Tampere University

Md Abu Hemjal

SIGFOX BASED INTERNET OF THINGS: TECHNOLOGY, MEASUREMENTS AND DEVELOPMENT

Faculty of Information Technology and Communication Sciences
Master of Science thesis
May 2019

ABSTRACT

MD. ABU HEMJAL: Sigfox based Internet of Things: Technology, Measurements and Development
Master of Science thesis
Tampere University
Master's Degree Programme in Electrical Engineering
May, 2019

Nowadays, Internet of Things (IoT) has emerged as a powerful platform for solving everyday problems. In order to make our life easier and more efficient, the physical objects which surround us have to become smarter. Also, due to saving of valuable economic and human resources when IoT is used, it becomes important for both household and industrial sectors to incorporate IoT products one way or another in their applications. In the new global economy, IoT is expected to save billions of dollars in the near future.

The concept of IoT was developed to connect billions of low power devices over a large area commonly referred as low power wide area network (LPWAN). Because of its scalability, low cost, and high security, IoT is becoming a highly popular technology nowadays. LPWAN has various technologies, and the most leading ones are: Sigfox, NB-IoT, and LoRa. Sigfox was first developed as a proprietary standard IoT protocol in Toulouse, France in the year 2009.

The first part of the thesis addresses the concept of IoT and why is it so important in the present world. In addition, the first part encompasses the most common IoT protocols and their features. Furthermore, first part describes some IoT applications and its impact on global economy. The second part of the thesis concentrates in depth on Sigfox-based IoT protocol. Also, the second part comprises technical details of Sigfox protocol, systems architecture, and most importantly issues related to Sigfox radio network planning and implementation. The third part of the thesis describes the Thinxtra Xkit device which is a prototyping platform for Sigfox network. In the third part, the Xkit device was used to evaluate Sigfox network performance in Tampere University (TAU), Hervanta campus area. All measurements presented in the third part were evaluated with the help of MATLAB, also they were illustrated through heat maps for further performance analysis.

Finally, this thesis proposes a way to integrate Sigfox network with other similar network technologies. Also, the final part suggests some possible ways to develop Sigfox network in terms of Quality of Service (QoS).

Keywords: IoT, Low Power Wide Area Networks, Sigfox.

PREFACE

The research and development work presented in this thesis has been carried out at the Department of Electrical Engineering of Tampere University (Hervanta Campus), Tampere, Finland. The thesis was done under the supervision of Dr. Joonas Säe and is part of the requirement to fulfill my Master of Science degree program in Electrical Engineering.

First and foremost, I have been extremely fortunate to work under the supervision of Dr. Joonas Säe, who has been very supportive and encouraging to complete my thesis. His unconditional efforts have improved my research work and capabilities significantly. Also, I would like to express my deepest appreciation to Prof. Elena Simona Lohan from Tampere University. As an instructor of the course "Internet of Things (IoT)", she initialized my interest to carried out my master's thesis in the field of IoT. I am highly grateful to my examiner Prof. Mikko Valkama for accepting me as a research worker with his team.

I would like to give special thanks to my friend Ibrahim Touman, who helped me to increase my knowledge in the field of Communication Engineering. His unconditional help and direction to improve this thesis will never be forgotten. I would also express my gratitude to my group-mates, classmates, and friends in TUT, we shared all the precious working and studying memories together.

My appreciation goes to my mother Halima Talukder, who has struggled hard throughout her life, put all of her effort for her children, and help me to think beyond our capabilities and my father Mohammed Shamser Ali, who is still working hard to keep my mothers dream alive. My parents constant support and encouragement have been considered as the most cogent motivation for me. Specially, I also want to take this opportunity to thank Asma Suhaily, for the sacrifices which you made during my stay in abroad. Each sprint in life is accompanied by you.

Finally, I thank Allah, Almighty for the gift of life, knowledge, and wisdom.

Tampere, 30.3.2019 Md. Abu Hemjal

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND SYMBOLS

5G	Fifth Generation Mobile Network
5GTN	Fifth Generation Mobile Test Network
6-LowPAN	IPv6 over Low-Power Wireless Personal Area Networks
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
API	Application Programming Interface
AWS	Amazon Web Services
BPSK	Binary Phase Shift Keying
BTS	Base Transceiver Station
BW	Bandwidth
CoAP	Constrained Application Protocol
D2D	Device to Device
DBPSK	Differential Phase Shift Keying
DL	Download
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
ECC	Error Correcting Code
FCS	Frame Check Sequence
FDMA	Frequency Division Multiple Access
FIIF	Finnish Industrial Internet Forum
GFSK	Gaussian Frequency Shift keying
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GUI	Graphical User Interface
HTTPS	HyperText Transport Protocol Secure
IDE	Integrated Development Environment
IoT	Internet of Things
IOE	Internet of Everything
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
LOS	Line of Sight
LBT	Listen Before Talk
LoRa	Long Range
LPWAN	Low Power Wide Area Network
LQI	Link Quality Indicator
LTN	Low Throughput Network
M2M	Machine to Machine
MIC	Message Integrity Code
MQTT	Message Queue Telemetry Transport
MSAN	Multi-service Access Node
NB-IoT	Narrowband IoT
OFDM	Orthogonal Frequency Division Multiplexing

OSS	Operational Support System
OTA	Over the Air
P2M	Person to Machine
P2P	Person to Person
PAC	Porting Authorization Code
PRR	Packet Reception Rate
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
REST	Representational State Transfer
RFID	Radio-frequency Identification
RFTDMA	Random Frequency and Time Division Multiple Access
RSSI	Received Signal Strength Indicator
SBS-T	Sigfox Base Station Transceiver
SNR	Signal to Noise Ratio
SQL	Structured Query Language
TAU	Tampere University
TCP	Transmission Control Protocol
UL	Upload
URL	Uniform Resource Locator
USB	Universal Serial Bus
UNB	Ultra Narrowband
VPN	Virtual Private Network
XSS	Cross-site Scripting

1. INTRODUCTION

The term internet of things (IoT) refers to a network of large number of low cost and low powered small scale devices connected with each other and equipped with sensors, software and a connection to the internet. IoT devices communicate, share, and exchange information with each other in a secure way while following the message queue telemetry transport (MQTT) and constrained application protocols (CoAP). Therefore, IoT can be used in nearly every sector, such as industry, agriculture and health care. IoT devices have very low data rate, hence the bandwidth required for data transmission between the devices and the IoT network server is minimal. Most of the present cellular networks offer high bandwidth and typically low range communications, not to mention the fact that they use limited and expensive spectrum, therefore they are not suitable as basis for an IoT network. IoT protocol addresses the aforementioned cellular networks limitations while offering an unlicensed spectrum for the IoT devices, which leads to a reduction in incurring communication costs.

Recently, IoT devices have become popular in many countries and widely accepted for many applications. In most of its applications, IoT provides smart solutions for everything around us. Consequently, in recent times, IoT has received a significant attention both in the academic research and in the industry. In addition, it is expected that IoT will create a billion dollar value at stake in the global market in the near future [1]. Nowadays, there are many available LPWAN technologies, and among them: long range (LoRa), Sigfox, IPv6 over low-power wireless personal area networks (6-LowPAN), Weightless, narrow-band IoT (NB-IoT), and DASH7, all are popular and widely used for commercial and research purposes. Aforementioned IoT technologies are different from each other in some respects, but all of them follow a nearly similar architecture. This thesis investigates IoT and its protocols while focusing mainly on the technological details of one of the IoT protocols called "Sigfox".

Sigfox is a French based IoT operator founded in 2009, which offers IoT solutions at a very low cost [2]. Moreover, Sigfox offers a very wide range signalling scheme by utilizing ultra narrow-band signals for communication with the IoT devices, which

results into low power consumption as well. In [13], authors suggest that Sigfox can provide IoT communication in a noisy environment with a very low signal strength. Sigfox is a full stack IoT operator, where user can buy a Sigfox device and may use it without buying any other third party device or subscription. The potential applications of Sigfox device include, but are not limited to smart agriculture, smart industry, smart manufacturing, smart vehicles and environment sensing. In this thesis, Sigfox network technology and its limitations are discussed in details.

In this thesis, Sigfox network performance was tested in both indoor and outdoor environment by using different parameters. Sigfox certified development prototype 'Thinxtra Xkit' was used in Tampere University (TAU) campus area in different environments and the data sent by this device to the network server was collected for the analysis purposes. The device was also kept in different locations in the underground of the campus building in order to measure the lowest possible signal needed to communicate with the Sigfox base station. This thesis utilizes the signal to noise ratio (SNR) and received signal strength strength indicator (RSSI) values to find out the Sigfox network quality of service (QoS) at different location of TAU Hervanta campus.

This thesis also focuses on the study to find out the integration policy of the Sigfox network with other networks, for example, cellular networks, satellite networks and Wireless local area networks. In addition, based on the Sigfox network technical details, few MATLAB simulations are also presented to predict the network behavior in varying environmental conditions. To summarize, the motivation of this thesis is to find out the answers to the following questions:

(i) What is the Sigfox network behavior in the reference area?

(ii) What are the technological challenges of Sigfox systems and how to solve them?

(iii) How to plan Sigfox radio network for better QoS?

(iv) How to simulate Sigfox systems in MATLAB?

(v) How to integrate Sigfox network with other wireless technologies?

2. BACKGROUND OF IOT

The term IoT encompasses devices that are connected to the internet. Those devices might include sensors, actuators, wearables, and smartphones. Thus, the core idea behind the IoT, practically, is to increase device efficiency, to save time, to decrease the vulnerability of the devices and to make it compatible with modern technology. At present, a lot of IoT protocols have been developed to meet the growing needs of the home and industrial applications.

In what follows, this chapter discusses briefly the commonly used and well known IoT technologies that has been considered for many practical applications. It then discusses IoT generic architecture, security directions, applications and financial aspects in the global economy. Finally, the importance of IoT in the Finnish economic sector is presented at the end of the chapter.

2.1 What is Internet of Things?

The concept of the IoT is quite big with lots of different kind of definitions. The term IoT is related to the "Ubiquitous Computing". The main idea is to make the physical objects around us smarter and connected to the internet to make our life easier. For example, Figure 2.1 shows a global positioning system (GPS) tracking watch which is helpful to track the location of a person. IoT can also help to solve social issues, for example, disappeared people in many countries. According to the missing people organization and geographics of missing people article, each year many Britons are disappearing from their family, relatives or workplace [14, 15]. The missing people organization claimed that in every ninety seconds someone is reported as disappeared [14]. The number is rising every year and no one knows where they got lost. However, this social problem can be easily solved using IoT watch shown in Figure 2.1. In addition, nano IoT chip can be developed which can be inserted into the human body. These chips with sensors will have the ability to be connected to the internet or global navigation satellite system (GNSS), therefore they can be tracked and monitored when the person is reported as disappeared [16]. As can be seen from above, anyone can be benefited after getting connected with

IoT services.

Figure 2.1 *A GPS tracking IoT watch.*

As discussed above, IoT can be defined as a system where the physical objects are connected to the sensors, actuators and internet to manage everything in an efficient way. The world first experienced the internet which enables us to share resources and now the IoT and in future it will be internet of everything (IoE). The Physical objects are now also connected with the internet and created the concept of the Internet of Things (IoT). So, the equation of IoT [17] can be written as follows:

Objects(Physical)+ Sensors, Actuators, Controller + Internet = IoT

Physical objects (for example, most of the electronic devices in the world) can be designed with micro-controller and sensors to sense the environment and take real time data. The data may be processed at the end devices and then the necessary information will be send to the cloud server through internet. The information then can be retrieved by the appropriate user. The whole process is taking place in an efficient manner in terms of required time, power and scalability.

Typically, In order to support the application process for a long time, IoT devices operate with low power and have long battery life. The number of devices in a network are typically very high and they are scalable. Cisco published information about the estimated number of connected devices in each year which can be seen from Figure 2.2 [1]:

2.1.1 IoT Generic Architecture

A complete IoT system includes different kinds of devices, sensors, micro-controllers, wireless base stations, back-end servers, and a callback system. Therefore develop-

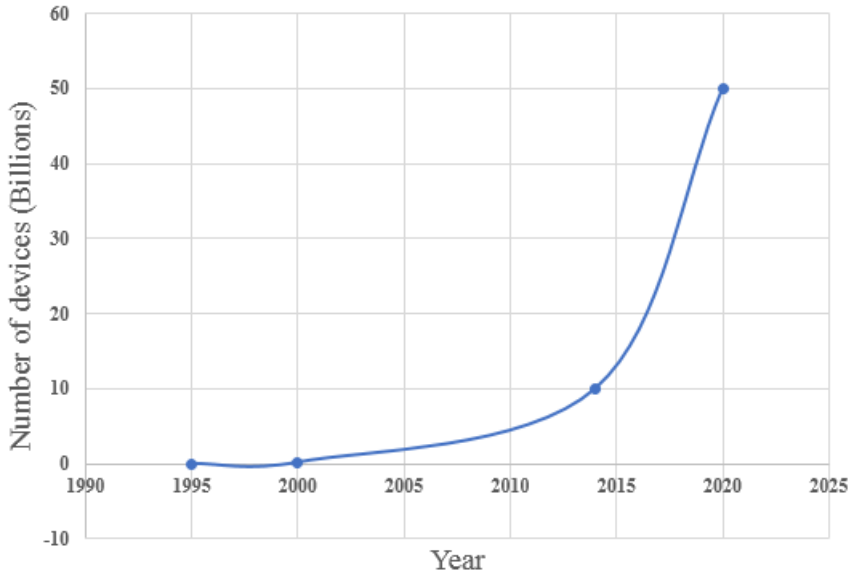


Figure 2.2 *Estimated number of devices connected to the internet.*

ing IoT architecture is a complex work. In order to manage all of these processes and systems, IoT needs a generic architecture with the consideration of the different application and business fields. Typically, an IoT architecture begins with a physical device which can sense the environment and ends up with an application or business ideas. The general structure of IoT can be divided into six layers as shown in Table 2.1 [9, 10].

Table 2.1 *IoT generic architecture.*

Business Layer
User Interface layer
Application Layer
Processing Layer
Transport Layer
Physical Layer

(1) **Physical layer:**
The physical layer is also known as the sensing layer or perception layer. This layer connects all physical devices which include sensors, controllers, radio frequency identification (RFID) readers to the transport layer. Most common and widely used sensors are temperature sensors, pressure sensors, location sensors (for example, GPS) and RFID tag readers. This layer is responsible

for collecting the required data from the real world. The device design challenges for this layer include modularization of the devices, self-configuration, intelligent operation and device longevity.

(2) **Transport layer:**
IoT devices send the generated data to the IoT back-end server with this layer. This layer can also be termed as the middleware layer. Secure transmission of data, device identification, and authorization are the main parts of this layer. In addition, in this layer, challenges for the IoT operator include ensuring available signal level at the device end, data transmission and reception at the base station.

(3) **Processing layer:**
The number of IoT devices in a network is so large that they can produce a large amount of data within a moment. Not only all of the data are necessary but also they can slow down the processing power of the back-end server. Furthermore, it is also unnecessary for clients. In order to filter out the unnecessary data, end devices and the cloud servers process them and sent to the back-end server. This system envisioned to the intelligent cloud-based data storage system which only saves useful data.

(4) **Application layer:**
Application layer defines the IoT applications in different applied fields. IoT is now envisioned to connect everyday devices in a single network. It includes smart home, smart logistic, e-health care system, smart environmental system and much more.

(5) **User Interface layer:**
This layer provides options to the user to view sensors results and take action accordingly. Cloud-based call back system provides an easy and secure interface to see the results. In addition, users can manage a thousand devices in a simple way. In some IoT protocol, it also allows the user to send data to the end devices individually or in a group. A practical and the most common example is to update the firmware of a thousand of devices nearly at the same time.

(6) **Business layer:**
IoT business layer addresses the current IoT applications and demands for specific IoT product in the market. It helps IoT operator to focus on appropriate IoT products. The biggest challenge for IoT is that there are too many possibilities and uncertainties in the business model thus make IoT as a challenging business model. It can also create practical graphs from the device sales report and usage which can help a manager to take accurate and realistic

decisions about IoT business strategies and future road maps.

2.1.2 IoT Protocols

There are different kinds of IoT protocols available in the market. Among them, some are proprietary based and some are open standard. For instance, Sigfox was one of the first IoT standard developed in 2009 [2]. Different IoT application has a different kind of flexibility. However, choosing the best IoT protocol needs some considerations based on the application of the IoT. Typical specification of IoT protocols given in Table 2.2. In the following table, the following abbreviations are utilized: bandwidth (BW), gaussian frequency shift keying (GFSK), 3rd generation partnership project (3GPP), mega hertz (MHz), differential phase shift keying (DBPSK), Orthogonal frequency-division multiplexing(OFDM), single carrier frequency division multiple access (SC-FDMA), offset quadrature phase-shift keying (O-QPSK), direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), gaussian minimum-shift keying (GMSK), advanced encryption standard (AES) and cipher-based message authentication code (CMAC).

Table 2.2 Comparison of different IoT standards [18–33].

Features	**Sigfox**	**Lora**	**NB-IoT**	**6Low - PAN**	**Blue-tooth**	**Zigbee**	**Weight-less-P**
Year Founded	2009	2012	2016	2015	2016	1998	2011
Standard	Own, Propri-etary	Own, Propri-etary	3GPP, Open	IEEE 802.15.4	IEEE 802.15.1	IEEE 802.15.4	Open
Frequency Bands [MHz]	868, 902, 928	863 - 870	700 - 900	868, 915, 2400	2400	2400	138, 433, 470, 780, 868, 915, 923
BW [kHz]	192	0.5 - 125	200	125, 500	500	2000	12.5
Data Rate [kbps]	0.1 or 0.6	0.3 - 50	DL: 200 UL: 144	250	3000	250	100
Range [km]	30 - 50	10 - 15	<35	0.01 - 0.1	0.3	<1	2
Modula-tion	DL: GFSK UL: DBPSK	SS Chirp	DL: OFDM UL: SC-FDMA	BPSK O-QPSK	GFSK	QPSK	GMSK, Offset-QPSK

Table 2.2 Comparison of different IoT standards [18–33].

Features	**Sigfox**	**Lora**	**NB-IoT**	**6LowPAN**	**Bluetooth**	**Zigbee**	**Weightless-P**
Spreading	-	-	No	DSSS	FHSS	DSSS	-
Scheduling	Uplink initiated	Uplink initiated	Network sheduled	-	Round robin	-	-
Latency [s]	2.08	1 - 2	<10	8	6	1	very low
Duplex Mode	Full	Full	Half	Full	Half/Full	Half/Full	Full
Network	LPWAN	LPWAN	LPWAN	WPAN	WPAN	WPAN	LPWAN
Network Topology	Star	Star	Star	Star, Mesh	P2P	STAR, Mesh	Star
TxPower [dBm]	UL: 14 DL :27	14 - 27	UE: 23	-	10	8	UE: 14
Power Consumtion [mA]	10 - 50	10	100	20	30	30	Very low
Security	AES	AES, CMAC	AES	AES	AES-CCM	AES - 128	AES-128/256
Mobility	Yes	Yes	No	-	Yes	Yes	Yes
Battery Life [Years]	>10	>10	>10	1 - 2	Few days	<1	Few years

Most importantly, in order to choose the best IoT protocol for a specific application, following consideration should be taken into account:

- Coverage
- Battery life
- QoS and Security
- Cost and Scalability
- Latency and Throughput
- Roaming and User Interface

2.2 IoT Security and Vulnerabilities

Nowadays, security is the biggest concern for internet-based services. In order to make the IoT more successful in the technology market, it needs to conform to a certain level of security standard. For instance, in a smart home, a smart smoke detector is installed with malicious software. Furthermore, the smoke detector is connected to the other home electronic devices. If a hacker can get unauthorized access to the smart smoke detector, then the attacker might have access to other devices too. Therefore every IoT device must need to meet a certain level of security standards. IoT device must have to conform to the following security requirements [34]:

- ✓ Access and device authentication control
- ✓ Users privacy
- ✓ Data security
- ✓ Resilience to the malicious attacks
- ✓ Connection security
- ✓ Failure tolerance

In order to gain unauthorized access to the IoT devices, the attacker or hacker can attack the network system from inside or outside the network. IoT devices are low-cost device, so IoT operators or users need to be more considerate on how they will implement security in the IoT devices. An attacker can launch different kinds of attacks on each IoT layer as depicted in Table 2.3.

Table 2.3 *IoT threats and vulnerabilities [6, 7].*

IoT layers	**Threats and Vulnerabilities**
Business layer	Baiting, quid-pro-quo, pretexting, tailgating.
User interface layer	Cross-site scripting (XSS) attack, command injection attacks, phishing attack, user deception attack, social engineering attack.
Application layer	malware attack, overwhelm, reprogram
Processing layer	Brute force attack, birthday attack, password attack, SQL injection attack.
Transport layer	Mac address flooding, black hole attack, sink hole attack, frame collisions, session hijacking, denial of service (DoS) attacks
Physical layer	Device tampering, Radio signal jamming, Spoofing, Signal interference.

In order to protect the IoT network from different kinds of malicious attack, IoT operators and users can take various steps. Few of the most important steps are listed below:

(a) Implement a secure authentication, authorization and access control system.

(b) Define a well secure firewall and intrusion prevention (IPS) system.

(c) Encrypt all of the data frames in the transmission path.

(d) Implement a secure storage system and identity management system.

(e) Update device firmware regularly.

2.3 IoT Applications

At the present time, IoT has become one of the most attractive future technology that can be used for different purposes. For instance, nowadays, nearly every embedded electronic devices need sensors and operators to operate those devices. Those sensors can IoT connectivity and can be managed more efficiently. IoT is now able to connect most of the devices in the industry and became a global network for devices and machines and provisioned machine to machine (M2M) and device to device (D2D) communication in an industry. Not only in the industrial cases but also in other cases, for example, IoT can be used to keep track of home electronic devices too. In order to save money and energy, electronic devices in every home, for example, refrigerator, light, fan, and air-cooler can be monitored with the help of IoT. In the same way, IoT is now playing a big role in the smart wearable device, smart city, smart grid, smart health care system, smart agriculture, and smart logistics service. For example, smart IoT temperature sensor can be used to track the temperature of the cargo container that helps the user to take real-time steps to keep the goods in good condition. To prioritize the use cases of IoT, it can be categorized to two groups as follows: massive IoT and critical IoT [35–37]. The most common use cases of those two cases tabularized in Table 2.4.

Table 2.4 *IoT category.*

Massive IoT	**Critical IoT**
Smart building	Traffic control
Smart agriculture	Remote health care
Logistics tracking	Smart grid
Smart agriculture	Smart industry
Smart metering	Remote manufacturing
Capillary networks	Remote surgery

Furthermore, IoT can be referred to as an intelligent network and its application also includes the necessity of intelligent processing of sensors or devices data. IoT application server filtered out unnecessary data and store only the valuable data.

As a result, IoT draws applications in many fields. Typical IoT application can be summarized as in Table 2.5.

Table 2.5 *IoT applications [7–10].*

Fields	**Typical applications**
Smart home	Home security, smart control of home electronic devices,smart energy saving, smart metering.
Smart agriculture	Environmental monitoring, green houses, air and soil condition tracking, smart agricultural product monitoring.
Smart health care	Hospital management, patient health monitoring, remote health care, medicine control.
Smart logistics	Product management, item tracking, product transport tracking, supply chain and inventory management.
Smart industry	Smart devices, production control, safety in the industry, smart energy saving, product location and life time tracking.

2.4 IoT in Global Economy

According to the global economy experts, IoT will create a new trillion dollar market within 2020 [18]. Cisco predicted in their white paper that IoT will have a strong impact on global economy in the near future [1]. It will help to reduce the cost for industrial production, city infrastructure management and agricultural production by its state-of-the-art technology. In the same way, IoT will enhance employee productivity, supply-chain and logistics efficiency and company asset management system. All of this will lead to a big economic impact in global economy.

