Development and analysis of wireless sensors and associated Internet of Things systems

A dissertation submitted in fulfillment of the requirements for the degree of:
Doctor of Philosophy in Electronic Engineering
at the University of Valencia
Doctor of Philosophy in Electronic and Telecommunication
at Abdelmalek Essaadi University

Author:
Mohamed Saban

Supervisors:

Prof. Dr. Alfredo Rosado Muñoz

GPDD Lab, University of Valencia, Valencia, Spain.

Prof. Dr. Otman Aghzout

SIGL Lab, Abdelmalek Essaadi University, Tetouan, Morocco.

July 08, 2023

Declaration of Authorship

The doctoral candidate Mr. Mohamed Saban, and the thesis supervisors **Prof. Dr. Alfredo Rosado Muñoz** and **Prof. Dr. Otman Aghzout**, guarantee, by signing this doctoral thesis that:

The research work contained in the present report, entitled "Development and analysis of wireless sensors and associated Internet of Things systems", has been done by the doctoral candidate under the direction of the thesis supervisors at the university of Valencia and the university of Abdelmalek Essaadi, and, as far as our knowledge reaches, in the performance of the work, the rights of other authors to be cited when their results or publications have been used.

Valencia, March 23, 2023

Mr. Mohamed Saban
Ph.D candidate

MS

Prof. Alfredo Rosado-Muñoz
University of Valencia
Valencia, Spain

Prof. Otman Aghzout
University of Abdelmalek Essaadi
Tetouan, Morocco

Université Abdelmalek Essaadi
Tetouan

Pr. Otman AGHZOUT
Telecommunication
Engineering National
School of Applied Sciences

Abstract

The advent of the Internet of Things (IoT) technology has become increasingly important in recent years. By offering a means of linking devices and establishing real-time connections, IoT has facilitated the monitoring and management of tangible entities, such as appliances, vehicles, and buildings. Typically, an IoT system consists of numerous devices that communicate with one another via gateways, and cloud servers that host web and mobile applications. The end-users can seamlessly interact with their IoT devices, thereby granting greater accessibility and convenience. Given its capacity for providing real-time control and automation, IoT presents numerous opportunities for cost savings and increased efficiency across various sectors, including healthcare, manufacturing, and transportation. As such, IoT has the potential to improve our lives and create new prospects for businesses, making it an essential technology for the future. However, as IoT applications continue to become increasingly complex and diverse, there is an growing demand for sensors capable of accurately and reliably collecting highly specific data and transmitting it to other devices within the network. Additionally, the IoT landscape is constantly evolving, with new technologies emerging at a rapid pace. Therefore, to effectively address the need for highly specialized and customized IoT solutions, it is necessary to study and analyze the communication technologies employed, and remain up-to-date with the latest developments in order to ensure effective design, implementation, and management of these applications. Furthermore, developing new sensors from scratch can offer a solution to this problem by optimizing the design for specific use cases, thereby achieving optimal performance and functionality in IoT systems. By developing a sensor from scratch, greater control can be exercised over the hardware and software, thereby allowing for greater flexibility.

This thesis presents a systematic analysis of IoT systems in terms of communication, power consumption, and security. The study analyzed the communication technologies used in IoT systems, including short-range systems based on protocols such as Wi-Fi and Bluetooth, as well as long-range systems based on technologies like LoRa. The thesis includes the development of new sensors from scratch for specific applications, enabling greater control over the hardware and software. Additionally, the thesis addresses the security risks associated with cloud-centric IoT systems by incorporating blockchain technology, which provides a decentralized database infrastructure, thereby adding an extra layer of security. These studies help to better understand IoT systems and optimize their deployment, resulting in improved performance and functionality, and offers valuable insights into the design, implementation, and management of IoT systems for researchers, industry practitioners, and stakeholders.

