A COMPARATIVE EVALUATION OF LORA AND NB-IoT TECHNOLOGIES IN A REAL ENVIRONMENT

Christia Charilaou

A Thesis
Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Science
at the
University of Cyprus

Recommended for Acceptance
by the Department of Computer Science

December 2020

APPROVAL PAGE
Master of Science Thesis

A COMPARATIVE EVALUATION OF LORA AND NB-IoT TECHNOLOGIES IN A REAL ENVIRONMENT

Presented by
CHRISTIA CHARILAOU

Research Supervisor ____________________________________

Research Supervisor’s Name

Committee Member ____________________________________

Committee Member’s Name

Committee Member ____________________________________

Committee Member’s Name

University of Cyprus
December, 2020

ACKNOWLEDGEMENTS

I would first like to express my special appreciation to my advisor Professor Dr. Andreas Pitsillidis, who has been a tremendous mentor to me. I would also like to thank him for his invaluable advices and guidance that helped me evolving as a student and as a computer specialist.

I would also like to thank my family and friends who have always been there for me and helped me achieving my goals. I would like to thank them for their love, guidance, support and strength that they have given me in this journey.

ABSTRACT

The Internet of Things (IoT) has already intruded into people's lives, as its primary purpose is to create a new digital world by interconnecting the different devices together. Sensors and actuators are all collaborating together in order to offer intelligent services to a number of users. Consequently, smart environments were created such as smart homes, smart cities etc. Many IoT applications were invented in order to support this remarkable evolution. However, the IoT requires some high technical demands in order to operate well and offer its services. These demands involve a long battery lifetime, low latency in order to inform immediately, low battery consumption in order to attain the long battery lifetime, massive number of connections, low cost and in some cases a long transmission range with uninterrupted connectivity, and high throughput.

The current wireless technologies cannot support this evolution since they offer high data rates with the cost of short range, or they offer acceptable data rates with the cost of a high battery drain and high device costs. Consequently, LPWAN technologies were created in order to serve this remarkable growth since they can accomplish all of the IoT demands. They are separated into two groups, those that transmit in an unlicensed spectrum such as Lora, Sigfox etc and those that transmit in a licensed spectrum such as NB-IoT, LTE-M etc. Each technology cannot serve all of the IoT applications requirements and therefore each one was created in order to serve specific kinds.

This project focuses on two Wide Area Networking technologies, namely Lora and NB-IOT, since they are the most popular technologies in industrial and research communities. Both technologies offer security, confidentiality, low power consumption, low latency, mobility and long transmission range in contrast to other LPWAN technologies which don not offer all ofs the above. More precisely, this project analyses the two technologies and compares their technological similarities and dissimilarities. Further, some experiments were performed in a real environment in order to confirm some of their specifications and find which technology is more appropriate for which application domain. Also as a means of an example, it is shown that both technologies are capable to be used into the near future and create a smart city.

Table of contents

LIST OF TABLES

LIST OF FIGURES

Chapter 1

General Introduction-Internet of things and LPWAN technologies

The term Internet of things (IoT) refers to the creation of a new more productive and autonomous environment, by interconnecting the different devices. In the IoT, devices can communicate with each other or/and interact with humans. Moreover they can be accessed, controlled and monitored remotely, thus, creating a new digital world. As a result smart environments can be created such as a smart home or a smart city. Sensors, actuators and devices are all collaborating together in order to offer a given smart service. As an example of a smart home automatically switches off an energy hungry device when the house occupants are away and inform them of such a decision. Another example is of a smart city, where actuators and sensors collaborate with each other or with citizens in order to protect the environment by locating a fire, or by informing the citizens of available parking slots etc.

IoT applications can make the humans life quicker, simpler and more comfortable. They can be divided into the following four representative categories: Business/Manufacturing, Security, Healthcare and Retail as shows in the picture [Figure1.1 Categories of IoT applications[16]]. Each IoT application focuses on different domains and requires different demands from the technology that will be used to connect it to the internet

For instance some IoT applications require on e.g. minimum power consumption, whereas others IoT applications require minimum latency, maximum reliability and Qos, etc.

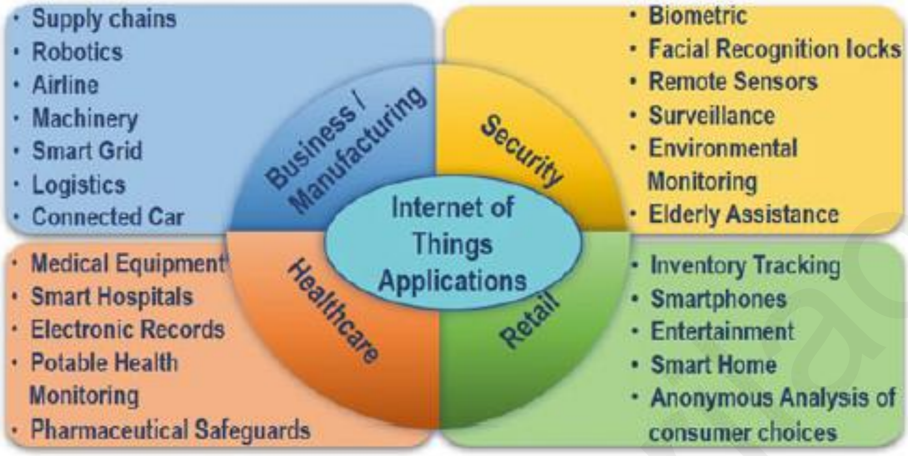


Figure1.1 Categories of IoT applications[16]

Over the last few years, IoT have been developed significantly, invading people's everyday life since they have already been incorporated in various fields. It is expected that millions of different devices will be connected with each other requiring extremely high demands for this interconnectivity. One of the main requirements is that these devices have continuously connectivity while consuming low power in the transmission. It's essential to keep the connection on in order to monitor, process, analyse and send the appropriate information on time and thus allow the receiver to take the necessary actions. Also, they must consume minimum power while operating because it's impossible to change frequently the battery of devices. Furthermore, they need a technology that will help them reach their final destination and decode the packets successfully even if their destination is kilometres apart. Devices may be located in a remote or in hard to reach areas such as deep in forests, so it's essential that the packets successfully arrive at the receiver and are decoded correctly. Also, this must be performed with minimum latency since latency is extremely important for the IoT as it can be fatal in some cases. Further, the goal is to connect these devices into the internet with low cost. Subsequently, devices must have simple hardware and low complexity in order to reduce the manufacturing cost. The final requirement is a large coverage with the support of hundreds or even thousands of devices without any interference with each other.

The current technologies such as Wi-Fi, cellular networks, Bluetooth etc. cannot support this remarkable evolution and its extremely high requirements.

- Wifi is able of sending data with high data rates and achieving low latency. However, the signal can travel only in small distances which it’s not ideal for the IoT connectivity. The higher the data rate, the smaller is the produced electromagnetic wave and as a consequence it weakens more easily as it passes through obstacles. Therefore, it can travel only in small distances.
- Cellular networks can achieve longer distances with the disadvantage of battery drawn due to the need of sending the signal with higher power in order to successfully arrive and be decoded correctly from the receiver.
- Bluetooth can be battery efficient but the maximum achieving distance is only 100m which is not ideal for the IoT interconnectivity.

For instance, considering IoT applications for “smart applications”, Wi-Fi , Bluetooth or Zigbee technology can be used for the smart home. However, all of them have a limited distance of only 100m and thus they are not possible candidates when the distance increases to the range of kms, for example to cater for a smart city. Cellular networks are candidates in such a case, since they can achieve longer distances. Nevertheless, even though cellular networks can achieve longer distance, they have high licensed cost and low battery lifetime and subsequently they are not ideal for the WAN IoT interconnectivity.

Since several issues have been raised in the current technologies, solutions have been created in order to connect these IoT devices over longer distances (in the order of kms). One of the most attractive solutions is the creation of the LPWAN technologies. LPWAN technologies are a group of technologies that can effectively connect the IoT devices into the internet meeting all of their high demands. They are a low cost, low data rate and low power solution, and they are considered suitable for applications that exchange small amount of data and infrequently in a wide area. However, note that they are considered unsuitable for applications that need high data rates.

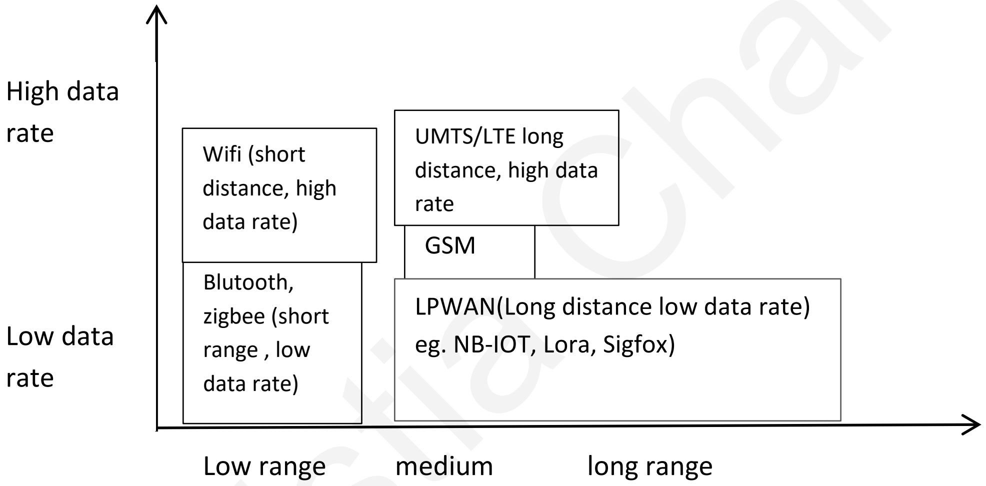

High data rate
Low data rate
Wifi (short distance, high data rate)
Blutooth, zigbee (short range , low data rate)
UMTS/LTE long distance, high data rate
GSM
LPWAN(Long distance low data rate) eg. NB-IOT, Lora, Sigfox)
Low range
medium
long range

Figure 1.2 Range and data rate for different wireless technologies

LPWAN technologies can achieve the best compromise of highest range with low data rate in contrast to other wireless technologies such as Wifi, Bluetooth, Cellular Base Stations, etc which can attain smaller distances with either high or low data rate as shows in the picture [Figure 1.2].

LPWAN technologies were created in order to serve efficiently the IoT connectivity and they have already become popular in industrial and research communities. Their success lies on the ability to massively connect distributed devices that are located over a large geographical area and also on the ability to achieve a reliable connection and a long communication link with low cost and low power consumption. Besides their similarities they have some different manufactured specifications since each one of them was designed to serve specific kinds of applications. The most popular LPWAN technologies are the Lora and NB-IOT technology which are going to be analyzed and compared through their manufactured specifications and through some experiments in a real environment.

Motivation:

Over the decades the term IoT has been raised significantly. It's a fact that IoT devices and applications can improve people's everyday life as they can connect millions of different devices such as sensors, cameras etc into the internet. IoT has already been incorporated in various fields and it's expected that more IoT devices will be interconnected into the near future. However, IoT connectivity is very demanding as in most applications it needs low latency, high capacity, long transmission range, long battery life and low power consumption while transmitting data. IoT devices may be located far away from a GW or in hard to reach areas so it's essential that the technology that will used to connect the IoT devices will successfully transmit the data into the receiver and will provide continuously connectivity with low power consumption. As current technologies are unable to transmit in long range with low power consumption new technologies were created. Therefore, LPWAN technologies were created in order to serve the IoT connectivity. LPWAN technologies have a mutual goal, to effectively connect the IoT devices into the internet. Although, they are different and they were created in order to serve different kinds of applications. Some of them are using unlicensed spectrum to transmit data like LoRa , SigFox etc and some others are using licensed spectrum such as NB-IoT,LTE-M,EC-GSM-IoT.

Subsequently, the motivation arose since the creation of LPWAN technologies to analyze and compare these. As there are a lot of LPWAN technologies this project will focus only in the most popular technologies which are NB-IOT and Lora. From the unlicensed spectrum group Lora was chosen because:

- It's the only technology that can build a private network and offer integrity and confidentiality to the applications.
- send many packets per day. The number of packets that lora can send is regulated by the duty cycle and the use of the spreading factor
- Could be established in Cyprus and thus explore its real performance.

From the licensed spectrum group NB-IOT was chosen because:

- it can be implemented both in GSM and LTE whereas LTE-M and EC-GSM-IOT can only be implemented in LTE and GSM respectively
- LTE-M can achieve higher data rate because it can support real time applications which was not the aim of this project. EC-GSM-IOT has higher power consumption than the other two technologies so it's not an option.
- Could be also be established in Cyprus and therefore explore its real performance

Both technologies can be compared as they can achieve mobility, long transmission range, battery saving, integrity, confidentiality and continuously connectivity. Although, they have some different specifications and they can serve different kinds of applications.

Objectives:

Despite their mutual goal each LPWAN technology can be used on specific kinds of applications. Therefore, the main purpose of this project is to analyze the NB-IOT's and Lora's main networking characteristics and architecture, compare their manufacture similarities and dissimilarities and finally establish some experiments using both technologies into environments in order to observe their real performance. The primary aim is to

- perform different experiments into line and non-line of sight environments (LOS, NLOS),
- observe their transmission range and latency, under a realistic scenario.
- confirm or not their published manufacturer's specifications
- conclude, if the two technologies can serve efficiently the IoT
- identify in which applications each one is more appropriate to be used based on real data.

Chapter 1: describes with details the IoT(internet of things) and the need of the creation of the new LPWAN technologies. This chapter also explains the motivation and the objectives of the current project.

Chapter 2: describes the LPWAN technologies and focuses on Lora and Nb-IoT which are the main technologies in this project. Also, in this chapter for both technologies their architecture, specifications, any possible interferences due to use of the unlicensed spectrum considering the Lora technology and their real performance according to real experiments that were established around the world are explained.

Chapter 3: Compares the manufacture similarities and dissimilarities of the two technologies
Chapter 4: Report the results from real experiments that were established using the two technologies in Cyprus. Also describes the hardware and software that was used in order to make these experiments.

Chapter 5: Summarize the above results and make a final comparison of the two technologies.

Chapter 6: specifies the overall conclusions about Lora and Nb-IOT technology. Further, future work for this project is described.

Chapter 2

Background on IoTs Wide Area Networking Technologies

LPWAN technologies are ideal candidates for serving the IoT efficiently and with low cost. More precisely, their design allows them to have an excellent signal penetration, making them appropriate for devices that are located in hard to reach areas such as basements or deep in forests. Thus, they are sufficient for indoor or outdoor areas as they can achieve a long distance ranging from meters to tens of kilometers. This is due to the low data rate and low frequencies that they use. Therefore, a bigger waveform is produced and consequently it can reach longer distances and experience less attenuation. Furthermore, they can accomplish ultra-low power operation due to the fact that devices only wake up when they transmit or receive data. In the uplink communication they wake up only when they have data to transmit whereas in downlink they make sure to listen when the base station has data to send[9]. This is accomplished by listening for downlink info for a short while after an uplink transmission or with scheduled time slots. Further, some of the technologies use the ALOHA method which saves them even more energy as they do not consume extra power for the synchronization. Thus, their battery can last up to 10 years. Moreover the hardware complexity is removed from LPWAN chips and as a result this saves energy because devices do not make unnecessary complex operations causing drawn of battery and also the cost is reduced substantially.

To continue with, they are separated into two groups: those that transmit in a licensed spectrum such as NB-IOT,LTE-M and those that transmit in unlicensed spectrum such as LORA,SigFox etc. Technologies that transmit in a licensed spectrum are characterized as more securable, with low latency as they use a licensed spectrum in their operation. NB-IOT, LTE-M and Ec-GSM-IOT are able to coexist with other technologies without any interference due to the lower frequencies that they use. Subsequently, they have easier implementation, because there is no need to create a new network in order to use them, as current cellular networks can be used. However, their deployment is restricted to the areas containing the cellular networks.

Contrariwise, technologies that transmit in an unlicensed spectrum have the advantage to be deployed in all areas with the ability to be expanded in all desired areas. Extra securable algorithms must be added to these technologies in order to keep the confidentiality and integrity of the packets as they use an unlicensed frequently used spectrum(2.4 Ghz) in order to operate. This unlicensed spectrum is also used by other wireless technologies such as wifi,Bluetooth and Zigbee so interference can be caused , resultantly with higher latency. Although, Lora technology faced the higher latency problem by creating the Class C which can be used for real time applications and offer extremely low latency.

2.1 LoRa and LoRaWan

One of the new technologies that have been created is the Lora and LoRaWan protocol which is a low power wide area network technology that can be constructively used in many applications such as in smart cities or in smart environments. This is due to its long range coverage that is estimated to reach several kilometres and also for its extremely low power capabilities. The technology was released by the Lora Aliance and it uses the 2.4GHz unlicensed spectrum in order to operate. Further, LoRawan is a mac layer protocol which is based on the ALOHA approach and as a result lower energy is consumed. The physical layer uses the Lora modulation to send the data which is based on the CSS(Chirp Spectrum technique)[1].Spread spectrum techniques are more resistant to interference and noises and they offer higher security as they are robust to attacks. Lora can use a spreading factor ranging from 7 to 12 and choose between three different bandwidths: 125,250,500 Khz. The higher the bandwidth, then the higher is the data rate that can achieve[8],whereas the higher is the chosen spreading factor the lower is the achievable data rate. Moreover, it’s the only technology that can built private networks[5] as it uses two layers encryption, one for the network and one for the application .

Due to its suitable characteristics, LoRaWan protocol is one of the most attractive protocols for the IOT interconnectivity. It can achieve mobility, long range communication, low power consumption, high immunity in noises, a reliable and a securable link supporting millions of devices. The Lora network has the potential to extend in the future by only adding new Lora gateways.

Despite its attractive characteristics, the technology operates in the frequently used unlicensed band 2.4GHz so coexisting issues must be considered and studied further. It’s essential to study its coexistence with: other wireless technologies and with other Lora networks

2.1.1 LoRaWan main chatacteristics

Characteristics	**LoRaWan**
Topology	Star of Stars
Modulation	SS chirp
Access method	Class A: ALOHA, Class B:Slotted Aloha, Class
Date Rate	290bps - 50kbps
Link Budget	157 dB
Packet size	154 dB
Battery Lifetime	8 -10 years
Power Efficiency	Very High
Security/Authentication	Yes (32 bits)
Mobility Latency	Low(almost zero)
Range	2-5 km urban,15 km suburban,45 km rural
Interference Immmunity	Very High
Duty cycle	1%
Scalability	Yes
Adaptive Data rate	Yes
Mobility/Localization	Yes

Table 1 LoraWan main characteristics

One of its' main characteristics is the great devices' battery lifetime that is estimated to last 8-10 years. This is due to a number of reasons:

i. due to the ADR(adaptive data rate) which regulates the devices transmission power when the SNR is too high or too low. The primary purpose it to send maximum data with minimum power consumption

ii. Due to the low transmission power which can be only 14dB. This low transmission power is based on the fact that the protocol uses the spread spectrum technique, which means that devices can send data with lower power and data still be decoded from the receiver.

iii. Due to the fact that nodes are not continuously connected to the network collecting network results, which can consume significant power. This asychronization is due to the LoRawan protocol that is based on the mac protocol ALOHA and it uses different classes to regulate the power consumption and the latency. If it uses the class A it saves great amounts of energy causing a bigger device battery lifetime. Thus, the amount of energy that is being consumed by a device depends on the selection of the LoRaWan classes.

More precisely, LoraWan devices check the downlink channel and the synchronization messages based on programmable intervals [1]. The LoraWan uses 3 types of classes in order to specify the frequency of those intervals as it is shows in the picture[Figure2.1.1.2]. First class A, is considered to be power efficient but it has high latency. A device after transmitting a packet it waits for two intervals to get downlink information. If it doesn't receive the info during this time, then it must wait for the next programmable intervals to get it. Therefore, this cause high latency and reduced power consumption. The second class B has medium power and low latency as it gets extra scheduled downlink slots, thus reducing the latency. These extra scheduled time slots can increase the power consumption of the device. Finally, the third class is type C and it has high power consumption but extremely low latency. A device can continuously listen for downlink info as it has continuously open downlink slots and it stops listens only when transmitting a new packet. Therefore the latency is extremely small, whereas the power consumption is extremely high. This class is mostly used in real time applications and when this drawn of the battery is not a problem. Subsequently, the low power consumption is contradicted with the latency. The selection of the appropriate class is according to the application needs and a device can switch between classes in order to reduce great amount of energy. Therefore, all the devices must support at least class A whereas classes B and C are optional.[6]

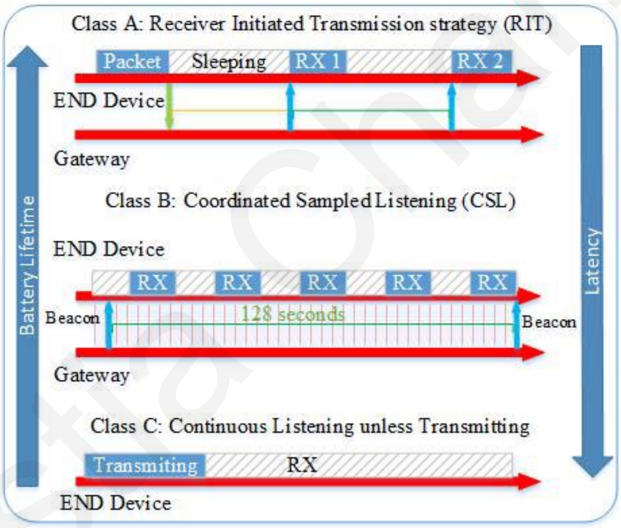

Class A: Receiver Initiated Transmission strategy (RIT)
Packet
Sleeping
RX 1
RX 2
END Device
Gateway
Class B: Coordinated Sampled Listening (CSL)
END Device
RX
RX
RX
RX
RX
Beacon
128 seconds
Beacon
Gateway
Class C: Continuous Listening unless Transmitting
Transmiting
RX
END Device
Battery Lifetime
Latency

Figure2.1.2.2 Implementation of the three classes A,B and C

Another great characteristic is that it can achieve long transmission range(2-5 km urban,15 km suburban,45 km rural) because of the spread spectrum technique that it uses. As mentioned, LoRa technology is based on the Chirp Spread spectrum which means that it can get extremely high immunity in noise, transmit the data in a noisy environment and the decoder still is available to successfully decode to message. Another advantage of the spread spectrum technique is that multiple users can send data simultaneously without any interference due to the different spreading codes which are unique for each user. Furthermore, spread spectrum technique adds extra security because the message can be decoded only from the one who knows the spreading code. Lora uses a spreading factor ranging from 7 to 12. A spreading factor determines the length of the spreading code and calculates the encoded bits. Each bit is encoded using the spreading code. A higher spreading factor results in greater noise immunity, further distances and thus lower transmission rate, more power consumption and higher latency due to the fact that extra transmissions will be created in order to send the data. Therefore, if it uses SF=12 then it can achieve even longer distances and the total covered area will be even higher since the signal can travel further .In addition, LoraWan uses coding rate which help decoding the packet correctly and find the approximate bits without sending the packet again. Coding rate is like a probabilistic algorithm that corrects the error bits in the receiver with the correct bits. Another factor that helps to achieve the long transmission range is the link budget that is estimated at 157dB. The greater the link budget then the greater is the distance that can be achieved.

