NOVA SCHOOL OF SCIENCE & TECHNOLOGY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

PAULO ANTÓNIO SOUSA GASPAR

PERFORMANCE ANALYSIS OF IOT WIRELESS CELLULAR SYSTEMS

MASTER IN ELECTRICAL AND COMPUTER ENGINEERING

NOVA University Lisbon
March, 2022

DEPARTMENT OF ELECTRICAL
AND COMPUTER ENGINEERING

PERFORMANCE ANALYSIS OF IOT WIRELESS CELLULAR SYSTEMS

PAULO ANTÓNIO SOUSA GASPAR

Adviser: Rodolfo Oliveira
Associate Professor with Habilitation, NOVA University Lisbon

MASTER IN ELECTRICAL AND COMPUTER ENGINEERING

NOVA University Lisbon
March, 2022

Performance Analysis of IoT Wireless Cellular Systems

Acknowledgements

First, I would like to express my sincere gratitude to my advisor, Professor Rodolfo Oliveira, for his insights into the subject and for his guidance in critical moments of decision making.

I would also like to thank Altice for providing the SIM cards that made this research possible.

I am very grateful to my parents for encouraging me to complete this work and giving me the opportunity to graduate. Without them, none of this would have been possible.

Finally, I would like to thank my friends who have been good listeners, especially in difficult moments, and have set a good example for me to follow.

Abstract

The Internet of Things (IoT) is becoming a reality and with it comes the need to support more devices with better coverage and low power consumption on the wireless network. One of the Low-Power Wide Wan (LPWA) technologies that aims to meet these requirements is Narrow-Band IoT (NB-IoT). NB-IoT is a 4G cellular technology particularly focused on IoT scenarios demanding for low throughput and very low energy consumption.

This dissertation investigates the capacity and performance of NB-IoT technology in real-world scenarios by comparing the results of measurements performed under different radio conditions around Lisbon's metropolitan area. Inspired by related works presented in the dissertation, the approaches adopted in this work are explained and the metrics collected are described in detail. Through practical measurements campaigns we characterize different metrics of NB-IoT performance for different propagation scenarios, identifying hypothetical causes for the observed performance.

Keywords: NB-IoT, real-world scenarios, radio conditions

Resumo

A Internet das Coisas (IoT) está a tornar-se uma realidade e com ela surge uma necessidade de albergar mais dispositivos com melhor cobertura e menor consumo de energia nas redes sem fios. Uma das tecnologias Low-Power Wide Area (LPWA) que visa atender a esses requisitos é Narrow Band IoT (NB-IoT). NB-IoT é uma tecnologia celular 4G particularmente focada em cenários de IoT que exigem baixo débito e baixo consumo de energia.

Esta dissertação investiga a capacidade e o desempenho da tecnologia NB-IoT em cenários do mundo real, comparando os resultados das medições realizadas sob diferentes condições de rádio na área metropolitana de Lisboa. Tomando como inspiração alguns trabalhos relacionados apresentados na dissertação, as abordagens adotadas neste trabalho são devidamente explicadas e as métricas descritas em detalhes. Através de medições práticas, são caracterizadas diferentes métricas de desempenho de NB-IoT para diferentes cenários de propagação, identificando causas hipotéticas para o desempenho observado.

Palavras-chave: NB-IoT, cenários do mundo real, condições de rádio

Contents

List of Figures **ix**

List of Tables **xii**

Acronyms **xiii**

1 Introduction **1**

1.1 Motivation . . . 1
1.2 Objectives . . . 2
1.3 Contributions . . . 2
1.4 Dissertation Structure . . . 2

2 NB-IoT Standard: brief overview **4**

2.1 Motivation . . . 4
2.2 Physical Layer . . . 5
2.2.1 Resource Organization . . . 6
2.2.2 Downlink . . . 7
2.2.3 Uplink . . . 12
2.2.4 Protocol Stack . . . 15
2.2.5 System Information . . . 16
2.2.6 Cell Selection . . . 16
2.2.7 Random Access Procedure . . . 17
2.2.8 Connection Control . . . 17
2.2.9 Capability Tranfer . . . 18
2.3 Core Network and Data . . . 19
2.3.1 Control Plane CIoT Optimisation . . . 19
2.3.2 User Plane CIoT Optimisation . . . 20

3 Related Works **22**

3.1 Uplink, downlink and channel occupancy . . . 22

3.2 NB-IoT vs LoRaWAN 23
3.3 Real-Time Demand-Response Application 26
3.4 Evaluation of NB-IoT Energy Consumption 28

4 Evaluation Setup **31**
4.1 NB-IoT Device 31
4.2 Metrics Description 33
4.3 Evaluation 35

5 NB-IoT Performance Evaluation **36**
5.1 Data Collection Locations 36
5.1.1 Outdoor Parque Eduardo Sétimo 37
5.1.2 Outdoor Póvoa de Santo Adrião 37
5.1.3 Outdoor Vila Chã 37
5.1.4 Outdoor Sintra 38
5.1.5 Outdoor Parque das Conchas 40
5.1.6 Outdoor Cemitério do Lumiar 40
5.1.7 Outdoor Monsanto 40
5.1.8 Indoor Damaia 40
5.1.9 Deep Indoor Vila Chã 41
5.2 Results 42

6 Conclusions **46**
6.1 Final Remarks 46
6.2 Future Work 47

Bibliography **48**

List of Figures

2.1 Graphic representation of the three different Narrowband Internet of Things (NB-IoT) operation modes, adapted from [24]. 6
2.2 NB-IoT time resource division or frame division hierarchy adapted from [18]. These periods correspond to the downlink. 7
2.3 Slot structure or resource map for Downlink (DL), adapted from [16]. . . . 8
2.4 Resource mapping for NB-IoT reference signal when operating with one antenna port or two adapted from [18]. Blue corresponds to Antenna Port (AP)0 Narrowband reference signal (NRS) and pink to AP1 NRS. 9
2.5 Slot structure or resource map for Uplink (UL) when using 3.75 kHz spacing (48 subcarriers) and 15 kHz spacing (12 subcarriers), adapted from [16]. . 12
2.6 Example of the resource elements used in three preamble repetitions in a set of subcarriers, adapted from [24]. 13
2.7 Comparison between NB-IoT's and Long Term Evolution (LTE)'s protocol stacks, adapted from [25]. The blue colored blocks represent new or changed features. 15
2.8 Graphic representation of the connection states across time, adapted from [2]. The periods of eDRX both connected and idle and Power Saving Mode (PSM) can also be obseved. 18
2.9 Diagram of the NB-IoT core network. Blue represents the *User Plane* and red represents the *Control Plane*. Adapted from [18]. 19
2.10 UL data representation. (a) Resource Unit (RU) division. (b) Slot composition. (c) Transmission Sequence of the slots. Adapted from [18]. 21

3.1 Channel occupancy on UL and DL (left and right, respectively) for different realistic scenarios with different inter-site distances. From [7]. 23
3.2 Relation between traffic generated by the User Equipment (UE)s and free network resources and throughput for 500 m Inter-Site Distance (ISD) (left) and 100 m ISD (right). From [7]. 24
3.3 Active time and energy spent for transmitting 1, 5, and 10 packets (400 B per packet). From [2]. 25

3.4 Comparison between Long Range Wide Area Network (LoRaWAN) and NB-IoT battery life (in years) and Energy Per Byte (EPB) in DR0, DR2, and DR5 conditions for LoRa and Bad, Medium and Good coverage levels for NB-IoT. From [2]. 27
3.5 Average NB-IoT latency from Demand Response Server (DRS) to Demand Response Controller (DRC) for different message sizes and different radio conditions (0, 30, 60dB attenuation for outdoor, indoor, and deep indoor), adapted from [21]. 28
3.6 Pie chart of the energy consumption of different phases during the transmission of a 64 bytes User Datagram Protocol (UDP) packet. [15]. 29
3.7 Energy consumption pie chart of different phases during the transmission of 16, 64, 256, and 1024-bytes-long UDP packets.[15]. 30
3.8 Graphic representation of the total energy consumed with the transmission of a 16, 64, 256, and 1024-bytes-long UDP packet.[15]. 30

4.1 BC66-TE-B interface distribution diagram. [3] 32

5.1 Satellite image of the test site location in Parque Eduardo Sétimo with a yellow line between the base station and the module. The module is on the left side, the base station is on the right, and the distance between them is 404 meters. 37
5.2 Satellite image of the test site location in Povoa de Santo Adrião with a yellow line between the base station and the module. The module is on the left side, the base station is on the right, and the distance between them is 530 meters. 38
5.3 Satellite image of the test site location in Vila Chã with a yellow line between the base station and the module. The module is on the right side, the base station is on the left, and the distance between them is 2260 meters. 38
5.4 Three satellite images of the test site location in Sintra with a yellow line between the base station and the module. The second image is the same angle as the first one but has 3D buildings and foliage. The third image is the 2D view from above. The module is on the right side, the base station is on the left, and the distance between them is 2391 meters. The distance was obtained using the Haversine formula. 39
5.5 Satellite image of the test site location in Parque das Conchas with a yellow line between the base station and the module. The module is on the right side, the base station is on the left, and the distance between them is 2407 meters. 40
5.6 Satellite image of the test site location in Cemitério do Lumiar with a yellow line between the base station and the module. The module is on the right side, the base station is on the left, and the distance between them is 2967 meters. 41
5.7 Satellite image of the test site location in Monsanto with a yellow line between the base station and the module. The module is on the right side, the base station is on the left, and the distance between them is 3404 meters. 41

5.8 Three satellite images of the test site location in Damaia with a yellow line between the base station and the module. The second image is the same angle as the first but has 3D buildings and foliage. The third image is the 2D view from above. The module is on the right side, the base station is on the left, and the distance between them is 5558 meters. 42
5.9 Satellite image of the test site location in Vila Chã with a yellow line between the base station and the module. The module is on the right side, the base station is on the left, and the distance between them is 6516 meters. 43
5.10 Graphical representation of Received Signal Strength Indicator (RSSI), Reference Signal Received Quality (RSRQ) and RSSI in all 10 scenarios. 45
5.11 Graphical representation of the percentage of Signal-to-interference-plus-noise (SINR) and RSSI when compared to the best value across scenarios. 45
5.12 Block Error Rate (BLER) for the UL and DL in the MAC layer. 45

List of Tables

3.1 Average RSSI over 50 measurements for 10, 50, 100 and 400 bytes of payload size in three different defined coverage levels (Good, Medium, and Bad) [2]. 24

5.1 Results of the average measurements obtained for each scenario for the most important metrics on signal analysis for NB-IoT (RSSI, Reference Signal Received Power (RSRP), RSRQ, SINR). The scenario number corresponds to the subsection of numbers from the previous section, for example scenario 1 corresponds to the scenarios described in Subsection 5.1.1. 44

Acronyms

3GPP	3rd Generation Partnership Project 4, 34, 35, 43, 46
AP	Antenna Port ix, 8, 9, 10, 31
API	Application Programming Interface 29, 35, 36, 41
ARQ	Automatic Repeat Request 34
BER	Bit Error Rate 33, 35
BLER	Block Error Rate xi, 34, 44, 45
BS	Base Station 36, 37, 40, 42, 44
CoAP	Constrained Application Protocol 47
CQI	Channel Quality Indicator 35
CRS	Cell Specific Reference Signal 8, 10, 34
DL	Downlink ix, xi, 5, 6, 7, 8, 11, 12, 14, 19, 20, 21, 44, 45, 47
DMRS	Demodulation Reference Signal 12, 14
DRC	Demand Response Controller x, 26, 28
DRS	Demand Response Server x, 26, 28
DRX	Discontinuous Reception Cycle 32
eDRX	extended Discontinuous Reception Cycle 25, 28, 29, 32
eNodeB	Evolved Node B 28, 33
EPB	Energy Per Byte x, 25, 26, 27
FDD	Frequency Division Duplexing 5
GSM	Global System for Mobile Communications 1, 4, 5

HARQ Hybrid Automatic Repeat Request 34
HF Hyper Frame 6, 7, 11

IoT Internet of Things 1, 2, 4, 5, 19, 26
ISD Inter-Site Distance ix, 22, 23, 24

KPI Key Performance Indicator 1, 22, 25, 35

LoRaWAN Long Range Wide Area Network x, 23, 25, 27
LPWA Low Power, Wide Area 1
LPWAN Low Power, Wide Area Network 4, 24, 26, 46, 47
LTE Long Term Evolution ix, 4, 5, 6, 8, 9, 10, 11, 12, 14, 15, 16, 17, 19, 25, 26

MCL Maximum Coupling Loss 1
MIB-NB Master Information Block 8, 9, 10, 11, 16, 18
mMTC massive Machine Type Communications 5
MQTT MQ Telemetry Transport 29, 35, 42, 47
MQTT-SN MQTT For Sensor Networks 29

NAS Non-access stratum 15, 16, 19
NB-IoT Narrowband Internet of Things ix, x, xii, 1, 2, 4, 5, 6, 7, 8, 9, 12, 14, 15, 16, 17, 19, 22, 23, 24, 25, 26, 27, 28, 29, 31, 33, 35, 36, 43, 44, 46, 47
NCellID Narrowband Cell ID 8, 9, 11, 13, 16
NLoS Non-Line-of-Sight 37
NPBCH Narrowband physical broadcast channel 7, 9
NPDCCH Narrowband physical downlink control channel 7, 10, 11, 14, 20
NPDSCH Narrowband physical downlink shared channel 7, 10, 11, 14
NPRACH Narrowband Physical Random Access Channel 12, 22, 23
NPSS Narrowband primary synchronization signal 7, 8, 9
NPUSCH Narrowband Physical Uplink Shared Channel 7, 10, 11, 12, 14, 22, 34
NRS Narrowband reference signal ix, 7, 8, 9, 10, 16
NSSS Narrowband secondary synchronization signal 7, 8, 9, 16

OFDM Orthogonal Frequency Division Multiplexing 33
OFDMA Orthogonal Frequency Division Multiple Access 6, 7

PCI Physical Cell ID 8
PRB Physical Resource Block 6, 7, 9, 16, 34
PSM Power Saving Mode ix, 18, 24, 25, 28, 29, 32

QoS Quality of Service 23, 26

RAP Random Access Procedure 14
RE Resource Element 6, 7, 8, 9, 12, 34
RF Radio Frame 6
RRC Radio Resource Control 10, 15, 17, 19, 20, 29
RSRP Reference Signal Received Power xii, 33, 34, 35, 36, 44
RSRQ Reference Signal Received Quality xi, xii, 33, 34, 35, 36, 44, 45
RSSI Received Signal Strength Indicator xi, xii, 24, 25, 28, 34, 35, 36, 43, 44, 45, 46, 47
RTC Real Time Clock 32
RU Resource Unit ix, 7, 14, 20, 21

SC-FDMA Single Carrier Frequency Division Multiple Access 6, 12
SF Subframe 5, 6, 7, 8, 9, 10, 11, 12, 17, 20, 21
SFN System Frame Number 6, 7
SIB System Information Block 16, 21
SIB1-NB System Information Block Type-1 9, 11, 16
SINR Signal-to-interference-plus-noise xi, xii, 34, 35, 43, 44, 45
SoA State-of-the-art 46
SRB Signaling Radio Bearer 15, 16, 17, 20

TAU Tracking Area Update 18, 29
TCP Transmission Control Protocol 29, 35, 47
TDMA Time Division Multiple Access 33

UART Universal asynchronous receiver-transmitter 31
UDP User Datagram Protocol x, 29, 30, 47
UE User Equipment ix, 5, 6, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 28, 29, 33, 34, 35, 46, 47
UL Uplink ix, xi, 5, 6, 7, 10, 11, 12, 14, 20, 21, 44, 45
USIM Universal Subscriber Identity Module 31

WLAN Wireless Local Area Network 26

1

Introduction

The ideas and possibilities that can arise from devices connected to a wireless network are immense. But sometimes technology is just not there yet. Thankfully, technology evolved, and radio equipment costs reduced, making it possible to build small "things" with the capability to perform radio communication (a simple sensor that sends information over radio to a wireless sensor network, for example). These "things" gave birth to the concept of the Internet of Things (IoT) and with it came the prediction of an exponential increase in the number of devices connected to the Internet. IoT can have a wide variety of applications, ranging from the industry to smart cities and smart buildings, alarm systems, waste management and many other services. For that reason, there is a growing demand for Low Power, Wide Area (LPWA) Services capable of supporting long-range low power communications [9].

1.1 Motivation

IoT applications need to find novel technologies supported in licensed bands to enable a high number of devices on a national coverage level with guaranteed QoS. In order to address this issue, a set of requirements must be met:

- Reliability, in [16] as being the most important key Key Performance Indicator (KPI) and directly influenced by the success rate of power outage notifications.
- Improved link budget, since certain applications will need high coverage performance. This performance is measured by the Maximum Coupling Loss (MCL), which is 164 dB (+20 comparing with Global System for Mobile Communications (GSM)) for NB-IoT [5], better than competing technologies;
- Scalability, like the capacity to work alongside existing technologies without the need of dedicated gateways and networks [10];
- Low power consumption and better efficiency;

NB-IoT is a good approach to these requirements. For that reason, an investigation on its effective performance, particularly in terms of radio reliability, delay (access to the core), and capabilities to support differentiated IoT services, will be conducted.

1.2 Objectives

The main goal of this work is focused on the understanding and experimentation of the NB -IoT technology and its performance evaluation in different practical scenarios.

To begin with, it is necessary to understand how the technology works. For this reason, the physical layer and the core network will be explored, identifying and describing the main processes involved. In addition, similar works on this technology will be analyzed.

The collected information will then be used to statistically analyze the data retrieved from a device in a real-world scenario.