According to Cisco, IoT will have $14.4 trillion value at stake for the next ten years [1]. Cisco predicted the situation based on the transformation of technology driven by IoT. In [38], authors claim that industrial IoT will have a major impact on the global economy as the M2M communication is increasing in a rapid number. In addition to this person to person (P2P) and person to machine (P2M) will also create the majority of the value at stake. Likewise, other analysts also put similar kind of prediction about IoT economics. For instance, Intel claims that the value will rise to $6.3 trillion by 2025. Most important industries that will drive the IoT economy by 2025 are listed below with their predicted economic value [1, 39, 40] :

- ✓ Manufacturing [$3.7 trillions]
- ✓ Cities [$1.6 trillions]
- ✓ Retail Environment [$1.1 trillions]
- ✓ Human [$1.5 trillions]

- ✓ Vehicles [$0.74 trillions]
- ✓ Finance and Insurance [$0.5 trillions]
- ✓ Health-care [$0.4 trillions]
- ✓ Offices [$0.15 trillions]

Statistics from different accredited sources claimed that the IoT will produce most of the economic value to the developed countries [1]. The total IoT economic distribution shown in Figure 2.3.

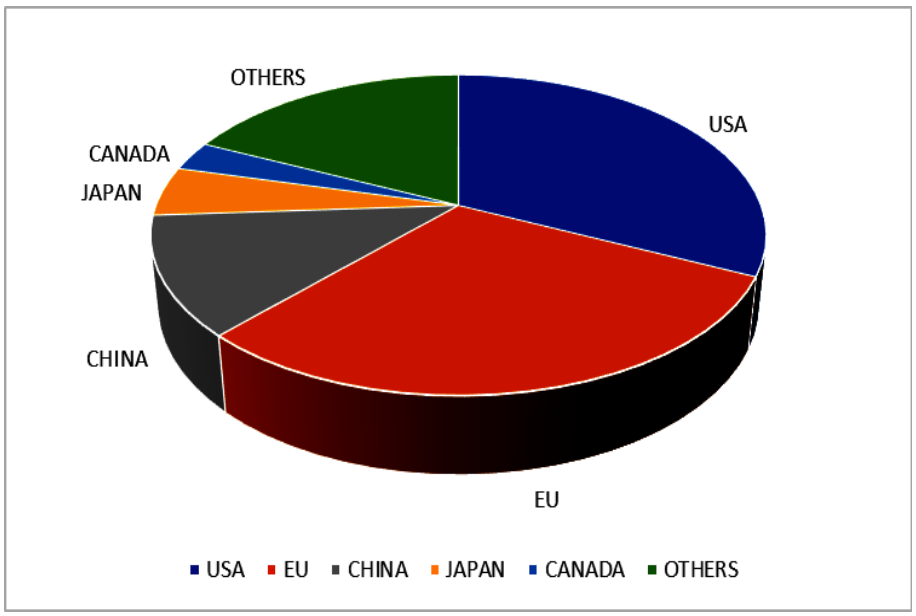


Figure 2.3 *Distribution of IoT economics around the world [1].*

A survey conducted by KRC research group predicted that the number of connected devices in smart appliances will be more than 35% within the next five years [41]. Summary of their prediction is given in Figure 2.4.

At present, a lot of IoT projects are implemented in different countries. Examples of few IoT projects that has been implemented in different countries given below [42]:

(i) Predictive control of vineyards in **Pago Ayles winery, Spain**.

(ii) Water quality control in the Volga river, **Russia** by using drones and sensors.

(iii) Smart car parking solution in Montepellier, **France**.

(iv) Air quality control for healthy lifestyle in **Lebanon**.

(v) Bins and dumpsters monitoring with ultrasonic sensor to reduce waste collection by 30% in **IL, USA**.

(vi) Smart lighting system to reduce electricity usage by 80% in **United Kingdom**.

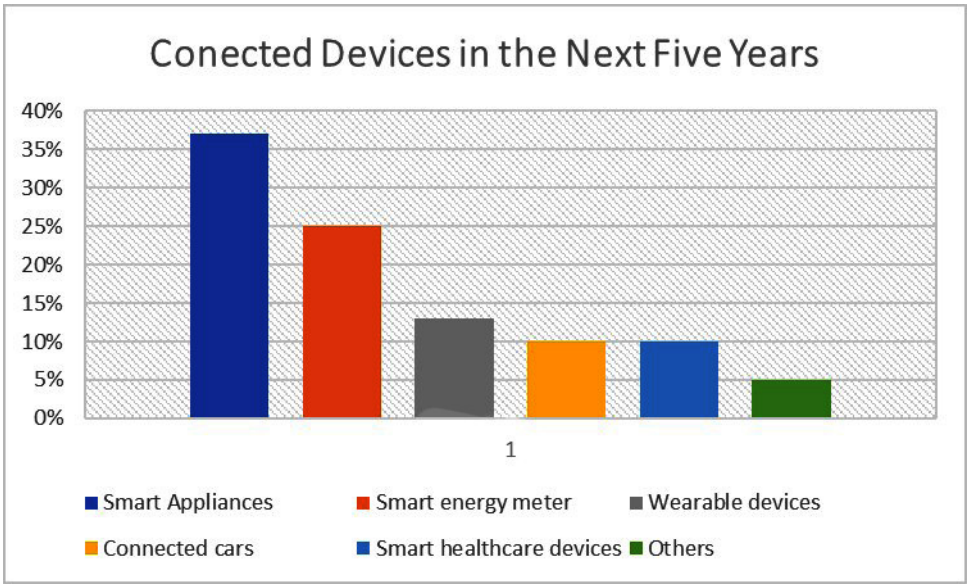


Figure 2.4 *Number of connected devices in the next five years.*

2.5 IoT in Finland

Finland is a Nordic country and its economy is mainly based on science and technology. Therefore IoT will have a strong impact on its economy. As the population of Finland is very small in comparison with its industrial needs, therefore IoT can play a major role to overcome this problem [43]. Finland has already deployed few IoT networks such as Sigfox, LoRaWAN, NB-IoT. A great number of applications are already in the market for commercial purposes. For instance, Telia and Posti developed the world first smart post system using NB-IoT. A smartpost provide information in real time, for example, if a mail is dropped in the mailbox, if it is full or empty and if it has been opened. According to the chief process officer of Posti, Smartpost can save up to 13 million euros per year [44]. It is worth mentioning that a lot of cost saving applications are now under development with the help of several IoT research program.

Finland has already started Internet of Things research program in 2012. The main focus of this program is to provide a better IoT management system to support IoT services and applications. The estimated cost for this program is about 50 million euros [45]. Finnish industrial internet forum (FIIF) is arranging events regularly on IoT to support and boost the IoT market. It also provide money for different organizations or institutes to make new IoT products and services. IoT companies which are leading the Finland's IoT market are Ericsson, Elektrobit, Wapice, Corenet, F-Secure, Intel, TeliaSonera, Siemens and Nokia.

3. SIGFOX BASED IOT

Sigfox technology was founded by Ludovic Le Moan and Christophe Fourtet in 2009 [2]. The company's headquarters is located in Labège near Toulouse which is well known as France's "IoT Valley". Sigfox is considered one of the most representative LPWAN systems among other LPWAN schemes [46]. It provides the connectivity between device and the cloud in a cost efficient manner. In [47], authors argued that Sigfox is the most cheap IoT service provider among other IoT operators. Sigfox technology is able to connect billions of devices in its networks. As its approach is to connect the devices to its central cloud infrastructure, there is no need for roaming services for the end user's devices. Sigfox devices operate in low energy thus it can be consider it as an eco-friendly technology.
Each Sigfox base station can handle up to three million devices [48]. The management of these devices is very easy and the number of connected devices can increase by adding more base stations. Sigfox system has very good indoor and outdoor performance and network failure rate is only 12% [49]. Sigfox cell can provide coverage about 30 - 50 km in rural areas and 3 - 10 km for urban areas. In case of free space and line of sight (LOS) connection, signal can travel over 1000 km [50–52].
Sigfox key achievement given in Table 3.1 (updated: March 29, 2019).

Table 3.1 *Sigfox key achievements [2].*

Peoples Connected	1 billion
Countries Covered	60
Areas Covered	5 million km^2

Technically, Sigfox signal is highly resistive with respect to noise signal and Figure 3.1 shows that only 8 dB SNR is required to recover the signal. Sigfox technical specifications are given in Table 3.2.

3.1 Sigfox Protocol

Sigfox protocol is mainly based on low throughput network (LTN) protocol. The message is 12 bytes long and it includes a sequence number for security purposes.

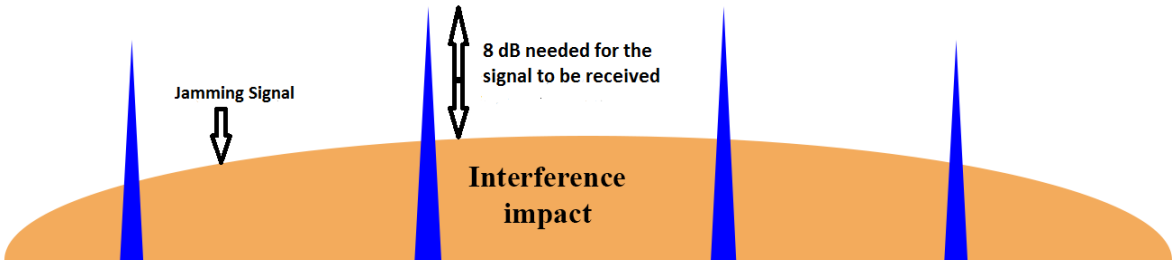


Figure 3.1 *Interference signal impact on Sigfox signal.*

Table 3.2 *Sigfox technical specifications.*

Frequency Bands (MHz)	Europe: 868, Others: 902 - 928	**Tx Output Power**	Europe: 14 dB, USA: 22 dB
Bandwidth	192 kHz	**Data Rate**	100 bps or 600 bps
Modulation	Uplink: DBPSK Downlink: GFSK	**Payload**	Uplink :12 bytes Downlink: 8 bytes
Power consumption	Active: 10 - 50 mA, Idle: 6 nA	**Number of Messages**	Per Hour: 6, Per Day: 140
Security	AES	**Roaming required**	No

Sigfox devices send 140 messages (maximum) per day and the rest of the time the devices stay in the sleeping mode. It helps to operate the device at low power and provides additional security for the system. The end device can only create communication with the base station and transmits each message three times in three different frequency. Sigfox network protocol uses both time and frequency diversity. Sigfox base station transmits the signal by using a random frequency and time division multiple access (RFTDMA). Sigfox protocol structure given in Table 3.3.

Table 3.3 *Sigfox protocol stack [11, 12].*

Application Layer
Transport Layer
MAC (Medium Access Control) Layer
Physical Layer

Physical layer handles the modulation and demodulation of the Sigfox signal. In a Sigfox based communication system, there is no need for signalling messages.

Sigfox uses ultra narrowband (UNB) modulation to send and receive messages. To be specific, Sigfox sends three messages using multiple channels and the packet duration is 2 ms [53]. The physical layer also handles the framing mechanism process during transmission and reception. Sigfox messages are 0 to 12 bytes long. Each Sigfox message frame includes preamble bits, frame synchronization bits, device identifier bits, payload bits, authentication codes and also the frame check sequence (FCS) bits. The generic structure of uplink and downlink frames are given in Table 3.4. In the first place, a preamble is used for synchronization purposes and certain bit words are used by the receiver to unscramble the bits. This technique removes the need for additional flags and in addition to this, it leads to the reduction of the packet size [47, 53–56]. Sigfox frames are not encrypted by the Sigfox protocol itself rather the encryption is done by the client themselves at the application layer. Application layer also provides other necessary functionality required by the clients and the most important of them are messaging, web-services and the call back function.

Table 3.4 *Sigfox frame structure.*

Uplink Frame	Preamble (32 bits)	Frame Sync (16 bits)	Device ID (32 bits)	Payload (0 - 96 bits)	Message Authentication Code (16 - 40bits)	FCS (16 bits)
Down link Frame	Preamble (32 bits)	Frame Sync (13bits)	ECC (32bits)	Payload (0-64 bits)	Message Auth Code (16bits)	FCS (8 bits)

3.2 Modulation and Multiple Access Technique

Sigfox uses DBPSK in the uplink and GFSK in the downlink. In DBPSK modulation, the modulated signal changes its phase shift, when there is a data bit 1, thus provide high spectral efficiency. Due to the noisy communication channel, the transmitted signal phase shift changes at a very low rate. Therefore, DBPSK is able to provide a reliable way of communication, thus making it a more efficient choice than other modulation schemes. DBPSK signal modulation scheme shown in Figure 3.2. Practically, there is no need to send data regularly via the downlink as there is no handshake method available in this technology. But in case of device firmware update, a user may send data via downlink.

Sigfox, as well as other ultra narrowband (UNB) technology, uses random frequency and time division multiple access (RFTDMA), where nodes (end devices)

access to the wireless medium randomly both in frequency and time domain without having any containment method. It is an ALOHA-based protocol, which operates in a certain range of random frequency and time without having any knowledge of the channel state. Sigfox chosen this multiple access technology because it offers following benefits [57, 58]:

(i) Frequency diversity: Sigfox devices broadcast its one message in three different frequency.

(ii) Time diversity: Sigfox devices broadcast its one message in three different time.

(iii) Spatial diversity: Each Sigfox message received by more than one base station at a time.

(iv) Noise robustness and spectrum interference avoidance.

(v) No need for time synchronization and beacon packets.

(vi) Highly energy efficient and energy consumption is nearly zero when there is no transmission.

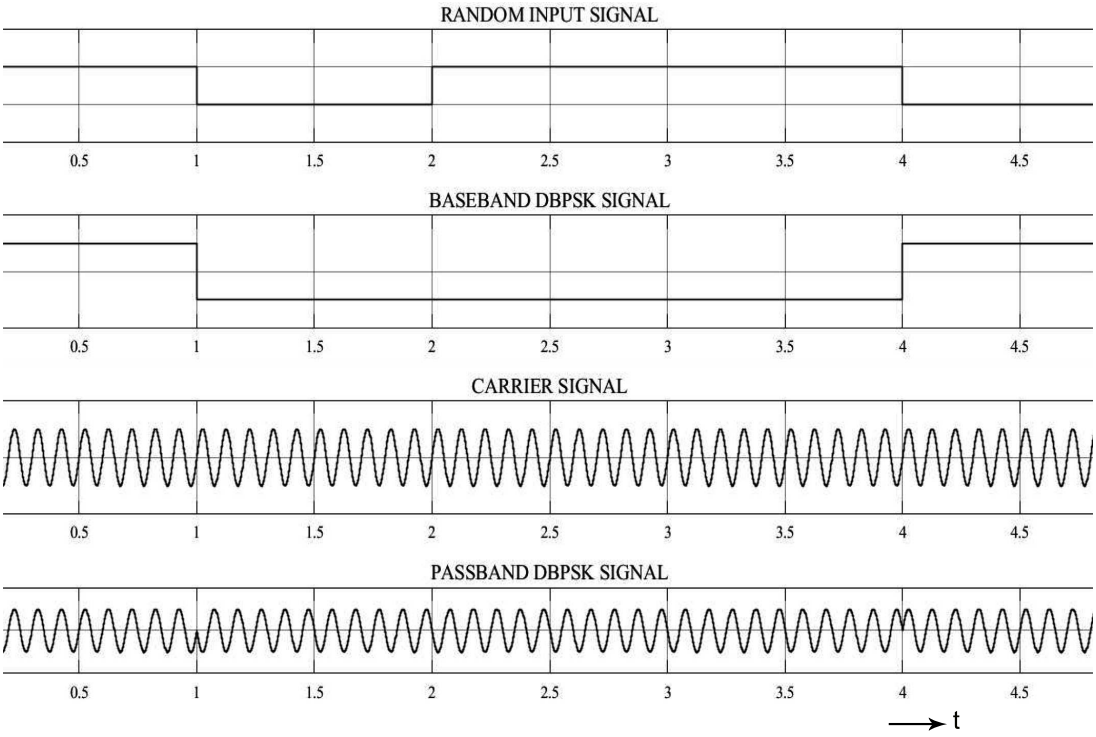


Figure 3.2 *DBPSK modulation.*

3.3 Sigfox Platforms

In order to use the Sigfox network, a user needs to have Sigfox network compatible device known as the Sigfox IoT device. Sigfox IoT devices are normally a

lightweight device equipped with a battery and pre-installed software and drive by a Sigfox compatible module. However, Sigfox operates in different frequency bands in different country. Hence, different regions of the world may need different kind of Sigfox device and module. A typical example of Sigfox module and device shown on Figure 3.3. At present, Sigfox divided the whole world into six different region. Each region has unique radio configurations and unique or shared modules and devices. Sigfox regions specifications and few of the available Sigfox modules and devices in different regions itemized below:

- **Zone:** RC1
  - (i) **Countries:** Europe, Oman, Iran, South Africa, Tunisia, UAE.
  - (ii) **Modules:** WSSFM10R1, RC1682-SIG, WSSFM20R1, UPLYNX Sigfox verified RCZ1 module, SIPY 14 dB, WSG303S, WSG304S.
  - (iii) **Devices:** Water Health Smart Device, NashTag™Mini, NashTag™Poucet, Main-IoT leak guard, All Sense Smart Industry, All Sense Smart city, Water Pressure Smart Device, All Sense Sensor Controller, Nexxtender Mobile, Web things AMR, Smart Connect, Water Pulse Smart Device etc.
  - (iv) **Other Features:** Operating Frequency: 868 - 878.6 MHz, EIRP: 16 dBm, Frame Transmission Time: 2 s.
- **Zone:** RC2
  - (i) **Countries:** USA, Mexico, Brazil.
  - (ii) **Modules:** SIPY 22 dB, S01 (SIPY) OEM MODULE 22 dBm.
  - (iii) **Devices:** Main-IoT leak guard.
  - (iv) **Other Features:** Operating Frequency: 902.1375 - 904.6625 MHz, EIRP: 24 dBm, Frame Transmission Time: 350 ms.
- **Zone:** RC3
  - (i) **Country:** Japan.
  - (ii) **Modules:** S-WING Sigfox extension board for BOSCH XDK, WF 923, SN10-13, SN10-23, WF931.
  - (iii) **Devices:** OTO Hunter, Door Opening Sensor, Digital Nano Strain Gauge, Service button RC3, Esense Pro CO2 etc.
  - (iv) **Other Features:** Frequency: 922.3 - 923.5 MHz, EIRP: 16 dBm, Frame Transmission Time: 2 s, Listen before talk (LBT).
- **Zone:** RC4
  - (i) **Country:** Latin America, Asia Pacific.

(a) A Sigfox module. (b) A Sigfox device.

Figure 3.3 *Example of a Sigfox module and a Sigfox device [2].*

(ii) **Modules:** WSSFM60R4, WSG300S .

(iii) **Devices:** Connected airwits, Connected pressguard, OneSense Agriculture UC16 Irrigation and Soil Salinity Monitoring RC4.

(iv) **Other Features:** Operating Frequency: 920.1375 - 922.6625 MHz, EIRP: 24 dBm, Frame Transmission Time: 350 ms, Frequency hopping.

- **Zone:** RC5
  - (i) **Country:** South Korea.
  - (ii) **Modules:** WSG303S RC1/RC3C/RC5.
  - (iii) **Devices:** Base for smoke alarm, Marine smart hub RC5.
  - (iv) **Other Features:** Operating Frequency: 920.8 - 923.4 MHz, EIRP: 14 dBm, LBT.
- **Zone:** RC6
  - (i) **Country:** India.
  - (ii) **Modules:** None.
  - (iii) **Devices:** Base for smoke alarm GS511 - RC6.
  - (iv) **Other Features:** Operating Frequency: 865 - 867 MHz, EIRP: 16 dBm.

3.4 Sigfox Network Dimensioning and Planning

Sigfox is a low power wide area radio network provider for IoT systems. In Sigfox based radio network, usually multiple radio base stations are deployed in the coverage area to provide coverage and connectivity to the IoT devices. Therefore the QoS of the network depends on the radio network planning and mostly on the number of deployed base stations. So, network dimensioning and planning is a very important task to set up a wireless network connection between the base

transceiver station (BTS) and the end devices. In addition, it reduces the cost for implementation of the network and also removes additional complexity. A proposed initial Sigfox network planning procedure given in Figure 3.4.

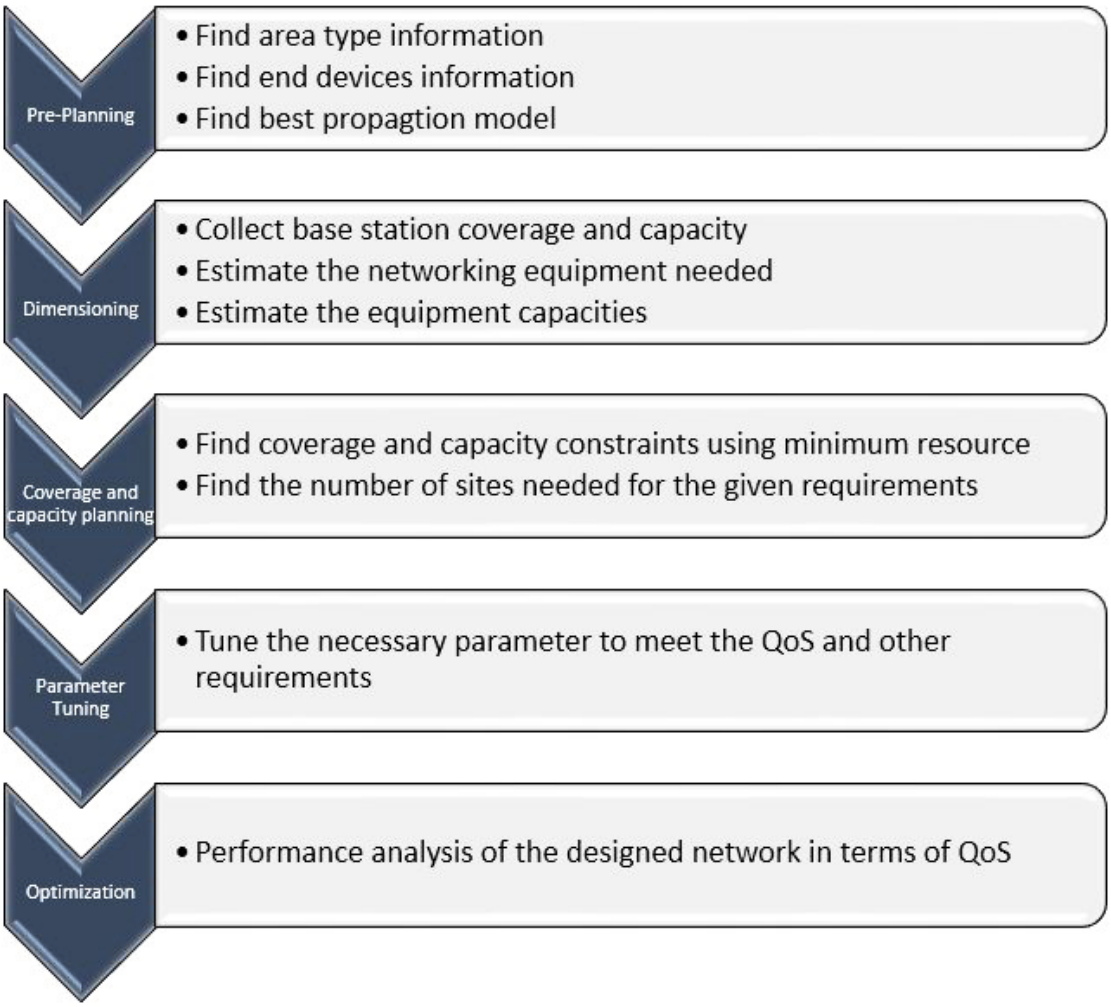


Figure 3.4 *Sigfox network planning procedures.*

3.4.1 Sigfox Network Dimensioning

Since Sigfox network only supports the packet switched data, so a packet switched traffic model is needed for the network operation. The traffic model should be based on a large number of devices because a cell area which is located in a big city could have millions of devices and those devices broadcast three copy of each message. According to the Sigfox technical specification, each message is only 12 bytes long and one Sigfox device send maximum 144 messages per day in a random time and random frequency. In addition, the attempts of sending messages to the BTS can

be successful or unsuccessful. In this kind of scenario, Bernoulli trial coupled with a binomial distribution can be used to model the uplink success rate [49]. Following consideration should be taken into account for the Sigfox device traffic model (uplink traffic model) [13]:

(i) Categorize the information sent to the network based on importance and size.