To continue with, when an end device is in a static position, then the ADR(adaptive data rate) can be performed by the network server allowing the end device to send messages in different data rates according to its SNR. Thus, the data rate is selected differently for each end device. When the network server regulates the transmission power then either smaller or greater amounts of data will be sending according to the regulation. This data rate has a range from 290bps-50kbps and it depends on the selecting frequency and spreading factor. If the end device is in a non-static position then the data rate is selected by the application layer of the end device [7].

Moreover LoraWan can also achieve mobility which is important in the IoT because the devices may change location while transmitting. Whenever an ED changes location it is configured to send a message to the NS in order to inform it about this action. As a result a

NS always know the location of the end device and can send to it downlink info. If the end device sends vulnerable and important data it can use the acknowledgment method to indicate if the NS received the packet. Consequently, the end device will know if the NS received the data during its mobility. Further, the signal is not forwarded to a single GW but is catch up by all the gateways that can catch this signal. Therefore the mobility latency is almost zero.

The LoRaWan protocol is the only protocol that can create private networks[5]. The protocol allows devices to transmit data only if they got the necessary permission through the activation procedure. Also the packets are encrypted into two layers, network and application layer in order to achieve confidentiality and integrity. It uses the powerful AES algorithm for the encryption/decryption for each message in the network.

Further, the technology as every other unlicensed technology has a duty cycle. Duty cycle is the amount of time that the technology can occupy the channel and for Lora is 1%. Subsequently for 1% duty cycle it can occupies the channel for about 36seconds/hour.

2.1.2 LoRaWan security

One of the most important aspects of LoRaWan is that it uses AES128 encryption to encrypt the packets through the network transmission. Lora is considered to be the only technology that can be used to construct private networks [5]. The creators of the technology released two versions of LoRaWan, V1.0 in 2015 and v1.1 in 2017 with security improvements inside. The first version seemed to have security vulnerabilities whereas the second version corrected them, thus making it a more securable protocol. Therefore, the manufacturer must be extremely careful and add additional security to the application if the confidentiality is really important.

In order for a device to send a message in the LoraWan network it must be activated at first. The activation can be done in two ways: either via Over-The-Air(OTTA) or via Activation by personalization (ABP). The ABP is the same in both versions [5] and it can be done by the pre confirmation of the appropriate keys that will be used in the end devices. The only difference in the ABP is that there are different keys used in V1.1 and in V1.0. The OTTA activation can be achieved by the exchange of two messages: join-request message that is send from the end device and join-accept message that is send after the device validation from the network. Every time that an end device losses communication it must be activated again, be verified with the network and get again the appropriate keys to establish the secure communication.

2.1.2.1 Version 1.0

In order to perform the activation the end device must send the join-request and then the application server response with an answer if the message passes all the checks as shows in the picture[Figure 2.1.2.1.1]. After the successful activation the end device can encrypt the messages and relay them to the network preventing malicious attacks.

An end device has as pre-configured the AppEUI and the Appkey which is only known by the device and the application server. A DevNonce key is also generated which is a random unique key produced by the ED and its primary purpose is to prevent replay attacks. The end device in order to join the network it sends the join-request message which includes all of the above keys. The message is forwarded to the gateways and the gateways relay the message to the network server. The network server then checks the integrity of the message by performing some security checks and if it’s valid then it forwards the request to the application server. Then the application server is responsible to check if the device belongs to the supported devices and assign to this device a unique key. This key will be later be used by the end device in the encryption procedure.

Specifically, it responses back to the Network server with “AppNonse” key. The network server before forwards back the response message to the gateways it appends a NETID key, some configuration parameters and the Message Integrity Code(MIC) [5]. The MIC helps to determine if the given message have been changed. Further, when the response message reaches its final destination then the end device decrypts it in order to get the information from the network. The most important info that will help the device encrypt the messages is the APPNonse key that was given by the application server. This key is used to create unique session keys: the AppSKey(Application session key) and NwkSKey(Network session key). These keys are unique and changes in every new activation and in every device and they are responsible for the integrity and the confidentiality of the messages. The network session key is responsible for keeping the integrity of the packet and the application key is responsible for the confidentiality of the payload and only the application server can decrypt the payload.

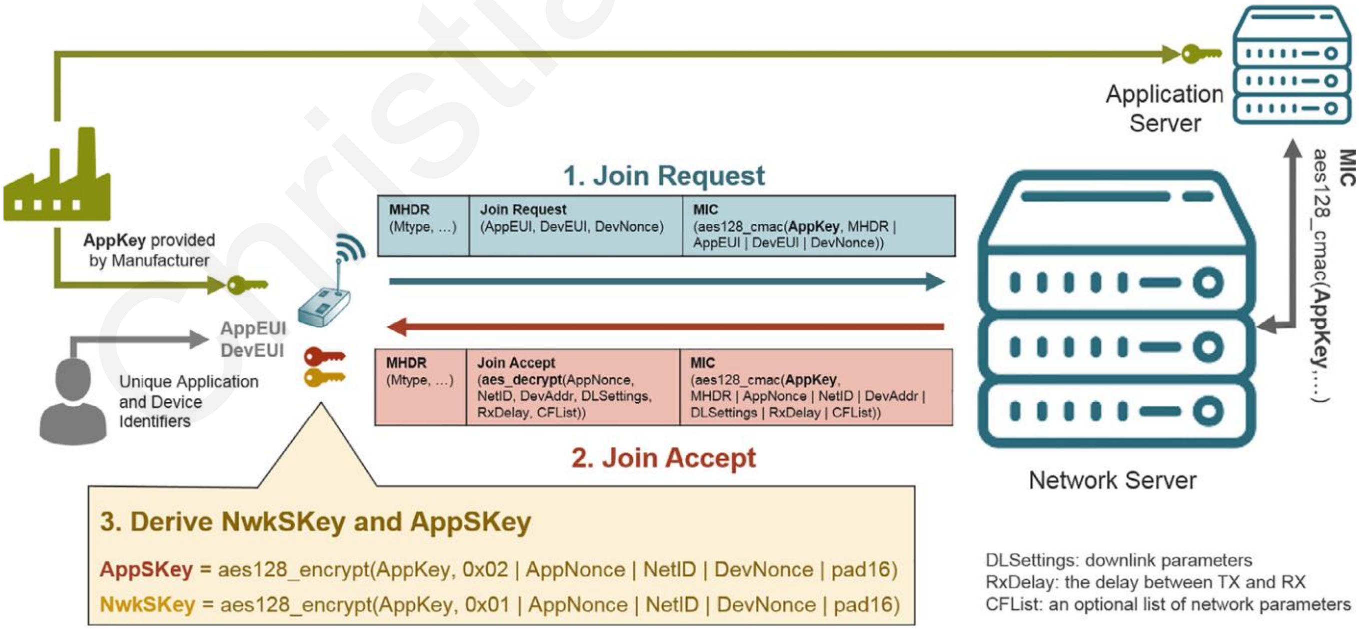

Application Server
MIC
aes128_cmac(AppKey,...)
1. Join Request
MHDR (Mtype, ...)
Join Request (AppEUI, DevEUI, DevNonce)
MIC (aes128_cmac(AppKey, MHDR | AppEUI | DevEUI | DevNonce))
AppKey provided by Manufacturer
AppEUI
DevEUI
Unique Application and Device Identifiers
MHDR (Mtype, ...)
Join Accept (aes_decrypt(AppNonce, NetID, DevAddr, DLSettings, RxDelay, CFList))
MIC (aes128_cmac(AppKey, MHDR | AppNonce | NetID | DevAddr | DLSettings | RxDelay | CFList))
2. Join Accept
Network Server
3. Derive NwkSKey and AppSKey
AppSKey = aes128_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce | pad16)
NwkSKey = aes128_encrypt(AppKey, 0x01 | AppNonce | NetID | DevNonce | pad16)
DLSettings: downlink parameters
RxDelay: the delay between TX and RX
CFList: an optional list of network parameters

Figure 2.1.2.2.1 LoraWan v1.0 over the air activation procedure(OTAA)[5]

The most important problem that was observed in the version 1.0 was that the derivation of AppSkey and NwtSkey was created from the same AppNonce key which was generated by the application server. This was vulnerable to attacks and therefore in the new version the two keys are generated using different keys.

2.1.2.2 Version 1.1

In the newer version a new server is introduced called Join Server (Js). As in V1.0 there are some preconfigured keys in the devices. The preconfigured keys in V1.1 are JoinEUI, DevEUI,NwkKey and Appkey. A DevNonce key is generated as in V1.0 and as mentioned it is responsible to prevent replay attacks. The OTTA procedure is performed as follows. The ED communicates with the gateways, then gateways relays the message to Network server (NS) and NS to the new Join Server. As the Network server receives the join request from the ED it performs some security tests and it passes it to the Join Server. Then the Join Server checks if the ED belongs to the supported devices list. If there is a match then it response with JoinNonce as the application server did in the version 1.0. Then it forwards the packet back to the NS. The NS in its turn appends the NetID, some configuration parameters and the MIC. The ED receives the packet decrypts it and get the necessary info.

In the final part session keys are generated using the JoinNonce,DevNonce,JoinEUI and Nwkkey keys for creating FNwkSintkey, SNwkSintkey and NwkEncKey and using the JoinNonce, JoiEUI,DevNonce and Appkey the AppSkey is generated . A FNwkSintkey(Forwarding network session integrity key) and a SNwkSintkey(Serving Network Session integrity key) are used for the MIC for uplink and downlink messages respectively[5]. Further, NwkEncKey and AppSkey are responsible to keep the integrity and confidentiality of the packets[5]. The appSkey is responsible to keep the confidentiality of the payload.

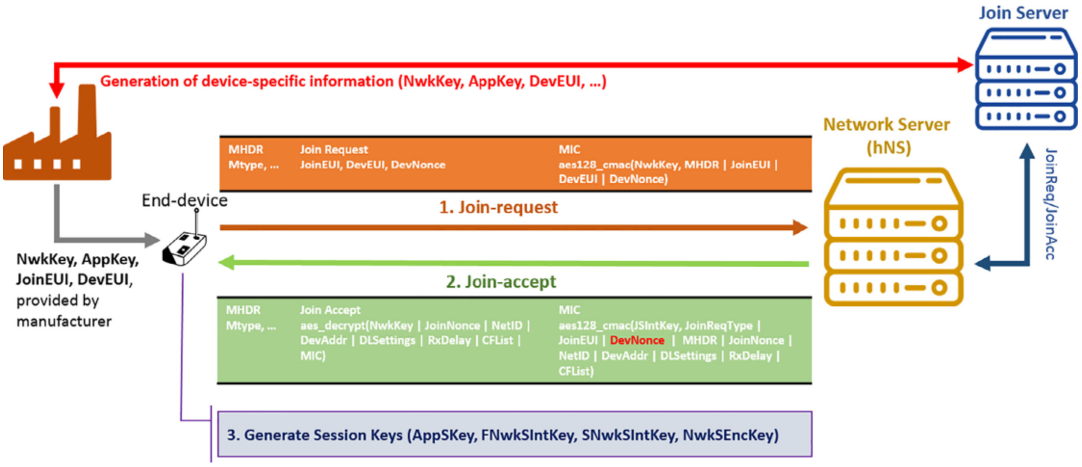

Join Server
Generation of device-specific information (NwkKey, AppKey, DevEUI, ...)
Network Server (hNS)
JoinReq/JoinAcc
End-device
NwkKey, AppKey, JoinEUI, DevEUI, provided by manufacturer
MHDR
Mtype, ...
Join Request
JoinEUI, DevEUI, DevNonce
MIC
aes128_cmac(NwkKey, MHDR | JoinEUI | DevEUI | DevNonce)
1. Join-request
2. Join-accept
MHDR
Mtype, ...
Join Accept
aes_decrypt(NwkKey | JoinNonce | NetID | DevAddr | DLSettings | RxDelay | CFList | MIC)
MIC
aes128_cmac(JSIntKey, JoinReqType | JoinEUI | DevNonce | MHDR | JoinNonce | NetID | DevAddr | DLSettings | RxDelay | CFList)
3. Generate Session Keys (AppSKey, FNwkSIntKey, SNwkSIntKey, NwkSEncKey)

Figure2.1.1.1.2 LoRaWAN v1.1 Over the Air Activation (OTAA) procedure

2.1.3 LoraWan Architecture

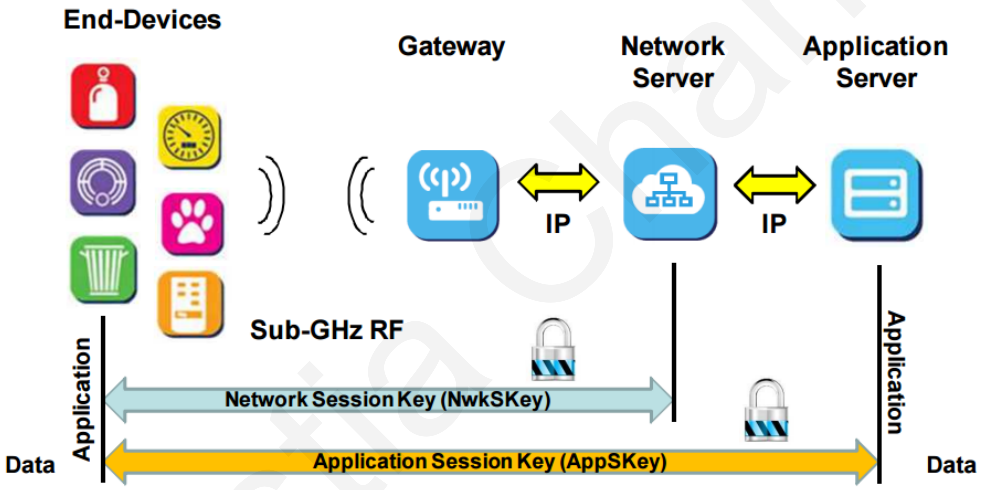


Figure 2.1.3.1 *How the packet is transmitted and manipulating using the LoRaWan protocol and LoRa modulation*

A device that wants to use the LoRa technology and the LoRaWan protocol at first it must get the appropriate permission through the activation procedure as mention in *2.1.2 LoRaWan security part.* During this procedure it receives a unique key that will use later to encrypt the following messages. Every device that uses the LoRaWan protocol has a preconfigured key that is essential for the activation procedure. The end devices' key is also recorded in a preconfigured list in the application server. The application server uses this list to match the two keys and decides if the end device is allowed to send messages through this technology.

After the activation the end device can send messages using the technology. A device transmits its data to a number of gateways not to a preconfigured one using the LoRa modulation for the transmission and LoRaWan protocol to check when to transmit it. An end device according to the class that it uses, either it sends directly a message that it has to send either it waits for the begin of the time interval to send it. This message is catch up by all the gateways that can catch this signal. Then GWs append their RSSI to the message and they relay it to the network server using other MAC protocols such as Ethernet,3G/4G etc.

The network server is the intelligent part and is responsible for a number of things. As it catches all the messages from the gateways it decides which one has the best signal according to their RSSI. Therefore, the gateway that has the highest RSSI is closer to the end device. The network server adds this gateway in the forwarding table in order to use it later to send the messages back to the end device. If the end device is not available to receive the downlink info the network server stores it until the ED wakes up[3] and be able to receive it.

Furthermore, it’s also responsible to check the integrity of the message and it performs some security tests to check it. If its integrity is stable then it forwards the message to the application server. Moreover, the network server performs the adaptive data rate when the end device is in a static position which means that it regulates the transmission power of the end device. More precisely, when a device is in a static position then the ADR is enabled and it sends measurements to the network such as signal to noise ratio and number of gateways that receives these signals[4]. The network server examines these measurements by taking into consideration the current SNRs and the appropriate SNR in order to decode correctly the packet. As a consequence this examine may increase the devices’ transmission power because the data did not decoded correctly due to low SNR or decrease the devices' power due to high SNR.The goal of using the adaptive data rate is to increase the device battery lifetime and optimize the data rates by manipulating the device transmission power.

To continue with, the network server forwards the message to the application server in order to perform the appropriate actions. The application server is the only one that can decrypt and read the message from the end device. When it receives the message it performs security tests in order to check the integrity of the message. Then if the message passes the tests it performs the appropriate actions and response back to the end device.

The NS reply to the end device with latency according to the class that it uses:

- If the end device used the class A then the NS will respond immediately after it receives the uplink message. If the end device is in sleeping mode and the network server has data to send to this specific end device then these data are being queued in the NS until the NS receives a message from this ED, indicates that it has been waken up.
- If it uses class B then the NS will respond according to the pre-defined time interval
- If it uses class C then it response immediately [7]

2.1.4 Lora coexistence

Lora uses the frequently used unlicensed band 2.4 Ghz in order to operate which lead to coexistence considerations and issues that can occur in the future. Many wireless technologies are using the same frequency band such as Wifi,Zigbee, Bluetooth and other LPWAN technologies and therefore coexistence issues drove the attention of many researchers. After many experiments they conclude that Lora network seems to be robust against other wireless technologies when they use the same or neighbouring frequencies. In contrast, considering the inter -interference, Lora devices with same parameters such as frequency and spreading factor can lead to collisions as devices will interfere with each other. Lora exhibits the capture effect in which only the strongest signal survives whereas the weakest signal disappears and as a result packet loss will be created. Therefore, parameters should be regulated if possible in order to avoid those situations especially when Lora devices may be used for critical based applications.

2.1.4.1 Lora inter-interference

Lora devices can develop the capture effect in which the stronger signal suppresses the weakest and only the strongest one survives. Consequently, this causes an unfair network because the further signal never reach its destination as it get supressed from the signal near the base station. This is the near far problem and it’s important to control the receiving signal power in order to avoid unfairness. Subsequently, this can happen when two or more Lora devices use the same parameters such as frequency and spreading factor. If the signal arrives with the different power at the receiver only the stronger one will survive. Further, this will cause many packet drops and retransmissions.

This was the result from an experiment that was established in paper [11] where two Lora devices with same parameters (bandwidth=125kHz and spreading factor=10)started to transmit packets. It was observed that the strongest signal supressed the weakest and the receiver got only the strongest signal. Subsequently, the weakest signal could not be received from the receiver. Thus, they resulted that this is evident that Lora devices cannot use the same parameters[11], otherwise, network degradation will be caused such as packet loss and retransmissions[11].

To continue with, spreading factors are theoretically orthogonal and as a consequence concurrent transmissions with different spreading factors can be created with minor interference with each other. Subsequently, it is desirable to use Lora devices with different spreading factors if possible in order to avoid interferences with each other.

2.1.4.2 Lora coexistence with other wireless technologies

After some experiments that they were established in paper [8] they conclude that Lora devices are robust against wifi signals when using the same or adjacent frequencies. In addition, they deduce that Lora devices with maximum spreading factor(SF=12) can achieve higher immunity against Wi-Fi than Lora devices with lower spreading factors(SF<12). This experiment included only 802.11b/n protocols and Lora devices and they resulted that Lora has high immunity to both technologies. Moreover, it was observed that Lora has higher immunity in 802.11n rather than 802.11b due to the fact that 802.11b is based on Direct sequence spectrum technique and uses complementary code keying modulation[8]. Therefore, this noise-like signal has more influence on lora signals but still Lora signal can be decoded well from the decoder.

For the experiments, they calculated three measurements:

- The power level of lora signal measured at the receiver (C)
- The power level of wifi interfering signal (I)
- The bit error rate , which has to be under 10^{-2} in order for the decoder to decode correctly the signal.(BER)

The power level of the signal was calculated as C-I.

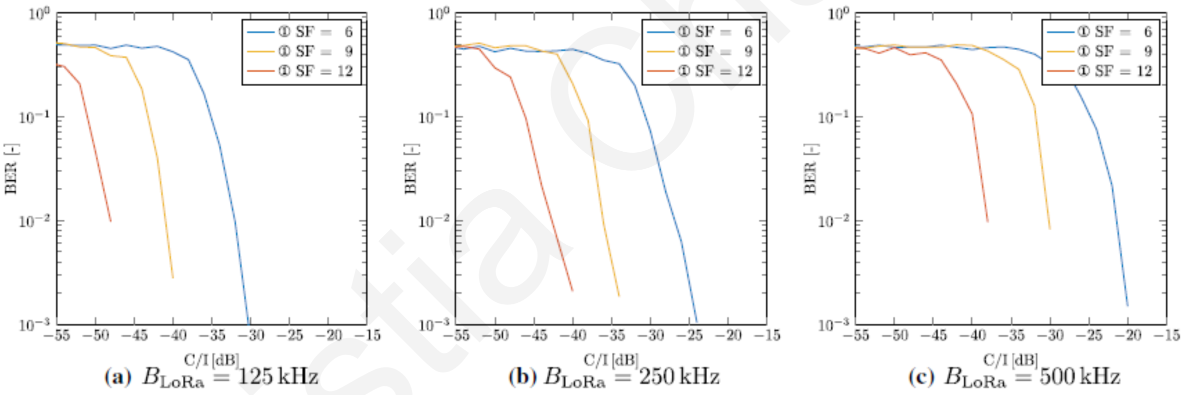
2.1.4.2.1 Co-channel interference

Co-channel interference is a term that is used to describe the possible interferences between two or more devices that are operating on the same frequencies. From the graphs

Results from **802.11b** they resulted that all C-I have negative values and the BER is in a desire level which mean that wifi signals can be higher(20-45dB higher) than the measured Lora signal at the receiver and the lora signal can still be decoded correctly[8]. These values prove that Lora has high resistance at co-channel coexistence senarios[8]. Further, they changed the Bandwidth in which they could choose from 125,250 and 500 Khz and the spreading factor(SF) which can be from 7-12. Subsequently, Lora with the maximum spreading factor (SF=12) and lowest bandwidth =125KHz has the highest resistance at co-channel interference. High spreading factor lead to higher processing gain and thus higher immunity in noises since the signal can travel in even lower values and still be decoded on the receiver. To continue with, signals in a low bandwidth experience less congestion and thus they can be decoded easier from the receiver. Therefore, Lora devices with max spreading factor and lowest bandwidth can offer the highest resistance. Moreover, it was observed that Lora with maximum spreading factor(SF=12) has the highest immunity against Wi-Fi signals in all bandwidths.

In addition, they execute the same experiment using the 802.11n technology and they observed that the C-I values were even lower and the BER was at a desired level as it shows in *Results from 802.11n*. Subsequently, Lora has higher robustness against 802.11n.As mentioned this higher robustness is due to the fact that 802.11b is based on Direct sequence spectrum and the resulted noise-like signal has more influence on Lora. Again the parameters with maximum spreading factor and lower bandwidth have the highest resistance. Thus, they resulted that Lora has high resilience to 802.11n technology.