1.3 Contributions

This contributions of this work are summarized as follows:

- a study of the operation and main technical features of NB-IoT is carried out and presented in Chapter 2;
- we describe the most common performance metrics available in experimental NB-IoT devices, capable of gathering information about the network's performance for further processing;
- we propose and describe multiple practical scenarios of interest, which are used for evaluation of the NB-IoT network;
- a characterization of the performance achieved in the multiple NB-IoT scenarios is provided, and possible causes for the observed performance are introduced.

1.4 Dissertation Structure

The dissertation is divided into six chapters.

The first chapter introduces the meaning of IoT and explains why LPWA technologies are necessary to meet its requirements.

The second chapter addresses the current state of the art in regard to the NB -IoT standard. An overview of all physical layer components is given and the organization of resources, all channels and signals for downlink and uplink, and all procedures for connection establishment, configuration and data transmission are explained.

Throughout the chapter, it is explained how the technology helps to reduce energy consumption and improve coverage. The core network and user and control pane optimisations are explained, and a brief comparison is made between LTE and the NB -IoT protocol stack.

Chapter 3 covers related work that provides knowledge and perspectives on other technologies and approaches to the performance evaluation. Some work can also serve as a basis for expected performance in terms of coverage levels and metrics for NB -IoT.

Chapter 4 describes the approaches and methods used to assess technology performance and explains how the metrics are collected and what they represent. The hardware and software used are also described.

The fifth chapter contains the results of the study conducted. Several scenarios were proposed and described in detail. The data collected was then compared to data from previous work as well as between scenarios and used to derive some assessments about the technology.

The sixth and final chapter provides insight into the work done, highlights what did not go as expected, and proposes solutions for future research.

2

NB-IoT Standard: brief overview

2.1 Motivation

IoT applications are getting increasingly popular and the number of devices connected to the network will raise exponentially. Unfortunately, LTE does not present a solution for this matter. If we used it to connect that many devices to the network the result would be a network overload because even if the amount of data they generate is small, the amount of signalling is the same, as stated in [18], and the coverage does not fit the requirements of the typical IoT applications. For this reason, it is necessary to prepare our current cellular network to handle so many devices with these specifications.

The NB-IoT is a relatively new radio technology which aims to address this issue while also offering additional features (optimizations) to better fit the necessities of machine type communication devices.

The Radio Access Network Plenary Meeting 69 of the 3rd Generation Partnership Project (3GPP) took place in September 2015 and with it came the decision of standardizing the technology [8]. The core specifications and physical specifications were completed in June and October of 2016 (3GPP Release 13, LTE Advanced Pro), respectively. It falls under the Low Power, Wide Area Network (LPWAN) category alongside Sigfox and LoRa but unlike these it works with licenced spectrum and can take advantage of the already available GSM and LTE infrastructure.

The main objective of the NB-IoT is to facilitate and optimize machine type traffic for devices that:

- are typically stationary, which means it offers little to no support for handovers;
- need a very large battery life (around 10 years) and therefore need low power consumption since they are usually placed in places of difficult access;
- only need to transfer small amounts of data and do not use all the resources available on the network (sensors sending information from time to time, maybe even just once a day or less);

- often need to operate in extreme radio conditions from low coverage zones like basements;
- need to be low cost, in order to build lots of UEs capable of using it;

To support these devices a set of requirements was specified for the NB-IoT, as defined in [18]:

- Minimize the signalling overhead, especially over the radio interface;
- Appropriate security to the complete system, including the core network;
- Improve battery life;
- Support delivery of IP and non-IP data;
- Support of SMS as a deployment option;

It works in compatibility with LTE and in order to fulfil these requirements, the technology must simplify the communications as much as possible, removing the unused capabilities of the LTE and adding new features to support new applications. In addition to this, NB-IoT also makes LTE capable of handling a massive number of devices (massive Machine Type Communications (mMTC)) which fits one of the main requirements of the IoT.

2.2 Physical Layer

The communication type normally used in LTE is Frequency Division Duplexing (FDD) which means that the UL and DL are transmitted at different frequencies simultaneously. NB-IoT, however, works on half-duplex FDD type B that also uses different frequencies for DL and UL but cannot transmit simultaneously and needs to respect a guard period of one Subframe (SF) when alternating between UL and DL. Using this scheme helps reduce the cost and complexity of the UEs [18].

NB-IoT offers three different operation modes or deployment options:

- Standalone operation/carrier: for dedicated spectrum [4] or reusing GSM frequencies;
- In-band: utilizing LTE's resource blocks;
- Guard-band: reusing the LTE's guard-band resource block;

The operation mode should be transparent to the UE and it learns the mode and cell identity through initial acquisition. NB-IoT requires a minimum bandwidth of 180 kHz (the same as an LTE resource block) and when replacing GSM carriers (200 kHz) there is a guard-band interval of 10 kHz at each side. Also, when working in-band there is a restriction to the Physical Resource Block (PRB)s that NB-IoT devices can use for cell connection and that depends on the LTE system bandwidth. It may even be impossible to use any PRBs if the bandwidth is too low (1.4 MHz for example).

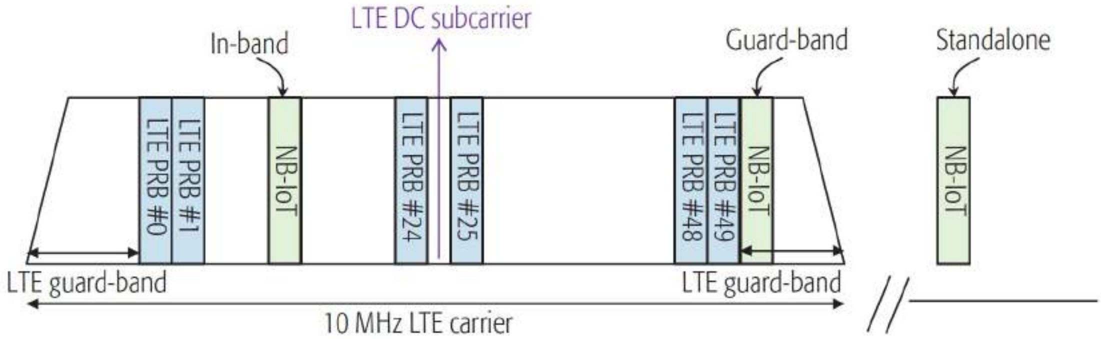

Figure 2.1: Graphic representation of the three different NB-IoT operation modes, adapted from [24].

In Figure 2.1 we have an example of the different operation modes in a 10 MHz LTE carrier. It is important to understand that certain PRBs cannot be used for cell acquisition by NB-IoT because they are specifically allocated for LTE. The six PRBs in the middle (in this case from PRB 22 to 27), for example, cannot be used because LTE occupies most of their Resource Element (RE)s with synchronisation and broadcast signals. For a PRB to be used as an NB-IoT anchor carrier (intended to facilitate UE initial synchronization) it cannot be more than 7.5 kHz away from a 100 MHz grid over the LTE carrier and the same happens for the guard-band operation mode because NB-IoT UEs have a search raster of 100 kHz and support a maximum offset of 7.5 kHz [24]. Knowing that the centre of PRB 25 is at 97.5 kHz in the grid, we can estimate that every five PRBs (900 kHz) there is a subcarrier that fits the band distance requirement (the same reasoning applies to PRB 24 and under). This means that PRB 30, 35, 40 and 45 are available for NB-IoT cell connection (specifically for 10 MHz bandwidth).

2.2.1 Resource Organization

The transmission scheme applied in the DL is the Orthogonal Frequency Division Multiple Access (OFDMA) with a 15 kHz spacing. This grants a good coexistence performance with LTE because it uses the same scheme [24]. NB-IoT UL works differently and it uses Single Carrier Frequency Division Multiple Access (SC-FDMA). Although slot structure is different between the UL and the DL, there is a common structure on which both are based. The biggest block is the Radio Frame (RF). Every 1024 RFs represent a System Frame Number (SFN) period and with every period the Hyper Frame (HF) number increases by 1. RFs are composed by 10 subframes (SF) and every SF is divided into 2 slots. For the DL the slot time is 0.5 ms as it can be seen in Figure 2.1. This means that the SFN period is 10.24 seconds and the HF period is around 3 hours [18]. For the UL a slot lasts 2 ms and there is also a new block called RU whose structure depends on the Narrowband Physical Uplink Shared Channel (Narrowband Physical Uplink Shared Channel (NPUSCH)) format and the subcarrier spacing used, as will be explained later in the document.

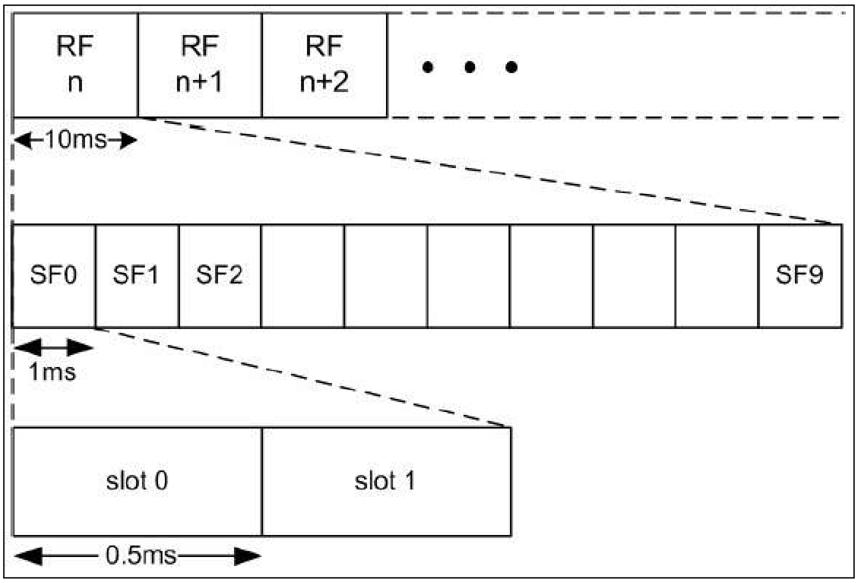

Figure 2.2: NB-IoT time resource division or frame division hierarchy adapted from [18]. These periods correspond to the downlink.

2.2.2 Downlink

We should start by describing the slot structure for the DL. Note that one slot occupies 0.5 ms in time (7 OFDMA symbols) and one PRB in frequency (180 kHz with 15 kHz spacing makes 12 subcarriers) creating the resource element (RE) grid as shown in Figure 2.3.

Knowing this we can estimate that every SF (2 slots) has 168 (12 subcarriers times 14 symbols) REs available.

NB-IoT DL is based on three physical signals and three physical channels [24]:

- Narrowband primary synchronization signal (NPSS)
- Narrowband secondary synchronization signal (NSSS)
- Narrowband reference signal (NRS)
- Narrowband physical broadcast channel (NPBCH)
- Narrowband physical downlink control channel (NPDCCH)
- Narrowband physical downlink shared channel (NPDSCH)

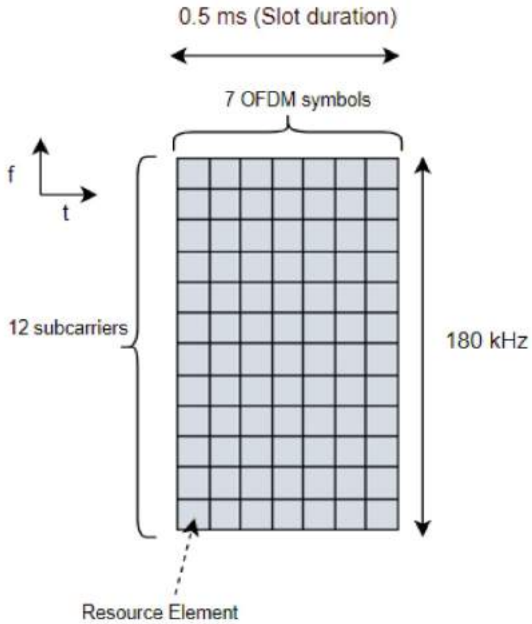

Figure 2.3: Slot structure or resource map for DL, adapted from [16].

In contrast with LTE, there is no need for Multimedia Broadcast Multicast Service (MBMS) and so the Physical Multicast Channel (PMCH) was removed [18].

2.2.2.1 NRS

The NRS is used for phase reference [24] and works similarly to LTE's Cell Specific Reference Signal (CRS). It is transmitted in all SFs except the ones carrying synchronization signals (NPSS and NSSS) and the ones that are not broadcast or DL dedicated. Even though NB-IoT has its own reference signal, it still needs to account for LTE's CRS when working in-band and because of this some REs may have to be skipped. It can also work with one Antenna Port (AP) or two. As an example, we can see in Figure 2.4 what REs are used by the NRS in the two different cases possible. The position of these REs does not change in the time domain but may shift in frequency depending on the Narrowband Cell ID (NCellID). In case the NCellID is equal to the Physical Cell ID (PCI) used in LTE, then the UE may use the CRS instead of the NRS since there is a parameter called *operationMode* in the Master Information Block (MIB-NB), which will be explained later, that indicates it. In addition, when using two antennas, in every NRS for AP0, the elements corresponding to the other antenna (AP1) are set to 0 and the same happens in every NRS for AP1 [18].

2.2.2.2 NPSS and NSSS

The NPSS and NSSS are synchronization signals that allow the UE to search for a cell and know its identification. They are also used to adjust time and frequency in the UE.

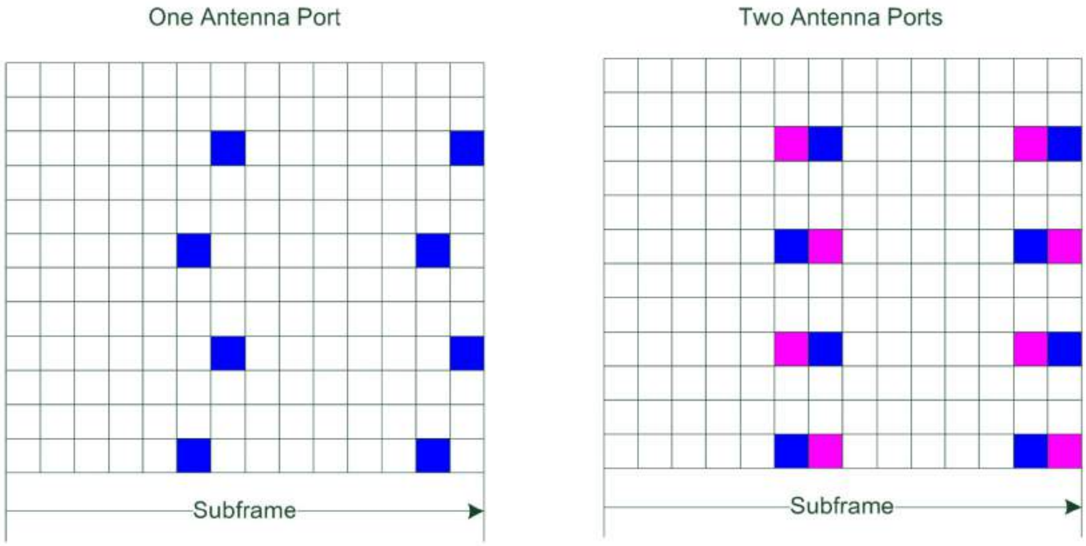

Figure 2.4: Resource mapping for NB-IoT reference signal when operating with one antenna port or two adapted from [18]. Blue corresponds to AP0 NRS and pink to AP1 NRS.

Legacy LTE has its own synchronization signals and they occupy 6 PRBs in one radio frame [24]. For that reason, NPSS is transmitted in every SF5 (of the 10 SFs starting at SF0) and NSSS is transmitted in SF9 but only on even number frames which means NSSS is repeated every 20 ms whereas NPSS is repeated every 10 ms. The first 3 columns or symbols of the resource map are not used because, in in-band mode, they are already used to transmit PDCCH for LTE and when the UE is searching for a cell it may not know the operation mode yet. To generate the signals a Zadoff-Chu (ZC) sequence is used. NPSS requires a length-11 ZC sequence and will be transmitted only in the frequency domain (one column of the resource map or one symbol) with each sequence mapped to the lowest 11 subcarriers of one of the available symbols. This way the UE can detect frames position in order to synchronize. NSSS uses a length-131 sequence multiplied with a binary scrambled sequence to be generated and is transmitted in all the 132 REs (11 symbols times 12 subcarriers). From these values the UE derives the NCellID [18].

2.2.2.3 NPBCH

NPBCH is transmitted in the first SF of every radio frame (excluding, again, the first 3 symbols) and carries the master information block (MIB-NB). MIB-NB contains different types of useful information like the operation mode, system information, System Information Block Type-1 (SIB1-NB) (explained further ahead) scheduling and size, among others. It is composed of 34 bits and spans over 640 ms of transmission. Before being sent, MIB-NB is separated into 8 different blocks (BL) and each of those blocks, one at a time, is repeatedly sent on the first SF of 8 radio frames in a row. This way, MIB-NB is transmitted without risk of collision with LTE when working in in-band mode. Note that the UE assumes that the NRS and the CRS have 2 and 4 APs defined, respectively, since it only learns AP information through MIB-NB [18].

2.2.2.4 NPDCCH

The next two channels, NPDCCH and NPDSCH are considered dedicated channels and SFs are assigned to them via a bitmap from the Radio Resource Control (RRC) signalling. They have a similar structure and are mapped taking into account the NRS and CRS. The first one is a control channel mainly responsible for scheduling information [24]. It contains paging and system information and indicates which UE should read data from NPDSCH, which SFs carry it and how many times it is repeated. This channel also carries UL schedule information, showing the UE which resources should be used to send data. A parameter, I^Nstart, is defined with the objective of indicating the first symbol for the UE to start reading the channel, avoiding collision with LTE's control channel for in-band operations. In the other operation modes, the value of the parameter is, by default, 0 providing more resources to use [18].

NPDCCH also defines two narrowband control channel elements (NCCE) with two different formats. The NCCE0 corresponds to the lowest 6 subcarriers of the SF and the NCCE1 to the remaining. Format 0 takes one NCCE (but allows two per SF to be transmitted) and format 1 takes both NCCEs.