Resumen

En los últimos años, la tecnología del Internet de las cosas (IoT) se ha vuelto cada vez más importante. Al ofrecer un medio para conectar dispositivos y establecer conexiones en tiempo real, el IoT ha facilitado el monitoreo y la gestión de entidades tangibles, como electrodomésticos, vehículos y edificios. Típicamente, un sistema IoT incorpora numerosos dispositivos que se comunican entre sí a través de gateways y servidores en la nube que alojan aplicaciones web y móviles. Los usuarios finales pueden interactuar sin problemas con sus dispositivos IoT, lo que les otorga una mayor accesibilidad y conveniencia. Dado su capacidad para proporcionar control y automatización en tiempo real, el IoT presenta numerosas oportunidades para ahorrar costos e incrementar la eficiencia en varios sectores, incluyendo salud, manufactura y transporte. Como tal, el IoT tiene el potencial de mejorar nuestras vidas y crear nuevas oportunidades para los negocios, convirtiéndolo en una tecnología esencial para el futuro. Sin embargo, a medida que las aplicaciones IoT continúan volviéndose cada vez más complejas y diversas, hay una creciente demanda de sensores capaces de recopilar datos altamente específicos de manera precisa y confiable, y transmitirlos a otros dispositivos dentro de la red. Además, IoT está en constante evolución, con nuevas tecnologías emergiendo a un ritmo acelerado. Por lo tanto, es necesario estudiar y analizar las tecnologías de comunicación empleadas, y mantenerse al día con los últimos desarrollos para abordar de manera efectiva la necesidad de soluciones IoT altamente especializadas y personalizadas y para garantizar un diseño, implementación y gestión efectivos de estas aplicaciones. Además, el desarrollo de nuevos sensores puede ofrecer una solución a este problema al optimizar el diseño para casos de uso específicos, logrando así un rendimiento y funcionalidad óptimos en los sistemas IoT. Al desarrollar un sensor novedoso, se puede ejercer un mayor control sobre el hardware y software, lo que permite una mayor flexibilidad y personalización.

En esta tesis se presenta un análisis detallado de los sistemas IoT en cuanto a su comunicación, consumo de energía y seguridad. El estudio analizó las tecnologías de comunicación utilizadas en los sistemas IoT, incluidos los sistemas de corto alcance basados en protocolos como Wi-Fi y Bluetooth, así como los sistemas de largo alcance basados en tecnologías como LoRa. Además, se desarrollaron nuevos sensores específicos para aplicaciones particulares. Asimismo, se abordaron los riesgos de seguridad asociados con los sistemas IoT centrados en la nube mediante la incorporación de la tecnología blockchain, que proporciona una infraestructura descentralizada de base de datos y añade una capa extra de seguridad. Los resultados de estos estudios pueden ayudar a mejorar la comprensión y la optimización de los sistemas IoT, mejorando su rendimiento y funcionalidad, y proporcionando información valiosa sobre el diseño, implementación y gestión de sistemas IoT para investigadores, profesionales de la industria y otros interesados en esta tecnología.

ملخص

تزايدت أهمية تقنية إنترنت الأشياء (IoT) في السنوات الأخيرة بشكل ملحوظ، هذه التقنية تمكن من ربط الأجهزة والأشياء عبر الإنترنت بغرض إنشاء اتصالات فورية لمراقبتها والتحكم بها عن بعد، مما يسهل استخدام هذه الأشياء التي نستعملها في حياتنا اليومية سواء في المنازل أو المنشئات أو المركبات. يتكون نظام إنترنت الأشياء من شبكة أجهزة متنوعة مرتبطة ببعضها البعض عبر الإنترنت من خلال البوابات والخوادم السحابية، حيث يمكن للمستخدمين التحكم في أجهزتهم بسهولة من خلال متصفحات الويب أو تطبيقات الهاتف المحمول التي تستضيفها هذه الخوادم. تتيح تقنية إنترنت الأشياء ربطا فعالا ومباشرة بالأجهزة يمكّن من التحكم بها ومراقبتها في الوقت الفعلي، الشيء الذي يوفر الوقت والتكاليف ويزيد الكفاءة. إضافة إلى أنها تتيح العديد من الفرص في مختلف القطاعات كالرعاية الصحية والتصنيع والنقل. على هذا النحو، فإن إنترنت الأشياء لديها القدرة على تحسين حياتنا وخلق آفاق جديدة سواء للأفراد أو الشركات، مما يجعلها تقنية أساسية للمستقبل.