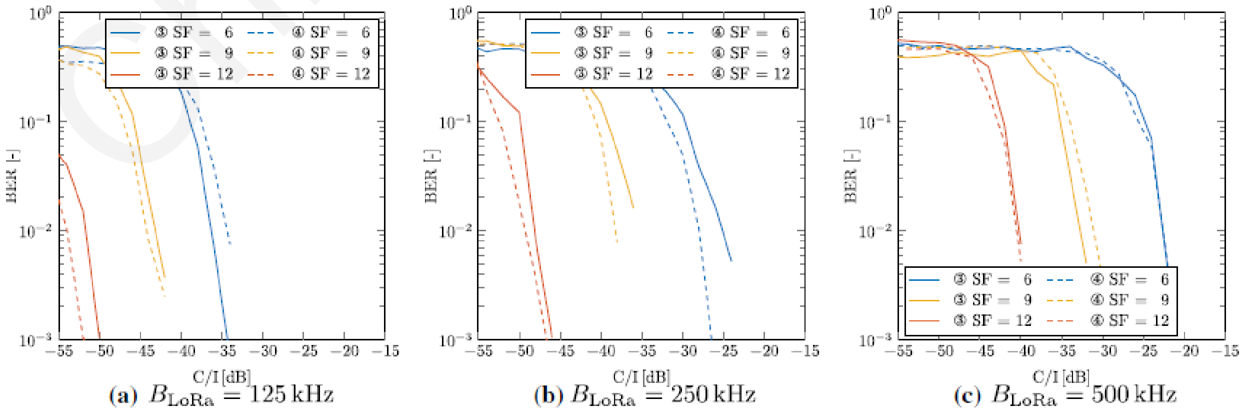
Results from 802.11b



(a) $B_{\text{LoRa}} = 125\,\text{kHz}$ (b) $B_{\text{LoRa}} = 250\,\text{kHz}$ (c) $B_{\text{LoRa}} = 500\,\text{kHz}$

Figure 2.1.4.2.1 Results from co-channel interference for 802.11b

Results from 802.11n



(a) $B_{\text{LoRa}} = 125\,\text{kHz}$ (b) $B_{\text{LoRa}} = 250\,\text{kHz}$ (c) $B_{\text{LoRa}} = 500\,\text{kHz}$

Figure 2.1.4.2.2 Results from co-channel interference for 802.11n

2.1.4.2.2 In-band interference

In band interference refers to the interference that two or more devices may experience due to the fact that they are using neighboring frequencies. In order to observe any possible in-band interference between lora devices and wifi they varied a frequency offset(Δfc) and focused on the BER level and the C-I values. More precisely the C-I values in the vertical axis indicate that the 1%*BER is achieved for every frequency offset (Δfc)[8]. In addition, they examine again the Lora signals with the two technologies 802.11b/n and noted the results.

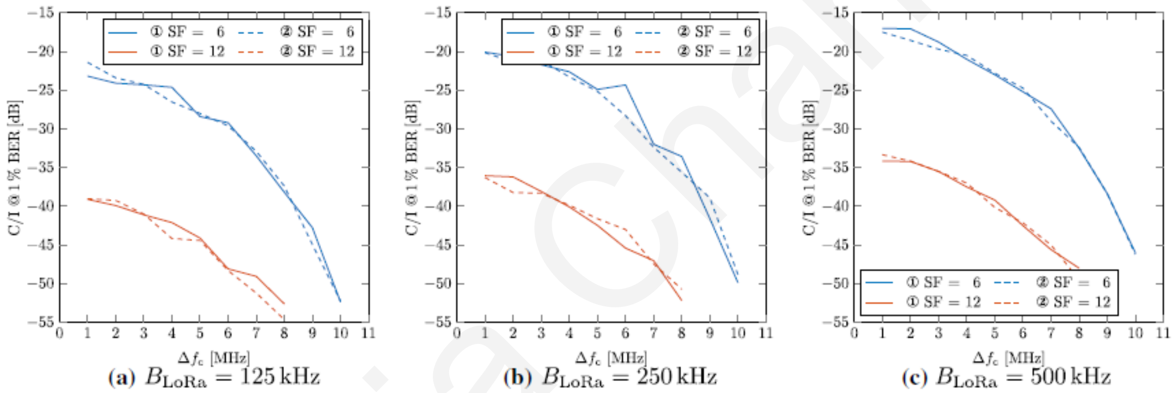
To continue with, the higher is the Δfc means that the frequency space increases and thus lower C-I value(signal power) is required [8]. From the graphs

Taking all the above into consideration, as all the experiments showed Lora has high immunity against both 802.11b/n technologies when using the same and neighboring frequencies. This high performance is due to the spread spectrum technique that it uses which allows it to achieve high interference immunity since the signal can travel under noise and still be successfully decoded. Thus, Lora can coexist with Wi-Fi technologies. However, its performance depends on the power of the interferer signal.

In-band results they resulted that 802.11n technology has a constant resistance against wifi signals and only when the Δfc reach high values there is a rapid decrease in C-I values. This is because the 802.11n uses sub-carrier spacing of 312.5kHz and a single sub-carrier causes a gap (center frequency leakage) [8][19][20]. Subsequently this gap is responsible for causing the constant behavior and only when the frequency increases there is a decrease in the achievable BER. On the other hand in 802.11b technology there is a decrease each time the Δfc increases. Subsequently, this is observed because the space between the adjacent frequencies is increased and thus there is lower need for C-I value.

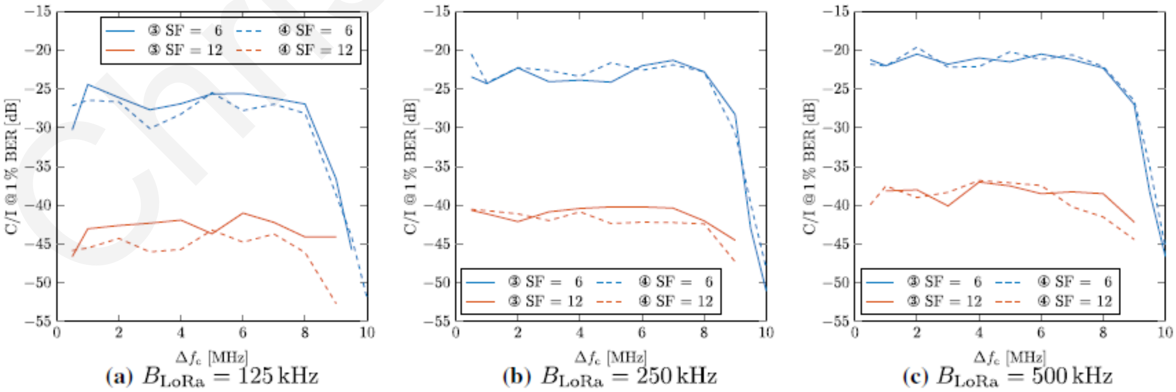
Taking all the above into consideration, as all the experiments showed Lora has high immunity against both 802.11b/n technologies when using the same and neighboring frequencies. This high performance is due to the spread spectrum technique that it uses which allows it to achieve high interference immunity since the signal can travel under noise and still be successfully decoded. Thus, Lora can coexist with Wi-Fi technologies. However, its performance depends on the power of the interferer signal.

In-band results



(a) $B_{\text{LoRa}} = 125\,\text{kHz}$ (b) $B_{\text{LoRa}} = 250\,\text{kHz}$ (c) $B_{\text{LoRa}} = 500\,\text{kHz}$

Figure 2.1.4.2.2.1 results from in-band interference with lora signals interfered with 802.11b wifi signals



(a) $B_{\text{LoRa}} = 125\,\text{kHz}$ (b) $B_{\text{LoRa}} = 250\,\text{kHz}$ (c) $B_{\text{LoRa}} = 500\,\text{kHz}$

Figure 2.1.4.2.1.2 results from in-band interference with lora signals interfered with 802.11n wifi

2.1.5 Performance analysis of Lora

Lora technology drove the attention of many researches the last couple of years due to its promising characteristics. According to [22] there are some important factors and limitations that researches and constructors must know before using the technology. Further, many experiments were established in order to observe its performance in real environments.

2.1.5.1 Overview of capabilities and limitations

As mentioned in the 2.1.1 LoRaWan main chatacteristics , Lora is based on the spread spectrum technique and can use the spreading factor ranging from 7-12. Despite the fact that higher spreading factor can lead to greater immunity in noises and achieve a longer distance because the signal can travel in ever lower values and still be decoded, this technique has also some disadvantages. One disadvantage is the longer time on air as shows in picture [Figure 2.1.5.1] since the packet transmission time last longer due to higher communication range and thus the silent period has a higher duration. Lora as every other unlicensed technology has a duty cycle in which it determines the time that an end device can occupy a channel. The most common duty cycle for the unlicensed bands is 1%. The silent period which refers to the period that the end device remains silent calculates as Ts=Ta(1/d-1)[22] where Ts refers to the silent period, Ta refers to the packet transmission time(time on air) and d is the duty cycle[22]. As shows in[Figure 2.2.5.1] as the spreading factor increases the time on air also increases for a payload of 50bytes having a coding rate 4/5 and a 125khz bandwidth, due to the longer communication link and so as the silent period. Also another disadvantage is the higher latency and lower data rate. The higher the spreading factor means the higher is the spreading code and thus there are more encoded bits in the payload. Therefore, this causes extra transmissions and subsequently a higher delay.

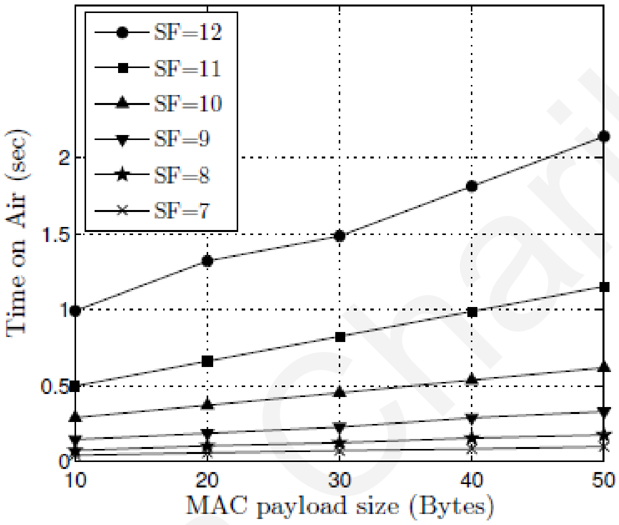


Figure 2.3.5.1 Time on Air of LoRaWAN with code rate 4/5 and a 125 kHz bandwidth.

To continue with, Lora experiences another limitation. As the number of devices increases there is a significant decrease in the throughput due to possible collisions and interferences that can occurred. As mention in 2.1.4.1 Lora inter-interference end devices with the same bandwidth and spreading factor can experience interferences as the technology exhibits the capture effect and thus only the strongest signal survives. The decrease in the throughput and therefore the decrease in the number of received packets as the number of nodes increases is showing in the picture[Figure 2.1.5.1.2]. It is observed that for the maximum number of devices (5000), with 10bytes payload and 3 channels, they have the lowest number of received packets. The graph also shows that for low number of nodes e.g 250 the number of received packet increases, but again it is limited due to the duty cycle[22]. End devices have limited time of using the channel based on duty cycle that they are using. So, after the completion of the allowing time of using the channel the duty cycle stabilizes the throughput as it cannot let it increase [22].

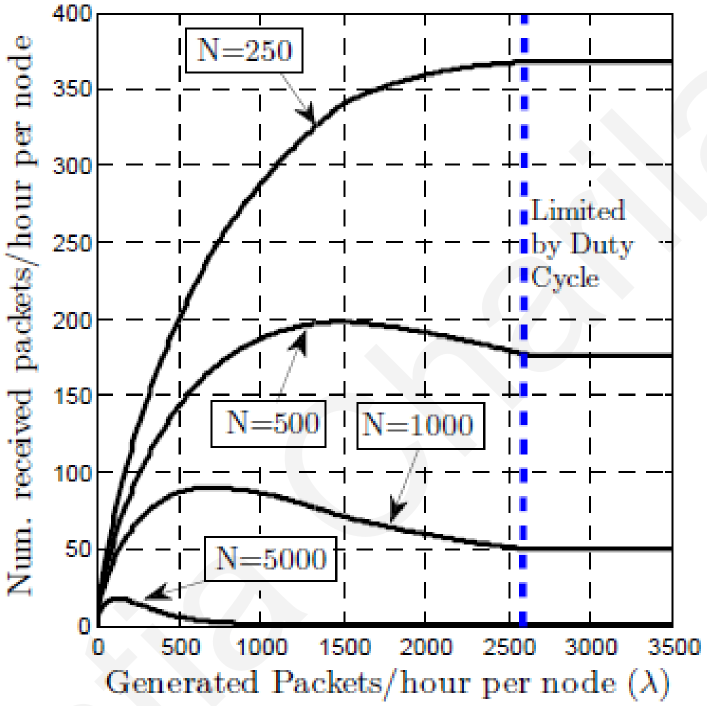


Figure 2.1.5.1.2 Number of received packets in (250,500,1000,5000) nodes

2.1.5.2 Experiments in real environments:

Many experiments were performed in order to observe the real performance of the Lora technology in different environments. One of them that was established by [18] focused on the performance on the technology considering its operation in three different environments: line of sight where there were no any distractions so as to examine its real performance, in a dense forest in order to investigate if there are any distractions due to the dense vegetation and in a urban area in order to study its performance when there are obstructions such as buildings, towers etc. They evaluate the Lora network considering any packet loss in the different environments. They used a small distance of only 1km for this experiment since the maximum range was not considered in this investigation. A final investigation that was performed was the elevation of the GW in order to attain a free line of sight and noted if the elevation would improve the Lora network performance.

Experiment:

For the experiment they used an ED which was preconfigured to send a 2 byte packet for every 10 seconds. They used the 125kHz bandwidth and spreading factor ranging from 7 to 12 which was selected from the GW. Further, they used a transmission power of 14dB and coding rate 4/5. They include aligned and misaligned antennas in order to investigate the difference in its performance using these two kinds of antennas. The ED was moving apart from the GW until the 1km which was the maximum distance. The experiment took place in the three different environments: environment with no obstructions (line of sight), dense forest and urban area and they noted the results. The final experiment was the elaboration of the GW while the ED remained stable in order to determine any network performance improvement.

Results:

In order to determine the network's performance they observed the RSSI and SNR values. RSSI indicates that signal quality where, as the ED moves apart from the GW the signal quality decreases. The SNR values indicate if the packet can be decoded or is being corrupted. As the ED moves apart the SNR decreases since the signal experience more noise and interference. Under ideal circumstances signals that have values under zero cannot be decoded from the receiver. However, Lora is based on the spread spectrum technique which means that the signal can have negative SNR value and still be decoded from the receiver due to the processing gain that can attain.

i. Line of sight (environment with no obstacles):

The results for the environment with no obstacles are shown in the figure [Figure2.1.5.2.1]. It is observed that for the aligned antennas the performance is better than in the misaligned antennas. As expected the RSSI decreases as the ED reaches its maximum distance (1Km). The misaligned antennas had a packet loss at 900m whereas the aligned antennas experienced no any packet loss. Therefore, this confirms the theory assumption that the signal can travel in long distances with minimum attenuation.

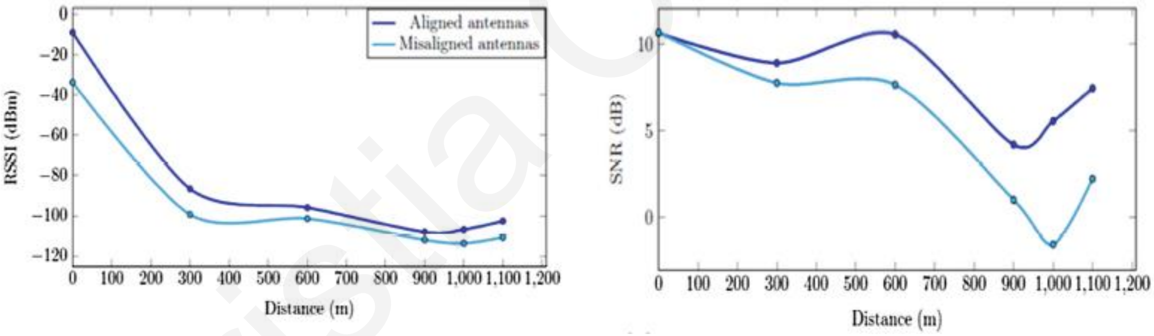


Figure2.1.5.2.1 Results from environment without any obstructions

ii. Dense forest:

Again the results show that the aligned antennas have a better performance than the misaligned antennas. In a dense forest the RSSI decreases as the ED moves apart from the GW and the signal quality gets lost in a smaller distance. This is due to the dense vegetation where the signal experience attenuation and therefore can reach smaller distances than the environment without obstacles. For the misaligned antennas the signal reached maximum distance of 500m and for the aligned antennas the maximum distance was 600m. The signal got weak from the 400m in the misaligned antennas whereas in the aligned antennas the signal got weak from the 500m. When the signal got weak (in 400m and 500m) the SNR values were decreased and reached negative values. However, due to the fact that Lora is based on the spread spectrum technique the packet can travel in a noisy environment and still be decoded from the receiver. Therefore, the packet could be decoded even if the SNR values were below 0.

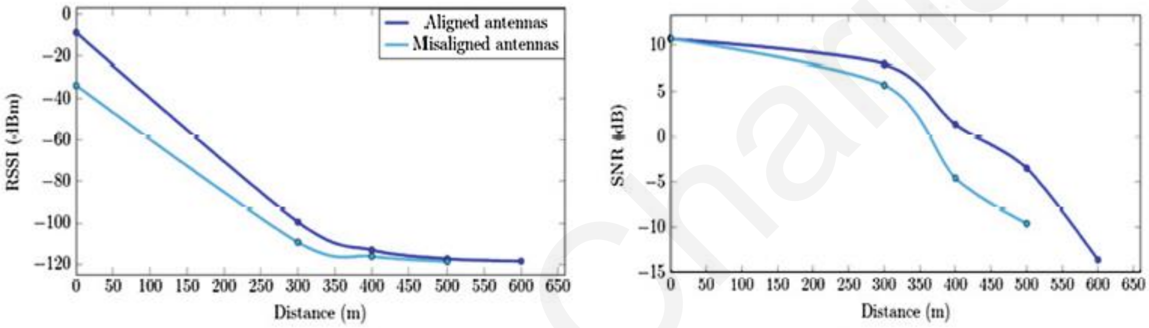


Figure 2.1.5.2.2 Results from dense forest environment

iii. Urban area:

They also performed the same experiment in a urban area where there were houses located on the same height[18]. The results from this experiment were as expected. The distance was even smaller due to the obstructions that the signal faced during its transmission. For the aligned antennas packets could be decoded until the 300m whereas for the misaligned antennas the signal could be decoded only in 150m distance. Therefore, obstructions like houses have more impact on the signals since they get more attenuation while passing through them.

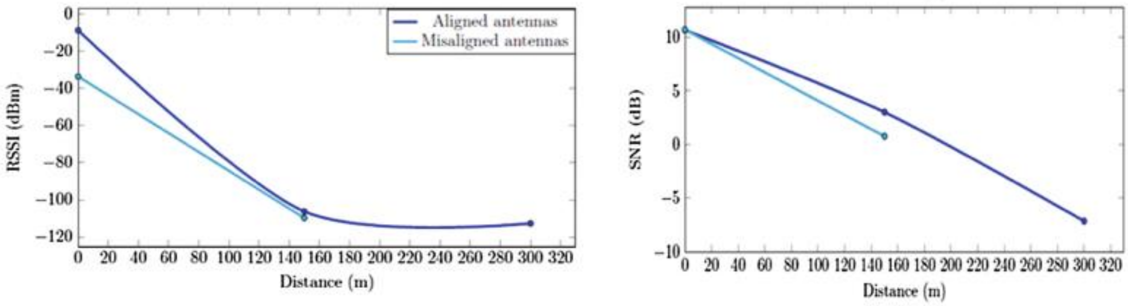


Figure 2.1.5.2.3 Results from urban area

iv. Elaboration of GW:

The final experiment involved the elaboration of the GW whiles the ED was in a static position**.** The results are shown in the figure[] and as expected the GW as it is elaborated the quality of signal and thus the RSSI is getting stronger as it is close to reach the free line of sight. Further, it is observed that while the GW reach a height of up to 30m the RSSI remained stable with a fair quality of signal. In the SNR while the height was increasing the SNR values were increasing as well. Therefore, the signal could be decoded well.

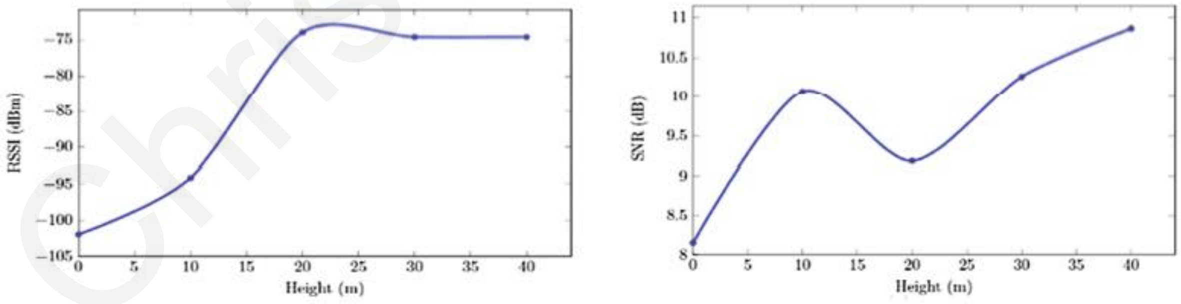


Figure 2.1.5.2.4 Results from GW elaboration

From the experiments above it is clear that the aligned antennas can increase the network performance as they offer stronger signal than the misaligned antennas. In the line of sight-environment without any obstructions a great performance of the technology can be achieved thus confirming its great characteristics. Using the aligned antennas in this environment zero packet loss was observed, thus the technology is possible to achieve a long transmission range in an environment without any obstructions. In dense environment and in urban area packet losses and lower performance were observed due to the signal attenuation especially in the urban area.

Therefore, from the last experiment which conclude that the height can increase the networks performance when it is close to reach the free line of sight the performance in dense areas such as in forest or in urban areas can be increased [18]. Further, another way to increase the performance is by adding more gateways. More precisely, by adding more gateways packets can be reached from multiple GWs and thus avoiding any packet loss. Even if one gateway could not catch the signal another gateway may caught it and thus offer a great performance. In Lora technology there are no any retransmissions so packets may be lost forever subsequently by adding more GW can reduce this undesirable situation. To continue with, another way to increase the performance is to try to regulate if possible the frequency and spreading factor in order to avoid any interference.

2.2 Narrow Band Internet of Things-NB-IOT

Despite Lora, Narrow Band Internet of things- NB-IOT is another solution for the IoT interconnectivity due to its promising characteristics. NB-IOT was released by the 3GPP in 2016 and it can be used in many IOT applications. The protocol uses a license frequency band in its transmission and it is built from the existing LTE functions. Although, many features from the LTE that lead to higher complexity have been removed and replaced by simpler functions in order to keep the protocol simple, with power efficient capabilities and with low device cost. Therefore, the primary purpose for this reduction was for the NB-IOT technology to meet the IOT demands and be used easily into IOT applications. The identification of the end device before any transmission, the licensed spectrum, the benefit from the LTE functionalities and the continuously synchronization with the network are the major factors that can guarantee integrity, security, confidentiality, low latency and quality of service.

Further, the technology can be quickly and easily be deployed as there is no need to create a new network since it is supported by current cellular networks. More precisely it can be deployed in cellular networks that support either GSM or LTE. It uses in-band operation or guard band when deploying in LTE and stand-alone when deploying in GSM. A great characteristic of this technology is that it can coexist with the other cellular technologies such as 2G/3G/4G etc. However, the in-band mode operation in LTE can cause minimum interferences if the if the two technologies use adjacent RBs without guard space between them. Nevertheless, this can be easily moderate by allocating guard RBs between the two technologies.