The channel is also grouped in three search spaces to facilitate UEs search for control information. Type-1 common search space, for paging, Type-2, for random access, and the UE specific search space. RRC plays an important role here because it defines a limit for how many times NPDCCH may be repeated and provides the Type-2 and UE specific search spaces. Type-1 common search space is provided by the paging opportunity SFs.

Each UE will have three unique radio network temporary identifiers (RNTIs) for random access (RA-RNTI), paging (P-RNTI) and one specific for the UE (C-RNTI). These identifiers are obtained through NPDCCH's cyclic redundancy check (CRC) and if they match UE's RNTI then the channel information is decoded.

Three different downlink control indicator (DCI) formats are defined. N0, 23 bits related to UL, N1, 23 bits containing the NPDSCH scheduling and RACH procedure initiation, and N2, 15 bits for paging and direct indication. The UE differentiates formats by the way CRC scrambles with RNTIs. When CRC is scrambled with P-RNTI, format N2 is implicit. When it is scrambled with C-RNTI, the first bit tells if it is format N0 or N1. And finally, when it is scrambled with RA-RNTI, NPDCCH comes in format N1 containing only the random access response (RAR) information.

There is also a scheduling delay for NPDSCH, NPUSH and format N2 direct indications to be transmitted after the NPDCCH transmission. The delay's information can be found in the N0 and N1 DCI formats and it is, normally, 5 SFs for the NPDSCH, 8 for the NPUSCH and 10 for DCI format N2.

2.2.2.5 NPDSCH

As previously stated, NPDSCH assumes a similar structure to NPDCCH. It is a traffic channel that carries system information, paging and RAR messages, and uses a tail-biting convolutional code (TBCC) to reduce UE complexity [24]. It has a maximum transport block size (TBS) of 680 bits and uses specific parameters to span that transport block over N_{SF} frames and to be repeated N_{Rep} times. These values can be found in the DCI [18].

This channel supports the transmission of the system information block type-1 (SIB1-NB). Mapped like the MIB-NB, with a period of 256 radio frames and a variable TBS of 208, 328 and 680 depending on the number of repetitions (4, 8 and 16 respectively), SIB1-NB is transmitted over NPDSCH in SF4 of every radio frame. SIB1-NB remains unchanged during 4096 frames (40.96 seconds) which is equivalent to 4 SFN. That mean the UE can look at the 2 LSBs of the hyper frame available in the MIB-NB to know if SIB1-NB changed. The starting radio frame depends on the number of repetitions and the NCellID. Changes in SIB1-NB are indicated by paging.

It is also important to mention that all the acknowledgements of DL transmissions are sent over the NPUSCH, an UL channel, and the timing and subcarriers for that purpose are indicated in the DCI.

Paging Messages

NPDSCH carries paging messages. These messages are intended for UEs in the RRC_IDLE mode and can indicate a system information change or a connection request. Each paging message contains a list of UEs that, upon receiving the message, know that they are being paged which triggers a connection setup. Additionally, UEs may learn that system information has changed and start checking SIB1-NB, as well as other SIBs for that information.

The discontinuous reception cycle (DRX cycle) found in SIB2-NB determine, along with the IMSI and USIM card, the paging frames (PFs) and paging occasions (POs) of a UE. These cycles may cover 128, 256, 512 or 1024 frames and are meant to help UEs save battery by only monitoring frames for paging within that period. Every UE has a different paging occasion. By knowing the HF the UE will only check paging frames within a paging time window (PTW) inside a HF period.

Legacy LTE introduced the DRX cycle, but NB-IoT can also take advantage of the extended DRX cycle (eDRX) which can go up to 3 hours. Devices that need to receive messages but have low uplink data, greatly reduce their power consumption with this feature. Devices using eDRX have 2 states, Connected-eDRX and Idle-eDRX. When a device is connected, it alternates between active listening and sleep periods for the duration of the Inactivity timer (set by eNodeB). Upon data transmission, the timer resets. When in Idle, the device tracks the downlink channel following the paging window (PW) keeping network synchronization and checking if it has data to receive. The duration of the Idle-eDRX is set by the PW period and is equal to two times that. [2]

2.2.3 Uplink

As stated before, in the UL, the scheme used is SC-FDMA and it can be used with a 15 kHz or 3.75 kHz spacing. 15 kHz spacing results in 12 subcarriers and so the slot structure is similar to the DL. For the 3.75 kHz spacing 48 subcarriers are needed and the symbol duration increases 4 times. For that reason, the resource map changes and the slot length increases to 2 ms as we can see in Figure 2.5.

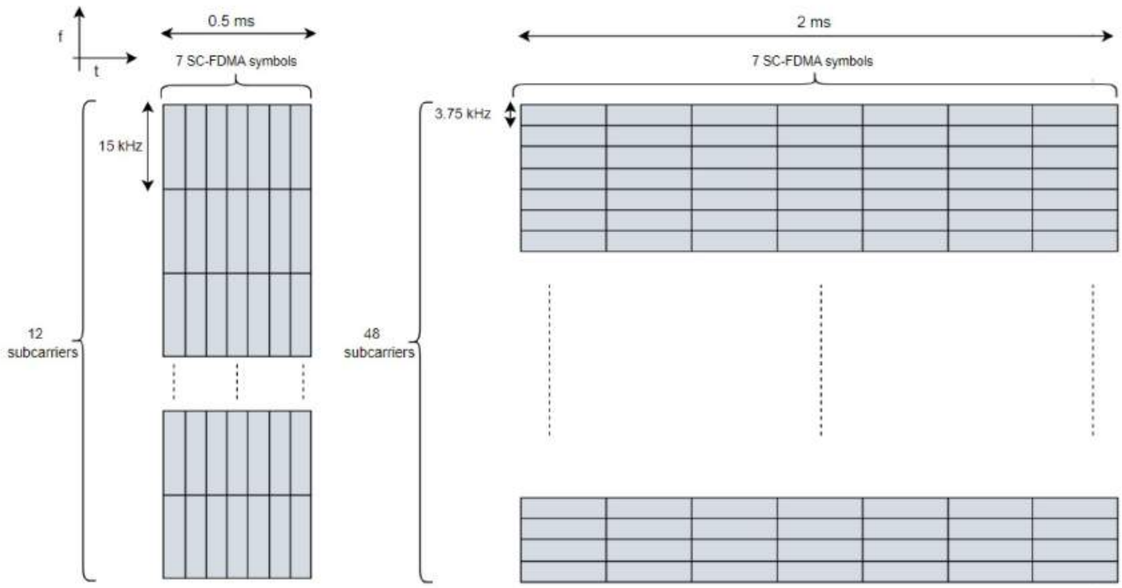

Figure 2.5: Slot structure or resource map for UL when using 3.75 kHz spacing (48 subcarriers) and 15 kHz spacing (12 subcarriers), adapted from [16].

The number of REs per SF in the UL, with a 3.75 kHz spacing, is much bigger than in a DL SF counting with 336 REs in just one SF. But UL SFs have a 4 ms duration whereas DL SFs only last 1 ms making the total number of REs in a 4 ms transmission equal for both cases.

NB-IoT UL has two physical channels and one signal:

- Narrowband Physical Random Access Channel (NPRACH)
- Narrowband physical uplink shared channel (NPUSCH)
- Demodulation Reference Signal (DMRS)

2.2.3.1 NPRACH

NPRACH had to be redesigned from legacy LTE because NB-IoT UL has less bandwidth available. It uses a preamble with 4 symbol groups and each group has one cyclic prefix

(CP) with two CP lengths defined, 66.67 µs (format 0) and 266.7 µs (format 1), and 5 symbols. Each symbol group is modulated on a different 3.75 kHz carrier introducing single-tone frequency hopping [24].

CP length changes with the format but the 5-symbol duration is always 1.333 ms. That makes a total length of 1.4 ms for format 0 and 1.6 ms for format 1. The UE may have to repeat the preamble 1, 2, 4, 8, 16, 32, 64, or 128 times and the number of repetitions changes with the coverage level. Normally, a contiguous set of 12 subcarriers is used for the frequency hopping but this number can change between 24, 36 and 48. In addition, resource allocation may be different for UEs that support multi-tone transmission and for UEs in different coverage enhancement (CE) groups [18].

As an example of the preamble repetition we can look to Figure 2.6. The orange rectangles represent one symbol group and four of them make one preamble. There are two different algorithms running. One of them just determines the subcarrier for the next 3 symbol groups to be transmitted (1 and 6 tone hopping). It depends, only, on the position of the first one and uses a ZC sequence. The second algorithm is the pseudo-random hopping that happens between repetitions. It depends on the NCellID and the repetition number. Both algorithms are designed in such a way that the hopping schemes never overlap.

NB-IoT also offers a mechanism of congestion control for occasions when a large number of devices try to access the network. This mechanism consists of triggering a backoff function on the RACH or using congestion status to apply access control, reducing the amount of signaling messages. [6]

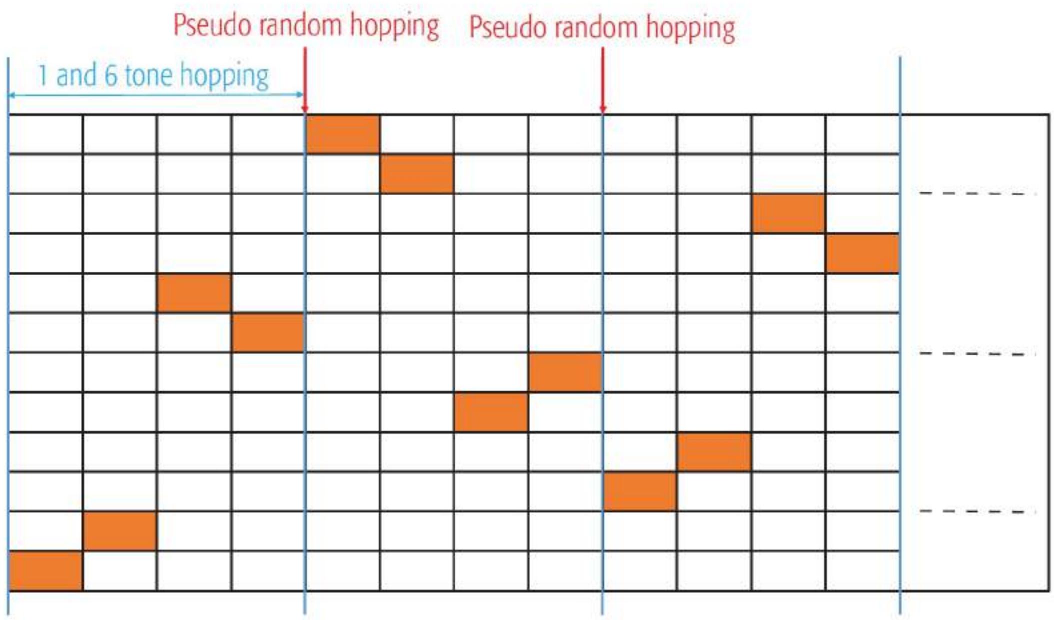

Figure 2.6: Example of the resource elements used in three preamble repetitions in a set of subcarriers, adapted from [24].

2.2.3.2 NPUSCH

NPUSCH can assume two different formats. Format 1, to transfer UL channel data with a maximum TBS of 1000 bits and using LTE's turbo code for error correction. And format 2, to carry HARQ acknowledgments (acknowledgment of a DL transmission) of the DL channel NPDSCH using a repetition code for error correction [24].

As mentioned before, UL defines a new unit called resource unit, which is the smallest unit that can be used to map NPUSCH. Depending on the spacing, the number of slots and the channel format, the RU's length is different. For a format 1 channel with 3.75 kHz spacing, an RU spreads along 16 slots in one subcarrier (32 ms). For a 15 kHz spacing with format 1 (multi-tone transmission is supported [24]) the number of subcarriers can be 1, 3, 6 or 12 that use 16 (8 ms), 8 (4 ms), 4 (2 ms) or 2 (1 ms) slots respectively. NB-IoT devices normally only use the 3 or 6 subcarrier option because they cannot take advantage of the extra bandwidth [24]. In format 2 the RU always spreads along 4 slots (2 or 8 ms) in one subcarrier regardless of the subcarrier spacing.

For multi-tone transmissions the modulation used is always QPSK. But for single-tone the modulation will depend on the format used. Format 2 assumes a BPSK modulation scheme whereas format 1 can use BPSK or QPSK with the objective of reducing peak-to-average power ratio (PAPR) [24].

It is also important to note that the information about NPUSCH like the start time, number of repetitions, RUs per transport block, subcarriers and modulation scheme is obtained by the UE through DCI format N0 in the NPDCCH.

2.2.3.3 DMRS

DMRS main purpose is to guarantee a proper signal demodulation at the eNB [17]. It is only sent when UL data transmission happens since it is time multiplexed with that data. As seen earlier, data can be sent over NPUSCH with a different number of slots, subcarrier spacing and format. DMRS is transmitted in one symbol or three for the formats 1 and 2 respectively and regardless of the number of subcarriers or the spacing. The differentiation happens in the symbol they occupy. For format 1 with 3.75 kHz spacing DMRS is transmitted in symbol 5 whereas with 15 kHz it is transmitted in symbol 4. For format 2 with 3.75 kHz the first three symbols are used whereas with 15 kHz the symbols used are the ones in the middle (symbol number 3, 4 and 5) [18].

sectionAccess Network and Cell Access

NB-IoT's access network is the same as the one from legacy LTE [18]. With the eNodeBs and the interface S1, between them and the MME/S-GW, and X2, mainly responsible for hand-overs and localized between eNodeBs. NB-IoT does not recognize hand-overs but keeps using the interface X2 to enable a fast resume for the UE connection establishment [18].

Following LTE's standard procedure, the UE searches for a cell on a certain frequency, reads SIB information and starts the Random Access Procedure (RAP) [18]. However, NB-IoT was developed for a specific category of devices that are low-cost, need high coverage levels and durable batteries (low power). These devices are not equipped as well as an LTE device and they have crystal oscillators that may cause a high carrier frequency offset (CFO). For that reason, changes were made in the synchronization sequences with the intention of attenuating the frequency offset and the symbol timing problems while keeping a low signal-to-noise ratio (SNR) [24].

2.2.4 Protocol Stack

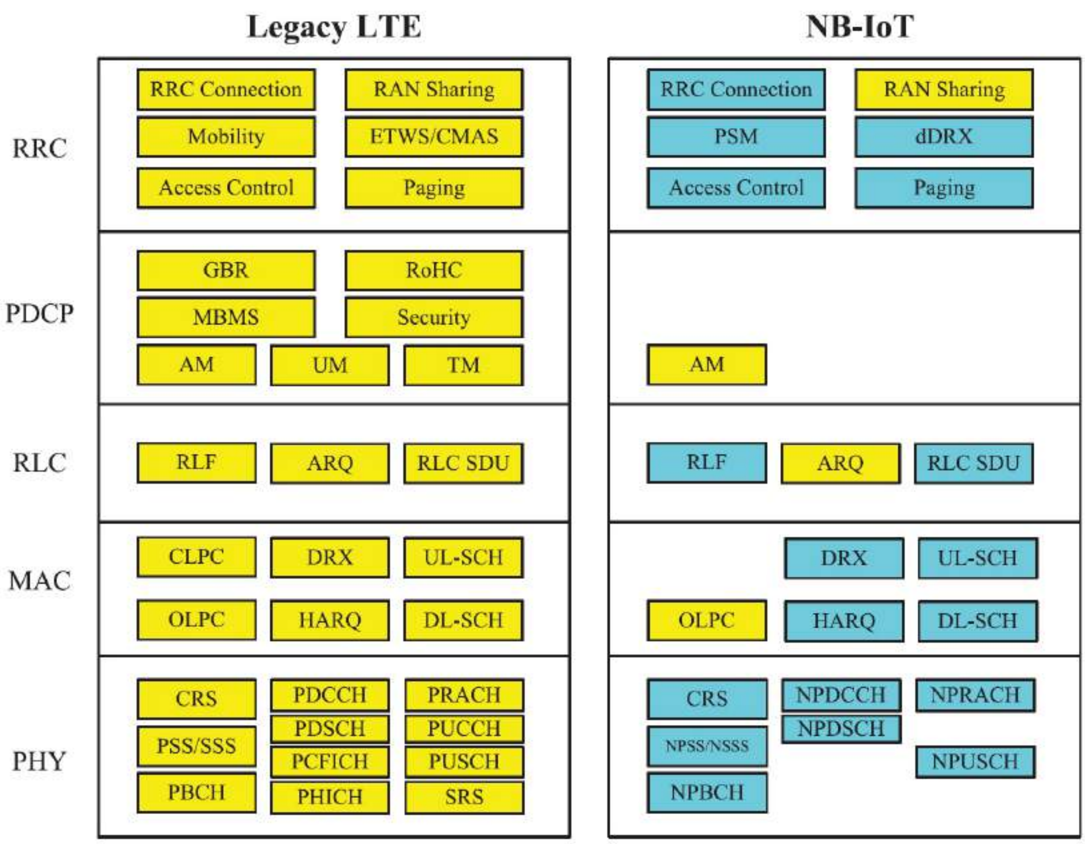

Figure 2.7: Comparison between NB-IoT's and LTE's protocol stacks, adapted from [25]. The blue colored blocks represent new or changed features.

NB-IoT keeps LTE's protocol stack, at least in a structural manner, but simplifies it in order to reduce UE complexity [25], Figure 2.7. The physical layer has been already covered in previous sections.

Radio Bearers

NB-IoT removes the Signaling Radio Bearer (SRB) 2 previously used in legacy LTE for RRC messages, Non-access stratum (NAS) messages and measurement information [11] and introduces a new one called SRB1bis [18]. This SRB assumes responsibility for RRC messages and NAS messages before security is active [12] and because of this it is the only SRB used in the control plane optimisation since there is no security activation in this mode.