إن استمرار تعقيد وتنوع تطبيقات إنترنت الأشياء، والتطوير المستمر الذي يحدد بُنيتها وظهور تقنيات جديدة بوتيرة سريعة، ويزيد الطلب على أجهزة إنترنت الأشياء ومستشعرات قادرة على جمع بيانات محددة للغاية بدقة وموثوقية لنقلها إلى الأجهزة الأخرى داخل الشبكة، مما يتطلب حلولا متجددة ومتخصصة. تشكل دراسة وتحليل تقنيات الاتصال المختلفة المستخدمة ومواكبة أحدث التطورات حلاً فعلياً من شأنه ضمان التصميم الفعال لأنظمة إنترنت الأشياء والتغلب على هذه المشكلة. كما أن تطوير مستشعرات جديدة ومتخصصة لأنظمة معينة يعتبر حلا مثاليا لتخصيص التصميم وإنشاء أنظمة إنترنت الأشياء ذات الأداء الأمثل والفعال. علاوة على ذلك، يتيح تطوير أجهزة استشعار جديدة مزيداً من التحكم على مستوى الأجهزة والبرامج، الشيء الذي يعطي هذه الأنظمة مزيداً من المرونة.

تقدم رسالة الدكتوراه هذه تحليلًا منهجيًا لأنظمة إنترنت الأشياء من حيث الاتصال واستهلاك الطاقة والحماية. هذه الأطروحة تسعى لدراسة مختلف التقنيات المستخدمة لربط الأجهزة في أنظمة أنترنت الأشياء، بما في ذلك الأنظمة قصيرة المدى مثل الواي-فاي (Wi-Fi) والبلوتوث (Bluetooth)، أو الأنظمة الطويلة المدى مثلا لورا(LoRa). تقدم هذه الأطروحة وصفا مفصلا لتطوير مستشعرات جديدة كليا مخصصة للاستخدام في أنظمة أنترنت الأشياء، كما تتناول حلولا لصد المخاطر الأمنية المرتبطة بهذه الأنظمة، من خلال دمج تقنية البلوكشن (Blockchain)، والتي تسمح بتوفير بنية تحتية لقاعدة بيانات لامركزية، وبالتالي إضافة طبقة إضافية من الحماية. الدراسات المقدمة في هذه الأطروحة تساعد على فهم أفضل لأنظمة إنترنت الأشياء بهدف الدفع بعجلة التقدم لبناء المنازل والمدن الذكية وتحسين الأداء والوظائف، كما توفر رؤى قيمة فيما يتعلق بتصميم وإنشاء وإدارة أنظمة إنترنت الأشياء للباحثين والمتخصصين وكل المهتمين بالمجال.

Résumé

L'avènement de la technologie de l'Internet des objets (IoT) est devenu de plus en plus important ces dernières années. En reliant les dispositifs et en établissant des connexions en temps réel, l'IoT a facilité la surveillance et la gestion des appareils, des véhicules et des bâtiments. Un système IoT intègre généralement de nombreux dispositifs qui communiquent entre eux via des passerelles, et des serveurs cloud qui hébergent des applications web ou mobiles. Les utilisateurs finaux peuvent interagir de manière transparente avec leurs appareils IoT grâce à ces applications, offrant une grande accessibilité et commodité. L'IoT offre des possibilités de réduction des coûts et d'amélioration de l'efficacité dans divers secteurs, notamment les soins de santé, la fabrication et les transports. Cependant, les applications IoT sont de plus en plus complexes et diversifiées, ce qui demande des capteurs capables de collecter des données précises et fiables et de les transmettre à d'autres appareils. De plus, l'IoT évolue rapidement grâce aux nouvelles technologies émergentes, et pour répondre à la demande de solutions IoT spécialisées et personnalisées, il est nécessaire d'étudier et d'analyser les technologies de communication employées et de rester au fait des dernières évolutions. Le développement de nouveaux capteurs peut offrir une solution en optimisant la conception pour des cas d'utilisation spécifiques, ce qui permet d'obtenir des performances et des fonctionnalités optimales dans les systèmes IoT. En développant un capteur à partir de zéro, un plus grand contrôle peut être exercé sur le matériel et le logiciel, permettant une plus grande personnalisation et flexibilité.