As every other LPWAN technology, NB-IOT can provide continuously connectivity, long transmission range, low power consumption, long battery life, low cost and low latency. Moreover it can provide mobility functionality to the end devices, hence allowing a wider range of possible applications.

2.2.1 NB-IOT main characteristics

Deployment	In Band LTE, LTE Guard Band, GSM standalone
Downlink and uplink rate	250kbps and (250kbps multi-tone, 20kbps single-tone)
Downlink Modulation	OFDMA
Uplink Modulation	SC-FDMA
Latency	1.6-10s
Number of antennas	1
Duplex mode	Half duplex and FDD
Device Receive Bandwidth	180kHZ
Receive chains	(SISO)
Device Transmit Power	20/23dBm in Release13/14dBm in Release 14
Power Saving mode	PSM, eDRX
Voice	X
Mobility	Cell reselection only
Scalable	√
Devices per cell	~ 50 000

Table 1 NB-IoT main characteristics

NB-IoT is based on the LTE protocol where some LTE functionalities were reduced and optimized especially for the IOT connectivity. Hence, the protocol remained with simple functionalities and thus it has low device cost. NB-IoT can send small and infrequent data[12], thus saving great amount of energy.

One of its great characteristics is that it can provide long battery life that is estimate to last up to 10 years. This is due to:

i. the extremely low transmit power that is uses which is 20-23dBm in Release 13 and only 14dBm in release 14.
ii. the low frequency and data rates which allow the technology to send the data with minimum power
iii. the use of both PSM and eDRX power saving modes.

More precisely, PSM turns-off the device in order to avoid the unneeded waiting between the transmission and reception time with the goal to minimize the power consumption. Every time the devices are turned back on they don't reattach themselves into the network because this would require more battery consumption. eDRX mode can be combined with PSM in order to achieve better power efficient. This mode extends the idle mode, thus devices remain longer in idle mode and subsequently they achieve greater power efficient. Before switching to deep sleep mode they wake up periodically to check for possible incoming data.

The protocol can reach up to 164dB Maximum coupling loss (MCL) which is 20dB greater than the GPRS which can attain 144dB[12]. It has great penetration and the signals can travel deep indoors and far outdoors thus provide continuously connectivity even if the devices are located kilometers apart, or deep in basements. This is achieved through:

- the use of extremely low frequencies and bandwidth which is only 180Khz. Therefore a bigger waveform is produced and has the opportunity to travel through obstacles with minimum attenuation.
- the use of low modulation scheme, thus the receiver can easily decode the packets
- ability to retransmit the packets. Hence, if the packet is corrupted for any reason it can be retransmitted from the transmitter. Although, retransmission help in the coverage it can also cause more power consumption and increase latency as the packets are retransmitted.

Specifically, it uses QPSK and OFDM (orthogonal frequency division multiplexing) for downlink with 15kHz subcarrier spacing [21]. For the uplink is uses BPSK or QPSK and the SC-FDMA(single-carrier frequency-division multiple access) and it's able to use single subcarrier (12 subcarriers with 15 kHz spacing or 48 subcarriers with 3.75khz spacing) or multiple subcarriers with 15khz subcarrier spacing[21]. When using the single tone the data can be send in serial whereas when using the multi-tone data are sending in parallel. The choice between the two possible subcarriers is made according to the channel quality at terminal [21]. By using the 3.75khz spacing it can be benefit from the higher coverage because there is longer time between subsequent symbols thus reducing even more the ISI phenomenon.

Moreover, NB-IoT sends small amount of data and infrequently, so it's hard for the technology to continuously check for the channel quality. Therefore, the protocol follows a different way by using three coverage classes. The first class is for normal coverage, second class for robust coverage and third class for extreme coverage[21]. The necessary parameters such as retransmissions are selected according to the class.

In addition, one of its major characteristics is that it uses both the licensed spectrum in its operation and the LTE functionalities with some reductions and improvements, including functionalities for ensuring the security and privacy. Before using the NB-IoT the ED must first be identified by the network and then it gets the necessary permission in order to proceed in the transmission using the technology. Hence, security, Qos, less interferences, confidentiality and integrity are guaranteed using the NB-IoT technology.

Another great characteristic of the technology is that it can coexists with other cellular networks such as 2G,3G etc and can be easily deployed in current cellular networks specifically in both GSM and LTE. It has three operation modes: standalone when deploying in GSM and Guard band or in-band when deploying in LTE. It utilizes 180KHz bandwidth for both downlink and uplink and it corresponds to one resource block for each LTE and GSM carrier [12].

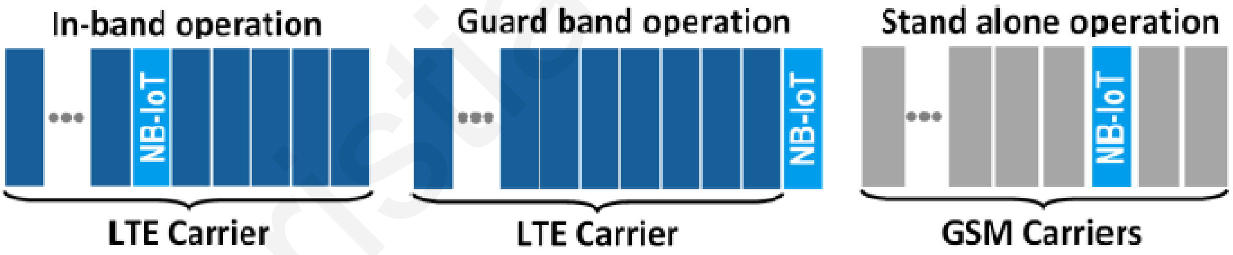


Figure 2.2.1.1.1NB-IoT operation modes [12]

Stand-alone operation: independent resource blocks are given to the NB-IOT in order to operate.

Guard Band operation: There are guard resource blocks which are the unused part from the LTE technology in order to avoid any interference. These guard resource blocks are given to the NB-IoT technology.

In-band operation: resource blocks with the appropriate frequency are given to the NB-IoT technology from the LTE carriers. More precisely, LTE RBs are replaced by NB-IoT.

To continue with, NB-IoT as mentioned can send the data using multi-tone or single tone, achieving 250kbps and 20kbps data rate respectively. It uses half duplex mode which means that it cannot upload and download at the same time but instead it can only perform one action at a time. Further, it uses frequency division duplexing (FDD) where the receiver and the transmitter operate using different frequencies.

Another great characteristic of the technology is that it supports the mobility functionality which allows the end devices to change location and still send/receive data. End devices using the NB-IoT are connected to a single GW and each time that they want to move they must change to RCC_IDLE mode and reselect another GW. Hence, changing to RCC_IDLE can save great amounts of energy. There are two possible states for an end device using the NB-IoT technology. RCC_IDLE and RCC_CONNECTED as shows in the picture [Figure 2.2.2.2]. RCC_IDLE estimates that ED is in a sleeping mode thus not consuming any unnecessary energy and RCC_CONNECTED estimates that the connection has been establish and it can transmit data.

To continue with, when the current GW releases the connection it sends to the ED some important information to store them. This info will be used later by the new GW in order to resume the connection faster. The new GW has two choices: accept the connection with the ED, or reject it. If it rejects the resume connection, the ED must repeat the connection setup. The mobility latency is estimated to be 1.6-10 seconds.

Moreover, the NB-IoT can be characterized as scalable since current cellular networks can be upgraded and support the NB-IoT technology. The technology was design to support massive connections per cell. More precisely, according to a research that was performed, and assuming that services were evenly distributed in one day NB-IoT could serve 52547 connections per cell[13][14].

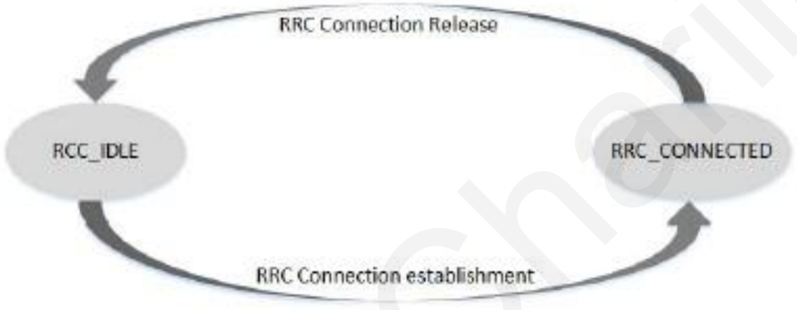


Figure 2.2.1.2 States of NB-IoNB-IoT UE

2.2.2 NB-IoT architecture

NB-IoT as mentioned above can be deployed in current cellular networks and the protocol is built from existing LTE functionalities with some improvements in order to make them simple and appropriate for the IoT. Therefore, NB-IoT uses the same network architecture as the LTE but with some optimizations to meet the IoT requirements[7].

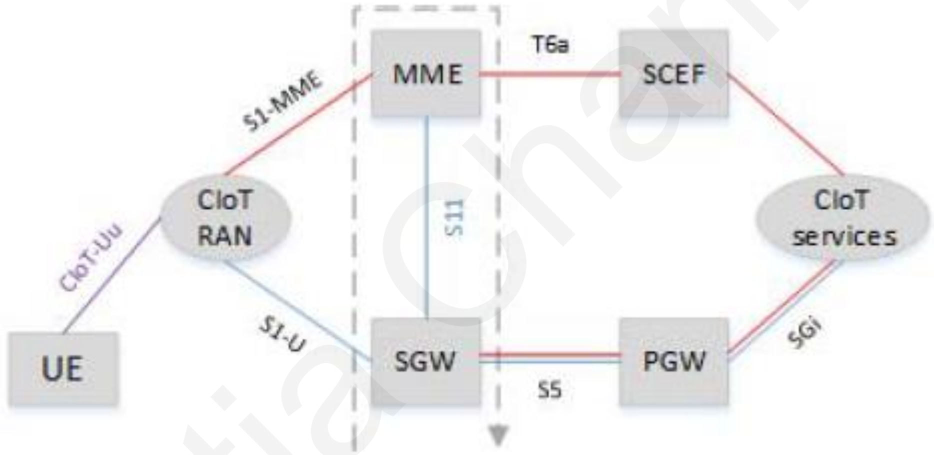


Figure 2.2.2.1 NB-IoT architecture

The protocol is based on the Evolved packet system as the LTE[7] where an ALL-IP approach is adopted. Data and voice are converged and not switched and processed separately. For the NB-IoT a new node has been added called SCEF (Service Capability Exposure Function) which is responsible to deliver the Non-IP data to the application server. In addition it’s responsible for providing an interface for the network services such as authentication, discovery, network access etc. [7]. To continue with, two more optimization were made in the control and in the user plane. In the picture [Figure 2.2.2.2] the red lines represent the control plane whereas the blue lines represent the user plane. The difference between the two lines is that the control plane is responsible for handling the user connection, whereas the user plane is responsible only for the transmitting data.

The CIoT Ran represents the GWs and is connected to the SGW and MME with S1 interface as shows in the picture [Figure 2.2.2.3]. The SGW manages the user data between the GWs and the PGW. To continue with, the PWS represents the gateway router to the internet and it provides internet connection to the UE. The data are forwarded from the UE with the goal to reach the application server in order to perform the appropriate actions. Moreover the MME(Mobility Management Entity)is one of the most important parts of the network as it provides user authentication, locate a UE, establish bearers and help in the handover. Although the handover has been removed in order to keep the protocol simple and with low cost the handover can still be performed with max mobility latency of 10sec.

Further, the IP and non- IP data on the user plane are forwarded with the same way, by reaching the SGW at first then PGW and finally the application server. Contrariwise, the non-IP data on the control plane are forwarded by the new node SCEF to the application server whereas the IP data are forwarded in the same way as in the user plane.

2.2.3 NB-IoT connection set up

In order for an ED to use the NB-IoT technology there are two important factors. Firstly, NB-IoT end devices must have an installed sim card and secondly the NB-IoT technology must be supported from the BSs near the ED. The enodeB/GW has a major role as it is responsible for scheduling and informing the ED about the time and frequency that it can transmit or expect downlink info from the network[15].

To start with, each ED is associates to a single GW and it must establish again the connection every time the connection gets lost. At first an ED searches for the appropriate frequency in order to connect to the appropriate BS[7] and get the permission in order to transmit its data using the NB-IoT technology. After a successful search the ED receives the NBCelID which is broadcast from the GW using the NPSS(Narrowband Primary synchronization signal) and NSSS(Narrowband secondary synchronization signal) channels. NPSS and NSSS channels are broadcast synchronization channels that help to set up the connection between the ED and the GW. More precisely, NPSS help the devices to be synchronized in both time and frequency into NB-IoT cell whereas NSSS is responsible to forward the NBCellID. NPSS is transmitted every 10ms whereas NSSS is transmitted every 20ms[7].

To continue with, the Narrow Band Physical Broadcast channel is responsible to transmit the Narrow Band Master Information Block (MIB-NB) to the ED. The ED can decode this Master Block by using the NBCellID that received earlier from the NSSS channel. The NB-MIB is transmitted eight times and its content remains stable for 640ms. The QPSK modulation is used to transmit this block to ensure that the data will successfully be decoded from the receiver even if the ED is located far from the GW. The NB-MIB block contains necessary information for the ED in order to successfully operate in NB-IoT network, including the System Information Block(SIB). Further, the ED decodes the SIB1-NB and SIB2-NB in order to complete the connection set up. Both SIB1 and SIB2 include essential information that can help the ED to proceed. Specifically, the SIB2 include information that is required for the uplink synchronization such as the RACH configuration [7]. In order to initiate the uplink synchronization the ED sends to the GW a RACH preamble. If the GW receives the preamble it responds with a msg2 as shows in picture[Figure 2.2.3.1]. If the ED doesn’t receive the msg2 then it retransmits the preamble to the gateway as long as it reaches the maximum retransmissions. NB-IoT can reach up to 128 repetitions in uplink and up to 2048 repetitions in downlink[14]. If it received the msg2 then it responds with a msg3 in order to start the contention resolution process. The GW responds back to the ED completing the connection set up procedure.

In the random access procedure multiple devices are using the same preamble in order to establish the connection. Thus, they receive the same response from the GW since they have the same temporal identifier. Therefore, the contention resolution process which is established in msg3 is to ensure that each ED has a unique and different identifier. Finally, the ED sends an RCCConnection Request which estimates that it wants to connect to the current network[7].

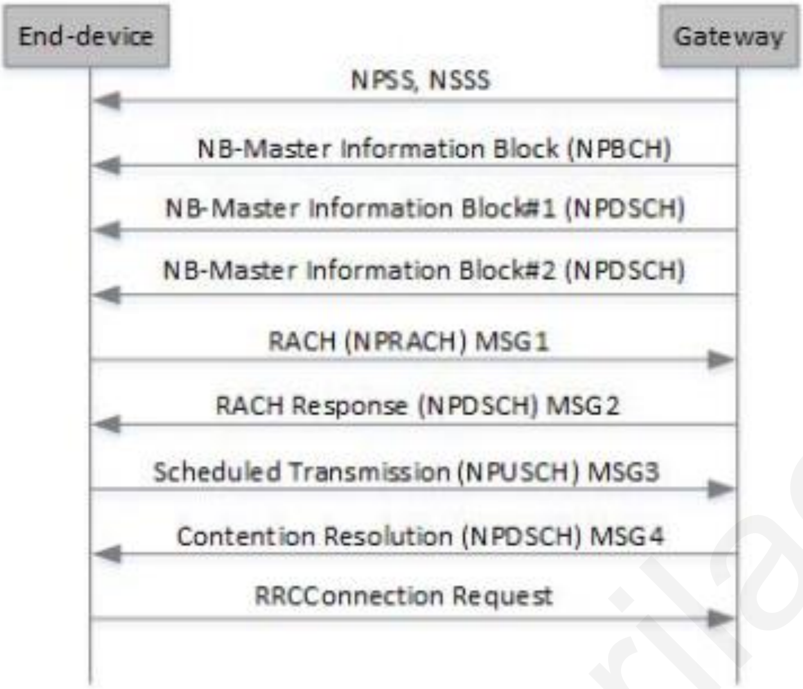

End-device
Gateway
NPSS, NSSS
NB-Master Information Block (NPBCH)
NB-Master Information Block#1 (NPDSCH)
NB-Master Information Block#2 (NPDSCH)
RACH (NPRACH) MSG1
RACH Response (NPDSCH) MSG2
Scheduled Transmission (NPUSCH) MSG3
Contention Resolution (NPDSCH) MSG4
RRCConnection Request

Figure 2.2.3.2 NB-IoT Connection set up

2.2.4 NB-IoT and LTE coexistence

Nb-IoT can be deployed in LTE in guard-band and in in-band mode. When deploying in guard-band the guard unused resource blocks are given to the NB-IoT technology in order to operate. On the other hand, when deploying in in-band mode RBs are given to the NB-IoT technology from the LTE carriers. Through some experiments that were established it was observed that in-band mode interferences can be occurred between the LTE and NB-IoT if there is no guard space between the RBs. However, this can be greatly moderated by leaving the adjacent RBs empty. Contrariwise, when using the guard- band mode little interference can be experienced from the two technologies which can be negligible even if there is no space between the RBs.

To continue with, NB-IoT uses the LTE functionalities with some improvements. Thus, it uses the same frequency allocation and spacing as in LTE[17]. Hence, NB-IoT reserved RBs can be characterized as additional RB and therefore in downlink there is insignificant interference between the two technologies. More precisely, NB-IoT channels are orthogonal to LTE channels causing insignificant interference[17].

2.2.4.1 NB-IoT and LTE coexistence while operate in in-band mode

In order to observe any coexistence issues between the two technologies experiments were performed in [16]. The experiments showed that NB-IoT with 3.75khz subcarrier bandwidth and LTE with 15khz subcarrier bandwidth in uplink can experience interferences when both technologies allocate adjacent RBs.

More precisely, the experiment included a 20MHz bandwidth for the LTE technology and 100 RBs ranging from 0-99. The NB-IoT technology allocated the RB located at 45[16].

There were not guard spaces between the RBs thus the LTE technology reserved RBs 0-44 and 46-99. The goal for this experiment was to observe the behaviour of each technology having adjacent RBs. The experiment showed that when the signal from the NB-IoT was transmitted and the LTE system received it had an interference of about -10 - ~-15dB. On the other hand, when the signal was transmitted from the LTE and received from the NB-IoT the Nb-IoT technology had an interference of about -20 ~ -10 dB. Thus, they resulted that the two technologies can experience interferences when they are using adjacent RBs.

Moreover, they performed the same experiment but this time they used guard RBs located at 44 and 46 and noted the results. They found that with guard RB between the two technologies the interferences can be greatly moderate. Therefore, in order to avoid interferences between the two technologies, if it’s possible the operators must leave the adjacent RBs empty.

2.2.4.2 NB-IoT and LTE coexistence while operate in guard-band mode

In order to observe any coexistence issues using the guard-band mode, experiments were established in [Analysis of NB-IoT Deployment in LTE Guard-Band]. They wanted to observe the influence from NB-IoT to the LTE and from the LTE to the NB-IoT. The final result was that the interference from either of the two technologies is very small.

In the experiment there was no separtion between the adjacent RBs and they calculated the power at each time in order to observe the influence for each technology. They resulted that both technologies have very small affect on the other. However, NB-IoT to the LTE seems to have smaller affect rather than LTE to the NB-IoT. This is because the LTE have greater bandwidth than NB-IoT and therefore is less affected[17].

2.2.5 Performance analysis of NB-IoT

In order to observe its performance many experiments were established. Some of them focused on the latency and on the throughput that the technology can attain when the communication link varies or when the packet sizes vary. To continue with, other investigations were establish in order to observe the difference between the three operation modes in-band, guard-band and stand-alone and noted the results from all of them.

2.2.5.1 Experiment in real environment

An experiment was performed in Belgium by [14] in order to observe the NB-IoT performance in a real environment. They focused on two more parameters: the latency and the throughput when the communication link and the packet sizes vary. As expected the technology had a great performance and didn't lose any packets even in a poor communication link. It was also confirmed that the downlink has less latency than the uplink due to the fact that in downlink OFDMA is used in contrast of SC-FDMA for uplink. OFDMA is much faster than the SC-FDMA and therefore lower latency can be experienced. Further, it was also validated that the NB-IoT can achieve 164dB maximum cabling loss(MCL).

They observed the uplink and downlink latency and throughput for packet sizes 8,64 and 512 bytes in three zones where the zone1 indicated a link with good conditions, zone 2 indicated a link with average conditions and zone 3 a poor communication link. In order to note the latency for uplink and downlink they measured the time difference between the two hosts. More precisely, they measured the time difference between packets' departure and arrival [14]. They measured the Reference signal receive power(RSRP) which is a type of RSSI measurement.

Results:

They measure the RSSI and SNR with the RSRP measurement as shows in the figure [Figure 2.2.5.1.1]. As shows in the graph as the RSRP increases the link conditions are improved and therefore there is an increase in both SNR and RSSI. Contrariwise, as the RSRP decreases there is a decrease in both SNR and RSSI which indicates less good conditions. The device was transmitted with power 23dB and the maximum RSRP was -141dB where the device lost connection in that value[14]. They confirmed that (23-(-141))=164dB[14] which is the theory achievable maximum cabling loss that the technology can attain.

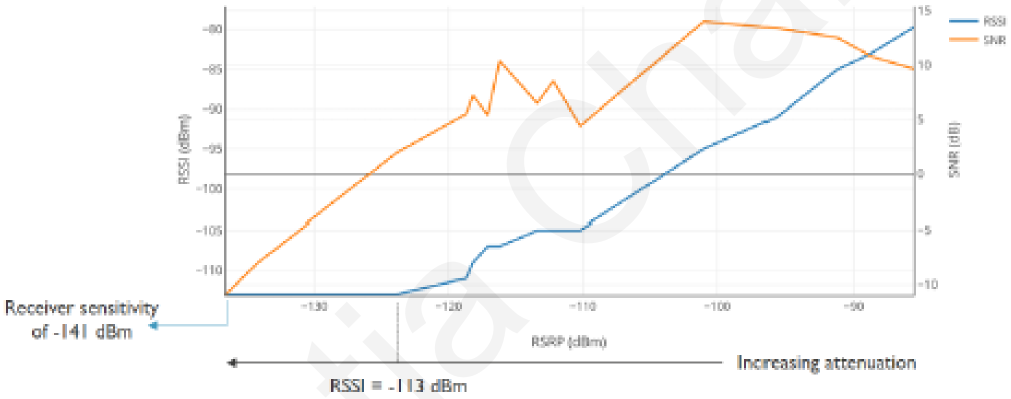


Figure2.2.5.1.1 RSSI and SNR graph

In figures[Figure 2.2.5.1.1 Downlink latency] and [Figure2.2.5.1.2 Uplink latency] there are the results from the downlink and uplink latency respectively. As it can be seen the latency in downlink is lower than the uplink due to the use of OFDMA which is faster than the SC-FDMA. In both uplink and downlink the packet with the maximum bytes has the maximum latency because of the bigger packet size. It is also observed that even for poor signal quality the latency is small of about 16 seconds in uplink and around 8 in downlink. Also in [14] it was mentioned that no packets loss were experienced even in poor conditions, thus confirming its strong reliability that can offer.

