University of Genoa, ITALY

Politechnic School

DITEN - Department of Electrical, Electronics and Telecommunication Engineering and Naval Architecture

Ph.D. in Science and Technology for Electronic and Telecommunication Engineering – Cycle XXXIV (2018-2021)

Doctoral Thesis

Integrated Satellite-terrestrial networks for IoT: LoRaWAN as a Flying Gateway

Author:

Aya Moheddine

Advisor:

Prof. Mario Marchese

PhD Course Coordinator:

Prof. Maurizio Valle

XXXIV Cycle

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other universities. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements. This dissertation contains fewer than 65,000 words including bibliography, footnotes, tables and equations and has fewer than 150 figures.

Acknowledgment

This thesis, like any other work I have attempted in my life, wouldn't have been possible without the sustenance of certain people around me. It is my genuine intent to acknowledge their efforts and contributions through my journey to earn my PhD. which has been a life changing experience.

This thesis appears in its current form due to the assistance and guidance of several people who, I believe, deserve this honor more than myself. I feel relieve to have the opportunity to express my gratitude for all of them.

I am greatly indebted to my supervisor *Prof. Mario Marchese* for his excellent advice, support and encouragement he had given me over the last three years. This thesis would not have been possible without *Dr. Fabio Patrone*, whose guidance from the initial step in research enabled me to develop an understanding of the subject. I am thankful for the extraordinary experiences they arranged for me and for providing opportunities for me to grow professionally. It is an honor to learn from Prof.Marchese and Dr. Patrone.

My sincerest thanks are directed to *Dr. Ali Ibrahim*, for all the guidance and encouragement I received from their side at every step during this journey. He influenced me to work hard and persist in my determination.

I would like to thank all members of the SCNL laboratory. It was a pleasure to meet and work with you. I would like to thank my Lebanese friends in Genova, especially *Farah* who always gives me love, respect and support.

I am deeply indebted to my Father *Hasan* and my Mother *Lina* who have encouraged me to continue my studies and overcome all the challenges. They are always the basic reason behind all the successes that I did and I would do. I thank my lovely sisters, *Hiba* and *Zeinab*, my brothers in law, *Fadi* and *Amer*, my nieces *Nour* and *Roukaya* and my nephew *Ali* for their love, support and encouragement.

Not to forget my partner, *Mohammad*. Thank you for your support, encouragement and love during this year.

Dedicated to Him, my Imam.... Mahdi

Abstract

When Internet of Things (IoT) was introduced, it causes an immense change in the human life. Recently, different IoT emerging use cases, which will involve an even higher number of connected devices aimed at collecting and sending data with different purposes and over different application scenarios, such as smart city, smart factory, and smart agriculture. In some cases, the terrestrial infrastructure is not enough to guarantee the typical performance indicators due to its design and intrinsic limitations. Coverage is an example, where the terrestrial infrastructure is not able to cover certain areas such as remote and rural areas. Flying technologies, such as communication satellites and Unmanned Aerial Vehicles (UAVs), can contribute to overcome the limitations of the terrestrial infrastructure, offering wider coverage, higher resilience and availability, and improving user's Quality of Experience (QoE). IoT can benefit from the UAVs and satellite integration in many ways, also beyond the coverage extension and the increase of the available bandwidth that these objects can offer. This thesis proposes the integration of both IoT and UAVs to guarantee the increased coverage in hard to reach and out of coverage areas. Its core focus addresses the development of the IoT flying gateway and data mule and testing both approaches to show their feasibility.

The first approach for the integration of IoT and UAV results in the implementing of LoRa flying gateway with the aim of increasing the IoT communication protocols' coverage area to reach remote and rural areas. This flying gateway examines the feasibility for extending the coverage in remote area and transmitting the data to the

IoT cloud in real time. Moreover, it considers the presence of satellite between the gateway and the final destination for areas with no Internet connectivity and communication means such as WiFi, Ethernet, 4G or LTE. The experimental results have shown that deploying a LoRa gateway on board of a flying drone is an ideal option for the extension of the IoT network coverage in rural and remote areas.

The second approach for the integration of the aforementioned technologies is the deployment of IoT data mule concept for LoRa networks. The difference here is the storage of the data on board of the gateway and not transmitting the data to the IoT cloud in real time. The aim of this approach is to receive the data from the LoRa sensors installed in a remote area, store them in the gateway up until this flying gateway is connected to the Internet. The experimental results have shown the feasibility of our flying data mule in terms of signal quality, data delivery, power consumption and gateway status.

The third approach considers the security aspect in LoRa networks. The possible physical attacks that can be performed on any LoRa device can be performed once its location is revealed. Position estimation was carried out using one of the LoRa signal features: *RSSI*. The values of RSSI are fed to the *Trilateration* localization algorithm to estimate the device's position. Different outdoor tests were done with and without the drone, and the results have shown that RSSI is a low cost option for position estimation that can results in a slight error due to different environmental conditions that affect the signal quality.

In conclusion, by adopting both IoT technology and UAV, this thesis advances the development of flying LoRa gateway and LoRa data mule for the aim of increasing the coverage of LoRa networks to reach rural and remote areas. Moreover, this research could be considered as the first step towards the development of a high quality and performance LoRa flying gateway to be tested and used in massive LoRa IoT networks in rural and remote areas.

Keywords— *IoT, LoRa, LoRaWAN, LPWAN, UAVs, Flying Gateways, IoT Data Mules, Satellite Simulation, Localization, Position Estimation.*

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

Information and Communication Technology (ICT) is leading to continuous emergence of new technologies due to its dynamic and evolutionary nature. Recent developments in computing resources, software systems and communication networks as well as the ongoing miniaturization of hardware components have enabled ICT to be integrated in almost anything. This results in the emergence of a new computing paradigm known as *Internet of Things* (IoT). Figure 1.1 shows the number of IoT and non-IoT devices connected since 2017. As noticed, the incredible increase in the number of IoT connected devices from 6.1 billion device to 13.8 billion devices by 2021 demonstrates the great potential and importance of IoT nowadays. According to IoT analytics, the global number of IoT connected devices is expected to grow to 20.9 billion devices by 2025. An old dream is being realized today due to IoT, where every object is turning to a smart one connected to the Internet, able to collect and exchange data and make decisions, autonomously. The *"smart"* part in IoT covers both communication infrastructure and applications including monitoring systems, smart cities and industrial automation, etc. Such applications require short-range radio communication technologies (for example: ZigBee) such as applications targeted towards restricted small areas. On the other hand, different applications like smart agriculture require communication

technologies able to cover distances up to tens of kilometers in rural and remote areas. Recently, a great interest towards the latter category is noticed and is denoted as *Low Power Wide Area Network* (LPWAN). The coverage is not the only concern or requirement of such applications, but also the power consumption or the battery life of the devices is of great interest.

These LPWAN solutions are classified into two categories based on the frequency band. Some

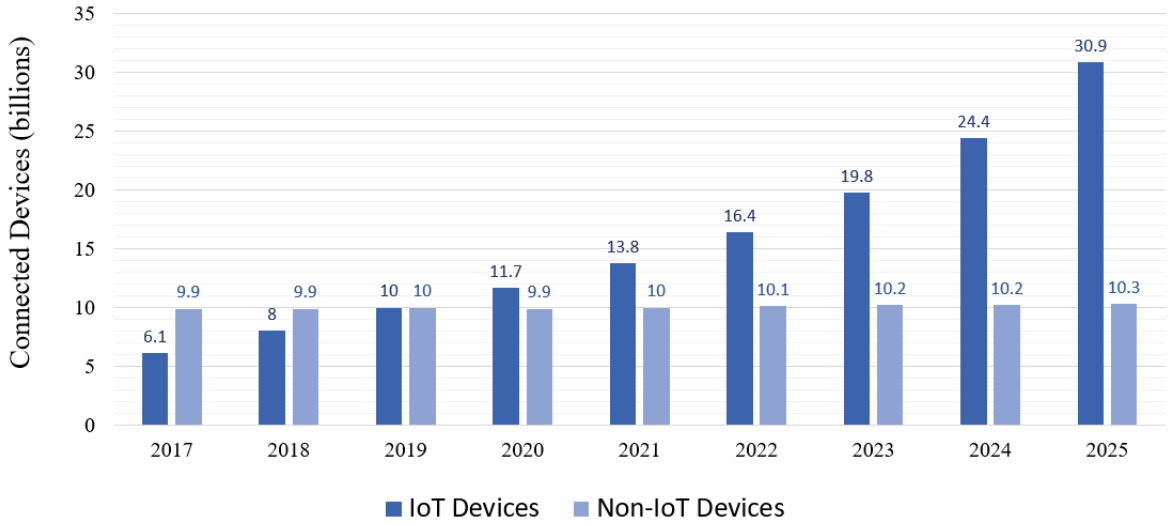

Figure 1.1: Number of connected and the estimated IoT & non-IoT devices from 2017 to 2025 [9].

of these solutions that operate in the unlicensed bands such as the Industrial, Scientific and Medical (ISM) bands at 433 and 868 MHz have been already deployed in specific regions: SigFox for example. It operates both as a communication technology and as a provider. Another solution is the Long Range, or LoRa. Initially, LoRa was established in the Mobile World Congress in 2015 [10] announcing its proprietary IoT communication technology known as LoRaWAN that operates in the ISM unlicensed band. Differently, the 3rd Generation Partnership Project (3GPP) has been supporting different LPWAN standards that operate in the licensed band: (i) *Extended Coverage Global System for Mobile Communications* or ECGSM-IoT, (ii) *Long Term Evolution-Machine Type Communication Category M1* or LTE-MTC Cat M1, and (iii) *Narrowband IoT* or NB-IoT.

On the other hand, Unmanned Aerial Vehicles (UAVs) are witnessing a great growth, development and improvement. Recently, UAVs gained popularity and have been utilized in different applications such as remote sensing, rescuing as well as military purposes. The graph in Figure 1.2 shows the incredible growth of the use of drones and how the estimation in the number of purchased ones is increasing. This increase is due to their reduced acquisition cost and flexibility in deployment. Lately, UAVs attracted a great attention in various research studies regarding IoT. The integration of UAVs and IoT promises long transmission ranges respecting the IoT end device battery life. Various studies suggested the use of UAVs with LoRa IoT communication protocol as a helping factor for data collection regarding different applications such as air, temperature, humidity or gas monitoring [11–16]. This UAV acts as a LoRa node which is used for sensing data from the surrounding to be forwarded to a LoRa gateway and then to the LoRa server.

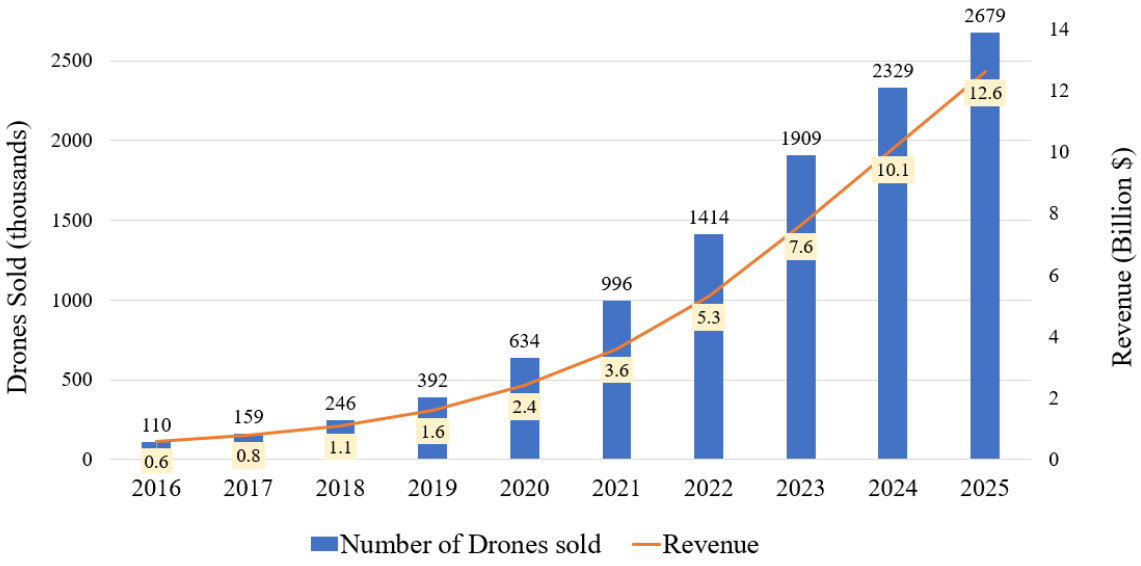

Figure 1.2: The number of drones deployed and estimated along with the revenue from 2016 to 2025 [17].

With the introduction of long-range terrestrial IoT technologies, the different limitations of short range wireless technologies have been addressed, and thus extending & increasing the number of application and scenarios in which IoT can be successfully deployed [18]. The main

requirement of IoT is to guarantee the continuous connectivity of all the devices whenever they are installed. This can be provided by using different communication means such as WiFi, SigFox or 4G cellular networks. However, they cannot provide seamless and ubiquitous coverage satellites can provide [19]. The integration of satellite in IoT environments despite the application has been introduced and presented in different studies such as in [20]. The aim is to extend the coverage of healthcare IoT devices in areas that lack Internet connectivity using on one side LoRa and LEO satellite on other side. [21] proposed a preliminary design of LEO constellation-based IoT network focusing on NB-IoT technology. An Iridium LoRaWAN prototype has been presented in [22] which includes a GEO satellite segment. This prototype has been used for data exchange formats testing in an IoT application running on hybrid networks.

Further more, due to recent advances in both automated vehicles and communication technologies, UAVs are being used to enhance the performance of a wide range of applications such as IoT or Wireless Sensor Networks (WSN) applications. Data collection is the most used application for UAVs, where these vehicles are utilized to travel over a specific area equipped with different sensors generating data. Different research studies considered this use case using different communication technologies. [23] and [24] for example considered the use of UAVs for data collection in a WSN/IoT using 802.11b and 802.15.4 as communication protocols between the network and the vehicle respectively. Considering remote locations where having the suitable infrastructure for collecting data from installed sensor networks is impossible, UAVs play an efficient role taking the advantage of the important and significant data generated in such regions. They can be easily deployed on demand and keep flying for a time sufficient to let them perform their task. UAVs, also called drones, are considered as *Data Mules* flying over a large remote area and retrieving data. These mules can reduce time, energy and increase the performance efficiency through deploying the convenient communication protocol. LPWAN technologies are the most suitable for applications that require low power consumption and long transmission range. They can offer both low power consumption for long-life battery-powered IoT devices and long-range coverage with bidirectional communication at the cost of a limited data rate. However, all these solutions are based on

the mobile telecommunication infrastructure (NB-IoT, LTE-M, ...) or ad-hoc infrastructures. Commercially available solutions, such as SigFox and Telensa, and more open-source solutions, such as LoRaWAN, are based on a network of base stations, also called gateways, which have been deployed with the only purpose of offering connectivity to each solution's devices. A consequent drawback is the limited coverage due to the not possible reuse of the already existing telecommunication access infrastructure. Besides, the employment of terrestrial fixed base stations, on one hand, could be economically inefficient in case of a low number of users and devices per base station and, on the other hand, could involve additional problems for connecting them to the Internet. Integrating all the aforementioned technologies, a new research domain is emerging and receiving a great interest, known as IoFT [25, 26]. The concept of IoFT is to integrate flying objects, whether autonomous or not, with a network of physical and interactive objects able to communicate with Internet-enabled devices [27]. This new field widens the role of unmanned vehicles by enabling new applications, extending coverage, increasing their connectivity and scalability. The IoFT applications are diversified and are increasing everyday and are not limited to: smart agriculture as in [28–30], environmental pollution monitoring as in [31–35], disaster management as in [36–40], video streaming surveillance such as in [41–43], smart cities [44, 45], smart industry [46, 47] etc.

Besides, implementing data mule functionalities onboard UAV allow them collecting data while flying and forward data only when they come back to the starting point, without the need to connect them to the Internet for the entire flight.
In addition to data collection purpose using flying objects or UAVs, UAVs can be used for localization or position estimation of IoT nodes in a network. Localization is becoming a hot topic with different IoT applications such as traffic monitoring. Most of the research targets localization in indoor environments for example in [48–52]. Concerning outdoor environments, satellite based positioning system [53] such as Global Positioning System (GPS) is one of the most used technologies in different applications [54, 55]. However, such technologies are considered as non-feasible ones due to their high cost and power consumption. To better exploit the IoT technologies, LoRa can be used for both data transmission in any IoT network and for estimating & calculating the position i.e *localization* without the need of any

additional special device. It is suitable for both outdoor and indoor environments [56].
Several studies adopted the use of Angle of Arrival (AoA) and Time Difference of Arrival (TDoA) -for example- [57, 58] for localization purposes, although such techniques require special hardware or accurate synchronization respectively. Another possible technique that doesn't require additional hardware components and has low power consumption is Received Signal Strength Indicator (RSSI). This technique is easy to use compared to the other techniques in IoT networks, because the RSSI values can be received and retrieved in a simple way by the user. The RSSI information associated with these IoT devices can be retrieved and given as input to different algorithms to reveal their location. Once the location is exposed, possible attacks can be carried out by attackers known as *"Physical Attacks"*. A physical attack is the physical violation of a network through either wired or wireless medium or directly on a specific device. Tampering, malicious code injection, Radio Frequency interference or jamming, fake node injection, sleep denial attacks and permanent denial of service are examples of physical attacks [59], leading to data leakage, fake data manipulation, node shutdown or distortion in the node communication [60]. To carry out a physical attack, the attacker misuse the security keys stored in the device for the purpose of transmitting fake messages to other IoT devices or the gateway, recording the data transmission or blocking it. Such attacks are targeted on the PHY/MAC layers of the TCP/IP and the perception and application layers in the IoT network architecture.

1.2 Contribution

Compared to ground-based LoRa communication systems, UAV-based LoRa networks have the advantage of a direct line-of-sight between UAVs, flying at an altitude of tens of meters. This ensures direct visibility among themselves and even with some ground base LoRa stations, allowing the users to exchange data across longer ranges than are possible with ground communication [28]. Real-time UAV-based LoRa communication network can be classified by two different roles (UAV as a LoRa node or LoRa gateway) and objectives (communication or localization). As a LoRa node, the UAV carries a LoRa module and

sensors to perform measurements and collect data. Then, it communicates with the nearest LoRa gateway, where protocol conversion is performed from LoRa to message queuing telemetry transport (MQTT) or other formats, so the payload can be read by a web server. A UAV-based LoRa gateway can replace a compromised fixed LoRa gateway or be delivered to a specific remote location to increase the network coverage of specific IoT devices. One of the main advantages of using UAVs as LoRa gateways is that they can be deployed on demand, and increasing their number can increase the efficiency of the system [29].

1.3 Thesis Outline

The remainder of this thesis is structured as follows. Chapter 2 reports the LoRa technology and its different features along with the different applications where LoRa is being deployed. Chapter 3 presents a detailed description of proposed solution along with the main testbed developed. Chapter 4 describes the concept of the *LoRa flying gateway* deployed in rural and remote areas with simulated satellite link. The outdoor testing using an UAV and the results obtained from this test along with the gateway status are reported. Chapter 5 introduces another concept of the LoRa flying gateway which is the *LoRa Date Mule* used to more extend the coverage to reach remote areas out of coverage of traditional communication means. Chapter 6 deals with another aspect of LoRa, the one related to security. The aim is to benefit from the different parameters a LoRa signal provides such as RSSI value to estimate the position of a specific LoRa device installed in an outdoor area for the target of physical attack. Conclusions and potential future works are drawn in Chapter 7.

Chapter 2

State of the Art

Summary

In this chapter a brief introduction about Internet of Things and LoRa communication protocol is given for acquiring the needed knowledge for a better understanding of the thesis.

2.1 Internet of Things

The term of Internet of Things (IoT) was initially introduced in 1999 by *Kevin Ashton*. The concept of IoT is to connect anything, anywhere at anytime. The strength of the idea behind IoT is giving the ability of communication to different objects within each other and with the Internet. To reach the Internet, different means of connection are available such as WiFi or by adopting the use of some embedded circuits with communication interface.

The IoT structure consists of three main layers: *perception layer*, *network layer* and *application layer*. The lower layer represents the different sensors and actuators deployed in a specific environment to generate data. The device must be a smart one equipped with control and processing algorithms. The data generated by these devices is transmitted by the network layer which has the ability to control and manage the large amount of traffic exchanged. The third and upper layer corresponds to the interface that allows the direct communication

between the service it provides and the user [61]. These three main layer are given in Figure 2.1.

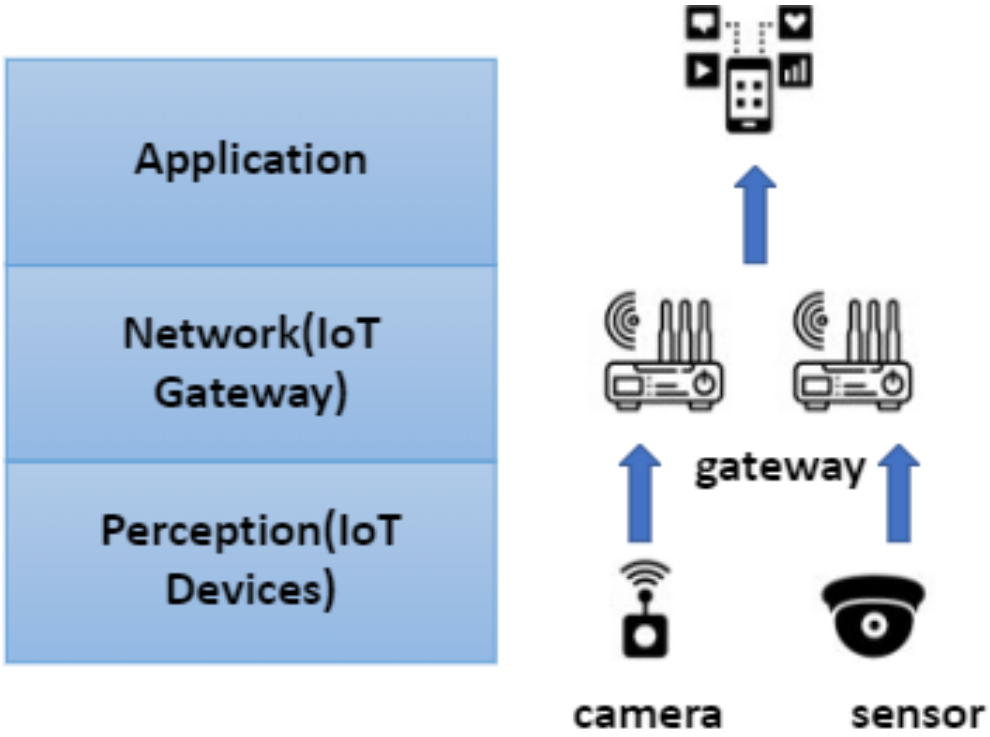

Figure 2.1: Overview of the 3-layer IoT architecture.

2.2 IoT Technologies

Different network technologies exist to develop and implement an IoT system depending on the application. The choice of which technology to use depends on different factors such as coverage distance, power constraints and costs. Such technologies are classified into two categories: short range (for example: WiFi, Bluetooth & ZigBee) and long range (for example: LPWAN, LTE, & 5G). Some of the most recognized and adopted network technologies are:

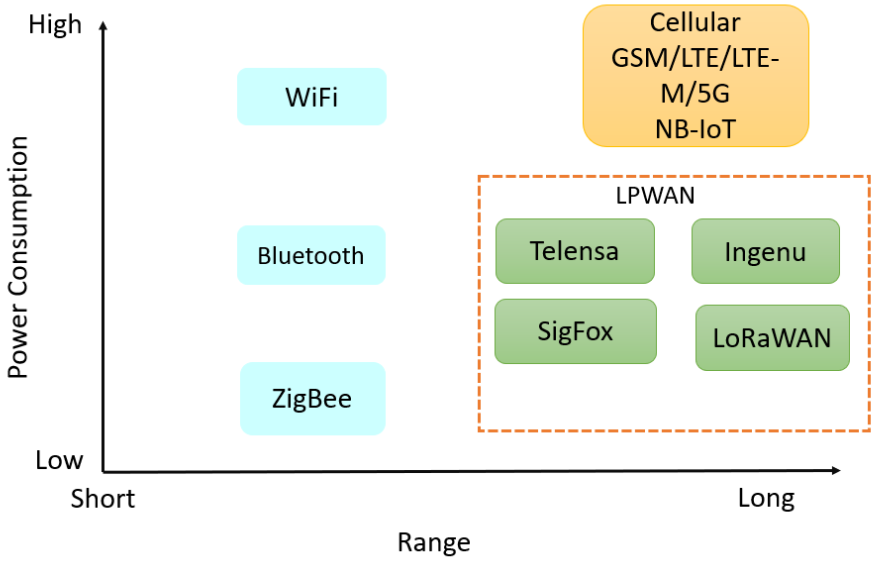

Figure 2.2: IoT Technologies Comparison: Range vs Data Rate.

Low Rate Wireless Personal Area Networks

IoT is been used in different applications and use cases, for example, smart houses. Such applications need a technology that allows the easy, simple and power efficient communication between the different devices deployed in a closed and small area. Wireless Personal Area Network or WPAN is a standard communication technology that permits the connection between devices up to tens of meters [62].

- **ZigBee**: based on the IEEE 802.15.4 protocol, it offers low power and low rate solution for short range IoT applications (up to 100 meters). It operates in the 2.4 GHz band mainly aiming applications which don't need frequent data exchange supporting mesh, star and tree network typologies [63].

- **Bluetooth**: a short range communication technology which allows the data transfer between different devices within the same room using the star network topology. It offers a low power and low latency solution for IoT applications. Bluetooth operates in the 2.4 GHz band and uses *Frequency Hopping Spread Spectrum* (FHSS) technique to avoid

collisions or co-existence [64].

- **WiFi**: based on the IEEE 802.11 standard, used in different environments such as in public places, offices or homes. It operates in the 2.4 GHz and 5.6 GHz ISM frequency band and adopts the star network topology. Although it is considered as a non-efficient solution regarding its high power consumption, but it can be easily set and integrated with any technology in an IoT environment [64].

Cellular IoT

Cellular IoT (CIoT) standards operate in the licensed bands and take advantage of the existing cellular network coverage to enable Internet access to IoT devices. Having the network infrastructure already in place is a big benefit that speeds up implementation. EC-GSM, LTE-M, NB-IoT and 5G are three different standards that have been suggested [65]. EC-GSM was created to work with and improve earlier EDGE and GPRS systems in order to deliver improved coverage and range while using less power. LTE-M will work alongside LTE to take advantage of its capacity and performance while also introducing new power-saving features to extend device battery life. NB-IoT or Narrowband IoT set up by 3GPP, operates in the licensed frequency band and can be integrated into LTE standard. To ensure low power consumption, some of the LTE features are removed [66]. Finally comes the 5G technology which allows the possibility of massive IoT devices deployment within a network and the massive data processing & mining [67].

Low Power Wide Area Networks

2.3 LPWAN Technologies

For the IoT devices to communicate and transfer data, different wireless communication technologies and standards are available. In relation to IoT, Low-Power-Wide-Area Network (LPWAN) is regularly adopted. The main advantage of using LPWAN technologies in IoT

applications is the low power consumption solution these technologies provide to battery powered IoT devices. Different LPWAN technologies are available to be used in the IoT field such as LoRa, SigFox and NB-IoT. In this thesis, LoRa is used as the main IoT communication means, however a brief explanation of the different LPWAN technologies is given.

- SigFox: one of the LPWAN communication protocols designed for IoT applications. SigFox offers transmission of small amounts of data over long distances reaching a coverage up to tens of kilometers. SigFox operates and efficiently uses the unlicensed ISM (Industrial, Scientific and Medical) frequency band offering very low noise levels making it a power efficient solution for battery based IoT applications [68].
- Ingenu: a solution that involves the use of patented and proprietary technology for multiple access to the downlink channel called RPMA (Random Phase Multiple Access) and Direct Sequence Spread Spectrum (DSSS). It operates in the unlicensed ISM frequency band. It has the ability to increase its coverage range when needed by supporting multiple spreading factors.
- Telensa: LPWAN technology that operates in the unlicensed ISM frequency band. It offers low data rate transmissions and it is mainly used in smart cities especially in the deployment of smart lightning networks [69].

Table 2.1 shows the technical details of the different LPWANs IoT wireless technologies used.

2.4 Standardized LPWAN Technologies

In parallel with private commercial investments, plenty of standardization efforts in the IoT environment are promoted by various Standardization Bodies and Special Interest Groups such as Institute of Electrical and Electronics Engineers (IEEE), Third Generation Partnership Project (3GPP), WEIGHTLESS-SIG, European Telecommunications Standards Institute (ETSI) and DASH7 Alliance. All the proposed solutions fall in the category of the so called Low Power Wide Area protocols (LPWA) [70]. Table 2.2 summarizes the different technical specifications of the solutions created by the aforementioned groups.

Table 2.1: Comparison between the different LPWAN IoT technologies [1].

Communication Protocol	LoRaWAN	SigFox	Ingenu	Telensa
Frequency	868–870 MHz 902–928 MHz 915–928 MHz 470–510 MHz	200 KHz 868-869 MHz 902-928 MHz	2.4 GHz ISM band	868 MHz (EU) 915 MHz (US) 430 MHz (Asia)
Transmission Range	2-5 km (urban), 3-10 km (rural)	3-10 km (urban), 30-50 km (rural)	13 km (urban)	1 km (urban)
Data Rate	0.3-50 kbps	100 bps	78 kbps (UL), 19.5 kbps (DL)	62.5 bps (UL), 500 bps (DL)
Modulation	CSS	D-BPSK (uplink), GFSK (downlink)	RPMA-DSSS (UL), CDMA (DL)	UNB 2-FSK

Table 2.2: Technical specifications for standardization bodies and special interest groups IoT solutions [2].

