Tampere University

Imran Khan

SUITABILITY OF LORA, SIGFOX AND NB-IOT FOR DIFFERENT INTERNET-OF-THINGS APPLICATIONS

Faculty of Information Technology and Communication Sciences
Master's Thesis
October 2019

ABSTRACT

Imran Khan: Suitability of LoRa, Sigfox and NB-IoT for Different Internet-of-Things Applications
Master's Thesis
Tampere University
Master's Degree Programme in Information Technology
October 2019

The large-scale implementation of the internet of things (IoT) technologies is becoming a reality. IoT technologies benefit from low-power wide area network (LPWAN) systems. These technologies include Long Range (LoRa), Sigfox, and Narrowband IoT (NB-IoT). Numerous networks have already been deployed around the world, which is expected to accelerate the growth of IoT.

This thesis discusses the performance of these three prominent LPWAN technologies in the market that have been specifically designed for IoT use. The main idea of LPWAN technologies is to provide wide coverage area using only small amount of base stations and to serve large amount of low-power and low-cost IoT devices.

The main purpose of this thesis work is to compare LoRa, Sigfox, and NB-IoT and evaluate their suitability to various IoT applications. The appropriate technology selection is possible through in-depth analysis and technological comparison of LPWAN systems. There are many technological differences among these LPWAN technologies. A single technology may not be able to meet all requirements of all IoT applications. Therefore, some IoT applications can benefit from one technology more than others. The right selection helps in fulfilling the need of IoT application to save cost, time and improve efficiency.

In addition to the literature-based suitability evaluation of the aforementioned technologies some practical measurements are performed using commercial off-the-shelf hardware. These measurements consider LoRa and Sigfox user devices in both outdoor and indoor locations. The key performance indicators obtained from the measurements are signal-to-noise ratio (SNR) and received signal strength indicator (RSSI). In addition, also penetration loss from outdoor to indoor is derived. The obtained measurement results were in line with the ones found from the literature.

Keywords: Low-Power Wide Area Network, LoRa, Sigfox, IoT, NB-IoT.

The originality of this thesis has been checked using the Turnitin Originality Check service.

PREFACE

This thesis is supervised by Markus Allén for completion of my Master of Science degree program in Information Technology, Communication Systems and Networks in Faculty of Information Technology and Communication Sciences at Tampere University, Hervanta Campus.

I am grateful to my Supervisor Markus Allén for supporting me throughout the thesis, through valuable comments, and explanations to my work. I have learned different research methodologies and scientific writing. I also appreciate his patience and time spent in helping me.

I am also thankful to my Co-supervisor Joonas Säe for his guidance and encouragement in enriching my knowledge.

Further, I would like to admire my friends, entire faculty members who all have been so helpful and supportive in my master's study period and have contributed their part to my learning.

Finally, I thank my family for their cooperation and sacrifices during my stay at Tampere University.

Tampere, 17 October 2019

Imran Khan

CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

2G	Second generation
3G	Third generation
3GPP	Third generation partnership project
4G	Fourth generation
ABP	Activation by personalisation
AES	Advance encryption standard
API	Application programming interface
BPSK	Binary phase-shift keying
BS	Base station
CF	Carrier frequency
CIoT	Cellular internet of things
CR	Coding rate
CRC	Cyclic redundancy check
CSS	Chirp spread spectrum
DBPSK	Differential binary phase-shift keying
DL	Downlink
eDRX	Expanded discontinued reception
EPS	Evolved packet system
ETSI	European Telecommunications Standards Institute
FCS	Frame check sequence
FDMA	Frequency-division multiple access
FEC	Forward error correction
FSK	Frequency shift keying
GFSK	Gaussian frequency-shift keying
GPRS	General packet radio services
IoT	Internet of things
ISM	Industrial, scientific and medical radio bands
Kbps	Kilobit per second
LPWAN	Low-power wide-area networks
LTE Cat-M1	Long term evolution (LTE), category M1
M2M	Machine-to-machine
MCL	Maximum coupling loss
MIC	Message integrity code
MME	Mobility management entity
MTC	Machine type communication
NB-IoT	Narrowband IoT
OFDMA	Orthogonal frequency-division multiple access
OSI	Open systems interconnection
PRB	Physical resource block
PRS	Positioning reference signal
PSM	Power saving mode
QoS	Quality of service
QPSK	Quadrature phase shift keying
R13	Release 13
R14	Release 14
RSSI	Received signal strength indicator
SF	Spreading factor
SNR	Signal to noise ratio
SRS	Sounding reference signal
TP	Transmission power
UL	Uplink

UNB	Ultra narrowband modulation
VPN	Virtual private network

1 INTRODUCTION

1.1 Background

Internet of things (IoT) is the concept where multiple devices are interconnected to collect and exchange data. Human life is more secure, comfortable by the merger of internet and things through its numerous applications in daily life. IoT enables the connectivity at anytime, anywhere and to anything [1]. Devices can be remotely monitored through the utilization of cloud services. Coverage and data rate comparison among wireless technologies is shown in Figure 1.

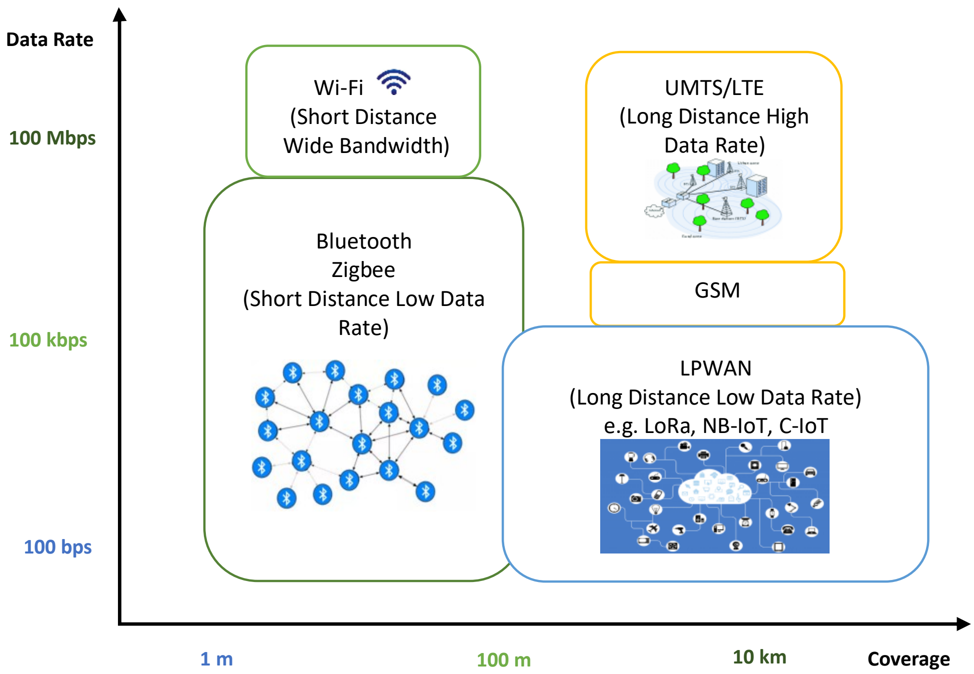

Figure 1. *Coverage and data rate comparison among wireless technologies. Adapted from [6].*

Number of IoT devices are exponentially growing, by 2020 roughly 212 billion smart objects will be deployed in the market [1]. Low-power wide-area networks (LPWAN) will bring revolution in this technology. Wi-Fi, ZigBee and Bluetooth are shortrange wireless systems. LPWAN offers long range and low-power consumption for varies IoT applications. Therefore, characteristics like low-cost operation, better power efficiency LPWAN are the key enablers for IoT solutions. LPWAN consist of various low-power wide-area technologies including LoRa, Narrowband IoT (NB-IoT), Sigfox, LTE Cat-M1, Ingenu, Telensa, Qowisio, DASH7 etc [2].

1.2 Problem statement

Today, there are numerous technologies that involve artificial intelligence and technologies that aid in automation of systems. The invention of IoT technology seamlessly combines the operations of various machines and activities into a single entity through which they can be controlled. Variables such as temperature, humidity, gas level, geolocation and power levels are some of the most important parameters used in the control and maintenance of a system. Sensors and other modules are connected to these systems to detect these parameters and later perform the required action and sends a message through a network to a specific location. Therefore, wireless communications form a very important aspect of the implementation of the IoT technologies. Most of these applications require recurring communication with the servers to maintain the right conditions or undertake the required operations. To achieve this, there is need to implement the low-power wide-area (LPWA) technologies to help in the minimization of power consumption in the modules since they use batteries. The thesis considers three common technologies namely LoRa, Sigfox, and NB-IoT to evaluate their suitability in terms of IoT applications. The suitability decision of LPWAN for application is made by studying major differences in these technologies for example in terms of data rates, coverage, quality of service (QoS).

Choosing the right technology for the application in IoT is a great challenge since there are many aspects which should be considered in each technology. Hence, in this thesis firstly a detailed study is conducted on LoRa, Sigfox, and NB-IoT. Then a comparison is done to find the major differences in these LPWAN technologies. From comparison, it is possible to evaluate the suitable technology for different IoT applications. The suitability evaluation is performed using different IoT use cases to explain how to select the best LPWAN technology.

Finally, the practical validity check is done using LoRa, and Sigfox. The received signal strength indicator (RSSI) and signal-to-noise ratio (SNR) values of both technologies are measured in indoor and outdoor locations to test performance of LoRa and Sigfox network. The base station positions of LoRa and Sigfox were different in these measurements which may have impact on network performance.

1.3 Thesis structure

The thesis content is divided into five chapters. First chapter introduces the IoT technology and a background of the LPWAN. The chapter also describes the different types of technologies used and the purpose of the study. In addition, the problem statement and the approach are clearly described, and related studies undertaken previously.

The second chapter gives theoretical review of the study by describing the most essential characteristics and features of LoRa, Sigfox, and NB-IoT technologies. The network architecture, operation, and design of these technologies is also described thoroughly in this chapter.

The third chapter gives an in-depth comparison of the three technologies in different aspects including cost, energy efficiency, frequency bands, capacity, mobility, regulations, and coverage. Based on this theoretical comparison, advantages and disadvantages of all three technologies are clearly explained.

After the theoretical comparison is done, chapter four gives the locations where the modules are placed and the measurement procedures of the SNR and RSSI. The chapter gives a map of the university of the different locations where the testing is carried out. The results are also given, and the graphs extracted are discussed accordingly.

The fifth chapter gives a conclusion of the experiments undertaken. It explains the suitability of the technologies chosen for the use in IoT and their effectiveness. The chapter also gives explanations of the importance of these findings in the study and implementation.

2 OVERVIEW OF LOW-POWER WIDE-AREA NETWORK TECHNOLOGIES

2.1 Introduction to low-power wide-area networks

A LPWAN is a wireless technology which interconnects devices that are powered by battery, having low data rates usage and supports several devices connected to over a large area. Several companies aim is to minimize cost and enable remote monitoring. Hence, LPWAN serve the best since they operate at lower cost compared to the traditional mobile networks. LPWAN is one of enablers of internet of things it offers wide area coverage for several IoT applications. Devices are interconnected to a central access point enabling efficient data collection and exchange [2]. LPWAN consists of multiple technologies but this thesis mostly focuses on LoRa, NB-IoT and Sigfox.

The LPWAN networks use licensed or unlicensed, proprietary or non-proprietary frequencies. LoRa is developed by LoRa alliance innovated by Semtech. LoRa is a frequency modulated chirp that operates within the unlicensed bands. LoRa has some restrictions on duty cycle, it normally fits non-real time applications to tolerate delays. LoRa is a physical layer and LoRaWAN is the data link media access control (MAC) address protocol for a high capacity [3].

NB-IoT is wireless network technology it enables a wide range of cellular devices. The NB-IoT emphasis mainly on indoor coverage with affordable cost and long-life time of battery [6]. It was introduced by third generation partnership project (3GPP) to allow thousands of devices in the world of IoT. The NB-IoT was completed in 2017, it is particularly designed to have better coverage and lower cost than any other cellular IoT technologies. It supports machine type communication and limits the bandwidth to a single narrow-band of 200 kHz [4].

Sigfox in collaboration with other network providers provides global wireless network. It enables low-power wide-area network solution in this evolving world of IoT. Sigfox follows a similar approach with mobile network providers but different in how they provide the service to the devices [2].

In terms of power consumption where Sigfox is characterized with low power consumption and minimal cost. Another advantage of Sigfox technology is being resilient to interference and noise. Sigfox utilizes bandwidth efficiently and experiences very low noise levels, hence high receiver sensitivity, low-power consumption and inexpensive antenna design is achieved. All these benefits come at an expense of maximum throughput of only 600 bps [2] [13]. LoRa and Sigfox utilizes unlicensed frequency band while LTE CAT-M1 and NB-IoT operate in licensed bands.