2.2.5 System Information

Only a small part of LTE System Information Block (SIB) is kept by NB-IoT. Namely, the MIB-NB, SIB 1 to 5 and SIB 14 and 16. All these contain different information that the UE may need to perform certain functionalities. The first six ones, including MIB-NB, are mandatory for the UE to be connected but the UE is expected to read system information, only, in the idle state.

SIB1-NB and MIB-NB are a particular case of system information blocks because they are transmitted in a different way, as already explained in previous chapters. The other SIBs are, instead, grouped into SI messages that will be transmitted within a specific SI-window. These windows have a maximum TBS of 680 bits and may be repeated.

Some SIBs have a modification period, but others need to change whenever needed.

There is a field in MIB-NB called systemValueTag that helps UEs returning out of coverage or longer DRX cycles to know if there were changes in SIB1-NB. This option fits UEs that were unable to receive the paging message.

2.2.5.1 Summary

First, the UE obtains the NCellID from the NSSS. Then, they learn the size and number of repetitions of SIB1-NB by reading the *schedulingInfoSIB1* in MIB-NB. With that information the UE infers SIB1-NB starting position. Reading SIB1-NB gives the UE the information about where to find the other SIBs. Now the UE just needs to update SIB information and knows when to do that either by paging, modified value tags or the 2 LSBs of the hyper frame number in MIB-NB [18].

2.2.6 Cell Selection

As stated before, NB-IoT does not support handovers since its target devices are stationary. To change cells, the UE needs to enter the RRC_IDLE state and only then re-select the cell. Nevertheless, the notation of inter and intra frequencies still exist. Intra frequency means that the UE will use the same 180 kHz carrier (PRB) it was using in the previous cell and inter frequency is when it uses a different carrier, even if that 180 kHz carrier belongs to the same LTE carrier.

UEs are in coverage of a cell if the received power and quality of the NRS signal is above the thresholds defined by the cell, obtained by the UE through SIB-NB.

The UE may start a re-selection if the receiving NRS power of other cells exceeds a re-selection threshold (may be different for intra and inter frequency). In order to do that, the UE ranks suitable cells by their power excess over another threshold and chooses the better one. To prevent frequent re-selections the process has hysteresis and intra frequency re-selections may have a cell specific offset.

When leaving RRC_CONNECTED state the eNB sends a RRCConnectionRelease message. This message may contain frequency information for the UE to start searching for another cell. The UE only searches other frequencies if it does not find a cell in the frequency indicated by the message.

2.2.7 Random Access Procedure

In order to start transferring data, the UE must execute the random access procedure. The UE starts by sending a preamble, as already explained in previous sections, and calculating its RA-RNTI. With the RA-RNTI the UE can now decode PDCCH and get DCI format N1 with the Random Access Response (RAR), expected within a response window (3 SFs after the preamble). The UE can now send the msg3 with the right timing because of the C-RNTI and the time advance from the RAR message. Finally, the UE waits for the Contention Resolution with its identification to confirm the success of the procedure.

2.2.8 Connection Control

RRC state model has only two states, RRC_IDLE and RRC_CONNECTED, regardless of the technology used.

When the UE wants to establish a connection, it sends an RRCConnectionRequest indicating also the Establishment Cause (purpose for the connection) and capabilities like multi-tone traffic and multi carrier support. The eNB then responds with a RRC-ConnectionSetup indicating protocols, SRB and data radio bearer (DRB) configuration. Lastly, the UE responds with an RRCConnectionSetupComplete with the PLMN and MME chosen.

Depending on the optimisation in use, different things happen after the connection establishment. User Plane optimisation follows the standard LTE approach with a security, connection reconfiguration and re-establishment procedures, whereas Control Plane optimisation does not.

Terminating a connection, i.e. returning to the RRC_IDLE state, is a simple process. The eNB sends an RRCConnectionRelease and it is done. If the UE wants to establish a connection again it will need to repeat the connection setup explained above. However, with the User Plane optimisation the eNB may set a rrcSuspend flag and save the AS context of the UE. In this case the UE will also be in the idle state but if it wants to connect again it will, instead, send an RRCConnectionResumeRequest and avoid the whole connection setup. This optimisation significantly reduces signalling overhead because NB-IoT devices tend to send small data packets in spaced periods of time.

When resuming a connection, the eNB may not accept the request. When this happens, instead of sending a RRCConnectionResume followed by a RRCConnectionResumeComplete from the UE, the eNB sends an RRCConnectionSetup.

Additionally, the UE may not be able to start a connection because of access barring or because there are no resources available. For the first case it is indicated in the MIB-NB that access barring is applied, so the UE must first check in the SIB14-NB if its class is barred or not. The classes range from 0 to 9 and are indicated by 10 bits in SIB14-NB. If the bit corresponding to the UEs class is set, the UE cannot establish a connection and so it must wait and check SIB14-NB for changes in the access barring. For the second case, the eNB sends a RRCConnectionReject indicating a time interval for the UE to wait until it tries to establish connection again. Useful in network overload situations.

NB-IoT also benefits from a feature called Power Saving Mode (PSM). In Figure 2.8 During PSM, the device stays registered to the network, but only its internal clock is active greatly reducing power consumption and improving battery life. This feature eliminates the need to re-establish the connection to eNodeB, and the device can exit PSM as soon as it has data to send. If it does not have data to send, it only exits the PSM state to check if it has downlink data pending when the T3412 timer expires. This timer is set following the network policies during the tracking area update (Tracking Area Update (TAU)) procedure. All the timers (Inactivity timer, Active timer, and TAU) and paging periods are defined by the network.

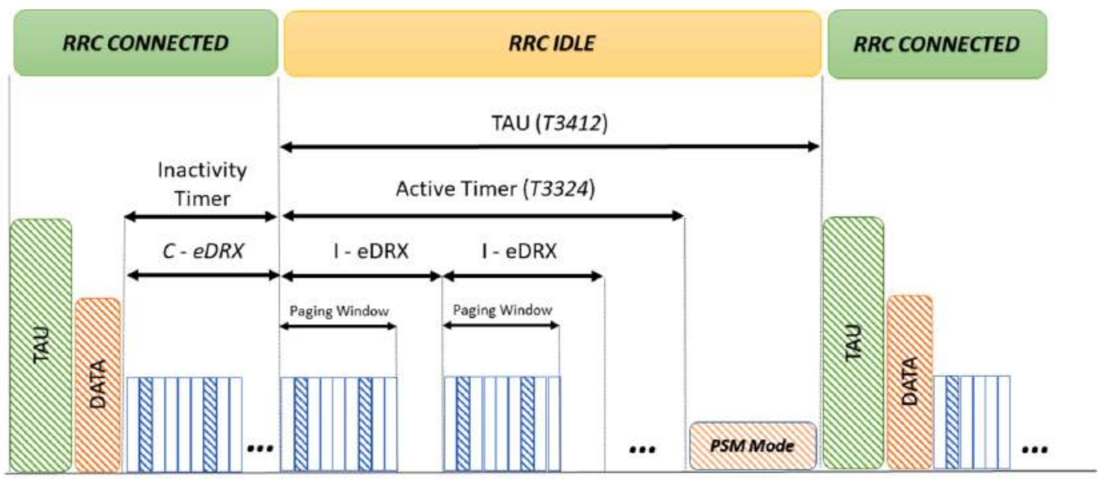

Figure 2.8: Graphic representation of the connection states across time, adapted from [2]. The periods of eDRX both connected and idle and PSM can also be obseved.

2.2.9 Capability Tranfer

Different UEs are built based on different releases and support different features. The eNB needs this information and so it starts the UE Capability Transfer procedure by sending an *UECapabilityEnquiry*. The UE responds with information about its release, category, supported bands, and multiple bearer, carrier and tone transmission capabilities.

2.3 Core Network and Data

Working over the already established LTE core network, the evolved packet system (EPS), two optimizations were made in order to better fit the necessities of IoT devices. The User Plane cellular internet of things (CIoT) and the Control Plane CIoT. These optimizations were not specifically made only for NB-IoT.

In Figure 2.9 we can find a diagram of the architecture. In it appears a new block called Service Capability Exposure Function (SCEF) intended to deal, only, with non-IP data traffic, mainly the machine type traffic originated by most of NB-IoT UEs. It works as an alternative route over the control plane with DL data being transmitted in the reverse path without the need of radio bearers like SGW and PGW. It is better for small amounts of data that needs to be transmitted with less frequency (like a simple temperature value of a temperature sensor).

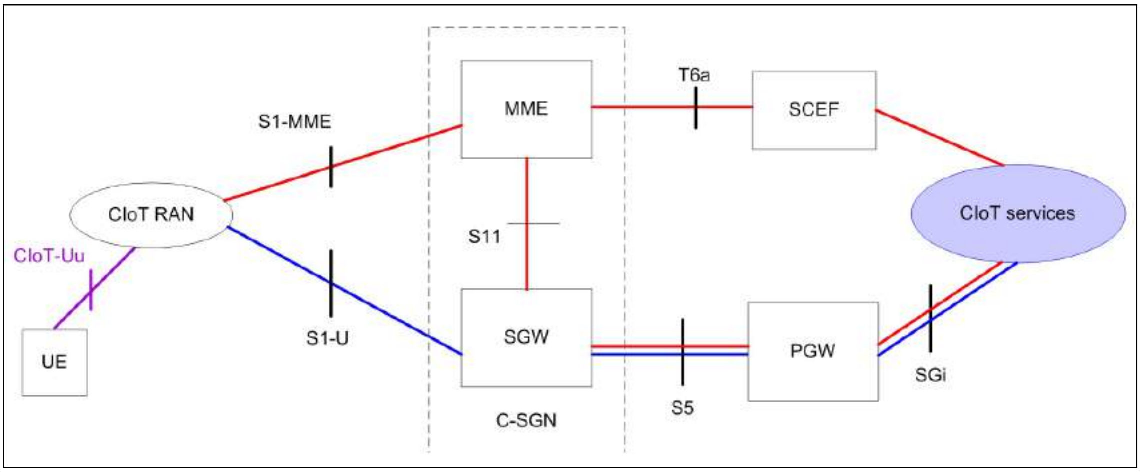

Figure 2.9: Diagram of the NB-IoT core network. Blue represents the *User Plane* and red represents the *Control Plane*. Adapted from [18].

The user plane optimization can be seen in Figure 2.9 in blue. It supports IP and non-IP data packets and supports sending bigger amounts of data better than the control plane optimization. In contrast, some overhead is expected when establishing a connection.

UEs choose which optimisation they want to use when sending data. When receiving, the choice is made by MME considering the UE preference.

2.3.1 Control Plane CIoT Optimisation

In the control plane, data is piggybacked in the messages of the connection setup and if that is not enough, *DLInformationTransfer* and *ULInformationTransfer* messages will carry the remainder. In order to do that, the messages contain a byte array with NAS information (data) and an interface between the eNB and MME, S1-MME, will carry the dedicatedInfoNAS. This makes the NAS information transparent to the RRC layer and, consequently, does not apply security or connection reconfiguration.

2.3.2 User Plane CIoT Optimisation

Here, data flows through the S-GW node with the help of one or two DRBs. In this optimisation UEs can be suspended when entering RRC_IDLE and reconnect with a resume procedure, as will be explained later. This helps reducing signalling overhead caused by the security and reconfiguration that happens after the UE connects.

2.3.2.1 Connection Configuration

The Initial security activation procedure is executed right after the RRC_Connection is established. The eNB sends a SecurityModeCommand message containing two algorithms. One that the UE will use to decipher SRB1 and DRBs, and another to apply integrity protection to SRB1. This procedure changes SRB1bis to SRB1.

Following this, comes the RRC connection reconfiguration procedure whose objective is setting up DRBs for the UE. The eNB sends a RRCConnectionReconfiguration message indicating the DRB and other configurations like RLC and logical channels priority balancing, as well as the configurations for time alignement and slot and frequency mapping.

2.3.2.2 Multi Carrier Configuration

In the reconfiguration procedure UEs that support multiple carriers may get an additional one for DL and UL, the non-anchor carrier. These additional carriers will be used by the UE to send or receive data except paging and synchronization and broadcast information. While in the connected state, the UE will listen (DL) or send (UL) data, only, in the non-anchor carrier whereas in the idle state it will work only with the anchor carrier.

2.3.2.3 Control Channel

UEs in the connected state will monitor the UE specific search space (USS). The number of repetitions of the channel will depend on the number indicated in the reconfiguration message and may be smaller than that. When that happens, the remaining SFs are used to transmit another UE's NPDCCH. NPDCCH's period is also indicated in the reconfiguration message. Within this period the USS starts at an offset of 3/8, ¼, or 1/8 of the length.

2.3.2.4 UL Data

NPUSH transport blocks have a repetition pattern that is dependent on the number of repetitions, the number of subcarriers per RU and the subcarrier spacing. In Figure 2.10 we see an example of a transport block composed of two RUs, T and W. Each RU spans over 8 slots and 3 subcarriers with a 15 kHz spacing and the number of repetitions applied is 8. The numbers next to the letters represent the slot number of that RU. As you can see the SFs (2 slots) are repeated 4 times, half the number of total repetitions (the upper limit is 4 for multiple subcarriers and 1 for single subcarrier). Then, when all the SFs have been repeated 4 times, the pattern starts again until all SFs have been repeated 8 times.

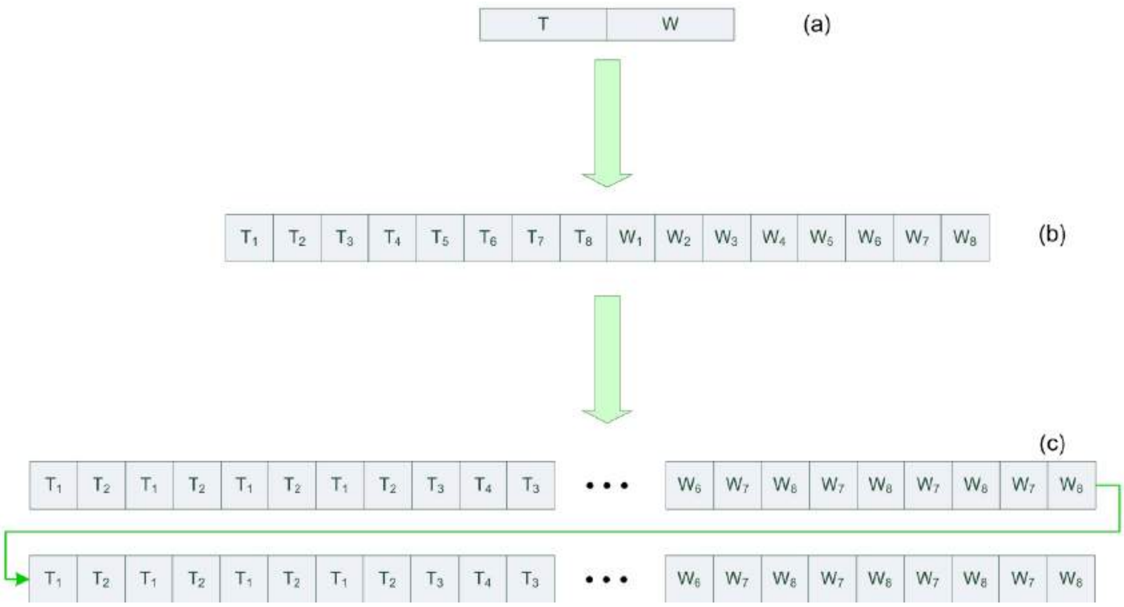

Figure 2.10: UL data representation. (a) RU division. (b) Slot composition. (c) Transmission Sequence of the slots. Adapted from [18].

For the 3,75 kHz the pattern is similar but instead of 2 by 2 slot repetition, it is done separately.

NPUSH transmissions have a maximum duration of 256 ms. If they exceed that limit, by having a big number of repetitions, they stop and a 40 ms gap is applied before resuming transmission. This happens because UEs cannot receive and transmit at the same time but they need to read the DL channel in order not to lose synchronization.

2.3.2.5 DL Data

Similar to what happens in the UL, but data is mapped in data packets instead of RUs. However, when transmitting SIBs, an entire block is sent before there is any repetition. Instead of repeating SFs with an upper limit of 4 at a time, the repetition happens at the SIB level.

Like what happen in the UL channel, gaps are applied to the DL. However, MIBs ans SIBs are an exception and these gaps are not static like in the UL. Instead, RRCConnectionReconfiguration message indicates the transmission max length and gap length.

3

Related Works

This chapter presents an overview of different evaluations of NB-IoT's KPIs that are similar to the ones proposed in this dissertation, focusing on evaluations done on real network scenarios utilizing different infrastructures. The objective here is to present the related work that has been done already and to provide knowledge and similar approaches for the KPI evaluation performed on this dissertation. NB-IoT can assume several different configurations that differ between network providers. This should be taken into account when performing and comparing the evaluations as it affects the results obtained. For this reason, when available, all those configurations will be shown. Throughout the chapter, small comparisons between results obtained with different configurations are presented.

3.1 Uplink, downlink and channel occupancy

In [7] a model-based performance evaluation of several realistic use cases is presented. The performance is characterized for the uplink, downlink, and channel occupancy. Different use cases are considered, including different UE densities (UEs/Km2), percentages of UEs in different radio conditions (indoor, deep indoor, and outdoor), different payload sizes (PS), and different report periodicity (RP) ranging from gas metering and bike fleet management, with faster RP (30 minutes), to vending machines and electricity metering, with the RP of 24 hours. In Figure 3.1, an evaluation considering a deployment scenario of three-sectorial base stations in a hexagonal grid with a variable inter-site distance (ISD) can be observed. Scenarios that experience a better channel will consequently have a better channel occupancy since they will need fewer repetitions to transmit data. This fact is observed in Figure 3.1 for the bike fleet management scenario since UEs are mostly deployed outdoors. It can also be observed that larger cells (that cover more UEs) will experience an increase in the percentage of channel occupancy used for the NPUSCH and NPRACH. For the Gas Metering example with an inter-site distance (ISD) of 1732 m, it is found that the network is almost saturated in the UL, even though it has the same RP, less density, and shorter PS than the bike fleet management example. A good explanation for this would be the coverage level, or radio conditions of the UEs, which is also the most important factor when it comes to performance as will be later described in this chapter.