Standardization Bodies and Special Interest Groups	Name	Modulation	Band	MAC	Data Rate	Coverage	Number of Channels
IEEE	802.15.4k	DSSS, FSK	ISM SUB-GHz & 2.4GHz	CSMA/CA, ALOHA with PCA	1.5-128 kbps	5 km (urban)	multiple (depends on channel and modulation)
	802.15.4g	FSK, OFDMA, OQPSK	ISM SUB-GHz & 2.4GHz	CSMA/CA	4.8-800 kbps	up to several kms	multiple (depends on channel and modulation)
Weightless-SIG	-W	16QAM, DBPSK	TV white spaces (470-790 MHz)	TDMA/FDMA	1 kbps - 10 Mbps	5 km(urban)	16 or 24
	-N	DBPSK	ISM SUB-GHz	ALOHA	30-100 kbps	up to 3 km (urban)	multiple, 200 Hz each
	-P	GPSK, QPSK	ISM SUB-GHz or licensed	TDMA/FDMA	200 bps - 100 kbps	up to 2 km (urban)	multiple, 12.5 KHz each
DASH Alliance	DASH7	GFSK	SUB-GHz	CSMA/CA	9.6,55.6 or 166.7 kbps	up to 5 km(urban)	multiple, 25 or 200 kHz each
3GPP	EC-GSM	8PSK,GMSK	Licensed GSM	TDMA/FDMA	74-240 kbps	up to 15 km	124 channels, 200 KHz each
	NB-IoT	QPSK, 16QAM, 64QAM	Licensed LTE	SC-FDMA (UL) OFDMA (DL)	20 kbps (UL) 200 kbps (DL)	35 km	multiple, 180 kHz each
	eMTC	QPSK, 16QAM, 64QAM	Licensed LTE	OFDMA/SC-FDMA	1 Mbps (UL,DL)	up to 15 km	multiple, 200 kHz each
ETSI	LTN	BPSK (UL) GFSK (DL) or OSSS	ISM SUB-GHz (433, 868 and 915 MHz)	BPSK (UL) GFSK (DL)	10-100 bps	up to 60 km	multiple, 200 Hz each

2.5 LoRa and LoRaWAN

LoRa is a new communication technology adopted in different M2M (Machine-to-Machine) and IoT applications. It gained a high interest due to the long range coverage it offers besides to its ability to operate in noisy environments [71]. In the following subsections, a detailed description about LoRa and LoRaWAN and the difference between them is presented.

LoRa

Long Range or LoRa is a physical radio protocol designed for IoT applications. This technology offers long range connectivity, low power consumption for IoT nodes and noise & interference robust solution. It uses Chirp Spread Spectrum (CSS) modulation technique making it more robust to noise where the signal is spread over a wider bandwidth thus reducing the Signal to Noise Ratio (SNR) and increasing the range. LoRa employs the unlicensed ISM frequency band which reduces the deployment costs, and a set of frequencies are reserved for each region as stated in [72] and as shown in Figure 2.3.

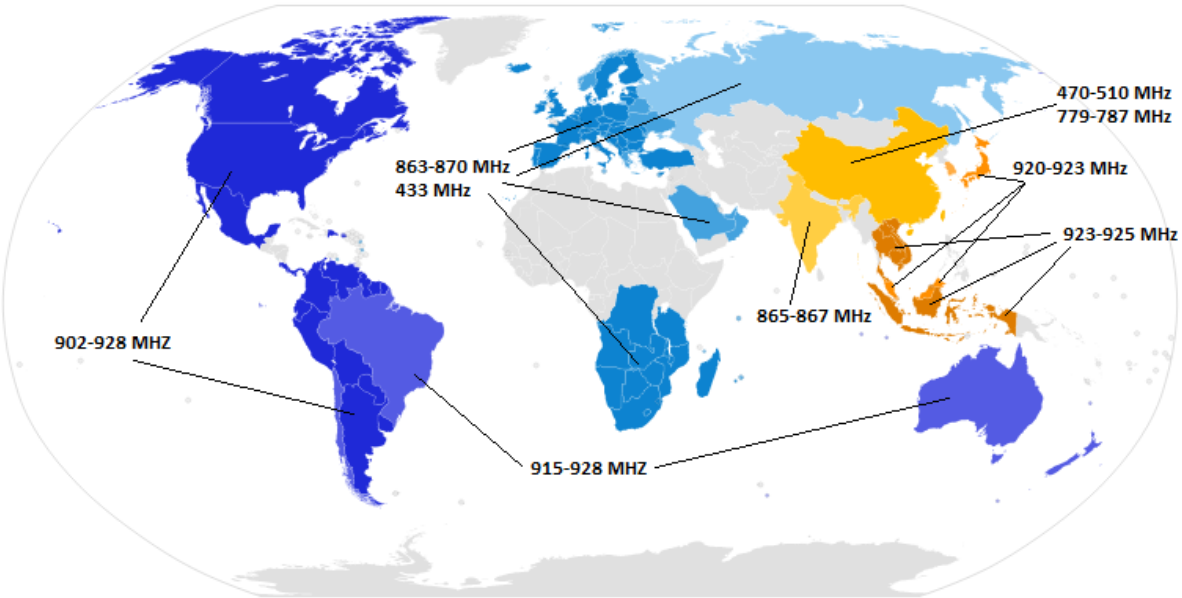

Figure 2.3: LoRa frequencies allocated in different world regions [72]. (the map is taken from TTN [73]).

LoRa Modulation

Generally, LoRa is a physical layer technology patented by Semtech [74]. LoRa is based on a proprietary *Chirp Spread Spectrum (CSS)* modulation which is considered as a useful technique in deploying a large network transmitting limited data payloads over long distances with low power improving the signal robustness against interferences, multi-path and Doppler's effect [75]. The concept of CSS is the use of frequency chirps in information encoding where the frequency varies linearly with time. In LoRa, two types of chirps are adopted: (i) base chirp and (ii) modulated chirp. The base chirp starts with minimal frequency ($f_{min} = -BW/2$) and increases linearly to the maximal frequency ($f_{max} = +BW/2$) where BW represents the spreading bandwidth of the signal. Such chirps are known as up-chirp and the inverse is called down-chirp that starts with $f_1 = +BW/2$ and ends with $f_2 = -BW/2$. On the other hand, the modulated chirp is cyclical time shifted base chirp. In brief, this modulation technique utilizes pulses having increased and decreased frequencies linearly over time, occupying a bandwidth (BW) of 125, 250 or 500 KHz.

Every symbol in a LoRa payload is encoded by 2^{SF} chirps, where SF corresponds to *Spreading Factor* and its value ranges between 7 and 12. SF is a tunable parameter that represents the number of bits used to encode a LoRa symbol. In other words, a LoRa symbol is composed of 2^{SF} chirps covering the whole frequency band, starting with a series of up-chirps known as the *preamble*. The preamble is followed by a *Syncword* which is 1-byte value used to distinguish the LoRa networks followed by 2.25 down-chirps followed by the LoRa payload as shown in Figure 2.4.

In addition, SF besides the BW, affects the data and symbol rate and is expressed in Equation 2.1 where *SR* corresponds to the symbol rate.

$$SR = SF \cdot \frac{BW}{2^{SF}} \tag{2.1}$$

This SF has a trade-off between the distance covered and the payload size, i.e., the lower the SF is, the highest the payload size (highest the data rate) the lower the distance covered is, and the highest the SF is, the lower the payload (lower the data rate) the highest the covered distance

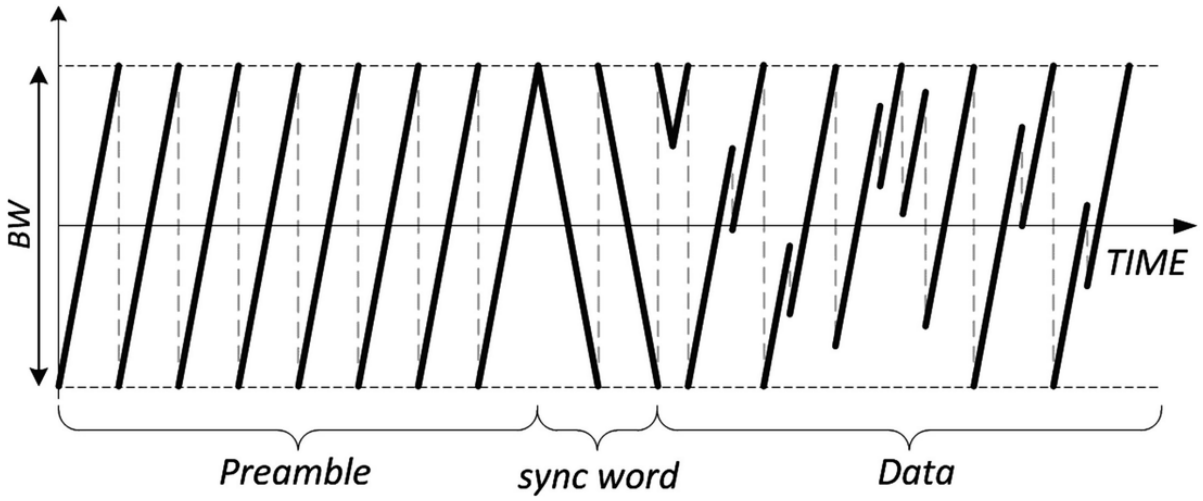

Figure 2.4: Transmission of the preamble and data in the time and frequency domains [76].

Table 2.3: Data rate for EU863-870 [3].

Data Rate (DR)	Configuration	Indicative Physical bit rate (bit/sec)
0	SF12/125 KHz	250
1	SF11/125 KHz	440
2	SF10/125KHz	980
3	SF9/125 KHz	1760
4	SF8/125 KHz	3125
5	SF7/125 KHz	5470
6	SF7/250 KHz	11000

is. This is summarized in Table 2.3 for the European configuration and it shows clearly that the increment in the data rate corresponds to a decrement in the SF.

LoRa Topology, Device Classes & OSI Layers

LoRa Topology

A LoRa network adopts the star-of-stars network topology and is formed mainly of four components: (i) end nodes, (ii) LoRa gateways, (iii) network servers and (iv) application servers where end nodes communicate only with gateways and not with each other. The LoRa gateways

are connected to the core of the network which is represented by the network server. These gateways are responsible of packets transmission from end nodes to network server using LoRa communication protocol. On the other hand, the network server transfers these packets using the standard IP technology to the application server, and in some times sends downlink messages and MAC commands back to end nodes [77, 78]. The resulting LoRaWAN network architecture is shown in Figure 2.6. The components of the LoRa network are as follows [79]:

- **End Nodes**: represents the LoRa embedded sensors which are composed of three main parts: sensors, LoRa antenna and micro-controller. The sensors are used to detect changing parameters from the surrounding such as temperature or GPS. LoRa antenna is used to transmit the data from the sensors and the micro-controller is utilized for sensor programming. These nodes are classified into three main classes: *Class A, Class B and Class C* depending on the application employed [80].
- **Gateway**: corresponds to the bridge that connects the sensors or IoT nodes to central element of the LoRa network.
- **Network Server:** the brain of the LoRa network which is responsible for controlling the whole network such as security, radio resource management. It de-duplicates the data packets received from sensors, routes them to the relevant application server.
- **Application Server:** it represents the device or end node inventory part, where the user is able to interact with the network through a web interface. It is responsible for join handling and payloads encryption/decryption. In other words, the application server do something with the data received from the network server.

LoRa Device Classes

In this subsection, a detailed description of the different classes of LoRa devices is given and a summary is reported in Table 2.4:

- Class A: the default class for all LoRa devices and considered the most power efficient device class among others. It allows a bidirectional communication where every uplink

message initiated by the device is followed with 2 downlink receive windows. In other words, the device sends an uplink message and waits for 1 & 2 seconds to receive a downlink message from the network server before going to sleep for acknowledgment purpose. This kind of devices is suitable for monitoring applications where data is needed to be collected by a control station.

- Class B: this class extends class A and allows additional receive windows at scheduled times. The concept of "synchronized beacon" is introduced where a beacon is required to be sent from the gateway to the end device allowing the network server to know when the device is in the listening mode. Such devices are used in applications which require to receive commands from a remote controller.

- Class C: the most power consuming class where it allows bidirectional communication with the maximal receive slots. The devices of this class are always awake and ready to receive any downlink message from the network server. These devices are perfect for applications that provide continuous power supply.

In brief, both LoRa and LoRaWAN technologies are represented in 2.5 where LoRa represents the physical layer (PHY) responsible for the wireless modulation used for creating long range communication link. However, LoRaWAN is the open network protocol responsible for delivering secure bi-directional communication.

LoRa OSI Reference Layers

The layered network design provides a comprehensive communication between different network elements. The LoRaWAN network layers can be mapped to the OSI model to better understand the underlying technology as presented in Figure 2.7. A typical LoRaWAN network involves multiple end nodes, one or more gateways and at least one network server to run and control the entire network. LoRa operates on layer one (L1) and its main function is to transmit application layer data to the medium. The second layer, the data link layer (L2), is compatible with the LoRaWAN protocol that defines a secure medium access and end node management techniques. The communication between the end nodes and the gateway is LoRa

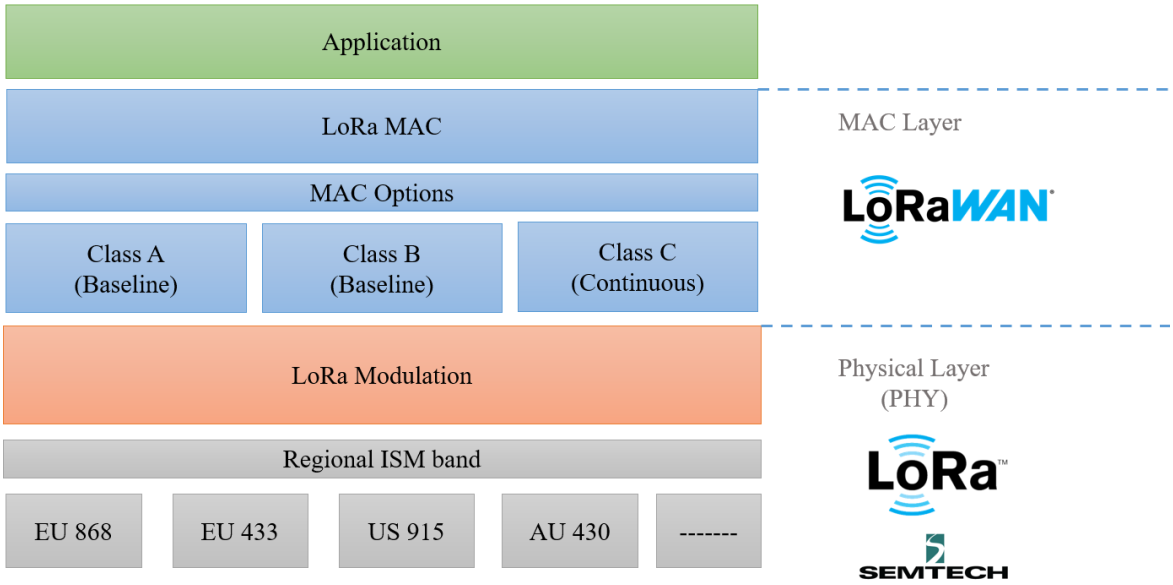

Figure 2.5: LoRaWAN technology stack.

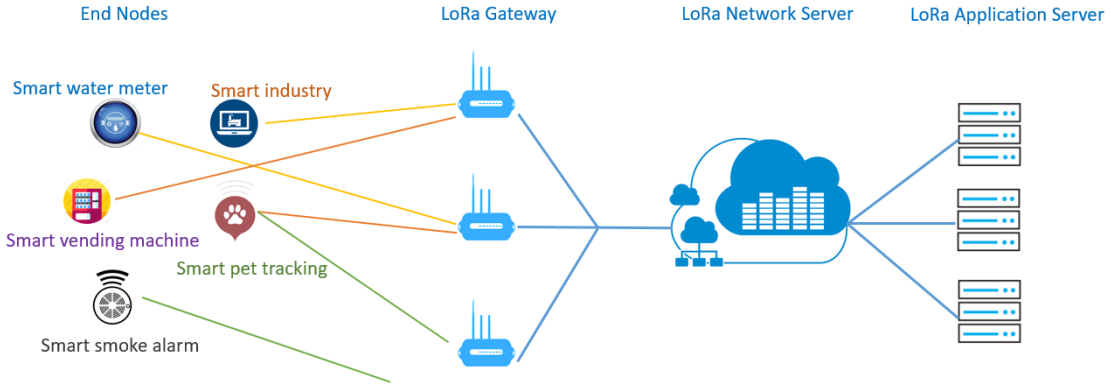

Figure 2.6: LoRa network architecture.

protocol, while the LoRaWAN network server and the gateway are separated with classical TCP/IP links. The network server is a simple application service that operates in the transport layer and is responsible of controlling all the MAC level functions of the entire network [78].

Table 2.4: LoRa classes summary [4].

Class A	Class B	Class C
Bidirectional communication	Bidirectional communication with scheduled receive slots	Bidirectional communication
End device initiates the communication	Server can initiate the communication at fixed intervals	Server can initiate the communication at any time
Uni-cast messages	Uni-cast and multicast messages	Uni-cast and multicast messages
Server sends downlink messages (acknowledgments) to end device in predetermined time windows	Opens extra receive window (ping slot)	End device is always open for receiving
Battery powered with sleep mode	Battery powered with low latency	Continuous power with no latency

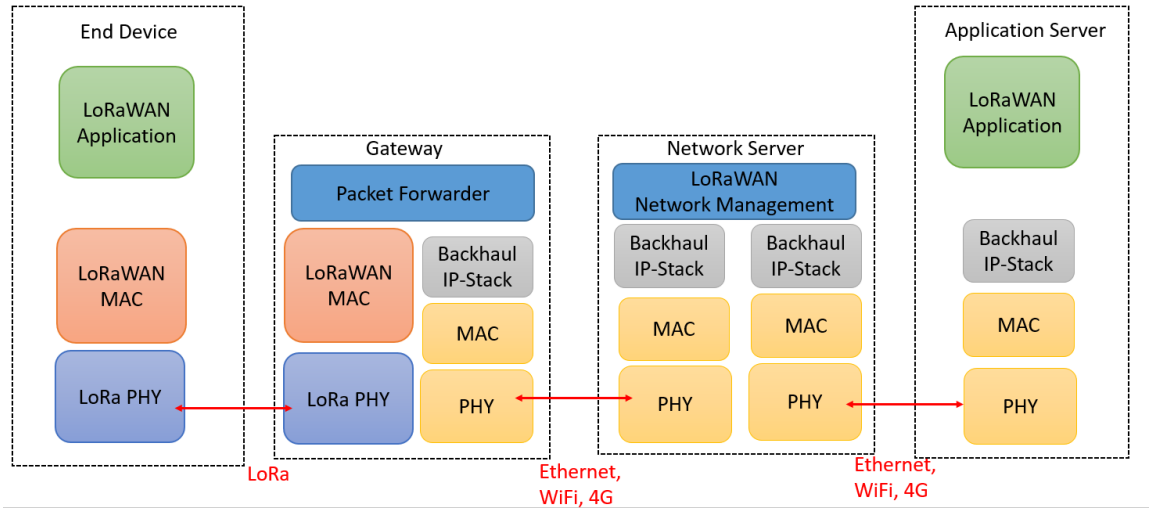

Figure 2.7: LoRaWAN protocol stack.

2.6 LoRa Security Features & Activation Process

As any wireless communication protocol, LoRaWAN has its own security features. LoRaWAN characterizes the confidentiality and integrity of the data transmitted between end

devices and servers. This is handled by the exchange of symmetric cryptography keys for encryption and decryption purposes [81]. For confidentiality, LoRaWAN uses a 128-bit application session key (AppSKey) for payload encryption between end devices and application server. On the other hand, for integrity LoRaWAN sign the messages exchanged with a *Message Integrity Check (MIC)* obtained from hashing the message with 128-bit network session key (NwkSKey). These two keys are derived from an initial key called the *root key* known by both the end device and the network server. These aforementioned keys are used in the activation process carried by the end device to join a LoRaWAN network [82]. LoRaWAN initial specification v1.0 [83] (and next specifications) defines two activation procedures to obtain the keys for ensuring security.

Over The Air Activation (OTAA)

Over The Air Activation or OTAA is the remote activation of end devices upon joining a LoRaWAN network. It is considered the most secure activation process because the end device requests to join the network every time it wants to. In OTAA, an end device sends a *Join Request* message to the network server including Device Unique Identifier (DevEUI), Application Identifier (AppEUI) and Device Nonce (DevNonce). The DevEUI is a global unique identifier associated with each end device, AppEUI is a unique identifier that identifies the entity which is able to process the Join-request and DevNonce is a unique and random value generated by the end device used by the network server to track the device. An AppKey shared between both the end device & the network server, is an AES-128 root key used for calculating the MIC that is used for signing the join request message which is not encrypted. When received by the network server, it checks if the end device is authenticated using the MIC, DevEUI and AppEUI then forwards it to the respective application server. The response to this join-request message can be rejected or accepted. If rejected by the application server, the end device will not receive any response and the process will be terminated by the network server. However, when the join-request is accepted by the application server a *join-accept* message is sent to the end device by the network server. This join-accept message includes different parameters used in deriving

the Network Session Key (NwkSKey) and Application Session Key (AppSKey) used in MAC commands encryption/decryption and payload encryption respectively. The *AppNonce* is given to the end device by the network server and used for AppSKey and NwkSKey generation besides the AppKey, and sends the AppSKey to the application server too, hence the activation process in accomplished. The overall OTAA procedure is represented in Figure 2.8.

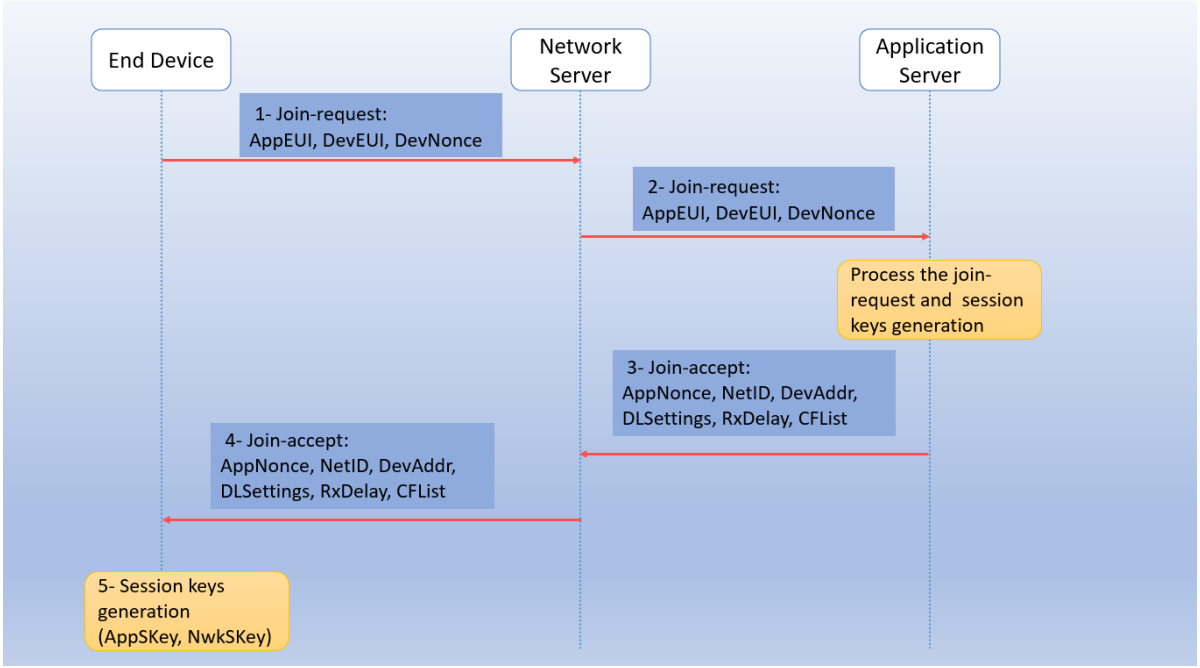

Figure 2.8: Message flow for Over-The-Air-Activation (OTAA) in LoRaWAN v1.0.x.

This OTAA activation is followed by devices that support LoRaWAN 1.0.x versions. In LoRaWAN v1.1 [84], a new server is introduced called *"Join Server"* [85, 86]. The main purpose of this server is to orchestrate the activation process in a more secure way. Another difference is the presence of three network servers instead of a single one as in previous versions: the *home, forwarding and serving* network servers. For the activation process, new parameters are included which are: *JoinEUI* and *DevEUI*. JoinEUI is a unique identifier for each end device used to identify the join server that will assist the join procedure and session keys generation and it must be stored in the end device, and DevEUI is a unique identifier for each end device required by the network server to identify the device roaming across the network. Beside these two keys, the AppKey and NwkKey must be stored in the end device too before activation.

Both AppKey & NwkKey are AES-128 bit secret root keys used for AppSKey derivation and Forwarding Network Session Integrity Key (FNwkSIntKey), Serving Network Session Integrity Key (SNwkSIntKey) & Network Session Encryption Key (NwkSEncKey) session keys generation respectively. The FNwkSIntKey is used for MIC calculation of all the up-link messages for data integrity purpose, and it is a public network session key shared with the forwarding network server. However, the SNwkSIntKey is a private session key used for MIC calculation of all downlink messages for ensuring data integrity and not shared with the forwarding network server. Finally, the NwkSEncKey is also a private network session key used for encryption and decryption MAC layer commands or the payloads. The OTAA process begins when the end device sends a *Join-request* message to network server containing: (i) DevEUI, (ii) JoinEUI and (iii) DevNonce. This message when received by the network server, it lookup the IP address of the join server using DNS based on the JoinEUI included in request message. If the lookup succeeds, the network server forwards a back-end message to the join server including these parameters:

1. PHY payload of the join-request message
2. MAC version
3. DevEUI
4. DevAddr which is a 32-bit address allocated to each end device by the network server.
5. DLSettings which is a 1-byte field size consists of the downlink settings that the end device have to use.
6. RxDelay corresponds to the delay between TX and RX.
7. CFList is a list containing channel frequencies to be used for the end device.

After the successful processing of this join request message by the join server, it sends back to the network server a JoinAns message containing the following:

1. PHY payload with Join-accept message

2. Network session keys
3. Serving Network session integrity key (SNwkSIntKey)
4. Forwarding Network session integrity key (FNwkSIntKey)
5. Network session encryption key (NwkSEncKey)
6. Encrypted AppSKey which the network server can not read.

The network server prepares this join accept message and encrypts it using the NwkKey and forwards it to the end device. After the success of the activation step, the end device calculates the MIC, then generates the NwkSKey and AppSKey and starts sending data packets to the application server. When the network server receives an uplink message from the end device, it sends both the DevEUI and the encrypted AppSKey with the application payload. The application server will decrypt the AppSKey using a secret key shared between the join server and application server and then uses this AppSKey to decrypt the payload. This detailed description of the OTAA in LoRaWAN v1.1 is summarized in Figure 2.9.

Activation By Personalization (ABP)

Activation By Personalization or ABP is an end device activation process to an existing LoRaWAN network. It works on tying the end device directly to a pre-selected network avoiding the join procedure carried in OTAA case. ABP is considered to be less secure compared with OTAA because the keys used are not changed every time the device joins the network. Unlike OTAA, the DevAddr, NwkSKey and AppSKey are directly stored in the end device instead of DevEUI, AppEUI and AppKey. In addition, the DevAddr and NwkSKey are stored in the network server and the AppSkey is stored in the application server. Note that if an end device is activated using this method, it can communicate only with a single network keeping the same security session keys for its entire life.
On the other hand, in LoRaWAN v1.1 ABP is almost the same, however introducing three new network session keys stored in both the end device and the network server which are: (i) FNwkSIntKey, (ii) SNwkSIntKey and (iii) NwkSEncKey.

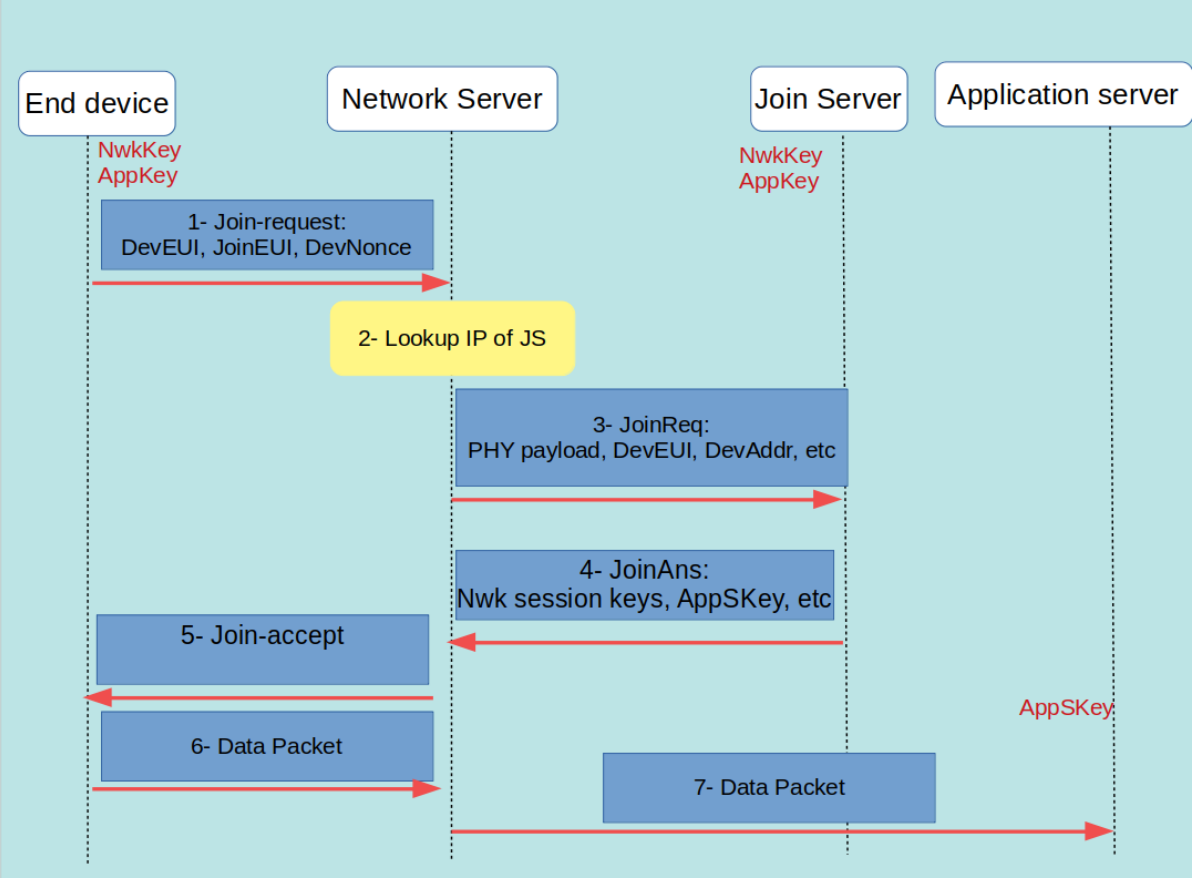

Figure 2.9: Message flow for Over-The-Air-Activation (OTAA) in LoRaWAN v1.1.

