June 12, 2017.

[4] Breecham Research. Bosch thermotechnology, 2017. Available at http://www.bosch.de/en/de/our_company_1/business_sectors_and_divisions_1/thermotechnology_1/thermotechnology.html, accessed last time June 12, 2017.

[5] Cisco visual networking index predicts near-tripling of ip traffic by 2020. Technical report, CISCO, 2016.

[6] McKinsey Global Institute. Internet of things: Mapping the value beyond the hype. Technical report, McKinsey & Co, June 2015.

[7] OECD. Gdp long-term forecast, 2017. Available at https://data.oecd.org/gdp/gdp-long-term-forecast.htm//, accessed last time June 8, 2017.

[8] P. Suresh, J. Vijay Daniel, Dr.V.Parthasarathy, and R.H. Aswathy. A state of the art review on the internet of things (iot). 2014.

[9] Michael A. Jensen. A history of mimo wireless communications. pages 681–682, 2016.

[10] Muzaiyanah Hidayab, Abdul Halim Ali, and Khairul Bariah Abas Azmi. Wifi signal propagation at 2.4 ghz. 2009.

[11] World Bank International Telecommunication Union (ITU) and United Nations Population Division. Internet users in the world, 2017. Available at http://www.internetlivestats.com/internet-users//, accessed last time June 8, 2017.

[12] Inc. Link Labs. Selecting a wireless technology for new industrial internet of things products. a guide for engineers and decision makers. Technical report, LinkLabs, 2016.

[13] Carles Gomez and Josep Paradells. Wireless home automation networks: A survey of architectures and technologies. 2010.

[14] Ashwin Barve, Jaimin Shah, Sahil Shah, Anirudh Menon, Dr. Ken Baker, and Bruce Montgomery. Implementing 802.11ah – the sub-1 ghz wi-fi standard. April 2016.

[15] N. Ahmed, H. Rahman, and Md.I. Hussain. A comparison of 802.11ah and 802.15.4 for iot. pages 100–103, August 2016.

[16] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen. A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi. November 2007.

[17] Jonas Olsson. 6lowpan demystified. Technical report, Texas Instruments, 2014.

[18] Jukka K. Nurminen Matti Siekkinen, Markus Hiienkari and Johanna Nieminen. Wifi signal propagation at 2.4 ghz. 2012.

[19] Midhya Mohan E, Neena George P, and Diana Davis. Zigbee technology for data communication - a comparative study with other wireless technologies. 2014.

[20] Kedar Nath Sahu, Dr. Challa Dhanunjay Naidu, and Dr. K Jaya Sankar. Study of rf propagation losses in homogeneous brick and concrete walls using analytical frequency dependent models. pages 58–66, October 2014.

[21] Matthias Lott and Ingo Forkel. A multi-wall-and-floor model for indoor radio propagation. pages 464–469, 2001.

[22] Robert Wilson. Propagation losses through common building materials: 2.4 ghz vs 5 ghz. August 2002.

[23] Omar Abdul Aziz and Tharek Abdul Rahman. Investigation of path loss prediction in different multi-floor stairwells at 900mhz and 1800mhz. pages 27–39, June 2014.

[24] Jonas Medbo and Jan-Erik Berg. Simple and accurate path loss modeling at 5 ghz in indoor environments with corridors. pages 30–37, 2000.

[25] Nurul I. Sarkar and Kevin W. Sowerby. Wi-fi performance measurements in the crowded office environment: a case study. 2007.

[26] Joseph Weibler. Properties of metals used for rf shielding. December 1993.

[27] Hany Elgala, Raed Mesleh, and Harald Haas. Indoor optical wireless communication: Potential and state-of-the-art. pages 56–62, September 2011.

[28] William C. Stone. Nist construction automation program report no. 3 - electromagnetic signal attenuation in construction materials. Technical report, National Institute of Standards and Technology, October 1997.

[29] S. Loyka. Indoor propagation models, September 2015. University of Ottawa, Canada, available at http://www.site.uottawa.ca/~sloyka/elg4179/Lec_4_ELG4179.pdf, accessed last time June 6, 2016.

[30] Elaine Barker, Lily Chen, Allen Roginsky, and Miles Smid. Special publication 800-56a revision 2, recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography. Technical report, NIST, 2013.

[31] Texas Instruments Inc. A usb-enabled system-on-chip solution for 2.4-ghz ieee 802.15.4 and zigbee applications. Technical report, Texas Instruments Inc., 2010.

[32] Inc. Texas Instruments. Z-stack application programming interface. Technical report, Texas Instruments, Inc., 2011.

[33] Inc. Texas Instruments. Cc1310 simplelink^{TM} ultra-low-power sub-1 ghz wireless mcu. Technical report, Texas Instruments Inc., 2016.