There are also other LPWAN technologies exist. LTE CAT-M1 is very cost effective and efficient for applications such as security control, asset tracking and meter tracking having 1.4 MHz spectrum with average upload speeds between 200 kpbs and 400 kpbs. This technology has extended battery life up to 10 years [5]. Ingenu is proprietary LPWAN technology, which works differently than other technologies, it does not depend on better propagation properties of Sub-GHz band. Ingenu operates in 2.4 GHz industrial, scientific and medical radio bands (ISM) band and allows relaxation on the spectrum use in different regions. For example, the regulations in United states and Europe there is no restriction on duty cycle for 2.4 GHz band, resulting higher throughput and more capacity than other technologies. Coverage may reach up to 15 km in urban areas [2]. Many LPWAN applications are supported by Telensa, as it provides end to end solution along with third party software. To have a wireless connectivity between end-devices to base station it uses proprietary ultra-narrowband modulation (UNB). This technology focuses on smart city applications such as intelligent lighting, smart parking, etc [2]. QOWISIO utilize dual-mode LPWA networks incorporating their own proprietary UNB technology with LoRa. It gives LPWA connectivity to the end users [2]. In DASH7 sensors and actuators operate in the unlicensed bandwidth of 433 MHz, 868 MHz, and 915 MHz. DASH7 has coverage range up to 2 km and payload length is 256 Bytes. It has low latency, mobility support, 128-bit advance encryption standard (AES), and data rate up to 167 kbps [7].

The common thing about all technologies is that they all afford at least long battery lifetime. Through theoretical comparison of different technologies, it is possible to determine the most efficient LPWAN technologies. Some of the aspects considered are cost effectiveness, security, bandwidth, power consumption, coverage, sustainability for real time applications, data rates and quality of services.

2.2 LoRa

2.2.1 Introduction

The name LoRaWAN Stands for Long Range Wide Area Network first release came in 2015 by LoRa Alliance as a wireless standard.

LoRa and LoRaWAN are not interchangeable and there is the difference between them. LoRa describe the modulation in physical layer and LoRaWAN is MAC protocol which supports low power, long range and high capacity in LPWA network. Generally, system architecture and communication standard determine the technical performance of the technology, like energy efficiency to save battery charge, network capacity and data rates for various applications. The physical layer and MAC layer are shown in Figure 2.

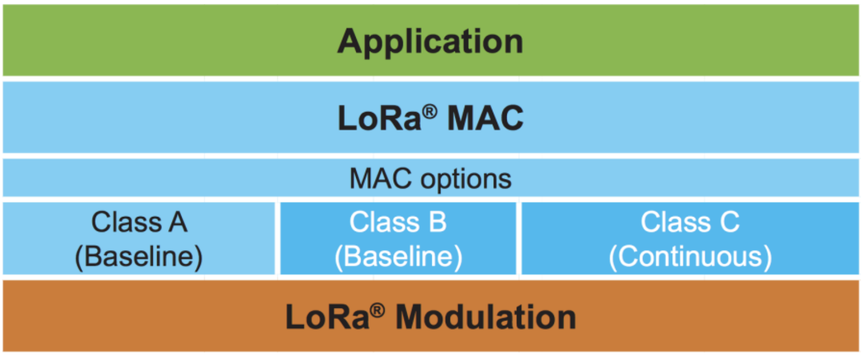

Figure 2. *LoRaWAN layers [17].*

2.2.2 Technology specifications

LoRaWAN is network protocol build for wireless communication that connects battery operated devices to internet in large networks. This protocol supports low-cost, mobile, and secure communication for IoT and machine-to-machine (M2M) applications. Lora Protocol key features such as data rate, capacity, modulation scheme, and battery life-time etc are shown in Table 1.

Table 1. *LoRa specifications [7].*

Characteristics	**LoRaWAN**
Topology	Star on Star
Modulation	SS Chirp
Data rate	290 bps - 50 kbps
Link Budget	154 dB
Battery lifetime	8 - 10 years
Power Efficiency	Very High
Range	2 - 5 km urban, 15 km suburban, 45 km rural
Interference Immunity	Very High
Mobility	Yes
Security	Yes (32 bits)

Frequency bands

LoRaWAN has different unlicensed frequency bands in US and Europe. It operates in ISM radio frequency bands of around 915 MHz, 868 MHz, and 433 MHz in US, Europe and Asia respectively [34]. Unlicensed radio frequency band mean that one can use it without paying anything but there is a limitation in networks of unlicensed sub-GHz bands. In case of LoRa network, duty cycle is described as a maximum amount of time an end-device can hold a channel and it is set by regional authorities. For example, in Europe the frequency band is 868 MHz with 1% duty cycle limitation, it means devices need to wait 100-times from duration of the last transmission before transmitting again in same channel [8]. LoRa operates in unlicensed bands therefore a limit is implemented on duty cycle.

Coverage

LoRa use chirp spread spectrum (CSS) modulation technique. LoRa modulation scheme has key features such as strong robustness against interference and losses compare to other modulation schemes in wireless systems for example frequency shift keying (FSK) [9].

A research conducted in North Jutland, Denmark where different kinds of technologies were tested in different areas. This research is based on simulation results, where they used Telenor's actual base station locations [11]. Base stations were equipped with omnidirectional antennas with maximum transmitted power which in case of LoRa is 14 dBm. Environment conditions are highly dependent on modeling the channel which impact signal propagation. The used propagation model was 3GPP macro non-line-of-sight model. From results, it shows that LoRa provides outdoor coverage better than 99%. In indoor environment, LoRa covered more than 95% users with 20 dB penetration loss [11].

Another research describes LoRa indoor coverage in flower industry, where trolleys had to move across auction area on floor. Availability of public LoRaWAN network to the trolleys in case when they move outside of auction area made it possible for them to still communicate to server without even changing technology. From the measurements it is evident that one LoRa gateway can provide coverage of around 34000 m^2, by only utilizing spreading factor (SF) 7. In SF 12, which is the maximum value in LoRa, the coverage will be larger, that is the reason the area outside the industry can be covered. Trolleys in this scenario are end-devices which get served by the gateway that is enough for up to 6000 end-devices [20].

End-device classes and power consumption

In LoRaWAN we experience battery life of up to 10 years. For better power efficiency the LoRaWAN introduce three types of end-devices which differ in downlink transmission schedule to have more power saving, though at the cost of latency. LoRaWAN has three end-device classes for different needs of wide range of applications:

Class-A by default is supported in all LoRaWAN end-devices. Communication starts at end-device that is asynchronous for example operations are controlled rather than regular intervals. Uplink transmission can happen anytime which is followed by two short downlink windows. Thus, bidirectional communication occurs. This class has lowest power consumption because there is no strict requirement for wakeups in end-devices, so end-devices enter in low-power sleep mode to save power. Downlink communications should always follow uplink communication depending on schedule described by the end-device, network server must buffer downlink transmission till next uplink event [12]. Class-A End-devices transmission is shown in Figure 3.

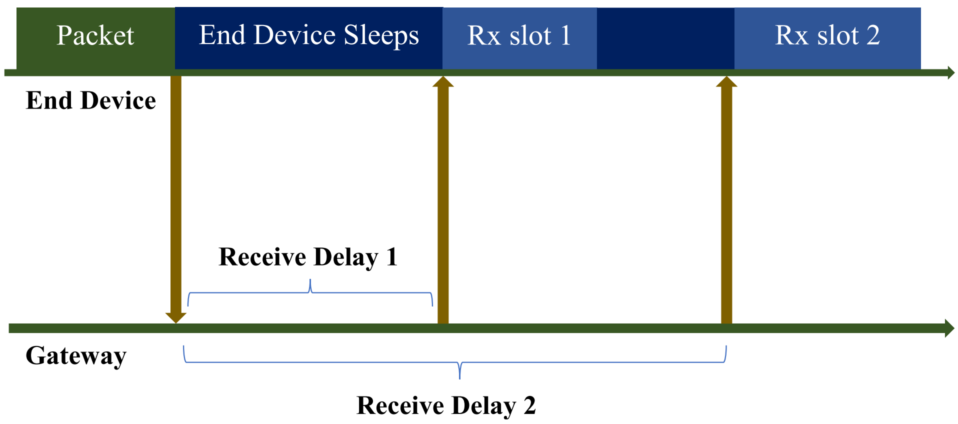

Figure 3. *Class-A type device transmission. Adapted from [4].*

Class-B also has received windows like in class-A with extra scheduled downlink 'ping slot' which is synchronised with the network by periodic beacons. Therefore, network can send downlink transmission with deterministic latency [12]. Class-B end-devices transmission is shown in Figure 4.

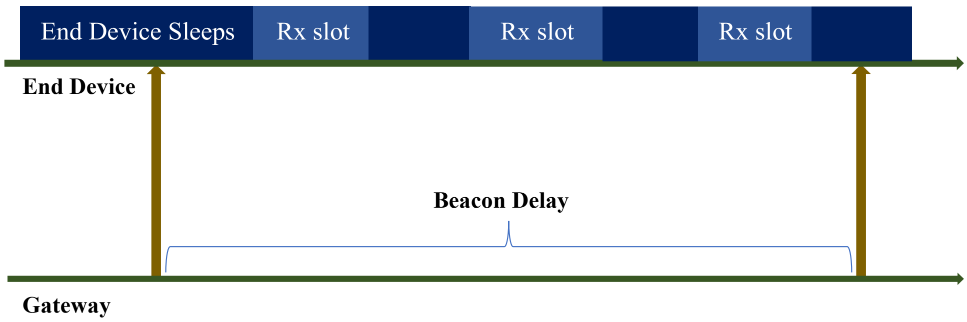

Figure 4. Class-B type device transmission. Adapted from [4].

In class-C end-device receiver remains constantly open at all the time; this reduces downlink latency because downlink transmission can start at any time by network server that utilize more power. So, this class-C is suitable for applications where either more downlink transmission is needed, or power availability is continuous [12]. Figure 5 illustrates working of class-C.

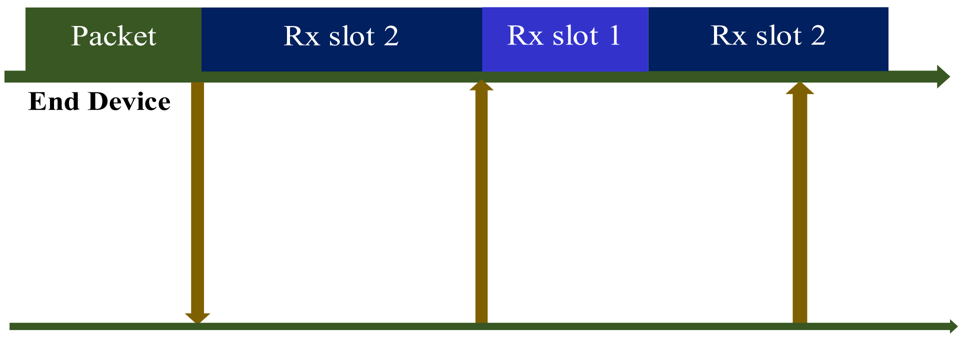

Figure 5. Class-C type device transmission. Adapted from [4].

All three classes offer bi-directional transmission, in class-A end-devices, acknowledgements are supposed to be sent in first or second reception slot. By default, class-A is available on all end-devices. Functionality of these devices affect battery lifetime. End-devices will only wakeup at predetermined timeslots when they have data to send, which saves energy as opposed to frequent need for synchronization in cellular networks. By studying all Classes, we can conclude that LoRaWAN allows few options that may adjust in different applications. But it gives trade-off between power consumption and latency where system has low latency in cost of more power consumption and vice versa.

LoRa transmission parameters

A LoRa device can get configured with different transmission power (TP), SF, bandwidth (BW), carrier frequency (CF) and coding rate (CR) to obtain better energy consumption and link performance [21].

In LoRa TP radio channel range from −4 dBm to 20 dBm, but there are some hardware limitations that is why this range often found between 2 dBm to 20 dBm. Any power levels above 17 dBm can only be used with 1% duty cycle [21].

CF is programmed between 137 MHz to 1020 MHz. It depends on specific LoRa chip and can be limited from 860 MHz to 1020 MHz [21].

SF is defined by the ratio between symbol rate and chip rate. As higher SF increases the SNR, therefore coverage is larger along with more airtime of the packet. The amount of chips in symbol is calculated by 2*SF. 128 chips per symbol are used for SF of 7. Each increase in SF value decrease transmission rate by half, thus twice the duration of transmission and power consumption. Different spreading factors make it possible to separate the networks. SF configuration and data rates are shown in following Table 2 [21].