2.7 LoRa Applications and Use Cases

This section summarizes the different applications and use cases where LoRa is considered as a major player besides the use of UAVs and satellite communications. For this purpose, this section is divided into two main subsections: (i) *LoRa Applications* focuses on the different researches and studies carried on the integration of LoRa as a communication protocol in any IoT network and (ii) *LoRa in Smart Grids* focuses on the deployment of LoRa in smart metering and smart grids along with a possible approach for integrating LoRa, UAVs and satellite with the smart metering systems.

Table 2.5: Comparison between OTAA and ABP.

OTAA	ABP
More secure	Not secure
Session keys are renewed regularly	Session keys are personalized and stored in end device during fabrication
End devices need to perform the join procedure	Join procedure is skipped
End devices can dynamically and securely switch between networks	End devices are tied to a specific network

LoRa Applications

With the great interest LoRa is witnessing in the IoT field, different studies have been carried on focusing on the usage and performance of LoRa in various applications. Various papers are presented in the literature where LoRa has been integrated as the IoT protocol or compared with other IoT protocol. Table 2.6 summarizes some of the different applications where LoRa has been deployed.

LoRa in Smart Grids

Focusing on the domain of smart grids and smart metering, IoT technologies are considered as an effective technology for different smart grid applications. IoT communication solutions can, on one hand, allow data gathering, processing, and exchange among different physical elements or components of the smart grid [93–98], while, on the other hand, improve the smart grid abilities, such as warning, disaster recovery, and reliability. It is considered to be a reliable mean of data transmission whether wired or wireless through different smart grid parts. IoT can be deployed to monitor power generation, energy storage, energy consumption, transmission lines and substations, and can be installed on the customer side smart meter for consumption measurement and energy management purposes [99].

Table 2.6: Summary of some studies using LoRa as IoT communication protocol.

Paper Reference	Application Domain	Brief Description
[87]	Environmental Monitoring	The research adopted LoRa besides 2G as communication protocols for the revival of rural hydro-logical control systems.
[88]	Healthcare	IoT healthcare monitoring system developed using MySignals platform adopting LoRa as the IoT communication protocol.
[89]	Tracking & Monitoring	Tracking or location finding system for indoor or outdoor applications adopting LoRa protocol.
[90]	Smart Homes	Analyze and predict application's performance allowing the distribution and management of the computation process.
[91]	Industrial	Simulated model using LoRa and LoRaWAN for industrial monitoring purpose.
[92]	Agriculture	LoRa adopted as the best alternative of the different IoT communication protocols to develop an agricultural monitoring system.

Several studies investigated the possible employment of these IoT-thought solutions in the smart grid scenario: the LPWAN category [2]. Thanks to its guaranteed low power consumption, achievable long transmission range, and ensured security and data protection through encryption, the solutions of this category seem of special interest in this context. A detailed description of the architecture of the Chinese smart grid when integrating IoT communication technologies is given in [100], also presenting some applications where IoT solutions can be of great benefit, such as for online monitoring of power transmission lines, smart patrolling, smart home services, and electric vehicle management. An overview of smart grids and of the different applications and services where IoT is integrated into smart grid is

provided in [99]. The integrated architecture is also presented concerning the necessary requirements of privacy, security, and reliability. LoRaWAN is used as a highly reliable communication technology for a smart grid installed in a rural area due to the coverage limitations of the cellular network in [101]. Supporting the Green Bali Provenance Program, authors in [102] evaluate the communication solutions belonging to the LPWAN category to deploy two-way communication smart meters replacing pre and postpaid digital ones. The performance results suggest the adoption of LoRaWAN, thanks to its low implementation cost, low power consumption, device availability, long distance coverage, and frequency allocation. Authors in [103] also evaluates the LoRa protocol performance deploying one gateway and several smart meters distributed over a 9-floors building. The results show that a single gateway is enough to receive data from thousands of smart meters. An application that uses EnergyHive [104] as energy platform is presented in [105]. Such a system consists of about 300 properties, each equipped with a smart meters connected through WiFi and a tablet to display the energy consumption in real-time. smart meters are used to provide automatic energy management through real-time consumption monitoring ability and report generation. IoT technologies use the information from smart meters to adjust the energy consumption within the building. The achievable performance of LoRaWAN in rural smart grids has been investigated in [106] by deploying the smart grid over an area of 4000 square kilometers and offering electric power to about 200 consumers. The obtained results show the importance of sending small data payload packets to avoid long latency. LoRaWAN is used as a communication protocol to transmit the data generated by smart meters in [107]. The aim is to study the QoS that the LoRaWAN solution can provide in a crowded city like Paris. The performance analysis shows good results in terms of guaranteed QoS but the network capacity decreases when both uplink and downlink communications are considered. The role of IoT communication is extended to overcome the problem of voltage regulation when deploying distributed energy resources. The authors in [108] presented an IoT model for voltage regulation by using sensors and actuators installed on micro-grids and 5G cellular communication to transfer the information about the grid status.

On the other hand, IoT in the domain of smart metering applications has been emerging as a

research field. Some studies were conducted by using IoT-based communication technologies in the field of power management. An IoT architecture has been adopted in [109] for the implementation process of a model predictive control of Heating Ventilation and Air Condition (HVAC) systems in smart buildings. The implemented system uses different sensors and actuators connected to a gateway by using ZWave and ZigBee communication protocols. The system is connected to a database via MQTT to allow the users to remotely control it. a management system to control the increasing energy demand-response due to the growing spread of IoT-enabled smart homes is proposed in [110]. An improvement of the IoT-enabled smart home sustainability is guaranteed by following a strategy which controls and manages the power consumption during peak times, reduces the power cost, and increases users comfort. An Energy Management System (EMS) to monitor domestic devices energy consumption and utilization is presented in [111]. The authors adopt a stochastic-based scheme to save energy in smart grid applications, which can be extended to cover all IoT components in a smart city. An Intelligent Smart Energy Management System (ISEMS) is introduced in [112] to handle the increasing energy demands in smart grid environments and to accurately predict energy consumption by using machine learning prediction models.

Different applications in smart metering systems based on the LoRaWAN solution have been deployed in the field, not necessarily linked to smart grids:

- Water Grid Transformation-Birdz [113]: a smart water metering network with LoRaWAN-based sensors has been deployed in France. The integration allows the utility to collect data more efficiently and control operations to reduce costs. This implementation provides a flexible deployment of sensors, such as water leak detectors and water quality probes, which can send and receive messages through a two-way communication network. Significant benefits have been obtained such as identification and faster repair of about 1200 water leaks in the distribution network. It allowed saving 1 million cubic meters of water on an annual basis.

- Nationwide Smart Metering [114]: a unique energy control system based on LoRaWAN devices has been developed by a Czech communication company in cooperation with a

technological start-up. This system collects real-time data from electrical meters installed in houses and industries and allows users to check their usage by using a smartphone application.

- Creating Energy Efficient Buildings [115]: a company in China developed a system to monitor their utility buildings through LoRaWAN-based devices. Building owners and managers can monitor usages and tune consumption in order to reduce waste.

- Energy Management and Smart Lighting-OrionM2M [116]: a lighting system based on LoRaWAN networks to access the cloud has been developed in Kazakhstan. This connectivity enables reliable transmission of data, reduces the cost, and creates a more efficient lighting system.

Possible Smart Metering System Evolution

Our Envisioned System

Among the different communication solutions discussed in Section 2.2, there could not be a ”best” solution. The most suitable one may depend on many factors, including the already present infrastructure, the geography of the areas, and the functionalities that the Distribution System Operator (DSO) wants to implement.

Our vision of possible future evolution of the smart metering system is based on the employment of IoT protocols and in particular the LPWAN ones. This solution is mainly based on the equipment of LPWAN solutions on the smart meters. In this way, information exchange from and to smart meters can be achieved both in urban and rural scenarios at low implementation cost.

The overall smart metering system can so be composed of two main possible scenarios depicted in Figure 2.10:

- Scenario A: Smart Metering in Urban Areas
  Fixed LPWAN solution gateways are deployed in specific locations aims to minimize their number while covering all the present smart meters. These gateways are directly

connected with the smart meters receiving/forwarding data from/to them. These nodes can also be equipped with high-computational and storage capabilities, exploiting the Mobile Edge Computing (MEC) paradigm, in order to allow them performing data analysis and processing at the edge of the network. In this way, the system can avoid forwarding the raw data to the end utility and allow the implementation of the mentioned additional functionalities closer to the user and the distribution portion of the network reducing the latencies. Another interface will allow processed data to be forwarded to the central End Utility nodes through the Internet exploiting more traditional communications solutions such as Fiber Optics or Cellular Network.

- Scenario B: Smart Metering in Remote Areas
  Many areas are rural and remote areas with low population density. In such areas, the deployment of fixed LPWAN gateways would be cost-inefficient. Besides, considering they could be out of coverage of all other traditional communication technologies, the links between the gateways and the End Utility centers could not be easy to establish. To solve this issue, we propose the use of UAV equipped with LPWAN gateways. In this way, UAV can be easily deployed in the areas to cover, establish bidirectional communications with the smart meters, and proceed with the data exchange, acting as moving LPWAN gateways. Satellite communication solutions can offer the missing link between UAV and End Utility centers thanks to their envisioned future worldwide coverage. Another viable solution could be to allow the UAV to operate as ”data mule”, i.e., collect the data while are flying above the rural area, store onboard the data and then proceed to forward them only when they come back to their starting point. This second solution is less expensive than the first one even if it cannot guarantee direct end-to-end connectivity between smart meters and End Utility centers. The inclusion of data server at the edge is also possible in this second scenario even if the most feasible locations could be the UAV or, considering the limited available resource onboard the UAV and maximum payload weight limitations, the satellite ground stations.

In urban areas, LPWAN can be a practical, low cost, low energy consumption, and easy

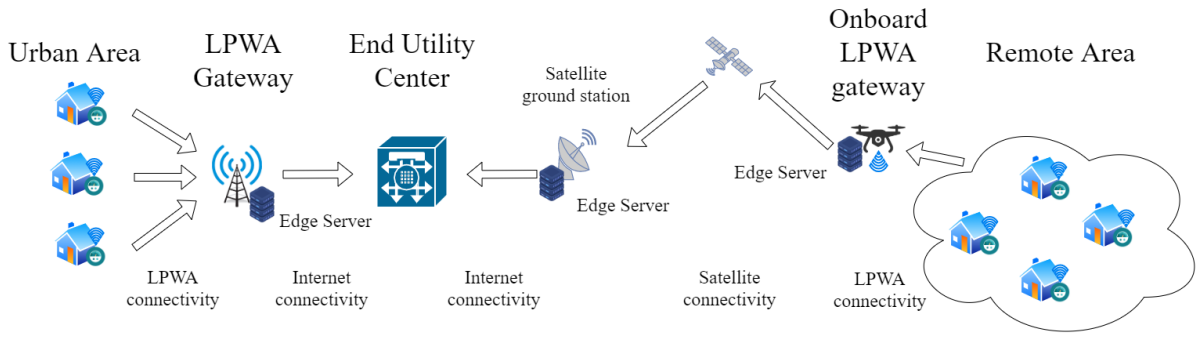

Figure 2.10: Proposed smart metering system architecture integrating IoT communication and MEC paradigm.

to deploy solution. It does not require a deep modification of the smart metering system and it would exploit the Internet infrastructure to forward data to the End Utility Centers instead of using an ad-hoc infrastructure. However, high smart meters density and the high interference typical of an urban scenario are the main drawbacks that could lead to different solutions employing more traditional communications means, more expansive but more able to guarantee the performance and security requirements. Anyway, the concept of exploiting the MEC paradigm at the gateway nodes and the Internet infrastructure is still valid.

In rural and remote areas, the proposed approach is very practical and cost effective. UAV flight path and frequency may depend on the structure of the area to cover, on the locations of the smart meters, and on the different needs. Energy measurements as frequent as in urban areas may not be feasible but it will be anyway a considerable improvement compared to the Manual Metering Reading (MMR) case, currently adopted in almost all rural areas. Moreover, in the data mule solution, UAV can be easily moved through different environments, but different moving objects can be also employed for this purpose, such as cars, taxis, and busses, as has been already proposed in other data communication initiatives [117–120].

The employment of the MEC concept in both urban and rural areas is the turning point to enable all the mentioned functionalities and make the future smart grid able to manage the higher amount of generated information traversing the all infrastructure and satisfy the user higher performance requirements offload part of the computation load from the End Utility Centers to the Edge Servers. This allows reducing network load and bandwidth utilization,

enhancing service performance, and decreasing the overall system delay.

The exploitation of Internet infrastructure is a further improvement. In this way, there is no need anymore of an ad-hoc infrastructure with the related periodic maintenance and upgrade costs. There are already Internet application protocols able to guarantee the needed security requirements and solutions to guarantee enough bandwidth to satisfy both users and DSO performance requirements.

Moreover, the applicability of the proposed solution may not be limited only to smart meters. Other entities of the smart metering system, belonging to all the portions of the smart grid infrastructure, can benefit from the employment of IoT communication protocols and the presence of flying UAV to send and receive data. Control messages from transmission lines, alerts from distribution substations, security and condition checks from multiple distributed power generation locations are just a few examples of the data that DSO and Transmission System Operator (TSO) could easily and efficiently collect thanks to the proposed approach.

2.8 Conclusion

In this chapter a detailed explanation about IoT, IoT communication protocols and LoRa/LoRaWAN is introduced. In addition, a brief and detailed example of how IoT in general, and LoRa in specific can be deployed in a smart grid and smart metering systems.

Chapter 3

Proposed Solution and Testbed Description

Summary

Chapter 3 includes the main aim of integrating flying objects with IoT. In addition to a detailed description of the testbed developed for testing and studying the feasibility of the different approaches described in this thesis.

3.1 Introduction

Due to the increasing number of connected devices and volume of exchanged data, an evolution in the communication solutions is witnessed. Different communication technologies and protocols have been adapted or developed ad-hoc to be suitable for the typical traffic features and performance requirements of the IoT applications. However, the current communication infrastructure and wireless communication technologies are not always able to guarantee a proper service to all of these IoT applications, for example in terms of a proper connection user density and a suitable coverage area extension. Non-terrestrial networks are expected to play a key role in communication networks in general, and IoT networks in

specific. Satellites, drones or UAVs are examples of non-terrestrial networks that extend the coverage of traditional terrestrial and IoT networks to reach remote and rural areas. Moreover, these actors are expected to be part of the upcoming 5G infrastructure [121].

Considering the case of UAVs or drones, when integrated with IoT networks they can be seen as *"mobile networks"*. Such mobile networks are able to move to more than one area, extend the terrestrial networks when needed and overcome the problem of installing new terrestrial infrastructure. In other words, these actors are able to dynamically and temporarily extend "on-request" the current terrestrial infrastructure to allow collecting data generated by nodes outside the current network coverage. When integrating both flying objects and IoT a new research domain is present known as *Internet of Flying Things* and is noticing a great attention and interest. As stated in the *Introduction* previously, the main aim of this work is to extend the coverage of LoRa IoT network to be able to reach remote and rural areas. Taking benefit of the growth and integration of drones in different applications, drones or UAVs are adopted for extending the LoRa coverage.
Our proposed solution for this new research domain is to implement a flying LoRa gateway acting as: (i) *LoRa gateway* as explained in Chapter 4 and (ii) *LoRa data mule* presented in details in Chapter 5 where both have the purpose of data collection from remote and rural areas. Moreover, satellite communication has been integrated within the proposed solution to test and examine its performance and feasibility in accessing areas out of coverage of any communication means.

3.2 Testbed Developed

To test the different proposed solutions whose aim is to extend the LoRa coverage, a LoRa special testbed has been developed. This testbed is composed of different components which were configured and set for this purpose. The developed testbed consists of:

- **IoT devices** or **IoT nodes**: the LoRa sensors or nodes are based on special Arduino board that belong to the MKR family. MKR WAN 1300 board which offers LoRa

connectivity and is shown in Figure 3.1. This board has been designed to offer a piratical and cost efficient solution for developing an LoRa based IoT node. It is based on Atmel SAMD21 Cortex-M0+ 32 bit low power ARM micro controller and Murata CMWX1ZZABZ which comprises a Semtech SX1276 ultra long range spectrum wireless transceiver. It is designed with the ability to be powered by using batteries. Two LM35 temperature sensors are associated to these MKR boards for data generation through sensing the surrounding environment temperature. 868 MHz LoRa antenna is connected to each board used for data transmission from the sensor to the gateway. The overall LoRa IoT node is shown in Figure 3.2.

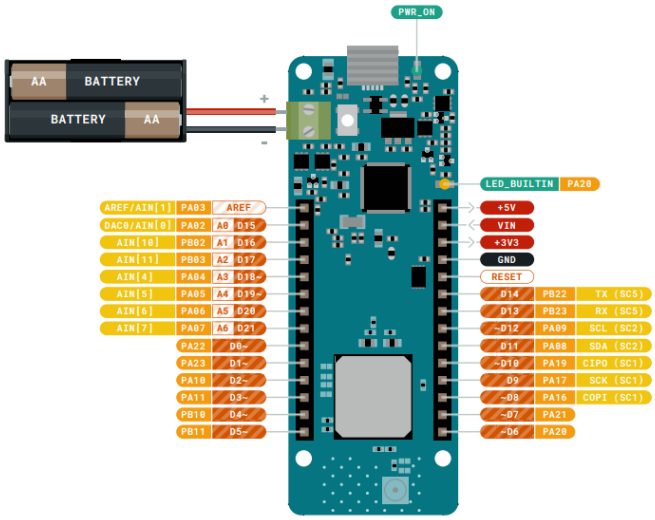

Figure 3.1: Arduino MKR wAN 1300 board scheme [122].

- **Main LoRa Gateway**: the gateway corresponds to the most important component of the LoRa testbed. This gateway is based on Raspberry Pi 3B+ single board computer. This board is equipped with a particular shield called *RAK 2245* shield represented in Figure 3.3. The gateway supports eight LoRa channels and is available for the different LoRa frequency bands, providing low data rate LoRa radio links in ultra fast speed. This Rak 2245 Pi HAT is considered as a complete, power and cost efficient gateway solution

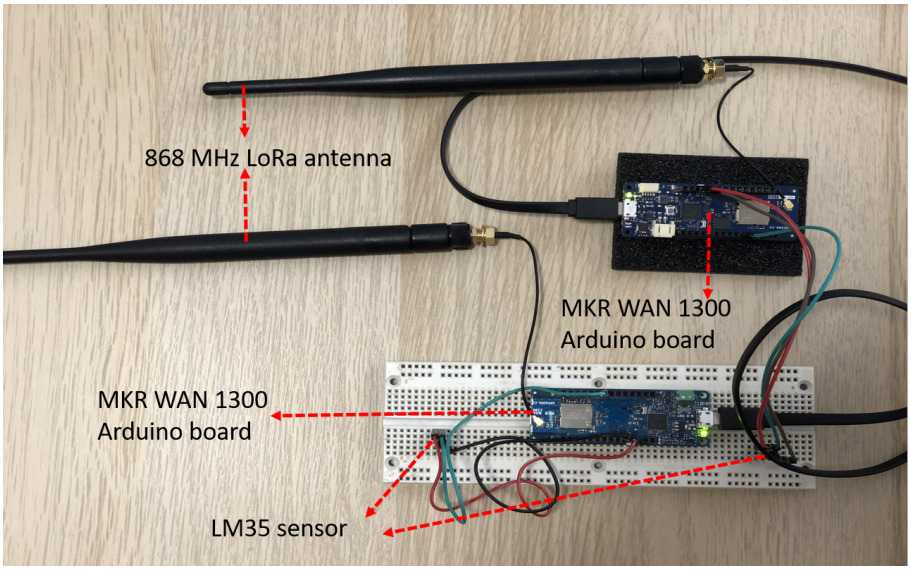

Figure 3.2: IoT LoRa node composed of: MKR 1300 Arduino board, LM35 temperature sensor and 868 MHz antenna.

which contributes in building and developing a full LoRa system. The complete LoRa gateway is given in Figure 3.4.

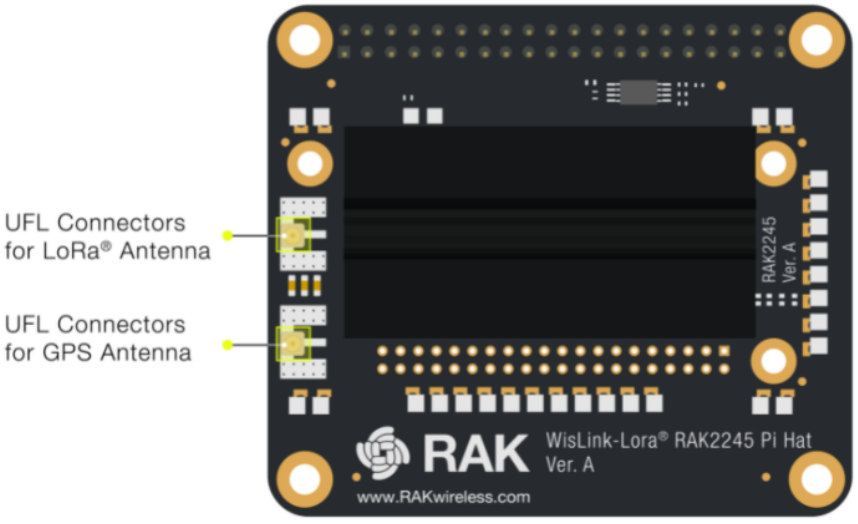

Figure 3.3: RAK2245 Pi HAT LPWAN shield [123].

Figure 3.4: LoRa gateway.

- **LoRaWAN Server**: the core LoRa element in the system. It corresponds to the network and application servers. LoRaWAN network server enables the connectivity and management. In addition, it is responsible for devices, gateways and user application monitoring. The network server main aim is to ensure security, scalability and reliability of data routing in the network. On the other hand, LoRaWAN application server is responsible for handling the LoRaWAN Application layer including uplink data decryption and decoding, in addition to downlink data encoding and encryption. Different LoRaWAN servers are present: (i) *The Things Networks (TTN)* and (ii) *ChirpStack* which have been used in the two approaches respectively. TTN represents the public cloud LoRa server whereas ChirpStack corresponds to an open-source private LoRa server.

- **Current Sensor**: an INA219 DC current sensor is used for monitoring the power consumption of the gateway. It saves the reading of the current, power, and voltage consumption of the gateway. This sensor was installed between the gateway and the battery pack allowing it to read the current consumed by the gateway. This current sensor was configured and programmed by using an attached Arduino board. The current data is saved in the raspberry pi memory through its serial port.

- **Drone**: A DJI Phantom drone has been used for performing outdoor tests, by which the gateway is attached on board this drone. This drone in given in Figure 3.5.

Figure 3.5: DJI Phantom drone with LoRa gateway attached..

3.3 Network Architecture

The network architecture of the proposed solution is similar to that described and explained in Chapter 2, Section 2.5. The proposed solution network architecture is represented in Figure 3.6. The difference is with the *Network Server* used that depends on the role of this flying gateway. A brief description of these two network servers is given as follows:

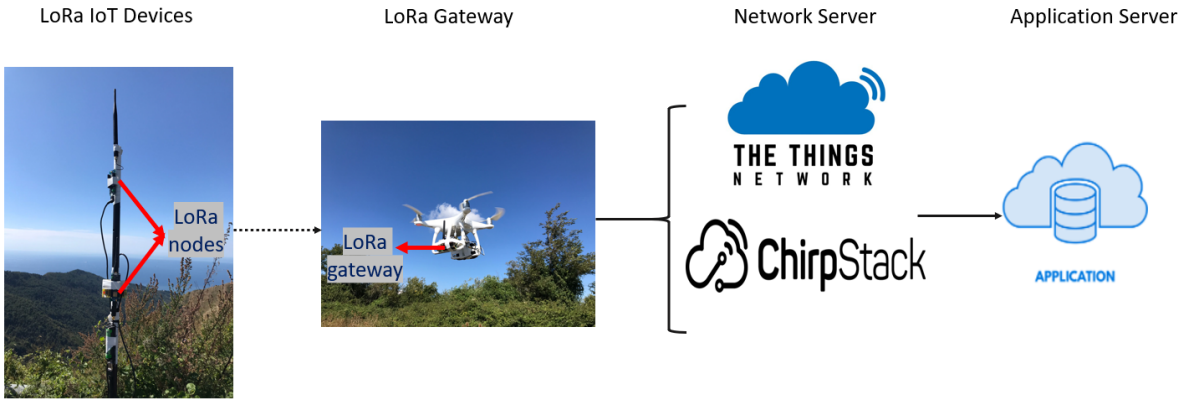

Figure 3.6: Network architecture of the proposed solutions.

1. **The Things Network (TTN):** TTN is a global open source cloud LoRa & LoRaWAN ecosystem. It allows the creation of networks, devices and solutions using LoRaWAN technology. Since the end devices shown in Figure 3.6 support LoRaWAN, a conversion from non-IP protocol to IP protocol is needed before forwarding the data packets to an application. This is carried out by the TTN and called "*Protocol Translation*", where it is responsible for routing and processing the data received from the LoRa gateway and forward it to its application. Moreover, the TTN LoRaWAN network server is responsible for the management and monitoring of the LoRa devices deployed along with the gateways, assigning addresses to each device, mapping the messages to the correct devices and application, processing uplink & downlink message flow and security keys management for encryption & decryption purposes [124].

2. **ChirpStack:** an open source LoRaWAN network server which provide a *standalone* LoRa platform. It allows the creation of a private LoRaWAN network with all its components, moreover it allows the installation of all these components on the gateway itself. It is responsible for the data routing, data format conversion to IP like format, de-duplication of received LoRaWAN frames, uplink & downlink frames scheduling and ensure the security through the network by security keys management [125].

3.4 Conclusion

IoFT is an emerging concept which is attracting the attention of both research and commercial activities. The integration of UAV in the IoT field leads to multiple advantages for the data collection aim. Some of the new emerging scenarios, especially the ones involving rural an remote areas without any kind of terrestrial infrastructure, can benefit from a flying and deployable on-demand solution to allow gathering all the data generated by multiple IoT devices spread in wide areas. In this chapter, a detailed explanation about the proposed solutions which adopt the concept of IoFT is presented. In addition, the testbed developed has been introduced with an explanation of each component in the LoRa network.

Chapter 4

LoRaWAN and Satellite Communication

Summary

This chapter presents the integration of IoT with satellite communication through simulation. The main aim is to integrate the LoRaWAN flying gateway with satellite communication to better reach remote areas with no Internet coverage.

4.1 Motivation

As stated before, the prominent evolution that happened with the Internet during the past decade is the Internet of Things (IoT). Smart grids, environmental monitoring and emergency management are examples of applications and use cases of IoT that require continuous connectivity. However, these applications are usually installed in remote areas with limited connectivity, and require the deployment of large number of devices with low power constraints distributed over a wide geographical area. Satellites, in such scenarios, play an important and critical role to overcome the connectivity problem. IoT and satellites are rarely integrated together in the communication world, but to meet the special demands of such

applications the IoT and satellite conjunction is required. Satellite communication is considered as a key communication technology since it offers the most reliable communication technology compared to the different wireless communication technologies. In traditional wireless technologies, such as cellular networks, do not provide the required reliability in such critical applications. Satellites provide 99.9% availability with the proper arrangements of constellations, and hence ensuring the higher reliability despite the environmental and diverse conditions. Moreover, normal cellular networks have limited coverage range especially in remote and rural areas. IoT networks deployed in such areas will suffer from poor connectivity issues causing problems in the IoT applications. On the other hand, satellite networks provide wider area coverage offering real time connectivity for IoT networks in remote and rural areas [126]. Since satellite networks have wider coverage than cellular ones, IoT networks deployed in remote areas need much less communication resources to that of cellular IoT networks. Figure 4.1 shows a satellite based IoT network where the IoT network falls within the coverage area of the satellite.

The integration of Low Earth Orbit (LEO) satellites in some IoT applications is becoming a new trend. Instead of using Geostationary Earth Orbit (GEO) satellites, LEOs are used as they provide lower propagation delays and lower losses. LEO satellites can be used as a powerful supplement for the IoT especially in, but not limited to, remote areas, due to the lack of proper coverage of the traditional terrestrial networks. To solve the problems related to remote sensing, such as the increasing system cost and the information analysis complexity, a LEO constellation-based IoT system is a possible solution. It will allow direct access to the information monitored by different types of sensors, ensuring more frequent data gathering than using a single sensing satellite and enhancing the prediction accuracy.

4.2 Reference Scenario

In this framework, the scenario we have decided to focus our attention is the typical smart agriculture one and it is depicted in Figure 4.2. A satellite link is simulated to study the

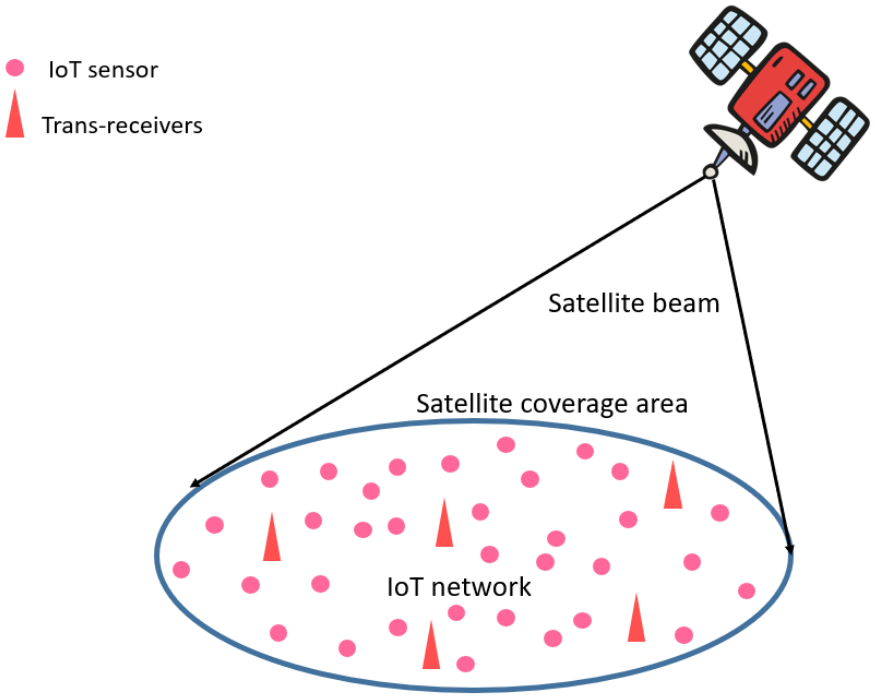

Figure 4.1: Satellite based IoT network: sensors are deployed under the coverage area of the satellite and the trans-receivers are for data transmission.

feasibility of including satellite communication with LoRaWAN and to monitor the behaviour of the network.