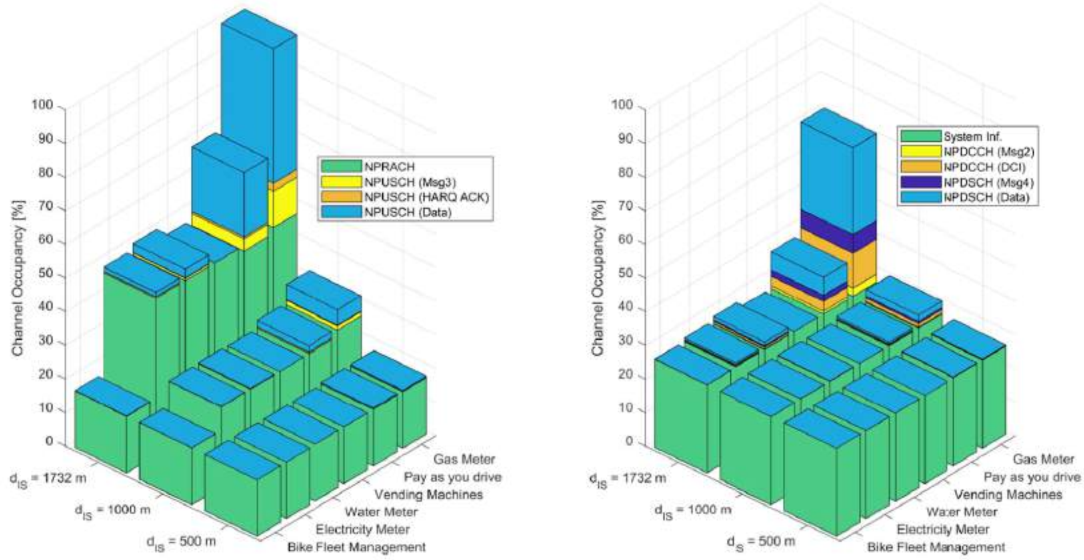

Figure 3.1: Channel occupancy on UL and DL (left and right, respectively) for different realistic scenarios with different inter-site distances. From [7].

Figure 3.2 represents the relation between the traffic generated by the UEs, network throughput, and the percentage of free resources in two different NPRACH configurations. It can be observed that in the 500 m ISD (left), which means a considerably smaller number of devices than the 1000 m ISD case (right), for a smaller NPRACH the utilization of resources only reaches 30% (70% free). This happens because most of the UEs will not be able to complete the RA procedure due to collision, leading to a 20kbps maximum throughput. For this case, a bigger NPRACH leads to a better resource utilization (100% at 80 packets/s), which consequently means that the network saturates at a higher throughput (62 kbps). However, this reasoning is not observed for the 1000 m ISD case because NPRACH may consume a significant amount of resources if a considerable number of devices is connected, limiting the maximum throughput of the network. In Figure 4, on the right, for a bigger NPRACH, the free resources start at about 40% and saturate at the 12 packets/s with a throughput of 8kbps. This means that the NPRACH alone is consuming about 60% of the network resources. In this case, a smaller NPRACH, although not utilizing all the network resources available, will lead to better network throughput.

3.2 NB-IoT vs LoRaWAN

In [2] a comparison between NB-IoT and LoRaWAN, concerning latency, energy consumption, coverage, and quality of service, can be found. It is stated that NB-IoT targets better latency, Quality of Service (QoS), and indoor coverage with support for a massive number of devices while LoRaWAN focuses on energy efficiency, long-range communications, and low-cost devices.

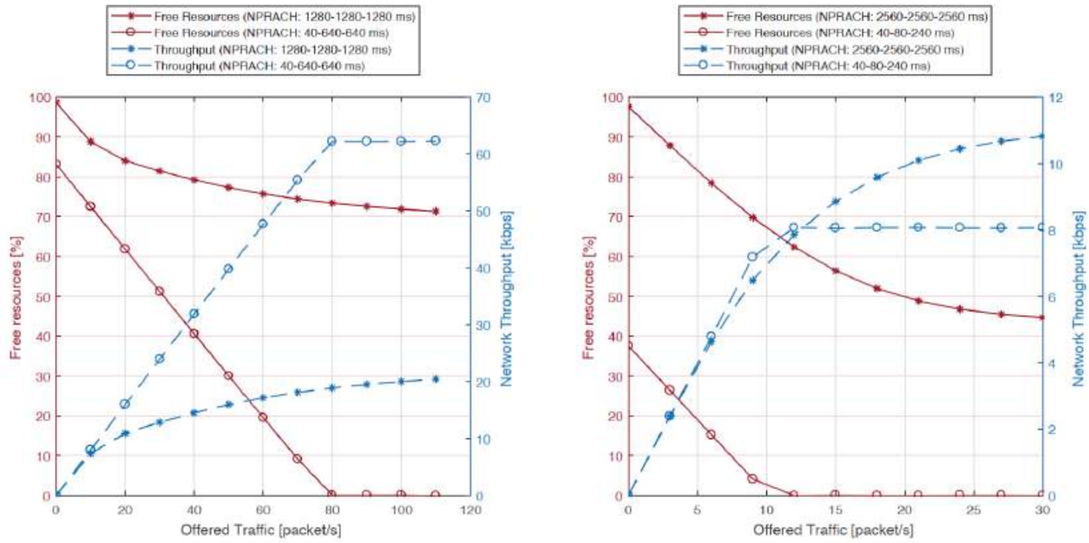

Figure 3.2: Relation between traffic generated by the UEs and free network resources and throughput for 500 m ISD (left) and 100 m ISD (right). From [7].

Both technologies are LPWANs, which means that battery life and efficiency are important aspects to consider when thinking about deploying one over the other. In the NB-IoT case, the device's energy efficiency is extremely dependent on the parameters defined by the network operators and the type of applications deployed, which may have different payload sizes, packet periodicity, and device configuration. Battery life can range from 13 years, for devices using power saving mode (PSM) and sending only one packet per day, to 88 days, for devices that send 1 packet per hour with extended discontinuous reception enabled, for example. NB-IoT targets 10 years of battery lifetime when transmitting 200 bytes per day.

ID	C	N bytes	$T_{act.}$ [s]	I_{max} [mA]	E_{mean} [mJ]	E_{max} [mJ]	E_{min} [mJ]	RSSI [dBm]
a	G	10	11.9	138	2063	3007	517	-83
b	G	50	11.9	146	1858	3111	486	-81
c	G	100	12.0	135	1856	3240	499	-75
d	G	400	12.2	138	2067	3232	550	-75
e	M	10	13.7	245	2677	4549	1847	-112
f	M	50	12.8	232	2453	4078	1890	-109
g	M	100	12.6	219	2379	4150	1903	-110
h	M	400	12.8	225	2386	3786	1972	-107
i	B	10	46.6	151	9047	17072	5453	-130
l	B	50	41.1	175	7641	16298	5579	-136
m	B	100	37.2	169	6818	13264	5200	-135
n	B	400	40.5	185	7552	17845	5745	-134

Table 3.1: Average RSSI over 50 measurements for 10, 50, 100 and 400 bytes of payload size in three different defined coverage levels (Good, Medium, and Bad) [2].

It is difficult to measure NB-IoT energy consumption because of the different parameters that influence this feature. Multiple configurations can be used with different transmission power, number of repetitions, and timers for extended Discontinuous Reception Cycle (eDRX) and PSM. In addition to this, network providers manage parameters differently which directly influences energy consumption and cannot be controlled by the user. For that reason, in [2], three coverage levels were defined using one specific KPI, already present in LTE, RSSI. This KPI was chosen because it is the parameter with the most impact on consumption. In Table 3.1, the results presented are a combination of measurements from a real NB-IoT testbed and the coverage levels defined by RSSI are -80 dBm average for Good (G), -110 dBm for Medium (M), and -130 dBm for Bad (B). It can be observed that for the same coverage level the time active and the energy spent have almost no variation even when sending 40 times more data (for a and d case). Also, with low RSSI levels, NB-IoT increases the number of re-transmissions from 32 to 2048 reinforcing the importance of RSSI over the payload size (N bytes). In [2], it is concluded that for single packet transmissions the energy per byte (EPB) is higher. This can be observed by looking at Figure 3.3. Ignoring the outliers, it can be seen that the differences between 1, 5, and 10 packets (400B per packet) communications are minimal both in the duration of the transmission and the energy spent while the number of packets transmitted is five and ten times higher. This proves that NB-IoT might be inefficient for sporadic transfers of only one packet.

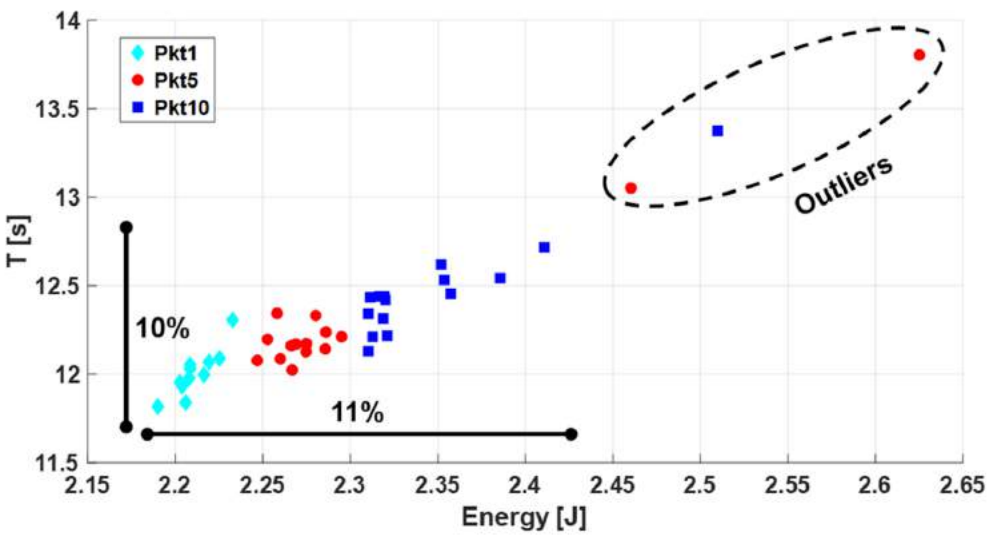

Figure 3.3: Active time and energy spent for transmitting 1, 5, and 10 packets (400 B per packet). From [2].

In Figure 3.4 it can be seen that LoraWAN outperforms NB-IoT in all scenarios where 1, 2, or 3 packets at a time are sent, even in the worst coverage conditions for LoRaWAN. However, if an application allows buffering information, and the number of packets sent increases the scenario is different. For clarification DR0, DR2, and DR5 are different LoRa data rates (progressively lower in order to allow communication) and can be compared to coverage levels in the NB-IoT. The figure shows that for 33 packets sent at a time the EPB in NB-IoT can be lower and battery life longer, in the Medium coverage level (or DR2 for LoRa) case. It can be argued that by increasing the number of packets sent NB-IoT can be even more efficient and have a longer battery life, but that may start getting out of LPWAN scenarios because most IoT applications won't benefit from that and it also affects the limited battery life.

Comparing both technologies we can see advantages on both sides depending on the application. As shown previously battery life is dependent on buffering and coverage but only NB-IoT has guaranteed QoS and works on an already implemented infrastructure which means less time to market (TTM) and national scale coverage. The cost of both technologies will also depend on the application. For applications with fewer devices, NB-IoT will probably be less expensive because, even if the module costs more than the LoRa module, LoRa apports infrastructure costs of gateways, servers, and maintenance while NB-IoT only needs a device and a SIM card from a network provider to be used.

3.3 Real-Time Demand-Response Application

Certain IoT applications have specific key requirements, for example, demand response applications require bounded latency, wide range, high data rate, high reliability, security scalability, and availability. All of them represent requirements that NB-IoT aims to meet and generally NB-IoT achieves higher performance when compared to competing technologies.

In [21] a system architecture to monitor indoor electrical appliances and report that information to a Demand Response Server (DRS) was proposed. This architecture follows the basic and widely used three-layer structure (device, network, application). It consists of a Smart Plug with a sensor module to collect data and an NB-IoT module that sends the data to the DRS using the already available LTE infrastructure. The DRS maintains the logs of the sensors, like power measurements, and plug states of each different device and manages the request of the Demand Response Controller (DRC). The DRC is the application that controls the plugs to minimize consumption and allows the user to visualize the data collected. The DRC could be implemented with other network technologies, like Wireless Local Area Network (WLAN), but NB-IoT presents several advantages. Using NB-IoT modules allows for easy device installation, freedom in choosing the location, support of a large number of end devices, large coverage, and deep indoor penetration.

The evaluation reported in [21] was focused on latency, data delivery percentage, and command delivery percentage. Similar to what we are proposing with this dissertation, the evaluations were made under a public NB-IoT network, which means that the latency value obtained includes the time it takes for the whole process of connection establishment. This means that grant acquisition, random access, signal processing, queuing delay

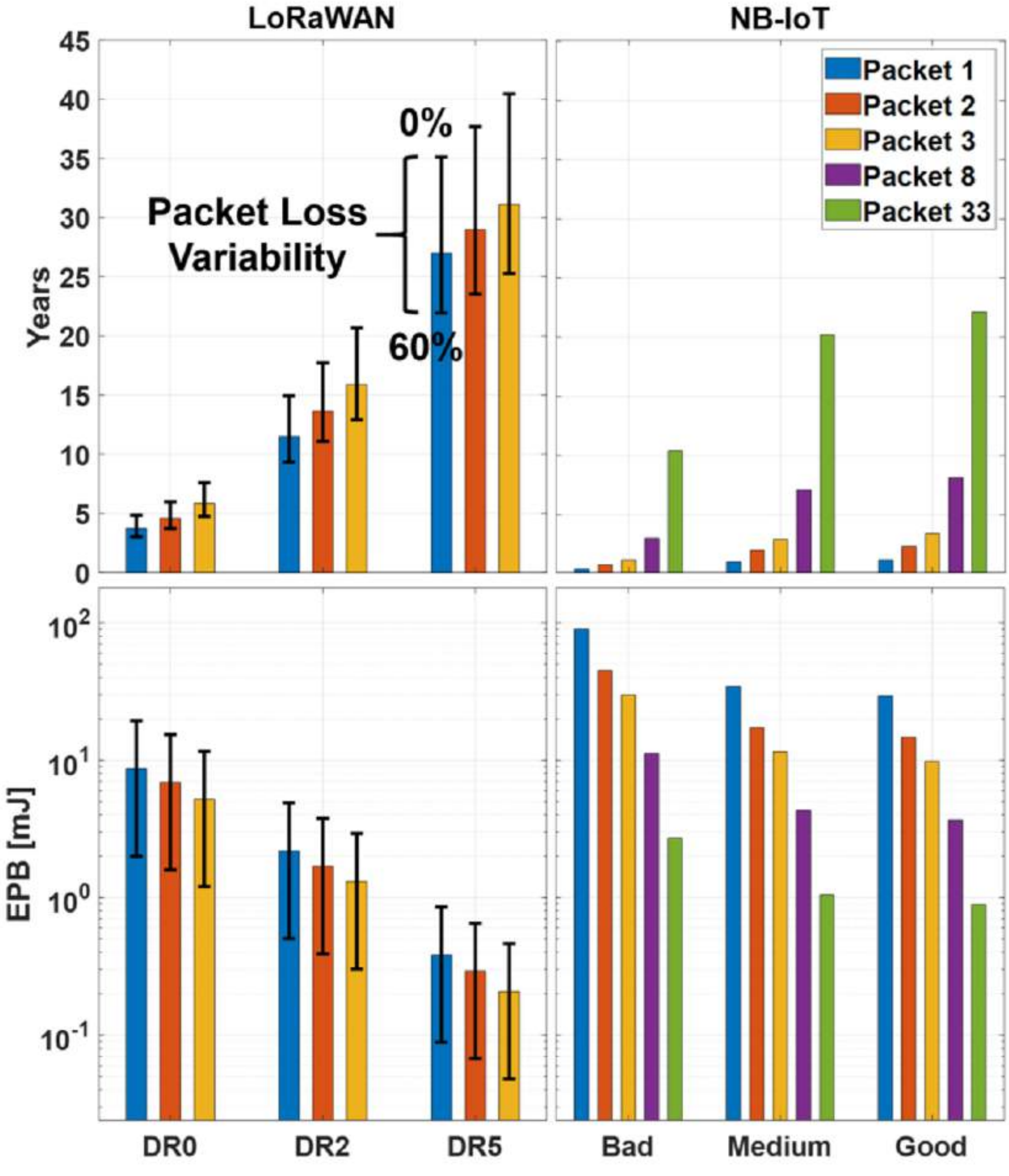

Figure 3.4: Comparison between LoRaWAN and NB-IoT battery life (in years) and EPB in DR0, DR2, and DR5 conditions for LoRa and Bad, Medium and Good coverage levels for NB-IoT. From [2].

due to congestion, propagation delay, packet re-transmission delay, and processing time were included in the latency value, not to mention that the network real-time load can affect the results. The tests were performed outdoors with an attenuator to simulate outdoor (0dB), normal indoor (30dB), and deep indoor conditions (60 dB).

The results from [21] show that NB-IoT meets the requirements for most demand-response applications reaching an average latency of fewer than 8 seconds in the worst environmental conditions for messages of 64 bytes. However, it is important to consider that different message sizes will have a different average latency. Figure 3.5 shows that the average latency for messages of 512 bytes can be up to 3 times more than for messages of 64 bytes. Again, RSSI is the most important factor and the outdoor example presents a negligible latency when compared to the indoor and deep indoor. This should be taken into consideration when choosing the technology for demand response applications as some may require less latency.