Cette thèse présente une analyse approfondie et systématique des systèmes IoT, en se concentrant sur les aspects clés de communication, de consommation d'énergie et de sécurité. L'étude a analysé les technologies de communication utilisées dans les systèmes IoT, notamment les systèmes à courte portée basés sur des protocoles tels que Wi-Fi et Bluetooth, ainsi que les systèmes à longue portée basés sur des technologies comme LoRa. En outre, cette thèse comprend le développement de nouveaux capteurs pour des applications spécifiques, permettant ainsi un plus grand contrôle sur le matériel et le logiciel. Un autre aspect important abordé dans cette thèse est la sécurité des systèmes IoT centrés sur le cloud. Pour réduire les risques associés, la technologie blockchain a été intégrée, fournissant une infrastructure de base de données décentralisée qui ajoute une couche supplémentaire de sécurité. Cette approche innovante peut aider à améliorer la sécurité des systèmes IoT, tout en offrant des perspectives précieuses sur la conception, la mise en œuvre et la gestion de ces systèmes pour les chercheurs, les praticiens de l'industrie et les parties prenantes. Dans l'ensemble, cette thèse permet une meilleure compréhension des systèmes IoT, ce qui peut conduire à des améliorations significatives en termes de performances et de fonctionnalités.

Acknowledgement

I would like to begin by expressing my sincere appreciation to my parents and siblings for their constant support throughout this research journey. Your love and encouragement have been invaluable to me, and I am deeply grateful for everything you have done.

I would also like to express my heartfelt gratitude to my thesis directors, **Prof. Otman Aghzout** and **Prof. Alfredo Rosado-Muñoz**, for giving me the opportunity to work on this interesting topic and for their invaluable guidance and support throughout this process. Their expert guidance and patience have been invaluable to me, and I am deeply grateful for their commitment to my work.

I would also like to extend my thanks and appreciation to Prof. Silvia Casans-Berga, Prof. Rafael García-Gil and Prof. A. Edith Navarro-Antón for their collaboration and support during the course of this thesis.

Finally, I would like to thank the members of my research groups, the GPDD-Lab (Processing and Digital Design Group Laboratory) and the SIGL-Lab (Computer Science Systems and Software Engineering Laboratory), for their valuable contributions to this thesis. I am grateful for the stimulating exchanges and fruitful discussions I have had with each of you. Your hard work and dedication have been instrumental in the success of this thesis.

Thank you all.
Mohamed

Contents

List of Figures

List of Tables

Acronyms

ABP Activation by Personalization.

AC Alternating Current.

ADC Analog-to-Digital Converter.

ADR Adaptive Data Rate.

API Application Programming Interface.

ATT ATT Attribute protocol.

BLE Bluetooth Low Energy.

BPSK Binary Phase Shift Keying.

BSS Basic Service Set.

BTC Bitcoin.

CSRF Cross-site Scripting.

CSS Cascading Style Sheets.

CSS Chirp Spread Spectrum.

DC Direct Current.

DDoS Denial-of-service attack.

DES Data Encryption Standard.

DNS DomainName System.

ECC Elliptic Curve Cryptography.

ECU Electrical Control Unit.

eDRX extended Discontinuous Reception.

eMTC nhanced Machine-Type Communication.

ER Entity-Relationship.

ESS Extended Service Set.

EVM Ethereum Virtual Machine.

FAN Field Area Networks.

GAP Generic Access Profile.

GATT Generic Attribute Profile.

GPIO General Purpose Input/Outputs.

GSM Global System for Mobile Communications.

HCI Host Controller Interface.

HID Human Interface Device.

HRM Human Resource Management.

HSM Hardware Secure Modules.

HTML HyperText Markup Language.

IAM Identity and Access Management.

IBSS Independent Basic Service Set.

IDC International Data Corporation.

IEEE Institute of Electrical and Electronics Engineers.

IIoT Industrial Internet of Things.

IoT Internet of Things.

IP Internet Protocol.

ISM Industrial, Scientific, and Medical.

JSON JavaScript Object Notation.

L2CAP Logical Link Control and Adaptation Protocol.

LAMP Linux, Apache, MySQL, PHP.

LEACH Low energy adaptive clustering hierarchy.

LNS LoRaWan Network Server.