There are some sensors of different kinds deployed in a wide area not covered by other terrestrial access technologies. Each sensor is equipped with a LoRaWAN transmission interface and they are all connected to a LoRaWAN gateway located within the maximum achievable transmission range (up to 15 km in rural areas). In our case, the LoRaWAN gateway is located on-board a UAV which keeps collecting data while flying above a certain area. To guarantee end-to-end connectivity, the UAV is connected to the Internet through a satellite link, which can be considered always active. In this way, each sensor periodically senses the environment generating one temperature, humidity, atmospheric pressure, or another kind of measurement which is received by the UAV-gateway and forwarded through a satellite until it reaches a LoRaWAN cloud platform, where an user can see it just opening a browser in his/her device.

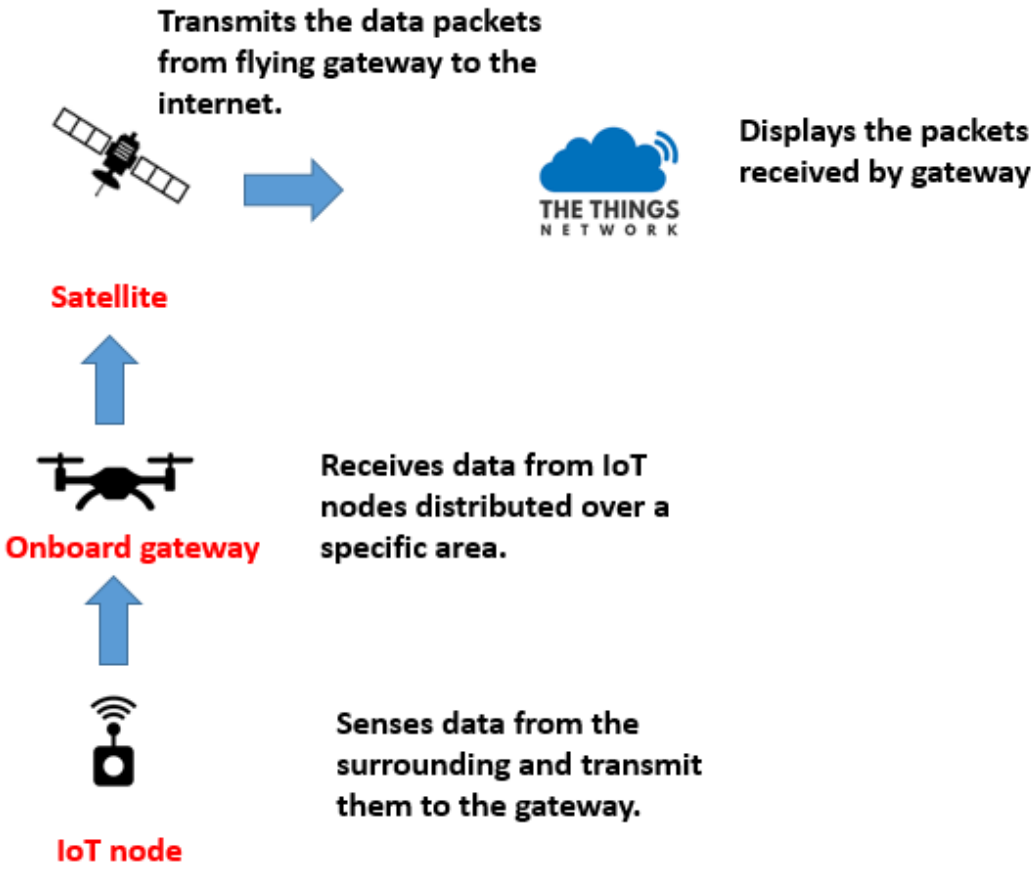

Figure 4.2: Scenario followed for the IoT and satellite integration.

The testbed we developed to assess the feasibility of the proposed solution and to evaluate the obtained performance is described previously in Chapter 3. A brief explanation of specific elements in the overall network is given as follows:

- Satellite: the presence of the satellite link between the gateway and the cloud platform has been simulated introducing delays and losses for the packets transmitted and received by the gateway in the Raspberry's operative system. In practice, the gateway is linked through its WiFi interface to an Access Point linked to the Internet through the cellular network.
- IoT Cloud platform: we exploited The Things Network (TTN), an open LoRaWAN cloud

platform where we registered our devices and gateway and allow us to see the data coming from the sensors in real-time through its browser interface.

Figure 4.3: IoT devices based on Arduino MKR WAN 1300

Figure 4.5 shows the communication process that is established between the IoT devices and the gateway before the nodes start sending data.

4.3 Performance Evaluation

The IoT cloud platform used: The Things Network (TTN) defines its *Fair Access Policy*. This policy limits and restricts the data each IoT end device can send. Each device has uplink airtime of 30 seconds per day, i.e 30 seconds of uplink messages for 24 hours and 10 downlink messages in 24 hours.

The SF (Spreading Factor) is automatically chosen by the LoRa cloud platform depending on

Figure 4.4: UAV equipped with the IoT gateway

different factors: (i) distance and (ii) signal strength. The higher the distance traveled by the signal to reach the gateway, the higher its sensitivity is and the higher its SF is and vice versa.

Quality of Performance

1. Signal Strength Each device dynamically selects its employed SF depending on the environment conditions and in order to offer the highest possible data rate and maximize both battery lifetime and communication range. In detail, each device computes the median Signal-to-Noise Ratio (SNR) of the last 10 received uplink packets and compares it with the limit SNR of each SF. This principle has to be taken into account since it affects some of the investigated performance variables.

   On-the-field test has been carried out with the aim to confirm the feasibility of the proposed solution and assess the obtained performance in terms of different output

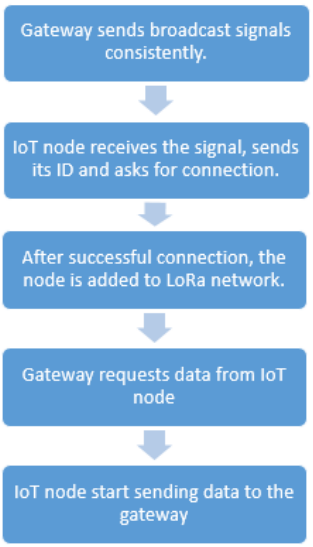

Figure 4.5: Communication between IoT node and gateway

parameters.

During this test, two IoT devices have been placed in an open area at an approximate distance of 100 meters from each other. The UAV flew above the area at an altitude of 20 meters for approximately 20 minutes following a random path. During that time, each sensor keeps sensing the environment temperature and sending one packet every 30 seconds (due to the limitation imposed by the TTN Fair Access Policy).

Received Signal Strength Indicator (RSSI) and Signal to Noise Ratio (SNR) are two information the user can see among the others and allow to keep monitoring the quality of the channel between the devices and the gateway. Figures 4.6 and 4.7 show the density functions of the RSSI and SNR, respectively, obtained from on-the-field test. The signal propagates in both Line-of-Sight (LoS) and Non-Line-of-Sight (NLoS) which is reflected in the low values of both RSSI and SNR. This is due to the changing distance between the flying gateway and the sensors, the change in the UAV altitude during the flight, and the imperfect alignment between gateway and sensor antennas.

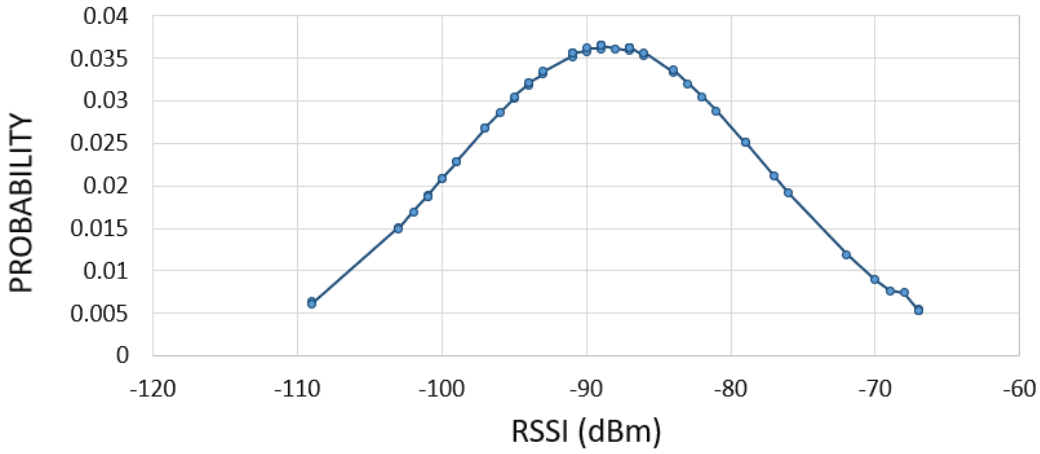

Figure 4.6: Density function of RSSI values obtained during outdoor test.

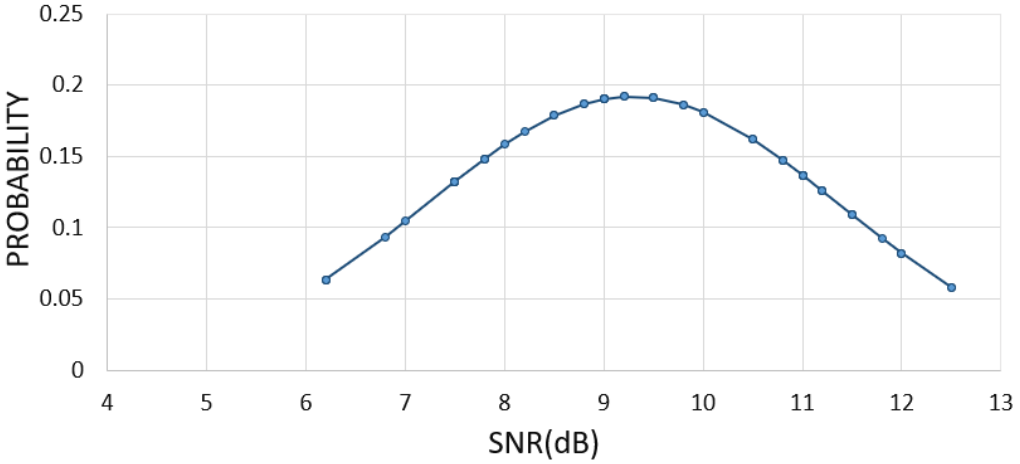

Figure 4.7: Density function of SNR values obtained during outdoor test.

2. **Current Consumption**

   One of the most concerned parameters dealing with the IoT and the UAVs is the energy consumption. We measured the current drained by the gateway from the battery pack through a current sensor. Figure 4.8 & 4.9 shows the density functions of the results

obtained during the on-the-field test in terms of consumed current when the gateway is waiting for data and when it is receiving and forwarding packets, respectively. The results obtained when the gateway is receiving packets is more spread values due to the higher and not constant distance between the gateway and the access point.

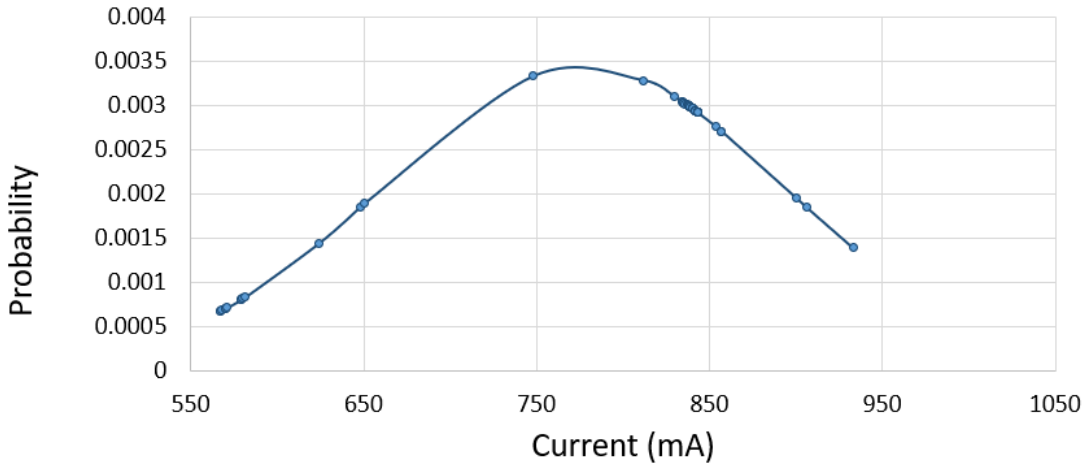

Figure 4.8: Density functions of consumed energy measured during the on-the-field test while waiting for data packets.

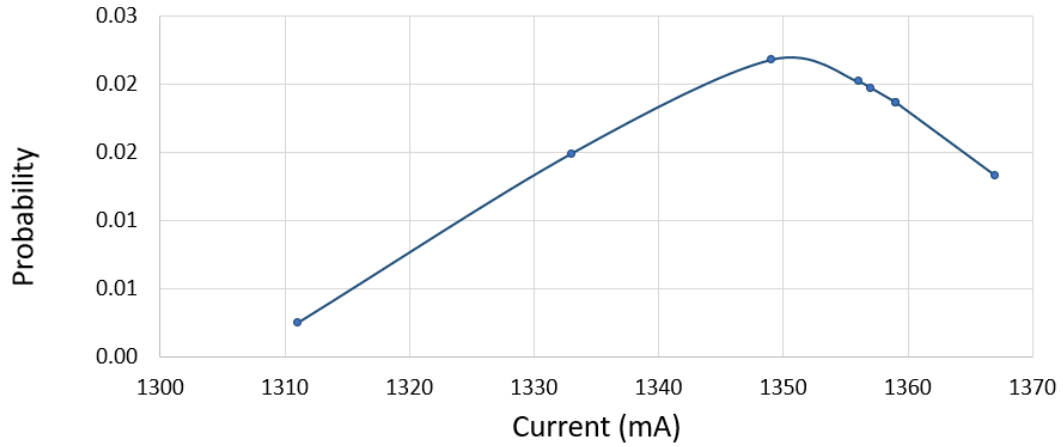

Figure 4.9: Density functions of consumed energy measured during the on-the-field test transmitting data packets.

Satellite Simulation

1. **Losses**:

   In order to simulate the loss of a satellite link, we performed some tests introducing 4 different loss values: 1%, 2%, 5%, and 10%.

   Figure 4.10 shows a screenshot of the TTN interface where the loss of one packet is highlighted in the case of a 10% loss. As highlighted, a LoRa packet with a specific *FCont* counter has been sent and the end device opens the two respective receiving windows *Rx1* and *Rx2* to receive the acknowledgement. When the end device did not receive the downlink message from the gateway during the two receive windows time, it re-sends again the packet with the same FCont until it receives from the gateway the downlink message within the time. It is noticed that the LoRa packet changed its SF increasing it to provide higher receiver sensitivity.

Figure 4.10: List of received packets highlighting the behavior upon loss simulation.

   The gateway keeps forwarding data in all cases, which proves the robustness and tolerance of the system in case of the satellite presence in the path between the gateway and the cloud platform in terms of loss.

2. **Delay**:

   The delivery time of the end-to-end communication between devices and the cloud platform t_{ee} can be defined as:

$$t_{ee} = t_t + t_p + t_s + t_c \tag{4.1}$$

where t_t is the transmission time between the device and the gateway, also called Time on Air (ToA), t_p is the propagation time between the device and the gateway, t_s is the delay of the satellite link, and t_c is the delay within the Internet until the packets reach the cloud platform. This delay is represented in Figure 4.11 where the simulated delay is inserted between the gateway and the LoRa server.

We performed some tests introducing 3 different delay values for t_s: 10 ms, 70 ms,

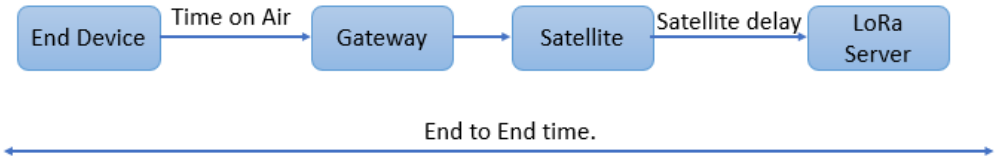

Figure 4.11: End to End time illustration using simulated satellite link between the gateway and network server.

and 250 ms, in order to simulate the presence of a LEO, a MEO, and a GEO satellite, respectively. Figure 4.12 shows the time by which the LoRa server received the packets after applying the simulated satellite delay link. The obtained results in terms of t_{ee} density function, whose samples are computed looking at the packet timestamp added by the device when it sends each packet and the time instant when the TTN receives it, are reported in Figures 4.13, 4.14 and 4.15.

Due to the low data rates of the LoRa protocol, in most cases t_t has the greatest value among the Eq. (4.1) terms. It is typically ranged between about 50 and 1,500 ms depending on the SF and the packet size. In our case, in both on-the-field and in-the-lab tests, the used SF is 7 as mentioned before. For this reason, $t_t = 51.5$ ms (as also shown in the sixth column in Figure 4.10) and t_p can be considered negligible.

The gateway keeps forwarding data in all cases, which proves the robustness and

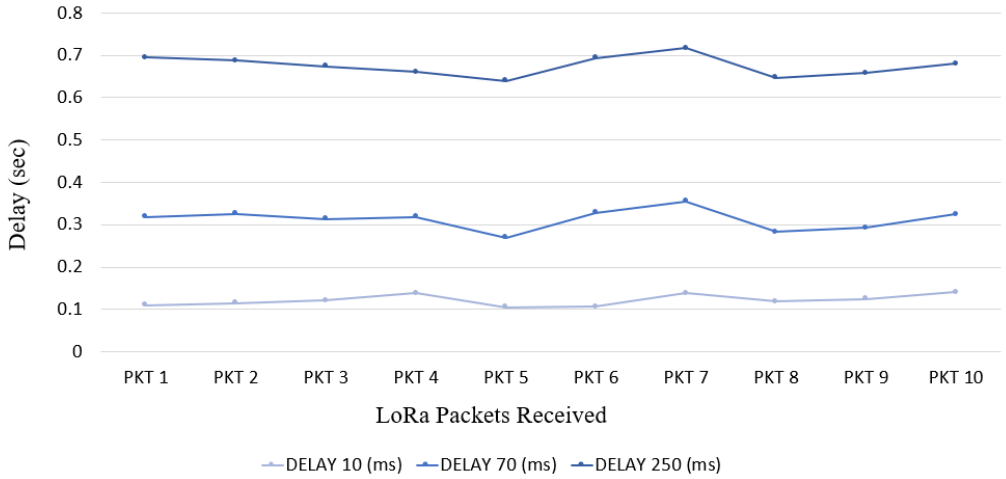

Figure 4.12: Delay of the end to end delivery time due to the simulated satellite link.

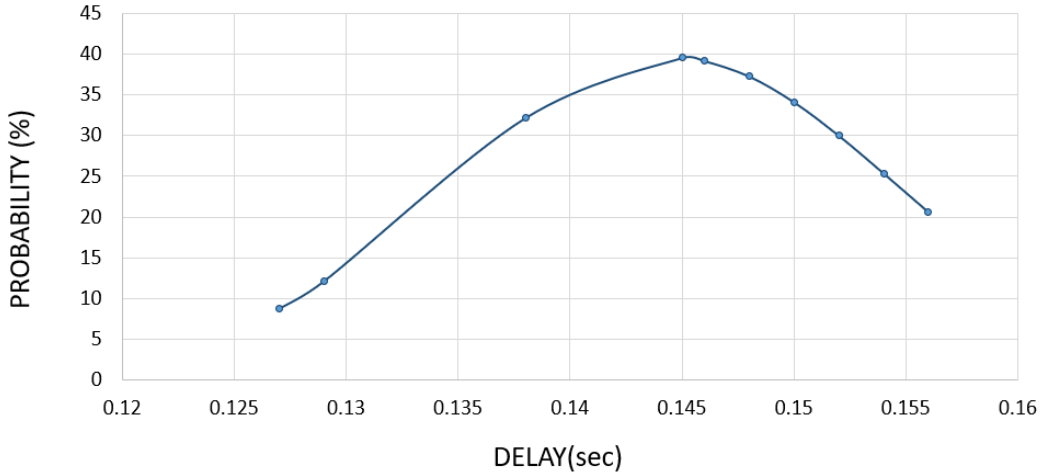

Figure 4.13: Density functions of the end-to-end delivery time with $t_s = 10$ ms.

tolerance of the system in case of the satellite presence in the path between the gateway and the cloud platform in terms of delay.

Gateway Status

The status of the RPI is monitored to analyze the state of the gateway and the data mule during operation using RPI Monitor software [127]. The CPU load, RAM memory and the

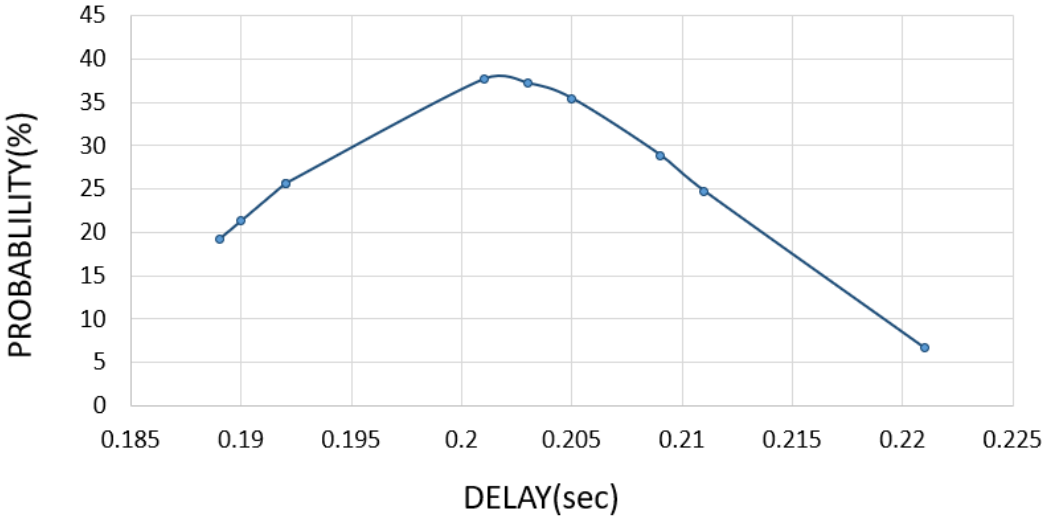

Figure 4.14: Density functions of the end-to-end delivery time with $t_s = 70$ ms.

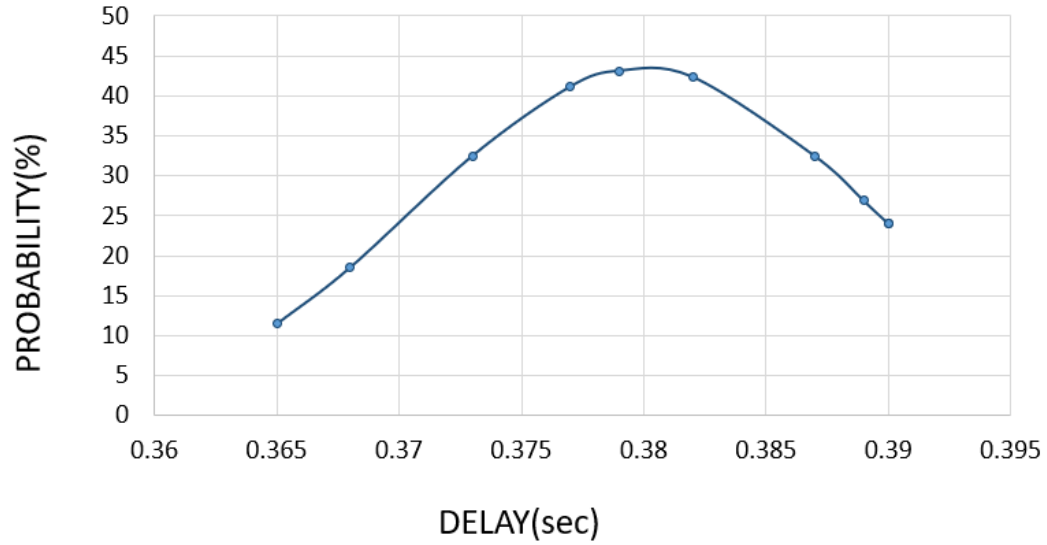

Figure 4.15: Density functions of the end-to-end delivery time with $t_s = 250$ ms.

temperature have been monitored and analyzed. The CPU usage of the RPI in both approaches include the loads computed on three different time windows: 1, 5 and 15 minutes. Figure 4.16 represents the CPU usage when the RPI acts as a flying gateway, and it is noticed that the LoRa process requires a very small fraction (less than 1%) of the overall CPU capacity for the processes not related to the RPI operative system. The RPI RAM memory has been monitored

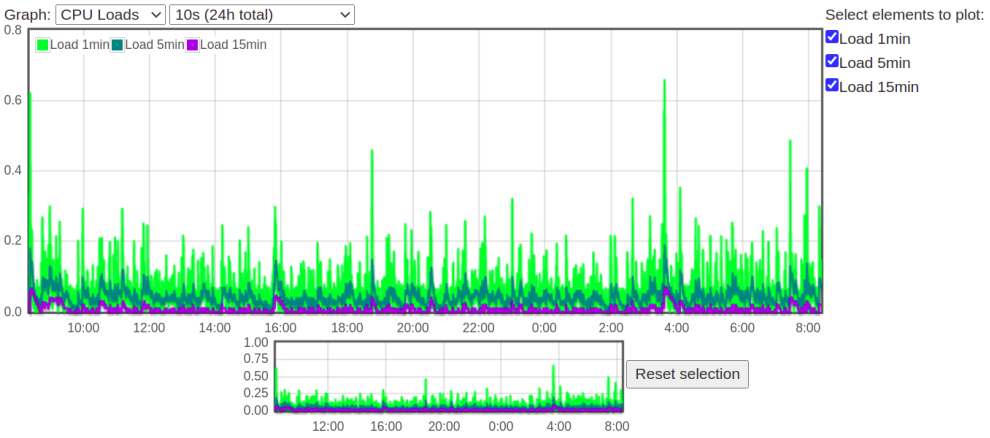

Figure 4.16: RPI CPU usage while operating.

and is represented in Figures 4.17. It shows the available and free memory of the RPI. The available memory is the memory that can be allocated by processes different than the ones of the RPI operative system, while the free memory is the portion of the overall memory not already allocated.

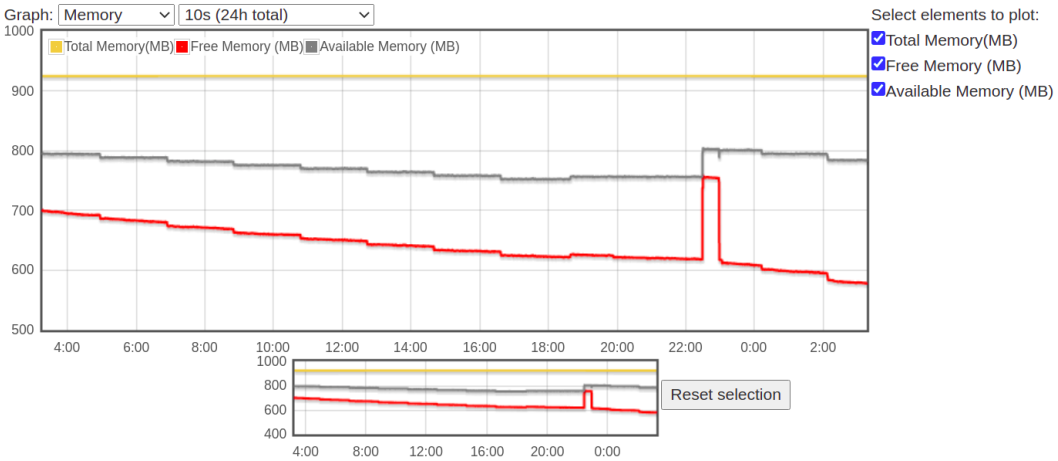

Figure 4.17: RPI RAM memory usage while operating.

With respect to the RPI temperature while operating in both approaches, Figures 4.18 shows that the temperature value range between 50 and 55 °C even if some lower spikes could be present due to different factors, such as the wind (in our case, the RPI is directly exposed

to the external environment without some protection like a case). This temperature value falls within the range of normal RPI functioning and so no additional cooling systems are required.

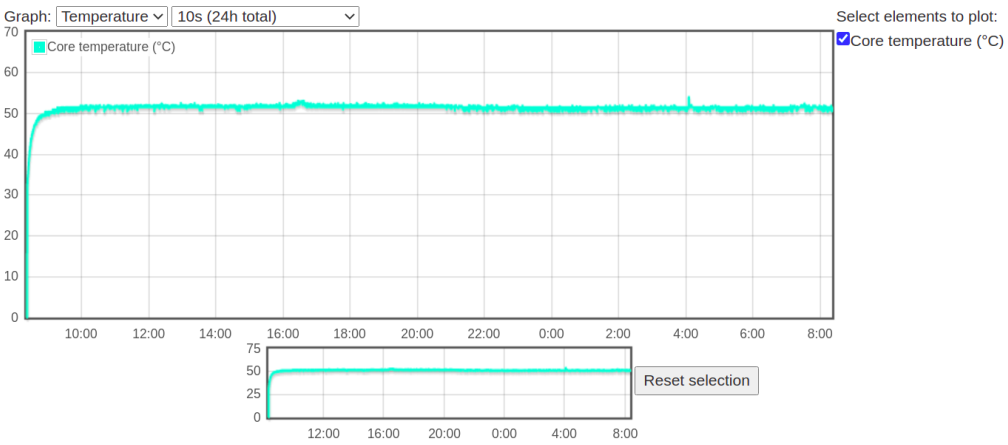

Figure 4.18: RPI temperature while operating.