Table 2. *Spreading factor configuration and data rates [15].*

SF Configuration	Bits per second	Payload Size (Bytes)
SF12 / 125 kHz	250	51
SF11 / 125 kHz	440	51
SF10 / 125 kHz	980	51
SF9 / 125 kHz	1760	115
SF8 / 125 kHz	3125	242
SF7 / 125 kHz	5470	242
SF7 / 250 kHz	11000	242

BW is the range of frequencies that a signal occupies. Data rates will be higher if we increase BW that is why in high bandwidth, packet airtime is less with lower sensitivity. In LoRa technology the available BW are 500 kHz, 250 kHz or 125 kHz, depending upon regional limitation only 250 kHz or 125 kHz are being used in Europe [21].

CR is the forward error correction (FEC) rate in LoRa modem which gives robustness against interference and can be configured using either 4/5, 4/6, 4/7 or 4/8. Higher CR will increase airtime. Radio with different CR but same CF, SF, and BW are still able to communicate among each other because of explicit header [21].

Adaptive data rate

Communication from end-devices to gateways is carried out on different frequency channels and data rates. The purpose of using adaptive data rate is to enhance battery life and network capacity. LoRa network manages data rate which range from 0.29 kbps to 50 kbps and radio frequency output for each device.

End-devices may choose any channel for transmission at any time, using available data rates. End-device take channel in a pseudo-random fashion which is a defined mathematical procedure for every transmission. Frequency variation in system causes robustness against interference. End-devices also value the duty cycle restrictions by local authorities, relative to sub-band [14].

LoRaWAN message format

LoRaWAN message format is shown in Figure 6. DevAddr represents short address of device. Multiplexing port field is denoted by Fport. The value zero shows that payload has only MAC commands. In this case FOptsLen field should be zero. FCnt shows a frame counter. MIC represents cryptographic message integrity code, which is calculated over the fields MHDR, FHDR, FPort and the encrypted FRMPayload. MType is used for message type that recognizes uplink or downlink messages. Major is LoRaWAN version. ADR and ADRAckReq manages the data rate adaptation by the network server. Last received frame is acknowledged by ACK. FPending specify that the network server has more data to transfer and that the end-device must send another frame to keep receive windows open. FOptsLen denotes the length of FOpts field in bytes. FOpts is for piggyback MAC commands in data message. CID identifies the MAC command, and Args are optional for command. FRMPayload is for the payload, that is encrypted using AES key of 128 bits. The minimum and maximum size of MAC header is 13 bytes and 28 bytes respectively.

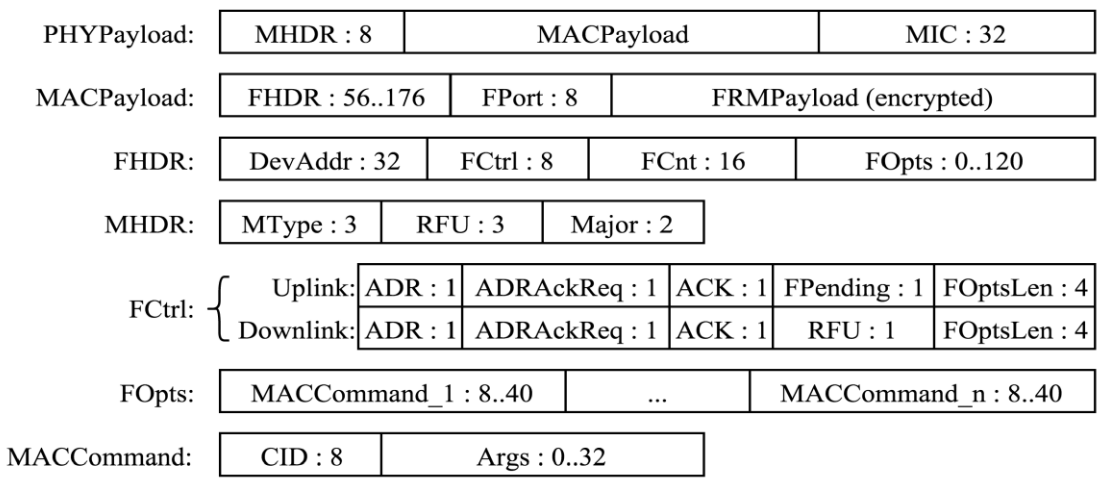

Figure 6. *LoRaWAN message format [19].*

Physical frame format

LoRa physical frame is identified by transmitter and receivers. The BW and SF remain constant for physical frame, that starts by a preamble having constant upchirps sequence extend over entire frequency band where last two upchirps encode the sync word which is one-byte value used to differentiate LoRa networks having same frequency bands.

Optional header is followed by preamble. If the optional header is present, it is transmitted with code rate of 4/8. The optional header contains the size of payload in bytes, the code rate used for the rest of the transmission and indicator for whether or not the optional Payload CRC is present. CRC in header enable receiver to discard packets containing invalid headers. One Byte is required for payload storage thus, setting the payload size to 255 bytes. As header is optional, so it can be disabled in case where it is not required, for example case where payload size, coding rate and CRC presence is known beforehand [19].

After header, Payload is sent, finally at last, frame contains optional CRC. The format can be seen in Figure 7.

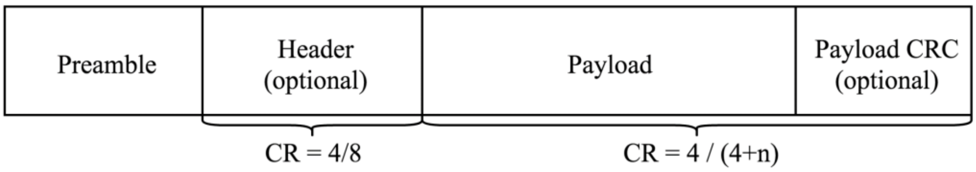

Figure 7. *LoRa frame format [19].*

2.2.3 Network architecture

LoRa is based on star network architecture. Star based architecture helps in maintaining higher battery lifetime as there is no extra data transferred among devices. Many networks have deployed mesh network architecture. In this type of network devices transfer data to other devices to achieve longer communication range [10]. The main drawback of mesh network architecture is it reduces battery lifetime and adds more complexity. Devices in mesh network receive and forward information which is not relevant to them.

In LoRaWAN star network end devices are not connected to a specific gateway. Data which is transmitted by end devices is received by multiple gateways. Each gateway after receiving packet from end device transfer it to cloud based network server. The backhaul between gateways and network server could be either cellular, Ethernet, satellite, or Wi-Fi. The main operations are carried out by network server to manage complexity and intelligence. Network server filters redundant received packets, implements security policies, and perform adaptive data rate etc. Complexity is taken out from end device to save battery power [10].

If end device is moving, there is no handover needed from gateway to gateway. This feature enables LoRaWAN for asset tracking applications in IoT. LoRa network architecture is shown in Figure 8.

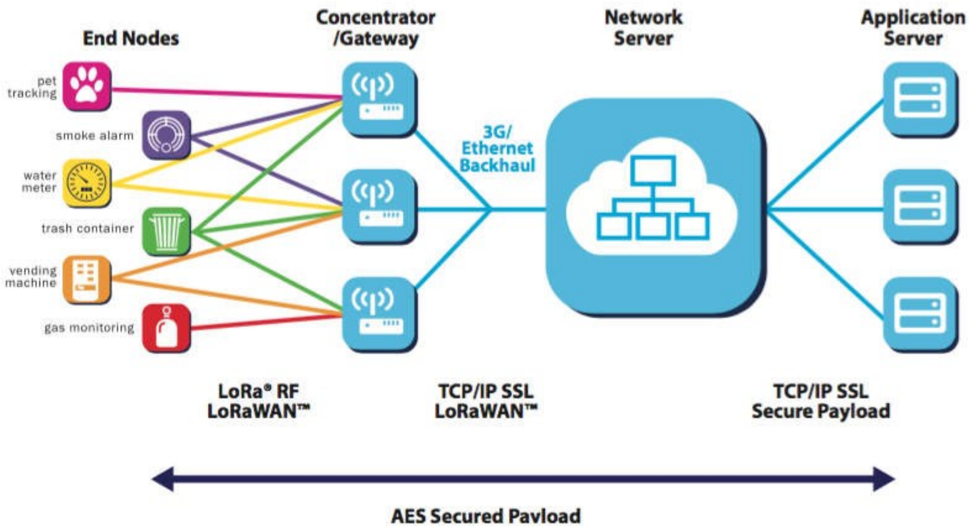

***Figure 8**. LoRaWAN network architecture [18].*

2.2.4 Security

Security is the main concern in IoT deployment. There are two cryptographic layers implemented in LoRaWAN specifications.

- A unique 128-bit network session key is used for communication between end-device and network server to ensure messages validity [16].
- A unique 128-bit application session key is responsible for encryption and decryption of the payload. The payload is encrypted between devices and application server.

Authentication and integrity of packets is provided to the network server through AES algorithms. Application server is provided with end-to-end encryption by AES algorithms. By implementing these two levels of security, shared networks can be implemented. Network operator will not have visibility of user’s payload data [12].

LoRaWAN security is implemented keeping in view LoRaWAN design standard: low power consumption, low complexity, low cost and high scalability. Security must be future proof as devices are deployed for longer time period (years) in the field. The key features supported in LoRaWAN security are mutual authentication, integrity and confidentiality. In order to join the network mutual authentication is established between LoRaWAN end-device and the LoRaWAN network. Authentication procedure ensures only legitimate and authorized devices gain access to authentic network. LoRaWAN messaging are origin authenticated, integrity protected and encrypted. This protection ensures network traffic has not been tempered, is coming from original source and is protected from attackers [31].

2.3 Narrowband IoT (NB-IoT)

2.3.1 Introduction

Narrowband internet of things (NB-IoT) is introduced by 3GPP release 13. The main objective of release 13 is to achieve longer coverage, low cost, low power, and to support many number of devices [36].

NB-IoT operates in licensed frequency bands which continue to function smoothly in the network even when data rate or user increases. It provides deep indoor coverage for thousands of low-data-rate applications. NB-IoT bandwidth is 200 kHz.

One of the major advantages of NB-IoT is that, it has support of all major mobile equipment, and manufacturers. It can coexist with existing cellular networks [36]. It also benefits from the security and privacy features of mobile operator, for example confidentiality, authentication, and data integrity [37].

In NB-IoT sensors are directly connected to the base station. Therefore, there is no extra need of gateway to provide connectivity. Hence, it will increase flexibility. Telecommunication providers like Huawei, Ericsson, and Vodafone introduce this NB-IoT standard in conjunction with 3GPP. NB-IoT has number of benefits that is why these telecom providers are interested in this technology [22] [38].

2.3.2 Technology specifications

NB-IoT technology specifications including bandwidth, data rate, battery life, TP, latency, cost, modulation and frequency are listed in Table 3 below.

Table 3. NB-IoT specifications.

Characteristics	NB-IoT
Bandwidth	200 kHz
Data Rate	250 kbps
Battery life	10 years
Transmitted power	23 or 20 dBm
Power saving	PSM, eDRX
Duplex	Half Duplex
Latency	1.6s – 10s
Cost	Low cost
Modulation	QPSK, BPSK
Frequency	Subset of LTE bands, standalone on GSM bands.

Power saving technologies

Power saving mode (PSM) and expanded discontinuous reception (eDRX) are two types of power saving technologies used in NB-IoT Release-12 and Release-13 respectively. PSM is based on the principle where terminal stays online but remains unreachable by signaling. Terminal stays mostly in deep sleep mode which achieves power saving. While in eDRX power saving technology which also achieves a lot of power saving by extending sleep cycle of terminal. Sleep cycles causes unnecessary wakeups of receiving cells. eDRX promotes downlink accessibility significantly [6]. Power saving mechanisms are shown in Figure 9.

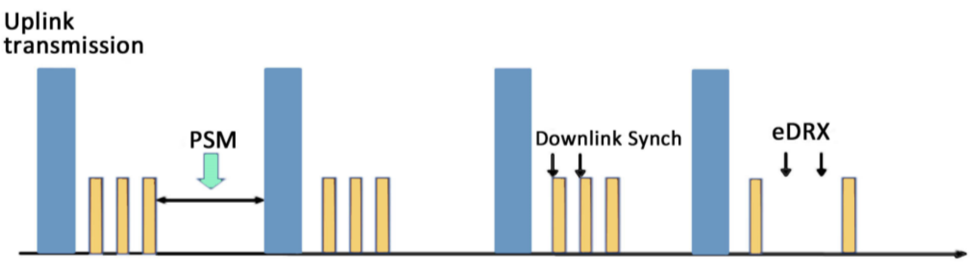

Figure 9. *Power saving technology in NB-IoT. Adapted from [39].*

Typically, in low data rate and low-frequency service battery lifetime of NB-IoT is expected to be 10 years. As per simulation results of 3GPP in TR45.820, in coupling loss of 164 dB with PSM and eDRX a five-watt-hour battery can reach to 12.8 years if terminal sends 200 bytes once a day. Table 4 illustrates battery life in different environments.