LPWAN Low Power Wide Area Network.

LTE Long-Term Evolution.

M2M Machine-to-Machine.

MC Moisture Content.

MEMS Micro-Electro-Mechanical Systems.

MNO Mobile Network Operators.

MVC Model-View-Controller.

NB-IoT Narrowband-IoT.

NFC Near-Field Communication.

NIST National Institute of Standards and Technology.

NPRACH Narrowband Random Access Channel.

NPUSCH Narrowband Uplink Shared Channel.

OBD On-board Diagnostics.

OEM Original Equipment Manufacturers.

OFDM Orthogonal Frequency Division Multiplexing.

ORM Object Relational Mapping.

OTAA Over-the-Air Activation.

PHP Hypertext Preprocessor.

PLC Programmable Logic Controller.

PoS Proof of Stake.

PoW Proof of Work.

PRB Physical Resource Block.

PSM Power Saving Mode.

RF Radio Frequency.

RFID Radio Frequency Identification.

RSSI Received Signal Strength Indicator.

SC-FDMA Single Carrier Frequency Division Multiple Access.

SF Spreading Factor.

SM Security Manager.

SMD surface mount device.

SMTP Simple Mail Transfer Protocol.

SoC System-on-Chip.

SQL Structured Query Language.

SWD Serial Wire Debugging.

SWIM Single-Wire Interface Module.

TDMA Time Division Multiple Access.

TLS Transport Layer Security.

TPS transactions per second.

TTN The Things Network.

UART Universal Asynchronous Receiver / Transmitter.

UI User Interface.

UNB Ultra-Narrow-Band.

URL Uniform Resource Locator.

UWB Ultra-Wide Bandwidth.

V2I vehicle-to-infrastructure.

V2P vehicle-to-pedestrian.

V2V vehicle-to-vehicle.

V2X vehicle-to-everything.

VoLTE Voice over LTE.

VPS Virtual Private Server.

WLAN Wireless Local Area Network.

WPA WiFi Protected Access.

WPAN Wireless Personal Area Network.

WSN Wireless sensor network.

XSS Cross-site Request Forgery.

Chapter 1

Introduction

"Trees that are slow to grow bear the best fruit."

- Molière

In recent years, there has been rapid progress in various technological areas, including embedded computing, miniaturization of hardware, sensing and wireless networking. This has enabled the internet to expand beyond the virtual world and connect physical objects, such as doors, cars, and trees, giving them unique identifiers and the ability to sense, process information, and respond to their environment, creating a smart world. Connecting these smart things to the internet to interact with them wirelessly introduce us to the concept of the Internet of Things (IoT). This PhD thesis is devoted to routing and sensor search in the IoT, analysing the communication technologies and the security of the IoT systems. In this introductory chapter, the motivation of this PhD thesis is described in Section 1.1. The objectives of this thesis are described in Section 1.2. The summary of the contributions is presented in Section 1.3, and finally Section 1.4 describes the overall structure of this PhD thesis.

1.1 Motivation

Applications based on IoT offer many solutions to facilitate our daily life. IoT is currently evolved in many domestic and industrial systems [1]. The International Data Corporation (IDC) expects that the number of IoT connected devices will reach 41.6 billions by 2025 [2]. These devices are connected to cloud servers that process the collected data, enabling users to remotely control and monitor them through web and mobile applications. Their small size allows them to be easily attached to objects such as people, desks, or plants, embedded in places like homes or offices, or scattered in large numbers in the environment, such as forests or farm fields. These wireless networks of embedded computing devices, can be utilized as tools for tracking, monitoring, and influencing the real world.

Developments in the wireless networking field have led to the creation of important wireless communication and identification technologies such as IEEE 802.15.4, Bluetooth, Bluetooth Low Energy (BLE), Ultra-Wide Bandwidth (UWB), IPv6, Radio Frequency Identification (RFID), Near-Field Communication (NFC) and Low Power Wide Area Network (LPWAN). Embedded computing devices, therefore, can be uniquely addressed as well as communicate among each other. Analysing these technologies is a must when it comes to deploy an IoT system in order to choose the suitable technology for the application. Table 1.1 demonstrates a brief summary associated to some common communication technologies in use [3].