4.4 Conclusion

The integration of UAVs and satellite in the IoT field is presented in this chapter. The idea of employing a flying gateway based on the LoRaWAN IoT solution equipped on-board a drone has been realized and tested in practice. The aim of this flying gateway is to extend the current limited coverage of the commercial IoT solutions and to integrate them with the terrestrial network. The exploitation of the satellite connectivity has been considered especially to overcome the lack of other communication infrastructure in certain locations, such as rural and remote areas, and looking for the possible integration of these network foreseen in the 5G framework.

Chapter 5

LoRaWAN Data Mule

Summary

This chapter introduces the concept of flying data mule based on LoRaWAN communication. The flying data mule presents an efficient solution to collect data generated from multiple sensors in remote and rural areas. Taking the advantage of both IoT and UAVs to introduce the Internet of Flying Things (IoFT) approach.

5.1 Motivation

The Internet of Things (IoT) is one of the currently emerging and wide spreading paradigms included in the evolution of telecommunication technologies and networks. It is strongly contributing to the birth and evolution of numerous use cases, such as smart city, smart home, smart industry, and smart agriculture. New and traditional functionalities can take place or be renewed by the use of IoT solutions, such as logistics, healthcare, mobility, and agriculture monitoring. An increasing number of connected devices and volume of exchanged data led also to an evolution of the related communication solutions. Different communication technologies and protocols have been adapted or developed ad-hoc to be suitable for the typical traffic features and performance requirements of the IoT applications.

However, the current communication infrastructure and wireless communication technologies are not always able to guarantee a proper service to all of these IoT applications, for example in terms of a proper connection user density and a suitable coverage area extension. IoT scenarios, such as smart agriculture, may involve the deployment of networks with a high number of IoT devices, deployed in vast areas, that generate data destined to human users or to other devices. Smart solutions are needed to overcome current terrestrial network limitations. For example, dynamically and temporarily extend "on-request" the current terrestrial infrastructure may be a viable solution to allow collecting data generated by nodes outside the current network coverage. Flying objects, such as Unmanned Aerial Vehicles (UAV), can help achieve this goal, also allowing to remotely manage the collected data. The use of these objects as data collecting nodes could be a viable solution belonging to the so called Internet of Flying Things (IoFT) concept.

5.2 Reference Scenario

The scenario we consider in this case integrates UAV and IoT technologies, in particular the LoRaWAN solution, to allow data collection in rural and remote areas. This gateway does not have Internet connectivity while it is flying, so it is not connected to the LoRaWAN servers while it is collecting data. The data cannot reach the Application Server in real-time due to the lack of an end-to-end connection between End devices and the Application Server, but are stored long-term stored onboard the UAV up until the UAV comes back to the starting point and gains access to the Internet. Figure 5.1 shows a representation of a data collection operation in the considered scenario.

In other words, this scenario considers the use of a UAV as a flying LoRaWAN gateway to avoid the employment of one or a set of fixed and permanents gateways which, especially in rural and remote areas, may not be cost efficient. Besides, we assume to provide a data mule functionality to the UAV in order to overcome the possible lack of a terrestrial communication infrastructure, required in case of real-time data collection and forward.

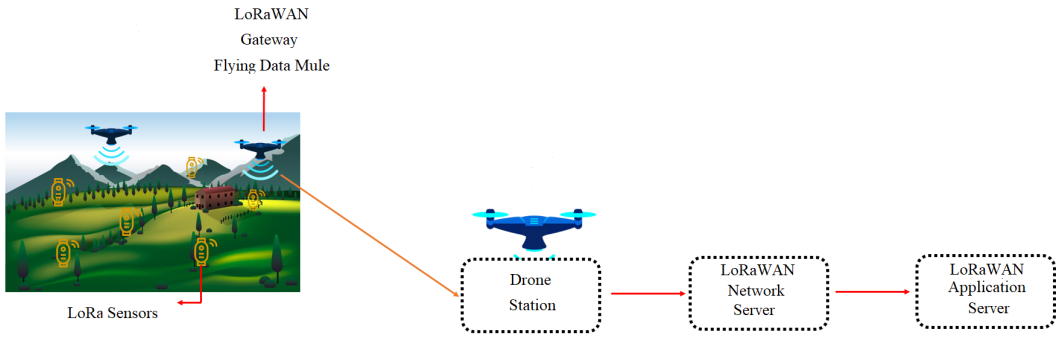

Figure 5.1: Reference Scenario: a drone implementing the data mule LoRaWAN Gateway flies over a specific rural area, collects data, and transmits them to the Network Server only when the fly is ended. Icon adopted from [128].

In detail, a set of IoT devices are distributed over a specific area generating data and sending them through LoRaWAN interfaces. A UAV equipped acting as a flying LoRaWAN gateway travels on a fixed path over this area only receiving data from the devices and keeping them stored in a memory located onboard the UAV. After the collecting and storing processes, i.e., at the end of the flight, the gateway downloads the stored data through an IP-based interface, such as Ethernet, Wi-Fi, or 3G/4G, towards the LoRaWAN network servers on the Internet (it could be on a Cloud platform or a user's dedicated PC). The single or multiple UAV flights can be performed manually by a drone pilot, guiding the drone over the selected area, or automatically, programming a predefined flight path in advance.

The testbed we developed to assess the feasibility of the proposed solution and to evaluate the obtained performance is given in Chapter 3. In this approach *ChirpStack* is adopted as the LoRaWAN server and is described as:

- LoRaWAN Network and Application Servers: it is based on the open-source *ChirpStack* software [129] which includes both Network and Application Servers. It allows implementing these two components as software modules in the same physical machine. It offers a web-interface to register the own devices and gateways and visualize the data received by the gateway from the IoT nodes. In our tests, it is installed on a Linux

physical machine that is connected to the gateway with a Wi-Fi link.

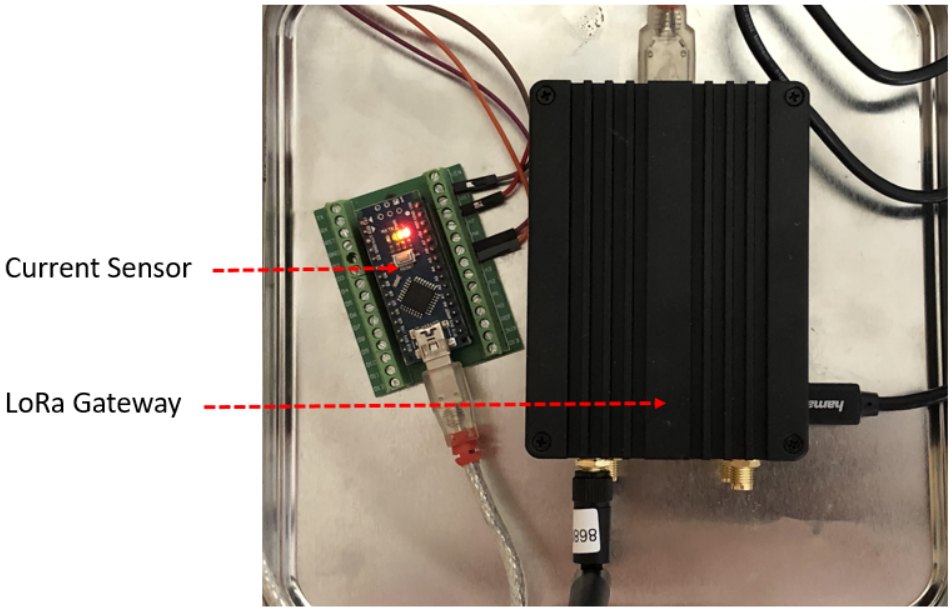

Figure 5.2: LoRaWAN gateway.

The achievable performance of communications through LoRaWAN links can depend on several parameters which can be manually configured or are automatically set and adjust by the system during data transmission and reception. SF and CR are an example of these parameters that directly affect the LoRa link performance, such as the achievable data rate. In standard applications, each end device automatically and dynamically set both SF and CR depending on the quality of the signal received from the gateway. Table 5.1 shows the relation between the SF values, the related data rate, and the sensitivity threshold of the used Semtech SX1301 chip, which depend on the measured SNR and the set Bandwidth.

To perform our test, we configured the mentioned parameters with the following values:

- Bandwidth: 125 KHz
- Frequency Range: 863-868 MHz
- Coding Rate: 4/5

Table 5.1: Semtech SX1301 SFs and related data rate [5]

Spreading Factor (SF)	**Data Rate (bps)**	**Sensitivity (dBm)**
7	5469	-126.5
8	3125	-129.0
9	1758	-131.5
10	977	-134.0
11	537	-136.5
12	293	-139.5

- Spreading Factor: between 7 and 12 depending on the environment conditions
- Data Payload: 4 Bytes

5.3 Performance Evaluation

In the implemented testbed, for technical implementation reasons, we used a software called ChirpStack, as detailed in Chapter 3, which allow us implementing a Gateway, a Network Server, and an Application Server instances onboard a UAV. In this way, the implemented scenario, shown in Figure 5.3, slightly differs from the typical reference one, since the UAV acts as the final endpoint of the LoRaWAN communication and no data forward takes place when the drone flight ends.

The ChirpStack software has been properly configured to collect and store the LoRaWAN packets transmitted from the end devices. This tool provides also additional information useful to understand the quality of the communication through the LoRa link. This information is available to the users through the ChirpStack interface.

The proposed solution has been evaluated through two tests performed in indoor and outdoor environments. Two useful parameters which reflect the quality of the communications through the LoRa link have been analysed: RSSI and SNR. Additional data regarding the status of the gateway have also been collected, in particular concerning the RPI RAM memory usage,

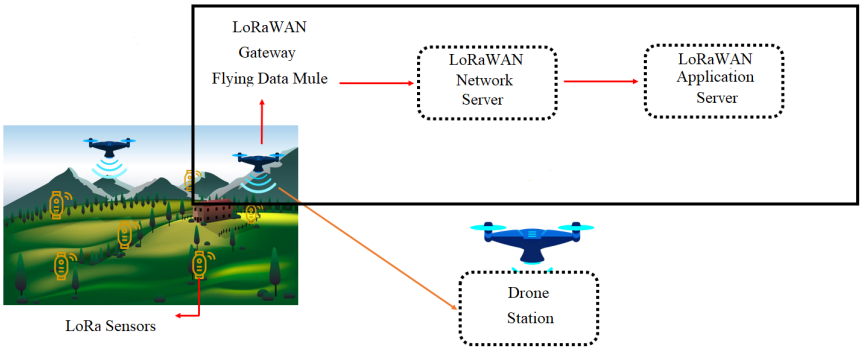

Figure 5.3: Implemented Scenario: a drone implementing the data mule LoRaWAN Gateway and the LoRaWAN Network and Application Servers flies over a specific rural area, collects data, and store them onboard for long term.

CPU usage, operational temperature, and energy consumption. The first parameters have been monitored by using the software RPI Monitor [127], while the energy consumption has been monitored by using an INA219 DC current sensor as described in Chapter 3. The gateway was connected to a general purpose 10000 mAh battery pack.

Signal Strength

Two useful and available parameters which reflect the quality of the communications through the LoRa channel are the RSSI and the SNR.

Indoor Testing

The two sensors represented in Figure 5.4 and the gateway were positioned at a few meters distance approximately 3 meters distance in LoS conditions. This test was aimed at showing the feasibility of our data mule solution. The empirical density functions of RSSI and SNR values are shown in Figures 5.5 and 5.6, respectively. They will be compared with the ones obtained in the outdoor test.

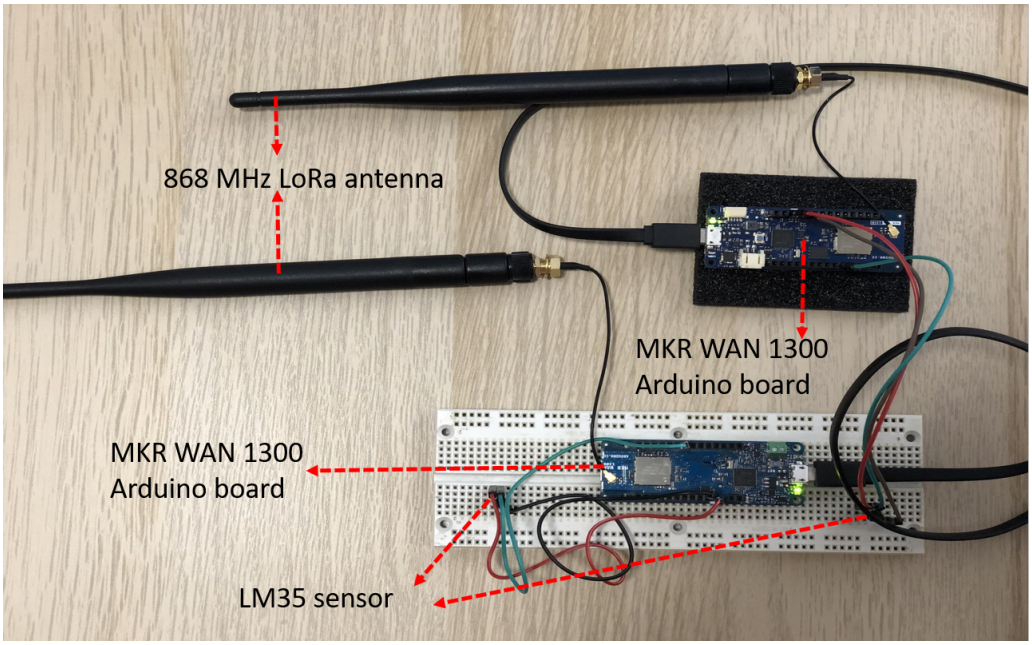

Figure 5.4: LoRaWAN IoT nodes.

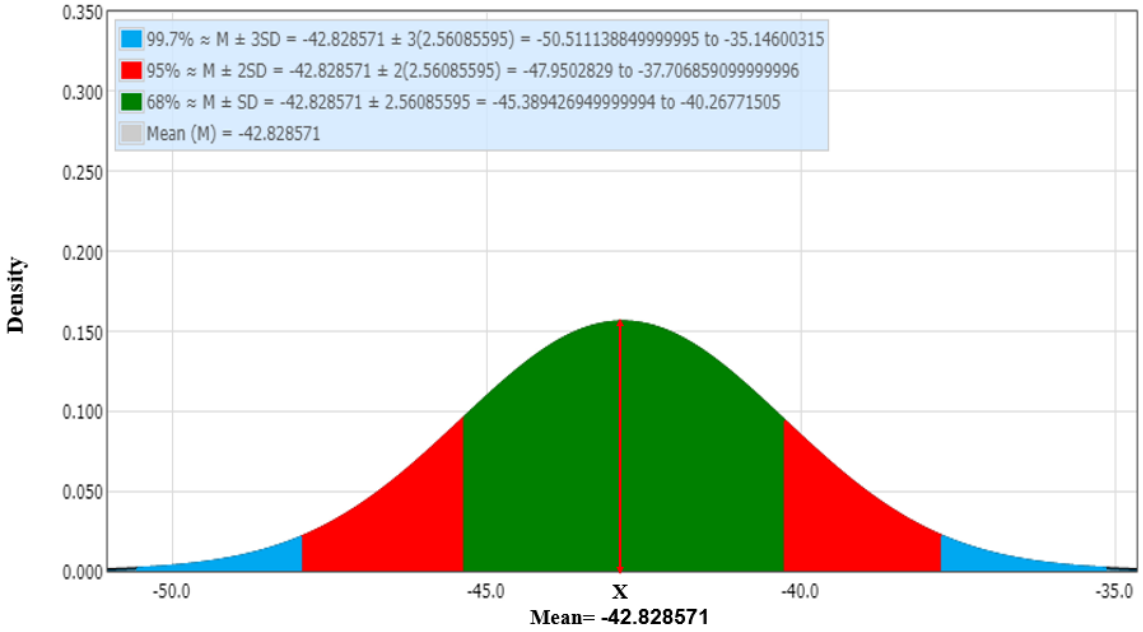

Figure 5.5: Density function empirical rule of RSSI values collected during indoor testing.

Outdoor Testing

The LoRaWAN gateway was located onboard a DJI Phantom drone, as shown in Figure 5.7.

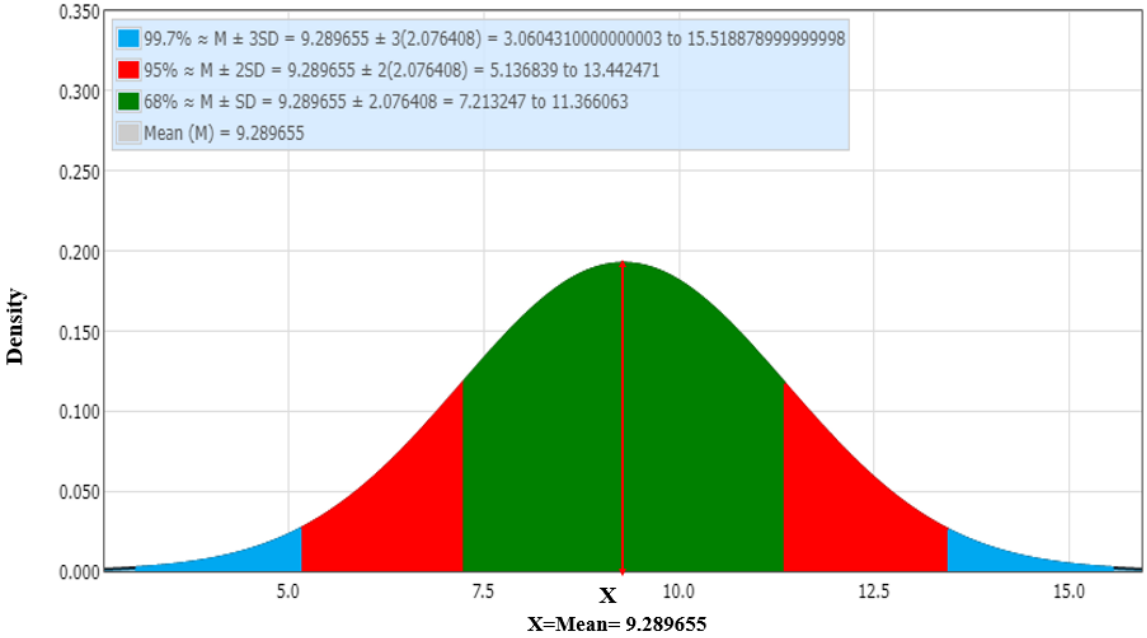

Figure 5.6: Density function empirical rule of SNR values collected during indoor testing.

Figure 5.7: UAV equipped with our IoT LoRaWAN gateway

During the test, the sensors were located close to each other in a specific position in an open area and the UAV flew at an altitude of about 10 m for approximately 20 minutes following a random path above the area among three positions, as shown in Figure 5.8. The distance between the sensor and the UAV was ranged between 40 and 160 m, with only a few measurements we took manually moving at a fourth location (position 4) at 630 m from the sensor.

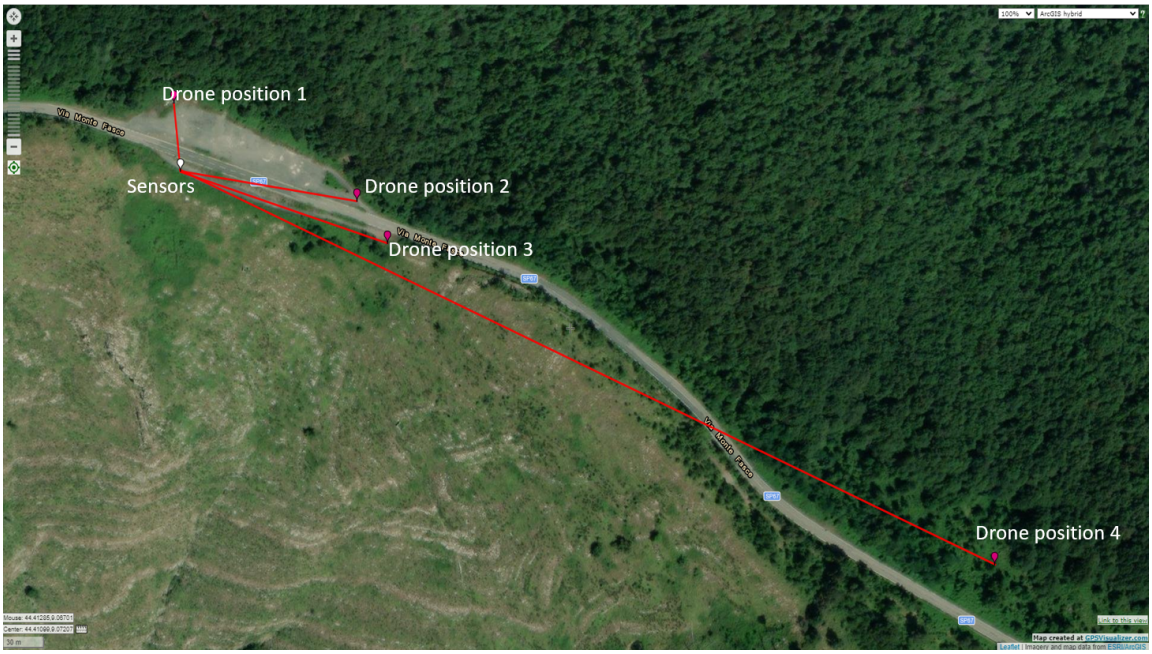

Figure 5.8: Map of the deployment scenario pointing out the different drone and sensor positions during the outdoor test

The empirical density functions of RSSI and SNR values are shown in Figures 5.9 and 5.10, respectively. The obtained results show satisfying channel quality. The lower values of RSSI and SNR are due to the partial lack of LoS, the variable and increased distance between the flying gateway and the IoT devices, the change of the drone altitude while flying, and the not perfect alignment between gateway and device antennas.

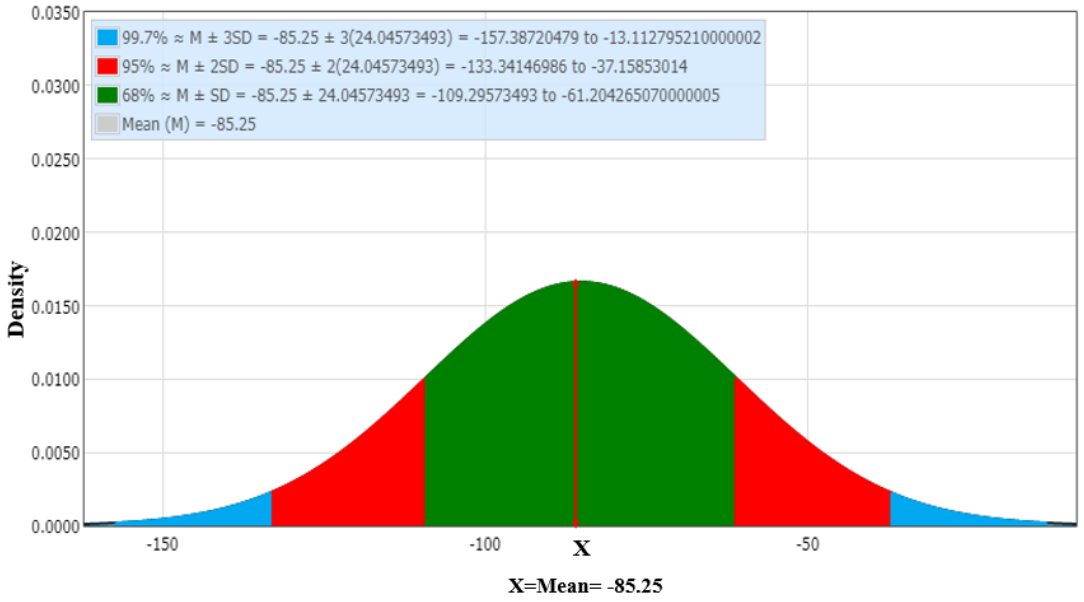

Figure 5.9: Density function empirical rule of RSSI values collected during outdoor testing

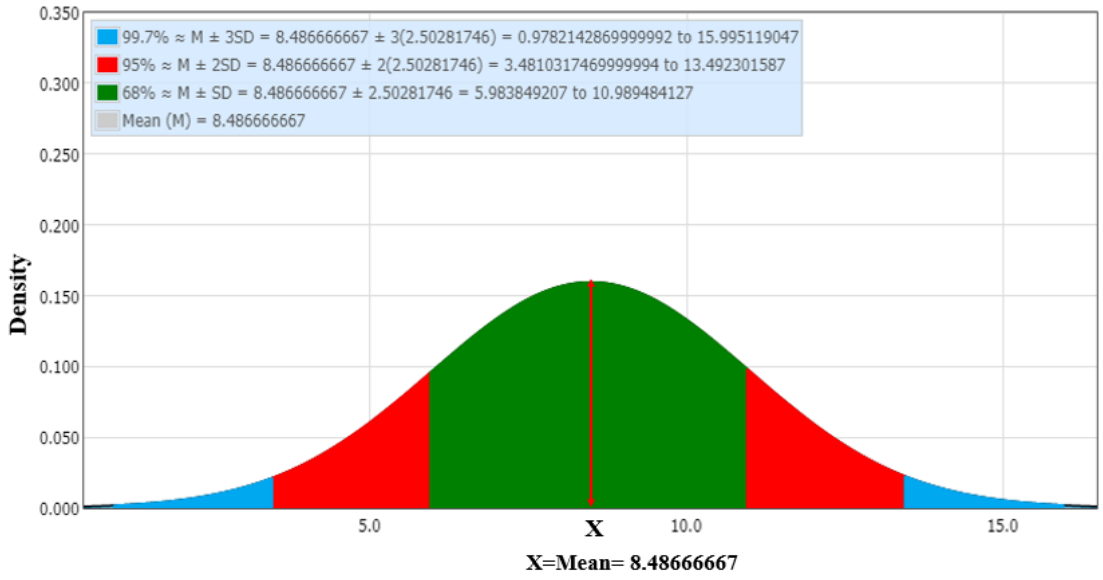

Figure 5.10: Empirical density function of SNR values collected during the outdoor testing

Power Consumption

Another parameter has been monitored that is the current consumption of the gateway, as representative of energy requirements. The two possible ways to provide power to the gateway

onboard a UAV are: 1) the battery of the UAV, or 2) a dedicated external energy source, such as a battery pack, as done in the tests. In both cases, the energy consumption of the gateway is critical because it can impact the UAV flight duration and can limit the gateway activity. To monitor the current consumption of the gateway, a current sensor between the power supply source and the RPI has been installed as described previously in Chapter 3. Similar values have been measured in both indoor and outdoor tests.

Current consumption includes the current consumed by the whole gateway, i.e., by the RPI and the LoRaWAN shield. The energy consumption data have been collected during the 20 minutes outdoor test. The measured current consumption varies within the range 810-1020 mA and it is composed of a fixed value (about 810 mA) due to the RPI standard operations and of multiple spikes when the gateway receives data from the LoRaWAN sensors. This trend confirms that a standard battery pack (such as the 10000 mAh battery pack we used) is enough to provide power to the gateway for the entire current typical UAV flight duration, i.e., it is realistic to assume that the battery pack for the gateway will last longer that the UAV battery, so making feasible the data mule service. From the data shown in Figure 5.11, we compute that the mean energy consumption is 820 mA, with a consequent estimated decrease of the battery change level of just 2.7%. This estimation allows us stating that even a battery with a lower capacity is enough to keep the gateway hardware operative even in case of a much longer flight duration.

Gateway Status

RAM memory usage, CPU load, temperature, and energy consumption of the gateway have been monitored to further assess the feasibility of the proposed solution. All the shown data have been collected during a 24 hours indoor test in order to have a higher and statistically valid set of information. Data have also been collected during the outdoor test and show similar trends even though for a lower time window. Figure 5.12 shows the available and free memory of the RPI. The available memory is the memory that can be allocated by processes different than the ones of the RPI operative system, while the free memory is the portion of the overall

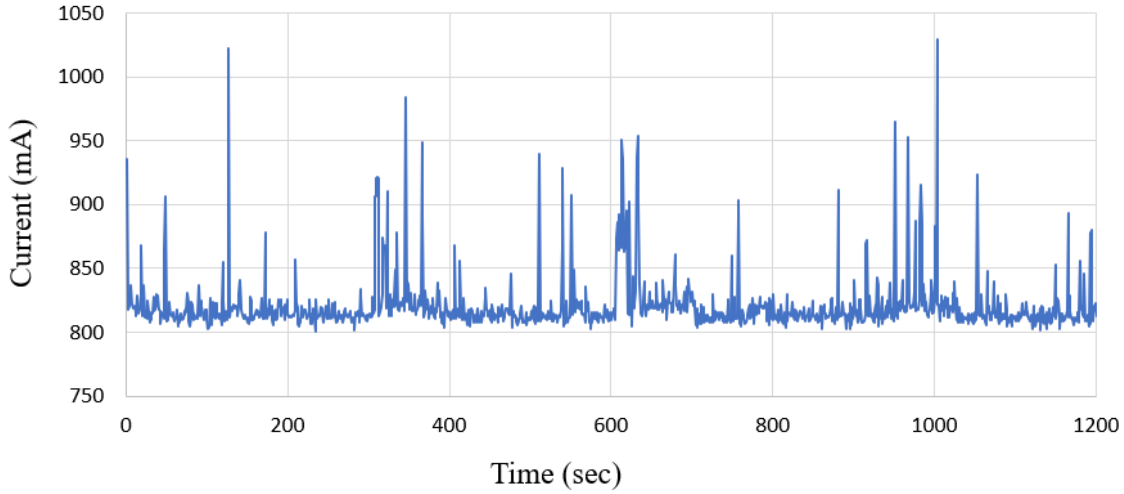

Figure 5.11: Current consumed by the LoRaWAN gateway while flying the drone for 20 minutes time.

memory not already allocated. Figure 5.13 shows the CPU usage of the gateway while operating. It includes the load computed on three different time windows: 1, 5, and 15 minutes. It can be noticed that the RPI requires a very small fraction (less than 1%) of the overall CPU capacity for the processes not related to the RPI operative system. Looking at Figure 5.14 it is clear how two of the first three processes in terms of CPU usage time within the 24 hours period (the first and the third ones) are the ones related to the LoRaWAN operations and communications. Figure 5.15 shows the temperature of the gateway while operating. During the monitored time, the temperature value was ranging between 50 and 55 °C even it some lower spikes could be present due to different factors, such as the wind (in our case, the RPI is directly exposed to the external environment without some protection like a case). This temperature value falls within the range of normal RPI functioning and so no additional cooling systems are required.