Table 4. *Estimated battery service life in years [6]. © 2017 IEEE.*

	Battery life (year)		
Message size / message interval	Coupling loss= 144 dB	Coupling loss = 154 dB	Coupling loss= 164 dB
50 bytes / 2 hrs	22.4	11	2.5
200 bytes / 2 hrs	18.2	5.9	1.5
50 bytes / 1 day	36.0	31.6	17.5
200 bytes / 1 day	34.9	26.2	12.8

NB-IoT deployment modes

NB-IoT currently supports 3 types of deployment modes [6].

1. Stand-alone as a dedicated carrier, which uses independent frequency band.
2. In-band within the occupied bandwidth of a wideband LTE carrier.
3. Guard-band of an existing LTE carrier [6].

The deployment of NB-IoT is restricted to LTE base stations. Therefore, it is not suitable for regions that do not have fourth generation (4G) mobile network coverage [4]. Figure 10 further illustrates NB-IoT deployment modes.

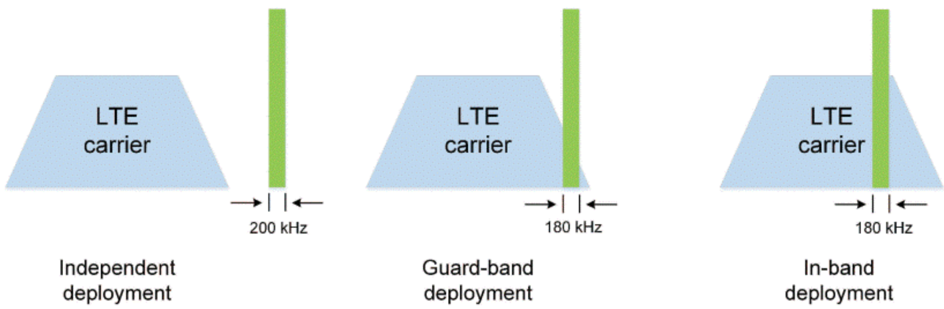

Figure 10. *Deployment modes in NB-IoT [6]. © 2017 IEEE.*

Frame structure

In NB-IoT eNodeB supports E-Utran wireless frame structure both uplink and downlink for sub-carrier spacing of 15 kHz, as shown in Figure 11.

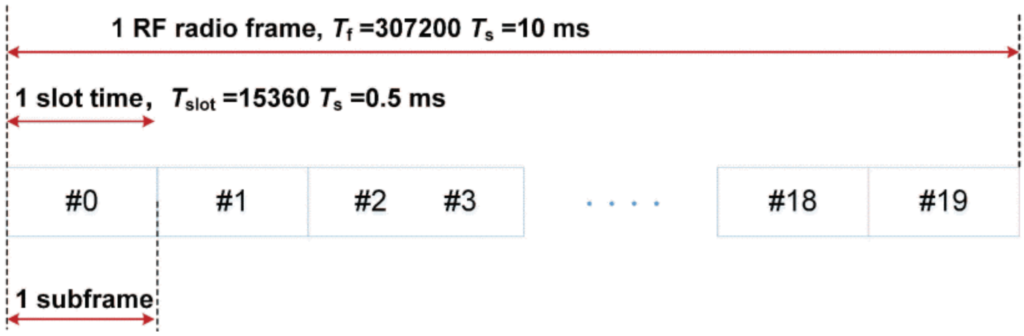

Figure 11. *NB-IoT frame structure for 15 kHz sub-carrier spacing [6]. © 2017 IEEE.*

NB-IoT defines new frame structure for uplink with sub-carrier spacing of 3.75 kHz, as shown in Figure 12.

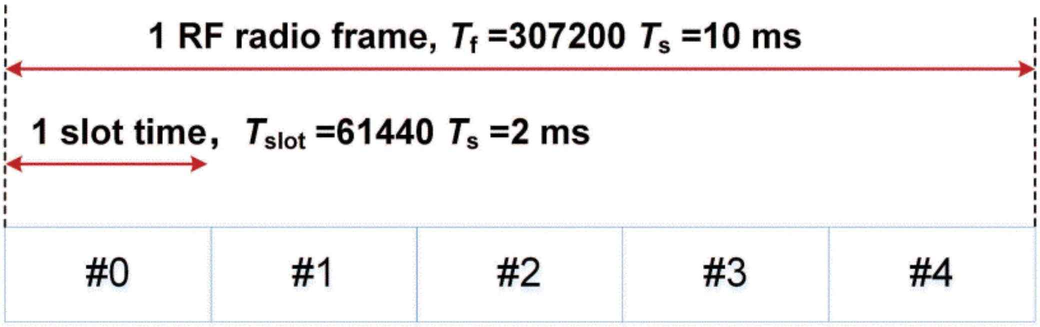

Figure 12. *NB-IoT frame structure for 3.75 kHz sub-carrier spacing [6]. © 2017 IEEE.*

Uplink and downlink transmission mode

The development of NB-IoT depends on LTE. The improvements are mainly made on relevant technologies of LTE according to NB-IoT unique feature. In downlink transmission NB-IoT uses quadrature phase shift keying (QPSK) and orthogonal frequency-division multiple access (OFDMA) technology with sub-carrier spacing of 15 kHz. While in uplink transmission binary phase shift keying (BPSK) or quadrature phase shift keying is being utilized. Single-carrier frequency-division multiple access (SC-FDMA) is also used in uplink transmission including single and multiple subcarrier. A single sub-carrier technology is for sub-carrier spacing 3.75 kHz. The sub-carrier spacing of 15 kHz is adopted for IoT terminal having very low rate and power consumption. Table 5 indicates NB-IoT technical features.

Table 5. *NB-IoT physical layer, adapted from [6]. © 2017 IEEE.*

Physical Layer	Technical Characteristics	
Uplink Transmission	QPSK or BPSK modulation	
	SC-FDMA	Subcarrier interval is 3.75 or 15 kHz, data rate 160 - 200 kbps
	Multi-Carrier	Subcarrier interval 15 kHz data rate 160 - 250 kbps
Downlink Transmission	QPSK Modulation OFDMA subcarrier interval is 15 kHz → data rate 160 - 250 kbps	

NB-IoT Mobility management in Release 13

In 3GPP Release 13 (R13) of NB-IoT, devices cell handover cannot be made in connected state. Cell reselection can be conducted if devices are in idle state. Most of the time the devices are in the idle state to save energy, but also to enable handover as it is not possible in the connected mode [6].

Coverage comparison

A simulation-based research was conducted to study the coverage of general packet radio services (GPRS), NB-IoT, LoRa, and Sigfox. The research is based on realistic scenario where covering area is 7800 km^2 using Telenor's commercial second-generation (2G), third-generation (3G), and 4G deployment [40]. The main aim of this research [40] is to know which technology provides best coverage for IoT devices, located deep indoor.

In this deployment [40] devices are located both in rural and urban areas. Results indicate that NB-IoT has an outage below 1% for locations experiencing 20 dB indoor penetration loss. Similar results were found in Sigfox. LoRa was unable to provide coverage to 2% of those locations. In more deep indoor case, with 30 dB additional penetration loss NB-IoT has the best coverage among all with only 8% outage. While Sigfox and LoRa was unable to cover 13% and 20% locations respectively.

Connection count

Connection count plays a vital role specially in large scale application in IoT. In start of NB-IoT the main aim was to have 50 000 connections per cell [6]. In R13 of NB-IoT after preliminary evaluation, it is found that it can meet this requirement. However, in practice it depends on few factors. One of the main factors is terminal service model in the cell. Therefore, more tests are still required for accuracy.

Release 14 functionalities to be added

In NB-IoT R13 localization is supported through enhanced cell ID at base station with less accuracy. In Release 14 (R14) there is a need of introducing new features to the design to enhance localization accuracy [6].

Release 13 does not support multicast feature in NB-IoT. However, in IoT services base station can send data packets simultaneously to the multiple terminals. R13 can waste system resources and increases message delivery time by not supporting multicast. In R14 multicast functions can be considered to improve the performance.

The R13 of NB-IoT designed is focused on static and low-rate users. Reselection among cells in NB-IoT is only supported in idle state. In new R14 switchover among cells will be supported in connected state [6].

2.3.3 Network architecture

NB-IoT network architecture has 5 main parts:

1. All NB-IoT terminals in any industry can access NB-IoT network by having SIM card installed.
2. NB-IoT base station which is deployed by telecom providers. All three types of deployments (Standalone, Guard-band, and In-band) are supported by base stations.
3. NB-IoT core network connects base station to NB-IoT cloud.
4. NB-IoT cloud platform is responsible for computations and process various services. The results are then sent to business data centre or NB-IoT terminal.
5. NB-IoT business data centre receives the data from cloud to service the data or take control of NB-IoT terminal-IoT network architecture is shown in Figure 13.

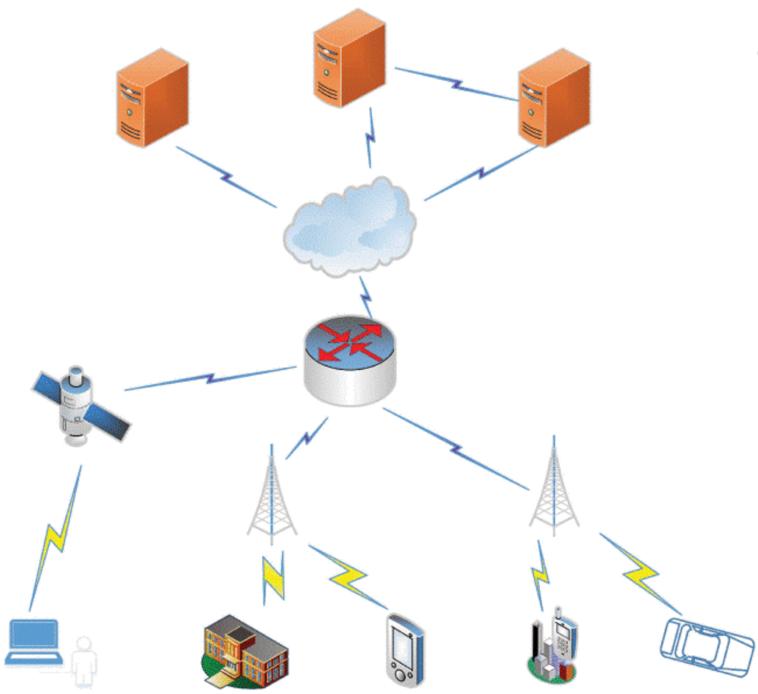

Figure 13. *NB-IoT network architecture [6]. © 2017 IEEE.*

2.3.4 Security

The security of NB-IoT depends on many factors such as IoT hardware, network communication mode, and service requirement [6]. Low power equipment consumes less power and have low computing power. These hardware features make terminal expose to threats from different security issues. The resource consumption can cause denial of service. Additionally, in real deployment scenario the number of low-power consumption terminals devices are in great numbers. Therefore, a tiny security vulnerability causes serious security accidents. The lightweight protocols make it easier for attacker to access sensitive information on system.

The NB-IoT security system is based on 3-layer architecture including perception layer, transmission layer and application layer.

Perception layer

The perception layer of NB-IoT is the bottom layer to provide foundation for upper layer services. The perception layer can be attacked by both passive and active attacks. Passive attacks are the type of attacks where attacker only steals information and not change them. There are multiple methods for attacker, mainly are traffic analysis and eavesdropping. The NB-IoT network is established as wireless network, so there are multiple options for attackers to steal sensitive information [6].

Active attacks cause more harm to system than passive attacks as it includes alteration of information. Active attacks are made by capturing the node and tempering the message. For example, if attacker access NB-IoT terminal and change information such as meter readings that will negatively affect users.

Cryptographic algorithms play their role to prevent active and passive attacks. The algorithms used for protection are data encryption, identity authentication and integrity verifying. The crypto algorithms are frequently used to pre-allocate keys and password mechanism based on identity.

The NB-IoT battery service life is expected to be 10 years. The data rate at NB-IoT terminal is low. The short lightweight password deployed in perception layer to reduce load and increase battery life.

The bidirectional identity authentication process between nodes and base station in the cell is carried out in perception layer of NB-IoT. Base station authenticates the node and it must also be done by NB-IoT node to the base station in the cell. This bidirectional authentication method prevents security threats from false base station or node [6].

Transmission layer

The transmission layer in NB-IoT is simpler. Network deployment does not need gateway to collect information and then send to base station. Therefore, many problems are avoided of multi networking, higher cost and battery power. A single network in a city is easier to manage and install. Security threats are still present in this network too [6].

A single NB-IoT sector supports thousands of terminals. Hence the big challenge is to conduct efficient identity authentication to manage access control for these massive connections. Malicious node false information injection is avoided through identity check mechanism.