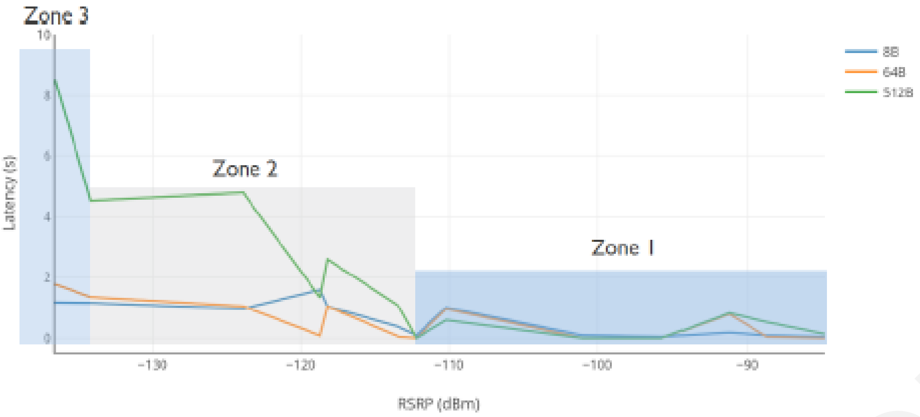


Figure 2.2.5.1.1 Downlink latency

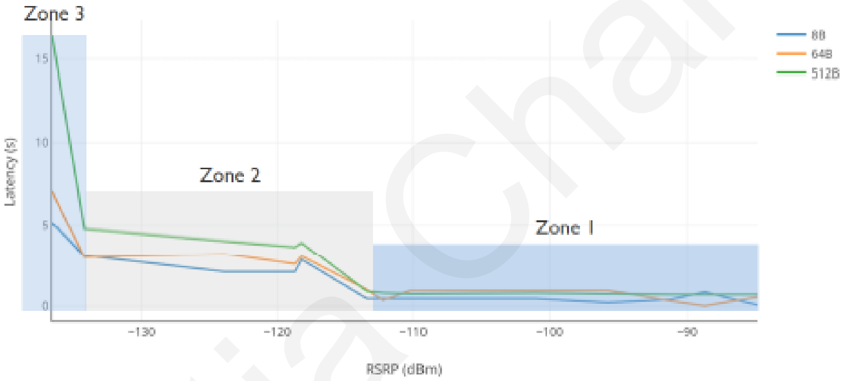


Figure2.2.5.1.2 Uplink latency

In figures [Figure2.2.5.1.3] and [Figure2.2.5.1.4] there are the measurements from throughput in uplink and downlink for packet sizes 8,64 and 512 bytes. The graphs show that the maximum achievable throughput for uplink was 11kbps in zone 1 which is the good conditions for 512bytes packet and 17kbps in downlink again in zone 1 and for 512bytes packet. The throughput in the downlink is higher because of the lower latencies that the technology can attain[14]. Further, in zone 1 which has the greatest conditions it is observed that it has the higher throughput in contrast to other zones. As mentioned in the paper all of the packets arrived at the destination confirming again the high reliability that the technology can provide.

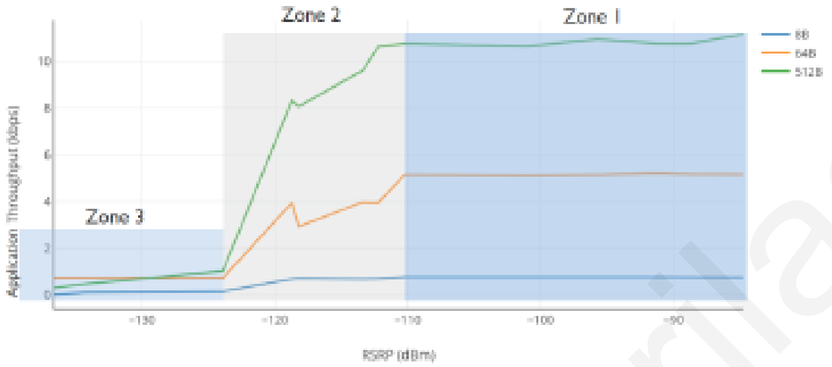


Figure 2.2.5.1.3 Throughput in downlink

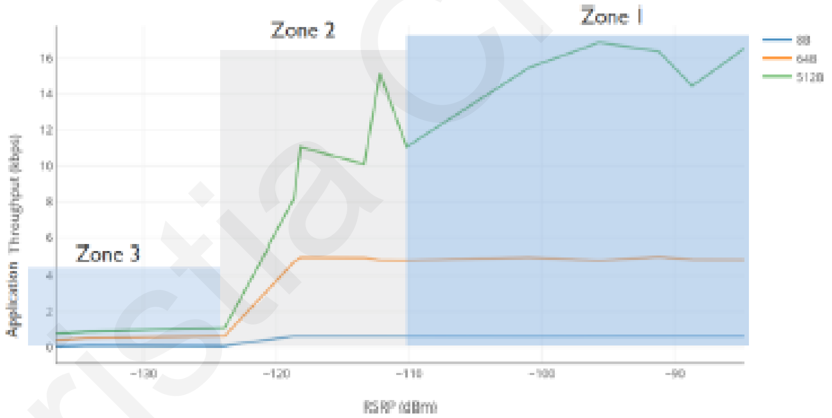


Figure 2.2.5.1.4 Throughput in uplink

2.2.5.2 Guard-band,In-band and stand-alone analysis

In [17] a performance analysis of the NB-IoT technology was established, considering its three operation modes stand-alone, guard-band and in band-mode in order to observe its performance. They used the three modes and they value the throughput and MAPL(Maximum allowable path Loss) and noted the results. The MAPL for the NB-IoT technology is 164dB. For the downlink they measure the sustained downlink throughput and they found out that for good conditions the three operation modes have the same results as they offer the same throughput. This is showed in the figure[] where the MAPL is less than 140dB the three operation modes have the same throughput. For values greater than 140dB and where there are lower good conditions the stand-alone mode has the best performance as it offers the highest throughput. Considering the guard-band and in-band mode the guard band offers little higher throughput than the in-band.

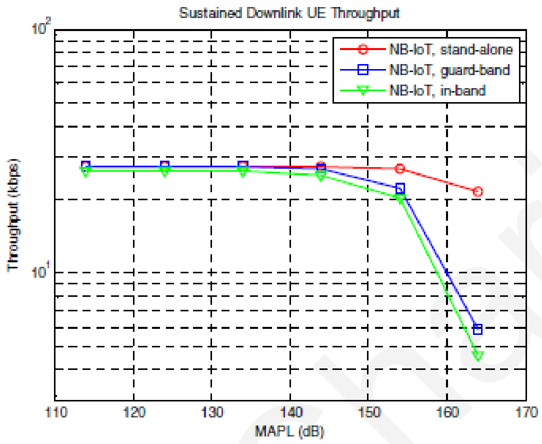


Figure 2.2.5.2.1 Downlink Throughput for NB-IoT using the three operation modes[17]

To continue with, the uplink throughput was measured as well. In the uplink since the experiment included a single UE no interference could occur and since the transmitting power is the same eg.23dB in all modes there was no difference in the throughput [17].

2.3 Other LPWAN technologies

Despite Lora and NB-IoT there are other technologies that belong to the LPWAN category. SigFox and Dash7 are LPWAN technologies that use the unlicensed spectrum for their transmission whereas LTE-M and EC-GSM-IOT are LPWAN technologies that use the licensed spectrum in their operation. As every other LPWAN technology all of them can achieve low battery consumption, low device cost and a long transmission range. Although, in contrast to Lora and NB-IoT they have some limitations such as limit messages per day, higher power consumption than the others, restricted to specific areas and limit expansion. Each one of them can be used in specific kinds of applications.

For instance, SigFox can only send 140 messages with 12 bytes payload and only 4 downlink messages with 8 bytes payload. Thus, it's appropriate for applications that only send messages(less than 140 per day) without requiring any downlink info from the network in order to proceed. Further, dash7 has the lowest range than the other LPWAN technologies reaching only 1-2km so is preferable to be used in applications that require this transmission range.

Contrariwise, EC-GSM-IOT and LTE-M are restricted to areas that contain GSM and LTE networks respectively. EC-GSM-IOT offers low latency and higher power consumption than the other LPWAN technologies whereas LTE-M can attain the highest data rate and lowest latency in contrast to the other technologies. Both technologies have a voice support and subsequently they are able to support real time applications.

2.3.1 SigFox

SigFox is another LPWAN technology that uses the unlicensed 2.4 GHz band and offers an end to end connectivity. It can provide a long communication link, low power consumption and battery saving due to its suitable characteristics.

SigFox main characteristics:

	SigFox
Modulation	UNB BPSK(UL),GFSK(DL)
Band	Sub-GHz ISM: EU(868MHz),US(902MHz)
Data rate	100bps(UL),600bps(DL)
Range	10km Urban,50km rural
Number of channels	360
Mac	Unslotted aloha
Topology	Star
Adaptive data rate	X
Payload length	12byte(UL),8byte(DL)
Handover	End devices do not join a single base station
Authentication/encryption	Not supported

Table 1 SigFox main characteristics

In contrast to other LPWAN technologies, SigFox can send limited messages per day with maximum throughput 100bps. Devices that use this technology can send 140 uplink messages with 12 bytes payload and only 4 downlink messages with 8 byte payload. Downlink messages are only followed after an uplink message. Therefore, acknowledge messages are not supported from the technology and as an alternative to ensure reliability it transmits each message many times (by default three times) using different random channels. It has the option to choose between 360 channels as it uses 868.180Mhz and 868.220Mhz band which is divided into 400 orthogonal 100Hz channels. The 40 channels are reserved but not used, resultantly in 360 available channels for the technology. The technology doesn’t support encryption and authentication but it can achieve low power consumption and a long communication link of 10km in urban and 50 km rural due to the ultra-narrow bandwidth (100Hz) that it uses. Subsequently, SigFox can be used in non-sensitive applications and when the number of exchanging messages is limited to 140 for uplink and 4 for downlink.

Moreover, it uses Binary phase shift key (BFSK) for the uplink modulation and Gaussian frequency shift key(GFSK) for downlink communication achieving 100bps and 600bps respectively. Low modulation schemes can achieve less power consumption since the decoder can easily determine the correct phases and successfully decode the signal. The lower the modulation technique the easier is for the decoder to decode correctly the signals. Both ultra-narrow bandwidth and BPSK modulation technique have the advantage of low noise levels since a bigger waveform is produced which has minor attenuation as it passes through obstacles. Thus, the BFSK combined with UNB(Ultra-narrow bandwidth) can help the decoder to successfully decode the signals.

Further it uses the unslotted aloha which means that it doesn't consume any unnecessary power for the synchronization. Devices do not wait for scheduled timeslots to transmit their data but rather they transmit them every time they have data to transmit. Thus, longer distances, lower power consumption and lower cost devices can be achieved as the antenna is inexpensive.

2.3.2 Dash7

Dash7 is another LPWAN technology that was specified by the DASH7 Aliance and it operates in the unlicensed spectrum. There were two publications of the protocol, in 2013 they published the 0.2 version and in the 2016 they published the 1.1 version[7]. As every LPWAN technology DASH7 can provide long communication link(up to 2 km), low latency and low battery consumption.

DASH7 main characteristics:

	DASH7
Operation frequencies	Unlicensed ISM band
Modulation	2-GFSK
Range	1-2Km
Data Rate	13,55,200(16,8,4 channels)
Topology	Tree,simple routing 2 hops
Device classes	Endpoint,Subcontroller,Gateway

Table 2 Dash7 aliance protocol main characteristics[7]

Dash7 is an open source Wireless Sensor and Actuator protocol that is based on the ISO/IEC 18000-7 standard which is the air interface for RFID operating in the 433 MHz band[7]. It can achieve low data rates such as 13kbps when using the channel 16, 55kbps when using the channel 8 and 200kbps when using the 4 channel. It supports three device classes in which each device have different functionalities. An endpoint can only send information to the gateway in an asynchronous manner. It consumes minimum power consumption as it falls asleep most of time and it weak up periodically to listen to possible incoming packets[7]. A sub-controller is a device that is used to relay messages from an end device to the gateway and vice versa. A GW is always on receiving mode unless it transmits and its main operation is to receive packets and forward them to the network server using ALL-IP network. The network server checks the packets and finds the nearest GW in order to be used later to send the downlink info to the end devices. Finally the network server forwards the packets to the customer cloud in order to perform the appropriate actions.

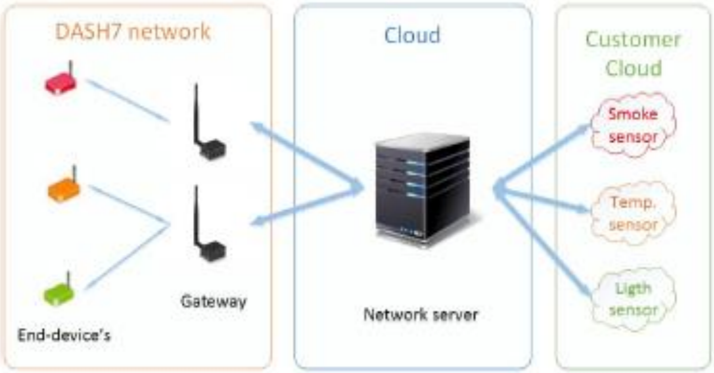


Figure 2.3.2.1 Dash architecture

2.3.3 EC-GSM-IOT

Extender coverage GSM was released by 3GPP in 2016 and it belongs to the LPWAN technologies. EC-GSM-IOT was created in order to achieve greater communication link than GSM and in order to achieve better penetration[9].In contrast to Lora,DASH7 and SigFox it operates in a licensed spectrum which mean that it can achieve higher reliability since the spectrum is less congested than 2.4GHz band. As every other LPWAN technology it can achieve long communication link, low power consumption and low latency.

EC-GSM-IOT main characteristics

	EC-GSM-IOT
Deployment	In GSM
Operation	Licensed spectrum
Downlink and uplink rate	74kbps and 240kbps
Latency	700ms-2s
Number of antennas	1-2
Duplex mode	half duplex
Device Receive Bandwidth	200kHz
Receive chains	1-2
Device Transmit Power	23/33dBm
Link budget	154-164dB
Number of Devices	50000 per cell
Modulation	GMSK,8PSK
Power Saving mode	PSM, eDRX
Voice	Supported

Table 4 EC-GSM-IOT main characteristics

EC-GSM-IOT can be deployed in cellular networks that support the GSM network. Thus, this technology is appropriate for regions that have strong GSM coverage. Due to the low frequencies that it uses it can coexists with other technologies such as 2G,3G,4G without any interferences. Also as other mobile networks it can provide security, privacy and confidentiality. Further, it can be used in a wide number of applications including applications that require voice transmissions since this functionality is supported from the technology. Further, it can be used in applications that require low latency since it can achieve only 700ms to 2s latency.

EC-GSM was created in order to achieve longer communication link reaching a link budget ranging from 154-164dB. The technology can accomplish extremely low battery consumption and thus longer battery life due to a number of reasons. At first, it transmits its packets with low power consumption of 23/33dBm. To continue with it uses two power saving modes, PSM and eDRX. As mentioned, PSM turns-off the device in order to avoid the unneeded waiting between the transmission and reception time with the goal to optimize the battery life. eDRX mode can be used with PSM in order to maximize the power efficient of the device battery. This mode extends the idle mode which means that they fall asleep longer. Thus, more energy can be saved and therefore the battery life is extended.

Moreover, it uses GMSK(Gaussian Minimum Phase Shift Key) for uplink and 8PSK(Phase Shift key) for downlink achieving 74kbps and 240kbps respectively. For the communication it uses half duplex mode which means that devices can either upload or download data each time. Further, every base station can support up to 50000 devices without any interference due to the licensed spectrum that is used.

2.3.4 LTE-M

LTE-M is another LPWAN technology that it has been released by the 3GPP. As NB-IoT and EC-GSM-IOT it transmits in a licensed spectrum which means that confidentiality and reliability are ensured. The difference between LTE-M , NB-IoT and EC-GSM-IoT is that LTE-M can provide the highest data rate and thus the lowest latency. However, as the other technologies it can provide a reliable long communication link and a long battery life.

LTE-M main characteristics:

	LTE-M
Deployment	In LTE
Operation	Licensed spectrum
Downlink and uplink rate	1 Mbps
Latency	10-15ms
Number of antennas	1
Duplex mode	Both full and half duplex
Device Receive Bandwidth	1.4MHz
Receive chains	(SISO)
Device Transmit Power	20/23dB
Power Saving mode	PSM, eDRX
Voice	Supported

Table 5 LTE-M main characteristics

LTE-M it can be developed in current cellular networks that support the LTE. Thus, the technology is appropriate only in regions that support the LTE functionality. It can be benefit from the mobile networks' security and confidentiality and as the NB-IoT and EC-GSM-IO=oT it can coexists with other wireless technologies such as 2G,3G,4G etc.

It uses greater bandwidth than the other licensed technologies and thus it can achieve higher data rate of about 1Mbps.It uses both full duplex and half duplex mode which means that either it can upload and download data at the same time, either it can upload or download each time. Moreover it can provide extremely low latency of only 10-15ms and supports the voice transmission. Therefore, the technology can be used for real time applications and for applications that are time critical due to its extremely low latency and voice capabilities.

To continue with, as all the other LPWAN technologies LTE-M can provide a long battery life. It uses the PSM and eDRX as the NB-IoT and EC-GSM-IoT for better power saving. Also it uses only 20/23dM to transmit its data. Thus, it can ensure a battery life of up to 10 years.

Chapter 3

Comparison of technical specifications of LoRa and NB-IoTs technologies

NB-IoT and Lora are the most popular technologies for the IoT connectivity since they meet all of its high demands. Both technologies can achieve low latency, security, low power consumption, high battery efficient and low cost. However, they have some manufacture dissimilarities as well since each one was created in order to serve specific kinds of applications.

To continue with, different IOT applications have different demands from the technology. For instance, smart metering applications focuses especially in long coverage and minimum power consumption whereas e-health applications focuses in security, privacy, high reliability, low power consumption and minimum latency in order to operate well in emergency situations[14]. Hence, an appropriate technology must be selected for every IOT application. Each LPWAN technology cannot serve all the IOT applications equally[12] but instead each one focuses on different aspects that are important to be mentioned.

3.1 Manufacture Similarities of NB-IoT and Lora

Both technologies seem to be extremely important for the IoT connectivity due to their attractive characteristics. Both Lora and NB-IoT can effectively connect the IoT devices into the Internet meeting all of their high demands. More precisely, both technologies:

- Can be used in multiple types of applications such as time-critical, data-critical or applications that require confidentiality and integrity since they both can ensure security, confidentiality, low latency and privacy.

- Can attain long transmission range achieving several kilometers while consuming extremely low battery consumption, thus offering the IoT devices continuously connectivity with great battery life. The long transmission range can be achieved through the low frequencies that they use in their operation. Therefore, a bigger waveform is created and experience minimum attenuation as it passes through obstacles. Further, the lower the modulation scheme the easier is for the decoder to decode the packets. The NB-IoT uses low modulation schemes and as a result the decoder can easily decode the packets. Therefore, long transmission range can be achieved from the technology. On the other hand, Lora uses the Lora modulation which is based on the spread spectrum technique. Spread spectrum techniques can achieve high immunity in noises since the signal can travel into the noise and still be decoded. Thus, Lora can achieve a long transmission range. Hence, long transmission range can be achieved from both technologies.

- Can achieve long battery life of up to 8-10 years due to the power saving functionalities that they use. NB-IoT is using both PSM and eDRX in order to achieve high power efficiently while LoRa uses the Adaptive data rate which allows sending max data with minimum power consumption, and class A which offers minimum power consumption. Therefore, they are appropriate for the IoT connectivity since there is no need to frequently change the battery of thousands of devices.

- Use encryption algorithms for integrity and confidentiality. More precisely, NB-IoT uses the LTE encryption whereas the Lora uses the AES algorithm with two level encryption. In both technologies before any transmission the devices must be verified and get the necessary permission in order to proceed. Subsequently, packets are transmitted securely over the network ensuring reliable transmissions especially in critical based transmissions.

- Can be scalable by adding more devices or more gateways in LoRa or BSs in NB-IoT. Therefore, many devices can be used in both technologies.

- Can achieve low latency which is necessary for the IoT, since latency is extremely important for the IoT connectivity. Some IoT applications are time-critical and low latency is essential. NB-IoT has continuously synchronization with the network thus allowing to achieve low latency and Lora can use the class C which offers low latency as it has continuously open intervals in order to receive downlink information.

- Can perform mobility, thus ensuring the delivery of the data even if an end device changes location. Therefore, they can be used in multiple applications even in those that require mobility.

Despite their theoretical and manufacture similarities they are different and their selection must be made according to the application's requirements. This project compares the two LPWAN technologies based on their manufacturing specifications, concerning their differences in quality of service(QoS), cost, deployment, network coverage, range, throughput, mobility latency, data rate, reliability, latency and battery life.

3.2 Manufacture Dissimilarities of Lora and NB-IoT

	LoRaWan	**Nb-IoT**
Spectrum	Unlicensed	Licensed
Topology	Star of Stars	Star of Stars
Modulation	SS chirp	OFDM/SC-FDMA
Access method	Class A: ALOHA, Class B:Slotted Aloha, Class	QPSK/ QPSK(multi-tone, BPSK single-tone)
Date Rate	290bps - 50kbps	250kbps and (250kbps multi-tone, 20kbps single-tone)
Link Budget	157 dB	154dB
Standard	LoRa Alliance	3Gpp
Battery Lifetime	8 -10 years	8-10 years
Power Efficiency	Very High	Very high
Security/Authentication	Yes (32 bits)	Yes(LTE)
Mobility Latency	Low(almost zero)	High(1.6-10s)
Device Transmit Power	14-27dBm	20/23dBm
Deployment	Need to create a network	In Band LTE, LTE Guard Band, GSM standalone
Support real time apps	Yes with Class C	No
Adaptive Data Rate	Yes	No
Scalability	Yes	Yes

Table 6 Table with the specifications of each technology

QoS(Quality of Service):

Qos is an important factor for many IoT applications. More precisely, QoS refers to the high network reliability, low packet loss and transmission delay and ensuring that the data will arrive and be decoded well from the receiver. However, Qos is a challenge in asynchronous protocols, and protocols that uses the unlicensed frequently used spectrum in order to transmit because collisions and interferences can occurred. Contrariwise, Qos is guaranteed in synchronous protocols that use the licensed spectrum in their operation since there is lower packet loss and lower transmission delay due to the lack of possible collisions and interference.

Lora is an asynchronous protocol that uses the frequently use unlicensed spectrum so interferences can occur due to this popular spectrum. According to researches and experiments that were established Lora seems to be robust against other wireless technologies when using the same or neighboring frequencies. This is due to the spreading factor which can lead to coexistence with other technologies. However, its limitation is that it can experience inter-interference when two or more Lora devices use the same parameters such as bandwidth and the same spreading factor. This is because it exhibits the capture effect where only the stronger signal survives. Thus, Lora signals must arrive with same power at the receiver in order to avoid any interference. With different parameters it can achieve multiple simultaneous communications without any interference. Further, collisions may be created because the protocol uses the ALOHA and pure ALOHA method which means that when it has data to send it send it. Thus, possible collisions can be created. In both situations packet loss can be experienced.