5.4 Conclusion

In this chapter, we proposed a flying data mule IoT gateway based on the LoRaWAN technology and installed onboard a UAV. This proposed solution aims to extend the limited

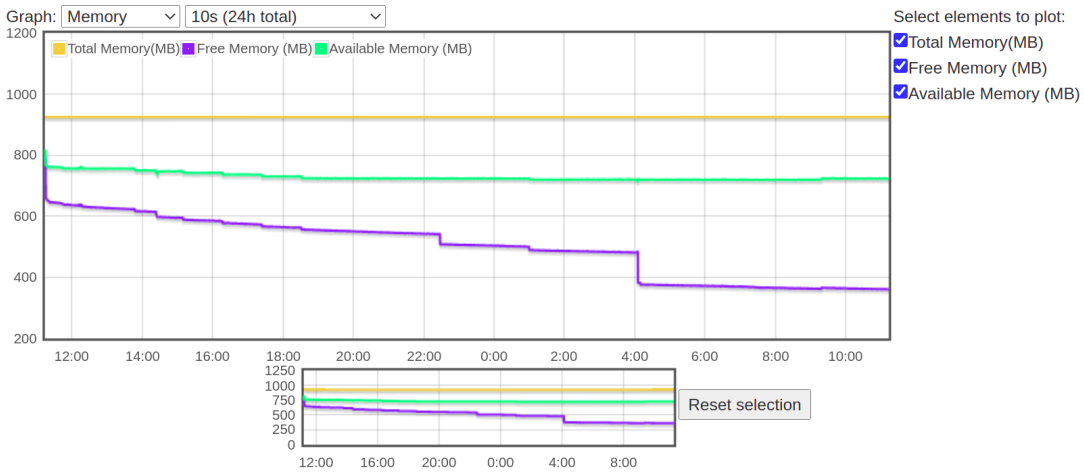

Figure 5.12: RPI RAM memory usage while operating.

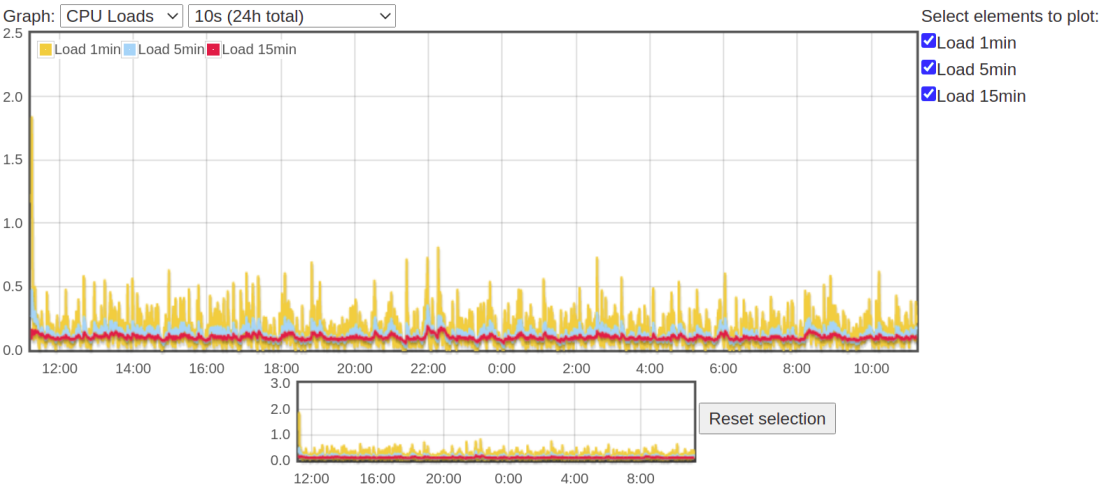

Figure 5.13: RPI CPU usage while operating.

coverage of the different commercial IoT solutions allowing data collection and temporary storage onboard the UAV during its flight, without the need for direct connectivity with the Internet. The UAV downloads the data after the end of the flight, when it reaches back its starting point, in order to make them available to the users through the Internet.

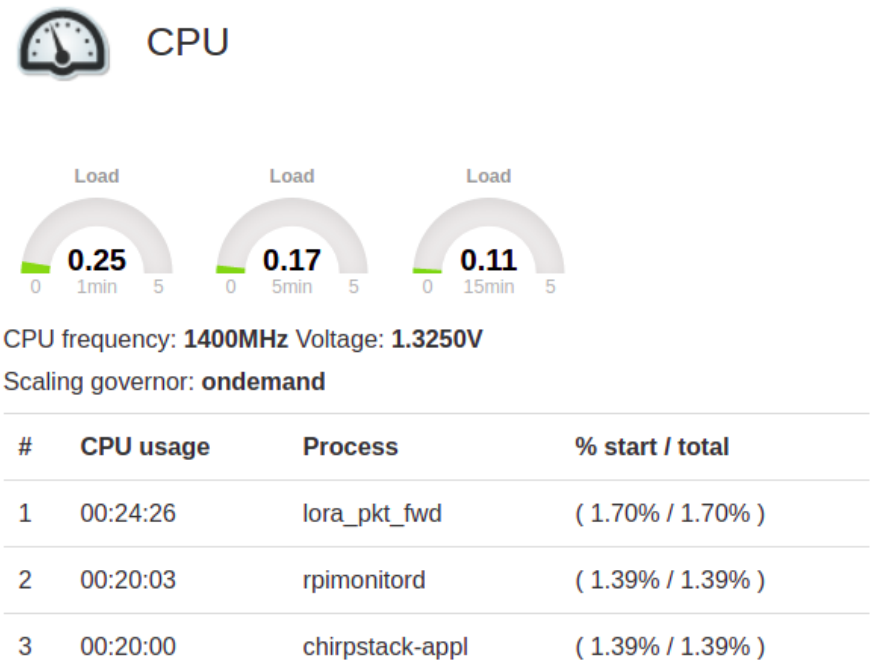

Figure 5.14: The first three processes in terms of CPU usage running on the RPI

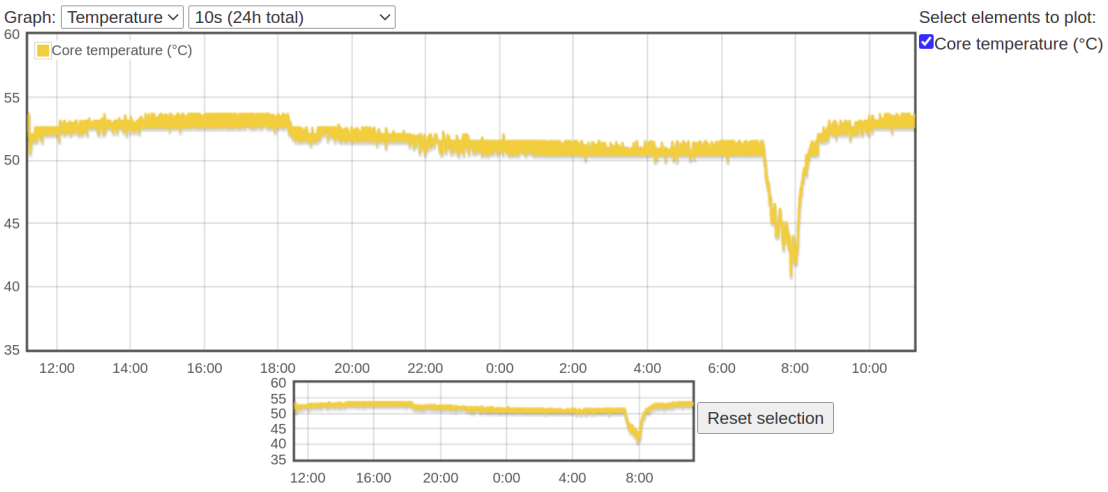

Figure 5.15: RPI temperature while operating.

Chapter 6

LoRaWAN Security: Localization using RSSI

Summary

In this chapter, a localization algorithm based on RSSI in a LoRaWAN network is introduced. The localization problem is represented from security perspective showing that any attacker is able to perform and carry out a physical attack against IoT devices and sensors installed in a specific area.

6.1 Motivation

Recent advances and improvements in technology have led to the development of intelligent nodes and sensors used in the creation of a large number of smart wireless networks connected to the Internet and transmitting data continuously. Smart cities, smart houses, smart grids, smart agriculture and environmental surveillance in rural areas are examples of IoT applications that adapts the use of a huge number of sensors and nodes for data transmission and monitoring. Various communication technologies in LPWAN are available, such as SigFox, NB-IoT, and LoRa which is gaining a great attention in data exchange between the sensors and end users.

This last technology can allow long distance communications (up to kilometers) with low power consumption, and consequent long device's battery life, thanks to the used a CSS modulation [130].

Due to the huge spectrum of IoT applications, the security and privacy issues rise. These applications cannot operate without ensuring reliable and trusted IoT ecosystem. Managing the security and privacy of any IoT application is of great interest and necessary to avoid any possible attack that can be performed in an IoT network. Since IoT devices are connected to the Internet to perform their tasks, they are exposed to different attacks for data and information stealing or data modification. In IoT the security issues differ between the IoT layers: sensing layer, networking layer or application layer. Each layer has its own security issues and threats due to the various technologies used in each. The security attacks that can be performed in any IoT network are based on the different IoT architecture layers summarized in Figure 6.1. Starting with the perception layer, the main aim is to put the IoT node out of service

Node tampering, malicious code injection, false data injection and sleep denial or sleep deprivation are common attacks that can be performed on the physical layer in an IoT network. The main aim of conducting attacks on this layer is to put the sensor or IoT node out of service and not performing its task. The networking layer is responsible for transferring the data from the sensors to the computational & processing unit. DoS, MITM, Sybil and sinkhole attacks are examples of the different security attacks that can be performed on the transmission link between the IoT nodes and the end user or computational unit. The application layer in the IoT network architecture is in charge of providing the services to the end user. Data theft, malicious code injection of service interruption are possible attacks an attacker can carry on for the aim of stealing private & critical data or disturbing the user from accessing a specific service.

On the other hand, localization is becoming a hot topic with different IoT applications such as traffic monitoring. Most of the research targets localization in indoor environments for example in [48–52]. Concerning outdoor environments, satellite based positioning system [53] such as GPS is one of the most used technologies in different applications [54, 55]. However, such technologies are considered as non-feasible ones due to their high cost and power consumption. To better exploit the IoT technologies, LoRa can be used for both data transmission in any IoT

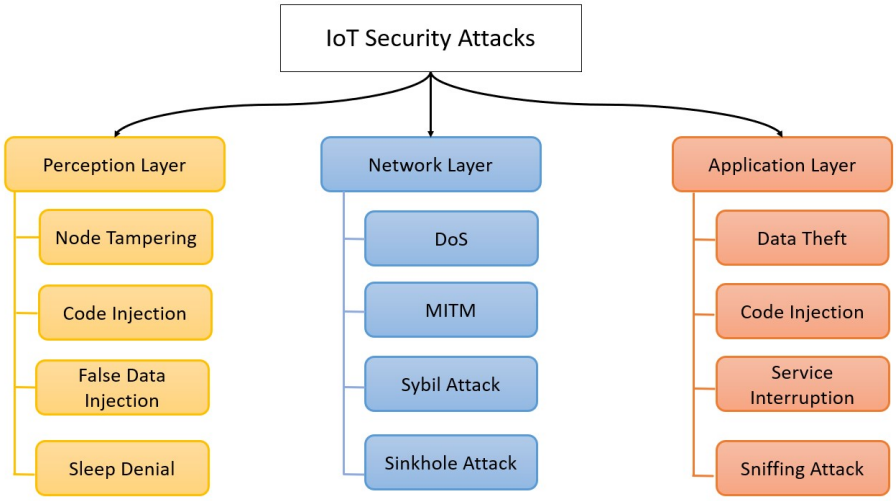

Figure 6.1: Security attacks that can be performed on the different IoT layers [131–133].

network and for estimating & calculating the position i.e *localization* without the need of any additional special device. It is suitable for both outdoor and indoor environments [56].

Several studies adopted the use of Angle-of-Arrival (AoA) and Time Difference of Arrival (TDoA) -for example- [57, 58] for localization purposes, although such techniques require special hardware or accurate synchronization respectively. Another possible technique that doesn't require additional hardware components and has low power consumption is RSSI. This technique is easy to use compared to the other techniques in IoT networks, because the RSSI values can be received and retrieved in a simple way by the user.

RSSI information associated with these IoT devices can be retrieved and given as input to different algorithms to reveal their location. Once the location is exposed, possible attacks can be carried out by attackers known as *"Physical Attacks"*. A physical attack is the physical violation of a network through either wired or wireless medium or directly on a specific device. Tampering, malicious code injection, RF interference or jamming, fake node injection, sleep denial attacks and permanent denial of service are examples of physical attacks [59], leading to data leakage, fake data manipulation, node shutdown or distortion in the node communication [60]. To carry out a physical attack, the attacker misuse the security keys stored in the device for the purpose of transmitting fake messages to other IoT devices or the gateway, recording

the data transmission or blocking it. Such attacks are targeted on the PHY/MAC layers of the TCP/IP and the perception and application layers in the IoT network architecture.

Considering the case of LoRaWAN - in its two versions v1.0 [134] and v1.1 [135] - the root keys used in session keys generation are stored in the end devices allowing the attacker to expose the data stored in that device. The main aim of this activity is to expose and uncover the position of any LoRa node or device making it easier to perform either (i) physical attack by destroying the device, altering its job or stealing the session keys or (ii) jamming attack on the LoRa signal generated by the device avoiding it from reaching the gateway.

6.2 Localization Techniques

Various localization algorithms have been proposed for position estimation of any node in an IoT or WSN network. These algorithms are categorized into two groups: *range-based* and *range-free* presented in Figure 6.2.

Focusing on range based techniques, such techniques require distance or angle for estimating the position of a node. In other words, these techniques measure the distance between the transmitter node and the receiver node. ToA, AoA, TDoA and RSSI are the different methods used in this technique as represented in figure 6.2. A brief description of these methods is given as follows:

1. AoA: Angle of Arrival method requires an array of antennas by which this method measures the difference in the direction of a single radio wave received by these antennas. Due to its sensitivity to multi-path and shadowing this method causes high localization error. To overcome such error and guarantee an acceptable accuracy, large antenna arrays could be deployed and used, however, requiring additional hardware components and cost [136, 137].

2. TDoA: the Time Difference of Arrival method, the distance between the sender node and receiver is calculated by knowing the difference between the times of arrival of a signal received by two receivers in addition to the speed of the propagation medium. Its

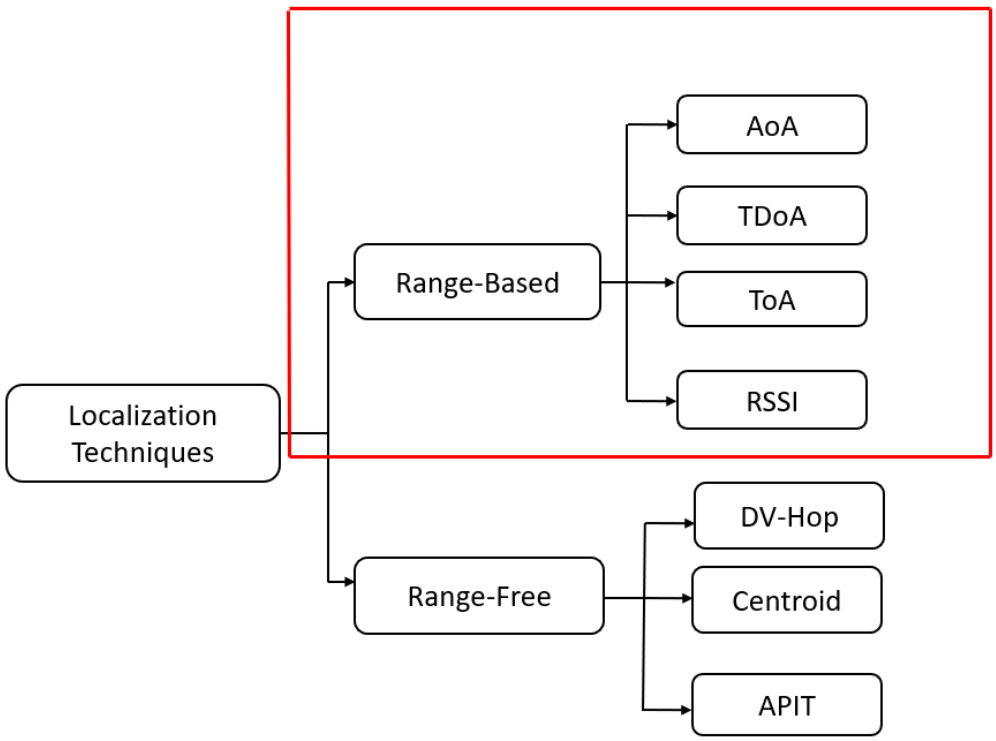

Figure 6.2: Classification of the localization techniques.

accuracy is good when the nodes are calibrated well prior sending since it is affected by the surrounding humidity and temperature [137–139].

3. ToA: in Time of Arrival method, the estimation of the position node is based on the speed of the signal's wavelength and time. In other words, the distance between the sender node and the receiver node is the direct measure of the propagation time of the signal. It gives highly accurate results, however it requires high precision timing and synchronization [137].

4. RSSI: this method calculates the distance between the sender node and receiver node based on the strength of the signal. It is a cheap technique for distance estimation compared to other techniques, and its performance is affected by the multi-path radio signal propagation [8, 137].

A comparison of the accuracy and cost of each of the range-based and range-free localization techniques is given in Table 6.1.

RSSI values for position estimation has been adopted in different scenarios due to its low cost

Table 6.1: Comparison between the range-based localization methods in terms of accuracy and cost [6–8].

	Measurement Method	Accuracy	Cost
Range Based	ToA	High	High
	AoA	Low	High
	TDoA	High	High
	RSSI	Medium	Low

compared to other localization or position estimation algorithms. Different studies adopted the use of RSSI for estimating the position of a node in an IoT network whether indoor or outdoor one using various IoT communication technologies [49, 140–145]. For example, [56] presented an experimental data set of different RSSI values collected from both indoor and outdoor environments using LoRa as IoT protocol. The experiments conducted showed some promising results of the use of RSSI for localization purpose, however it still needs more investigation especially that the experiments were conducted in urban areas. [146] proposed the use of RSSI values of a LoRa transmitting node adopting trilateration and multilateration localization algorithms. The authors concluded that increasing the number of receiving nodes can increase the accuracy of locating the position of the transmitting one. In [51] RSSI values generated from signals operating using WiFi, Bluetooth, ZigBee and LoRa communication protocols have been compared for providing the most accurate technology for estimating the position of an IoT in an indoor environment. [147] presented a position tracking system using RSSI values in an indoor region adopting trilateration algorithm for position estimation. To overcome the RSSI impairments caused by the LoRaWAN frequency hopping feature, Software Defined Radios (SDR) has been employed in [148]. The experimental results showed an improvement in the performance of RSSI in locating the position of IoT nodes.

The main aim of this activity is to allow an attacker or intruder to estimate the position of a LoRaWAN node deployed in an area using a flying gateway. Once the estimation is made, the attacker will have enough knowledge and information about the possible location of the node, then perform different kinds of attacks on this node. This work is the first and preliminary step of LoRaWAN security in an open area: (i) estimating the position of a node, (ii) perform physical attack or jamming attack.

6.3 System Description

LoRaWAN communication is adopted since it offers a power efficient and long range connectivity in remote areas without the need of Internet connectivity. Before starting with the system details, the channel modeling and localization algorithm followed are explained.

Channel Modeling

Radio channel characterization in an environment can be obtained from the relation between RSSI values and the distance between two radio devices. Given the received signal power (P_R), transmitted signal power (P_T), receiver antenna gain (G_R), transmitter antenna gain (G_T), and signal wavelength (λ), the distance (d) and signal propagation constant (N) which indicates the rate at which the path loss increases with distance depending on the surrounding environments can be expressed as in Equation (6.1), called Friis' Equation.

$$P_R = P_T \cdot G_T \cdot G_R \cdot \left(\frac{\lambda}{4\pi}\right)^2 \cdot \frac{1}{d^N} \tag{6.1}$$

The log distance path loss is considered as a generic and extended model of the Friis' equation (6.1). This log distance model predicts the propagation loss in a wide environment, unlike the Friis' model which is restricted to unobstructed path between the receiver and transmitter. It is given in Equation (6.2):

$$P_L(d) = P_L(d_0) + 10nlog_{10} \cdot (d/d_0) + X \tag{6.2}$$

where:

- *P_L(d)*: is the path loss at any distance d
- $P_L(d_0)$: is the path loss at distance d0
- n: is the path loss exponent
- X: is used when there is a shadowing effect and it is a zero-mean Gaussian distributed random variable.

On the other hand, the relation between the transmit power and the received one in a wireless signal is given in Equation 6.3:

$$P_R = \frac{P_T}{d^N} \tag{6.3}$$

The Friis' Equation is converted from Watt to dBm to express the RSSI by using the following Equation:

$$P(dBm) = 10 \cdot log_{10}(P \cdot 10^{-3}) \tag{6.4}$$

The relation between the signal strength and the distance can be expressed by using the Log Normal Shadowing Equation:

$$RSSI = -10 \cdot n \cdot log_{10}d + A \tag{6.5}$$

where:

- A: received power when the distance between the two antennas is 1 m (absolute value of RSSI value at distance d=1m)
- n: the loss parameter or loss exponent which depends on the environment conditions

RSSI has been widely used for positioning purposes since it does not require any special hardware, no time synchronization, easy to implement and low power consumption solution. RSSI is a relative indicator for the received signal strength and it reflects the power of the

signal in a given environment.

To obtain the distance from this RSSI value, just reverse the Equation presented in 6.5 as follows:

$$d = 10^{\frac{A-RSSI}{10 \cdot n}} \tag{6.6}$$

Localization Algorithm

The localization of an IoT device is carried out through the RSSI values. In other words, the distance between two radio devices (LoRaWAN gateway and the LoRaWAN device) is estimated based on the RSSI values of the data packets generated by the device when they are received from the gateway.

The Trilateration Algorithm is then used to estimate the precise position of the device P from the estimated distance. It is a geometry-based algorithm where a set of circles (at least three) are drawn having the known position of the gateway as the center L and the estimated distance as radius d.

With one stable gateway, the exact position of the device cannot be identified as shown in Figure 6.3. The only information that can be obtained is how close this device is from the gateway. Each point at distance d from the center L is a potential candidate for P. This situation can be improved by adding a new gateway L2, as shown in Figure 6.4.

Now the device is along the circumference of the red circle and the blue one, i.e. on the intersection of the two circles. The possible candidates are now reduced to 2 possible locations. A third gateway L3 is needed to give a precise position which will meet with the two other gateways at one point that corresponds to the device precise location, as shown in Figure 6.5.

The position of the device is the intersection of the circles. This intersection is calculated by solving the system composed of the coordinates of the circles with center (x_i, y_i) and radius r_i:

Assuming that the coordinates of A are (x_a,y_a), B's coordinates are (x_b,y_b), C's coordinates are (x_c,y_c), and the distance from P to the three beacon nodes is (d_1, d_2, d_3), respectively. The

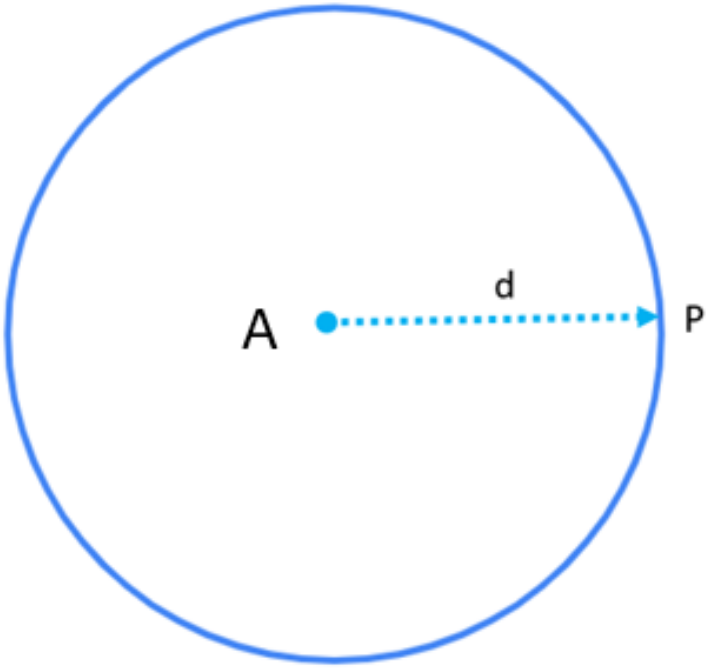

Figure 6.3: Circle drawn with one gateway

Equation 6.7 may be as follows:

$$\begin{cases} \sqrt{(x-x_a)^2+(y-y_a)^2} = d_1 \\ \sqrt{(x-x_b)^2+(y-y_b)^2} = d_2 \\ \sqrt{(x-x_c)^2+(y-y_c)^2} = d_3 \end{cases} \tag{6.7}$$

Based on Equation 6.7, the coordinates of the unknown point P can be obtained from Equation:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2(x_a-x_c).2(y_a-y_c) \\ 2(x_b-x_c).2(y_b-y_c) \end{bmatrix}^{-1} \begin{bmatrix} (x_a)^2-(x_c)^2+(y_a)^2-(y_c)^2+(d_c)^2-(d_a)^2 \\ (x_b)^2-(x_c)^2+(y_b)^2-(y_c)^2+(d_c)^2-(d_b)^2 \end{bmatrix} \tag{6.8}$$

The algorithm followed in this research is given in Figure 6.6.

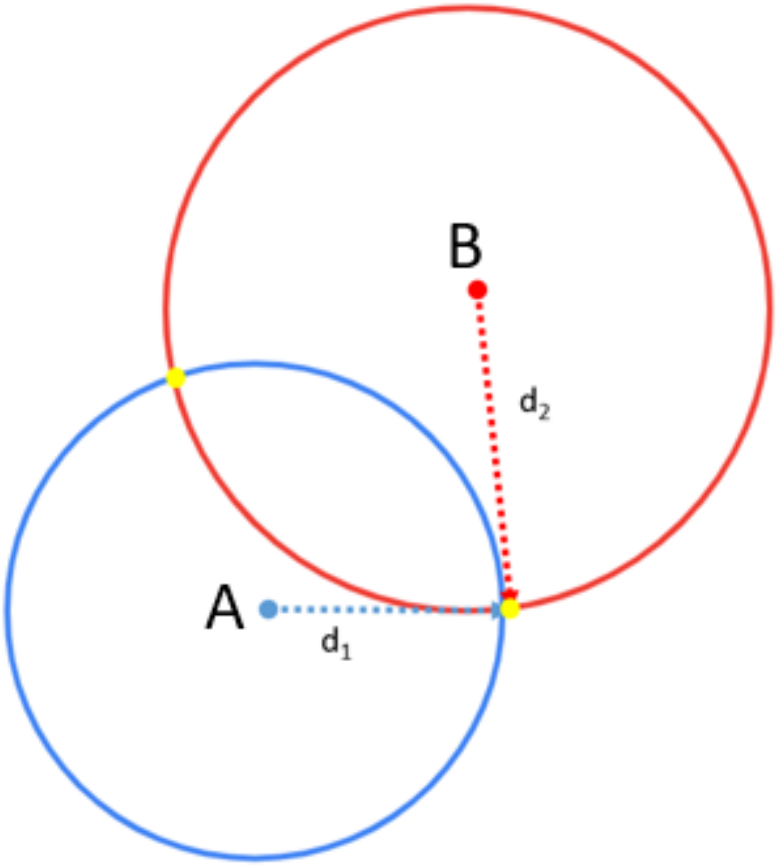

Figure 6.4: Circles drawn with two gateways with different positions

Hardware Setup

For the test on the field, a pilot gateway pro RAK7243 is used where the LoRa connectivity is provided by a RAK 2245 shield built on a Raspberry Pi 3B+ board. This shield is based on the Semtech SX1272 chipset which operates in the 868 MHz ISM unlicensed frequency band. On the other hand, the IoT device is based on Arduino MKR WAN 1300 boards which offer LoRa connectivity through an Atmel SAMD21 and Murata CMWX1ZZABZ LoRa module, and a DHT22 temperature and humidity sensor as the information source.

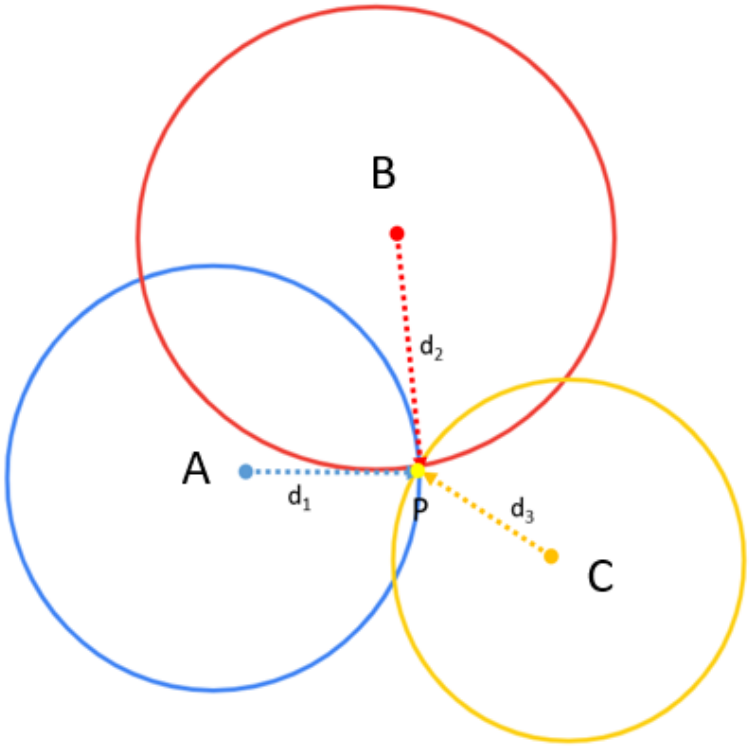

Figure 6.5: Circles drawn with three gateways with different positions: Trilateration Algorithm.