Wireless network is more vulnerable to network attacks. Attacker may transmit interference signal to jam the network.

As mentioned earlier there are thousands of nodes in a single cell. The node which is operated by attacker may cause denial of service to the actual nodes.

The importance of authentication is extremely important to make sure only authorized users access network. Attackers are kept away to influence network performance through end-to-end authentication and key agreement mechanism. Thus, it provides authentication and integrity for the protection of data.

There exists a method to detect intrusion and protect network from illegal information from malicious node. One way is to track a normal behaviour of NB-IoT node by profile configuration. If network detects abnormal behaviour in current and previous activities above a certain threshold in nodes. The system will consider current activity as intrusion behaviour. The system is supposed to take necessary timely actions to avoid harmful impact by attackers [6].

Application layer

The application layer is responsible for storing, managing, and processing the data. After transmitting through perception and transmission layers data is collected by application layer. In NB-IoT there may be massive number of nodes who send data to application layer. Therefore, a larger amount of data is collected by application layer [6].

There are various types of NB-IoT applications. Different types of data converged in application layer so, it causes complexity in data processing. The NB-IoT face the challenge to efficiently identify and manage data as per available computing resources. Necessary backups in case of any disaster must be taken into consideration under such situation.

The data usage in application layer may be influenced by security problems like integrity of data. Thus, this security concern must be addressed with efficient data integrity verification and synchronization mechanisms. There are many other technologies for data security during transmission and storage process such as data flow auditing technology etc.

There exist many user groups in NB-IoT. Hence, the need of setting authorities for different levels of users to control information sharing. The data access control mechanism is mandatory.

Applications in NB-IoT have different privacy concerns. On the basis of privacy needs of a particular application different security mechanisms are required for example, discretionary access control mechanism, attribute-based access control mechanism, and role-based access control mechanism [6].

2.4 Sigfox

2.4.1 Introduction

Sigfox technology was created in 2010. The main aim of this technology is to utilize billion of objects to play their role in digitalization and social development of our environment [32]. The objects worldwide connect to the internet; to store their data in cloud. Sigfox focuses on simple low-cost and low-power connectivity. This challenge in Sigfox solve by deploying dedicated network with low bandwidth, which is already being deployed in 45 countries [32].

Sigfox protocols and network enables object to share its data from anywhere in the world [32]. In Sigfox sensors function without the need of batteries. Many sources are being utilized for this purpose including solar, wind and electromagnetic waves. Sigfox technology offers simple approach to lower maintenance cost and enhance user experience. Many use cases will not need batteries to operate [32]. Sigfox uses lightweight protocol to send small messages. This helps in less energy consumption, for longer battery life [29]. In order to send data from device to cloud, Sigfox relies on core connectivity to make communication possible over the internet. Therefore, no SIM cards or complex connections are needed [30].

2.4.2 Technology specifications

Some of the key features of Sigfox are listed in Table 6. These features include Radio signal Modulation, BW, data size, Range, Applications, data rate, BS capacity, Battery life, Topology, Packet size, Messages per day, End node roaming.

Table 6. *Sigfox specifications, adapted from [13] [25].*

Characteristics	Sigfox
Radio signal Modulation	UNB with DBPSK (UL), GFSK (DL)
BW	100 Hz (per message)
Range	Rural (30-50 km), Urban (3-10 km)
Applications	IoT
Data rate	100 bps or 600 bps
Cost structure	Based on number of IoT devices connected.
Devices per access point	1 Million
Topology	Star structure
Payload size	12 bytes uplink, 8 bytes downlink
Messages per day	Up to 140 uplink messages (7 per hour), 4 downlink messages.
Battery lifetime	Long battery life up to 10 years

Radio configurations and modulation techniques

Sigfox operates globally, with radio frequencies ranging from 862 to 928 MHz There are some local regulations and operating constraints for Sigfox technology. Therefore, the network configuration differs from one country to the other [33]. Sigfox operations have been divided into six geographical zones. Each zone has its own set of parameters including frequency range, maximum radiated power, etc. Device hardware implementation is based on these parameters [33].

For messages which are transmitted from the end-devices to the BS (uplink), Sigfox uses DBPSK modulation, while in downlink transmissions (which are less frequent), it utilizes GFSK technique [2].

Payload size

An uplink message contains payload size of up to 12 bytes which takes 2 seconds on average to reach at the BS which checks the spectrum looking for ultra-narrowband signals to demodulate. A Sigfox frame is of 26 bytes with 12-byte data payload. In downlink messages payload size is 8 bytes [13].

Duty cycle & sleep mode

As per European Telecommunications Standards Institute (ETSI) directive for the utilization of the unlicensed frequency band, with 1% duty cycle time. Sigfox in uplink transmission can send 140 messages, where each message length is 12 bytes, as this is limited size per message which does not seem like a lot of data for few IoT use cases, still it fulfils the need and is more than enough for typical IoT cases. For example, asset tracking by transmitting asset's GPS coordinates (size 6 bytes), monitoring the climate changes to send temperature values (2 bytes) and so on [2][13].

On the other hand, only 4 messages of maximum 8 bytes each are allowed in downlink transmission. Hence, relation between uplink and downlink transmission is not symmetric in Sigfox technology, because there cannot be acknowledgement for each uplink message [2]. Devices stay in sleep mode by not using channel 99% of the time end up saving a lot of battery-life as shown in Figure 14.

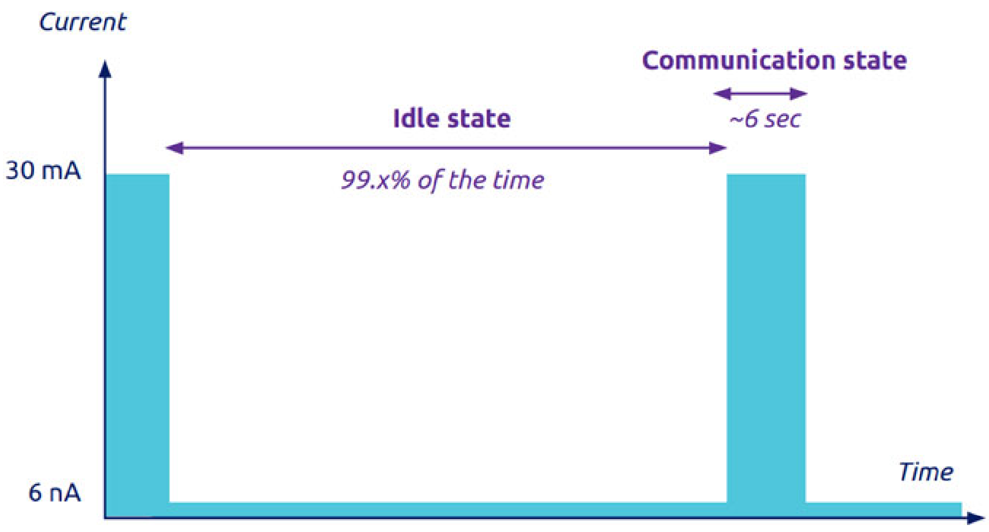

Figure 14. *Sigfox idle state [25].*

Frequency & time diversity

In Sigfox technology, we have seen earlier that number of uplink and downlink messages are not the same that is why there is a lack of acknowledgements for each uplink message causing uncertainty of message delivery. Therefore, Sigfox takes advantage of the idea of frequency and time diversity. The end-device transmits a message 3 times on different time slots and frequencies, this way if one message gets lost during transmission or interrupted due to interference, still more of them are available to make sure it arrives at BS [25]. Sigfox uplink transmission is demonstrated in following Figure 15.

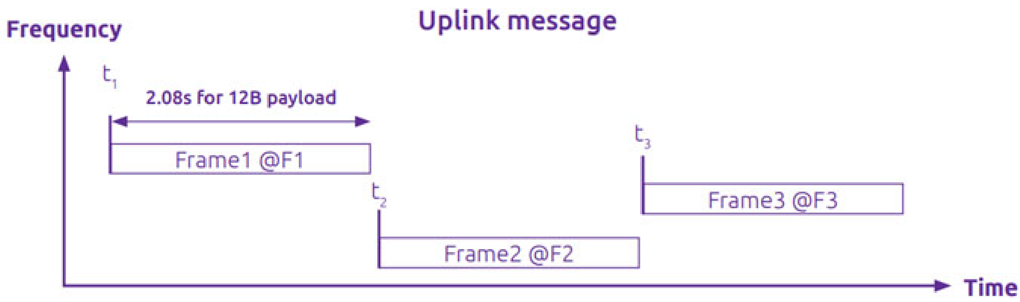

Figure 15. *Sigfox uplink transmission [25].*

Sigfox frame structure

Sigfox has two types of MAC frame structures for uplink and downlink transmission. There are certain features associated with each frame and are listed in below Figure 16. Uplink MAC preamble in UNB modulation scheme contains 4 bytes and synchronization of frame only takes 2 bytes, then end-device identification is done using another 4 bytes, payload size is 0-12 bytes. The authentication field is not fixed as it varies, frame check sequence (FCS) carry 2 bytes. Contrary to uplink MAC frame synchronization where it takes 2 bytes, downlink MAC frame synchronization only takes 13 bits. Flags, FCS and authentication fields are given 2, 8 and 16 bits respectively. But error code and payload lengths are variable [26].

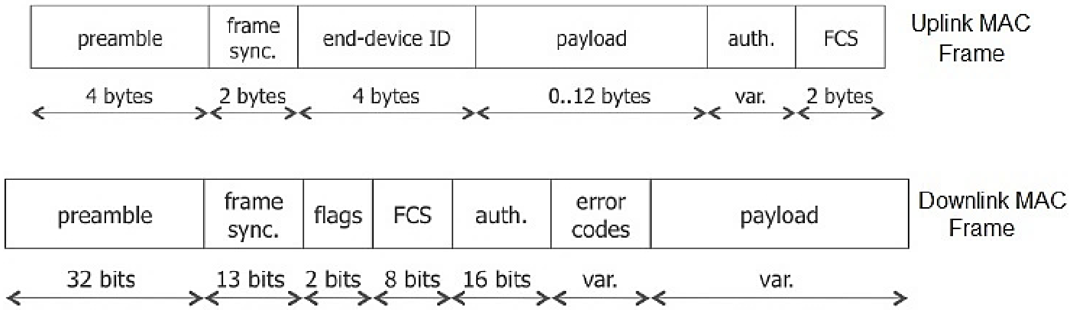

***Figure 16**.* *Sigfox frame structure [26].*

Spatial diversity

In cellular protocols, devices are connected to a set base station. In Sigfox transmitted message is received by all base stations, which are located nearby. This is known as spatial diversity [25]. Example of uplink data transmission in Sigfox network is shown in Figure 17.

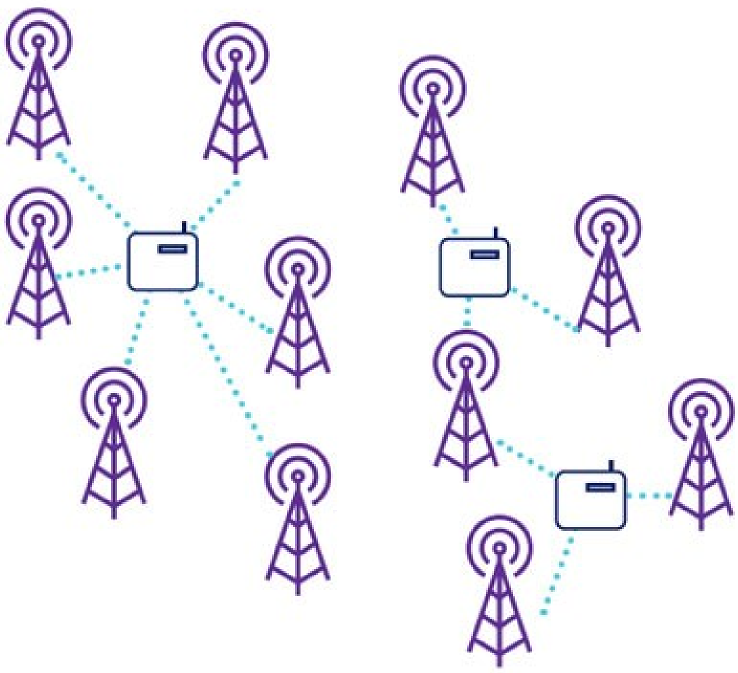

Figure 17. *Sigfox spatial diversity [25].*

2.4.3 Network architecture

The network architecture of Sigfox is presented in Figure 18. The network forms a star topology, where end-devices transmit data to the base stations using a wireless connection. Once the data is received by base stations, then it is resent to Sigfox cloud using existing 3G/4G or ethernet connection by cellular network providers. At this point the data is processed before being sent to customer servers where it gets stored. This means data is managed by Sigfox own cloud server, that remains in constant development [27].