On the other hand, NB-IoT is a synchronous protocol that uses licensed spectrum in order to transmit the data, achieving a greater quality of service than LoRa. This higher quality is due to the licensed spectrum and because it uses multiplexing techniques that allow multiple simultaneous communications. The aim of the multiplexing techniques is to give the appropriate resources and space to each user in order to achieve these multiple simultaneous communications without causing any interference between the simultaneous users. However due to experiments that were performed possible interferences can be occurred with the LTE by using the in-band mode and allocate adjacent RBs. However, this can be reduced and be negligible by leaving guard spaces between the RBs. Thus, NB-IoT has high QoS as it experiences less and negligible interference than Lora.

Subsequently, NB-IoT technology can attain high QoS due to the use of the licensed spectrum. As a consequence, devices that need high quality of service must use the NB-IoT where are devices that do not need Qos can be benefit from the LoRa technology.

Throughput & payload length:

NB-IoT has higher data rate and also it has the advantage of greater payload length reaching up to 1600bytes in contrast to LoRa that has lower data rate and lower payload length which is only 243 bytes. Further, Lora is based on the spread spectrum technique which means and it uses the spreading factor ranging from 7 to 12. The higher the spreading factor then the lower is the data rate and thus throughput that it can achieves.

Therefore, NB-IoT can attain higher throughput due to the higher data rates and greater payload length than Lora. Hence, applications that need higher throughput NB-IoT is more suitable.

Data rate:

Both technologies belong to LPWAN technologies thus they both use low data rate for their transmissions. However, NB-IoT seems to attain greater data rate than Lora reaching up to

250kbps while LoRa can reach up to 50kbps. Subsequently, applications that require higher data rate than 50kbps can be benefit from the NB-IoT technology.

Deployment and cost:

In order to deploy a Lora network a constructor must buy and set up the necessary equipment which involves gateways and end devices that support the technology. However, the cost for this equipment is low. Specifically, a gateway is estimated to cost 70-€1000 whereas each device is estimated to cause bellow €100. In contrast to other technologies Lora is the only one that can built private networks.

Contrariwise, NB-IoT can be deployed in current cellular networks thus there is no need to build a new network. In order to use the technology a constructor must only buy end devices that support the technology and pay monthly fees to the operators. A major disadvantage of the technology is that is restricted to areas that contain upgraded cellular networks thus it has limited usage. Further, a constructor always relies on operators to fix a problem which can be characterized as both an advantage and a disadvantage. An advantage because there is no worry about the network issues and a disadvantage because the application will immediately be affected after a network issue and a constructor will have to wait for the operators to fix the problem.

To summarize, Lora technology has an advantage into deployment and cost. It has lower deployment cost than the NB-IoT technology, it can built private networks and it doesn’t have any restrictions regarding the areas.

Network coverage & range:

LoRa can achieve a long transmission range with the capability to cover an entire city with only few GWs according to city’s dimensions. This long transmission range is due to the spread spectrum technique that it’s based on. The higher the spreading factor then the higher is the distance that the signal can reach. The coverage can be as long as the constructor wants due to the ability to add more gateways in order to support more areas and reduce the GW’s overhead.

On the other hand NB-IoT has lower range than Lora and it can provide services to end devices that are out of reach of regular cellular networks[12] (2G,3G,4G etc.). However, the technology is restricted to areas that are equipped with upgraded cellular networks that support the technology.

Thus, it’s preferable to use the Lora technology if an application is estimated to expand into areas that currently don’t support the NB-IoT technology.

Latency:

Both technologies NB-IoT and Lora can attain low latency due the synchronization and due to the use of class C respectively. Although, Lora is the only technology that can be used in real time applications since NB-IoT doesn’t support this functionality. However, latency depends on multiple factors such as the link quality, possible occurrence of collisions and interferences, distance from the receiver and packet size. The lower the link quality, the higher the collisions& interference, the higher the distance and packet size can increase the latency in both technologies.

In Lora technology an ED can choose between three classes, A , B and C. In those classes the battery is contradicted with the latency. More precisely, if an ED uses the class A then it has low power consumption but high latency, if it uses class B then it has higher power consumption and lower latency and if it uses class C then it has highest power consumption and the lowest latency. To be exact, if an end device transmits data using the class A it has only two downlink intervals to receive data from the network otherwise it has to wait for the next transmission in order to receive downlink info. However, if there the ED doesn’t receive the downlink info in those scheduled time intervals and waits for the next ones then the latency is increased. To continue with, if an ED transmits data using the class B then it has extra scheduled downlink intervals resultantly in lower latency than in the class A. Further, if an ED transmits data using class C then it has continuously downlink intervals which are closed only when the ED is transmitting. Thus, class C has the lowest latency but higher power consumption due to the continuously open downlink intervals. Further, the latency depends on the spreading factor that the technology uses. The higher the spreading the higher is the latency since more transmission will be created in order to send the appropriate data and a longer communication link will be created.

On the other hand devices that use the NB-IoT have continuously synchronization with the network since the ED is continuously connected to the GW receiving data from the network. Subsequently, NB-IoT can accomplish low latency and meet this IoT demand. However, the latency also depends on the device state such as the PSM or eDRX mode and on the link quality since retransmissions may be created in order for a packet to arrive at the receiver. Also, NB-IoT support 1600bytes payload so the latency decreases in this technology.

Therefore, applications that need low latency are preferable to use the NB-IoT technology and LoRa with class C whereas applications that are latency insensitive can use LoRa with class A and B. However, for real time applications only the LoRa technology is suitable. The protocol also has the ability to switch between classes in order to save energy.

Mobility latency:

There are IoT applications that require mobility since devices may be moving while operating. However, mobility in the IoT technologies has a different meaning than in the IP networks. Mobility in IP technologies refers to the soft or hard handover while the device changes location whereas mobility in IoT refers to ensuring the delivering of the data[3] when a device change its current location. Nevertheless, mobility latency is important since latency is major factor in the IoT. Both Lora and NB-IoT can achieve mobility and they both have low mobility latency. However, Lora seems to have lower mobility latency than the NB-IoT due to its ability to broadcast the messages to all of the accessible GWs.

More precisely, in LoRa technology each ED is not connected to a single GW but it broadcast the messages to all of the reachable GWs. The EDs have a pre-configuration to send their new location in order to inform the Network Server(NS) every time they change one. The NS then updates the forward table with the new GW and the new location of the ED. Therefore the Ns will send the new info to the new GW which is nearest to the ED. If the device didn't lose connection while moving and successfully sent its new location then the mobility latency is almost zero. If the device lost the connection then it must establish again the activation procedure in order to get the necessary permission to use the technology.

In contrast to Lora, an ED in the NB-IoT is connected to a single GW and the handover has been removed in order to keep the technology simple. An NB-IoT device has 2 states: RCC_IDLE and RCC_CONNECTED state. An ED must change to RCC_IDLE in order to reselect another GW and change its location. The new gateway will either reject or accept the connection with the ED. If it rejects it then the connection must be performed again. Thus, the setup time is estimated to last 1,6 to 10 seconds. Therefore, the latency is higher than in the Lora technology.

Subsequently, applications that require mobility are preferable to use the LoRa technology because of the lower mobility latency that it can provide due to its ability to broadcast the messages to all of the accessible gateways thus reducing the mobility latency.

Battery life

Both technologies can achieve great battery life, although Lora seem to be more power efficient than NB-IOT for a number of reasons.

As mention in the Lora part, devices that use the technology has the ability to choose between three classes A,B and C where Class A class can attain the lowest power consumption than the others. Further, Lora is an asynchronous protocol which means that it doesn't consume more unnecessary power for the synchronization. Also, it uses the adaptive data rate which means that the GW can regulate the data rate by sending maximum data with minimum power consumption. Thus, according to the regulation it can transmit the data with power ranging from 14-27dB. This regulation depends on the spreading factor that it will use. Lora as mentioned is based on the spread spectrum technique which means that the signal can travel in noise and still be decoded from the receiver. Thus, the higher the spreading factor, then the higher is the processing gain and the lower is the achieved data rate and the transmitting power.

On the other hand NB-IoT is a synchronization protocol which means that it consumes extra power for this synchronization even if that it's infrequent. It uses both PSM and eDRX as power saving functionalities and transmits its data with 20/23dB power in release 13 and 14dB in release 14. Due to this continuously synchronization with the network, NB-IoT consumes more power than Lora.

Thus the Lora technology with class A and high spreading factor can be characterized as more power efficient than NB-IoT and should be used when the application need extremely high power efficient.

Chapter 4

Comparative Evaluation of LoRa and NB-IoTs

In order to confirm some of the manufacture similarities and dissimilarities for the two technologies, experiments were performed in real environments. For the Lora technology The things network was used with Arduino devices that support the technology whereas for NB-IoT technology, current cellular networks that support the technology were used with Arduino Uno and Sim7000E.

4.1 Background

The things network:

The things network allows the user to integrate quickly and fast a LoraWan network using Lora devices and GWs with the aim to exchange data between the different IOT applications. It’s an open-source and decentralized infrastructure for the Internet of things[23]. It has already been used worldwide and it has already been incorporated in Cyprus. A simple registration in the platform is needed and the user can be benefit from the services that it can provide. Further, the user must select and buy the appropriate devices and GWs according to the application requirements. There is a list with plenty of devices, sensors and GWs that can choose with a normal cost. It also allows you to build both private and a public network. Subsequently, the Things network was the ideal solution to build the LoraWan network for this project.

To continue with, the Things Network can provide two specific services: management of the gateways and of the applications.

Applications and devices can be managed via the thing network console[23]. In this console, a user can monitor the data from the devices, register applications, devices and GWs, manage integrations in order to connect the things network with other external platforms and also add collaborations. It's essential to register the devices and the GWs into the things network in order to use the LoraWan technology and be benefit from its security.

Management of the applications

In order to add an application into the things network console two simple steps must be performed. The first step is to log in into the things network platform and select the console tab. After that, the only thing that remained to do is to add a simple ID and name for the application and the platform will provide the necessary keys and appEUI. These two parameters are essential in order to use the LoraWan network and exchange data with the devices. After creating the application the user can do the following:

- *Register devices into the application:* In order a device to communicate via the things network and perform the OTTA procedure as mention in the Lora part a registration must be performed [23]. After retrieving the Device EUI by writing a program on the ARDUINO IDE and after adding the application in the console, the devices can be register by entering the retrieved Device EUI. Then an App key is automatically generated and the App EUI is the same with the APP EUI that generated at the beginning when the app was created. Then in the devices these two parameters must be included in order to send data using the LoraWan network.

- *Monitor data:* The user can monitor in real time the data that are transmitted from the devices
- *Add integrations:* A user can also add integrations into the application. Integration gives the opportunity to connect to external platforms with the aim to manage, process and monitor data through these platforms. Integrations synchronize the external platform with the things network. Many external platforms collaborate with the things network such as storage integration for saving data into a database, tago which is a web platform and help to monitor, process and manage data etc.
- *Define the payload format*: Devices encrypt the data and send it to the application. This data are in “bytes” format. In order to extract these data, a decryption must be performed. This decryption can be done in the payload format tab by writing the necessary code in order to retrieve the data.

Management of the Gateways:

In order to complete the LoraWan network the Gateways must be registered as well into the things network platform otherwise, the packets would be marked as untrusted[23]. The registration of the GW is simple and similar as other registrations. After logging in into the console and select the Gw’s tab then the user can register the GWs by entering the necessary information. These information are the device readable ID that the user can determine, if the GW will only forward packets to the devices and to the network servers, the frequency that the GW will operate and since Cyprus is in Europe the European frequency plan would be used. Further, the user must determine if the GW is for indoor or outdoor usage. Also, the user determines the router that the GW will connect to. As mention in the

2.1.3 LoraWan Architecture the router forwards the packets into the network server using other Mac protocols such as wifi Ethernet etc. Finally, the user determines the exact location of the GW.

4.2 Hardware

In order to establish the experiments using the two technologies LoraWan and NB-IoT the necessary equipment had to be chosen and bought. It was necessary that the devices would:

- support the above technologies
- have a small cost
- be able to be expanded into a bigger network in the future

Therefore, after a research that was establish in order to build a LoRa network, the things network platform and devices were used since the things network offered many benefits and the devices had a low cost whereas in order to build an NB-IoT network Arduino UNO and SIm7000E expansion shield were used since sim7000E could support the technology.

ARDUINO

There are many kinds of arduino boards like arduino uno r3, arduino Leonardo etc. Each one of them have different characteristic and the user must choose between them. Arduino boards already become popular in research communities and they have already been used in different projects and investigations due to their suitable characteristics. They:

- can be used easily and they are ideal for different kinds of projects

- can be expanded by adding sensors and shields. More precisely, shields help the devices to connect into the internet and perform different actions(send an email, send measurements etc.) using different technologies. Also they provide other services such as sending a message to a mobile phone.
- can be managed quickly by using the ARDUINO IDE
- are inexpensive
- have an open-source software(ARDUINO IDE)

More precisely, ARDUINO IDE is a cross-platform that runs on different operating systems. It's an environment that let the users to write and upload their code into the arduino boards in order to flash light, read inputs from the sensors, connect to the internet etc. Users must only connect the arduino boards with the computer that has an installed arduino IDE, via a USB and the code would be uploaded on the microcontroller. Further, the arduino IDE uses the c++ programming language and can include many libraries in order to offer its services. There are libraries for the things network and therefore there are arduino modules which are able to connect and use the things network and thus the LoraWan technology. Further, there are libraries for sim7000E that help establishing the NB-IoT network. Subsequently, arduino modules were suitable for this project.

The things uno

The things uno is basically an arduino device and it‘s based on the arduino Leonardo board. It contains a lorawan chip and therefore, the technology can be used through this module. It's fully compatible with the Arduino IDE as every other arduino device and in order to operate the necessary code must be uploaded to the chip. It works with the “The things network” and consequently it was ideal for this project.

The things gateway

In order to use the lora technology a gateway had also to be bought. The things network has three kinds of gateways(the things indoor Gw, the things outdoor GW and the things GW). A constructor chooses between them according to the applications needs. The things network GW will let the devices use the Lora technology and take advantage of its features. Most of the Lorawan’s features are performed through the things network such as the connection with the network server and all of its performances such as the adaptive data rate, packets relay etc. The things network GW can achieve a range of 10km, connect easily with a wifi or an Ethernet and also create a secure network through the OTTA or ABR procedure. In order to use the GW an activation must be performed and registration to the things network platform. For this project the Things network GW was chosen since it was the most appropriate.

Figure 4.2.1 The things gateway

Arduino Uno R3

There are many Arduino modules like the Arduino Uno r3, arduino Leonardo, ARduino Mega etc. Each one consists of a microcontroller and analog and digital pins for input/output.However,each module has different memory size, different number of pins and a different microcontroller. Arduino Uno R3 is very popular module and it’s selected to this project.

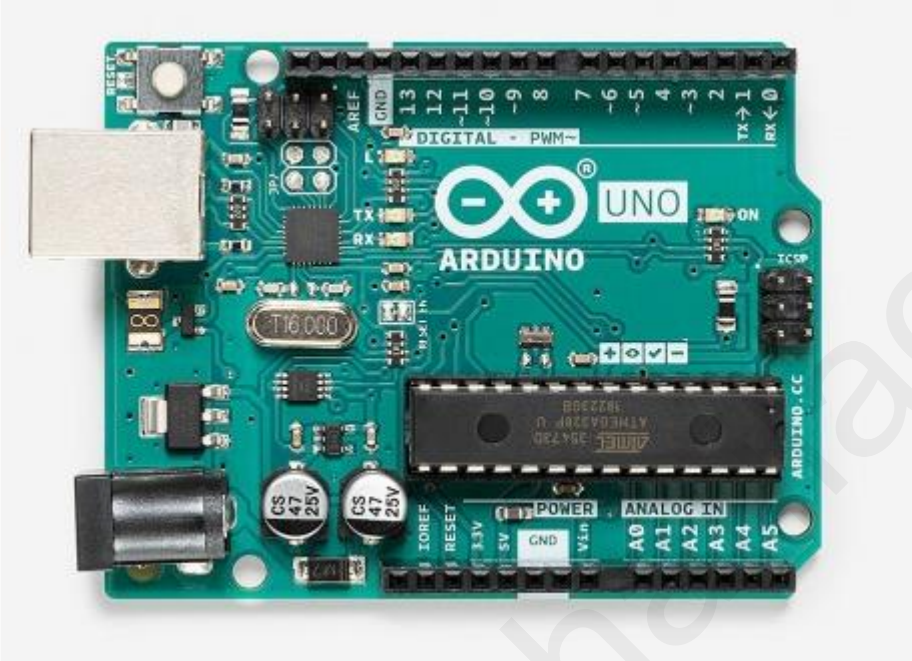


Figure 4.2.2 Arduino Uno R3

More precisely, arduino Uno has the following characteristics:

i. It has 14 pins which 6 of them are analog pins. Therefore, more sensors can be added and the project can easily be expanded.

ii. It can operate either with batteries or with electricity. The recommended voltage is 7-12V and the limited voltage that someone can use is estimated from 6-20V.

iii. It can connect to the Internet using ‘SHIELDS’. Shields can easily connect with arduino modules and they are responsible for establishing the connection with the network.

iv. A program can be uploaded via a USB cable which connects the PC with the module. The program is stored on the Arduino and every time it operates the program executes.

v. It has a 'reset button' which forces the program to start from the beginning.

vi. It uses the ATmega328P microcontroller which has three memories:

- FLASH 32KB. This memory stores the uploaded program
- SRAM 2KB which stores the variables which are created when the program start its execution. The variables are erased and re-created each time the program completes or starts respectively.
- EEPROM 1KB which stores long term variables. These variables are stored permanently on the device.

A major disadvantage of the arduino modules is it is not in a case and therefore the microchip can be overheated or damaged by environmental factors. Thus, this will affect the whole system as the arduino will not be able to work. A solution for this is to create a case for the module in order to protect it from dust , heat and cold.

SIM7000E ARDUINO NB-IoT/LTE/GPRS expansion shield

SIm7000E arduino expansion shield can use three technologies NB-IoT, LTE and GPRS according to the operating area. If the BS on the current area supports the technologies then the shield is able to connect the devices using these technologies. Furthermore, it can be easily connected with the Arduino UNO and it offers security as it needs a sim card for its operation. The sim card also allows the shield to perform some additional actions such as send messages and establish phone calls. Furthermore, the shield can find the exact position of arduino using a GNSS antenna and also additional sensors can connect to it. In order to operate and offer its services it needs to connect with external batteries. To continue with there are different types of sim7000 shields according to the operating area and the supporting frequency bands.

- Sim7000E supports the B3/B8/B20/B28 frequency bands and it's used mostly in Europe
- Sim7000C supports B1/B3/B5/B8 and it can be used in China
- Sim7000A supports B2/B4/B12/B13 and it can be used in America.

For this project the Sim7000E is used since Cyprus supports the B3/B8/B20/B28 frequency bands.

4.3 Experiments

4.3.1 NB-IoT experiments and Results

Many experiments were performed in order to investigate the real performance of NB-IoT in a real environment. For the investigation sim7000 which supports the NB-IoT technology was connected with the arduino uno r3. In addition, GNSS antenna and GSM/LTE was connected with the sim7000E module in order to be able to get the exact position of arduino and connect to the BSs using the NB-IoT technology. Finally, a sim card was inserted in order to operate. The connected devices are shown in the picture[Figure 4.3.1.1 Connection of Arduino Devices]. For each experiment the necessary code was written in the ARDUINO IDE and uploaded into the Arduino device. Further, each one was established many times in order to extract valid results.

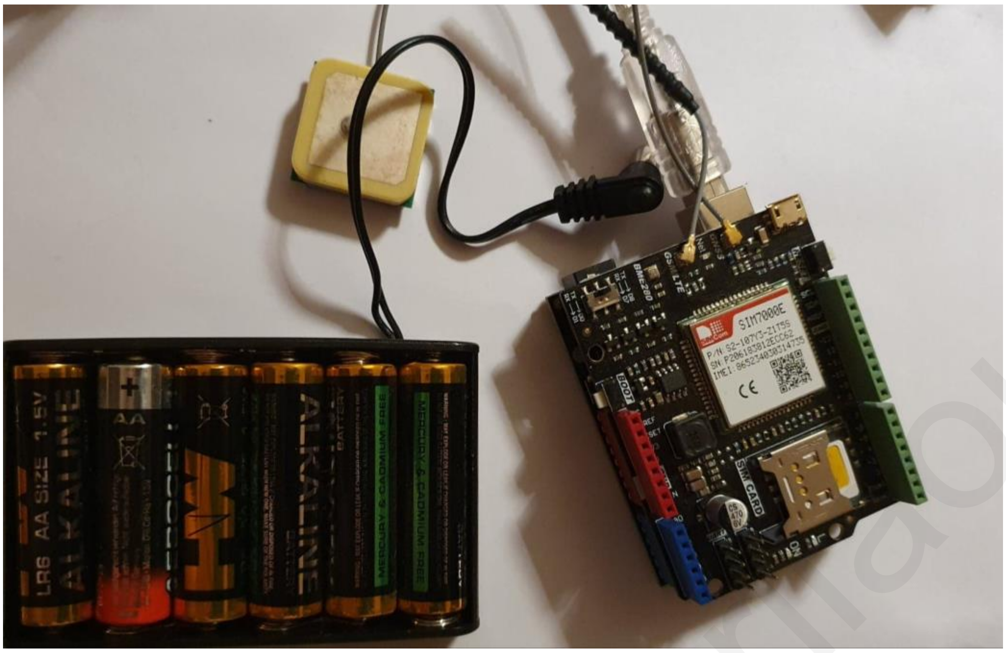


Figure 4.3.1.1 Connection of Arduino Devices

In the first experiment, 77bytes of data were sent in all of the environments because the primary goal was to observe the signal strength in a line of sight and non-line of sight environment with houses,buildings etc. Measurements were taken considering 5 different distances: 550,1200,1500,1800 and >2000 m far from the BS.

The second experiment was performed in order to observe the time that arduino needed to:

- Turn on the device
- Attach service. More precisely, after selecting the NB-IoT technology, a connection with the BS must be performed.
- Send data. More precisely execute the GET or POST request. In the current program GET requests were performed.

The time was measured in the above 10 different locations in order to observe any delay that could be caused due to obstacles or distance.

Problems:

The NB-IoT technology was aimed to be tested using two operators in order to observe its performance considering different providers. However, the second sim card was could not be connected to the BS and use the NB-IoT technology probably because of operators problem. The second problem that was observed during the use of the devices is that they were overheated during high temperatures. Therefore, new equipment had to be bought.

Experiment 1:

The first experiment was performed in order to determine the difference in the signal strength when the arduino was at a line of sight location and at the non-line of sight with obstacles. The precise locations that the measurements were taken are shown in the picture[Figure 4.3.1.2]. Locations 6,7,8,9,11 were for the line of sight and locations 1,2,4,10 were for the non-line of sight. Yellow color refers to the Arduino that got only excellent signal strength, orange refer to Arduino that reached lower values good/ok , red indicates that there was no any connection with the BS and green refers to the handover. The experiment took place in a village in Cyprus where for the line of sight, the locations, contained only fields with no obstacles. Contrariwise, for the non-line of sight measurements were taken in the heart of the village where obstacles such as buildings, trees etc were existed. After locating the BS of the operator that was chosen the arduino device moved into these locations and the signal strength was observed.