6.4 Outdoor Test & Results

The tests conducted with and without the drone are considered the first step for exposing the position of the IoT device before performing jamming attack on that device [1].

[1]This work was done as a team work in the lab composed of two parts: position estimation and jamming attack. The jamming attack was performed and tested successfully by another lab colleague: *Alessandro Fausto*

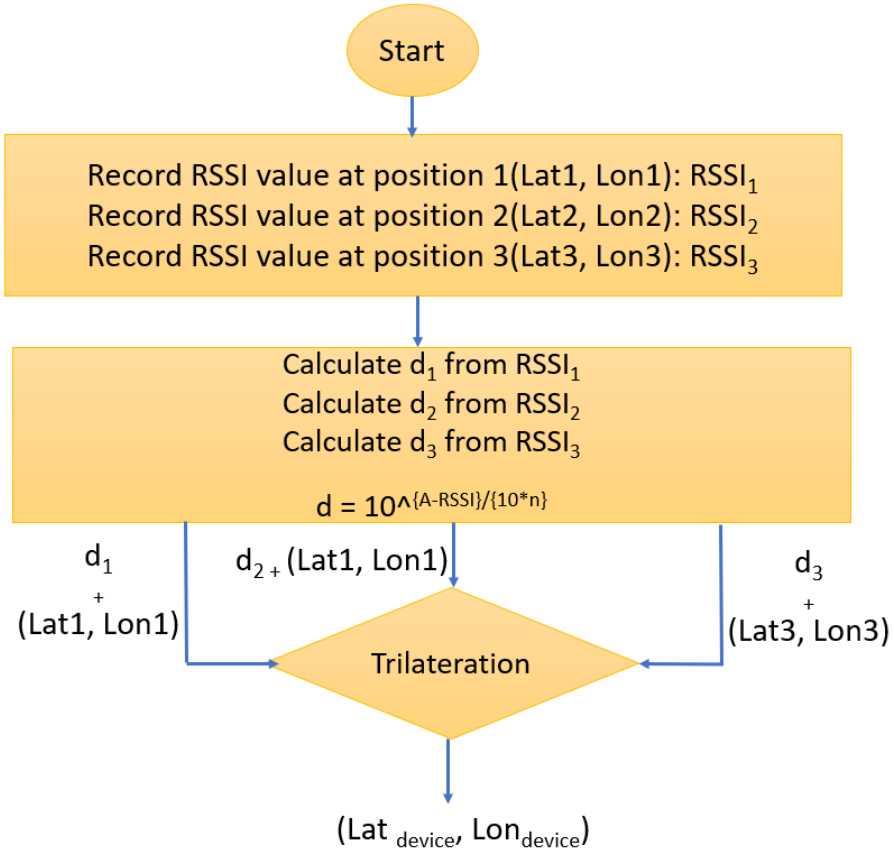

Figure 6.6: Flow chart for the localization of IoT device.

Test 1: Without Drone

The experiment was conducted according to the described procedure at an outdoor area in Line Of Sight (LOS) conditions between the gateway and the device (no obstacles between them) as shown in Figure 6.7.

Figure 6.8 shows the relationship between RSSI and distance between the gateway and the sensor, which is inversely exponential, i.e., When the distance between the gateway and the sensor node increases, the RSSI value gradually decreases due to the path loss effect.

To obtain the values of A and n for the LoRaWAN hardware setup and the outdoor environment, different RSSI values were collected at d = 1m between the gateway and the sensor. After this phase, the average value of A is obtained and is equal to -35.8 dBm. To get

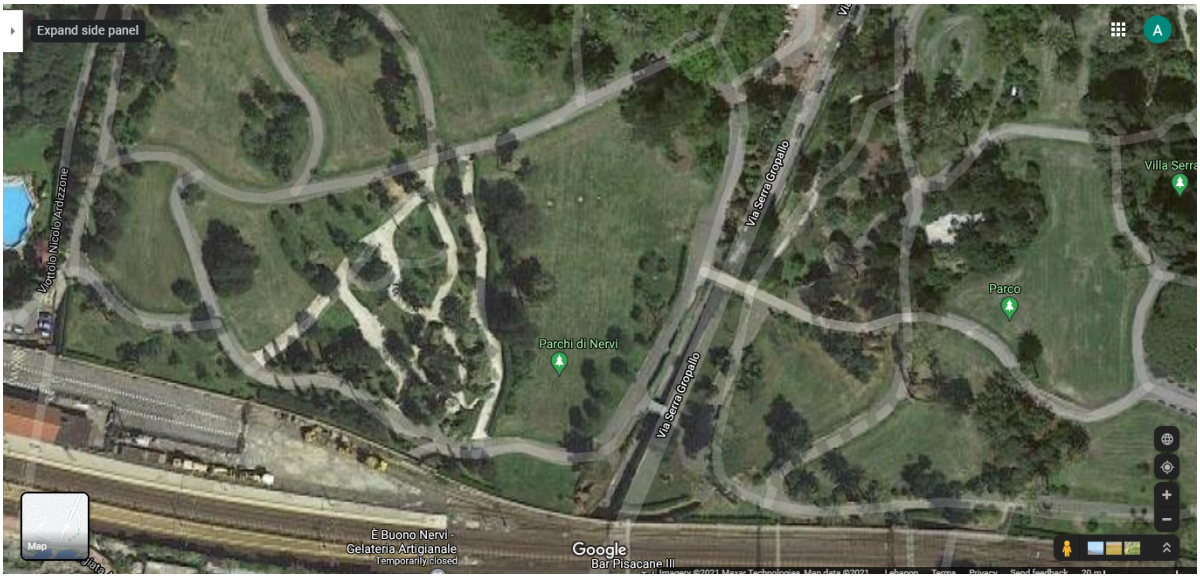

Figure 6.7: Outdoor testing environment

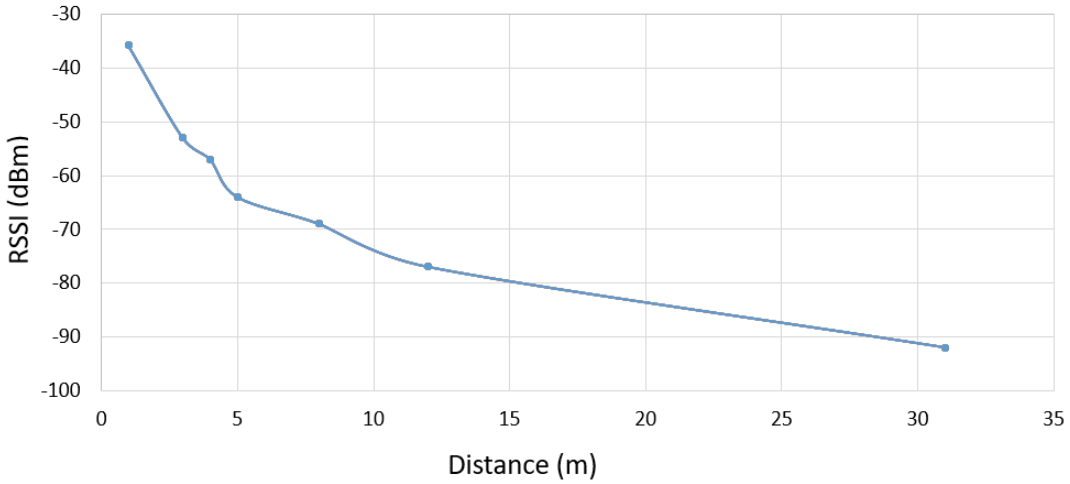

Figure 6.8: Variation of the RSSI values (in dBm) with respect to the distance (in meters)

the value of n, the distance between these nodes was increased from 2m to 8m with 1m step. Different values of n were obtained according to the following Equation, obtained reversing Equation (6.5):

$$n = \frac{A - RSSI}{10 \cdot log_{10} d} \tag{6.9}$$

and the average value of n is 3.75.

After obtaining the A and n values, the gateway was placed in three different positions at three different distances from the sensor: 3m, 12m and 31m, respectively. The values of the RSSI was measured at each position and saved to be used later for distance estimation using Equation (6.6). The distances obtained from the different RSSI values received by the gateway are given to the trilateration function to retrieve the coordinates of the sensor. To test our experiment, the GPS coordinates of the sensor were obtained before and then compared to the one obtained from the localization algorithm and presented on the map as shown in Figure 6.9. The accuracy is checked by calculating the distance between these two positions by using the Harvisne distance formula with an error of 11 meters.

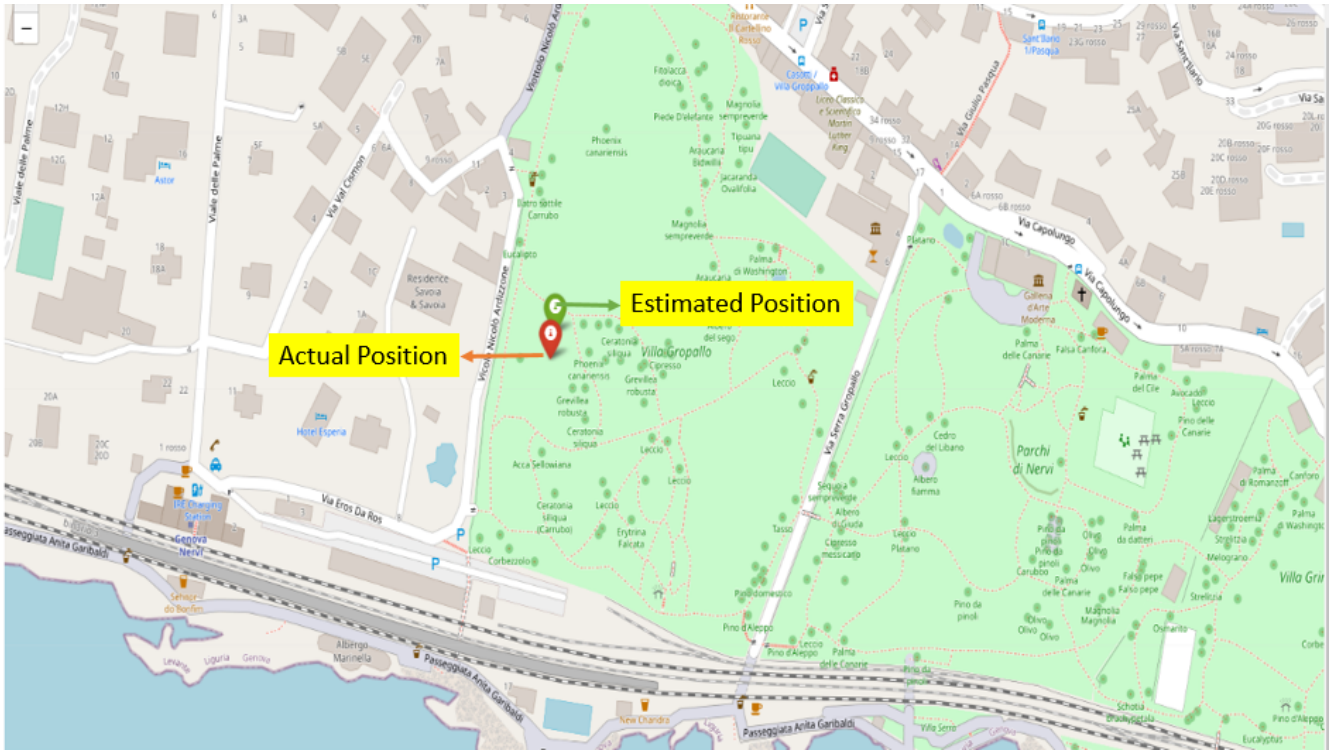

Figure 6.9: The position of the actual sensor(red marker) and the estimated position of the sensor(green marker) using trilateration algorithm.

Test 2: With Drone

Another test is performed using a drone where this drone flies at different positions over the area where the sensor is deployed as shown in Figure 6.10. A new parameter is considered when the drone is used: *altitude*. Equations 6.7 and 6.8 become as follows:

$$\begin{cases} \sqrt{(x-x_a)^2+(y-y_a)^2+(z-z_a)^2} = d_1 \\ \sqrt{(x-x_b)^2+(y-y_b)^2+(z-z_b)^2} = d_2 \\ \sqrt{(x-x_c)^2+(y-y_c)^2+(z-z_c)^2} = d_3 \end{cases} \tag{6.10}$$

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2(x_a-x_c).2(y_a-y_c).2(z_a-z_c) \\ 2(x_b-x_c).2(y_b-y_c).2(z_b-z_c) \end{bmatrix}^{-1} \begin{bmatrix} (d_b)^2-(d_a)^2+(x_a)^2-(x_b)^2+(y_a)^2-(y_b)^2+(z_a)^2-(z_b)^2 \\ (d_c)^2-(d_a)^2+(x_a)^2-(x_c)^2+(y_a)^2-(y_c)^2+(z_a)^2-(z_c)^2 \end{bmatrix} \tag{6.11}$$

The GPS coordinates of the different drone positions are recorded along with that of the sensor to test the final accuracy of the algorithm. These values are mapped as shown in Figure 6.11. The same values of A and n are used since the surrounding environment is a similar one.

After running the localization algorithm, the estimated position of the sensor was far from the actual one with 25 meters according to the Haversine formula as shown in Figure 6.12. This error is due to the different environmental conditions such as wind or the presence of some obstacles as hills, which affects the signal strength. However, RSSI can still give good results for localization which allows the attacker to perform different physical attacks on an IoT node in a simple and easy way.

6.5 Conclusion

In this chapter, the concept of using RSSI values from LoRa sensors can be useful for localization purposes. Using trilateration algorithm, the results show that the developed distance model for distance estimation works in outdoor environments in LoS path. On the other hand, it can affect the results when changing the path to Non-Line-of-Sight (NLOS) due

Figure 6.10: Flying drone with LoRa gateway on-board

to the presence of specific obstacles such as hills. In both cases, the results obtained can provide the attacker a great opportunity to perform physical attacks and destroy the IoT network. To improve the efficiency of using RSSI for position estimation, more RSSI dataset can be developed along with a filtering method to omit the RSSI outliers which affect the results.

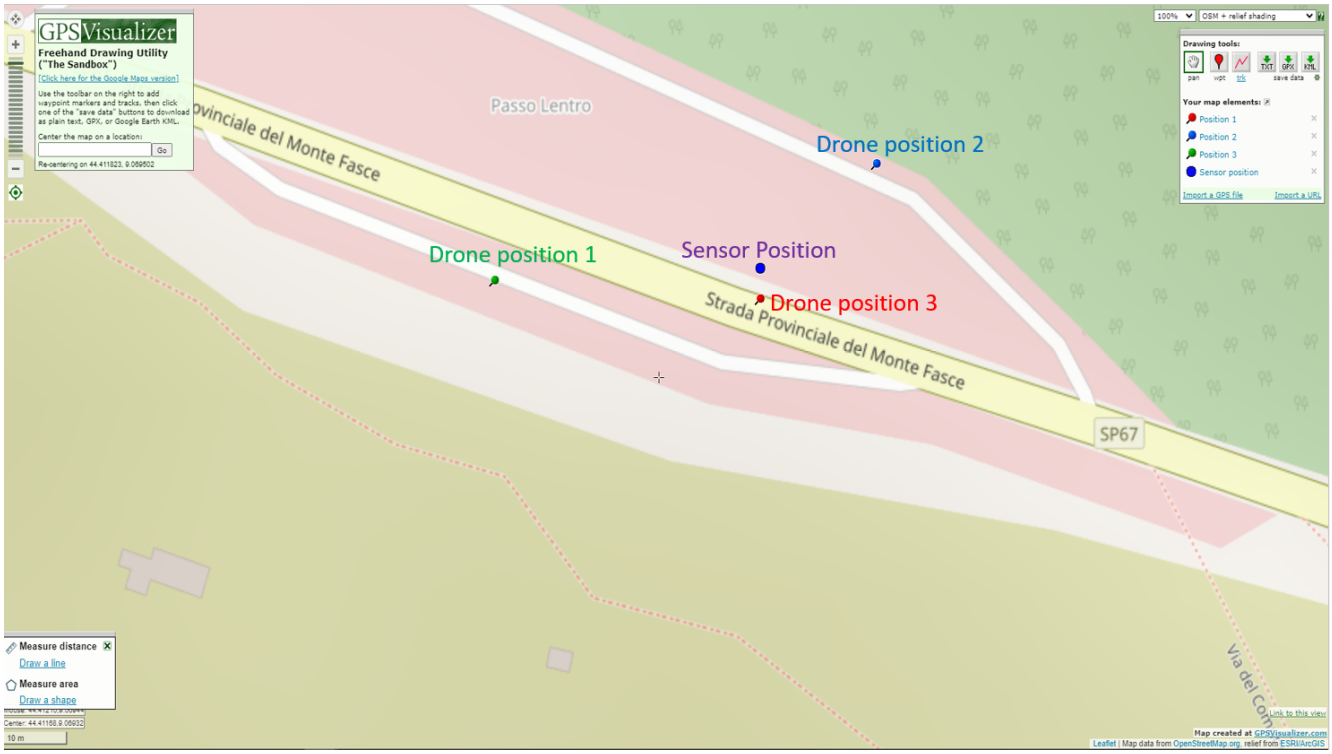

Figure 6.11: Layout of the different drone positions and the sensor position.

Figure 6.12: The position of the actual sensor VS the position of the estimation obtained from trilateration algorithm.

Chapter 7

Conclusion

7.1 Conclusion

We have investigated the problem of communication means lack in remote and rural areas. We have proposed a solution based on a flying gateway for IoT networks. This flying gateway exploits the LoRa IoT communication protocol extending the coverage to rural and remote areas through the usage of satellite links.

IoFT is an emerging concept which is attracting the attention of both research and commercial activities. The integration of UAV in the IoT field leads to multiple advantages for the data collection aim. Some of the new emerging scenarios, especially the ones involving rural an remote areas without any kind of terrestrial infrastructure, can benefit from a flying and deployable on-demand solution to allow gathering all the data generated by multiple IoT devices spread in wide areas.

We have decided to implement the flying gateway based on edge devices making it an efficient solution that guarantee the packets transmission from IoT devices to their cloud platform. The flying gateway has two different role whose purpose is to deliver data from rural areas to the Internet minimizing the average data delivery time and resource consumption. The first role is *"Flying LoRaWAN Gateway"*. This gateway is based on an edge device (RPI) equipped with LoRa shield providing the LoRaWAN connectivity to the IoT end devices deployed. The

aim of this role or solution is to extend the LoRa coverage range in rural and remote areas which are hard to reach. This flying gateway offers a power efficient and time minimizing solution for data collection purpose in hard to reach areas that lack the proper or traditional communication means. To more extend the coverage of a LoRaWAN flying gateway, satellite simulated link was presented and implemented between the gateway and the LoRa to study its performance. The aim of this flying gateway is to extend the current limited coverage of the commercial IoT solutions and to integrate them with the terrestrial network. The exploitation of the satellite connectivity has been considered especially to overcome the lack of other communication infrastructure in certain locations, such as rural and remote areas, and looking for the possible integration of these network foreseen in the 5G framework.

The second role of this flying gateway is *"LoRaWAN Data Mule".* Similar to the *LoRaWAN flying gateway*, the aim is to first extend the coverage and guarantee the data exchange between IoT devices and the cloud platform. However, this solution aims to collect and store the IoT device's data until it gains Internet connectivity. This data mule travels over the IoT sensors field, collect the data, store them on-board of the gateway and goes back to its starting point where Internet connectivity is available. This will assure the data delivery to the cloud from remote areas lacking for the traditional communication means.

In order to test the two proposed solutions and study their performance, we developed a testbed implementing the gateway functionality. The testbed is based on edge devices: Raspberry Pi 3B+ board that offers power and cost efficient solution. This RPI is equipped by special Rak2245 shield which provides the LoRa connectivity. This testbed provides low data rate LoRa radio links in ultra-fast speed and able of managing packets from many remote dispersed IoT end points, thus helps in the development of a full LoRa system. In addition, this gateway is installed on-board of a UAV and powered by a battery pack as an external power energy source for operating.

Both approaches have been tested in indoor and outdoor environments and their performance has been studied and analyzed. The results obtained regarding the signal quality, power consumption and the gateway status show the feasibility of the proposed solutions in terms of guaranteed data delivery and coverage extension. In addition, the exploitation of the satellite

connectivity has been considered especially to overcome the lack of other communication infrastructure in certain locations, such as rural and remote areas, and looking for the possible integration of these network foreseen in the 5G framework.
In addition to the aforementioned approaches purposed, the physical security of LoRa has been exploited using the RSSI value of the signal received by the gateway. Despite the fact that RSSI value alone does not give very accurate results when coming to localization or location estimation, we adopted this feature to identify and estimate the position of a LoRa IoT device for physical attack purpose since it does not require any special or additional hardware components. The main aim from the position estimation is to allow the attacker know the device position to perform different physical attacks such as changing the firmware, destroying the device, or even changing its functionality.
Trilateration was selected and developed for position estimation using RSSI values of the LoRa signal. Different outdoor tests were performed with and without the UAV to evaluate our localization algorithm and the results obtained allow us to estimate the position of IoT device with acceptable error.
The concept of using RSSI values from LoRa sensors can be useful for localization purposes. Using trilateration algorithm, the results show that the developed distance model for distance estimation works in outdoor environments in LoS path. On the other hand, it can affect the results when changing the path to Non-Line-of-Sight (NLOS) due to the presence of specific obstacles such as hills. In both cases, the results obtained can provide the attacker a great opportunity to perform physical attacks and destroy the IoT network. To improve the efficiency of using RSSI for position estimation, more RSSI dataset can be developed along with a filtering method to omit the RSSI outliers which affect the results.

7.2 Potential Future Work

The ideas put forward in this thesis can be extended as follow.
The implementation of the satellite link can be emulated using a specific software whose aim is to emulate the satellite behavior in real time, after which the whole testbed will be ready to

give more precise results with the LoRa flying gateway. This can be carried using the *OpenSand* satellite emulator which is composed of: (i) Satellite, (ii) Satellite Gateway and (iii) Satellite Terminal. These correspond to the main components in any satellite-integrated application. Thus, extending the coverage of LoRa network in rural and remote areas lacking for the traditional communication means.

Another option for improving the testbed is to increase the number of sensor or IoT devices used and deploy them in a wider area. This will increase the efficiency of both the flying gateway and data mule.

Regarding the position estimation using LoRa RSSI values for security reasons, it can be improved by using different LoRa hardware implementations that present better RSSI sensitivity and dynamic range at similar cost. Moreover, the temperature and humidity can be monitored to determine their impact on the RSSI and results obtained using temperature and humidity sensors.

Bibliography

[1] B. Foubert and N. Mitton, "Long-range wireless radio technologies: A survey," *Future internet*, vol. 12, no. 1, p. 13, 2020.

[2] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, 2017.

[3] "Rp2-1.0.3 lorawan® regional parameters," "https://lora-alliance.org/wp-content/uploads/2021/05/RP002-1.0.3-FINAL-1.pdf ".

[4] L. Alliance, "What is lorawan® specification," "https://lora-alliance.org/about-lorawan/".

[5] Semtech, "SX1301 Datasheet," https://semtech.my.salesforce.com/sfc/p/#E0000000JelG/a/44000000MDnR/Et1KWLCuNDI6MDagfSPAvqqp.Y869Flgs1LleWyfjDY, 2021.

[6] U. Nazir, N. Shahid, M. Arshad, and S. H. Raza, "Classification of localization algorithms for wireless sensor network: A survey," in *2012 International conference on open source systems and technologies*. IEEE, 2012, pp. 1–5.

[7] E. Shakshuki, A. A. Elkhail, I. Nemer, M. Adam, and T. Sheltami, "Comparative study on range free localization algorithms," *Procedia Computer Science*, vol. 151, pp. 501–510, 2019.

[8] E. Saad, M. Elhosseini, and A. Y. Haikal, "Recent achievements in sensor localization algorithms," *Alexandria engineering journal*, vol. 57, no. 4, pp. 4219–4228, 2018.

[9] Statista, "Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025," https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/, 2020.

[10] "LoRa™ Alliance to Officially Debut at Mobile World Congress; Now Accepting New Members," https://www.businesswire.com/news/home/20150219006638/en/LoRa%E2%84%A2-Alliance-to-Officially-Debut-at-Mobile-World-Congress-Now-Accepting-New-Members, 2015.

[11] L.-Y. Chen, H.-S. Huang, C.-J. Wu, Y.-T. Tsai, and Y.-S. Chang, "A lora-based air quality monitor on unmanned aerial vehicle for smart city," in *2018 International Conference on System Science and Engineering (ICSSE)*. IEEE, 2018, pp. 1–5.

[12] Y. Lin and R. Lee, "Application of multi-band networking and uav in natural environment protection and disaster prevention," in *2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)*. IEEE, 2019, pp. 176–178.

[13] B. Benites, E. Chávez, J. Medina, R. Vidal, and M. Chauca, "Lorawan applied in swarm drones: A focus on the use of fog for the management of water resources in lima-peru," in *Proceedings of the 5th International Conference on Mechatronics and Robotics Engineering*, 2019, pp. 171–176.

[14] L. Angrisani, A. Amodio, P. Arpaia, M. Asciolla, A. Bellizzi, F. Bonavolontà, R. Carbone, E. Caputo, G. Karamanolis, V. Martire *et al.*, "An innovative air quality monitoring system based on drone and iot enabling technologies," in *2019 IEEE International Workshop on Metrology for Agriculture and Forestry (MetroAgriFor)*. IEEE, 2019, pp. 207–211.

[15] A. Simo, S. Dzitac, I. Dzitac, M. Frigura-Iliasa, and F. M. Frigura-Iliasa, "Air quality assessment system based on self-driven drone and lorawan network," *Computer Communications*, vol. 175, pp. 13–24, 2021.

[16] S. Liu, X. Yang, and X. Zhou, "Development of a low-cost uav-based system for ch4 monitoring over oil fields," *Environmental technology*, pp. 1–10, 2020.

[17] K. Buchholz, "Commercial drones are taking off," https://www.statista.com/chart/17201/commecial-drones-projected-growth/, 2019.

[18] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Internet of mobile things: Overview of lorawan, dash7, and nb-iot in lpwans standards and supported mobility," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1561–1581, 2018.

[19] M. R. Palattella and N. Accettura, "Enabling internet of everything everywhere: Lpwan with satellite backhaul," in *2018 Global Information Infrastructure and Networking Symposium (GIIS)*. IEEE, 2018, pp. 1–5.

[20] A. Dimitrievski, S. Filiposka, F. J. Melero, E. Zdravevski, P. Lameski, I. M. Pires, N. M. Garcia, J. P. Lousado, and V. Trajkovik, "Rural healthcare iot architecture based on low-energy lora," *International journal of environmental research and public health*, vol. 18, no. 14, p. 7660, 2021.

[21] Z. Qu, G. Zhang, H. Cao, and J. Xie, "Leo satellite constellation for internet of things," *IEEE access*, vol. 5, pp. 18 391–18 401, 2017.

[22] I. I. Lysogor, L. S. Voskov, and S. G. Efremov, "Survey of data exchange formats for heterogeneous lpwan-satellite iot networks," in *2018 Moscow workshop on electronic and networking technologies (MWENT)*. IEEE, 2018, pp. 1–5.

[23] S. Goudarzi, N. Kama, M. H. Anisi, S. Zeadally, and S. Mumtaz, "Data collection using unmanned aerial vehicles for internet of things platforms," *Computers & Electrical Engineering*, vol. 75, pp. 1–15, 2019.

[24] R. Allen, M. Nekrasov, and E. Belding, "Data collection from outdoor iot 802.15. 4 sensor networks using unmanned aerial systems (poster)," in *Proceedings of the 17th Annual*

International Conference on Mobile Systems, Applications, and Services, 2019, pp. 564–565.

[25] D. F. Pigatto, M. Rodrigues, J. V. de Carvalho Fontes, A. S. R. Pinto, J. Smith, and K. R. L. J. C. Branco, "The internet of flying things," *Internet of Things A to Z: Technologies and Applications*, pp. 529–562, 2018.

[26] S. Zaidi, M. Atiquzzaman, and C. T. Calafate, "Internet of Flying Things (IoFT): A survey," *Computer Communications*, vol. 165, pp. 53–74, 2021.

[27] Q. F. Hassan, *Internet of things A to Z: technologies and applications*. John Wiley & Sons, 2018.

[28] M. A. Uddin, A. Mansour, D. Le Jeune, and E. H. M. Aggoune, "Agriculture internet of things: Ag-iot," in *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE, 2017, pp. 1–6.

[29] A. K. Saha, J. Saha, R. Ray, S. Sircar, S. Dutta, S. P. Chattopadhyay, and H. N. Saha, "Iot-based drone for improvement of crop quality in agricultural field," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2018, pp. 612–615.

[30] G. Faraci, A. Raciti, S. Rizzo, and G. Schembra, "A 5g platform for unmanned aerial monitoring in rural areas: Design and performance issues," in *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*. IEEE, 2018, pp. 237–241.

[31] O. Elijah, T. Rahman, H. Yeen, C. Leow, M. Sarijari, A. Aris, J. Salleh, and C. Han, "Application of uav and low power wide area communication technology for monitoring of river water quality," in *2018 2nd International Conference on Smart Sensors and Application (ICSSA)*. IEEE, 2018, pp. 105–110.

[32] J.-I. Hernández-Vega, E. R. Varela, N. H. Romero, C. Hernández-Santos, J. L. S. Cuevas, and D. G. P. Gorham, "Internet of things (iot) for monitoring air pollutants with an

unmanned aerial vehicle (uav) in a smart city," in *Smart technology*. Springer, 2018, pp. 108–120.

[33] A. Agarwal, V. Shukla, R. Singh, A. Gehlot, and V. Garg, "Design and development of air and water pollution quality monitoring using iot and quadcopter," in *Intelligent Communication, Control and Devices*. Springer, 2018, pp. 485–492.