(ii) Define the device active and hibernate time in an efficient manner to save the energy.

(iii) Define the efficient payload size to maximize the use of energy. Allowed payload sizes in Sigfox protocol are 1, 2, 8, 12 bytes.

(iv) Compress the payload data using the compression algorithm.

(v) Plan a backup method for a lost message in the transmission path.

(vi) Avoid sending the identical message and for minor change in the repeated message use notification with delta information.

(vii) Place the end device in a most suitable place from where it can easily get connected to the network.

In order to simulate the desired cell area, a simulation software can be used, for example, in this thesis MATLAB was used to do all of the simulations. First of all, choose the lowest possible values of the required parameters and then simulate multiple times by changing the values to the middle values or average values and finally for the highest possible values. In order to estimate the coverage and capacity, revise the primary assumptions, and simulate the program for multiple times. A detail simulation procedures and results using MATLAB are discussed on section 4.3.

3.4.2 Sigfox Network Planning

The aim of radio network planning is to predict and estimate the Sigfox radio network coverage and design the network efficiently based on the analysis from the network dimensioning.

(a) Make an initial plan to find the location of the cell site.

(b) Base station antenna parameters play the most important role for the best possible coverage. In this case, the antenna type, azimuth angle, tilt angle, altitude, feeder line type selection needs to be considered. Sigfox base stations are provided by the Sigfox and use Sigfox base station transceiver (SBS-T) Version 2 and 3. Both of them supports only omnidirectional antenna with gain less than 8 dBi [59] and supports bi-directional wireless communication. The Sigfox base station also equipped with a modem, a low noise amplifier (LNA) and a cavity filter to achieve high sensitivity [60].

(c) Define the required gateway parameters and set the DL power to the 27 dBm.

(d) Predict the coverage area and modify required parameter to meet the requirements.

(e) Find and use propagation models which is best suited to the given area.

(f) Simulate the output data to find network performance.

3.4.3 Sigfox Network Evaluation

In a Sigfox network, QoS found much more comfortable among the LPWAN networks. In an experiment conducted in Ireland shows that Sigfox end devices able to sent messages to the base station over a 25 km point to point distance [51]. A Sigfox device can successfully send a message to the Sigfox base station with RSSI as low as -145 dB, which distinguished itself from other LPWAN networks. The performance metric of Sigfox networks is path loss, collisions among the data packets, SNR, RSSI and packet error rate of a large number of devices at Sigfox specified frequency. Among them, path loss can be calculated from Equation 3.1.

$$PL = |RSSI| + SNR + P_{\mathrm{TX}} + G_{\mathrm{RX}} + 10n\log_{10}(d/d_o) \tag{3.1}$$

where,

PL	Path loss,
P_{TX}	Effective isotropic radiated Power,
G_{RX}	Receiver's antenna gain,
n	Path loss exponent,
d	Distance between the node and the base Station,
d_o	Reference distance.

Let us consider a case where a Sigfox device is 5 km away from the base station. In addition, the device is receiving the signal at SNR = 20 dB, RSSI = -122 dBm and path loss exponent is 2. If the device under test is in free space then, the simulation scenario of theoretical free space path loss and path loss at the described case can be shown in Figure 3.5.

The link budget is the most important tool for the system-level design of LPWANs systems, which is prepared by calculating all the gains and losses in the transmission paths and normally expressed in dB. A link budget analysis among LPWANs in Table 3.5 shows that Sigfox also provides a very good link budget among the LPWANs [61].

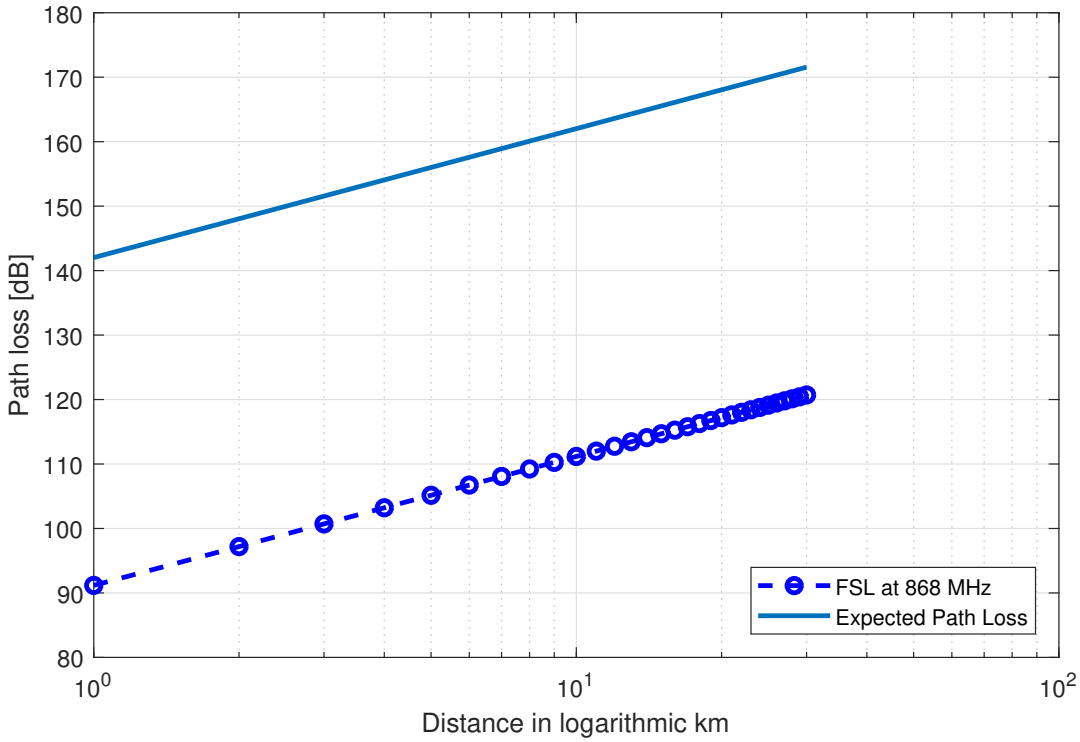


Figure 3.5 *Comparisons of path losses [3, 4].*

Table 3.5 *LPWANs link budget.*

LPWANs	Link budget (dB)
Sigfox	**156**
LORA	117-156
NB-IoT	164
Weightless	152

3.5 Sigfox Backend, Callbacks and API

As discussed earlier, Sigfox emerged as not only an IoT technology operator but also as a complete IoT service solution center. Sigfox devices are made by the Sigfox certified companies and also distributed by Sigfox authorized companies. In the first place, Sigfox devices sent its messages to the Sigfox network server which is called Sigfox backend [1]. In the backend, a user needs to authenticate the Sigfox device and the user to get the full IoT service.

Each Sigfox IoT device is equipped with a unique SigfoxID and a porting authorization code (PAC) identifier, both of them are hexadecimal numbers. After registering in the backend server, a user need to authenticate the device with SigfoxID and PAC identifier. The Sigfox backend provides a web-based graphical user interface (GUI)

1. https://backend.sigfox.com

for device management and configuration. Furthermore, it is a bridge between end devices and the user's where operational support system (OSS) defines the functionality of the Sigfox backend.

After successful authentication in the Sigfox backend, a user can view the menu tab with welcome message and the current Sigfox cloud version release notes as shown in Figure 3.6. After that Sigfox devices need to register to the Sigfox backend

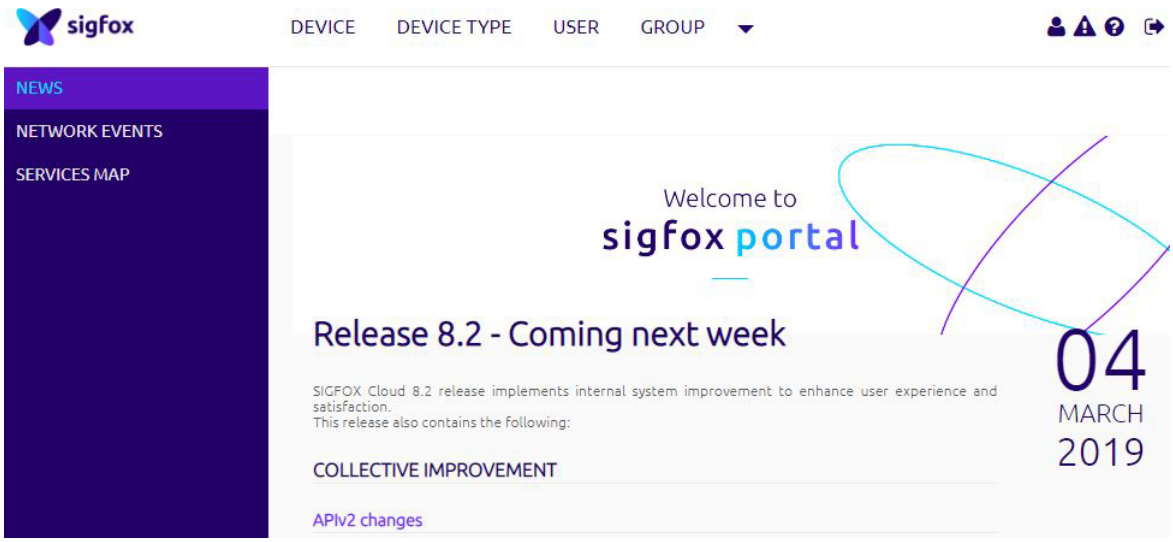


Figure 3.6 *Sigfox backend GUI (available at: https://backend.sigfox.com, accessed on: 29th March, 2019).*

services, which can be done by using SigfoxID and PAC identifier. At this point, a user can group their devices according to the type and functionality of the individual Sigfox device. Furthermore, Sigfox backend also provides the following functionality.

(i) New user creation: Sigfox backend allows the user to create new users to access the device information based on their rights to read and write predefined during role creation policy as illustrated in Figure 3.7. It is obvious that user roles can be fine-tuned at any time and composed of different custom roles in different groups.

(ii) Device: All of the added devices can be seen from Device tab separated by the unique SigfoxID and it also shows the deleted device, present status of the device including average RSSI, SNR and last seen of the device in the online. In addition, by clicking on the individual device ID it is also possible to see the callback status, statistics for message transfer, RSSI, SNR, and events or notifications related to that particular device.

(iii) Device type: Device type also provides other important functionalities like the callbacks creation, statistics for messages, devices status, the location of the devices and events configuration.

(iv) Service map: Sigfox backend also shows the network service map, where the device is located. For instance, Figure 3.8 shows the Sigfox network status in Finland, where the red area represents the regions with the availability of three base stations for receiving signals from the Sigfox device and green area for the two base station and blue for the one base station respectively.

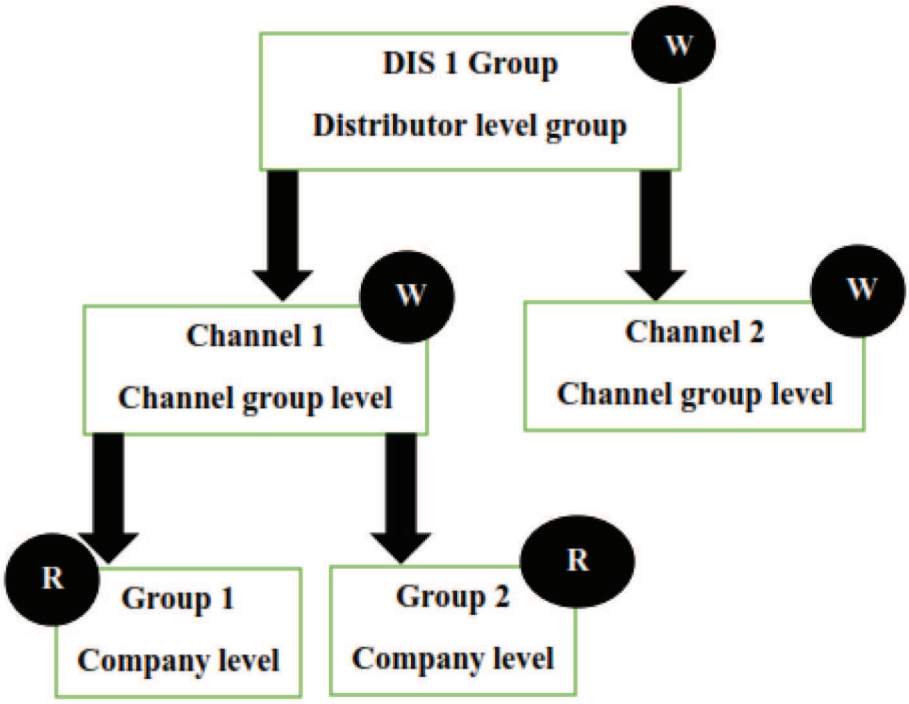


Figure 3.7 *Sigfox custom roles on different groups.*

3.5.1 Sigfox API

In order to control and manage IoT devices on the Sigfox network, user's can integrate their own platform or server with the Sigfox cloud platform. Sigfox backend has build in application programming interface (API) which works as a bridge between those two platforms and implements the data integration. The API's are based on HTTPS protocol, following the REST principles (PUT, GET, DELETE or POST) and the payload format is JSON. Even though it does not provide visualization facility of the received data but the user can configure their API's to send notifications or data to their external devices or their connected servers. In order to use API, a user need the API access right which can be granted from the group creation functionality. Sigfox API can return different response code for different events which are tabulated in Table 3.6. If a large amount of data retrieved from Sigfox server via API request, the reply will be sliced and this is called paging. In [62], Sigfox recommended to use API's in the recurring task that have rare occurrence and not to use to pool event based data.

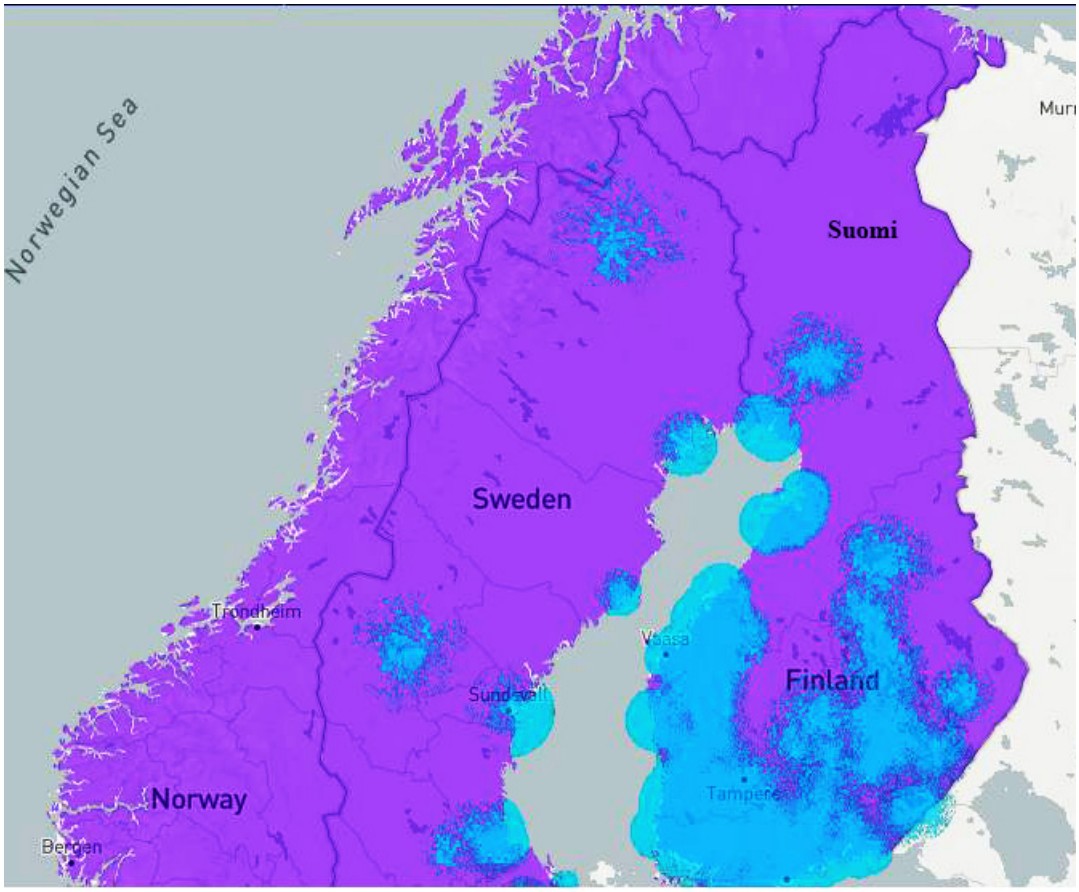


Figure 3.8 *Sigfox network service map in the reference area [2]. Accessed on: March, 2019.*

Table 3.6 *Sigfox API response codes.*

Code	Definition
200	Successful
204	No content
400	Illegal argument
401	Unauthorized
403	Forbidden
404	Not found
409	Conflict
500	Internal server error

3.5.2 Sigfox Callback System

Sigfox IoT devices are small in size and in most of the commercial cases, a lot of devices are needed to fulfill the company's requirement. In those cases, it is hard to check the incoming messages or device status for every device. In addition when the number is very big then it is very hard to manage those devices. For instance, if a user needs to send a firmware update to every device then it is hard to up-

date devices one after one. In those cases, some well-reputed companies provide easily manageable IoT devices in a secure way. They also provide options for view data in a more efficient way. Some well-known cloud platform service providers are Amazon Web Services (AWS) IoT, AWS Kinesis, Microsoft Azure™ IoT Hub, Microsoft Azure™ Event Hub, IBM Watson™ IoT Platform, Ubidots and Thinger.io. A typical procedure performed in a callback system shown in Figure 3.9. In order to successfully retrieve data from the Sigfox server to the Sigfox's own platform or another cloud platform, a user need to make a callbacks API in the Sigfox server along with an HTTP endpoint, where the API must be in a JSON format as an example illustrated below:

```
{
"device" : "{device}",
"data" : "{data}",
"time" : {time},
"snr" : {snr},
"rssi" : {rssi},
"station": "{station}",
"latitude": {lat},
"longitude": {lng},
"temperature" : {customData#temp}
}
```

Figure 3.9 *Sigfox callback schematics.*

(i) Callback via E-mail: In the first place, if one or few Sigfox IoT device needs for a particular project then it can be easily managed by the callback system via email services. The messages of the IoT devices sent directly to the user's e-mail address but no downlink message or information can be sent by this service. A typical example of email notifications shown in Figure 3.10.

(ii) Callback via Thinger.io: Sigfox supports interaction with many cloud platforms, and one of them is Thinger.io [2]. At first, a user need to create a data

2. https://thinger.io

bucket in the Thinger.io website, which will be used as a storage for the incoming messages from the Sigfox server. Data bucket can be created for one device or one data bucket for the multiple devices, based on the user requirement. Then the user needs to create an access token that will allow the Sigfox server to communicate with Thinger.io server in a secure way. Finally, a user needs to create a custom callback in the Sigfox backend server [3] to push the messages to the Thinger.io cloud platform. In the Sigfox backend, the callback type should be "Data, Uplink", Channel should be "URL", URL pattern should be "$https://api.thinger.io/v1/users/userId/buckets/data$", HTTP method should be "POST" and header should be "Authorization with the Access Token" [4]. In this thesis, ThinXtra Xkit device was used to take the necessary measurement to test the performance of the Sigfox network in the reference area. During the measurement, the Xkit device was connected to the Sigfox server and then the Thingr.io platform was used as a custom callback server. The dashboard of the callback server interface shows the values retrieved from the Sigfox server. For instance, Figure 3.11 and Figure 3.12 are showing RSSI and SNR values obtained from the measurements.

3.6 Integration with Other Networks

Sigfox is most likely the only one IoT operator which has a central database for all of the IoT devices operating on its network. In addition, Sigfox deploys only one operator in each country to provide Sigfox network coverage. Sigfox network coverage can also be extended through the easy integration with cellular network or satellite network or with local asymmetric digital subscriber line (ADSL) technology as shown in Figure 3.13. This might be necessary to make sure that Sigfox device can be used in most of the places of the world.