Technology	Range	Frequency	Throughput	Power Consumption
RFID	up to 100 m	LF/HF/Microwave	Varies with frequency	Varies with frequency
Bluetooth	100 m	2.4 GHz	2.1 mbps	1 W Varies with class
BLE	>100 m	2.4 GHz	0.27 mbps	0.5 W
NFC	10 cm	13.56 MHz	up to 424 kbps	<15 mA
802.15.4	< 10 0m	2.4 GHz	0.25 mbps	Varies with transceiver
WI-FI (802.11.n)	75 m	2.4 and 5 GHz	600 mbps	0.82 W
UWB	20 m	10.6 GHz	up to 400 mbps	100 mW
Zigbee	100 m	2.4 GHz	20, 40, 100 and 250 kbp	>100 mW
LoRa	5 km (urban), 20 km (rural)	868 MHz (Europe)	250 kHz and 125 kHz	>4.2 mA
SigFox	10 km (urban), 40 km (rural)	862 to 928 MHz	100 Hz	0.5 mA to 49 mA

Table 1.1: A brief summary of some IoT connectivity technologies

The selection of the appropriate IoT communication protocol is crucial and depends on the specific type of IoT application. Each protocol has its own advantages, disadvantages, and deployment conditions. When choosing the best option for an IoT project, the following criteria should be considered carefully to ensure that the chosen protocol aligns with the specific needs and constraints of the project:

- **Device capabilities.** IoT devices support a specific communication protocol. The selection of a device is related to the protocol to be used.

- **Power consumption.** This problem come to light when the IoT network is deployed in an outdoor environment, when the devices run on batteries and not on a direct power line such as smart home devices.

- **Synchronous response requirements.** If the IoT system require an immediate response to actions, a synchronous communication pattern should be selected.

- **Connectivity.** Factors like data transmission rate, communication range, and latency should be considered depending on the connection type.

- **Security.** The security of the communication protocols should be also considered depending on the aim of the system and the exchanged information.

- **Allocated budget.** The installation costs are depend on multiple factors such as the frequency band, the cost of the end-devices and the cost of the base stations.

Another important element in IoT systems is the web applications. These applications are widely used to simplify the management of IoT devices and to enhance the value that organizations can extract from their IoT deployments. Developing a robust web application for IoT is a complex task that requires careful consideration of various factors, including the choice of technology. The technology chosen must have the capacity to handle large data volumes efficiently and without sacrificing performance. Also, it should have robust security features, such as authentication, encryption, and access controls, to prevent unauthorized access to the application and data. As the number of IoT devices connected to the application increases, the technology must be capable of scaling up to handle the increased load without impacting performance.

The Web has undergone significant transformations over time, from the creation of static web pages in Web 1.0 to the user collaboration focus of Web 2.0 through platforms like Facebook and YouTube. The current Web is now transitioning to the next generation, known as Web 3.0 or the Semantic Web, which one of its fundamental aspects are ownership and decentralization. The use of decentralized databases powered by Blockchain technology, which is renowned for its solutions in financial fields, could address some of the most critical challenges facing the IoT. With blockchain, any data can be recorded immutably and distributed, unlike the current IoT infrastructure that relies on intermediaries and centralized entities to validate the data. In Web 3.0 IoT, blockchain would transform the structure of IoT from client-server to peer-to-peer. Consensus mechanisms can be used to verify transformations and address trustworthiness, making IoT a trustless system that allows direct communication between devices without intermediation [4]. However, with the increased number of the upcoming of IoT applications, further aspects have emerged that additionally need to be taken into account when deploying IoT environments. These aspects include, for example, the heterogeneity of processing nodes due to the existent different types of IoT objects. Also, different types of networks and technologies can be encompassed within IoT environments, whose heterogeneity also needs to be considered.

In this PhD thesis, the IoT communications protocols are studied and analysed under different circumstances in order to compare the theoretical are and the experimental results. This analysis helps to verify performance and the limits of each technology that will lead to a good distribution of the network end-nodes. Moreover, Specific sensors have been developed and tested. The development of new IoT sensors is also forming part of the study and it has different interests that should be considered. For example, costs, quality, and lead time. The balance between sustainability and economic gain is always present in an innovation process. An approach of securing the IoT using the Blockchain technology that provides a decentralized storing of data is also presented in this thesis. Through this approach, data processing of IoT applications will be safe and fast. All concepts of this PhD thesis are based on established standards or de-facto standards in order to ensure their long lasting applicability and future-proofness. The results of this thesis allow us to offer a detailed analysis of IoT solutions that can facilitate the implementation of these types of communication infrastructures.