[34] Q. Yang, L. Sun, J. Jie, C. Feng, J. Cao, and Q. Lai, "The design of quad-rotor environmental monitoring system based on internet of things," in *2015 IEEE 16th International Conference on Communication Technology (ICCT)*. IEEE, 2015, pp. 97–101.

[35] Z. Hu, Z. Bai, Y. Yang, Z. Zheng, K. Bian, and L. Song, "Uav aided aerial-ground iot for air quality sensing in smart city: Architecture, technologies, and implementation," *IEEE Network*, vol. 33, no. 2, pp. 14–22, 2019.

[36] N. Kalatzis, M. Avgeris, D. Dechouniotis, K. Papadakis-Vlachopapadopoulos, I. Roussaki, and S. Papavassiliou, "Edge computing in iot ecosystems for uav-enabled early fire detection," in *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*. IEEE, 2018, pp. 106–114.

[37] J. S. Kumar, M. A. Zaveri, S. Kumar, and M. Choksi, "Situation-aware conditional sensing in disaster-prone areas using unmanned aerial vehicles in iot environment," in *Data and Communication Networks*. Springer, 2019, pp. 135–146.

[38] X. Liu, Z. Li, N. Zhao, W. Meng, G. Gui, Y. Chen, and F. Adachi, "Transceiver design and multihop d2d for uav iot coverage in disasters," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1803–1815, 2018.

[39] C. Luo, J. Nightingale, E. Asemota, and C. Grecos, "A uav-cloud system for disaster sensing applications," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. IEEE, 2015, pp. 1–5.

[40] M. Choksi, M. A. Zaveri, J. S. Kumar, and S. K. Pandey, "Cloud-based real time data acquisition in iot environment for post disaster management," in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2018, pp. 1–6.

[41] N. H. Motlagh, M. Bagaa, and T. Taleb, "Uav-based iot platform: A crowd surveillance use case," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 128–134, 2017.

[42] S. Qazi, A. S. Siddiqui, and A. I. Wagan, "Uav based real time video surveillance over 4g lte," in *2015 International Conference on Open Source Systems & Technologies (ICOSST)*. IEEE, 2015, pp. 141–145.

[43] C. Grasso and G. Schembra, "Design of a uav-based videosurveillance system with tactile internet constraints in a 5g ecosystem," in *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*. IEEE, 2018, pp. 449–455.

[44] A. Giyenko and Y. Im Cho, "Intelligent uav in smart cities using iot," in *2016 16th international conference on control, automation and systems (ICCAS)*. IEEE, 2016, pp. 207–210.

[45] F. Qi, X. Zhu, G. Mang, M. Kadoch, and W. Li, "Uav network and iot in the sky for future smart cities," *IEEE Network*, vol. 33, no. 2, pp. 96–101, 2019.

[46] F. Al-Turjman and S. Alturjman, "5g/iot-enabled uavs for multimedia delivery in industry-oriented applications," *Multimedia Tools and Applications*, vol. 79, no. 13, pp. 8627–8648, 2020.

[47] V. Sharma, G. Choudhary, Y. Ko, and I. You, "Behavior and vulnerability assessment of drones-enabled industrial internet of things (iiot)," *IEEE Access*, vol. 6, pp. 43 368–43 383, 2018.

[48] R. Giuliano, G. C. Cardarilli, C. Cesarini, L. Di Nunzio, F. Fallucchi, R. Fazzolari, F. Mazzenga, M. Re, and A. Vizzarri, "Indoor localization system based on bluetooth low energy for museum applications," *Electronics*, vol. 9, no. 6, p. 1055, 2020.

[49] B. Yang, L. Guo, R. Guo, M. Zhao, and T. Zhao, "A novel trilateration algorithm for rssi-based indoor localization," *IEEE Sensors Journal*, vol. 20, no. 14, pp. 8164–8172, 2020.

[50] M. T. Hoang, B. Yuen, X. Dong, T. Lu, R. Westendorp, and K. Reddy, "Recurrent neural networks for accurate rssi indoor localization," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 639–10 651, 2019.

[51] S. Sadowski and P. Spachos, "Rssi-based indoor localization with the internet of things," *IEEE Access*, vol. 6, pp. 30 149–30 161, 2018.

[52] W. Xue, W. Qiu, X. Hua, and K. Yu, "Improved wi-fi rssi measurement for indoor localization," *IEEE Sensors Journal*, vol. 17, no. 7, pp. 2224–2230, 2017.

[53] A. Bhardwaj, "Terrestrial and satellite-based positioning and navigation systems—a review with a regional and global perspective," in *Engineering Proceedings*, vol. 2, no. 1. Multidisciplinary Digital Publishing Institute, 2020, p. 41.

[54] J. C. Guerrero, C. Quezada-V, and D. Chacon-Troya, "Design and implementation of an intelligent cane, with proximity sensors, gps localization and gsm feedback," in *2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)*. IEEE, 2018, pp. 1–4.

[55] H. Sallouha, A. Chiumento, and S. Pollin, "Localization in long-range ultra narrow band iot networks using rssi," in *2017 IEEE International Conference on Communications (ICC)*. IEEE, 2017, pp. 1–6.

[56] E. Goldoni, L. Prando, A. Vizziello, P. Savazzi, and P. Gamba, "Experimental data set analysis of rssi-based indoor and outdoor localization in lora networks," *Internet Technology Letters*, vol. 2, no. 1, p. e75, 2019.

[57] M. Aernouts, N. BniLam, R. Berkvens, and M. Weyn, "Simulating a combination of tdoa and aoa localization for lorawan," in *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*. Springer, 2019, pp. 756–765.

[58] M. Aernouts, N. BniLam, N. Podevijn, D. Plets, W. Joseph, R. Berkvens, and M. Weyn, "Combining tdoa and aoa with a particle filter in an outdoor lorawan network," in *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 2020, pp. 1060–1069.

[59] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot," *Journal of Network and Computer Applications*, vol. 149, p. 102481, 2020.

[60] M. M. Ahemd, M. A. Shah, and A. Wahid, "Iot security: A layered approach for attacks & defenses," in *2017 international conference on Communication Technologies (ComTech)*. IEEE, 2017, pp. 104–110.

[61] S. K. Lee, M. Bae, and H. Kim, "Future of iot networks: A survey," *Applied Sciences*, vol. 7, no. 10, p. 1072, 2017.

[62] S. Kahveci and T. Atasoy, "From wireless personal area network (wpan) to long range (lora) technology," in *2019 11th International Conference on Electrical and Electronics Engineering (ELECO)*. IEEE, 2019, pp. 679–681.

[63] F. Samie, L. Bauer, and J. Henkel, "Iot technologies for embedded computing: A survey," in *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)*. IEEE, 2016, pp. 1–10.

[64] P. Bhoyar, P. Sahare, S. B. Dhok, and R. B. Deshmukh, "Communication technologies and security challenges for internet of things: A comprehensive review," *AEU-International Journal of Electronics and Communications*, vol. 99, pp. 81–99, 2019.

[65] Ericsson, "Cellular networks for massive iot." https://www.ericsson.com/4ada75/assets/local/reports-papers/white-papers/wp_iot.pdf, 2016.

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

[67] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu, and X. Du, "From iot to 5g i-iot: The next generation iot-based intelligent algorithms and 5g technologies," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 114–120, 2018.

[68] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of things (iot) communication protocols," in *2017 8th International conference on information technology (ICIT)*. IEEE, 2017, pp. 685–690.

[69] Telensa, "Ultra narrow band (unb) smart city network," https://info.telensa.com/hubfs/Resources%20page%20files/datasheet_telensa_planet_network.pdf.

[70] Q. M. Qadir, T. A. Rashid, N. K. Al-Salihi, B. Ismael, A. A. Kist, and Z. Zhang, "Low power wide area networks: A survey of enabling technologies, applications and interoperability needs," *IEEE Access*, vol. 6, pp. 77 454–77 473, 2018.

[71] A. Zourmand, A. L. K. Hing, C. W. Hung, and M. AbdulRehman, "Internet of things (iot) using lora technology," in *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*. IEEE, 2019, pp. 324–330.

[72] L. Alliance, "Lora regional parameters," "https://lora-alliance.org/resource$_h$$ub/rp2-1-0-3-lorawan-regional-parameters/$", 2021.

[73] "Frequency plans by country," "https://www.thethingsnetwork.org/docs/lorawan/frequencies-by-country/ ".

[74] O. B. A. Seller, "Wireless communication method," May 9 2017, uS Patent 9,647,718.

[75] K.-H. Phung, H. Tran, Q. Nguyen, T. T. Huong, and T.-L. Nguyen, "Analysis and assessment of lorawan," in *2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)*. IEEE, 2018, pp. 241–246.

[76] K. Staniec, "The internet of things narrow-band lpwan/unb systems," in *Radio Interfaces in the Internet of Things Systems*. Springer, 2020, pp. 93–117.

[77] J. Haxhibeqiri, E. De Poorter, I. Moerman, and J. Hoebeke, "A survey of lorawan for iot: From technology to application," *Sensors*, vol. 18, no. 11, p. 3995, 2018.

[78] M. A. Ertürk, M. A. Aydın, M. T. Büyükakkaşlar, and H. Evirgen, "A survey on lorawan architecture, protocol and technologies," *Future Internet*, vol. 11, no. 10, p. 216, 2019.

[79] L. Vangelista, A. Zanella, and M. Zorzi, "Long-range iot technologies: The dawn of lora™," in *Future access enablers of ubiquitous and intelligent infrastructures*. Springer, 2015, pp. 51–58.

[80] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A study of lora: Long range & low power networks for the internet of things," *Sensors*, vol. 16, no. 9, p. 1466, 2016.

[81] M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund, "Formal security analysis of lorawan," *Computer Networks*, vol. 148, pp. 328–339, 2019.

[82] D. Basu, T. Gu, and P. Mohapatra, "Security issues of low power wide area networks in the context of lora networks," *arXiv preprint arXiv:2006.16554*, 2020.

[83] L. Alliance, "Lorawan® specification v1.0," https://lora-alliance.org/resource_hub/lorawan-specification-v1-0/, January, 2015.

[84] "Lorawan™ 1.1 specification," "https://lora-alliance.org/wp-content/uploads/2020/11/lorawantm$_s pecification_v$1.1.*pdf*".

[85] I. Butun, N. Pereira, and M. Gidlund, "Demystifying security of lorawan v1. 1," 2018.

[86] "End device activation," "https://www.thethingsnetwork.org/docs/lorawan/end-device-activation/".

[87] R. Nordin, H. Mohamad, M. Behjati, A. H. Kelechi, N. Ramli, K. Ishizu, F. Kojima, M. Ismail, and M. Idris, "The world-first deployment of narrowband iot for rural hydrological monitoring in unesco biosphere environment," in *2017 IEEE 4th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA)*. IEEE, 2017, pp. 1–5.

[88] M. Shahidul Islam, M. T. Islam, A. F. Almutairi, G. K. Beng, N. Misran, and N. Amin, "Monitoring of the human body signal through the internet of things (iot) based lora wireless network system," *Applied Sciences*, vol. 9, no. 9, p. 1884, 2019.

[89] Y.-B. Lin, Y.-W. Lin, C.-Y. Hsiao, and S.-Y. Wang, "Location-based iot applications on campus: The iottalk approach," *Pervasive and mobile computing*, vol. 40, pp. 660–673, 2017.

[90] S. Chen, B. Liu, X. Chen, Y. Zhang, and G. Huang, "Framework for adaptive computation offloading in iot applications," in *Proceedings of the 9th Asia-Pacific Symposium on Internetware*, 2017, pp. 1–6.

[91] M. Luvisotto, F. Tramarin, L. Vangelista, and S. Vitturi, "On the use of lorawan for indoor industrial iot applications," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[92] T. A. Ali, V. Choksi, and M. B. Potdar, "Precision agriculture monitoring system using green internet of things (g-iot)," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2018, pp. 481–487.

[93] Y. Saleem, N. Crespi, M. H. Rehmani, and R. Copeland, "Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions," *IEEE Access*, vol. 7, pp. 62 962–63 003, 2019.

[94] W. Meng, R. Ma, and H.-H. Chen, "Smart grid neighborhood area networks: a survey," *IEEE Network*, vol. 28, no. 1, pp. 24–32, 2014.

[95] G. Xu, W. Yu, D. Griffith, N. Golmie, and P. Moulema, "Toward integrating distributed energy resources and storage devices in smart grid," *IEEE internet of things journal*, vol. 4, no. 1, pp. 192–204, 2016.

[96] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[97] J. Pan, R. Jain, S. Paul, T. Vu, A. Saifullah, and M. Sha, "An internet of things framework for smart energy in buildings: designs, prototype, and experiments," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 527–537, 2015.

[98] W. Li, H. Song, and F. Zeng, "Policy-based secure and trustworthy sensing for internet of things in smart cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 716–723, 2017.

[99] A. Ghasempour, "Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges," *Inventions*, vol. 4, no. 1, p. 22, 2019.

[100] J. Liu, X. Li, X. Chen, Y. Zhen, and L. Zeng, "Applications of internet of things on smart grid in china," *13th International Conference on Advanced Communication Technology (ICACT)*, 2011.

[101] F. S. e Silva, C. Barriquello, L. Canha, D. Bernardon, and W. S. Hokama, "Deployment of lora wan network for rural smart grid in brazil," *IEEE PES Transmission & Distribution Conference and Exhibition-Latin America (T&D-LA)*, 2018.

[102] G. Wibisono, S. G. Permata, A. Awaludin, and P. Suhasfan, "Development of advanced metering infrastructure based on lora wan in pln bali toward bali eco smart grid," *Saudi Arabia Smart Grid (SASG)*, pp. 1–4, 2017.

[103] M. Nouman Rafi and M. Muaaz, "Performance evaluation of the lora protocol in the context of smart meter," *arXiv preprint arXiv:1907.12355*, 2019.

[104] "Energyhive," https://www.energyhive.com/, 2020, [Online; accessed 10-October-2020].

[105] D. Kyriazis, T. Varvarigou, D. White, A. Rossi, and J. Cooper, "Sustainable smart city iot applications: Heat and electricity management & eco-conscious cruise control for public transportation," *14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, 2013.

[106] C. H. Barriquello, D. P. Bernardon, L. N. Canha, F. E. S. e Silva, D. S. Porto, and M. J. da Silveira Ramos, "Performance assessment of a low power wide area network in rural smart grids," *52nd international universities power engineering conference (UPEC)*, 2017.

[107] N. Varsier and J. Schwoerer, "Capacity limits of lorawan technology for smart metering applications," *International Conference on Communications (ICC)*, 2017.

[108] M. M. Rana and L. Li, "Renewable microgrid state estimation using the internet of things communication network," *19th International Conference on Advanced Communication Technology (ICACT)*, 2017.

[109] R. Carli, G. Cavone, S. Ben Othman, and M. Dotoli, "Iot based architecture for model predictive control of hvac systems in smart buildings," *Sensors*, vol. 20, no. 3, p. 781, 2020.

[110] G. Hafeez, Z. Wadud, I. U. Khan, I. Khan, Z. Shafiq, M. Usman, and M. U. A. Khan, "Efficient energy management of iot-enabled smart homes under price-based demand response program in smart grid," *Sensors*, vol. 20, no. 11, p. 3155, 2020.

[111] A. Sampathkumar, S. Murugan, M. Sivaram, V. Sharma, K. Venkatachalam, and M. Kalimuthu, "Advanced energy management system for smart city application using the iot," in *Internet of Things in Smart Technologies for Sustainable Urban Development*. Springer, 2020, pp. 185–194.

[112] P. Pawar, M. TarunKumar *et al.*, "An iot based intelligent smart energy management system with accurate forecasting and load strategy for renewable generation," *Measurement*, vol. 152, p. 107187, 2020.

[113] "Digital water grid management," https://www.birdz.com/en/digital-water-grid-management/, [Online; accessed 08-October-2020].

[114] "Czech republic rolls out nationwide lorawan network," https://www.smartcitiesworld.net/news/news/czech-republic-rolls-out-nationwide-lorawan-network-3609, 2018, [Online; accessed 08-October-2020].

[115] "Kaifa: Innovation brings a better life." http://www.kaifametering.com/public/index.php, [Online; accessed 08-October-2020].

[116] "Orion m2m," http://orion-m2m.com/en/, 2016, [Online; accessed 08-October-2020].

[117] B. E. Bilgin, S. Baktir, and V. C. Gungor, "Collecting smart meter data via public transportation buses," *IET Intelligent Transport Systems*, vol. 10, no. 8, pp. 515–523, 2016.

[118] K. G. Ngandu, K. Ouahada, and S. Rimer, "Smart meter data collection using public taxis," *Sensors*, vol. 18, no. 7, p. 2304, 2018.

[119] R. Shenoy and B. Keshavan, "Hybrid drone for data transaction," *IEEE International Conference on Smart Energy Grid Engineering (SEGE)*, 2017.

[120] A. Trotta, M. Di Felice, L. Bononi, E. Natalizio, L. Perilli, E. F. Scarselli, T. S. Cinotti, and R. Canegallo, "Bee-drones: Energy-efficient data collection on wake-up radio-based wireless sensor networks," *IEEE Conference on Computer Communications (INFOCOM) Workshops*, 2019.

[121] G. Giambene, E. O. Addo, and S. Kota, "5g aerial component for iot support in remote rural areas," in *2019 IEEE 2nd 5G World Forum (5GWF)*. IEEE, 2019, pp. 572–577.

[122] Arduino, "Arduino mkr wan 1300 (lora connectivity)," https://store.arduino.cc/collections/mkr-family/products/arduino-mkr-wan-1300-lora-connectivity.

[123] RakWireless, "Rak2245 pi hat wislink lpwan concentrator datasheet," https://docs.rakwireless.com/Product-Categories/WisLink/RAK2245-Pi-HAT/Datasheet/#specifications.

[124] TTN, "Network architecture," https://www.thethingsnetwork.org/docs/network/architecture/.

[125] chirpstack, "Chirpstack lorawan network server," https://www.chirpstack.io/network-server/.

[126] ESA, "Types of orbits," https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits, 2020.

[127] X. Berger, "RPI-Monitor: Real time monitoring for embedded devices," https://github.com/XavierBerger/RPi-Monitor, 2017.

[128] Freepik, "Design vector created by macrovector," https://www.freepik.com/vectors/landscape.

[129] ChirpStack, "Chirpstack open-source lorawan® network and application servers," https://www.chirpstack.io/, 2021.

[130] Semtech, "Lora® and lorawan®:a technical overview," https://lora-developers.semtech.com/uploads/documents/files/LoRa$_a$nd$_L$oRaWAN − A$_T$ech$_O$verview − Downloadable.pdf, February, 2020.

[131] H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi, and G. B. Wills, "Security, cybercrime and digital forensics for iot," in *Principles of internet of things (IoT) ecosystem: Insight paradigm.* Springer, 2020, pp. 551–577.

[132] H. F. Atlam and G. B. Wills, "IoT security, privacy, safety and ethics," in *Digital twin technologies and smart cities.* Springer, 2020, pp. 123–149.

[133] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[134] L. Alliance, "LoRaWAN® Specification v1.0," https://lora-alliance.org/wp-content/uploads/2020/11/2015_-_lorawan_specification_1r0_611_1.pdf.

[135] ——, "LoRaWAN® Specification v1.1," https://lora-alliance.org/wp-content/uploads/2020/11/lorawantm_specification_-v1.1.pdf.

[136] A. K. Paul and T. Sato, "Localization in wireless sensor networks: A survey on algorithms, measurement techniques, applications and challenges," *Journal of sensor and actuator networks*, vol. 6, no. 4, p. 24, 2017.

[137] H. P. Mistry and N. H. Mistry, "Rssi based localization scheme in wireless sensor networks: A survey," in *2015 Fifth International Conference on Advanced Computing & Communication Technologies.* IEEE, 2015, pp. 647–652.

[138] M. Allen, S. Baydere, E. Gaura, and G. Kucuk, "Evaluation of localization algorithms," in *Localization Algorithms and Strategies for Wireless Sensor Networks: Monitoring and Surveillance Techniques for Target Tracking.* IGI Global, 2009, pp. 348–379.

[139] J. Rezazadeh, M. Moradi, and A. S. Ismail, "Fundamental metrics for wireless sensor networks localization." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 2, no. 4, 2012.

[140] J. Upadhyay, A. Rawat, D. Deb, V. Muresan, and M.-L. Unguresan, "An rssi-based localization, path planning and computer vision-based decision making robotic system," *Electronics*, vol. 9, no. 8, p. 1326, 2020.

[141] N. Chuku and A. Nasipuri, "Rssi-based localization schemes for wireless sensor networks using outlier detection," *Journal of Sensor and Actuator Networks*, vol. 10, no. 1, p. 10, 2021.

[142] T. Wattananavin, K. Sengchuai, N. Jindapetch, and A. Booranawong, "A comparative study of rssi-based localization methods: Rssi variation caused by human presence and movement," *Sensing and Imaging*, vol. 21, no. 1, pp. 1–20, 2020.

[143] R. Tazawa, N. Honma, A. Miura, and H. Minamizawa, "Rssi-based localization using wireless beacon with three-element array," *IEICE Transactions on Communications*, 2017.

[144] P. Anusha, S. Anand, and S. Sinha, "Rssi-based localization system in wireless sensor network," *Int. J. Eng. Adv. Technol*, vol. 8, no. 5, pp. 1765–1768, 2019.

[145] K.-H. Lam, C.-C. Cheung, and W.-C. Lee, "Rssi-based lora localization systems for large-scale indoor and outdoor environments," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 11 778–11 791, 2019.

[146] M. I. M. Ismail, R. A. Dzyauddin, S. Samsul, N. A. Azmi, Y. Yamada, M. F. M. Yakub, and N. A. B. A. Salleh, "An rssi-based wireless sensor node localisation using trilateration and multilateration methods for outdoor environment," *arXiv preprint arXiv:1912.07801*, 2019.

[147] J. Du, J.-F. Diouris, and Y. Wang, "A rssi-based parameter tracking strategy for constrained position localization," *EURASIP Journal on Advances in Signal Processing*, vol. 2017, no. 1, pp. 1–10, 2017.

[148] H. Kwasme and S. Ekin, "Rssi-based localization using lorawan technology," *IEEE Access*, vol. 7, pp. 99 856–99 866, 2019.

Appendix A

List of Publications

A.1 Journal Articles

1. Marchese, M., **Moheddine, A.**, Patrone, F. (2019). "IoT and UAV integration in 5G hybrid terrestrial-satellite networks", in *Sensors, 19(17), 3704.*

2. Gaggero, G. B, Marchese, M., **Moheddine, A.**, and Patrone, F. "A Possible Smart Metering System Evolution for Rural and Remote Areas Employing Unmanned Aerial Vehicles and Internet of Things in Smart Grids," in *Sensors, 21(5), 1627.*

A.2 International Conferences

1. **Moheddine, A.**, Patrone, F., Marchese, M. (2019, November). UAV and IoT integration: a flying gateway. In 2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS) (pp. 121-122). IEEE, 2019.

2. Marchese, M., **Moheddine, A.**, Patrone, F. (2019, November). Towards Increasing the LoRa Network Coverage: A Flying Gateway. In 2019 International Symposium on Advanced Electrical and Communication Technologies (ISAECT) (pp. 1-4). IEEE, 2019.

3. Marchese, M.,**Moheddine, A.**, Patrone, F. (2020, March). UAV and satellite employment for the Internet of Things use case. In 2020 IEEE Aerospace Conference (pp. 1-8). IEEE, 2020.

4. Marchese, M., **Moheddine, A.**, Patrone, F., De Cola, T., Mongelli, M. (2020, June). QoS-aware handover strategies for Q/V feeder links in VHTS systems. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-7). IEEE, 2020.

5. *Conference*: **Aya Moheddine**, Fabio Patrone, and Mario Marchese, "Comparison between UAV IoT solutions with and without satellite backhaul link", in *IEEE Aerospace Conference - March 2022*

Appendix B

Localization Code

```
pip install earthpy
from math import sin, cos, sqrt, atan2, radians, log, degrees, asin
import numpy as np
import os
import folium
import matplotlib.pyplot as plt
from folium import plugins
import rasterio as rio
from rasterio.warp import calculate_default_transform, reproject,
    Resampling
import earthpy as et
```

Listing B.1: List of libraries needed.

```
class GeoPoint:
  def __init__(self, x, y):
    self.x = x
    self.y = y
```

Listing B.2: Point coordinates.

```
class ReceiverConf:
```

```
  def __init__(self, A, n, d, rssi):
    self.A = A
    self.n = n
    self.d = d
    self.rssi = rssi
```

Listing B.3: Receiver coordinates.

```
receiver1 = GeoPoint(44.381983,9.042704)
receiver2 = GeoPoint(44.381878,9.042560)
receiver3 = GeoPoint(44.382406,9.04205)
sensor = GeoPoint(44.381903,9.042372)
receivers = [receiver1, receiver2, receiver3]
```

Listing B.4: Example of the receiver points which corresponds to three different positions of the gateway and the fixed sensor.

```
#the values of A and n obtained from the experiment
A = -35.8
n = 3.74
```

Listing B.5: A and n values obtained from outdoor environment.

```
#function to calculate the rssi using the shadowing algorithm
def calc_rss(n,d,a):
  cal_rss= (-10*n*(log(d,10)))+a
  print(cal_rss)
  return cal_rss
```

Listing B.6: Distance to RSSI function.

```
#function to calculate the distance knowing the rssi, A and n values:
def calc_dist(rss,a,n):
 cal_d= pow(10,((a-rss)/(10*n)))
 print(cal_d)
```

```
5  return cal_d
```

Listing B.7: RSSI to distance function.

```
1  #the distances obtained from calc-dist() are given (DistA, DistB, DistC
       ) to localisation algorithm
2      def trilat():
3
4  #assuming elevation = 0
5    earthR = 6371
6    DistA =dA /1000
7    DistB =dB /1000
8    DistC = dC /1000
9    LatA = receiver1.x
10   LonA = receiver1.y
11   LatB = receiver2.x
12   LonB = receiver2.y
13   LatC = receiver3.x
14   LonC = receiver3.y
15
16
17   xA = earthR * (cos(radians(LatA)) * cos(radians(LonA)))
18   yA = earthR * (cos(radians(LatA)) * sin(radians(LonA)))
19   zA = earthR * (sin(radians(LatA)))
20
21   xB = earthR * (cos(radians(LatB)) * cos(radians(LonB)))
22   yB = earthR * (cos(radians(LatB)) * sin(radians(LonB)))
23   zB = earthR * (sin(radians(LatB)))
24
25   xC = earthR * (cos(radians(LatC)) * cos(radians(LonC)))
26   yC = earthR * (cos(radians(LatC)) *sin(radians(LonC)))
27   zC = earthR * (sin(radians(LatC)))
28
29   P1 = np.array([xA, yA, zA])
```

```
30  P2 = np.array([xB, yB, zB])
31  P3 = np.array([xC, yC, zC])
32
33  ex = (P2 - P1)/(np.linalg.norm(P2 - P1))
34  i = np.dot(ex, P3 - P1)
35  ey = (P3 - P1 - i*ex)/(np.linalg.norm(P3 - P1 - i*ex))
36  ez = np.cross(ex, ey)
37  d = np.linalg.norm(P2 - P1)
38  j = np.dot(ey, P3 - P1)
39
40  x = (pow(DistA, 2) - pow(DistB, 2) + pow(d, 2))/(2*d)
41  y = ((pow(DistA, 2) - pow(DistC, 2)
42        + pow(i, 2) + pow(j, 2))/(2*j)) - ((i/j)*x)
43
44  try:
45      print(DistA, x, y)
46      z = sqrt(pow(DistA, 2) - pow(x, 2) - pow(y, 2))
47      print(z)
48  except:
49      z = float('nan')
50  try:
51      print(DistB, x, y)
52      z = sqrt(pow(DistB, 2) - pow(x, 2) - pow(y, 2))
53      print(z)
54  except:
55      z = float('nan')
56  try:
57      print(DistC, x, y)
58      z = sqrt(pow(DistC, 2) - pow(x, 2) - pow(y, 2))
59      print(z)
60  except:
61      z = float('nan')
62  triPt = P1 + x*ex + y*ey + z*ez
```

```
63
64    lat = degrees(asin(triPt[2] / earthR))
65    lon = degrees(atan2(triPt[1], triPt[0]))
66    print('Device or sensor coordinates:', lat, lon)
67
68    return lat, lon
```

Listing B.8: Trilateration algorithm.

```
1 #map the gps coordinates estimated and initial ones
2
3 m = folium.Map(location=[44.3833318, 9.0333332])
4 folium.Marker([44.381903,9.042372],
5 ipopup='Sensor position', icon=folium.Icon(color="red")).add_to(m)
6 folium.Marker([a,b],
7 popup="estimated position",  icon=folium.Icon(color="green")).add_to(m)
```

Listing B.9: Mapping the estimated position and initial position of the sensor.

```
1 #to visualize the map
2 m
```

Listing B.10: Visualizing the map.

Appendix C

List of Acronyms

- 3GPP: Third Generation Partnership Project
- ABP: Activation By Personalization
- API: Application Programming Interface
- AUV: Autonomous Underwater Vehicle
- CSS: Chirp Spread Spectrum
- CR: Coding Rate
- DSO: Distribution System Operator
- GPS: Global Positioning System
- ICT: Information and Communication Technology
- ISM: Industrial, Scientific and Medical band
- IoT: Internet of Things
- IoFT: Internet of Flying Things
- IT: Information Technology

- LEO: Low Earth Orbit
- LoRa: Long Range
- LoRaWAN:Long Range Wide Area Network
- LPWA: Low Power Wide Area
- LPWAN: Low Power Wide Area Network
- LoS: Line of Sight
- MMR: Manual Metering Reading
- MEC: Mobile Edge Computing
- MEO: Medium Earth Orbit
- NB-IoT: Narrow-Band Internet of Things
- OTAA: Over The Air Activation
- QoS: Quality of Service
- SCADA: Supervisory Control And Data Acquisition
- SG: Smart Grid
- SM: Smart Metering
- SMe: Smart Meter
- SF: Spreading Factor
- UAV: Unmanned Aerial Vehicles
- UAS: Unmanned Aerial System
- WSN: Wireless Sensor Network