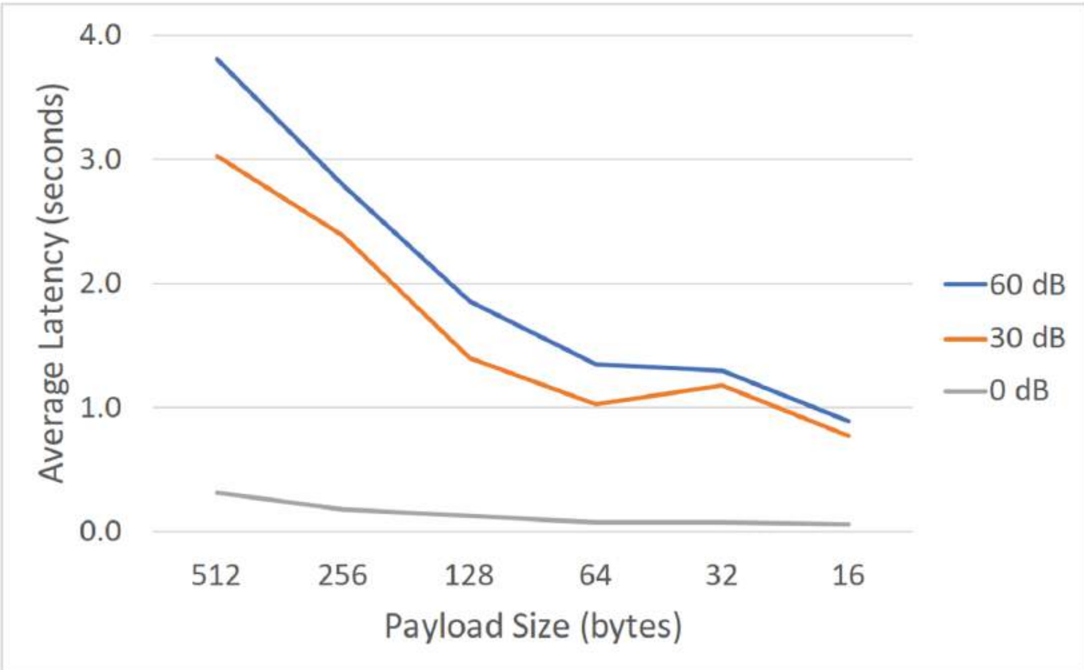

Figure 3.5: Average NB-IoT latency from DRS to DRC for different message sizes and different radio conditions (0, 30, 60dB attenuation for outdoor, indoor, and deep indoor), adapted from [21].

3.4 Evaluation of NB-IoT Energy Consumption

In [15] the effects of the parameter configuration on the consumption associated with NB-IoT UEs, both on the device side and the network side, are analyzed. As mentioned before, NB-IoT has two main ways of lowering power consumption: the PSM; and the eDRX. The PSM is a period in which the UE shuts off communication with the Evolved

Node B (eNodeB) and runs only its internal clock to keep track of time, thus saving power. The duration of the PSM is controlled via a parameter defined by the network. This parameter is the Tracking Area Update (TAU) or T3412 timer and can be up to 413 days. The eDRX is a period in which the UE stops monitoring radio channels between paging periods to reduce power consumption. The periods are set by the Active Time or T3324 which is a parameter defined by the network. Since most of these definitions are controlled by the network providers, NB-IoT energy performance will be different across them.

The device used in this evaluation is similar to the one we adopt in this Thesis: a Quectel module integrated in a board that offers an Application Programming Interface (API) and allows users to issue commands to the module. Through these commands, a set of parameters and metrics can be obtained. Most of the parameters used here will be described in chapters ahead, for our evaluation. It is also important to mention transport and application layers used in the solution since they may also influence the results obtained. For this solution, MQTT For Sensor Networks (MQTT-SN) over UDP was used since it is bandwidth-friendly and minimizes overhead. Another solution normally used is MQ Telemetry Transport (MQTT) over Transmission Control Protocol (TCP), which will be used in the solution proposed in this dissertation.

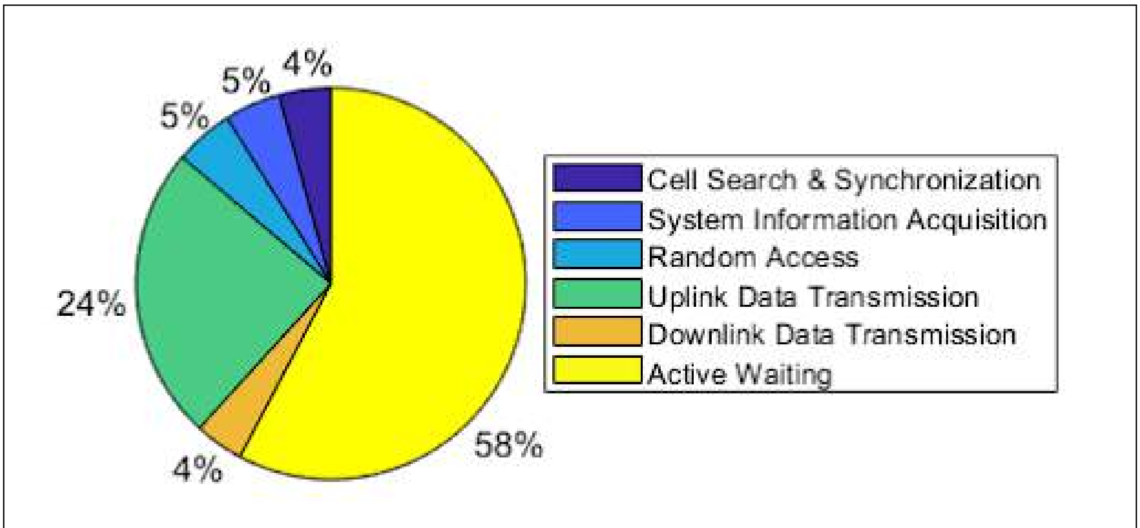

Figure 3.6: Pie chart of the energy consumption of different phases during the transmission of a 64 bytes UDP packet. [15].

The authors in [15] have verified that the most energy-demanding process was the Active waiting that the UE does when it waits for the network to release the RRC connection and enter RRC_Idle. It took about 64% of the total energy for packets of 16B. However, for a packet size of 1024B, the Uplink Data Transmission becomes the most energy-demanding process, as we can be seen in Figure 3.7. This happens because the Active waiting consumes the same amount of energy regardless of the size of the packet since the value of the Inactivity Timer is the same, but the UE has much more data to

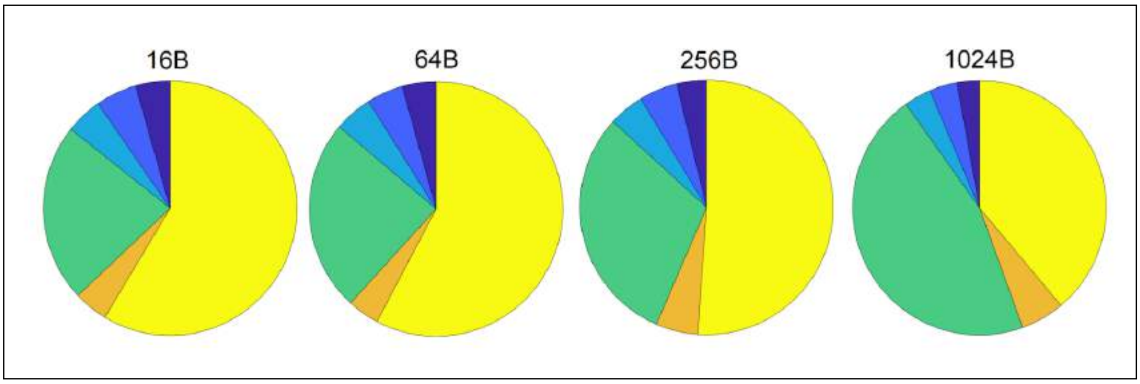

Figure 3.7: Energy consumption pie chart of different phases during the transmission of 16, 64, 256, and 1024-bytes-long UDP packets.[15].

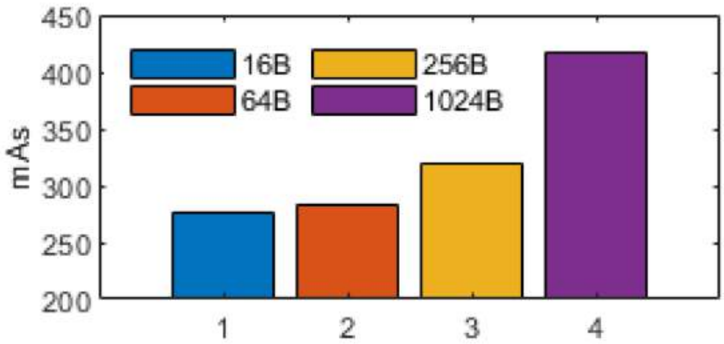

Figure 3.8: Graphic representation of the total energy consumed with the transmission of a 16, 64, 256, and 1024-bytes-long UDP packet.[15].

transmit, thus consuming more energy on that process. As shown before, even if sending bigger packets is more energy demanding, it is still a more energy-efficient process, as shown in Figure 3.8. A 1024-bytes-long UDP packet consumes about 0,415 mAs per byte while a 16-bytes-long packet consumes about 17,2 mAs per byte, which is 40 times more. For devices that have battery life targets of 10 years or more, this energy cost per byte should be taken into account.

4 Evaluation Setup

This chapter will focus on the setup used to evaluate the performance key indicators of the NB-IoT system. Here we have a description of the hardware and the metrics we can obtain with it. The purpose of this chapter is to give a better understanding of the metrics available in the adopted hardware and what those metrics represent in terms of network performance, i.e. their practical meaning.

4.1 NB-IoT Device

To perform the tests the BC66 module from Quectel was used. We chose this module because it has the necessary features needed to interact and monitor the network. More specifically, we used the BC66-TE-B development board so that we could use the Arduino interface to program the board and send commands to the NB-IoT module. The board comes in a small form factor (70mm x 74mm x 1.6mm), is powered by the USB interface connected to the computer we are using to program it, and supports three Universal asynchronous receiver-transmitter (UART) ports that have different uses, such as firmware updating and debugging. It has a power and reset button and an antenna interface with a 50 ohms impedance. To have a better understanding of how we did things, an interface diagram of the board is represented in Figure 4.1. J301 was the interface used to power the board and connect it to the computer. The figure depicts the most important interfaces for our project: the antenna interface (J304); the power and reset buttons used every time we reprogrammed the board (S101 and S02, respectively); and the Universal Subscriber Identity Module (USIM) interface (J303) where we plugged the USIM Card provided by Altice.

BC66 module has five different Access Point or Modem operating modes which are aligned with NB-IoT requirements:

- Normal: AP tasks are running and AT commands are being received;
- Idle: If AP tasks are suspended, it enters idle mode;
- Connected: It is registered to the network and can perform data transmission;

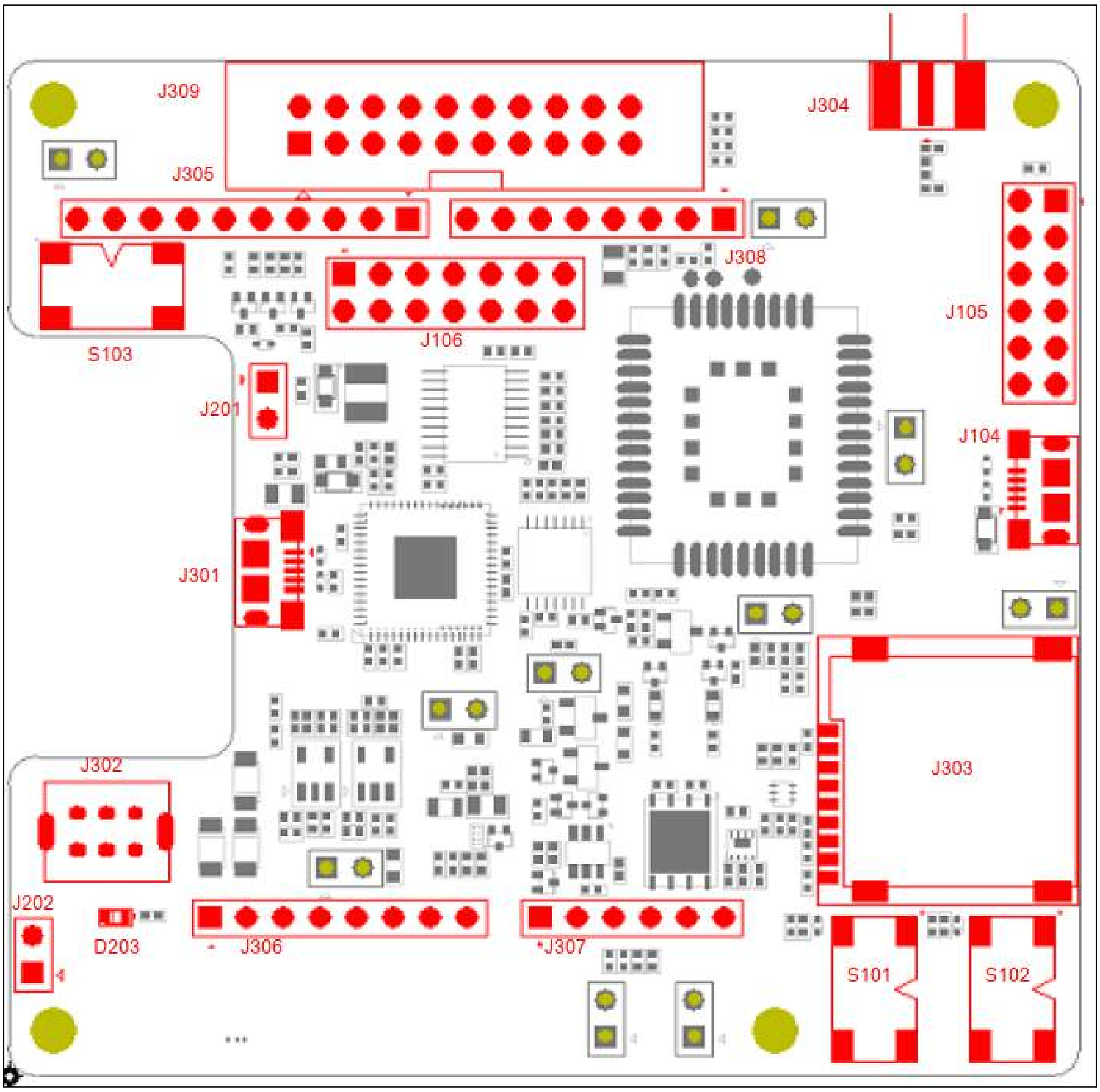

Figure 4.1: BC66-TE-B interface distribution diagram. [3]

- Discontinuous Reception Cycle (DRX)/eDRX: It is registered to the network but the modem is in idle mode. Only downlink data can be received and it depends on the paging windows, as explained in the chapters before;
- PSM: It is registered to the network but cannot receive data. Power Saving Mode is also a feature described in previous chapters.

The module itself has three different operating modes regarding power consumption. The modes are Active, Light Sleep, and Deep Sleep. Light Sleep happens when the modem is in DRX/eDRX mode and greatly reduces power consumption. Deep Sleep happens when the modem is in PSM. In Deep Sleep, the CPU is powered off and only the 32KHz Real Time Clock (RTC) clock is working consuming an ultra-low current (typically 3.5 uA). The module only wakes up from Deep Sleep when the periodic TAU timer times out, as explained in previous chapters, by pressing the PSM_EINT button on the board, or by LwM2M session lifetime timeout.

4.2 Metrics Description

The board provides various metric measurements through the use of AT commands. The most important for our case have to do with data and network status. Therefore, we used three main commands: AT+CESQ - Extended Signal Quality; AT+CSQ - Signal Quality Report; AT+QENG - Engineering Mode. With these we were able to retrieve the following parameters:

- <rxlev> or <rssi>: This parameter corresponds to the received signal strength indicator. It is a metric typically used in LTE and it measures the average total received power in Orthogonal Frequency Division Multiplexing (OFDM) reference symbols. It is normally measured over N resource blocks and 12 subcarriers but NB-IoT only uses one resource block and may use 12 or 48 subcarriers depending on the spacing. It accounts for the power from co-channel serving and non-serving cells, adjacent channel interference, thermal noise, and other factors. It is not directly reported to eNodeB by the UE. Instead, it is computed from RSRQ and RSRP that are reported from the UE [14]. The terminal will provide a value from 0 to 99 where a larger number indicates better signal quality (the value is computed and mapped according to [4]). This information is based on a single measurement so it is expected to change over short periods and values range from -110 dBm (0) to -48 dBm (63) in increments of 1 dBm.

- <ber>: This parameter corresponds to the bit error rate. According to [23] this metric relates to the received signal quality (RXQUAL) and represents the average Bit Error Rate (BER) before channel decoding in a full set or subset of Time Division Multiple Access (TDMA) frames. Measurements made in previous report periods are discarded. For this, eight levels of RXQUAL are defined and mapped to the BER:

RXQUAL_0	BER < 0,2 %	Assumed value = 0,14 %
RXQUAL_1	0,2 % < BER < 0,4 %	Assumed value = 0,28 %
RXQUAL_2	0,4 % < BER < 0,8 %	Assumed value = 0,57 %
RXQUAL_3	0,8 % < BER < 1,6 %	Assumed value = 1,13 %
RXQUAL_4	1,6 % < BER < 3,2 %	Assumed value = 2,26 %
RXQUAL_5	3,2 % < BER < 6,4 %	Assumed value = 4,53 %
RXQUAL_6	6,4 % < BER < 12,8 %	Assumed value = 9,05 %
RXQUAL_7	12,8 % < BER	Assumed value = 18,10 %

  There is also a table defining the accuracy of the MS reporting the error probability under static channel conditions, which is described in [23].