In order to connect the Sigfox devices from any places of the world, a satellite-based Sigfox network integration can be an excellent choice. In this method, a Sigfox base station will be connected with a specific satellite and the satellite will also be connected with the satellite receiver located at Sigfox cloud server. This will also help to provide coverage for a city on an island or in the desert. In contrary, the latency will be very high as well as the cost. In the same way, a Sigfox base station can also be connected to an ADSL router which is connected to the internet service provider (ISP) via the multi-service access node (MSAN). ISP then can forward the Sigfox data packet to the Sigfox cloud. The biggest issue in this type of integration

3. https://backend.sigfox.com
4. http://docs.thinger.io/sigfox

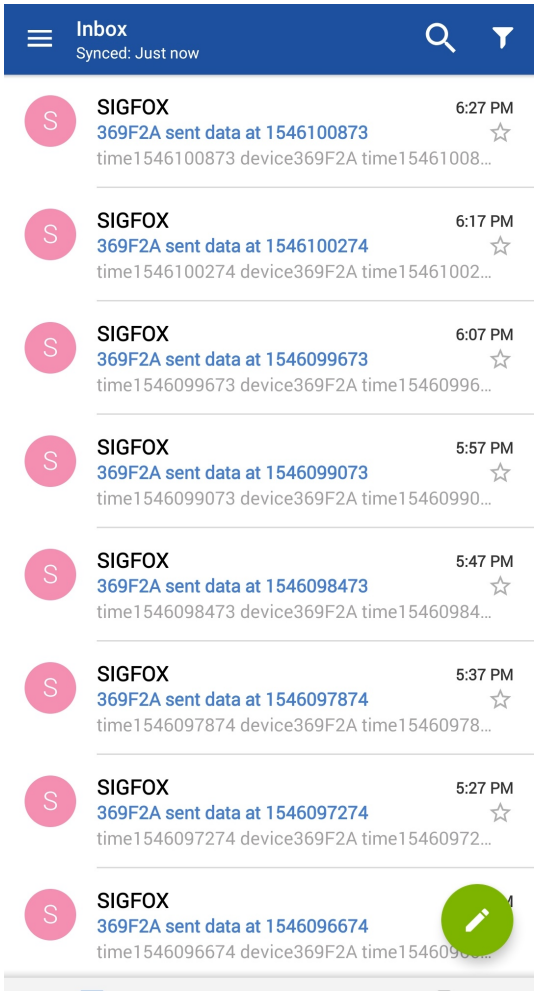


Figure 3.10 *Sigfox callback using E-mail services.*

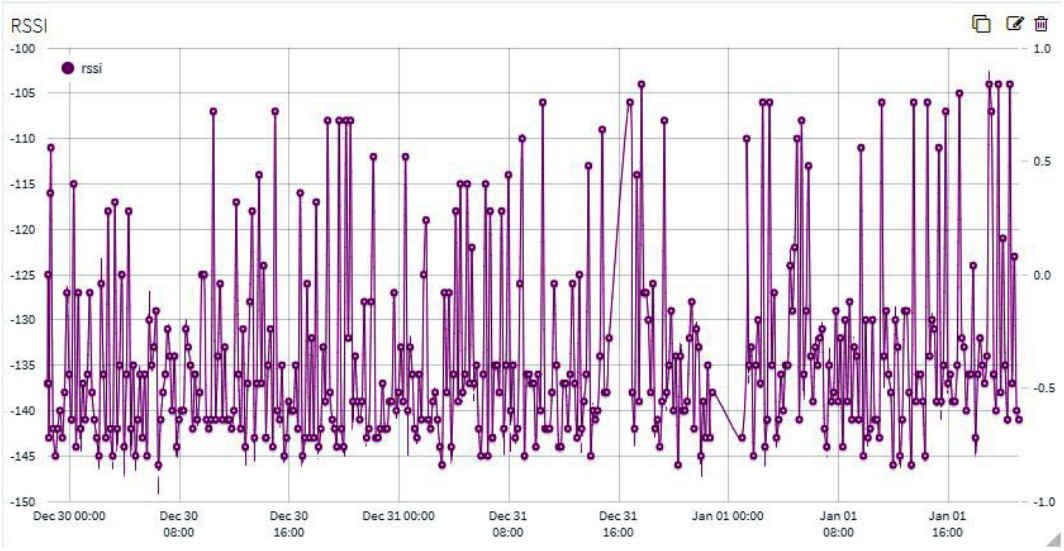


Figure 3.11 *Xkit RSSI graph in Thringer.io platform.*

could be the security of the Sigfox data packets as the packets will travel through

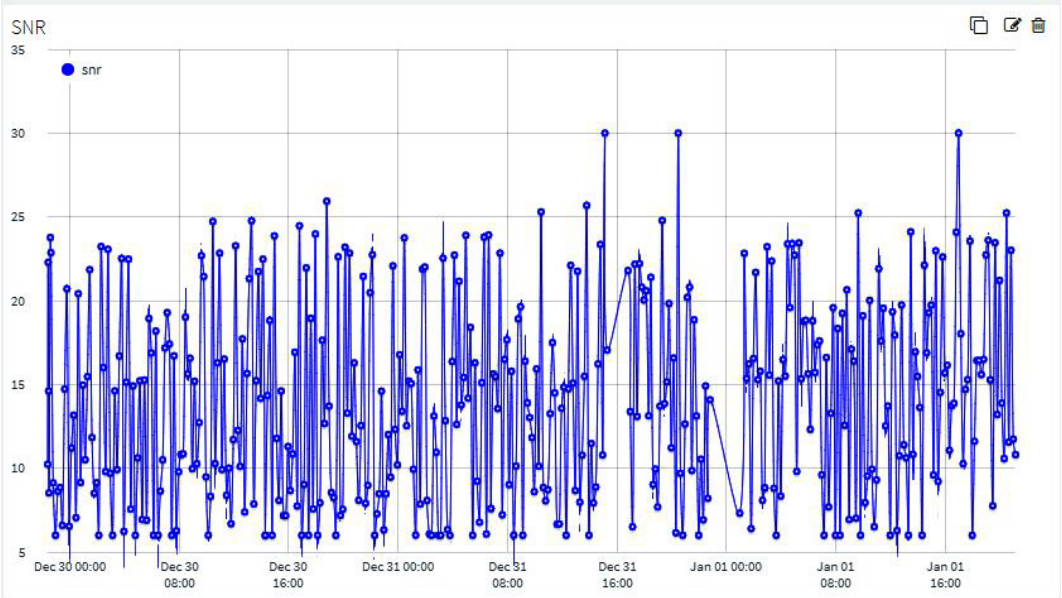


Figure 3.12 *Xkit SNR graph in Thringer.io platform.*

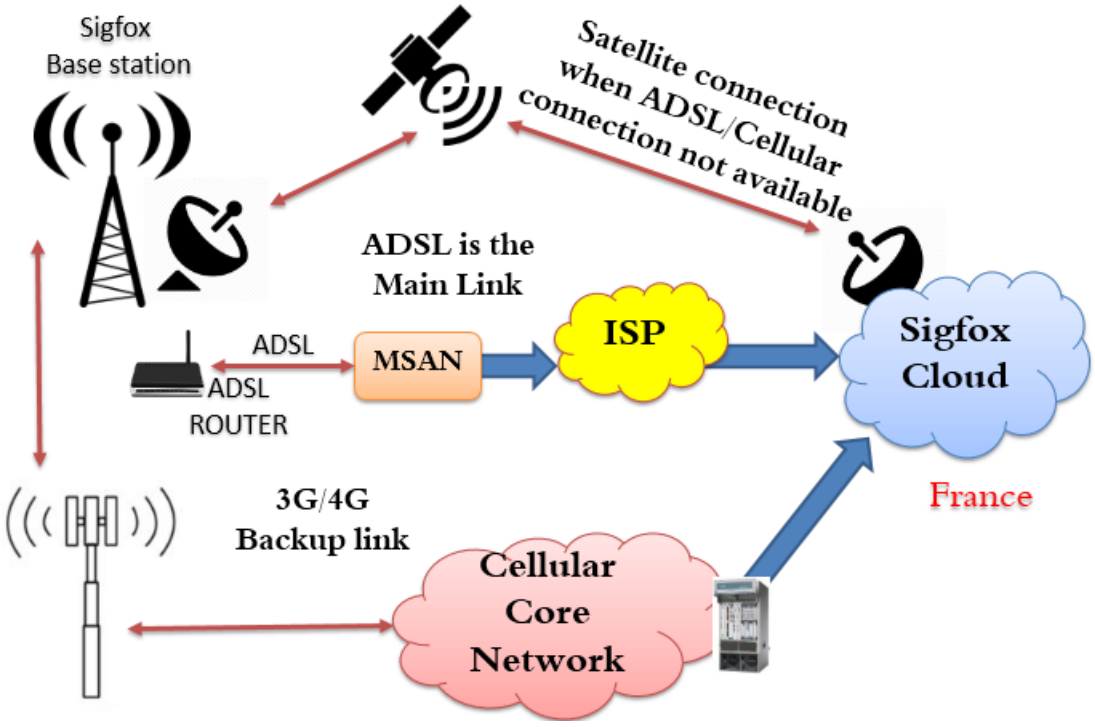


Figure 3.13 *Proposed way of Sigfox network integration.*

the third party vulnerable networks. The third and one of the better way could be the integration with the cellular network, where the cellular core network will open a node to receive the Sigfox data packets and forward those packets to the Sigfox cloud. The problem in this type of integration could be the system integration complexity and high cost for the service.

3.7 Security and Privacy

Security is the biggest concern for the Sigfox based IoT devices. Let us consider a case where a Sigfox device is installed in a laboratory to measure temperature. If this device is not secure then, there can be a big accident in the laboratory. In the same way, home IoT devices need to be secure otherwise hackers can hack the personal files for illegal use. In a worst-case scenario, a small IoT device can be used as a deadly weapon to kill its end users. So IoT devices need to be up-to-date in security matters. A secure IoT system should have four key elements: security, privacy, reliability and reliance.

In [52] and [63], authors point out the fact that Sigfox devices have a low level of security and have higher potential security risks. However, nowadays, Sigfox devices are more secured with the end to end device encryption. Moreover, Sigfox devices are not operated using the internet protocol (TCP/IP) and each device equipped with the unique device ID. In addition, it is not connected to any particular network or base station. Sigfox network built in such a way that it can protect itself from the threats of denial-of-service attacks (DDoS) or massive device cloning. Sigfox device transmits to or receives data from the internet. First, an IoT device broadcast a message in the air then those messages are received by several base stations. Those messages are then delivered to the core network. By default, Sigfox devices designed with a very strict firewall. So it never has the ability to send data to the unauthorized network via the internet as shown in Figure 3.14.

Figure 3.14 *Sigfox devices security schematics [5].*

Sigfox constructed security of its devices in the following ways [64]:

(1) Each Sigfox device equipped with unique authentication key. Device authentication is done with device ID and advanced encryption standard (AES) encryption method with no key over the air (OTA) transmission.

(2) Static manufacturer key, which is unique to every device and used during the registration of the device.

(3) A unique device ID for all of the device used for the device authentication.

(4) A message integrity code (MIC) which ensures the message sequence. A MIC is normally 2 - 5 bytes long.

(5) Finally, the AES - 128 encryption in the application layer.

Encryption, which performed in the application layer, is the responsibility of the customer to design an encryption model for their payload. In addition to this, the base stations also store credentials to communicate with the Sigfox core network. Sigfox backend also stores end devices authentication keys in order to exchange data securely. Sigfox messages contain a sequence number that is synchronized with the Sigfox cloud for the purpose of resistance against spoofing.

3.8 Sigfox Solutions

In a cellular communication system, a user can send a big amount of data at a greater speed. But the biggest problem is that the cost of cellular service is very high. When the number of the connected device is very high then the cost also increases proportionally. A practical solution to this problem is Sigfox based services. Sigfox is the best solution in case it is intended to connect hundreds or millions of devices. Sigfox also provides cloud services, therfore the user can easily view and manage their devices [65]. A cost comparison study shows that the cost of a SigFox module is almost one-third of a LoRa module and one-fifth of a cellular IoT module [66]. In contrast, Sigfox cannot provide services which require high BW, for example, like video streaming, large file transfer, and vehicular crowddensing [67]. On the other hand, a lot of practical applications that need to transfer a small amount of data can use Sigfox network. Some of the notable solution of the Sigfox based system given below [68]:

(1) Water monitoring system using Sigfox compliant device.

(2) Occupancy and chair utilization monitoring with SimplePack device.

(3) A cloud-connected sensor provides an easy way to monitor remote assets and collect data and real-time alarming using Sigfox technology.

(4) Energy management system and indoor air quality monitoring system using Sigfox technology.

(5) Forest fire detection system to prevent forest fire.

(6) Smart waste management system to reduce cost by 60% in cities.

4. MEASUREMENT USING XKIT

At present, Sigfox network is used by a lot of IoT operators around the world. According to the latest report from the Sigfox partner network, currently there are 631 IoT operator is using Sigfox network and there are 581 products are commercially available in the market [1]. In addition, there are a lot of IoT products, which are under development to meet market challenges and demands. Sigfox itself does not manufacture any device, rather it defines the specifications and technical details for the IoT companies to make devices compatible with the Sigfox network. As Sigfox uses license-free spectrum and different country reserves license-free frequency band in different frequency, therefore Sigfox needs to reserve certain frequency band for a specific region. As a result, Sigfox devices hardware and software specification differs from one region to another. The manufacturers of Sigfox device need to follow the Sigfox hardware and software specifications. Sigfox radio network divided into six radio zones worldwide and devices are made according to the regional specifications. There are many technical differences among the regions or zones as described in section 3.3. However, a device may be compatible with one or more regions to operate. Therefore, first, a device manufacturer needs to design and develop a device prototype then make a sample for testing and send them to the Sigfox authority for verification and certification. In this chapter, a Sigfox prototype Thinxtra Xkit is used to evaluate Sigfox system.

4.1 Introduction to Xkit

Thinxtra, one of the Sigfox partner company, founded in 2015 and head office located in Australia [2]. It is empowering the world of IoT by using Sigfox technology. Thinxtra developed few IoT devices and development kits and one of them is "Thinxtra Xkit" as shown in Figure 4.1 [5]. Xkit is a development kit or prototype, which is normally used by the Sigfox developers to test and manipulate Sigfox system. Xkit can be powered in several ways, such as using a 9 V battery or a USB COM port of a computer or with a Raspberry Pi module. This thesis uses Xkit to make

1. https://partners.sigfox.com
2. https://www.thinxtra.com/

necessary indoor and outdoor measurements in the Tampere University, Hervanta campus, Tampere, Finland. The purpose of this measurement is to validate Sigfox network performance and also make predictions of Sigfox radio network behavior in varying environments. This device was provided by the Connected Finland Oy [3] to the Electrical Engineering department of Tampere University for research purposes. Connected Finland Oy, a Finnish Sigfox IoT operator, which connects about 85% of the Finnish population and about 69% of the population (Connected Baltics) in Estonia to the Sigfox IoT services [69].

Thinxtra Xkit module includes few sensors and can be driven by Arduino, Rasberry Pi and also with the Computer. It also includes a USB port and an external 8.5cm omni-directional antenna to receive the signal. Xkit is designed to operate in four different Sigfox radio zones. The key features of a Thinxtra Xkit device given below:

(1) Embedded sensors: Temperature, Pressure, Light, Shock and 3D accelerometer, 2 LEDs and 1 push button, 1 USB port.

(2) Arduino Uno R3 board.

(3) Operating zones: RCZ1, RCZ2, RCZ3, RCZ4.

(4) Scalable and easy to install.

(5) Provide a fast and easy way to set up a prototype of a Sigfox IoT device.

(6) Cost effective.

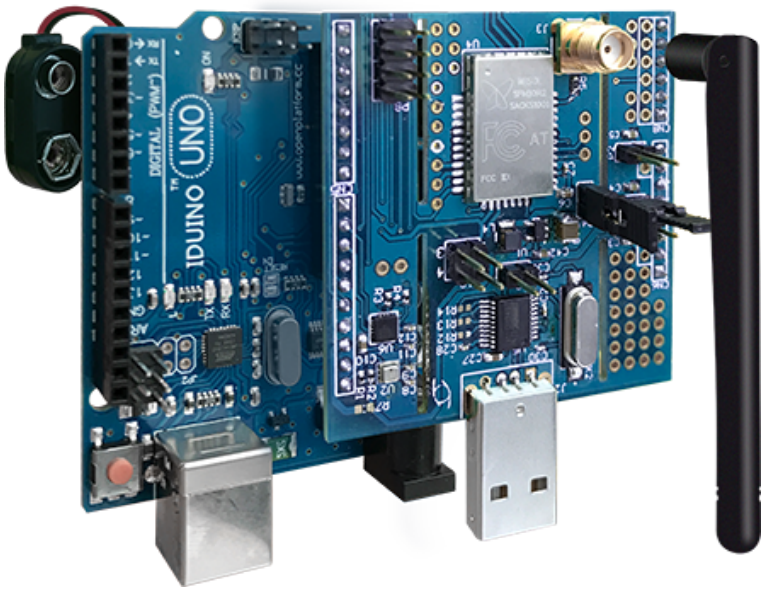


Figure 4.1 *Thinxtra Xkit development kit.*

3. http://www.connectedfinland.fi/

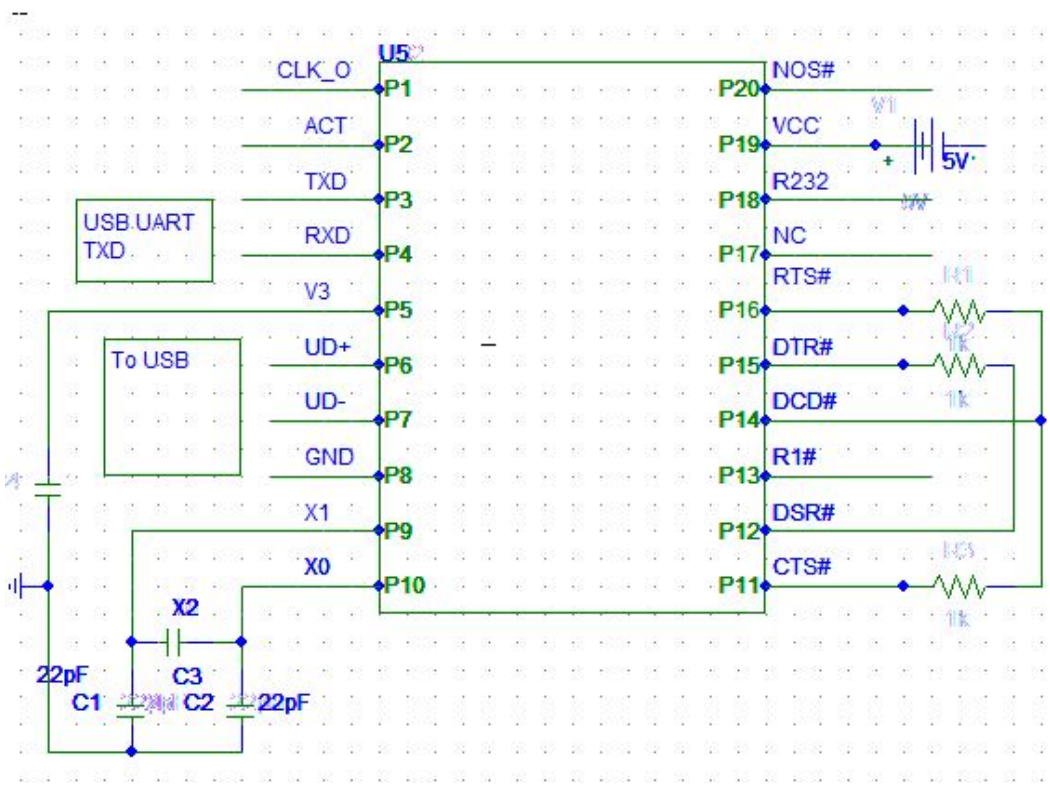


Figure 4.2 *Sigfox Xkit schematics.*

4.2 Xkit Hardware and Software

Recall that, the Xkit device was used to take the measurements, and it can be used with other external sensors to expand its functionality. This hardware configuration is only for research and development purposes, and it uses Arduino Uno to drive its main Xkit module. Xkit chooses Arduino because it is easy to program and cost-effective. In order to access the Xkit module, Arduino needs to program accordingly. The programming language used in Arduino is C. The Xkit has twenty I/O pins used for different purposes shown on Figure 4.2 [70]. To summarize, an Xkit module includes three main components which are described below:

(*i*) **Arduino Uno:** Arduino Uno is an open-source microcontroller board developed by Arduino.cc [4]. It has 14 digital pins, 6 analog pins, 16 MHz quartz crystal and can only be programmed with Arduino integrated development environment (IDE). Thinxtra chooses Arduino uno because it can be used for the low cost projects thus can be widely used for the IoT projects. In addition, Arduino uno has the following key technical specifications:

(a) Micro-controller: ATmega328P.

(b) Operating voltage: 5 V.

4. https://www.arduino.cc/

(c) Input voltage: 7 - 12 V

(d) SRAM: 2 kB.

(e) EEPROM: 1 kB.

(f) Clock speed: 16 MHz.

(g) DC Current per I/O: 20 mA.

(h) DC Current for 3.3 V pin: 50 mA.

(*ii*) **Wisol Module Microchip:** Thinxtra Xkit comprises of a radio module made by Wisol. The Wisol radio module has the following key technical features:

(a) Tx and Rx frequency: 868.13 MHz and 869.525 MHz.

(b) Data rate: Tx and Rx: 100 bps and 600 bps.

(c) Tx output power: 14 dBm (maximum).

(d) Rx sensitivity: -127 dBm.

(e) Input voltage: 1.8 - 3.6 V

(f) Power consumption: Tx: 54 mA, Rx: 15 mA, Idle: 2 μA

The model number of this Wisol microchip is **WSSFM10R1**AT which represents specific features of this radio module as given in Table 4.1.

The pin-diagram and pin-description of Wisol microchip given in Figure 4.3

Table 4.1 *Wisol module features.*

Code	**Description**	**Code**	**Description**
WS	WISOL	**SF**	SIGFOX
M	Module	**10**	Group Model No.
R1	Region	**AT**	AT Command Version

and Table 4.2 respectively [71].

(*iii*) **8.5 cm External Antenna:** Thinxtra Xkit uses an 8.5 cm external omnidirectional antenna to successfully send and receive the signal from and to Sigfox base stations. It is a low-cost antenna and it radiates the signal equally in each direction. As a result, Sigfox base station around a node can transmit and receive the signal from any direction more easily.

4.3 Simulation Study of Sigfox Network

In this thesis, the Monte Carlo simulation method was used to evaluate the Sigfox network. Sigfox device may only transmit 36 seconds per hour thus its time on air is 6 seconds. Each Sigfox uplink messages transmitted three times by the device thus the Sigfox uplink traffic can be modeled as Bernoulli trial with a binomial distribution.

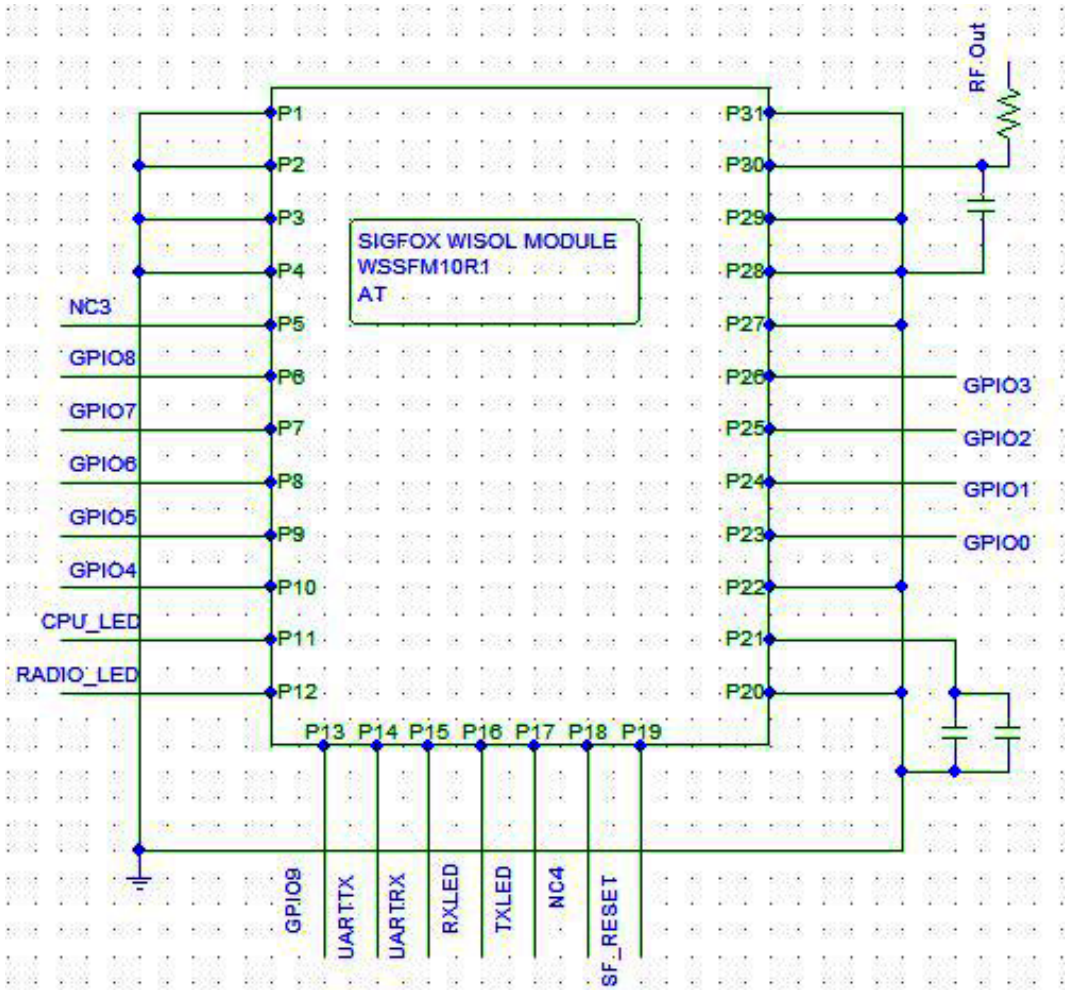


Figure 4.3 *Wisol module schematics.*

Table 4.2 *WISOL WSSFM10R1 pin description.*

1-4,20-22	GND	P	Ground
5,18	NCxx	N	Do Not Connect
6-10,13,23-26	GPIOxx	I/O/PU	General Purpose IO
11	CPU_LED	O	CPU Activity Indicator
12	RADIO_LED	O	Radio Activity Indicator
14	UARTX	O	UART Transmit
15	UARRX	O	UART Receive
16	RX_LED	O	Receive Activity Indicator
17	TX_LED	O	Transmit Activity Indicator
19	RST_N	I/PU	Reset Pin
21	VDD_IO	P	Power Supply
30	RF_IO	A	RF Input/ Output
27-29,31	GND	P	Ground

Sigfox protocol follows a pure ALOHA scheme (random time and random channel) where the probability of a single successful transmission is given by Equation 4.1. So the probability of successful transmission, P is given by Equation 4.2 [72, 73].

$$p = e^{-2.G} \tag{4.1}$$

$$P(X > 0) = 1 - \binom{3}{0} p^0 (1-p)^{3-0} \tag{4.2}$$

Time offset (TO) and the packet error rate (PER) can be calculated by Equation 4.3 and Equation 4.4 respectively.

$$TO = \frac{n_s - (S \cdot n_p)}{T} \tag{4.3}$$

$$PER = \frac{n_c}{n_p} \tag{4.4}$$

where,

G	Average transmission attempts,
P	Number of collision free transmission,
T	Time interval,
p	Zero transmission colliding with own attempt,
n_c	Number of collisions,
n_p	Number of Packets,
n_s	Number of slots.