In order to observe the measurements a connection with a server had to be established in order to send the data from Arduino. Also, the Arduino was connected to a computer in order to observe the results in the serial monitor through the Arduino IDE. Arduino code, contained a while loop in order to observe the Signal strength many times. The results were as expected were the signal was in an acceptable condition in all environments. In the line of sight the signal was strong even in 1800m far from the BS in contrast to the non-line of sight where the signal had lower values due to obstacles. More precisely, the results are shown in the tables [Table 7] and [Table 8]. At 550m results were taken in indoor and outdoor. It was observed that in both situations the signal had an excellent condition, thus confirming that the NB-IoT technology can perform well even in indoor. In 1500m in the line of sight the signal was good/excellent whereas in the non-line of sight it was ok/good. Therefore, even with obstacles and far from the BS the signal has an acceptable condition. In 1800m the signal in the line of sight was ok/good whereas in the non-line of sight a handover was observed because the signal strength increased. The current BS supports only 2000m range so when the arduino moved in a location that was >2000m two actions were observed:

- A handover
- Lost of signal, and therefore arduino had to establish the connection again with the BS.

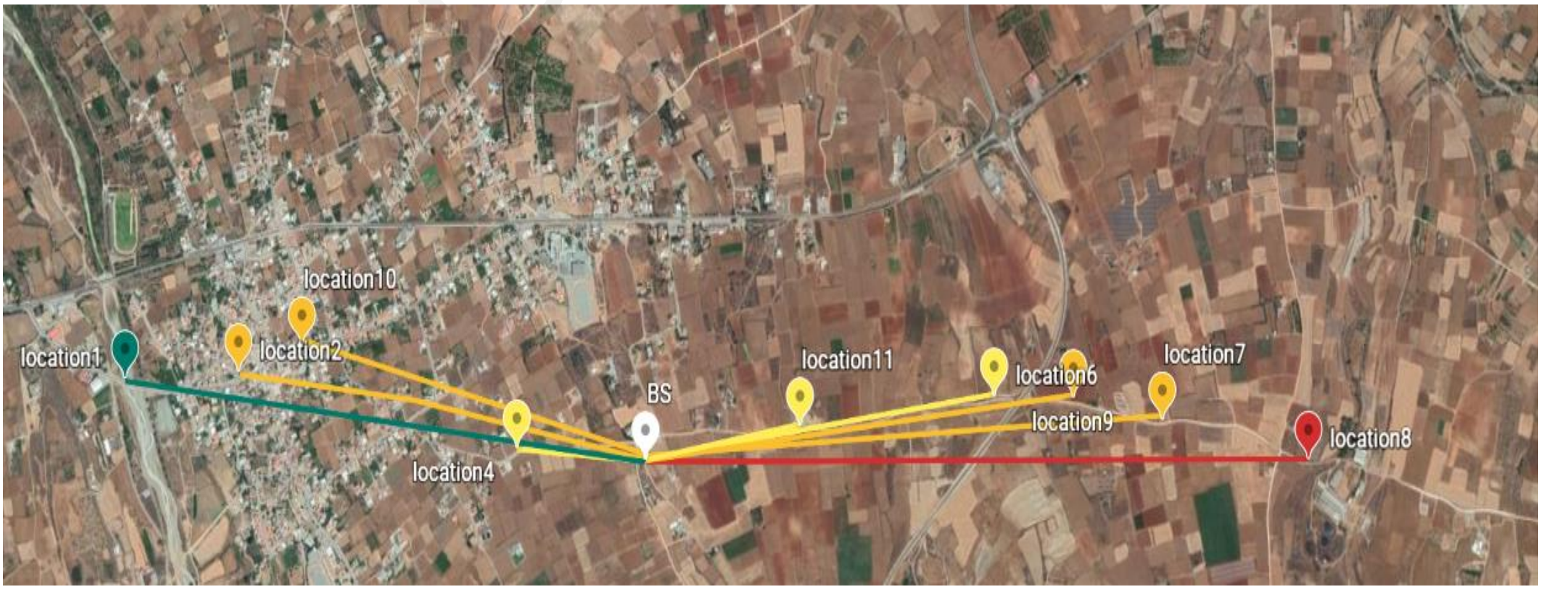


Figure 4.3.1.3 Locations in which NB-IoT measurements were taken

Line of Sight results:

	Distance (m)	Signal Strength	dBm	Condition
1	550	27-30	-59 - -53	Excellent
2	1200	25-30	-63 - -53	Excellent
3	1500	19-23	-75 - -67	19→Good, ≥20 Excellent
4	1800	13-19	-87 - -75	13-14→OK ,15-19→Good
5	>2000	0	>-110	No Signal

Table 7 NB-IoT line of sight results

Non-line of sight results:

	Distance (m)	Signal Strength	dBm	Condition
1	550(indoor)	24-30	-65 - -53	Excellent
2	1200	17-22	-79 - -61	17-19→Good, 20-22→Excellent
3	1500	13-17	-87 - -79	13-14→OK, 15-17→Good
4	1800	Handover	-	-

Table 8 NB-IoT Non-Line of sight results

Experiment 2:

The second experiment was performed in order to observe the time for sending data, connecting to the BS, turn on the device, and observe any delay due to the long distance or obstacles. For this experiment a function called millis() was used. This function returns the number of seconds passed since the Arduino program has started. Therefore, it could show the exact seconds for performing each instruction. However, due to the devices' overhead the times using a code are increased. The time was also calculated with an external clock in order to minimize the overhead and find the real results. Further, when it was possible the time was examined through the at commands.

Results:

Arduino serial monitor showed that arduino needed 32 seconds to turn on. Considering the overhead, the device in order to turns on, it needs 22 seconds.

After selecting the NB-IoT technology an attach with the BS is needed. According to code the seconds that the device needs to attach service with the BS is 20 seconds. With an external clock the time is ranging from 6-10 seconds. Thus, the theory where the NB-IoT needs maximum 10seconds for a BS connection is confirmed.

The time to establish the GET request and send 77 bytes of data to the server in the serial monitor using milis() was 25 seconds whereas with an external clock was 16 seconds. It's essential to mention that no latency was monitored in the line or non-line of sight environment since the time for sending the data was stable at 16seconds. Therefore there is no delay due to obstacles or distance confirming that the technology can operate well in all environments.

4.3.2 Lora and LoraWan experiments and results

In order to check the Lorawan's specifications many experiments had to be established. At first, for the experiments, the lora gateway had to be activated, registered to the things network in order to use its features and then connect it with a wifi network. The next step was to find the devices' EUI which is a unique identifier for the device and register it to the application in the things network console. The device EUI could be found by uploading the necessary code into the arduino module through the Arduino IDE. After registering the device the next step was to send the data using the device. Therefore, the necessary code was written to the ARDUINO IDE. In the code the OTTA procedure was used so that the device could get the necessary permission to send data through the Lora technology. The transmitted data and packets could be monitored through the things network console in the "data" tab.

To continue with, many problems were faced during those experiments where most of them successfully handled. The first problem was the "no-free-channel problem" where the devices could not send any data when higher spreading factors were used. No-free-channel means that there is no available channel for transmission. The things network GW offers eight channels and due to the duty cycle the time in each channel is limited. Therefore, when the spreading factor is higher the time on air is increased and thus the next available time to send the packets is decreased. Subsequently, in order to deal with this problem the frequency of sending the packets had to be decreased. Thus, devices were preconfigured to send data every 40 seconds instead of 10 seconds. The next problem that was not able to be handled was that spreading factors 11 and 12 could not be used.

Considering the experiments that were established, six experiments were made in order to observe the performance of lorawan. Signals, can be affected by many environmental or other factors and therefore each experiment was performed many times in order to extract the average number in distance, latency and packet drops. For every experiment 1byte was send every 40 seconds , coding rate of 4/5 was used , bandwidth of 125hz and different spreading factors. It’s important to mention that in the things network only the spreading factor could be change, the bandwidth and coding rate were stable.

The first experiment was aimed to observe the OTTA procedure, which is the procedure that is executed at the beginning in order to give the device the necessary permission to use the Lora technology.

The second experiment investigated the transmission range that the device can achieve using the Lorawan protocol. The transmission range was investigated by varying the SF(7,9, and 10) in two environments a line of sight until 1800m and+non_line of sight for the remaining km and non-line of sight environment. The distance for the available line of sight was only 1800m and therefore it was chosen to combine it with non-line of sight in order to find the transmission range. Further, the transmission range was tested again in a new experiment which involved the elaboration of the GW. Again the results were noted and were as expected since more high can increase the performance of Lorawan’s protocol and therefore confirming the paper [11].

The third experiment was aimed to investigate any interference between the devices when using the same of different spreading factors in order to observe the performance of the things network platform.

The fourth experiment investigates its performance when the GW was indoor and outdoor and the results were noted. Again the results were as expected since the outdoor GW could reach higher distances than the indoor GW.

The fifth experiment investigates the latency that the signal can experience, how many packet drops where observed, and also the RSSI and SNR values in distances 500,1200,1500,1800 for line of sight and non-line of sight. These factors were examined using two different SFs 7, 10 in order to investigate the difference between these values.

The sixth experiment investigates the duty cycle and more precisely the number of messages that a Lora device can send using spreading Factors 7, 8,9,10,11 and 12.

Experiments:

Experiment 1:

The first experiment observes the OTTA procedure which is the first procedure that is executed in order to give the device the appropriate permission to send packets through the Lora technology. As mentioned devices are registered to the things network and at the registration an app key is produced which is used in the Arduino code and it’s responsible for the OTTA procedure. At the beginning devices send this key through the things network and the things network which is responsible for the network and application server checks if the device belongs to group of devices that can use the technology. If it belongs then two extra keys are produced, the Network session key and the application session key in order for the two layer encryption to be established. The ABP procedure could also be used but the OTTA procedure is characterized as more reliable and securable since the session keys would be produced in every activation. In the ABP procedure session keys are assigning manually on the device.

Experiment 2:

The second experiment investigated the transmission range of LoraWan protocol in two different environments (line of sight until 1800m combined with non-line of sight for the remaining distance and non-line of sight) using different highs for the GW. Two different spreading factors were used when the GW was located at the second floor and not elaborated further, contrariwise, when it was elaborated , three spreading factors were used in order to observe its performance. The results were as expected since the SF with 10 reached the highest distance and the SF7 reached the smallest distance. Further, as expected when the GW was elaborated the distance increased substantially. More precisely:

- For the first environment and when the GW elaborated Lora device with SF=7 reached at average 2km, SF=9 it reached 2.5km, and SF=10 reached up to 3.45km.
- For the first environment and when the GW was at second floor but not elaborated further Lora device with SF=7 reached only 1700m, with SF=9 it reached 1900m.
- For the second environment and when the GW was elaborated Lora device with SF=7 reached 1450m, with SF=10 1700m.
- For the second environment and when the GW was not elaborated but was located at the second floor , Lora device with spreading factor 7 reached only 400m whereas with SF=10 it reached 600m.

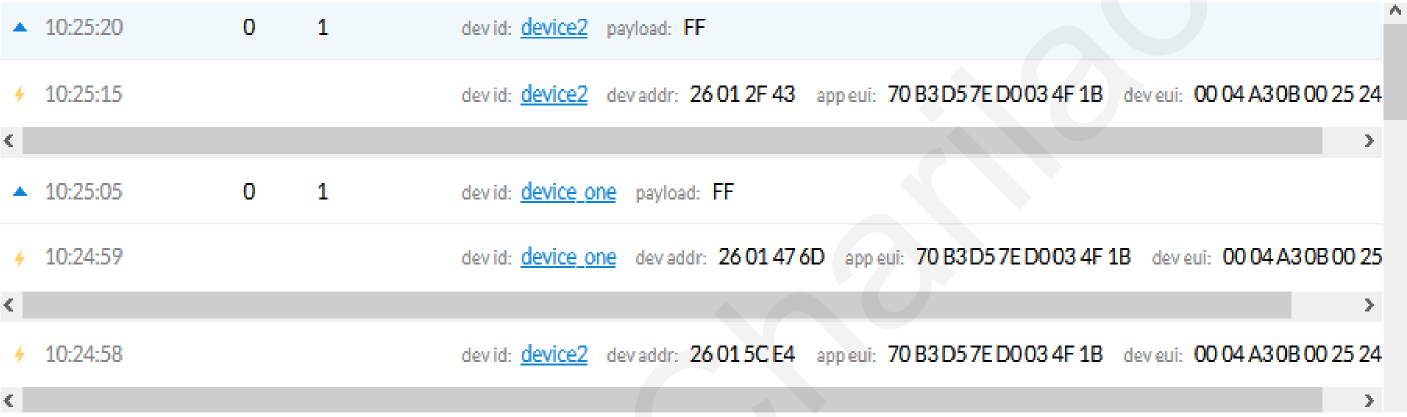
Clearly, the elaboration of the GW and the higher spreading factors can increase substantially the performance of the Lorawan's protocol in all environments since it can reach greater distances. Further, as it can be seen from the above, the line of sight combined with non-line of sight environment can reach greater distances than the non-line of sight. Obstacles can attenuate the signal and therefore significantly decrease the distance. Therefore, line of sight combined with non-line can achieve longer distances than the non-line of sigh. Although, high spreading factors can experience more attenuation due to the processing gain and thus the signal can travel longer. Taking all the above into consideration, line of sight, high spreading factors, and the elaborator of the GW can increase substantially the performance of the Lora technology. Further, from the results it is confirmed that the lora technology can achieve long distances especially in an ideal environment were no obstacles exists.

Experiment 3:

The third experiment explored the performance of the technology when using the same or different spreading factors with the same frequency(125hz) each time. Many experiments were established in order to observe its behavior.

- The first one included two devices using the same spreading factor(SF=10) transmitting on the same area.
- Second one included three devices with different spreading factors SF=7,9,10 transmitted in the same area.

It was observed that when the devices were connected at the same time only one of them performed the OTTA procedure and continued transmitting its packets while the second device failed to performed the OTTA procedure at the first time. The second device retried to perform the OTTA procedure after a few seconds, and then it succeed and continued transmitting its packets. This effect is shown in the picture[Figure 5.3.2.1] and it was re-established using same and different spreading factors. Each time only the strongest signal succeeds in the OTTA procedure and continues transmitting its packets. Further, considering all of the above experiments no interruptions or packet drops were observed when same or different spreading factors were used. Therefore, it can be concluded that there is no/minimum interference when using the same or different spreading factors. As mentioned, Lora technology is based on the spread spectrum technique which means that multiple used can use the technology with minimum interference. Each user uses a different spreading code and the spreading codes are orthogonal to each other. Therefore minimum interference can be experienced as the devices are located near to each other or with small distance.



```
▲ 10:25:20   0   1   dev id: device2     payload: FF
⚡ 10:25:15           dev id: device2     dev addr: 26 01 2F 43   app eui: 70 B3 D5 7E D0 03 4F 1B   dev eui: 00 04 A3 0B 00 25 24
▲ 10:25:05   0   1   dev id: device_one  payload: FF
⚡ 10:24:59           dev id: device_one  dev addr: 26 01 47 6D   app eui: 70 B3 D5 7E D0 03 4F 1B   dev eui: 00 04 A3 0B 00 25
⚡ 10:24:58           dev id: device2     dev addr: 26 01 5C E4   app eui: 70 B3 D5 7E D0 03 4F 1B   dev eui: 00 04 A3 0B 00 25 24
```

Figure 5.3.2.2 Result from connecting Lora devices at the same time

Experiment 4:

The fourth experiment examined the LoraWan's performance when the Gateway was indoor and outdoor. When the Gateway was indoor and the lora device transmitted its packets using SF=7 the maximum distance that could be attained was only 900m. Contrariwise, when the GW was outdoor and the lora device transmitted again its packets using SF=7 the maximum distance was 1.8km. Therefore, it can be observed that when the gateway is located outdoor the signal can reach higher distances. The results were as expected since buildings and obstacles attenuate more easily the signal strength and therefore they force it to attain shorter distances.

Experiment 5:

The fifth experiment examined the performance of Lora technology by investigating the:

- Latency
- RSSI & SNR
- any packet drops

into line of sight environment and non-line of sight environment for SF 7 and 10 and for distances 550,1200,1500,1800 and 550,1000,1500,1700 consequently.

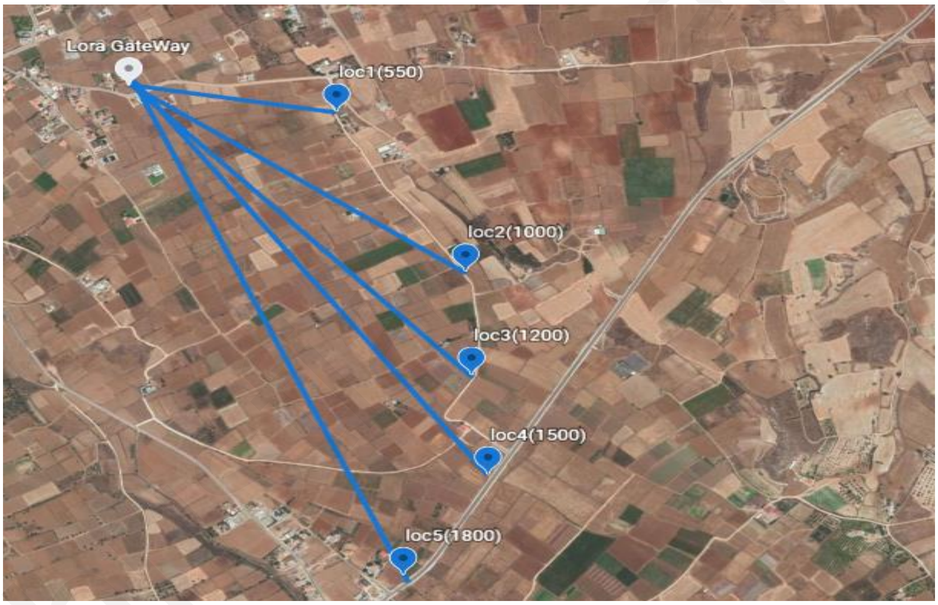


Figure 4.3.2.1 Line of sight locations

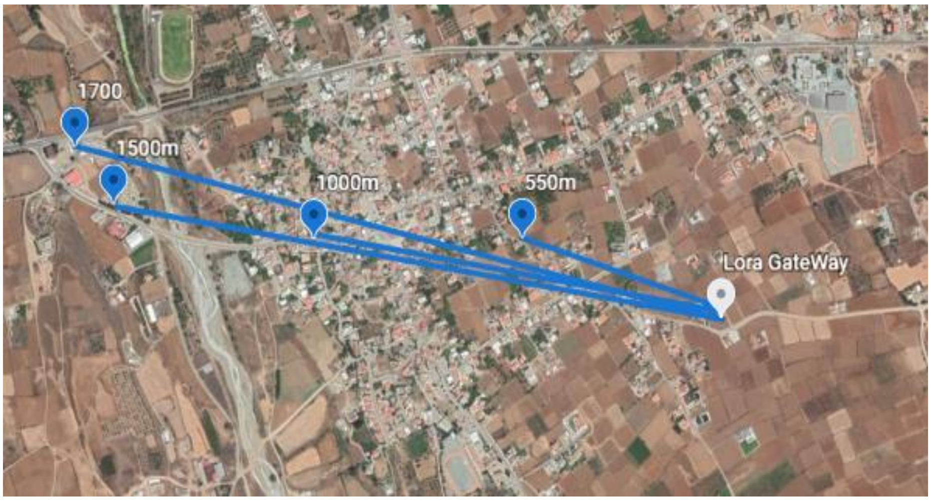


Figure 4.3.2.2 NLOS locations

In order to determine the network's performance RSSI, SNR, latency and packets drops were observed. RSSI referrers to the signal quality that the receiver receives and it decreases as the device moves apart from the GW. On the other hand SNR shows if the received signal can be decoded from the receiver. As the ED moves apart the SNR decreases since the signals attenuate due to long distances and also due to more noise and interference. In networks SNR that is below zero means that the signal is being corrupted and cannot be decoded from the receiver. However, in Lora due to the processing gain signal can be under zero and still be decoded well. Clearly, from the tables below this is confirmed as it is observed that the SNR can reach lower values as the SF increases. When the signal reaches its destination the processing gain is added and therefore the signal has higher power. The packet drops are also lower when the SF is higher and again this is due to the SNR where the signal can travel in a lot of noise and the decoder is still available to get the necessary info from it.

Line of sight:

Distance	**SF=7**	**RSSI**	**SNR**	**Latency**	**Packets drop**
550	√	-101 - - 108	8.5	2	0
1000	√	-107	6.5	2	0
1200	√	-117 - -119	-0.5 - 1.5	4	2
1500	√	-121- -123	-2- -4	4	2
1800	√	-115	0.5	2	0

Table 9 Lorawan Line of Sight results of SF=7

Distance	**SF=9**	**RSSI**	**SNR**	**Latency**	**Packets drop**
550	√	-113	6.75	2	0
1000	√	-87 - (-102)	8.75 – 11	2	0
1200	√	-109 - -117	5.5 – 7.5	4	2
1500	√	-117	3	2	0
1800	√	-117 - -121	-7.5 – 2.25	2	0

Table 10 Lorawan Line of Sight results of SF=9

Distance	SF=10	RSSI	SNR	Latency	Packets drop
550	√	-105	4	2	0
1000	√	-99 - -111	5.25 – 10.25	2	0
1200	√	-119	-3	2	0
1500	√	-120	2.5	2	0
1800	√	-111	8.25	2	0

Table 11 Lorawan Line of Sight results of SF=10

Non-line of sight:

Distance	SF=7	RSSI	SNR	Latency	Packets drop
550	√	-120	1.25	2	0
800	√	-121	-6	2	0
1000	√	-120	-1	2	2
1700	√	-121 - -123	-5.5 – -6.75	6	3

Table 12 Lorawan Non-Line of Sight results of SF=7

Distance	SF=10	RSSI	SNR	Latency	Packets drop
550	√	-121	-4.5	2	0
800	√	-121	-15	2	0
1000	√	-121	-6.76 - -10.25	2	0
1500	√	-123	-14	12	6
1700	√	-120	-12	12	6

Table 13 Lorawan Non-Line of Sight results of SF=10

From the tables above it can be observed the great performance of lorawan in a line of sight environment where minimum losses and attenuation are experienced. Further it is observed that the SNR decreases and the latency increases when the device transmits in a non-line of sight environment or when the distance is increased. The signal experiences more attenuation as it passes through obstacles or as it travels through long distances and as a result the SNR decrease, the latency increases and packet loss may be observed. Further, as it can be seen from above, that there are more packet loss in a non-line of sight environment than in a line of sight. The signal strength as it pass through obstacles and goes through a long distance it attenuates more easily and its harder for the decoder to decode the signal. Therefore there is more packet loss and thus the latency is increased.

<u>Experiment 6:</u>

The sixth experiment was aimed to investigate the duty cycle and the number of messages that a lora device can send when using Spreading factors 7-12. The things network regulate the duty cycle to be 1% in order to be fair and therefore the uplink airtime is estimated to be

30 seconds whereas in the downlink it allows only 10 messages. In order to check how many message a lora device can send using the above SFs the air time for each SF needed to be found. To continue with, it could be found by uploading three different codes(one for each SF) into the thing uno device. The code would force the device to send messages(of 1 byte) using the Lora technology and through the things network console the air time for each SF could be observed. The air time for SF=7 was as expected the smallest and it was only 25.856ms for each packet and for SF=12 was as expected the highest and it was 827.392ms. The air time in higher spreading factors is higher because of the longer communication link that is established. Therefore, the bits need more time to travel and arrive at the receiver.