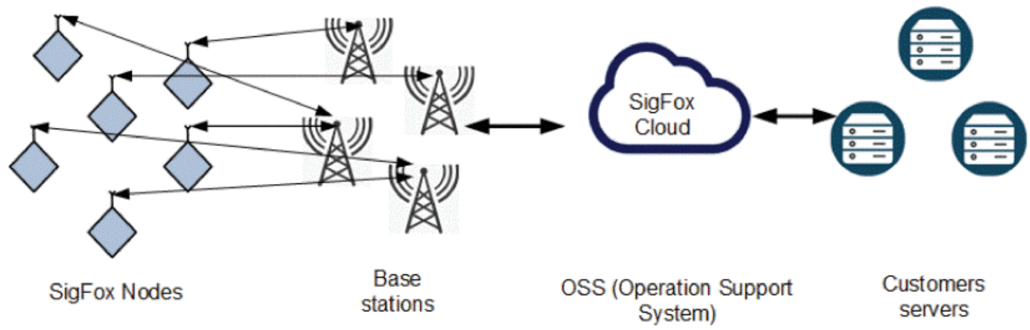

Figure 18. *Sigfox network architecture [27]. © 2019 IEEE.*

2.4.4 Security

Data messages and transmission must be secure to fulfil functionality of the IoT applications. Such as integrity, confidentiality, and authentication for secure communication to avoid hackers and unfortunate scenarios.

Figure 19. *Sigfox security [35].*

In Sigfox security mechanisms are implemented in several layers starting from end-devices up to applications on webserver, as illustrated in Figure 19. To start communication with Sigfox cloud, every message should have individual secret authentication key. End-devices send their encrypted messages to the BS using this secret key and generate a unique signature for each single message. In order to prevent redundancy of the same message, a sequence number is added to the packet to recognize messages. Further, in Sigfox each end-device transmits three messages each in different timeslots and frequencies provides an additional security as choice of receiving BS is not known in advance. Transmission from the BS to Sigfox cloud, this connection is being set-up via secure and encrypted Virtual Private Network (VPN). Moreover, Sigfox cloud gets replicated and managed on private datacentres. Eventually, end users access back end servers (cloud) to exploit data through application programming interface (APIs), via robust application layer HTTP protocol. It is also important to note that Sigfox devices mostly stay in sleep mode, so it is not vulnerable to harmful messages from hackers or eavesdroppers [35].

3 TECHNOLOGY COMPARISON AND SUITABILITY ANALYSIS

3.1 Introduction in terms of IoT factors

There are many elements to consider before choosing the suitable LPWAN among (LoRa, NB-IoT, and Sigfox) technology for a specific IoT application. The most important factors which affects the performance of the application are quality of service, battery lifetime, latency, data rates, scalability, payload length, range, and cost. LoRa, NB-IoT and Sigfox offer different features. One technology may be more suitable than the other depending on the need of an application. In the following section a brief comparison on these technologies on different parameters is explained. Moreover, different IoT applications are discussed to find better LPWAN technology for them.

3.2 Technology comparison

3.2.1 Quality of service

LoRa utilizes unlicensed spectrum and is an asynchronous protocol [4]. LoRa, in relation to chirp spread spectrum modulation, can effectively control intrusion, multipath, and fading however, it cannot provide the same quality of service that NB-IoT can offer. This is because NB-IoT exploits a licensed spectrum and its time–based synchronous protocol is ideal for quality of service. On the other hand, this benefit of quality of service is at the expense of cost [38].

Sigfox and LoRa use unlicensed spectrum together with asynchronous communication conventions [40]. These allow them to be capable of avoiding complications of interference, multipath, and fading. Sigfox and LoRa cannot provide the same quality of service offered by NB-IoT. The NB-IoT technology has a licensed spectrum as well as a long-term evolution-based synchronous convention, which are suitable for quality of service at the expense of cost. Due to quality of service feature, NB-IoT technology is ideal for IoT applications that need guaranteed quality of service. However, the applications that do not require guaranteed quality of service should select LoRa or Sigfox in their real life uses.

3.2.2 Spectrum, deployment, and end-device cost

LoRa and Sigfox use unlicensed spectrum. Hence spectrum cost is free. NB-IoT offers guaranteed quality of service but at the expense of cost. Licensed spectrum in NB-IoT cost over 500 million euro per MHz base station deployment cost of NB-IoT is higher than LoRa and Sigfox. LoRa and Sigfox end-devices cost is lower than NB-IoT [40]. Different costs comparison is shown in Table 7.

Table 7. *Costs comparison [40].*

Technology	Spectrum cost	Deployment cost	End-device cost
Sigfox	Free	>4000€/base station	<2€
LoRa	Free	>100€/gateway, >1000€/base station	3-5€
NB-IoT	>500 M€/MHz	>15000€/base station	>20€

3.2.3 Data rates and bandwidth

LoRaWAN provides maximum data rate up to 50 kbps when using frequency-shift keying (FSK). In LoRa network a single gateway can collect data from thousands of devices located at kilometres away. LoRa is applicable to typical IoT use cases [41]. Sigfox technology offers maximum data rate of 600 bps, where maximum packet payload size is 12 bytes. There is a constraint on number of packets per device in Sigfox which cannot exceed 140 packets/day. These restrictions of Sigfox has made this technology restricted to few use cases, compare to LoRa which is flexible and open. NB-IoT data rate is higher than LoRa and Sigfox. Therefore, application that require higher data rate prefer NB-IoT. Table 8 shows technology comparison.

Table 8. *Technology comparison (LoRa, Sigfox, and NB-IoT).*

Property	NB-IoT	LoRa	Sigfox
Data rate	UL 204.8 kbps, DL 234.7 kbps	290 bps - 50 kbps	100 or 600 bps
Duty cycle	100%	1% (EU)	1% (EU)
Bandwidth	180 kHz Guard-band, 200 kHz Standalone, 180 kHz In-band.	US: 500 kHz, 250 kHz, 125 kHz. EU: 250 kHz, 125 kHz	100 Hz (per message)

3.2.4 Battery life

In LPWAN technologies battery life is also important part as support of large number of connected devices and very long coverage areas compared to conventional technologies. All technologies (LoRa, Sigfox and NB-IoT) consume less energy, as end-devices mostly stay in sleep mode. The time outside of operation is sleep mode. There are different features of these technologies that affect power consumption. NB-IoT consumes more power because of synchronous communication protocol and QoS. Hence NB-IoT extra energy consumption reduces battery lifetime compare to LoRa and Sigfox [40].

3.2.5 Latency

Network latency is a delay which happens in data communication. Latency is one of critical factor to consider in IoT applications. Therefore, it is important to understand which technology offers low latency. There are 3 types of end-device classes in LoRa as we have seen earlier in chapter 2. Class-C of LoRa achieves low bidirectional latency, but in this case energy consumption would be higher. NB-IoT also offers low latency compare to Sigfox. Hence class-C of LoRa and NB-IoT are good technologies for applications that require low latency. On the other hand, Sigfox is suitable for those applications which are less sensitive to latency and require low data rate [40].

3.2.6 Network range

The network range of Sigfox is better than LoRa and NB-IoT. Sigfox cover whole Belgium, country with area of approximately 30 500 km^2 by deploying only seven base stations. One Sigfox base station can cover entire city with range greater than 40 km. LoRa has range less than 20 km and requires three base station to cover a city of Barcelona. In NB-IoT one of the original ideas was to enable better communication capabilities from outdoor networks to indoor locations [40].

3.2.7 Scalability

Scalability feature is supported by LoRa, Sigfox and NB-IoT. These technologies can support thousands of devices. There are many techniques to handle this scalability feature for example efficient use of channel, time and space. NB-IoT scalability is higher than that in LoRa and Sigfox [40]. In NB-IoT cell 100 000 end-devices are supported, while LoRa and Sigfox can have up to 50 000 devices per cell.

3.2.8 Payload length

Sigfox payload length is only 12 bytes, it is the lowest payload size compared to LoRa and NB-IoT. Therefore, IoT application that sends large data size prefer NB-IoT as it allows payload of 1600 bytes. LoRa allows up to 243 bytes of payload to be sent [40].

3.3 Internet of things applications

This following section discusses health monitoring, smart building, retail point of sale terminals, asset tracking, remote monitoring, and smart agriculture applications as the types of IoT application within LPWAN radio communication technology. In addition, then it presents an evaluation of the suitability of three technologies LoRa, Sigfox and NB-IoT for IoT applications on different parameters.

3.3.1 Smart building

LPWAN technologies help in smart buildings within the IoT environment. Technologies of IoT LPWAN, especially Sigfox and LoRa, can be regarded the most crucial currently as a result of its ability to make the smart city possible. Different parameters such as temperature, humidity, security, water flow, along with electric plugs sensors work cooperatively to increase the safety of the technology [23].

The sensors send alerts to property managers that can avoid damages and promptly react to requests without establishing a manual building monitor. The buildings' cleaning and utilization could also be performed more effectively. The building sensors have relatively lower cost and longer battery lifetime compare to NB-IoT, so they do not need quality of service or regular communication. As a result, Sigfox and LoRa are a better fit for this category of IoT applications based on the highlighted parameters.

3.3.2 Retail point of sale terminals

The Internet of Things is transforming several aspects of the retail sector, ranging from customer experience to supply chain management. The possibility of global roaming worldwide, together with other prominent features like very low power consumption, ability to localize, and low cost, makes the LoRa technology system a relatively good option for a global interoperable system for the immense IoT [24]. The sale-point systems require assured quality of service as they carry out regular communications [40]. These systems have uninterrupted electrical power supply, therefore, there is no limitation on the span of battery life. There is also a high need for low latency, such as long latency periods reduce the number of transactions that can be carried out in a store. Hence, the NB-IoT is a better option of IoT technologies to be used in retail point of sale terminals.

3.3.3 Health monitoring

Remote healthcare monitoring has substantially increased within the last decade along with the rising penetration of Internet of Things platforms. The IoT-centered health systems assist in increasing the quality of healthcare services using real-time data access and processing. LPWAN technologies counting the unlicensed ones such as Sigfox, LoRa and licensed ones like NB-IoT spectrum band are all suitable for use in health monitoring. This claim is based on the previous discussion on their ability to reduce power consumption, and overall costs, while boosting coverage.

3.3.4 Asset tracking

The feature of NB-IoT as being a cellular-grade wireless technology makes it look a bit complicated compared to Sigfox and LoRa [28]. This implies that users enjoy the benefits of high performance of devices linked to cellular connections, even though at the cost of more complexity and higher power requirements. The technology is beneficial in providing exemplary network coverage since NB-IoT devices depend on 4G network coverage for data communications. As a result, the technology can function properly indoors and in regions with dense urban population. The complicated aspect and high-power demands make NB-IoT unsuitable for tracking of assets, despite producing relatively shorter response times and better service quality. LoRa is a good preference for asset tracking attributable to its longer battery life than NB-IoT devices, as well as the ability to function properly when in motion. This makes the technology to be the most suitable for tracking assets that are on transit like shipment goods.

3.3.5 Agricultural applications

These applications transmit agriculture indicators, for example water usage, soil moisture and temperature data. In such application’s instant response (downlink transmission) is not needed so we can compromise on latency to some extent. Frequent transmission is also not required because above parameters like water level or moisture level only need to be reported at some specific intervals. Hence, LoRa and Sigfox are appropriate technologies for such case.

3.3.6 Remote monitoring

Remote monitoring of motor vehicles is an area that has lately enticed the attention of both academic circles and the industry at large. The emergence of IoT paradigm has led to the chances for accomplishing this task in the development of wireless transmission technologies. LoRa uses lower data rates than NB-IoT, with merely a few kilobits per second allowing the building of receiving modules having high sensitivity [42]. The characteristic allows LoRa’s receiving device to interpret the received signal at considerably lower power-levels.

4 PRACTICAL SUITABILITY VALIDATION USING OFF-THE-SHELF HARDWARE

4.1 Introduction

From the comparison in the previous chapter, it is evident that each LPWAN technology has their own advantages and disadvantages and place among the different IoT applications. However, it is important to note both technologies LoRa and Sigfox have unique characteristics that are advantageous. LoRa and Sigfox effectively offer wide range coverage and combining low power consumption. They can provide reasonably large coverage with a single gateway or base station. For this reason, they can easily be connected in the most remote areas. The measurement made in the experiment give the most important parameters for the real-life application.

4.2 Selected approach

The measurements are taken using both Sigfox and LoRa to test for the effectiveness and the operations in the outdoor and indoor conditions. The measurements were performed using an existing network infrastructure. Sigfox under the normal infrastructure, is able to measure numerous performance indicators including SNR and RSSI. However, it is important to note that LoRa also has these capabilities. Since both technologies were readily available, the experiment used both in the study to formulate the study results. For Sigfox, the Sigfox Thinxtra Xkit based on Wison Module (WSSFM10) was used and Adeunis ARF8123AA LoRaWAN Field Test device was used for LoRa.