- <rsrp>: While RSSI is an indirect value of the total received power in all symbols, the RSRP measures the average received power of REs that carry CRS and can be calculated from RSSI taking into account the PRBs used [14]:

$$RSRP(dBm) = RSSI(dBm) - 10log(12N), \tag{4.1}$$

  where N is the number of PRBs. The equation represents ideal conditions without considering noise and interference, which influences the RSSI value. Values range from -140 dBm (0) to -44 dBm (97) in increments of 1 dBm. According to the board manual, an RSRP greater than -115 dB is recommended when sending data.

- <rsrq>: This parameter corresponds to the reference signal received quality. The terminal mapping is compliant with 3GPP 36.133 for UEs that do not support the extended RSRQ range, as described in [22]. It is defined as the ratio between RSRP and RSRQ:

$$RSRQ = N\frac{RSRP}{RSSI}, \tag{4.2}$$

  where N is the number of PRBs. Both RSRP and RSSI measurements were made over the same set of RBs and RSSI still needs to take into account noise and interference. Values range from -19.5 dB (0) to -3 dB (34). According to the board manual, an RSRQ greater than -10 dB is recommended when sending data.

- <RLC_UL_BLER>, <RLC_DL_BLER>, <RLC_UL_tput> and <RLC_DL_tput>: This parameter represents the uplink and downlink block error rate (BLER) in the RLC layer (per Automatic Repeat Request (ARQ)) and the throughput. The BLER is represented in percentage and can range from 0 to 100 and the throughput is represented in kbits/s. Both are calculated from the beginning of the RRC connection establishment or since the last time the command that returns the parameter was called.

- <MAC_UL_BLER>, <MAC_DL_BLER>, <MAC_UL_tput> and <MAC_DL_tput>: This parameter represents the uplink and downlink block error rate in the MAC layer, in this case, for NPUSCH (per Hybrid Automatic Repeat Request (HARQ)) and the throughput. The BLER is represented in percentage and the throughput in kbit/s like the 4 parameters above.

- <sinr>: Signal-to-Interference and Noise Ratio (SINR) can also be used to estimate signal quality. It represents the relation between the usable measured signal power (measured in the reference signals), and the interference (signal power from other cells that cause channel interference) and the noise experienced. It is not defined in 3GPP specs, but it is widely used by operators and UEs to calculate Channel Quality Indicator (CQI) (Channel Quality Indicator) since it better quantifies radio conditions in relation to throughput. As it is not defined by 3GPP, UEs from different manufacturers measure SINR in different ways, which means that it is often not comparable between different UEs. [13]

4.3 Evaluation

We decided to analyze the NB-IoT performance under different radio conditions. Therefore, the measurements were performed in different locations in Lisbon, using the device described in this chapter to access the Altice network. The code used to program the board was developed in C programming language and flashed to the board using Arduino. Additional libraries provided by the authors of this repository [1] were also used. The code used can be found in [20]. Our approach consists of sending data to an MQTT broker (a public broker called EMQ X), while measuring the parameters described above. Using MQTT over TCP as this seems to be the only option available with our UE. In general, it is preferable to use UDP as it incurs in less overhead. It might also be interesting to compare the performance of both methods. The UE sends two MQTT messages every second with 64 bytes of information and calls the AT commands reporting the parameters. In this way, we can not only measure the throughput and BER, but also check the variations or fluctuations of the radio conditions (measured in RSSI, RSRP, RSRQ and SINR), since they are updated every second. Measurements are taken for 500 seconds (1000 MQTT packets are sent). We also collect information about the serving cell that the device is accessing. This information is later used in the Unwired Labs Location API to locate the wireless cell. In this way, it is possible to calculate the distance between the cell and the device and display a map of the area to provide a better understanding of the conditions in which the measurements were made. All data is obtained from the module's responses collected by the Arduino serial monitor. The data is then copied to an Excel file and a program developed with UiPath, also available in [20], will then be used to process this data and make the necessary conversions to obtain the correct values in a tabular format, which will then allow us to display this data graphically. With these measurements, the goal is to compare the results obtained between the different sites, make an evaluation of the KPIs and analyze each situation thoroughly.

5

NB-IoT Performance Evaluation

This chapter describes the results obtained from the data collection performed with the available hardware, as well as a context (geolocation and images of the area) for each site where data was collected. This information will be useful to analyse the impacts of different environments in signal propagation and hopefully give a better understanding of the relation between distance and the metrics that regard signal quality for NB-IoT, specifically RSRP, RSRQ, and RSSI. As previously mentioned, all data was obtained through Quectel's NB-IoT module and should be enough to provide a baseline on the expected performance for NB-IoT in the conditions described.

5.1 Data Collection Locations

Under ideal circumstances, it would be possible to choose a base station and perform separate tests at different distances to obtain data that better describes the relationship between distance and signal quality. Unfortunately, this is not the case as the tests were performed on a real cellular network (Altice), with the module choosing the base station according to the criteria jointly implemented in the network and device. For this reason, the test locations were chosen based on the type of environment (urban, rural, etc.). As explained before, the cell location was obtained through the information provided by the module using an open-source API (OpenCelliD). With the geographical coordinates of both the module and the cell, a 2D and a 3D image of the area was obtained using Google's services (Maps and Earth). The distances between the UE and the Base Station (BS) were calculated using the Haversine formula. For better clarification, the metrics are extracted from the UE which obtains that information from the serving cell. The signal propagation happens between the UE and the serving cell, and since latency is not analyzed, the time that data takes to go from the serving cell (entry point in the network) to the internet (MQTT server) is ignored.

Figure 5.1: Satellite image of the test site location in Parque Eduardo Sétimo with a yellow line between the base station and the module. The module is on the left side, the base station is on the right, and the distance between them is 404 meters.

5.1.1 Outdoor Parque Eduardo Sétimo

In Figure 5.1 it is possible to see tall buildings and big trees between the module and the BS. These characteristics make this scenario fall under the category of Urban high-rise environment and with a distance of 404 meters (less than 1 km) and the propagation is affected primarily by buildings and trees [19]. Unfortunately, it was not possible to know the height of the BS so we can only assume that it was a Non-Line-of-Sight (NLoS) layout. Given this information, it is safe to assume that either propagation over rooftops or propagation along street canyons is happening.

5.1.2 Outdoor Póvoa de Santo Adrião

In Figure 5.2 an Urban canyon can be observed, a typical Urban high-rise environment. This scenario is very similar to the one above with the exception that, for this one, the number of buildings is much larger suggesting that the impact on the signal propagation will be stronger.

5.1.3 Outdoor Vila Chã

Most of the scenarios explored are Urban. The same happens here. In this case, the buildings and foliage will be less impactful on signal strength because the distance is greater than 1 km, which means that ground elevation plays a more significant role. In Figure 5.3 it can be observed, by looking at the yellow line, that the ground elevation does not present a lot of variation. This means that the impact from the ground elevation on the signal propagation should be minimum. In this case, propagation should be affected primarily by the distance.

Figure 5.2: Satellite image of the test site location in Povoa de Santo Adrião with a yellow line between the base station and the module. The module is on the left side, the base station is on the right, and the distance between them is 530 meters.

Figure 5.3: Satellite image of the test site location in Vila Chã with a yellow line between the base station and the module. The module is on the right side, the base station is on the left, and the distance between them is 2260 meters.

5.1.4 Outdoor Sintra

For this scenario, the objective was to evaluate a mainly rural environment. Sintra is a mountain range with a considerable amount of vegetation and fits perfectly in this category. In this situation, impairments to the signal will come from the influence of terrain height, high-density foliage, and small houses (sometimes high traffic volume is also possible) [19]. As it can be observed in Figure 5.4, the terrain between the cell and the module is steep to the point that the module location can practically be considered a valley and they are, clearly, not in line of sight. At a distance of more than 2 kms, the foliage and the terrain will certainly impact the quality of the signal.

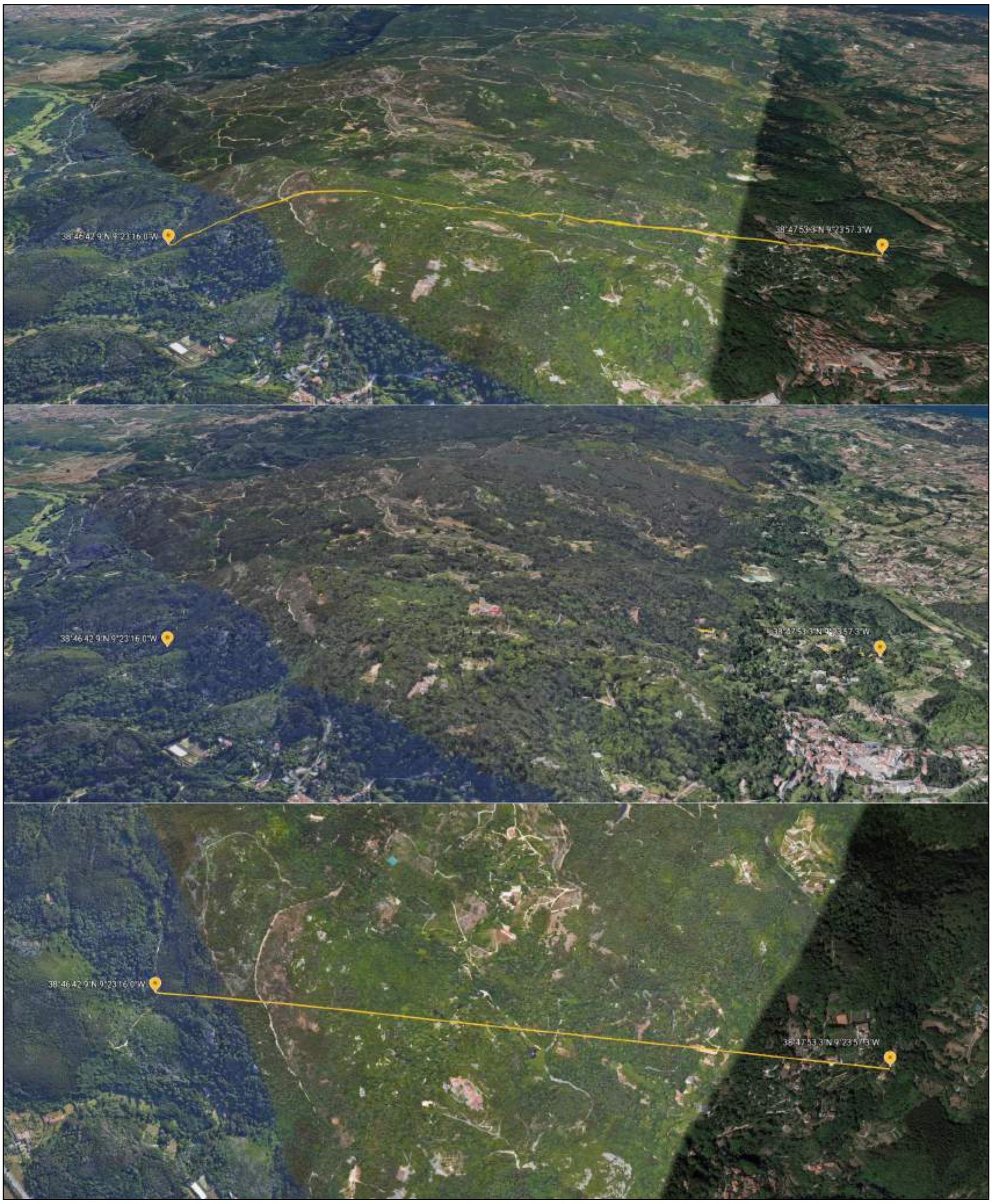

Figure 5.4: Three satellite images of the test site location in Sintra with a yellow line between the base station and the module. The second image is the same angle as the first one but has 3D buildings and foliage. The third image is the 2D view from above. The module is on the right side, the base station is on the left, and the distance between them is 2391 meters. The distance was obtained using the Haversine formula.

Figure 5.5: Satellite image of the test site location in Parque das Conchas with a yellow line between the base station and the module. The module is on the right side, the base station is on the left, and the distance between them is 2407 meters.

5.1.5 Outdoor Parque das Conchas

The choice of this scenario was made to observe the impact of foliage on the signal. The module was located in a park with a considerable amount of tall trees. Unfortunately, it was connected to a base station that was quite far from the park (2,4 kms). Due to this, the scenario becomes mainly Urban, as it can be observed in Figure 5.5, and the signal propagation will also be affected primarily by the distance.

5.1.6 Outdoor Cemitério do Lumiar

This scenario was mainly chosen to access the same BS as the previous scenario but in a different location. The data is useful as it represents a mainly urban scenario at a distance of 2,9 km (similar conditions), but this time it has no impact from the foliage. Also, in Figure 5.6, a football stadium in the middle of the propagation path can be observed, and it could be interesting to explore the impact of big structures like this on signal propagation.

5.1.7 Outdoor Monsanto

This scenario is mainly rural. In Figure 5.7, a mountain range with high foliage density can be observed. At a distance of 3,4 kms, the effect on signal propagation will come primarily from height differences on the ground, but the density of foliage around the module's location will certainly have an effect as well.

5.1.8 Indoor Damaia

This scenario is a combination between urban low-rise and rural areas. In Figure 5.8 it can be observed that both the module and the base station are located in urban areas but between them, there is a mountain range with a considerable size, Monsanto. High-density traffic is expected and the module was located inside the first floor of a building

Figure 5.6: Satellite image of the test site location in Cemitério do Lumiar with a yellow line between the base station and the module. The module is on the right side, the base station is on the left, and the distance between them is 2967 meters.

Figure 5.7: Satellite image of the test site location in Monsanto with a yellow line between the base station and the module. The module is on the right side, the base station is on the left, and the distance between them is 3404 meters.

which means that the building entry loss should be considered. Also, at a distance of 5 kms, the hearth's curvature should be taken into account.

5.1.9 Deep Indoor Vila Chã

The module location here is very near the Outdoor Vila Chã scenario. But for this case, the module was located inside the garage of a building on the -1 floor level. The data collected on this scenario is less when compared to the others because the radio conditions were very bad and did not allow the module to keep the connected state for the whole duration of the test. Also, a test on the 0-floor level was performed but the information on the base station location could not be found in the OpenCellID API, so it was not possible to present the distance or image for that case. One interesting aspect that can be observed

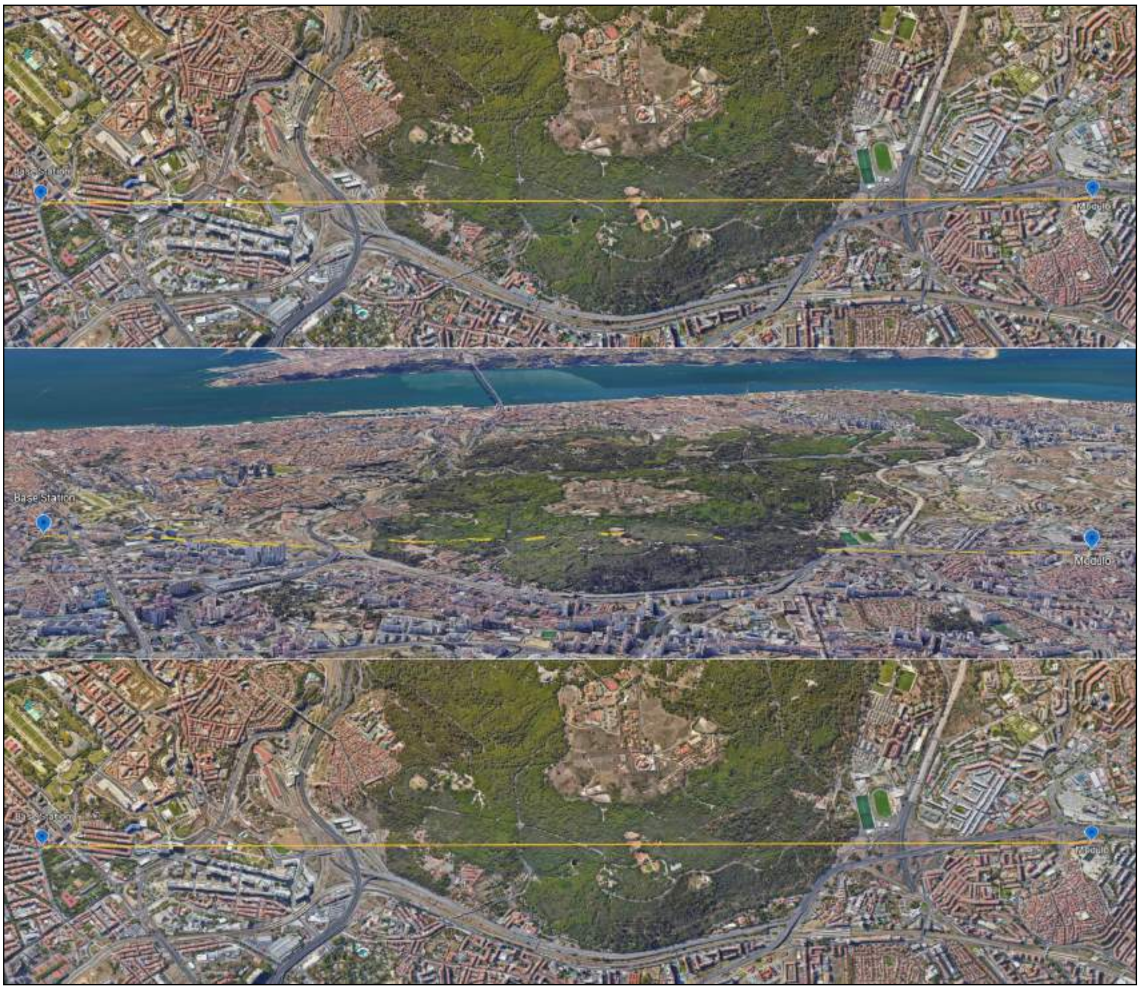

Figure 5.8: Three satellite images of the test site location in Damaia with a yellow line between the base station and the module. The second image is the same angle as the first but has 3D buildings and foliage. The third image is the 2D view from above. The module is on the right side, the base station is on the left, and the distance between them is 5558 meters.

here is that even though the module's locations from the Deep Indoor Scenario and the Outdoor Scenario are very close, they were connected to different BSs and in this case, not only is the module located on the -1 floor of a building presenting a very hard situation in terms of radio conditions, but also the BS is at a distance of 6,5 kms, much more than the Outdoor situation on the same street.