A Sigfox base station can support up to one million nodes at a time [59]. In a Sigfox network, base stations are always connected via a mesh network, which ensures less packet error rate than other LPWAN protocols. A packet transmission always fails when the devices transmit simultaneously and the time offset is more than the number of slots. By considering the above conditions, this thesis presents MATLAB based Sigfox network simulations, which shows the behavior of Sigfox network performance. Input parameters used in simulations are given in Table 4.3.

Table 4.3 *Sigfox network simulation parameters.*

Number of devices	1000/10000
Number of channels	2000
Number of Slots	6000 ms
Time interval	10 ms
Time span	60000 ms
Bandwidth	200 kHz
Frequency interval	100 Hz

Figure 4.4(a) shows the packet error rate for 1000 devices, where all of the devices are simultaneously sending data to the Sigfox system through one base station. The

packet error rate increases as the number of devices sending data increases. In the same way, if a single base station is connected to the 10000 nodes, then the packet error rate also increases as illustrated in Figure 4.4(b). Each sensor message received by more than one base station, thus, in that case, the number of packet error rate should be very low [73].

The results obtained from the next simulations of Sigfox system suggests that the number of collisions increased only if the number of transmitting nodes increases. The red dotted line was used to indicate the packet collisions and the green dotted line indicates the successful transmission of the packets. According to the results shown on Figure 4.5, it can be shown that there is a few number of red dotted line, which means less collisions among the packets. Numerical analysis of the number of packets collided shows that the number of collisions ranges from 17 to 25. Similarly, when the number of devices increases in a cell then the collisions among the packets also increased as seen in Figure 4.6.

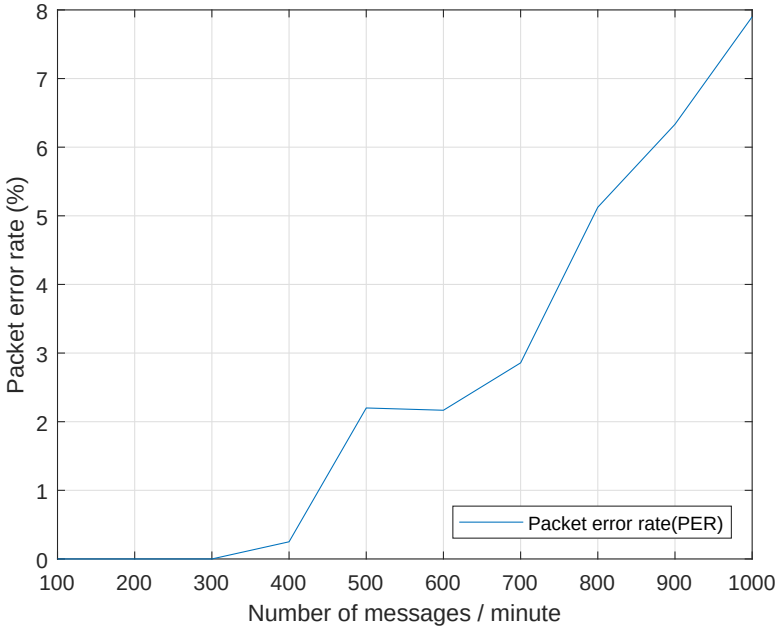
Overall, these results suggest that the Sigfox system performs very well even if there are considerable number of devices connected to one base station. By increasing the number of base station in the reference area, the performance of the system can be increased.

4.4 Measurement and Results

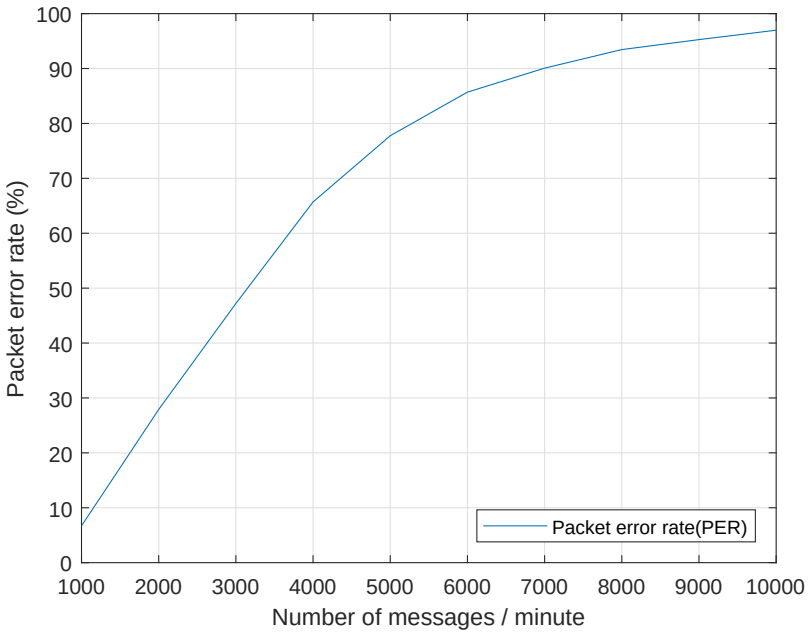
This thesis includes measurement procedures and analyzes the findings for experimental purposes. The hardware of Xkit was set up accordingly and a 9 V battery was used to power up the device. In order to view the data received by the Sigfox system, E-mail services, and Thinger.io was used as callback services. Two types of environment was chosen to perform the necessay experiment with Xkit device and tools, one outdoor and one was run on the indoor environment of the TAU, Hervanta campus. Following measurement methodologies were used to take the measurements:

(a) The most suitable places where the Sigfox device may be installed were identified. As Sigfox network operated through the license-free spectrum, therefore other devices which are operating at the same frequency, may create interference. This can provide an inaccurate result. Places with frequency interference were identified manually and were avoided to get the most suitable result.

(b) In order to make the Xkit device portable, it was powered up with a 9 volt battery and the distance between two measurement points was approximately 10 meters. Before starting the measurement, a printed blueprint of the university buildings [for indoor measurement] and university campus area [for outdoor measurement] was



(a) Sigfox PER for 1000 devices.



(b) Sigfox PER for 10000 devices.

Figure 4.4 *Sigfox system packet error rate.*

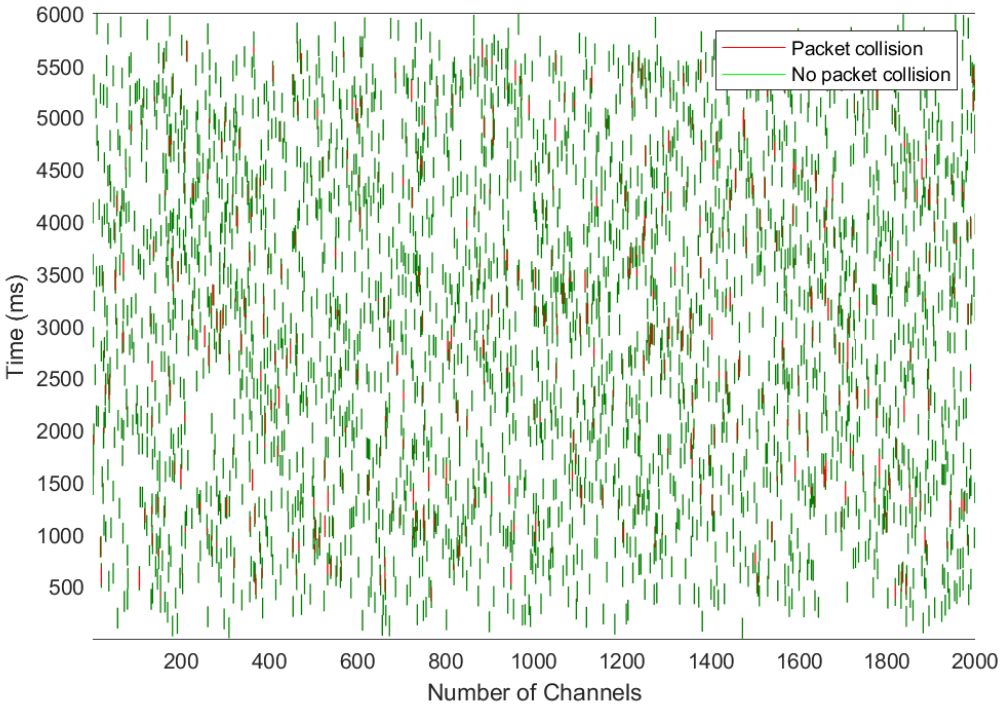


Figure 4.5 *Sigfox spectrum for 1000 devices.*

used and unique ID positions were manually marked (For example, P101, P102, P103), where the measurement will be taken. At each measurement point, the switch of Xkit was pressed manually to force the device to send data to the Sigfox system. Later successful reception of necessary parameters was checked via E-mail. The measurements were taken by visiting the selected measurements points both in indoor and outdoor locations.

(c) In order to get realistic values from the measurements, both open places and dead zones were considered. For example, in case of indoor measurements, a value was taken in an open place and another value was taken in the places where the signal most likely obstructed. It helped to plot and map the values in CDF and heat map accurately.

(d) In order to take the real-time values in an efficient manner, E-mail callback system was used. Another call back system, Thinger.io was also used to recheck the values and to observe change through visual representation. In the end, Sigfox back-end server was used to evaluate the data.

(e) The measured data was recorded in the excel file with respective position ID.

(f) First simulation study of Sigfox network was made to predict and understand the network behavior in different conditions.

(g) The analysis is based on, CDF of the received signal strength, mean of the received signal SNR, and the heat map which was evaluated in the reference area for both

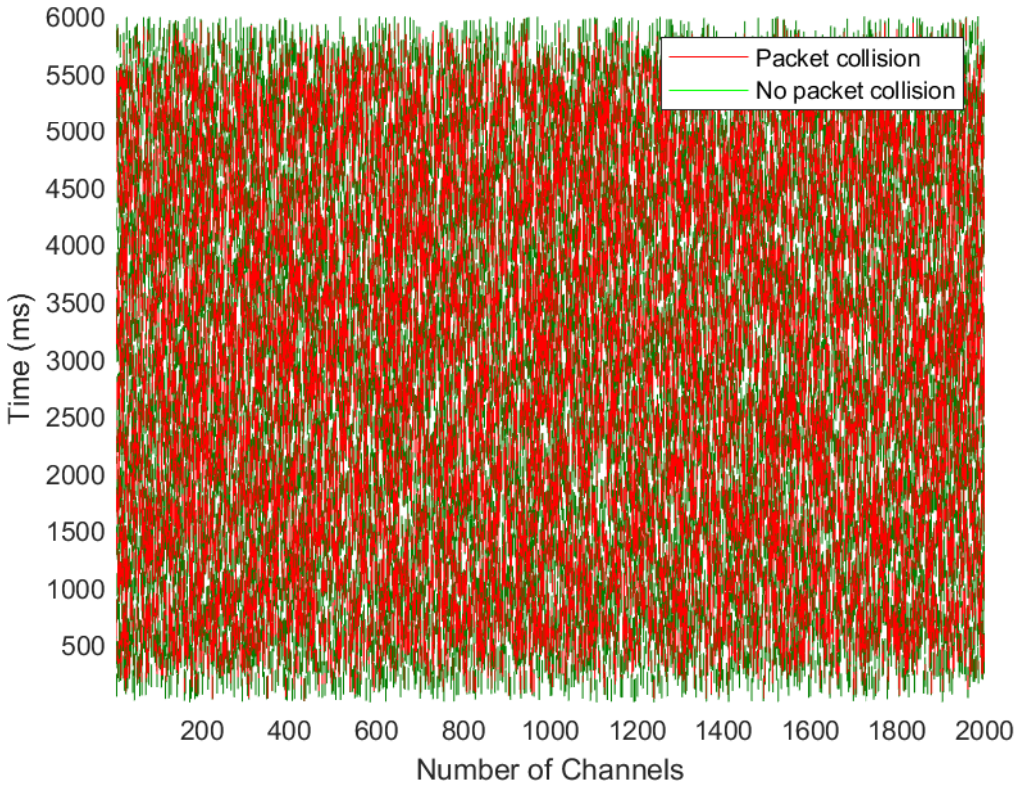


Figure 4.6 *Sigfox spectrum for 10000 devices.*

indoor and outdoor measurements. An analysis of the Sigfox signal behaviors and differences between the two measurements was presented for better understanding.

(h) RSSI, SNR and link quality indicator (LQI) are important parameter in wireless radio connectivity. RSSI can provide a very good estimator for the wireless network and also provide estimation for the packet reception rate (PRR) and the distance between the nodes and the base station [74, 75]. RSSI and SNR values were used to evaluate Sigfox network behavior in the reference area.

4.4.1 Indoor Measurement

Sigfox radio network performance in the indoor environment can be evaluated by surveying the reference area, taking measurements of link speed, interpreting RSSI and SNR values at key locations (for example, open spaces and dead spots). A Sigfox device may be installed in both indoor and outdoor location as required by the specific application. In this thesis, indoor measurements were taken in six buildings of Tampere University (TAU), Hervanta campus. They are Tietotalo, Sähkötalo, Rakennustalo, Kampusareena, Päätalo, Festia, and Konetalo. In case of indoor locations, the signal was most likely attenuated by the walls and the floors.

Thus the received RSSI and SNR is comparatively low than the outdoor locations. In case of underground locations, signal was obstructed quite often and was lost in some cases. Contrary to this, signal strength and SNR increases with the increase in floor number. The summary of the indoor measurement is tabulated in the Table 4.4.

Table 4.4 *Summary of indoor measurements.*

Number of measurement points	202
Measured parameters	SNR and RSSI
Maximum average SNR	26.45 dB
Minimum RSSI	-146 dBm
Minimum average SNR	8.66 dB
Maximum RSSI	-113 dBm
Number of points signal lost	26
Number of available base station	0 to 3
Standard deviation (SNR)	2.8478
Standard deviation (RSSI)	7.9263

The library of the TAU (Hervanta campus) is located in the basement of Kampusareena and the signal was lost in all places except under the holes in the rooftops as shown in the heat map of the library in Figure B.1. Therefore the Sigfox device can not function in a space like the library with the present Sigfox network condition.

A measurement study conducted on different floors of Tietotalo building is shown on Figure 4.8. In Figure 4.8, one can clearly see a trend of increased signal strength on the upper floors. This is happening because the Sigfox signal needs to penetrate more walls and floors to reach the nodes located on the ground floor whereas at the same time it can easily reach the nodes on the upper floor. This was observed in the case of other buildings too. Additionally, heat maps of the Sigfox signal measured on other buildings is shown in Appendix B.

4.4.2 Outdoor Measurement

Outdoor measurements were taken with the set of tools and equipment as described in section 4.4. The measurements were taken during winter season in Finland, and the outside temperature varied between -15 to -5 degree celsius. Therefore, the measurements in received signals were got affected by snowy and cold environment. The measurement were taken by starting from Tietotalo building, and measurements points were chosen manually. In outdoor locations, the signals have a

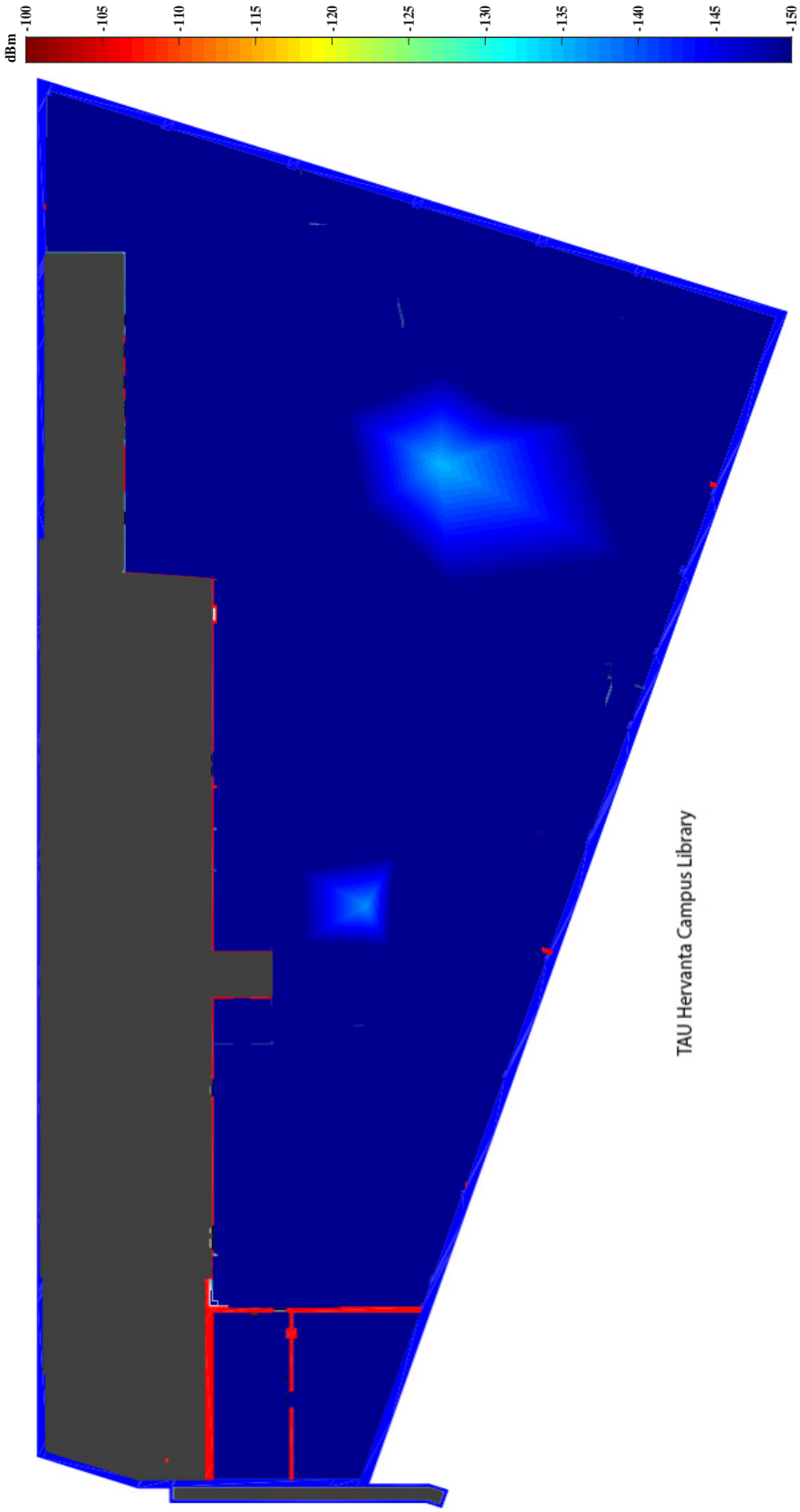
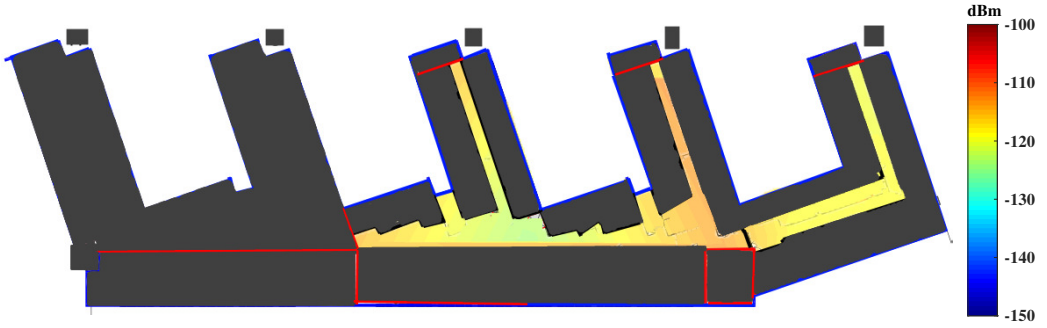
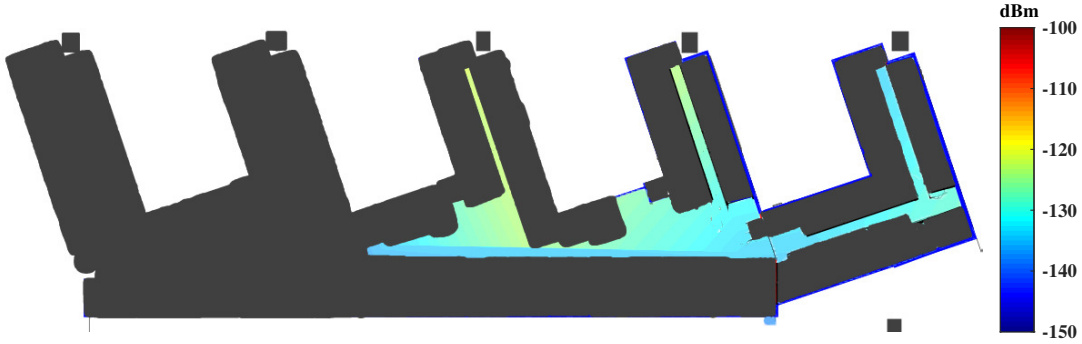


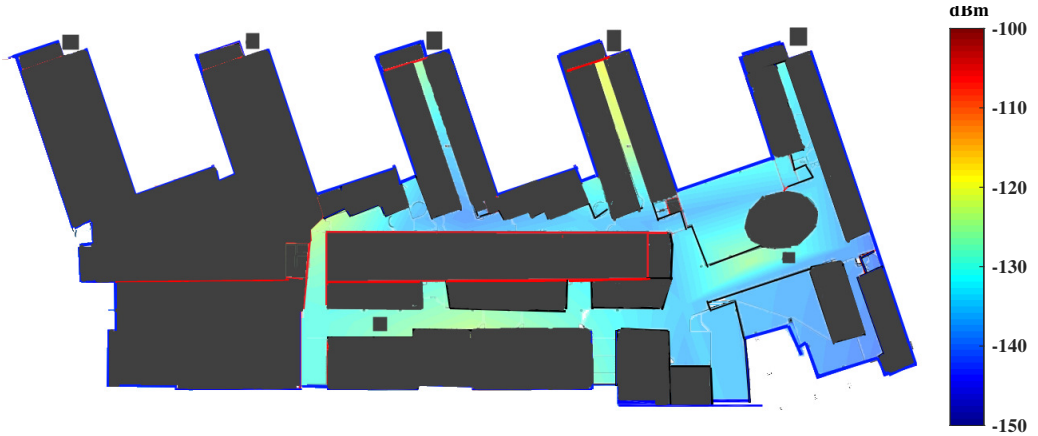
Figure 4.7 *Heatmap of RSSI values in TAU library, Hervanta campus.*



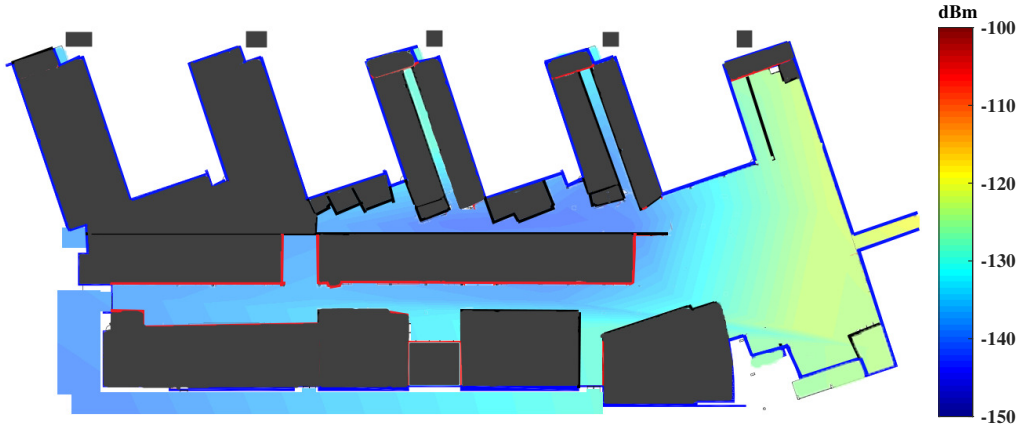
(a) Tietotalo fourth floor.