4.3 Measurement methodology

4.3.1 Equipment overview

Sigfox Thinxtra Xkit

The need and demand for IoT devices is seen to be increasing exponentially in the market. The Thinxtra Xkit has various features and other accessories that enable the achievement of IoT applications. The kit provides all the required parts and runs on the global Sigfox network. The Thinxtra shield has a load of sensors including temperature, pressure, shock, 3D accelerometer, light, and magnetic meter [43]. The measurement process was undertaken by the Sigfox Wison Module (WSSFM10) which was used to implement the Sigfox network. The module consists of an Arduino R3 board which is plugged in the shield to give it more performance features. Further, the module comes with a whole year Sigfox connectivity. Thinxtra offers better performance with the capability of adding more hardware development platforms for further developments and expertise. With the Xkit, one can easily design prototypes quickly in the Sigfox IoT design. The device is also ultra-low power consuming. The Sigfox Thinxtra Xkit is shown in below Figure 20.

Figure 20. *Sigfox Thinxtra Xkit [43].*

Adeunis ARF8123AA LoRaWAN Field Test Device

The Adeunis (LoRa) device has features which aid in the low power consumption. The module has a sensitivity of -140 dBm and operates at frequencies between 863-870 MHz [44]. In addition, the offered range of the device is up to 15 km with radio frequency power of 14 dBm. The main LCD screen is displayed when the device is operational on a network or when the device has been configured in activation by personalisation mode (ABP).

LCD screen display uplink and downlink transmission information. The first line shows the uplink information. The second line shows the SF and the power used. The third line shows the downlink information. The last line shows the SF, RSSI and SNR of the frame received. The device can be configured using the USB connector. The Adeunis ARF8123AA LoRaWAN Field Test Device is shown in Figure 21.

Figure 21. *Adeunis ARF8123AA LoRaWAN field test device [44].*

4.3.2 Deployment

The measurement locations are shown in the university map below. There are total of 14 measurement locations both indoor and outdoor.

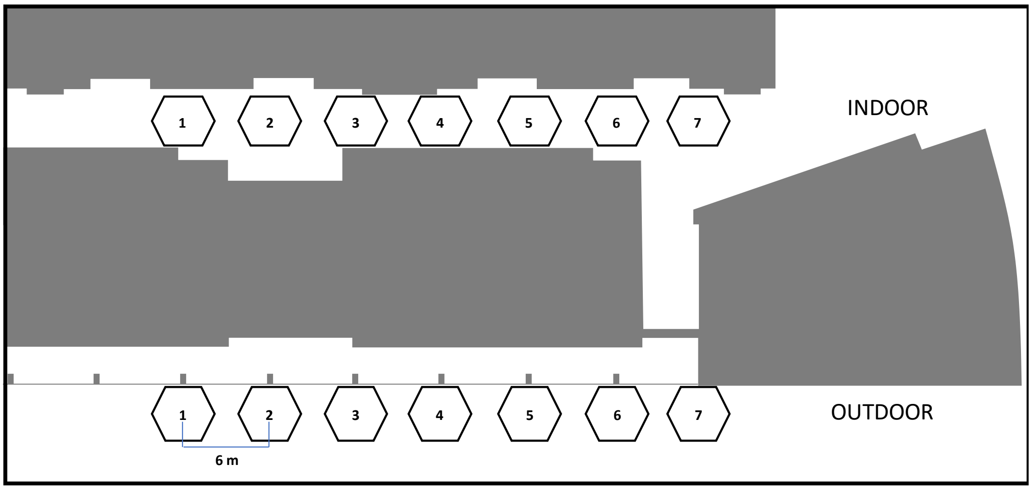

Figure 22. *Measurement locations map.*

To test the technologies for the different scenarios of communications, that is, indoor and outdoor, the transmitting and receiving devices were placed in the different locations as shown by labels 1 to 7 in Figure 22. The experiment was carried out during normal working hours so to include the influence of people moving around and other environmental stresses on the technologies. The local regulations (ETSI in Europe) limit the use of unlicensed frequency bands, used by LoRa and Sigfox, limiting for example transmit power and duty cycle [2]. Especially, the duty cycle limits how many measurements could be done within a certain time frame. IoT may involve technologies that have sensors operating either indoors or outdoors and hence the need to perform the measurements both indoors and outdoors.

4.4 Measurement results

The experiment concentrated on measuring the RSSI and SNR which are the most important aspects for the communication in LoRa and Sigfox. The results obtained on the parameters measured are represented in the following sections.

4.4.1 LoRa RSSI

RSSI simply measures how well the module 'hears' the signal sent from the base station antenna. The RSSI values in LoRa vary significantly in the indoor locations from one point to another. From the graph, in the indoor curve, we see that location 2 has highest value while locations 5 and 6 have the lowest values. For the outdoor locations, point 2 has recorded the highest dBm meaning that the signal is best received at this point while the lowest value is at location 6. LoRa RSSI values are further illustrated in Figure 23.

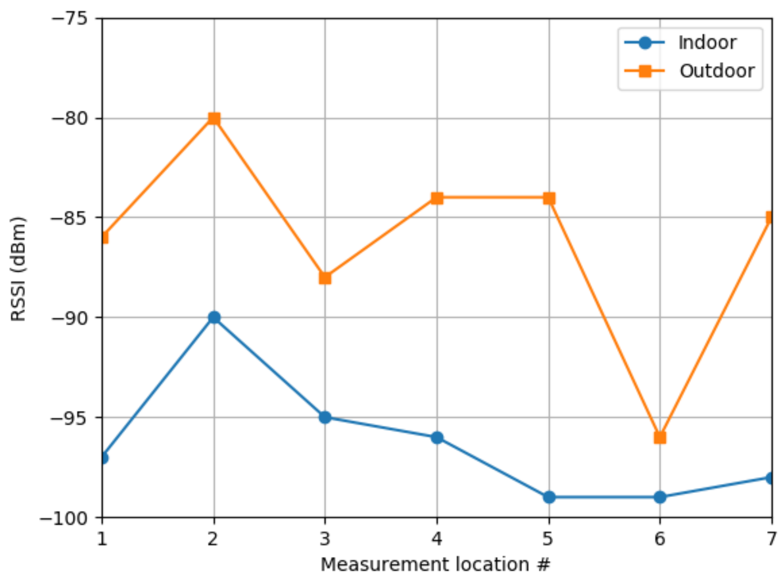

Figure 23. *LoRa RSSI.*

4.4.2 LoRa penetration loss

Penetration loss is calculated by taking difference between indoor and outdoor RSSI dBm values and are shown in Figure 24. Penetration loss refers to the loss in signal power when signal penetrates through obstacles. Here, the penetration loss specifically refers to situation where the signal penetrates from outdoor to indoor.

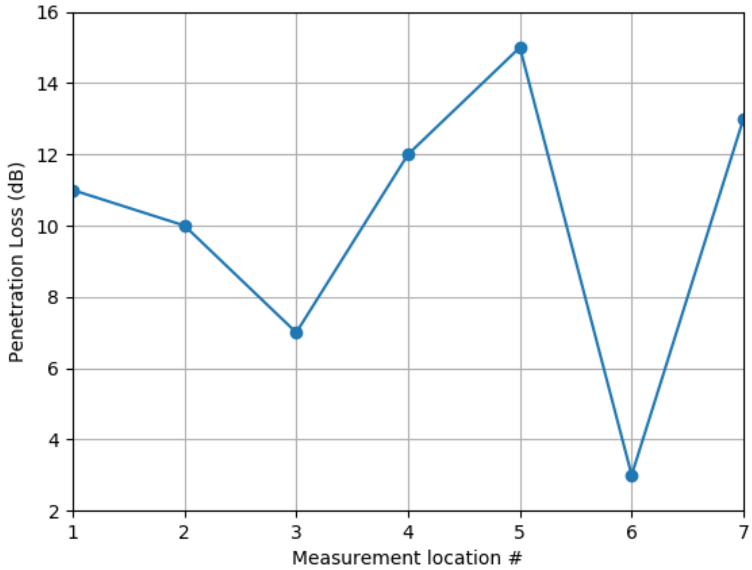

Figure 24. *LoRa RSSI penetration loss.*

4.4.3 Sigfox RSSI

For the Sigfox module, the fluctuation of RSSI values is quite irregular from one location to another. The outdoor locations have the highest RSSI value, with location 3 recording the most dBm and location 7 having the lowest as displayed in Figure 25. In the indoor locations, location 6 records the highest while location 3 has the lowest. These great fluctuations are mainly because the measurements performed in different locations (1-7) were using different base stations. That is shown by the fact that the base station ID is different for different measurements.

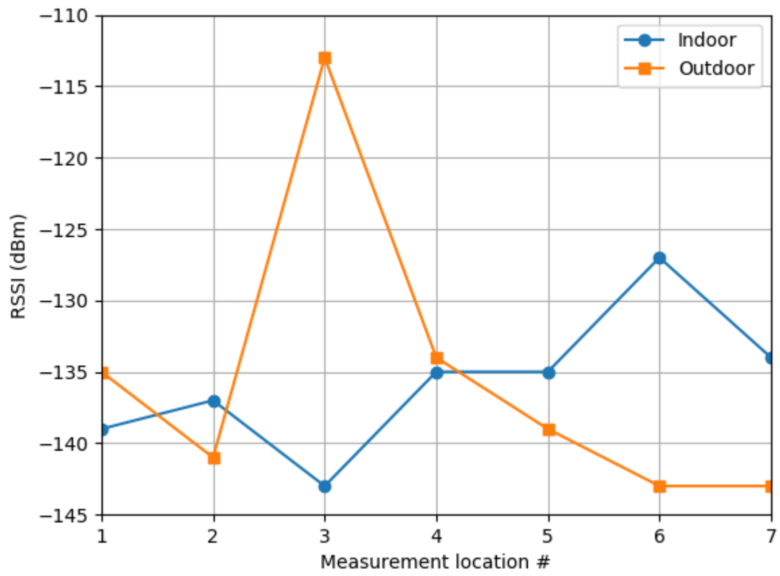

Figure 25. *Sigfox RSSI.*

4.4.4 Sigfox penetration loss

In Sigfox case, the base stations IDs were found to be different for both indoor and outdoor measurements, i.e., no measurement location (Indoor and outdoor) had the same base station ID. Hence those measurements cannot be compared for penetration loss.

4.4.5 Impact of RSSI

The RSSI values of the packets received are used to test the capabilities of the LoRa and Sigfox radio receivers. For the LoRa device, the lowest measured RSSI was at locations 5 and 6 for the indoor condition and location 6 for the outdoor. Generally, as the distance to the gateway increases and the number of obstructions increase, the RSSI drastically reduces. The RSSI values are higher for locations that are closer to the gateway.

4.4.6 LoRa SNR

The signal to noise ratio gives the fraction of noise present in the signal received by the module. The higher the value, the better the signal. A smaller value indicates that the noise embedded in the signal is higher and hence a poor-quality signal. From the graph, the outdoor locations have a varied value of SNR. At locations 2, 5 and 7, the value is at 15 dB. The lowest values are at locations 1, 4 and 6. The indoor locations on the other hand have great SNR variations from one location to another. The highest value is at location 4 and the lowest is at location 1 as shown in Figure 26.

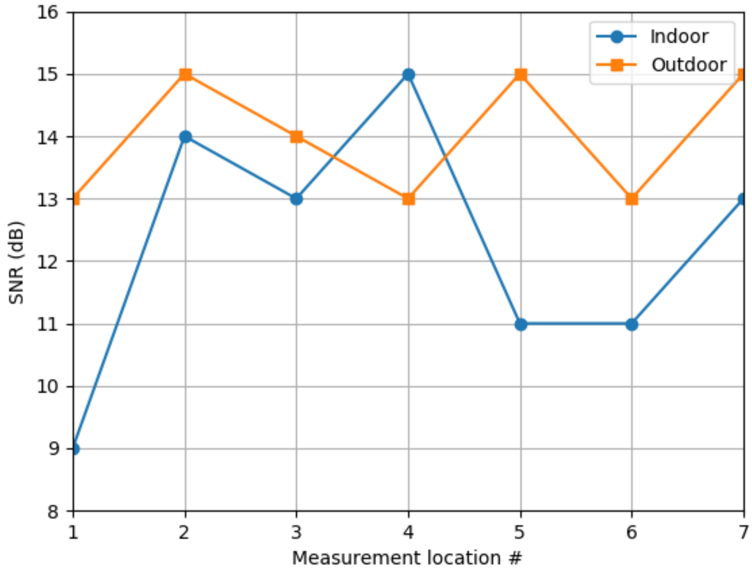

Figure 26. *LoRa SNR.*

4.4.7 Sigfox SNR

Sigfox SNR variations differ completely from those in the LoRa measurements. In the outdoor locations, the signal is of best quality at location 3 since the SNR value is highest. In the indoor locations the signal has poorer quality. In Figure 27 below location 3 and 7 have the poorest signals and location 6 has the best quality. The SNR values from different locations cannot be compared that well, because the measurements were obtained from different base stations.