More precisely, using SF=7 with air time 25.856ms and since the uplink air time is 30s the total messages that a lora device can send is estimated to be 1160 per day. (30000/25.856=1160.) By using SF=9 the messages are reduced substantially and are estimated to be 290 messages per day and by using SF=12 Lora device can only send 36 messages per day. It is observed from the table below that when the SF increases by 1 the air time is duplicated and the number of messages is reduced by half. Therefore, it is recommended to use lower SF if it’s possible and when the number of messages that a device sends per day is higher than 36 messages

SF	Air Time	Messages per day
7	25.856	1160
8	51.712	580
9	103.424	290
10	206.848	145
11	413.696	72
12	827.392	36

Table 14 Messages Per day

Further, the higher is the spreading factor the lower is the achievable data rate and the higher is the power consumption. The higher is the spreading factor means that the higher is the spreading code since the length of the spreading code depends on the number of the spreading factor. Therefore, by encoding each bit with the longer spreading code, and by having a stable bandwidth the achievable data rate is reduced. Also, more packets will be transmitted in order to send all the data and thus higher utilization and power will be experienced. Thus, in order to achieve longer battery life and less gateway utilization the SF must be kept at the minimum. Subsequently, a higher data rate can be achieved and lower power consumption.

Chapter 5

Comparison of NB-IoT and LoRa technology through real experiments

Many experiments were established in order to observe the real performance of both NB-IoT and LORA technology in different environments. Most of the results, for both technologies were as expected since they both confirmed their theoretical characteristics and other experiments that were established.

More precisely, in the Lora technology, the elaboration of the GW and the increase of the spreading factor showed a significant contribution in its performance and in the achievable transmission range. Further, as expected and as the experiments showed the transmission latency in the NB-IoT technology was significantly lower than the Lora technology due to the use of the licensed spectrum and the continuously synchronization with the network. Both technologies have great performance in the line of sight environment but in the non-line of sight as showed NB-IoT had a better performance.It is expected that NB-IoT showed better performance because the BS was high enough in order to avoid further interference due to obstacles. In lora the GW was elaborated but it could not be elaborated as high as the NB-IoT's BS. Therefore, Lora technology experienced many packet drops in the non-line of sight environment and the latency increased substantially whereas in NB-IoT the signal strength was at an acceptable level, the latency remained stable and all the data reached their destination.

Although both technologies have great characteristics they can’t be used in all application use cases. The two technologies will be compared considering their differences in Qos, reliability, messages per day, transmission range, latency, performance in line of sight and non-line of sight environments.

QoS(Quality of Service):

As mentioned before QoS refers to the high network reliability, low packet loss and transmission delay and ensuring that the data will arrive and be decoded well from the receiver. However, Qos is a challenge in asynchronous protocols due to possible collisions and interference. On the other hand, Qos is guaranteed in synchronous protocols that use the licensed spectrum in their operation. Therefore, it is confirmed through the experiments that NB-IoT have a great QoS in contrast to LORa.Every transmitted message arrived at its destination with minimum latency thus confirming the benefits of the licensed technologies.

As a consequence, devices that need high quality of service must use the NB-IoT where are devices that do not need Qos can be benefit from the LoRa technology.

Reliability:

Reliability is an important factor in the network communication especially for critical based applications when there is a need to ensure that the packet will arrive and successfully be decoded from the receiver. One of the benefits of the technologies that use the licensed spectrum is that they can provide reliability and thus better performance to the users thus they are a better fit for critical based applications. Therefore, NB-IoT which is based on the licensed spectrum can be benefit from that and provide reliability to its users since no interferences would occur during a transmission. Even if the packet doesn’t arrive at the first time, retransmissions will be used to ensure its arrival.

Contrariwise, Lora belongs to the technologies that operates in an unlicensed spectrum that reliability is not ensured. Collisions, interferences and many packet drops can be occurred as all experiments in the Lora technology showed. In Lora technology there aren't any retransmissions and thus the packet can be lost forever. However there are ways to ensure the arrival of the packet and improve the reliability but the performance will still not be as great as with the NB-IoT technology. To start with, more gateways can be used in order to increase the probability to receive the packet from the end devices and relay it to the network server. In Lora multiple GWs can receive the packets and therefore one of them may be closer to the end device and receive it. Furthermore, in order to ensure reliability acknowledgment messages can be used in order to confirm the packets arrival at the destination. However, this is limited because as every other technology that uses the unlicensed spectrum so as Lora has a duty cycle which defines the time that the ED can use the channel. By using ack messages for each end device will cause capacity drain[22] and the end devices will not able to send more messages until the next day. This is confirmed through the experiment six that was established were the number of messages is fixed node and per day.

Consequently applications that need reliability is better to be benefit from the NB-IoT technology whereas applications that need lower reliability can use the Lora technology.

Messages per day:

Every technology that uses the unlicensed spectrum in its transmission has a duty cycle in order to keep the fairness between the devices that transmit using these technologies. More precisely, duty cycle, refers to the amount of time that the device using the technology can occupy the channel. Usually for these technologies is 1% which means 30 seconds per day. Subsequently, these technologies have a limitation on the number of messages that can send per day. Lora technology which belongs to the unlicensed technologies uses a duty cycle of

1%. Therefore according to experiments that were established, Lora with SF=7 can send the maximum messages(1160) whereas Lora with the highest Sf=12 can send the minimum messages(36). Highest spreading factor can lead to longest distances but also on higher latency, more battery drawn, and fewer messages. Contrariwise, NB-IoT which belongs to the licensed spectrum technologies can send unlimited messages per day. Subsequently, applications that need usual updates can be benefit from the NB-IoT technology whereas applications that need few updates per day can be benefit from the Lora technology.

Latency:

Latency is an important factor in critical based applications and thus it is essential to use an LPWAN technology that can offer minimum latency. AS expected and as experiments showed NB-IoT can achieve lower latency than the Lora technology. Specifically, using NB-IoT to send 77 bytes of data it takes only 16 seconds. Contrariwise, in order to send only 1 byte of data with Lora technology it takes 2 seconds. To continue with, Lora can send only 51 bytes in each message whereas NB-IoT can achieve a higher payload. For this project only 77 bytes of data were tested. Thus, considering the above, sending 51 bytes of data will result in more latency (2*51=102 seconds considering no any packet loss) whereas for 77 bytes in NB-IoT it takes only 16 seconds. Therefore, as expected and since the NB-IoT is a technology that uses the license spectrum the latency is reduced. Further, packet loss are more often in lora technology since is a licence free technology where as in NB-IoT there are less packet losses due to the licensed spectrum. Therefore, extra latency can be observed in Lora technology.

Coverage-Transmission range:

Both technologies can achieve long range since they both use low frequencies for their transmission. Lora in the line of sight environment using high spreading factor(SF=10) showed that it can achieve a really long transmission range of up to 3.5km whereas for lower spreading factors the transmission range was lower. As experiments showed the greater is the elaboration of GW and the higher the spreading factor, the longest is the achievable range. It is expected that with the highest spreading factor(12), in a line of sight environment and with the elaboration of the GW the Lora technology can achieve really long distances, thus confirming its theoretical characteristics.

On the other for the NB-IoT technology the real transmission range could not be observed because every 2km a handover was performed. However, the signal strength was excellent/good indicating that the technology can achieve a long range. Further, considering their coverage, as mentioned lora can be expanded in all areas by only adding extra GWs. Contrariwise, NB-IoT is restricted to upgraded cellular networks. Therefore, for applications that are estimate to be expanded in the future into areas that doesn’t support the NB-IoT technology or they need a really long transmission range Lora technology is ideal for this purpose.

Performance in line and non-line of sight environment

Both technologies had a great performance in both environments. However, NB-IoT seems to have a better performance especially in a non-line of sight environment were even in 1800m it had acceptable signal strength. As mentioned , NB-IoT showed better performance because the BS was high enough in order to avoid further interference due to obstacles. In lora the GW was elaborated but it could not be elaborated as high as the NB-IoT’s BS. Therefore, Lora with SF=7 could reach at average only 1450m and it had many packet drops at high distances. Although, with higher spreading factors, it could reached higher distances but again many packet drops were experienced due to the attenuation of the signals. On the other hand, in the NB-IoT packet drops could not be observed. However, the latency was stable and the data were successfully received which can indicate that it didn't experience any packet drops. To continue with, considering the line of sight environment both technologies had a great performance. Lora didn't experience many packet drops even in a high distance at 3.45 km and the latency was at maximum 6 seconds for sending 1 byte. Higher spreading factors can reduce the packet drops because signals are more resistance to any environmental noises or any other interference due to the processing gain that can be achieved. However, NB-IoT had an excellent performance in a line of sight environment were the signal was good even in high distances (1800m).

	NB-IoT	**Lora**
Reliability & Qos	Guaranteed	No QoS, no guarantee of reliability
Messages per day	Unlimited	Limited according to SF
Latency	Small (16 seconds for 77 bytes)	Bigger (2 sec for 1 Byte)
Coverage-Transmission range	Restricted to areas that contain the cellular networks Range could not be observed- every 2000 there was handover or lost of signal	Bigger range-higher SFs and elevation of GW have greater distances Can be expanded in all areas
Performance in line and non-line of sight environment	Good in both environments	Good – higher SF have less packet loss&delays SF 7&9 had packet loss in LOS but SF10 didn't experience any packet loss

Table 15 Comparison of Lora and NB-IoT in a real environment

Chapter 6

Conclusion and Future work

Nb-IoT and Lora technology are two of the most promising technologies for the IoT and can be used efficiently into Cyprus. Lora can be used through the things network whereas NB-IoT can be used through the sim7000E arduino expansion shield combined with a sim card which supports the technology.

Both technologies confirmed their theoretical characteristics and can serve constructively the IOT. They both can offer security and confidentiality, long transmission range, low power consumption, scalability and mobility. As a reminder, NB-IoT uses the LTE encryption whereas Lora uses two level encryption/decryption with the AES algorithm and both technologies force the devices to get the necessary permission before using these technologies.

Experiments showed that in both technologies considering the line of sight environment the signal had higher strength and could reach higher distances in contrast to the non-line of sight. This is because line of sight is an environment without obstacles and therefore the signal only attenuates due to the long distances and environmental factors. As showed, obstacles can attenuate the signal and significantly reduce the achievable distance. Further, since NB-IoT has deep penetration when the device was located deep indoor the signal had good signal strength. Considering the lora technology, the signal could also be decoded well when it was located indoor but the transmission range reduced substantially. For SF=7 when it was located indoor the transmission range was only 900m whereas when it was located outdoor it was 1700m. Further, RSSI ,SNR ,packet drops and latency were able to show the real performance of Lora technology, whereas signal strength and latency could also show the performance of NB-IoT. To continue with, experiments showed that elaboration of the GW in the Lora technology and high spreading factors can increase substantially the transmission range. However, higher spreading factors reduce the number of messages due to the higher time on air due to the longer communication link. Real transmission range could not be found in NB-IoT because every 2000km a handover was performed. However, due to the good results in signal strength and latency NB-IoT is estimated to achieve high distances. On the other hand in lora technology, the only achievable line of sight environment was until 1800m and therefore it was combined with the non-line of sight and the transmission range for SF=10 was 3.5km. Higher spreading factors could not be used but it is estimated that can reach higher distance with higher spreading factors. Further, considering the interferences, NB-IoT uses the licensed spectrum so interferences are minimum/insignificant as experiment2.2.5.1 Experiment in real environment showed. On the other hand, considering the Lora technology, after some experiments that they were established in paper [8] they conclude that Lora devices are robust against wifi signals when using the same or adjacent frequencies. However considering the in-band interferences experiments in [11] and [18] showed the following results:

- As the number of nodes increased, the throughput was reduced due to possible collisions and interferences that occurred
- Using the same parameters could lead to capture effect when only the strongest signal survives.

These results could not be confirmed because of the small number of available nodes(only three) and also because there was no available way to monitor any capture effect when the device didn't send any packets. To summarize, NB-IoT can experience low /insignificant interference due to the license spectrum whereas Lora can experience higher interferences. However, as the experiments, the theory and this project showed each one is ideal for specific kinds of applications.

To continue with many problems were faced during those experiments were most of them were solved. The NB-IoT could only be tested using one operator probably because of operators problem. The second problem that was observed during the use of the devices is that they were overheated during high temperatures. Therefore, new equipment had to be bought. Considering the Lora technology, the first problem was the "no-free-channel problem" where the devices had to wait the next available channel to send their data when higher spreading factors were used. No-free-channel means that there is no available channel for transmission. The things network GW offers eight channels and due to the duty cycle the time in each channel is limited. Therefore, when the spreading factor is higher the time on air is increased and thus the next available time to send the packets is decreased. Subsequently, in order to deal with this problem the frequency of sending the packets had to be decreased. Thus, devices were preconfigured to send data every 40 seconds instead of 10 seconds. The next problem that was not able to be handled was that spreading factors 11 and 12 could not be used using the Things network..

6.1 IoT Application examples that can use NB-IoT or Lora

NB-IoT is considered more applicable for applications that need high Qos&reliability higher throughput and data rate and low latency whereas Lora is more appropriate for applications that need higher power efficient, lower cost, creation of private networks and expansion in rural areas.

More precisely, NB-IoT has higher reliability, lower latency and higher QOS due to the use of the license spectrum. Therefore its ideal for time-based applications and for applications that require high quality of service and low latency. As the experiments showed the latency is small and its 16 seconds to send 78 bytes of data in contrast to Lora technology which needs much more time. Also, NB-IoT is ideal for applications that send many bytes and many packets per day. Lora has a limit in the number of transmitted packets due to the duty cycle.

Some real life examples that can use the two technologies are electric metering, smart farming, pallet tracking for logistics etc. However, only one of them fits better for each application.

To start with, electric metering refers to the continuously monitoring of the electric energy that is consumed by a building using a device. These devices have continuous power source so power efficient and low power consumption is not a problem for this kind of application. Electric metering requires frequent communication to notify the users, low latency and high data rate in order to inform them immediately and also good signal penetration since devices may be located inside the premises. Both technologies can be used in this kind of application since both can achieve the above requirements. However, due to the fact that this app requires higher data rate and low latency, NB-IoT is a better fit because it can achieve 250kbps data rate whereas Lora can achieve 50kbps. Also, due to the continuously synchronization with the network and to the use of the licenced spectrum which is free of interferences NB-IoT have lower latency than Lora which may experience interferences due to the licenced free frequently used spectrum.

Another example of the IOT application is the smart farming which consists of sensors and actuators that can monitor, analyse and thus improve the agriculture. These devices require extremely low power consumption because devices cannot use any power source and also high coverage because a BS may be located kilometres apart. Lora technology is more appropriate than NB-IoT since NB-IoT is restricted to areas with upgraded cellular networks that support the technology. Thus, in rural areas cellular networks may not be able to support the technology yet. Further, even if rural areas support the NB-IoT, Lora is again a better choice because it can achieve higher power efficient than NB-IoT and also has higher coverage than NB-IoT.

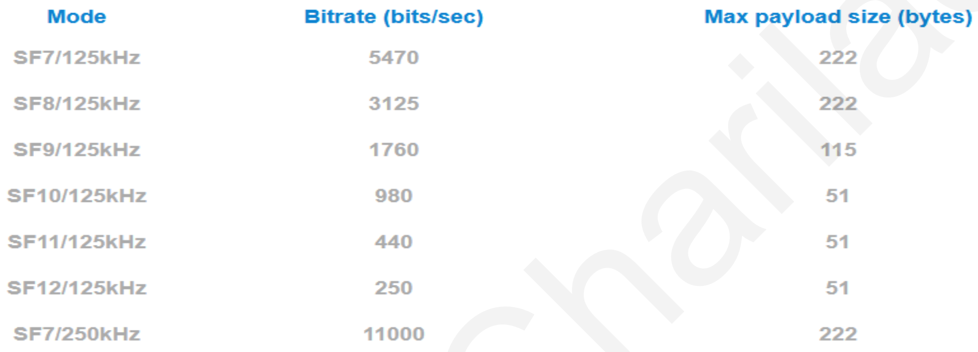
Moreover, another IoT example is the pallet tracking where devices are responsible to determine the location of the goods and also monitor their condition [12]. The technology that will provide connectivity to these devices must be power efficient since it’s difficult to frequently change the batteries of all those devices and also must be with low cost. Also, devices may change location frequently so the technology must be able to support the mobility functionality. Further, the technology must be able to cover all areas including rural areas since the goods may be located in different areas. Therefore, Lora is a better choice since it can achieve the above requirements. Although, NB-IoT support the mobility functionality, it’s difficult for the technology to keep changing BSs while the ED moves, as each ED is connected to a single BS and it needs to reselect another one for each time it moves. On the other hand, Lora is not connected to a single BS but rather all the BSs that they are near to the ED can catch the packets, thus causing a minimum latency. Further, Lora can be expanded and be supported in all areas whereas NB-IoT is restricted to areas with upgraded cellular networks. To continue with, Lora has lower cost than NB-IoT since the NB-IoT has monthly fees to the operators. Lastly, Lora has better power efficient that NB-IoT allowing the devices to have longer battery life. Subsequently, Lora is a better choice for this kind of application.

6.2 Future work

6.2.1 Best practises for LoraWan

According to the “The things Network” there are some practises that are good to be followed in order to build an efficient application for a smart city. In order to keep the device to be power efficient the utilization of both GWs and devices must be kept at minimum. Devices must send their data only when they have data to send, for instance when a sensor captures a change. Also in the transmission, devices must send their data with maximum data rate as it consumes in that way minimum power and air time. More air time, means more utilization of both GW and devices and this can lead to power drawn and also more latency. According to figure[Figure 6.2.1.1] and from the experiments above the minimum air time that can be achieved is by using the Spreading factor 7 with bandwidth of 125Hz.

To continue with, in the downlink the full duplex mode is not supported and therefore the GW can be either be in a transmitting or receiving mode. Therefore, if there is a lot of downlink info then devices will remain idle until the end of the GW transmission. Subsequently, it’s recommended to send only small amount of downlink data and infrequently in order to avoid those situations. Further, the things network have frame counter in uplink and in downlink in order avoid the replay attacks. During the activation procedure the frame counter are initialized to 0 and every time the device transmits a packet the frame up counter is increased by one. On the other hand when network sends info the downlink frame increases. If they don’t receive packet that has lower frame counter that the last one this message is dropped. This service will cause problems in the ABP procedure so it recommended using the OTTA procedure which is more securable since the permission is given every time the device losses connection.



Mode	Bitrate (bits/sec)	Max payload size (bytes)
SF7/125kHz	5470	222
SF8/125kHz	3125	222
SF9/125kHz	1760	115
SF10/125kHz	980	51
SF11/125kHz	440	51
SF12/125kHz	250	51
SF7/250kHz	11000	222

Figure 6.2.1.1 Bitrate of LoraWan

The experiments that were established are capable of showing the overall performance of both NB-IoT and Lora technology. Although, many aspects were not monitored due to limited time and lack of the necessary equipment including the real power consumption, the downlink time in each technology, class C in Lora, security vulnerabilities and also any possible interference between multiple devices considering the Lora technology. Therefore, by studying these aspects will help to understand completely these technologies and use them appropriately. To continue with, the NB-IoT technology can be compared with LTE-M which is another ideal IoT solution that uses the license spectrum in order to decide the best one to use in applications.

The best practices considering the Lora technology that were described above can help building an efficient application and serve probably the IOT interconnectivity. Lora devices were not tested in normal temperatures so it’s essential to investigate their performance in extreme weather conditions. On the other hand, as mentioned in the problems in the experiments of NB-IoT part , devices were tested during the summer time and the board was overheated due to high temperatures. It is possible that Lora devices will also be overheated since Lora uses arduino boards as the NB-IoT. Therefore, appropriate equipment must be invented in order to avoid those situations. An ideal solution is to create a box that will be able to stabilize the temperature and protect the devices from any weather condition. Further, devices need to be powered on in order to exchange data. Devices may be located in hard to reach areas so in order to keep their power on and operate a photovoltaic could be added to the devices.

Bibliography

[1] J. de Carvalho Silva *et al*, "LoRaWAN—A low power WAN protocol for internet of things: A review and opportunities," in *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech),* 2017, .

[2] M. LorIoT, A. Aljer and I. Shahrour, "Analysis of the use of LoRaWan technology in a large-scale smart city demonstrator," in *2017 Sensors Networks Smart and Emerging Technologies (SENSET),* 2017, .

[3] K. Q. Abdelfadeel, V. Cionca and D. Pesch, "Fair adaptive data rate allocation and power control in lorawan," in *2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM),* 2018, .

[4] The things network adaptive data rate.

[5] M. Eldefrawy *et al*, "Formal security analysis of LoRaWAN," *Comput. Networks*, vol. 148, pp. 328-339, 2019. . DOI: 10.1016/j.comnet.2018.11.017.

[6] https://lora-alliance.org/resource-hub/lorawanr-specification-v11

[7] W. Ayoub *et al*, "Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility," *IEEE Commun. Surv. Tutor.*, vol. 21, *(2),* pp. 1561-1581, 2019. . DOI: 10.1109/COMST.2018.2877382.

[8] L. Polak and J. Milos, "Performance analysis of LoRa in the 2.4 GHz ISM band: coexistence issues with Wi-Fi," Telecommunication Systems, pp. 1-11, 2020.

[9] U. Raza, P. Kulkarni and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys & Tutorials,* vol. 19, *(2),* pp. 855-873, 2017.

[11] K. C. Wiklundh, "Understanding the IoT technology LoRa and its interference vulnerability," in 2019 International Symposium on Electromagnetic Compatibility-EMC EUROPE, 2019, .

[12] K. Mekki *et al*, "Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT," in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops),* 2018,

[13]Cellular System Support for Ultra-Low Complexity and Low Throughput
Cellular Internet of Things, document 3GPP TR 45.820, 2015.

[14] S. S. Basu *et al*, "Experimental performance evaluation of NB-IoT," in *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob),* 2019, .

[16] S. Khare and M. Totaro, "Internet of things: An overview," in *International Conference on Soft Computing and Signal Processing,* 2019.

[17] R. Ratasuk *et al*, "Analysis of NB-IoT deployment in LTE guard-band," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring),* 2017, .

[18] A. Carlsson *et al*, "Measuring a LoRa network: Performance, possibilities and limitations," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*Anonymous 2018, .

[19] E. Perahia and M. X. Gong, "Gigabit wireless LANs: an overview of IEEE 802.11 ac and 802.11 ad," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 15, *(3)*, pp. 23-33, 2011.

[20] W. Primer, "Overview of the 802.11 Physical Layer and Transmitter Measurements," *Beaverton: Tektronix Inc,* pp. 4-7, 2013.

[21] M. Chen *et al*, "Narrow band internet of things," *IEEE Access*, vol. 5, pp. 20557-20577, 2017.

[22] F. Adelantado *et al*, "Understanding the limits of LoRaWAN," *IEEE Communications Magazine*, vol. 55, *(9)*, pp. 34-40, 2017.