1.2 Objectives

The aim of this thesis is to address different topics concerning the development, the design and implementation of sensor nodes for multiple IoT networks. Four objectives have been formulated:

- **Objective 1:** Experimental analysis of IoT communication protocols. This objective includes the development, design and implementation of new low-cost IoT sensors that can be used in several IoT applications.
- **Objective 2:** Optimization of the low level embedded program of the developed IoT node for better communication and low power consumption, especially in the stand-by mode. This objective involves the analysis, characterization, and evaluation of the sensors nodes in different environments. Multiple tests have been performed for this aim.
- **Objective 3:** Development of new IoT web applications that can display real-time data using a dynamic User Interface (UI) which is designed with user-friendliness in mind to provide an intuitive experience. This objective aims to provide valuable insights to users by enabling the display of constantly changing data.
- **Objective 4:** Enhancing the security of the IoT network, by leveraging decentralized databases using Blockchain technology which will strengthen the security of communication of the data thanks to the robust cryptographic protocols. Moreover, this technology will provide enhanced anonymity in IoT use cases where privacy is a primary concern.

1.3 Contribution

The following points are intended to contribute to the IoT ecosystem through this thesis:

- New IoT sensors are proposed. Three different low-cost, digitally controlled, and energy-efficient IoT sensors have been developed and tested as proposed by this thesis:
    1. The first sensor is a wood moisture sensor, that utilizes wireless BLE connectivity. This device employs a resistance measurement method that is valid for an ultra-wide range of resistance values. The sensor can be used in wooden buildings to monitor moisture content and prevent biological attacks.
    2. A second wood moisture sensor was developed using an advanced resistance method and long-range LoRa wireless connectivity. This device is designed for use in large wooden buildings and cultural heritage sites.
    3. The third sensor is a smart plug that utilizes LoRa technology. This device aims to monitor the usage of electric appliances in homes.
- New web applications based on the PHP Laravel framework for the management of the IoT systems. A web application is a crucial element when deploying an IoT system. Many open-source web applications can be found in the internet which can be used for some basic IoT projects like controlling the home devices, but they are not suitable for some specific tasks or complicated projects. Thus, four web applications based on Laravel have been developed as part of this PhD thesis, to address the requirement of the presented IoT systems.
- A new system based on BLE technology for monitoring the moisture content of wood in wooden houses. The system includes the development of a BLE moisture device and a new web application.
- A novel system based on LoRa technology for monitoring the moisture content of wood in heritage and historical wooden building. The system includes the development of a LoRa moisture device and a new web application.
- A novel system for wellness determination of elderly who are living alone in villages based on LoRa technology. Including the development of LoRa-based monitoring device to monitor the use of electric domestic appliances.
- A smart farming system based on LoRa technology by adding the LoRa wireless connectivity to a regular Programmable Logic Controller (PLC) that

are already used in the farms, along with the development of a new web application for monitoring and management.

- A security model for LoRaWan networks based on the Blockchain technology in order to have a distributed storage of the collected data. The Swarm Ethereum blockchain network was used for this purpose.

1.4 Structure

This dissertation is organized as follows:

- **Chapter 1** presents a general introduction about the concept of the IoT, and describes the motivation and the objectives of this doctoral thesis.
- **Chapter 2** presents the state of the arts in wireless communications of IoT systems. This chapter analyzes the short range and the long range communication systems, discusses the blockchain technology and its use as a security layer to protect the collected data of the IoT systems. The development of web applications used in this thesis is also described in this chapter.
- **Chapter 3** describes the development of a short-range BLE moisture sensor, and presents the results of the different functionality tests performed.
- **Chapter 4** presents the development of a new moisture sensor based on Long-range LoRa wireless communication protocols. The experimental results of the performance test are also presented in this chapter.
- **Chapter 5** describes the deployment of multiple IoT-based applications including a wood moisture monitoring system for wooden buildings, a Smart farming system and a home monitoring application for wellness determination of elderly who are living alone in villages. The last application integrates Blockchain technology with LoRaWan in order to enhance the security of data storage.
- **Chapter 6** concludes this dissertation and presents the future work.