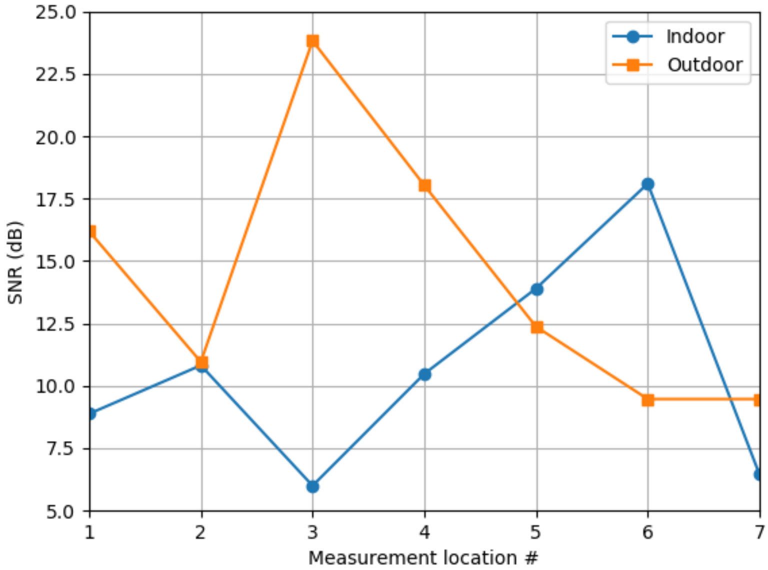

Figure 27. *Sigfox SNR.*

4.4.8 Impact of SNR

SNR compares the power level of the desired signal and that of the noise and gives a ratio. If SNR is greater than 0 dB, the signal power is higher than the noise power. If SNR is less than 0 dB, then the noise power is higher than the signal power. The value of the signal to noise ratio determines the quality of a signal. Most importantly, it is convenient to understand that any electronic equipment is subject to noise interference including electronic noise. SNR ratio in the LoRa equipment is seen to be lower in the indoor conditions compared to the outdoor conditions. The main reason why indoor SNR is lower than outdoor SNR is the penetration loss. Since the signal has to penetrate through a thick wall of the building, the signal attenuates and therefore the signal has less power, which makes its SNR lower. At location 4 indoor the SNR value is highest. Therefore, it offers the best location to place the equipment. At the outdoor locations 2 & 5 the SNR values are highest. LoRa module performs best at these locations. In the Sigfox equipment the SNR values are seen to vary significantly in the outdoor locations with the highest being at location 3. In the indoor locations, the SNR values are quite low and do not vary as those in the outdoor locations.

5 CONCLUSIONS

In this section, based on studies of three common LPWAN technologies and practical measurements using LoRa, and Sigfox the following conclusion are drawn.

LPWAN technologies are capable to bring revolution in IoT field because they offer long range, low data rates, low power consumption, and low-cost solution. Typical IoT applications require low data rates, long range, and long battery lifetime. Therefore, these LPWAN technologies fulfil the needs of these IoT applications in wide areas.

There are many differences in terms of coverage, data rates, bandwidths, payload size, and cost in these wireless systems. Thus, making right technology selection not only is cost effective but also meets the need of a specific IoT use case. The suitability decision is made depending upon the offered technological features in LoRa, Sigfox and NB-IoT and the need of certain IoT application.

The most important factors which affects the performance of the IoT application are quality of service, battery lifetime, latency, data rates, scalability, payload size, and range. In order to choose right LPWAN technology, an in-depth comparison and analysis is required of their technological specifications. However, based on LoRa, Sigfox and NB-IoT study it is found that there is no one technology that can meet needs of all applications. Hence applications like health monitoring or smart building can find one technology more suitable than other LPWAN systems.

The measured values RSSI and SNR in LoRa and Sigfox are critical for the implementation of IoT in daily activities. The purpose of the measurements in this thesis was to showcase the importance of the variables measured in the application of LPWAN in the implementation of IoT technologies. IoT applications often involve sensors, which must be put in some location where they can communicate over the network. Hence, through practical measurements of RSSI and SNR, similarly as shown in this thesis, the most suitable place can be selected for sensor placement.

REFERENCES

[1] H. U. Rehman, M. Asif and M. Ahmad, Future applications and research challenges of IoT, 2017 International Conference on Information and Communication Technologies (ICICT), Karachi, 2017, pp. 68-74.

[2] U. Raza, P. Kulkarni and M. Sooriyabandara, Low Power Wide Area Networks: An Overview, in IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 855-873, 2017.

[3] J. Petajajarvi, K. Mikhaylov, M. Pettissalo, J. Janhunen and J. Iinatti, Performance of a low-power wide-area network based on LoRa technology: Doppler robustness, scalability, and coverage, International Journal of Distributed Sensor Networks, 2017, Vol. 13(3), pp. 2–16.

[4] R. S. Sinha, Y. Wei, S.-H. Hwang. A survey on LPWA technology: LoRa and NB-IoT, ICT Express 3 (2017), pp. 14–21.

[5] What Is "Cat-M1" and What Does It Mean for IoT? Available online: https://ubidots.com/blog/what-cat-m1-means-for-iot/, accessed on 14/03/12019.

[6] M. Chen, Y. Miao, Y. Hao and K. Hwang, Narrow Band Internet of Things, in IEEE Access, vol. 5, pp. 20557-20577, 2017.

[7] J de C. Silva, J. J. P. C. Rodrigues, A. M. Alberti, P. Solic and A. L. L. Aquino, LoRaWAN — A low power WAN protocol for Internet of Things: A review and opportunities, 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech), Split, 2017, pp. 1-6.

[8] K. Phung, H. Tran, Q. Nguyen, T. T. Huong and T. Nguyen, Analysis and assessment of LoRaWAN, 2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), Ho Chi Minh City, 2018, pp. 241-246.

[9] B. Reynders and S. Pollin, Chirp spread spectrum as a modulation technique for long range communication, 2016 Symposium on Communications and Vehicular Technologies (SCVT), 2016, pp. 1-5.

[10] LoRa Alliance Technical Marketing Workgroup, November 2015, A technical Overview of LoRa and LoRaWAN. Available online: https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf.

[11] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovacs, P. Mogensen and M. Sorensen, Coverage and Capacity Analysis of Sigfox, LoRa, GPRS, and NB-IoT, 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, Australia, 2017, pp. 1-5.

[12] LoRa Alliance, Available online: https://lora-alliance.org/about-lorawan, accessed on 24/04/2019.

[13] Sigfox Technology Overview. Available online: https://www.sigfox.com/en/sigfox-iot-technology-overview, accessed on 29/05/2019.

[14] LoRa Alliance. LoRaWAN 1.1 Specification. Authored by the LoRa Alliance Technical Committee, pp. 1-101.

[15] P. Neumann, J. Montavont and T. Noël, Indoor deployment of low power wide area networks (LPWAN): A LoRaWAN case study, 2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), New York, NY, 2016, pp. 1-8.

[16] The things network group. Available online: https://www.thethingsnetwork.org/docs/lorawan/security.html, accessed on 28/04/2019.

[17] Utilizing the LoRa Network to Deliver Highly Scalable Solutions to the world of IoT. Available online: https://milandr.com/index.php/lorawan, accessed on 24/03/2019.

[18] LoRa Architecture. Available online: http://www.3glteinfo.com/lora/lora-architecture/, accessed on 14/03/2019.

[19] A. Augustin, J. Yi, T. Clausen, W M. Townsley, A Study of LoRa: Long Range & Low Power Networks for the Internet of Things, Sensors 2016, 16(9), pp. 2–18.

[20] J. Haxhibeqiri, A. Karaagac, F. Van den Abeele, W. Joseph, I. Moerman and J. Hoebeke, LoRa indoor coverage and performance in an industrial environment: Case study, 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, 2017, pp. 1-8.

[21] M. Bor and U. Roedig, LoRa Transmission Parameter Selection, 2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS), Ottawa, ON, 2017, pp. 27-34.

[22] Sacha Kavanagh, 2018, What is Narrowband IoT? Available online: https://5g.co.uk/guides/what-is-narrowband-iot/, accessed on 29/04/2019.

[23] J. Rubio-Aparicio, F. Cerdan-Cartagena, J. Suardiaz-Muro, and J. Ybarra-Moreno. Design and implementation of a mixed IoT LPWAN network architecture, 2019, Sensors, 19(3), 675.

[24] L. Vangelista and M. Centenaro, Worldwide Connectivity for the Internet of Things Through LoRaWAN, Future Internet, vol. 11(3), 2019, pp. 1-11.

[25] Wireless solutions #5 Sigfox - Fulfilling an IoT communications need. Available online: https://uk.farnell.com/fulfilling-an-iot-communications-need, accessed on 01/05/2019.

[26] Group Specification. Low Throughput Networks (LTN); Protocols and Interfaces. ETSI GS LTN 003 V1.1.1 (2014-09). Available online: https://www.etsi.org/deliver/etsi_gs/LTN/001_099/003/01.01.01_60/gs_LTN003v010101p.pdf, accessed on 25/06/2019.

[27] A. Lavric, A. I. Petrariu and V. Popa, Long Range SigFox Communication Protocol Scalability Analysis Under Large-Scale, High-Density Conditions, in IEEE Access, vol. 7, pp. 35816-35825, 2019.

[28] P. Ram. LPWAN, LoRa, LoRaWAN and the Internet of Things. Available online: https://medium.com/coinmonks/lpwan-lora-lorawan-and-the-internet-of-things-aed7d5975d5d, accessed on 30/06/2019.

[29] Sigfox Technology Overview. Available online: https://www.sigfox.com/en/sigfox-iot-technology-overview, accessed on 16/06/2019.

[30] Sigfox Services. Available online: https://www.sigfox.com/en/solutions/sigfox-services, accessed on 16/06/2019.

[31] LoRaWAN security full end-to-end encryption for IoT application providers. A white paper prepared for the LoRa alliance by Gemalto, Actility and Semtech, February 2017. Available online: https://lora-alliance.org/sites/default/files/2019-05/lorawan_security_whitepaper.pdf, accessed on 29/05/2019.

[32] Sigfox official website. Available online: https://www.sigfox.com/en/our-vision, accessed on 29/05/2019.

[33] Radio Configurations. Available online: https://build.sigfox.com/sigfox-radio-configurations-rc, accessed on 29/05/2019.

[34] Y. Ji and H. Yang. Comparation of LoRa and NB-IoT. Network and Communication Technologies; Vol. 4, No. 1; 2019 ISSN 1927-064X E-ISSN 1927-0658 Published by Canadian Center of Science and Education.

[35] Make things come alive in a secure way. Available online: https://www.sigfox.com/en/technology/security, accessed on 29/05/2019.

[36] J. Xu, J. Yao, L. Wang, Z. Ming, K. Wu and L. Chen, Narrowband Internet of Things: Evolutions, Technologies, and Open Issues, in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1449-1462, June 2018.

[37] Narrowband – Internet of Things (NB-IoT). Available online: https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/, accessed on 04/06/2019.

[38] What is Narrowband IoT (NB-IoT)? – Explanation and 5 Business Benefits. Available online: https://www.iotforall.com/what-is-narrowband-iot/, accessed on 04/06/2019.

[39] N. Tsavalos and A. A. Hashem. Low Power Wide Area Network (LPWAN) Technologies for Industrial IoT Applications. Master´s thesis. Department of Electrical and Information technology, Lund University Sweden, 85 p., June 2018.

[40] K. Mekki, E. Bajic, F. Chaxel, F. Meyer. A comparative study of LPWAN technologies for large-scale IoT deployment. ICT Express, Elsevier, 2019, 5 (1), pp.1-7

[41] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui and T. Watteyne, Understanding the Limits of LoRaWAN, in IEEE Communications Magazine*,* vol. 55, no. 9, pp. 34-40, Sept. 2017.

[42] J. Santa, R. Sanchez-Iborra, P. Rodriguez-Rey, L. Bernal-Escobedo and A. F. Gomez-Skarmeta, LPWAN-Based Vehicular Monitoring Platform with a Generic IP Network Interface, Sensors, 2019, vol. 19 (2), pp. 1-17.

[43] Thinxtra Empowering Internet of Things. Available online: https://www.thinxtra.com/solutions/thinxtraproducts/xkit/#av_section_2, accessed on 25/08/2019.

[44] Adeunis Wireless Products and Solutions. Available online: https://www.adeunis.com/en/produit/ftd-868-915-2/, accessed on 26/08/2019.