(b) Tietotalo third floor.



(c) Tietotalo second floor.



(d) Tietotalo first floor.

Figure 4.8 *Representation of Sigfox signal strength in different floor of Tietotalo building.*

different values as expected. The attenuation factor can be small hills, reflection from the building walls, obstruction, and reflection from the nearby trees, and the distance between the base station and nodes is also important.

Table 4.5 *Summary of outdoor measurements.*

Number of measurement points	105
Measured parameters	SNR and RSSI
Maximum average SNR	26.96 dB
Maximum RSSI	-100 dBm
Minimum average SNR	22 dB
Minimum RSSI	-145 dBm
Number of points signal lost	0
Number of available base station	1 to 3
Standard deviation (SNR)	1.2719
Standard deviation (RSSI)	9.4914

After evaluating values received from the Xkit, it is shown that the RSSI and SNR values increase in the open places and decrease in the places close to hills and the trees. Since location of the Sigfox base station is unknown and hence there might be no LOS connection between the base station and the nodes. The heat map of the RSSI values obtained from the measurements is shown in Figure 4.9.

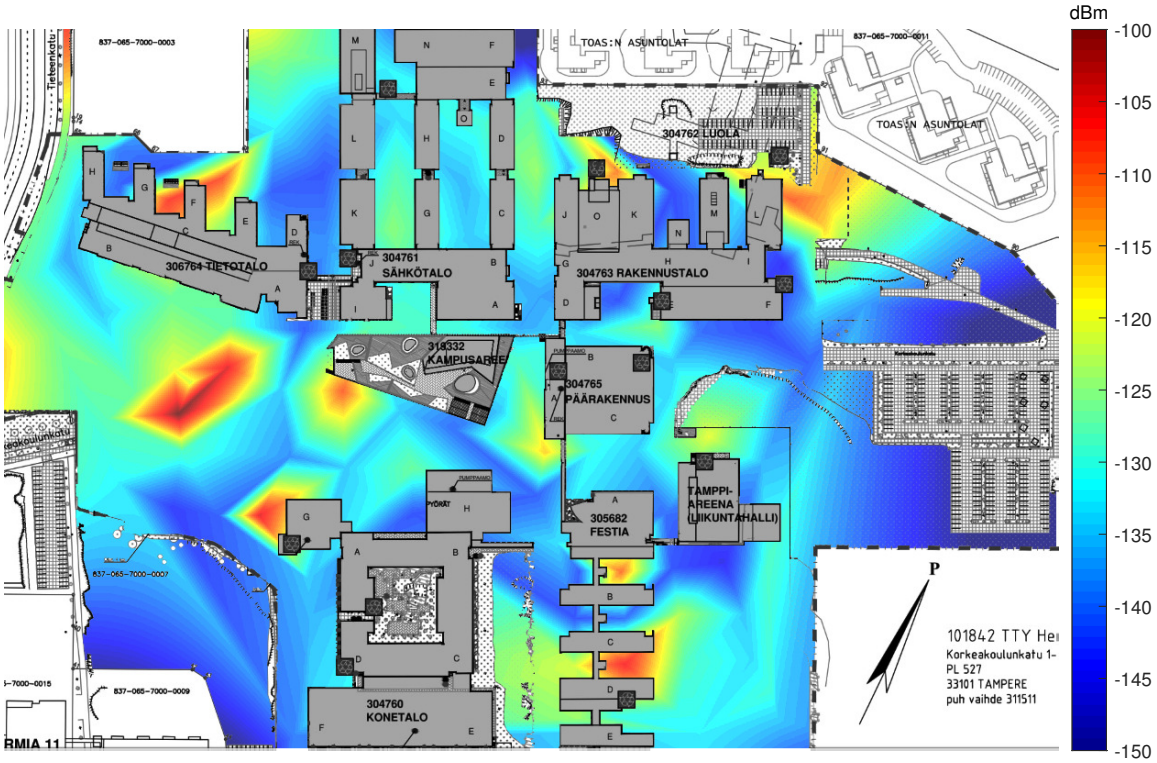


Figure 4.9 *Heatmap of RSSI values in TAU, Hervanta campus.*

4.5 Results of Analysis

This section summarizes the whole measurement results obtained from a Xkit device. The area of interest includes both indoor and outdoor places, which help to analyze and predict the Sigfox system performance in any other locations. Following the Sigfox network specifications, as described in Table 3.2 and the simulation studies of Sigfox network in section 4.3, this thesis compares results obtained in both indoor and outdoor measurements.

One of the primary metrics of these measurements were the RSSI values which represent the network strength at different points. At one particular point, it was observed that RSSI value was different in different trials. One possible cause might be, the signal that was received in the successive trials might be different from the previous base station. In addition to this, the nodes choose different channels at different times. The second metric used to conduct the analysis was SNR values, which shows the Sigfox signal power over the noise signal. Because of multichannel communication, the perceived SNR of a single point was also different at different times.

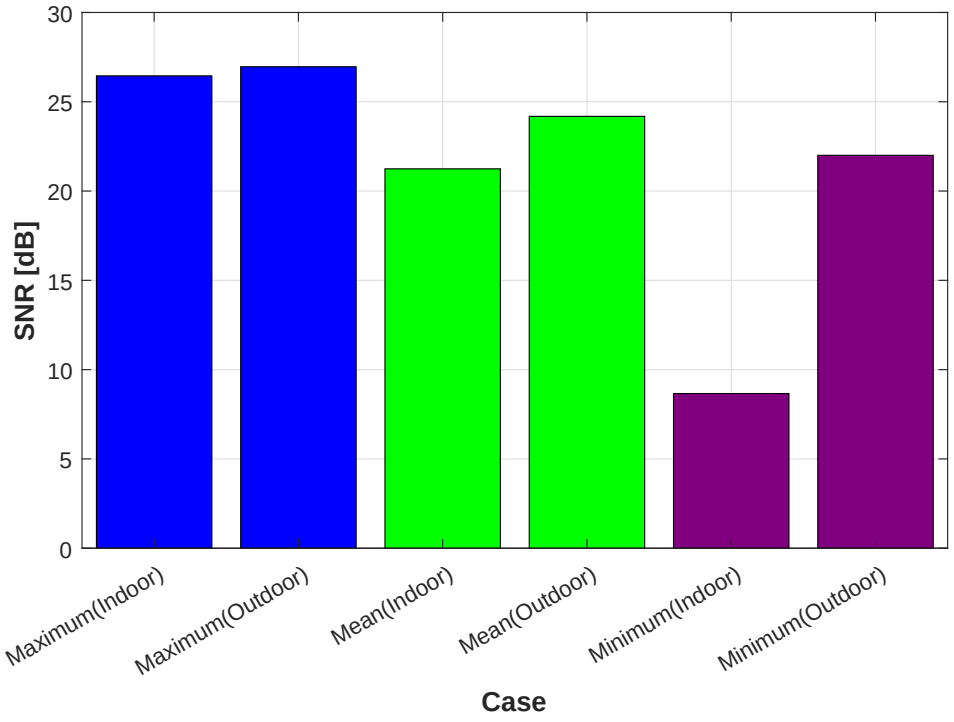


Figure 4.10 *Comparisons of SNR values in indoor and outdoor measurements.*

By observing the plots of SNR values presented in Figure 4.10, it was easy to conclude that the minimum received SNR value of the outdoor measurements was

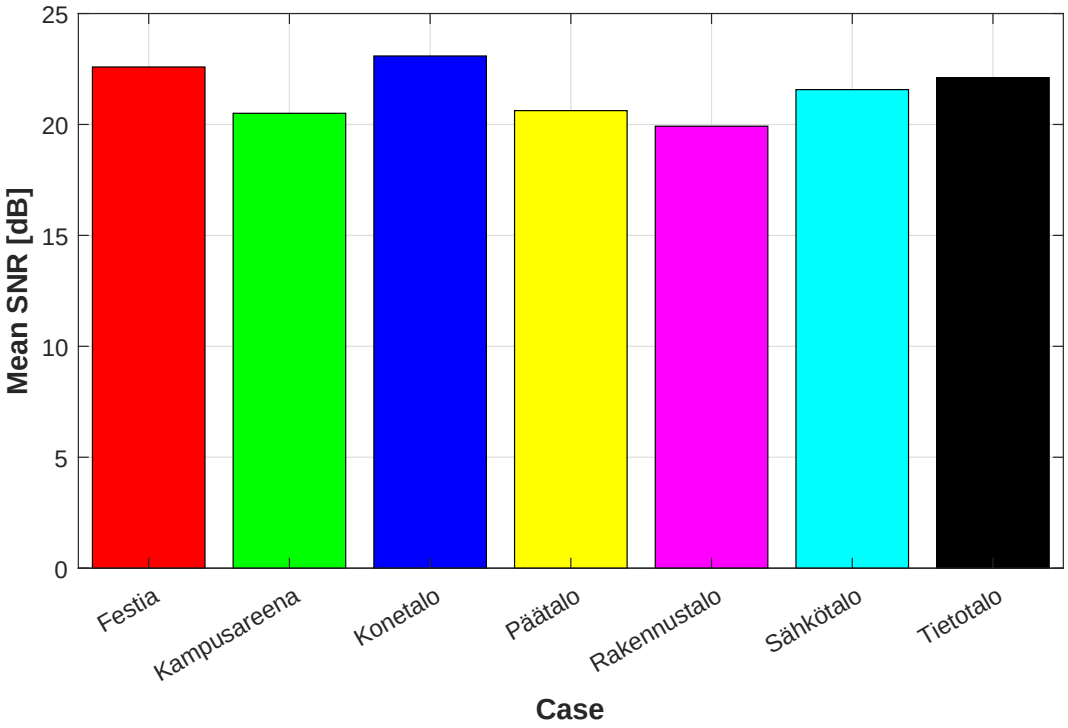


Figure 4.11 *Comparisons of mean SNR values in different building.*

higher than the indoor measurements. In case of indoor communication, the Sigfox signals need to penetrate ground, walls or rooftops which decreases its strength. A Sigfox end device can receive the signal up to a minimum SNR value, which is 8 dB. The comparison of maximum SNR value is nearly the same. Because the indoor measurement points also include places close to outdoor where there might be a glass wall in the middle. In addition, as the outdoor measurement points include a lot of open places compared to the indoor measurement points, the mean values were relatively higher. Similarly, the mean SNR values of different buildings shown on Figure 4.11. Figure 4.11 indicates that Konetalo and Festia building has the highest mean SNR value. Therefore signal strength was higher in those places than other places. In contrast, Rakennustalo has the lowest mean SNR value. The deviation of mean SNR value for every building was very small because all buildings are located at nearly the same place and have the same environmental conditions.

Another way to analyze the signal distribution is the CDF of the measured signal. The CDF presented in Figure 4.12 shows that in the case of indoor measurement the distribution of SNR values falls mostly between 17 dB to 25 dB. The range is quite large because of the varying environmental conditions at different measurement points. For outdoor measurement, the range of values is limited, and it falls between the values of 22 dB to 27 dB. CDF of measured SNR values of different building is

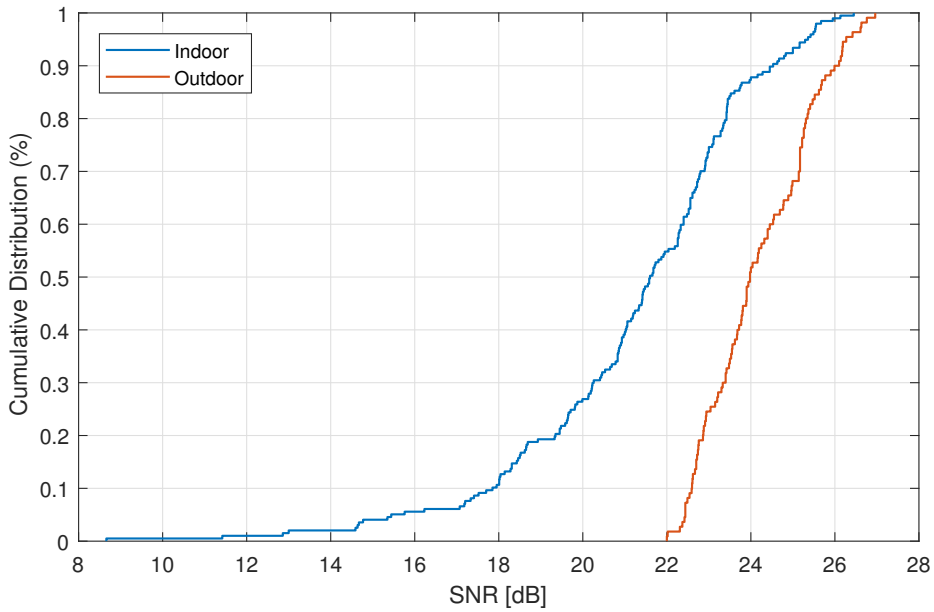


Figure 4.12 *CDF of average SNR values in indoor and outdoor measurements.*

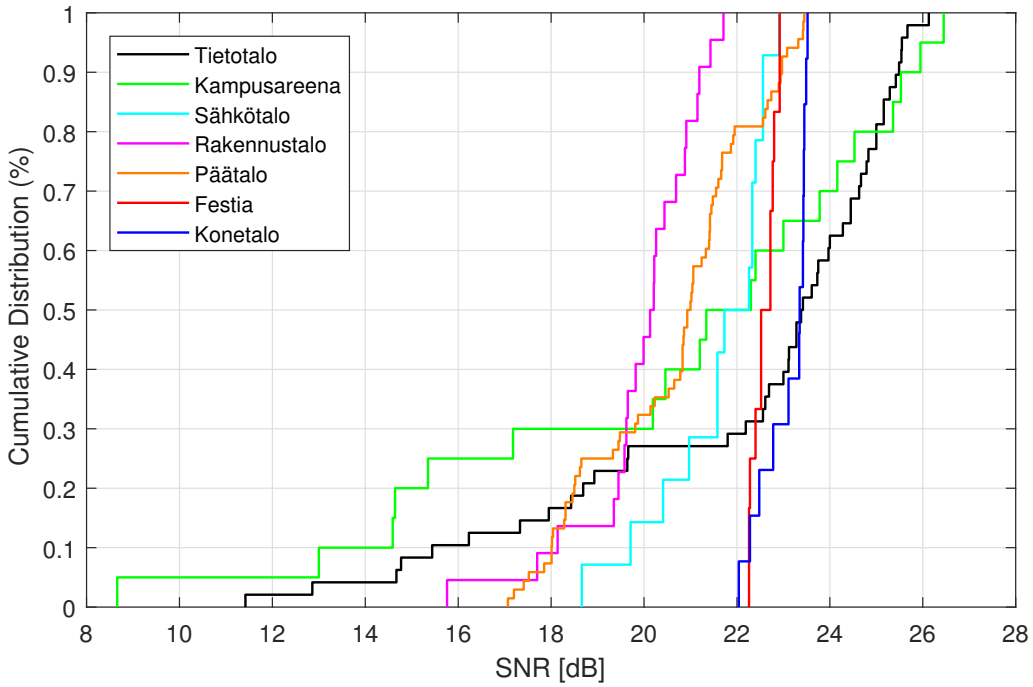


Figure 4.13 *CDF of average SNR values in different building.*

shown in Figure 4.15.

In this thesis, what stands out in the measurement is RSSI values which shows the power of the received signal. Whereas the low RSSI value means weak Sigfox signal and a strong noise signal. Contrary to this, high RSSI value meanings strong

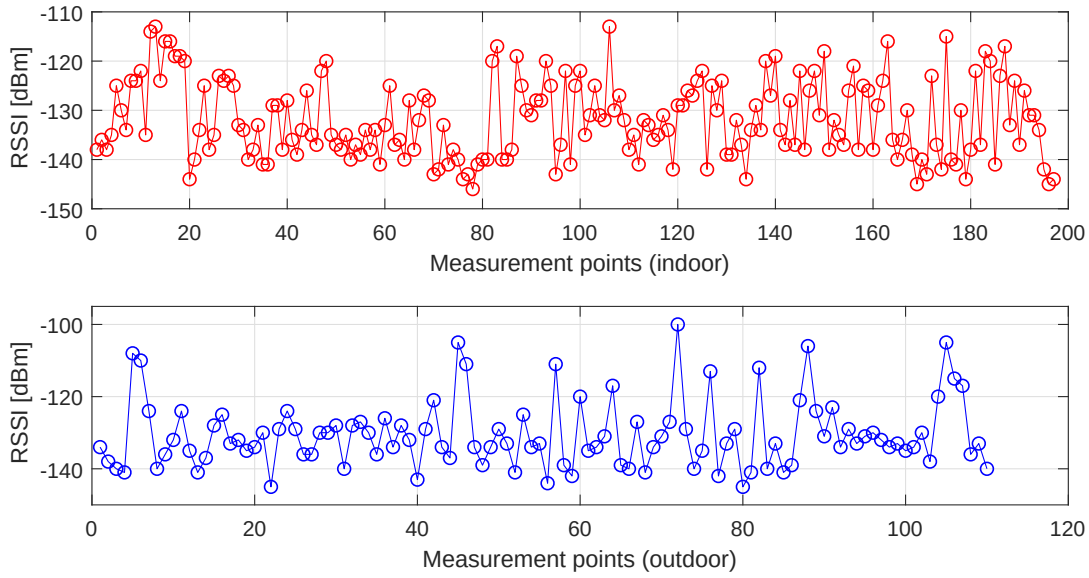


Figure 4.14 *Representation of RSSI values both in indoor and outdoor.*

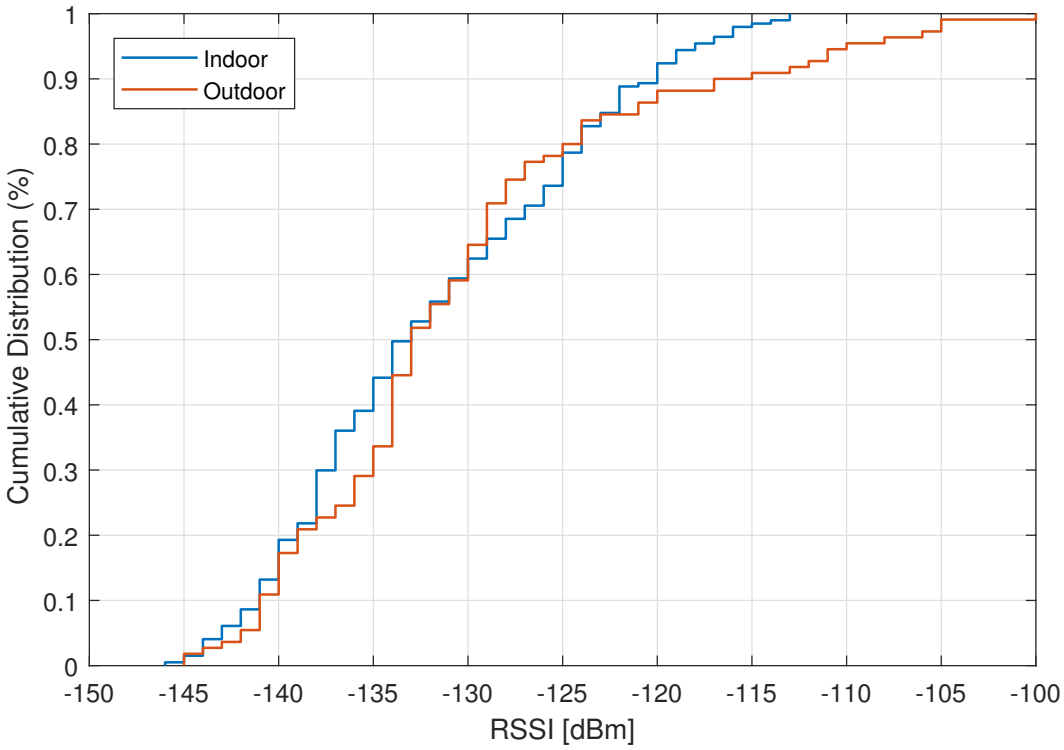


Figure 4.15 *CDF of measured RSSI values.*

received signal and low noise signal [75]. Figure 4.14 illustrates RSSI values for both indoor and outdoor measurements. While taking the measurements, a single point shows different RSSI values in different measurement. This is possibly because of multipath communication between node and base station and the presence of

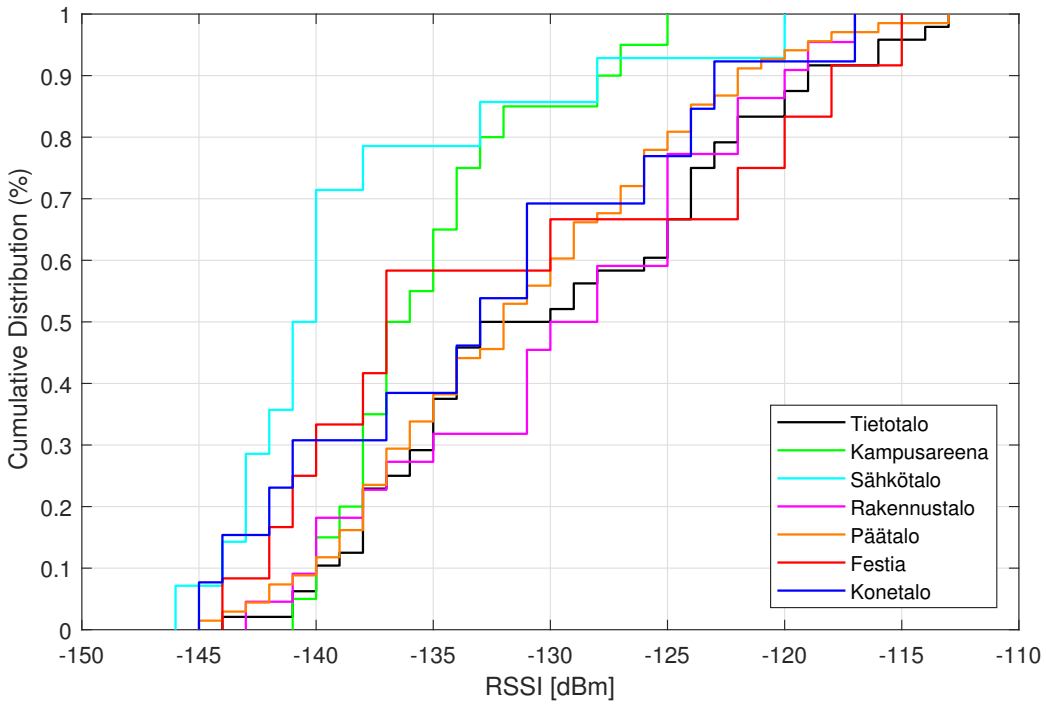


Figure 4.16 *CDF of RSSI values in different building.*

high moisture in the environment [75]. From Figure 4.14, it is clear that outdoor measurements has high RSSI values than the indoor measurements. Figure 4.15 and Figure 4.14 illustrates that the highest possible RSSI value in the reference area is -110 dBm, which was found in the outdoor location. In addition, most RSSI value ranges from -140 dBm to -120 dBm, both in indoor and outdoor locations. Figure 4.16 indicate the distribution of RSSI values in different buildings of TAU, Hervanta campus.

5. CONCLUSIONS

As a conclusion for the work carried out in the thesis, the key outline results are introduced next:

(1) Potential of IoT protocols, applications, security matters and economic impacts were investigated.

(2) The architectural aspects of Sigfox based IoT systems were covered with all necessary information.