5.2 Results

The results obtained aim at giving a perspective on the situation of the technology in the Portuguese panorama. As explained before, the tests performed had a duration of 500 seconds (about 8 minutes and a half), with 1000 MQTT messages of 64B sent (2 messages per second). Every second, the module gathered data about the radio metrics and its

Figure 5.9: Satellite image of the test site location in Vila Chã with a yellow line between the base station and the module. The module is on the right side, the base station is on the left, and the distance between them is 6516 meters.

average is shown in Table 5.1. Considering the average RSSI obtained in the worst-case scenarios, it is possible to denote a different level of expectations when it comes to the capacity of NB-IoT to work in bad radio conditions, in comparison with other works. From the tests performed, it was not possible to obtain a stable connection with an RSSI lower than -100 dBm. The results obtained in other works, as presented in Section 3.2, report levels of performance for good, medium, and bad coverage corresponding to the values of -80, -110 and -130 dBm, respectively. This means that the tests performed in this dissertation only cover a medium or good coverage level, which does not represent the totality of the use case proposed for this technology. One possible explanation for this situation is that, even though the module is compliant with the 3GPP standard, the AT Commands that retrieve the metrics of RSSI, for example, only retrieve a value as low as -113 dBm, according to the manual, which means that the device used might not be able to perform under such low RSSI conditions. Another plausible explanation is that the parameters controlled by the Altice network, of which we have no visibility, do not allow the establishment of a connection under a certain threshold of signal quality. Also, these parameters might be different from location to location, therefore, finding a place in which it would be possible to perform tests under a bad coverage level RSSI would be extremely difficult.

Nevertheless, by analyzing the obtained data, it is possible to make some statements about the technology. For example, from the data presented in Figure 5.10, it can be seen that the metrics of NB-IoT have a similar variation between different scenarios (when the RSSI is lower, the RSRQ and RSRP are also lower). This makes sense since their calculation depends on each other, as shown in Section 4.2. However, comparing the percentage change in SINR and RSSI in Figure 5.11, we can see discrepancies in scenarios that have a higher SINR value but present lower RSSI values. This shows that we observe

Scenario	Distance (m)	RSRP (dBm)	RSRQ (dB)	RSSI (dBm)	SINR (dB)
1	404	-62,7	-15,7	-47	11,6
2	530	-59,7	-15,3	-44,4	13,6
3	2260	-93,2	-18,7	-74,5	2,2
4	2391	-97,7	-21,9	-75,8	-2,1
5	2407	-98,6	-20,8	-77,8	1,8
6	2967	-67,6	-15,4	-52,3	16,3
7	3404	-103,7	-21,4	-82,3	-2,1
8	5558	-93,8	-19,4	-74,4	2,8
9	6516	-122,7	-22,9	-99,9	-3,4
10	N/A	-120,3	-20,2	-100,2	0,2

Table 5.1: Results of the average measurements obtained for each scenario for the most important metrics on signal analysis for NB-IoT (RSSI, RSRP, RSRQ, SINR). The scenario number corresponds to the subsection of numbers from the previous section, for example scenario 1 corresponds to the scenarios described in Subsection 5.1.1.

a stable RSSI level even under conditions of high signal interference. It was expected that scenarios 4, 7, and 9 would have the worst SINR values because of ground elevation changes, dense foliage in scenarios 4 and 7 and the deep underground position of scenario 9. Scenarios 3, 5, 8, and 10 also fall under what is expected in terms of SINR values (median values when compared to the highest and lowest values). Scenarios 8 and 10 are indoor, but not as deep as Scenario 9. Scenario 3 is in a ravine surrounded by buildings, which inevitably causes some interference, and Scenario 5 has some interference from foliage but not as much as Scenarios 4 and 7. Scenarios 1 and 2 are naturally at the top of the SINR table because of their close proximity to BS. Surprisingly, however, Scenario 6 has the highest SINR value, even though it is mainly an urban scenario at a distance of more than 2 km from the base station. One possible explanation for this value is that the module in Scenario 6 was located in a wide open area with clear skies, while in scenarios 1 and 2 it was located near a park with light foliage. The small amount of interference resulting from the lack of line-of-sight in short-range scenarios appears to have a greater effect on SINR than distance itself.

Figure 5.12 represents the percentage of block error rates for the UL and DL in the MAC layer for each scenario. By looking at the graphic bars, the resilience of the technology to errors is evidenced especially for the UL. The only scenarios minimally affected were scenarios 9 and 10, which is expected since they represent the scenarios with the lowest value of RSSI and require more penetration capacity for the garage and the -1 floor. However, less than 2% for scenario 9 is too optimistic since the connection was recurrently being lost. For the DL case, it seems that SINR is more important than RSSI. Scenarios 4 and 7 got the highest BLER (around 14%) and these are the scenarios with more vegetation and terrain height difference (and therefore less SINR) over the propagation path. Scenarios 1, 2, and 6 have achieved the highest SINR and the lowest BLER, reinforcing the SINR hypothesis.

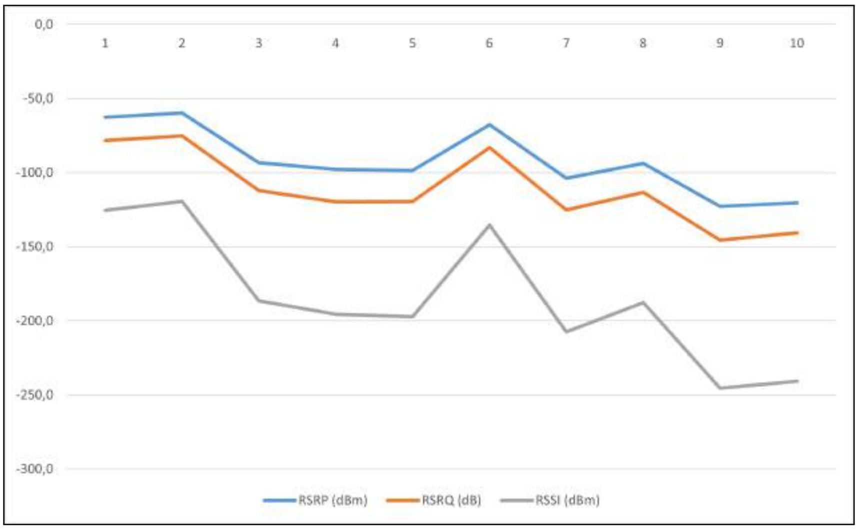

Figure 5.10: Graphical representation of RSSI, RSRQ and RSSI in all 10 scenarios.

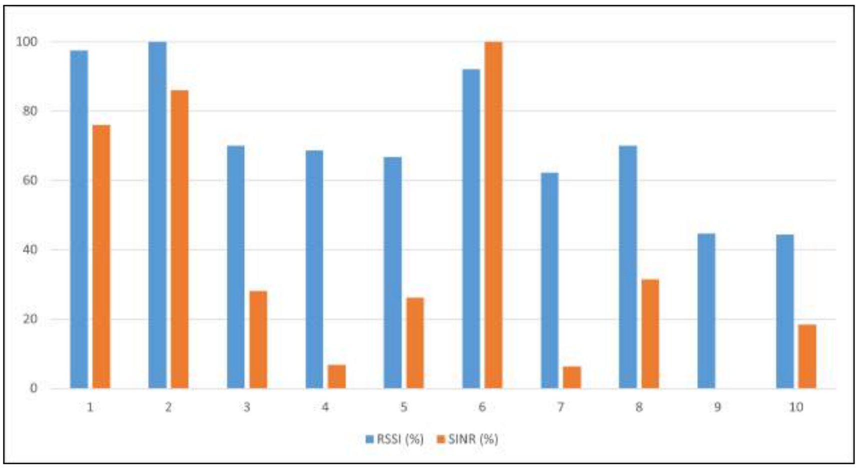

Figure 5.11: Graphical representation of the percentage of SINR and RSSI when compared to the best value across scenarios.

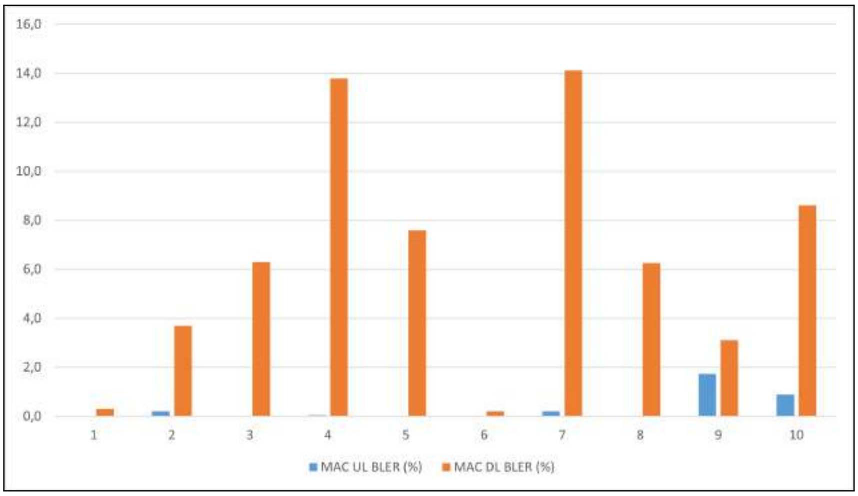

Figure 5.12: BLER for the UL and DL in the MAC layer.

6 Conclusions

6.1 Final Remarks

This work analyzes the capacity and usability of NB-IoT on a real network environment in Portugal, specifically using the Altice network. A brief overview of the technology State-of-the-art (SoA) and a performance evaluation on KPI's were also done. The overview describes the physical layer, including all channels, procedures to transfer data and features shared with 4G, as well as the core network and the optimisations that came in recent releases of the 3GPP Standard. For the performance evaluation, a Quectel device with an NB-IoT module, BC66-TE-B, was used and several propagation scenarios were considered. The evaluation performed is limited by the capacity of the device, especially in regards to coverage. Since NB-IoT is an LPWAN technology, one of the main objectives is to be able to establish a stable connection in low coverage situations (long-distance or underground penetration). When comparing the results obtained in this thesis with previous works it is clear that the device is not able to establish a connection on bad coverage conditions (RSSI lower than -100 dBm), which presents a problem when trying to evaluate the performance of the technology. For this reason, several scenarios intended to explore the coverage capacity of the technology had to be discarded. Another important aspect when considering the use of NB-IoT is the National coverage provided by the already established LTE network. In certain cases of underground coverage, the device could not connect to the 4G network but other UEs in the same location could connect to a 2G base station with a strong signal, which shows that coverage might be more limited than expected. Nevertheless, the results obtained show the real performance that a device can expect in the conditions described in each scenario and show that the use of the technology is viable in the locations the tests were performed, around the Lisbon metropolitan area. Also, we hope that they contribute to future research done around this topic as being standard levels of what is to be expected.

6.2 Future Work

The solution proposed to perform the tests uses MQTT over TCP as an application layer protocol, which might introduce more overhead than other protocols like Constrained Application Protocol (CoAP) over UDP. [15] A comparison between the performance of the different application protocols in similar scenarios could show the benefits of using one over the other. Also, a public broker was used to perform the evaluations. Using a proprietary solution would allow the collection of more data, like the delay, and introduce the possibility of not only sending messages from the device but also receiving them allowing a more in-depth study of the DL. All the data used in the evaluation was obtained through only one device. Using more devices, as well as having devices from different manufacturers with the capacity of reaching low RSSI levels of bad coverage enriches the scenario possibilities. One good example to study can be the performance obtained on different floors in an underground garage. Network load is also a factor to take into account. Even though it is not possible to purposely make the network overload, as that would require the use of thousands of devices in the same location, one possibility could be to try and find locations where the network load is known to be high at certain times of the day, collect data from those occasions and compare it with data from less busy network loads. As an LPWAN, one of NB-IoT's concerns is the energy consumption of the UEs. As such, collecting data from the energy consumption in different scenarios would be useful to make a better assessment of the battery life expected for devices in different conditions. Comparing the battery level of a device in a good coverage situation against one in a bad coverage situation, where both devices present the same behaviour, for example sending a certain number of messages in a defined timeframe, and started on a fully charged battery, could be a good starting point.

Bibliography

[1] G. Angelov. *Arduino-Quectel-BC66*. Version 2.0.0. Feb. 2020. URL: https://github.com/Wiz-IO/Arduino-Quectel-BC66 (cit. on p. 35).

[2] M. Ballerini et al. "NB-IoT Versus LoRaWAN: An Experimental Evaluation for Industrial Applications". In: *IEEE Transactions on Industrial Informatics* 16.12 (2020), pp. 7802–7811 (cit. on pp. 12, 18, 23–25, 27).

[3] "BC66-TE-B User Guide". In: (2019). URL: https://www.quectel.com/download/quectel_bc66-te-b_user_guide_v2-1/ (visited on 05/05/2021) (cit. on p. 32).

[4] "BC66&BC66-NA AT Commands Manual". In: (2020). URL: https://www.quectel.com/download/quectel_bc66bc66-na_at_commands_manual_v2-2/ (visited on 05/05/2021) (cit. on p. 33).

[5] M. Chen et al. "Narrow band internet of things". In: *IEEE access* 5 (2017), pp. 20557–20577 (cit. on p. 1).

[6] A. El Mahjoubi, T. Mazri, and N. Hmina. "M2M and eMTC communications via NB-IoT, Morocco first testbed experimental results and RF deployment scenario: New approach to improve main 5G KPIs and performances". In: *2017 International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE. 2017, pp. 1–6 (cit. on p. 13).

[7] L. Feltrin et al. "Narrowband IoT: A survey on downlink and uplink perspectives". In: *IEEE Wireless Communications* 26.1 (2019), pp. 78–86 (cit. on pp. 22–24).

[8] J. Gozalvez. "New 3GPP standard for IoT [mobile radio]". In: *IEEE Vehicular Technology Magazine* 11.1 (2016), pp. 14–20 (cit. on p. 4).

[9] S. Grant. "3GPP Low Power Wide Area Technologies-GSMA White Paper". In: *gsma. com* (2016) (cit. on p. 1).

[10] T. IOT. "Narrowband IoT The game changer for the Internet of Things". In: *White Paper* (Oct. 2017), pp. 1–10 (cit. on p. 1).

[11] *LTE Quick Reference*. ShareTechnote. URL: www.sharetechnote.com/html/Handbook_LTE_SRB_Mapping.html (visited on 02/06/2019) (cit. on p. 15).

[12] *LTE Quick Reference*. ShareTechnote. URL: http://sharetechnote.com/html/Handbook_LTE_NB_SRB_Mapping.html (visited on 02/06/2019) (cit. on p. 16).

[13] *LTE RSRQ to SINR*. CableFree. URL: https://www.cablefree.net/wirelesstechnology/4glte/lte-rsrq-sinr/ (visited on 12/07/2021) (cit. on p. 35).

[14] *LTE RSSI, RSRP and RSRQ Measurement*. CableFree. URL: https://www.cablefree.net/wirelesstechnology/4glte/rsrp-rsrq-measurement-lte/ (visited on 12/07/2021) (cit. on pp. 33, 34).

[15] M. Lukic et al. "In-depth Real-World Evaluation of NB-IoT Module Energy Consumption". In: *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*. IEEE. 2020, pp. 261–265 (cit. on pp. 28–30, 47).

[16] V. Nair. "Evaluating the suitability of Narrowband Internet-of-Things (NB-IoT) for smart grids". In: (2017) (cit. on pp. 1, 8, 12).

[17] F. Rayal and T. I. Inc. *An overview of the LTE physical layer–Part II*. June 2010. URL: https://www.eetimes.com/document.asp?doc_id=1278137 (visited on 02/01/2019) (cit. on p. 14).

[18] J. Schlienz and D. Raddino. "Narrowband internet of things whitepaper". In: *White Paper, Rohde&Schwarz* (2016), pp. 1–42 (cit. on pp. 4, 5, 7–11, 13–16, 19, 21).

[19] I.-R. R. Sector. "Recommendation ITU-R P. 1411-7: Propagation data and prediction methods for the planning of short-range outdoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 100 GHz". In: *P series* 9 (2013), p. 71 (cit. on pp. 37, 38).

[20] P. A. Sousa Gaspar. *BC66 TE-B Data Collection Arduino Code*. Version 1.0.0. Mar. 2022. URL: https://github.com/pgaspar96/BC66-TE-B-Arduino-Data-Collecting (cit. on p. 35).

[21] A. K. Sultania, F. Mahfoudhi, and J. Famaey. "Real-Time Demand Response Using NB-IoT". In: *IEEE Internet of Things Journal* 7.12 (2020), pp. 11863–11872 (cit. on pp. 26, 28).

[22] U. M. Tel. "ETSI TS 136 133". In: (2018) (cit. on p. 34).

[23] U. M. Tel. "ETSI TS 145 008". In: (2016) (cit. on p. 33).

[24] Y.-P. E. Wang et al. "A primer on 3GPP narrowband Internet of Things". In: *IEEE Communications Magazine* 55.3 (2017), pp. 117–123 (cit. on pp. 6–11, 13–15).

[25] J. Xu et al. "Narrowband internet of things: Evolutions, technologies, and open issues". In: *IEEE Internet of Things Journal* 5.3 (2018), pp. 1449–1462 (cit. on p. 15).