(3) Sigfox radio network planning procedures were briefly discussed. Also, MATLAB based simulations were presented for better understanding of the Sigfox radio network planning procedures.

(4) The performance evaluation of the Xkit device is performed, in particular, simulations and practical measurements were taken in the reference area.

5.1 Future Development of Sigfox Network

In order to make the Sigfox network and services more flexible, a lot of development can be made in its networking technology. For example, a convenient way for Sigfox network development can be given as following:

(1) Satellite: Nano satellite or geostationary satellite can be used for better coverage in large areas. It will also help to connect remote cities or islands together.

(2) Since the Sigfox devices only sense environment, which consumes minimal data traffic by the way, therefore D2D communication protocols come in handy in such situations. D2D communication protocols are known for saving devices energy while providing better information management system. As a result, for better services, D2D communication protocols are proposed for prospect Sigfox systems [76].

(3) Nano antennas: Nano antennas are one of the available options which can be used to provide better indoor coverage. In particular, nano antennas are very useful in providing better network coverage in poor network conditions, such as illustrated in Figure B.1.

(4) One device for all regions: Sigfox has six radio zones with six different radio configurations. Then, one of the possible ways to make the network more cost effective, is to let the device operate at all of the available radio zones.

(5) Improvement of the security system: Recall, Sigfox left the application layer encryption to the end user. Therefore, if the user did not configure the application layer encryption properly, then the most critical IoT applications might be hindered in the process. It is worth mentioning that some researchers found some Sigfox networks which were potentially vulnerable to high security risks [52, 63]. As a result, it can be conclude that more research should be focused on the Sigfox network security.

In addition to the previously mentioned proposals, Sigfox system can be also developed by using M2M communication protocols, not to mention the fact that it can be also integrated with available cellular networks.

5.2 Concluding Words

The main contribution of this thesis was presenting the Sigfox network behavior in the reference area using an evaluation kit. The measured parameters were presented using tables, CDF graphs and heat maps. It should be noted that, the graphical presentations of the measured data and the statistics had some limitations in them, such as:

(1) Because of the limited access right and the limited time given for the completion of the thesis, the indoor measurements were taken in a limited number of places.

(2) Measurements were not taken in fixed discrete distances. However, on average the distances between every two successive points were approximately 10 meters.

(3) Because of the limitations stated above, heat maps are not highly accurate.

Also, this thesis discussed the IoT protocol and its applications in details, in addition to the Sigfox technical details and Sigfox network simulations. Not to mention that few possible ways for integrating the Sigfox network with other similar radio technologies were also presented. Finally, there were some proposals made to develop Sigfox network including its services.

Sigfox brings a lot of possibilities in the IoT technologies which can be developed for a better world. This thesis leads to the following future work:

(1) Find out the suitability of the Sigfox devices for specific applications.

(2) Develop omnidirectional antenna usable in all regions for Sigfox devices.

(3) Develop D2D communication protocol for the Sigfox devices.

(4) Integrate Sigfox network with other available radio technologies.

(5) Design and develop Sigfox nanodevice for the human body.

(6) Design and develop wearable Sigfox IoT device.

BIBLIOGRAPHY

[1] C. SYStem, "Embracing the internet of everything to capture your share of $14.4 trillion," tech. rep., Cisco Systems inc, Cisco Sys Inc, 7 2013. Accessed: 2018-09-18.

[2] Sigfox, "Sigfox." `https://www.sigfox.com`. Accessed: 2018-09-22.

[3] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, and M. Pettissalo, "On the coverage of lpwans: range evaluation and channel attenuation model for lora technology," in *2015 14th International Conference on ITS Telecommunications (ITST)*, pp. 55–59, Dec 2015.

[4] J. Säe, "Macro cell capacity in mobile networks," Master's thesis, Tampere University of Technology, 1 2012. Examiner: Prof. Jukka Lempainen.

[5] Sigfox, "Make things come alive in a secure way," tech. rep., Sigfox, 2 2017. Accessed: 2018-10-2.

[6] L. Malisa, *Security of User Interfaces: Attacks and Countermeasures*. PhD thesis, ETH Zurich, 2017.

[7] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *2015 IEEE World Congress on Services*, pp. 21–28, June 2015.

[8] T. Saarikko, U. H. Westergren, and T. Blomquist, "The internet of things: Are you ready for whats coming?," *Business Horizons*, vol. 60, no. 5, pp. 667–676, 2017.

[9] G. S. Matharu, P. Upadhyay, and L. Chaudhary, "The internet of things: Challenges amp;amp; security issues," in *2014 International Conference on Emerging Technologies (ICET)*, pp. 54–59, Dec 2014.

[10] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with china perspective," *IEEE Internet of Things Journal*, vol. 1, pp. 349–359, Aug 2014.

[11] Sigfox, "Sigfox protocols." `https://www.youtube.com/watch?v=tGmFgaxKPRU`. Accessed: 2018-09-22.

[12] G. Ferré and E. P. Simon, "An introduction to Sigfox and LoRa PHY and MAC layers." working paper or preprint, Apr. 2018.

[13] Sigfox, "Sigfox device cookbook: communication configuration," tech. rep., Sigfox, 11 2018. url: www.build.sigfox.com/sigfox-device-cookbook.

[14] M. People, "Missing people in britian." `https://www.missingpeople.org.uk/about-us/about-the-issue/research/76-keyinformation2.html`. Accessed: 2018-09-12.

[15] O. Stevenson, H. Parr, P. Woolnough, and N. Fyfe, "Geographies of missing people: Processes, experiences, responses [online]," *University of Glasgow*, 2013.

[16] H. M. Layson Jr, "Body worn active and passive tracking device," Jan. 11 2000. US Patent 6,014,080.

[17] A. McEwen and H. Cassimally, *Designing the Internet of Things*. Wiley, 2013.

[18] Cisco, "The internet of everything global private sector economic analysis," tech. rep., Cisco Systems, Cisco Inc, 7 2013. Accessed: 2018-09-18.

[19] H. Al-Kashoash and A. Kemp, *Comparison of 6LoWPAN and LPWAN for the Internet of Things*. Australian Journal of Electrical and Electronics Engineering, 12 2017.

[20] Huawei, "Nb-iot, enabling new business oppurtunities," *Huawei Magazine*, 2016. Publisher: Huawei.

[21] J. Gozalvez, "New 3gpp standard for iot [mobile radio]," *IEEE Vehicular Technology Magazine*, vol. 11, no. 1, pp. 14–20, 2016.

[22] A. D. Zayas and P. Merino, "The 3gpp nb-iot system architecture for the internet of things," in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 277–282, May 2017.

[23] K. Mochizuki, K. Obata, K. Mizutani, and H. Harada, "Development and field experiment of wide area wi-sun system based on ieee 802.15. 4g," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp. 76–81, IEEE, 2016.

[24] H. Kroll, M. Korb, B. Weber, S. Willi, and Q. Huang, "Maximum-likelihood detection for energy-efficient timing acquisition in nb-iot," in *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pp. 1–5, March 2017.

[25] J. Lin, Z. Shen, and C. Miao, "Using blockchain technology to build trust in sharing lorawan iot," in *Proceedings of the 2nd International Conference on Crowd Science and Engineering*, pp. 38–43, ACM, 2017.

[26] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "Lorawan specification," *LoRa alliance*, 2015.

[27] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on lpwa technology: Lora and nb-iot," *Ict Express*, vol. 3, no. 1, pp. 14–21, 2017.

[28] IEEE, "Ieee standard for low-rate wireless networks," *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, pp. 1–709, April 2016.

[29] S. Bluetooth, "Bluetooth specification," 2003.

[30] B. Specification, "Version 1.0," *JSR*, vol. 168, 2003.

[31] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi," in *Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE*, pp. 46–51, Ieee, 2007.

[32] A. ZigBee, "Zigbee-2006 specification," *http://www. zigbee. org/*, 2006.

[33] W. Webb, "Weightless technology an overview," *Mar*, vol. 28, pp. 1–16, 2012.

[34] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the internet of things (iot)," in *International Conference on Network Security and Applications*, pp. 420–429, Springer, 2010.

[35] O. Novo, N. Beijar, M. Ocak, J. Kjällman, M. Komu, and T. Kauppinen, "Capillary networks - bridging the cellular and iot worlds," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pp. 571–578, Dec 2015.

[36] Qualcomm, *Qualcomm IoT*. Qualcomm, 1 ed., 9 2018.

[37] D. M. Benjillali, "Itu iot presentation." `https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2017/IoTSMW/Presentations-IoT/Session1/IoT4SSC_Session_1_Benjillali.pdf`. Accessed: 2018-09-19.

[38] R. Sanchez-Iborra and M.-D. Cano, "State of the art in lp-wan solutions for industrial iot services," *Sensors*, vol. 16, no. 5, p. 708, 2016.

[39] E. Guillén, J. Sánchez, and L. R. López, "Iot protocol model on healthcare monitoring," in *VII Latin American Congress on Biomedical Engineering CLAIB 2016, Bucaramanga, Santander, Colombia, October 26th-28th, 2016*, pp. 193–196, Springer, 2017.

[40] Statista. `https://www.statista.com/statistics/580778/worldwide-internet-of-things-economic-impact-forecast/`. Accessed: 2018-10-3.

[41] K. R. Group, "Gsma: The impact of the internet of things: The connected home," tech. rep., KRC Research Lab, 7 2013.

[42] L. projects. `http://www.libelium.com/resources/case-studies/`. Accessed: 2018-12-10.

[43] H. Hernesniemi, M. Lammi, P. Ylä-Anttila, and P. Rouvinen, "Advantage finland.-the future of finnish industries," tech. rep., The Research Institute of the Finnish Economy, 1996.

[44] S. projects. `https://www.teliacompany.com/en/news/news-articles/2018/posti-and-telia-pilot-worlds-first-smart-mailbox-with-nb-iot/`. Accessed: 2018-12-22.

[45] F. Projects. `https://fiif.fi/`. Accessed: 2018-12-20.

[46] D. M. Hernandez, G. Peralta, L. Manero, R. Gomez, J. Bilbao, and C. Zubia, "Energy and coverage study of lpwan schemes for industry 4.0," in *2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM)*, pp. 1–6, May 2017.

[47] S. S. Description. `https://datatracker.ietf.org/meeting/97/materials/slides-97-lpwan-25-sigfox-system-description-00`. Accessed: 2018-12-23.

[48] O. J. JOSEPH, "Ultra-narrowband internet-of-things technologies," Master's thesis, Tampere University of Technology, 11 2017. Examiner: Prof. Markku Renfors.

[49] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovacs, P. Mogensen, and M. Sorensen, "Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, June 2017.

[50] Sigfox, "One network a billion dreams," tech. rep., Sigfox, 1 2018. M2M and IoT redefined through cost effective and energy optimized connectivity.

[51] K. E. Nolan, W. Guibene, and M. Y. Kelly, "An evaluation of low power wide area network technologies for the internet of things," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 439–444, Sep. 2016.

[52] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: the rising stars in the iot and smart city scenarios," *IEEE Wireless Communications*, vol. 23, pp. 60–67, October 2016.

[53] H. Mroue, A. Nasser, and S. Hamrioui, "Mac layer-based evaluation of iot technologies: Lora, sigfox and nb-iot," in *MAC layer-based evaluation of IoT technologies*, May 2018.

[54] Sigfox, "Sigfox verified modem specification for rc1-udl-enc," tech. rep., Sigfox, 9 2018. Version 3.7.1.

[55] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of things (iot) communication protocols: Review," in *2017 8th International Conference on Information Technology (ICIT)*, pp. 685–690, May 2017.

[56] G. Margelis, R. Piechocki, D. Kaleshi, and P. Thomas, "Low throughput networks for the iot: Lessons learned from industrial implementations," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pp. 181–186, Dec 2015.

[57] G. G. Ribeiro, L. F. de Lima, L. Oliveira, J. J. Rodrigues, C. N. Marins, and G. A. Marcondes, "An outdoor localization system based on sigfox," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, IEEE, 2018.

[58] C. Goursaud and J.-M. Gorce, "Dedicated networks for iot: Phy/mac state of the art and challenges," *EAI endorsed transactions on Internet of Things*, 2015.

[59] S. B. P. Antoine, *Sigfox SBST3 Product Manual.* Sigfox, 1 ed., 12 2017.

[60] X. Zhang, A. Andreyev, C. Zumpf, M. C. Negri, S. Guha, and M. Ghosh, "Thoreau: A subterranean wireless sensing network for agriculture and the environment," in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 78–84, May 2017.

[61] V. Petrov, K. Mikhaylov, D. Moltchanov, S. Andreev, G. Fodor, J. Torsner, H. Yanikomeroglu, M. Juntti, and Y. Koucheryavy, "When iot keeps people in the loop: A path towards a new global utility," *IEEE Communications Magazine*, vol. 57, pp. 114–121, January 2019.

[62] Sigfox, *Sigfox API usage.* Sigfox, 1 ed., 9 2017.

[63] N. Poursafar, M. E. E. Alahi, and S. Mukhopadhyay, "Long-range wireless technologies for iot applications: a review," in *2017 Eleventh International Conference on Sensing Technology (ICST)*, pp. 1–6, IEEE, 2017.

[64] R. Fujdiak, P. Blazek, K. Mikhaylov, L. Malina, P. Mlynek, J. Misurec, and V. Blazek, "On track of sigfox confidentiality with end-to-end encryption," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, p. 19, ACM, 2018.

[65] Z. D. R. Gnimpieba, A. Nait-Sidi-Moh, D. Durand, and J. Fortin, "Using internet of things technologies for a collaborative supply chain: Application to tracking of pallets and containers," *Procedia Computer Science*, vol. 56, pp. 550 – 557, 2015. The 10th International Conference on Future Networks and Communications (FNC 2015) / The 12th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2015) Affiliated Workshops.

[66] A. Azari, *Serving IoT Communications over Cellular Networks Challenges and Solutions in Radio Resource Management for Massive and Critical IoT Communications.* PhD thesis, KTH, Sweden, 11 2018.

[67] V. Petrov, A. Samuylov, V. Begishev, D. Moltchanov, S. Andreev, K. Samouylov, and Y. Koucheryavy, "Vehicle-based relay assistance for opportunistic crowdsensing over narrowband iot (nb-iot)," *IEEE Internet of Things Journal*, vol. 5, pp. 3710–3723, Oct 2018.

[68] P. Di Gennaro, D. Lofú, D. Vitanio, P. Tedeschi, and P. Boccadoro, "Waters: A sigfox-compliant prototype for water monitoring," *Internet Technology Letters*, p. e74, 2016.

[69] C. F. Oy, "Thinxtra xkit from connected finland oy." `http://www.connectedfinland.fi/`. Accessed: 2018-12-31.

[70] Thinxtra, "Xkit module data sheet." `https://github.com/Thinxtra`. Accessed: 2018-12-30.

[71] Wisol, *Wisol Module Data Sheet*. Wisol, http://www.wisol.co.kr/, 12 ed., 5 2017. Accessed: 2018-12-31.

[72] N. Abramson, "The aloha system: another alternative for computer communications," in *Proceedings of the November 17-19, 1970, fall joint computer conference*, pp. 281–285, ACM, 1970.

[73] N. I. Osman and E. B. Abbas, "Simulation and modelling of lora and sigfox low power wide area network technologies," in *2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, pp. 1–5, Aug 2018.

[74] K. Srinivasan and P. Levis, "Rssi is under appreciated," in *Proceedings of the third workshop on embedded networked sensors (EmNets)*, vol. 2006, Cambridge, MA, USA., 2006.

[75] K. Benkic, M. Malajner, P. Planinsic, and Z. Cucej, "Using rssi value for distance estimation in wireless sensor networks based on zigbee," in *2008 15th International Conference on Systems, Signals and Image Processing*, pp. 303–306, IEEE, 2008.

[76] A. Prasad, K. Samdanis, A. Kunz, and J. Song, "Energy efficient device discovery for social cloud applications in 3gpp lte-advanced networks," in *2014 IEEE Symposium on Computers and Communications (ISCC)*, pp. 1–6, June 2014.

A. APPENDIX A: MATLAB CODE FOR THE FSL SIMULATION

```
clc;
clear all;
close all;

distance= 0:1:30; % distance to be measured
% Calculating Free space pathloss
FSL=32.4+20.*log10(distance)+20*log10(868);
d=5; % Distance between base station and end device
n=2;  % path loss exponent
rssi=122; % RSSI level
snr=20;  % Signal to noise ratio
ptx=14;  % Effective Isotropic Radiated Power
grx=0;   % Receiver's antenna gain
f=distance/d; % Just for simplification
% Calculating Normal sigfox based system pathloss
sigfox_path_loss= rssi+snr+ptx+grx+10*n*log10(f);
figure()
semilogx(distance,FSL,'b--o',distance,sigfox_path_loss,...
    'LineWidth',2);
title('Path Loss at Sigfox Radio Network')
xlabel('Distance in Logarithmic KM')
ylabel('Path loss [dB]')
ylim([80 180])
legend('FSL at 968MHz','Expected Path ...
   Loss','Location','southeast')
grid on
```

B. HEATMAP OF RSSI VALUES IN DIFFERENT BUILDINGS OF TAU, HERVANTA CAMPUS

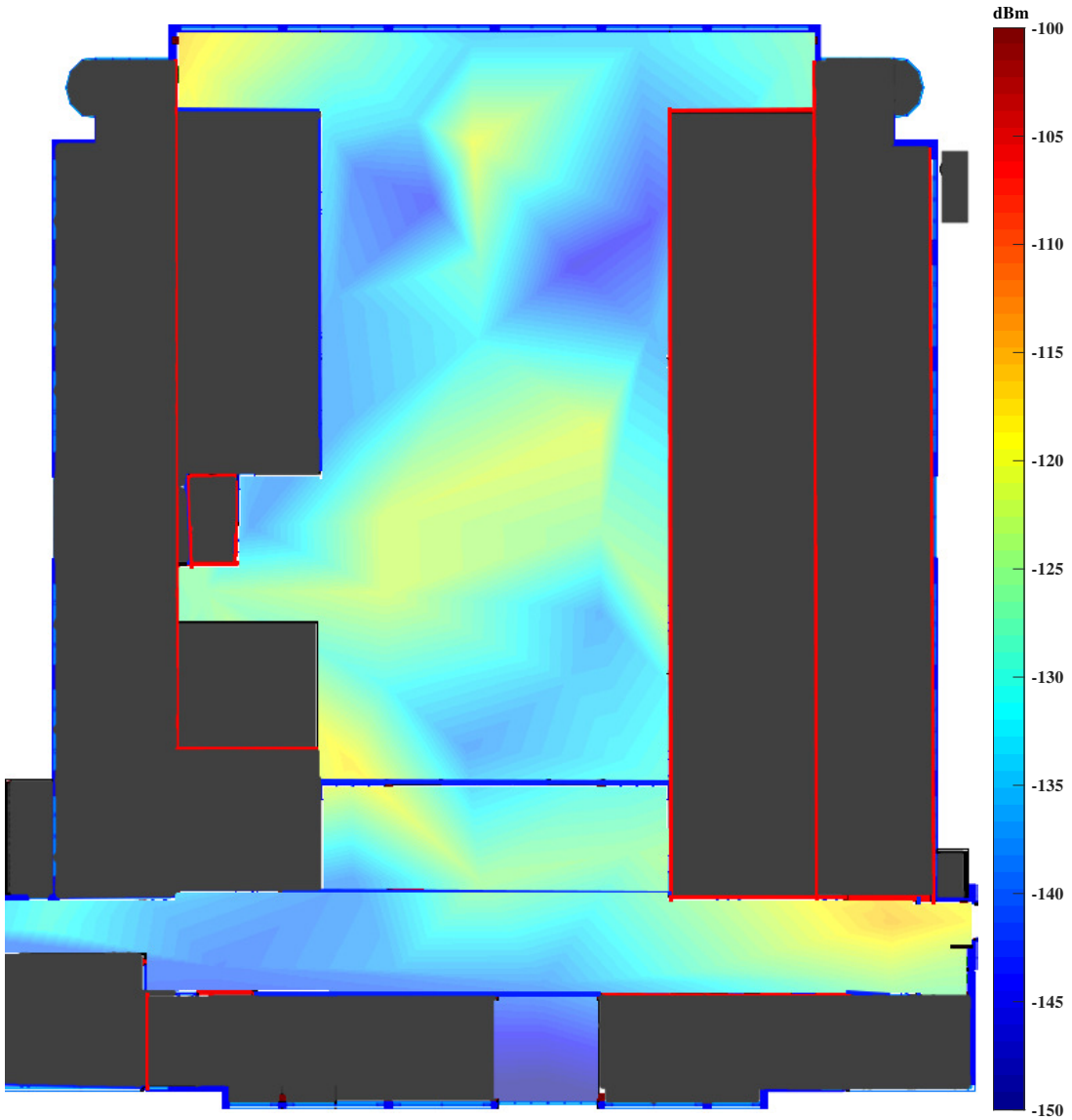


Figure B.1 *Heatmap of RSSI values in TAU Päätalo building (first floor), Hervanta campus.*

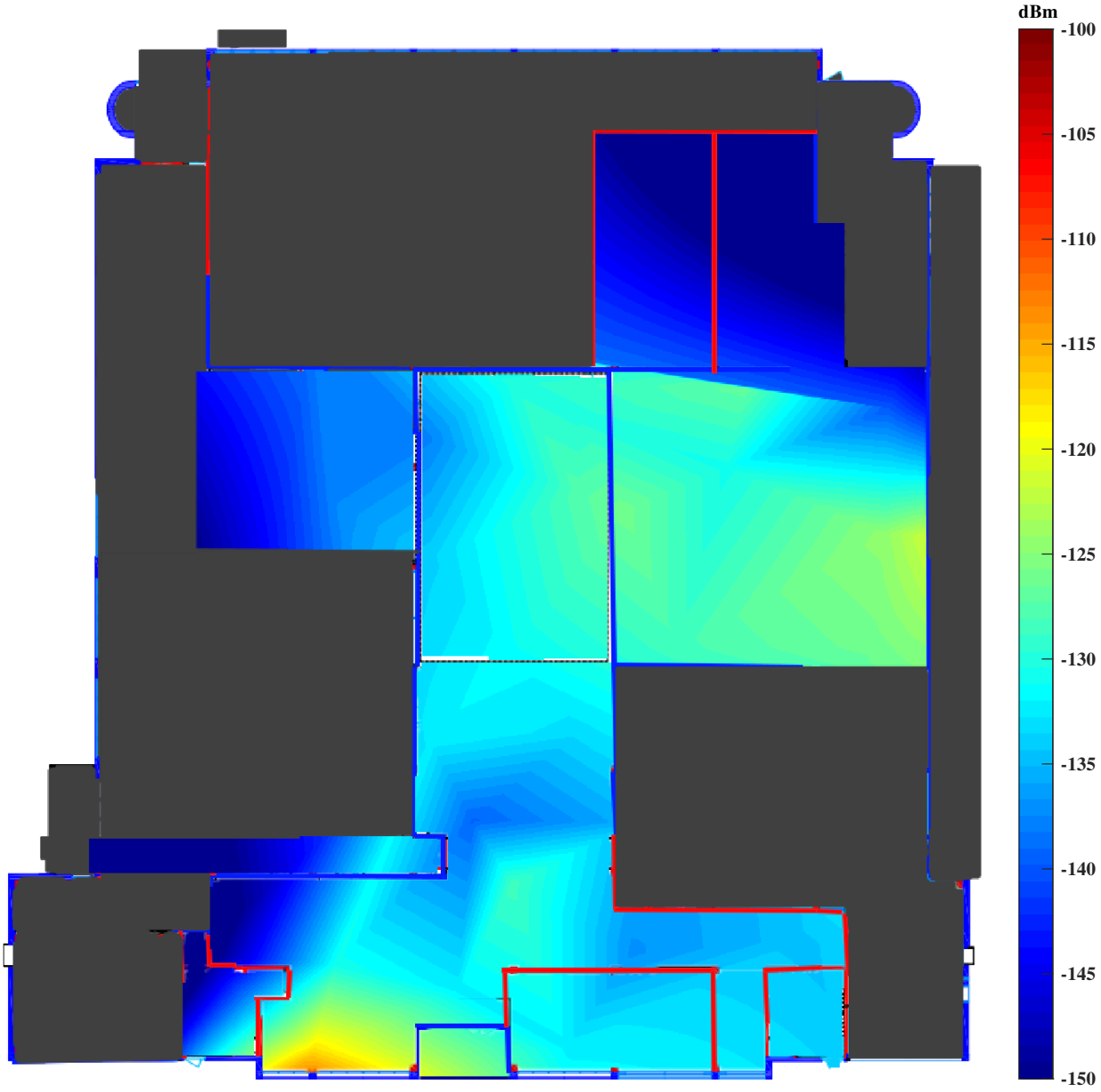


Figure B.2 *Heatmap of RSSI values in TAU Päätalo building (ground floor), Hervanta campus.*

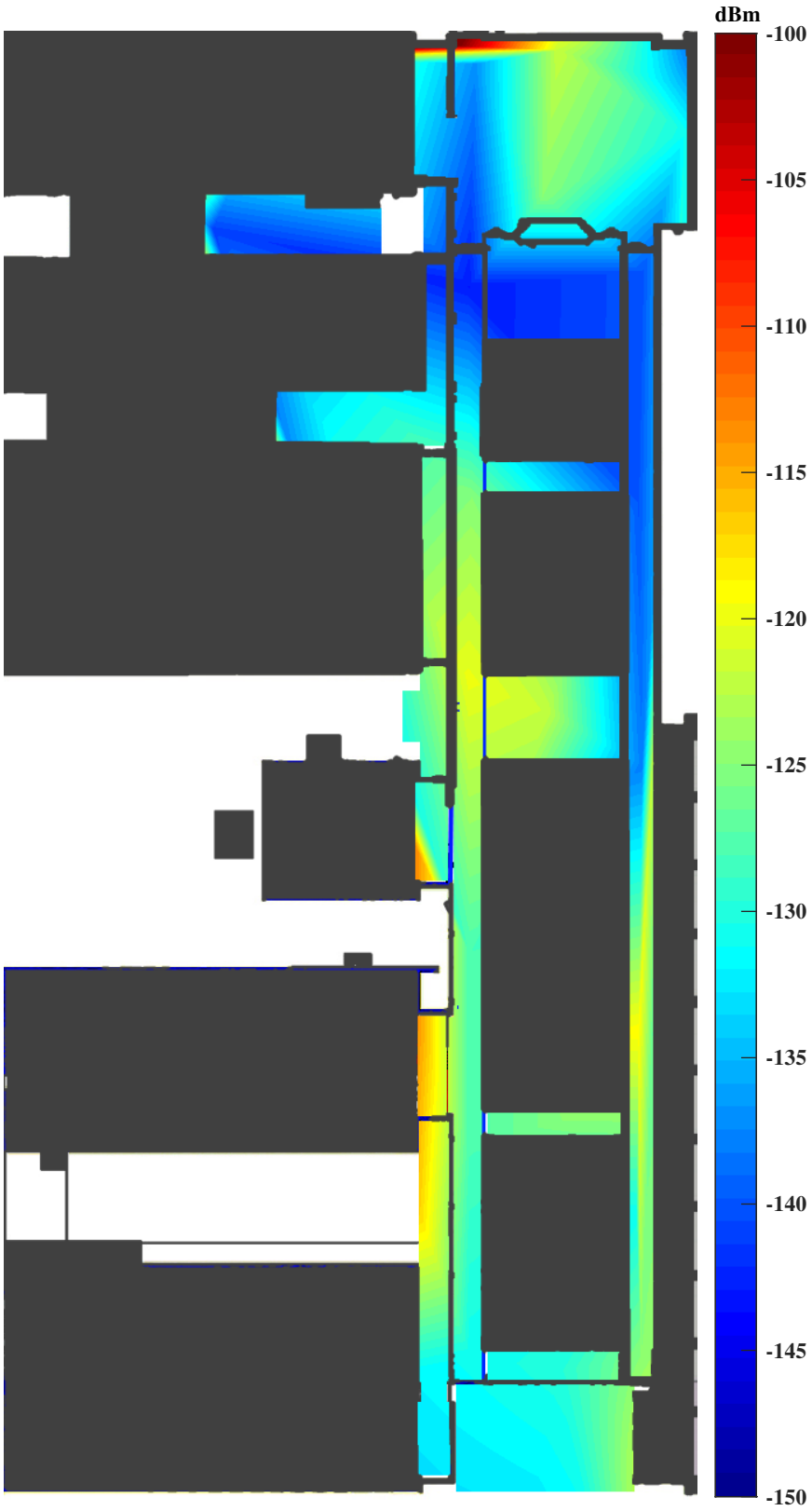


Figure B.3 *Heatmap of RSSI values in TAU Rakennustalo building (first floor), Hervanta campus.*

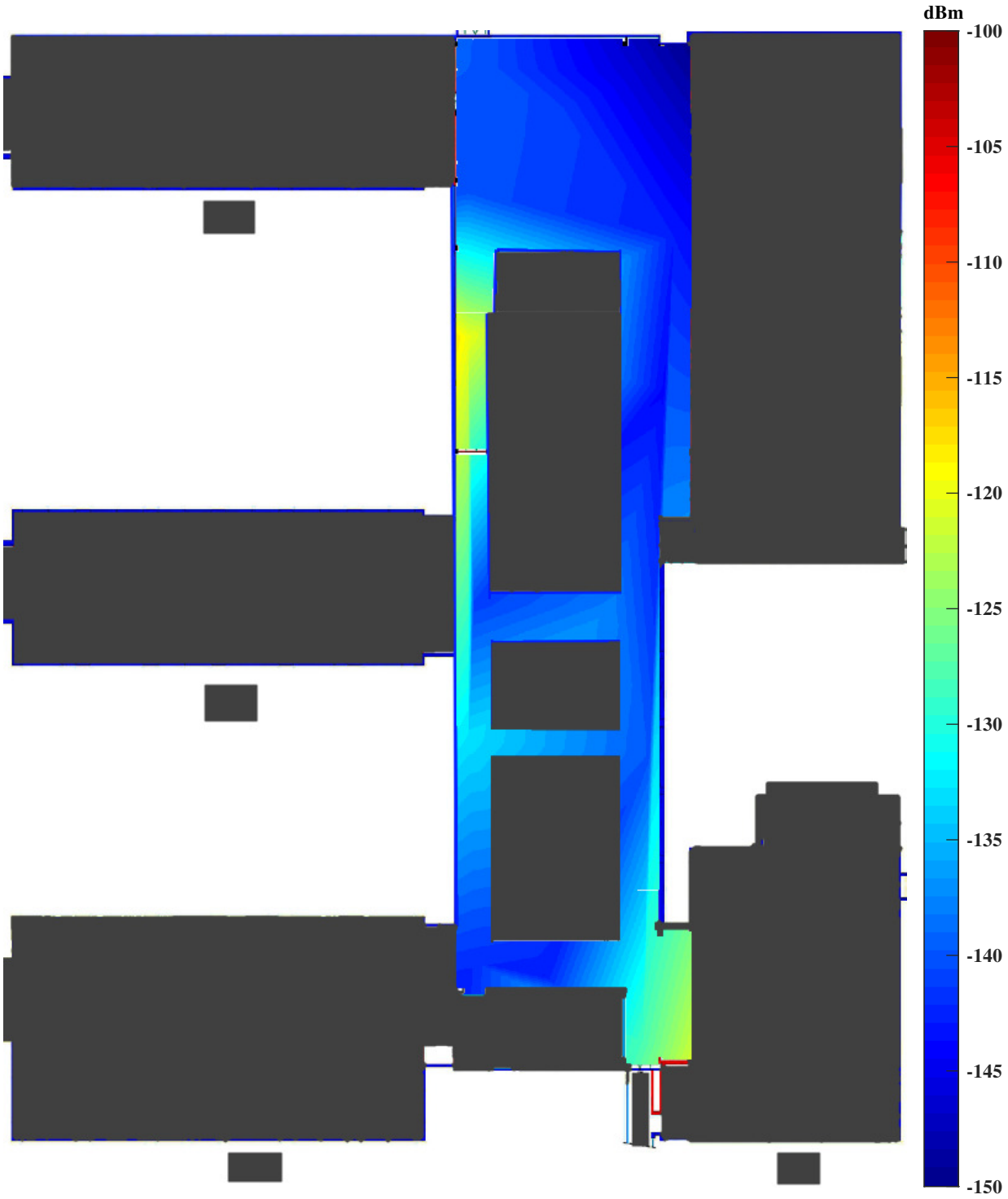


Figure B.4 *Heatmap of RSSI values in TAU Sähkötalo building (first floor), Hervanta campus.*

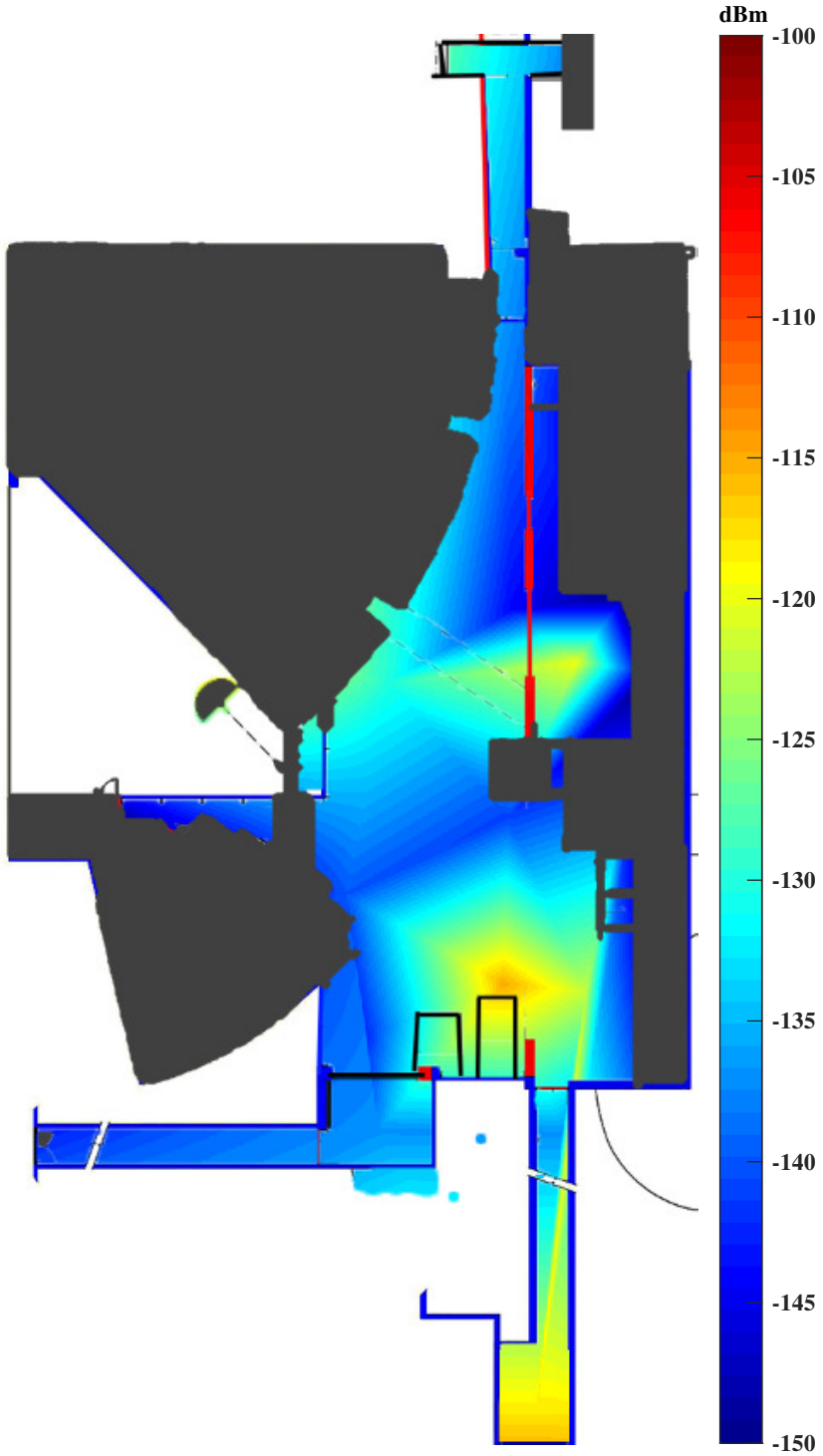


Figure B.5 *Heatmap of RSSI values in a part of TAU Festia building (first floor), Hervanta campus.*

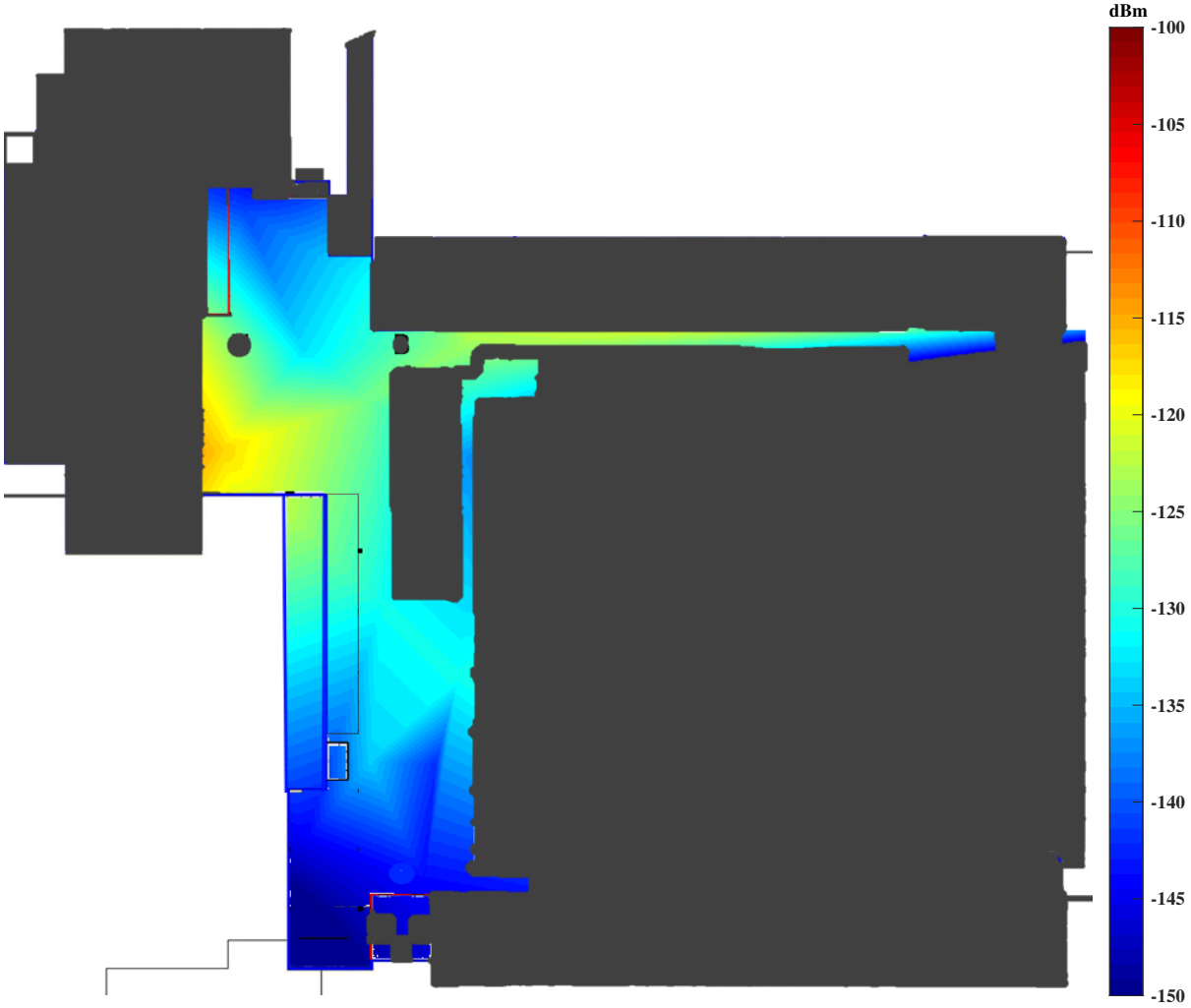


Figure B.6 *Heatmap of RSSI values in a part of TAU Konetalo building (first floor), Hervanta campus.*

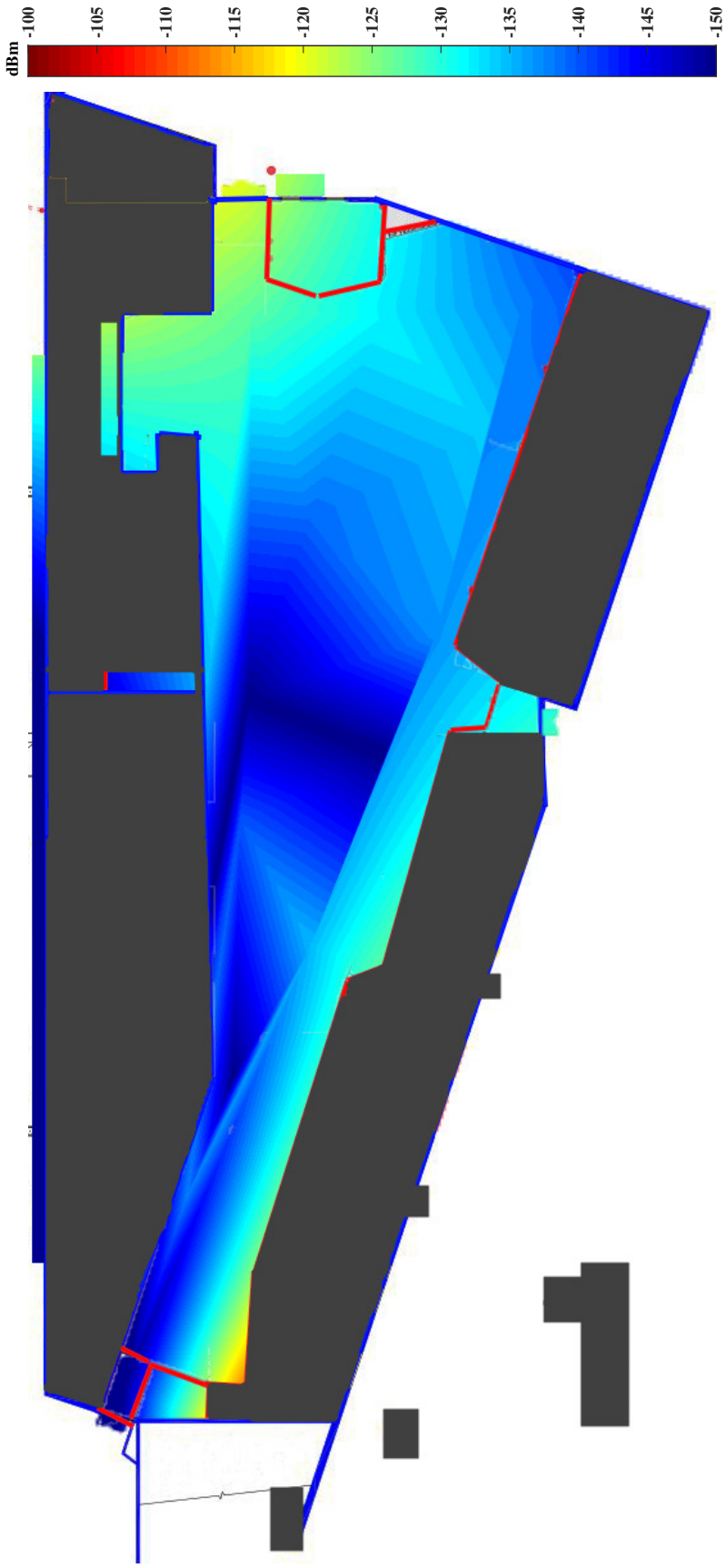


Figure B.7 *Heatmap of RSSI values in TAU Kampusareena (first floor) building, Hervanta campus.*

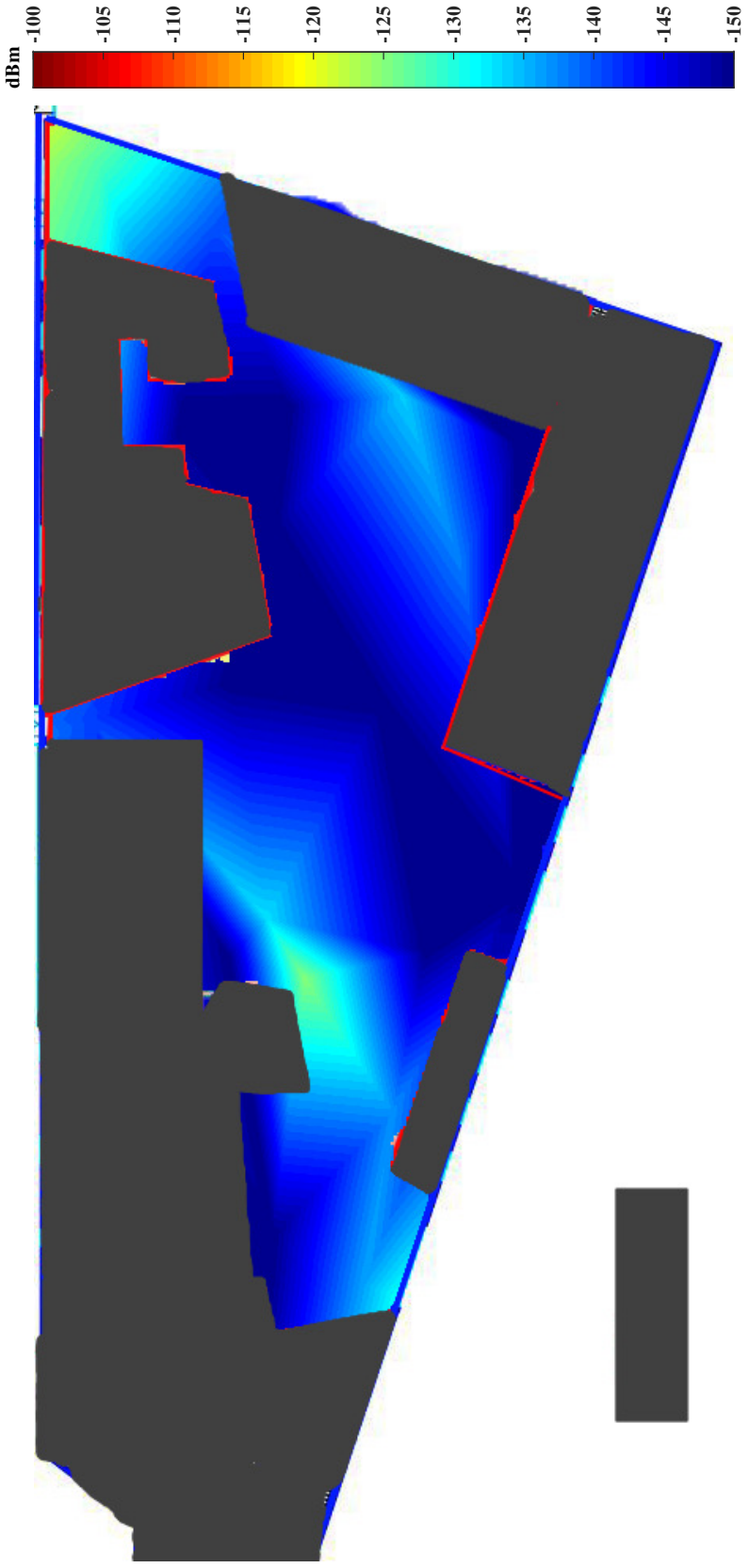


Figure B.8 *Heatmap of RSSI values in TAU Kampusareena (second floor) building, Hervanta campus.*