Chapter 2

State of the Art in IoT Technologies

"It's your road and yours alone, others may walk it with you, but no one can walk it for you."

- Rumi

This chapter provides an overview of the fundamental concepts of the IoT. A comparative study of various short-range and long-range technologies used in IoT applications is presented. Additionally, the development of web applications for IoT systems is explored. Lastly, the integration of Blockchain technology with IoT systems is discussed in the last section.

2.1 The Internet of Things (IoT): an Overview

The idea of a network of interconnected smart devices, known as the Internet of Things (IoT), was first proposed at Carnegie Mellon University in 1982 with a modified Coca-Cola vending machine that became the first Internet-connected appliance. This machine could report on its stock levels and the temperature of newly added drinks without the need for manual inspection [5]. The vision of the IoT was described by Mark Weiser in 1991 [6], before the term "Internet of Things" was coined by Kevin Ashton in 1999 [7]. However, the full potential of the IoT was not realized until between 2008 and 2009.

2.1.1 Definition of IoT

The Internet of Things is a network of physical objects that are connected to the Internet with the aim of improving efficiency, productivity, services, and more. It has been made possible due to the fast development and coming together of several technologies, real-time analytics, embedded systems, sensors, wireless systems, control systems, automation and machine learning. The connected objects in an

IoT environment share data to a platform that applies analytics and shares the information with applications designed to address specific needs [8]. These IoT platforms are designed to find problems, make recommendation and detect patterns by determining the useful and the useless data, which allows processes to become more efficient and automate many tasks.

The deployment map of an IoT system is depicted in Figure 2.1. The physical items are connected to the internet through wired or wireless connections. The integration of these technologies in various fields presents the concept of a smart city, which aims to optimize city functions, drive economic growth, enhance transportation and accessibility, promote sustainability, and empower citizens through the use of smart technologies and data analysis [9]. In today's world, the IoT plays a crucial role in managing the daily activities of individuals and automating tasks in industries such as healthcare, manufacturing, logistics and other business sectors.

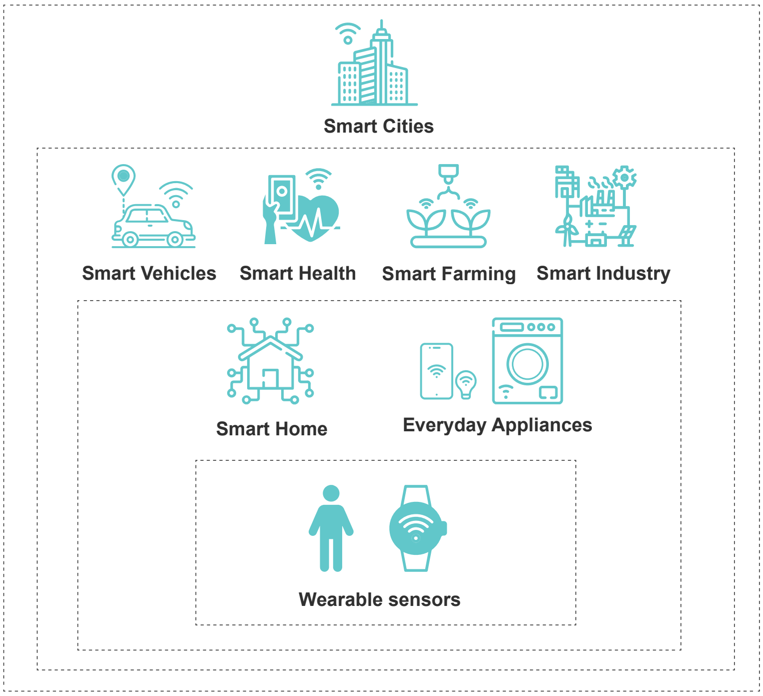


Figure 2.1: Deployment map of Internet of Things. Example of a Smart city

The IoT connects both inanimate and animate objects through the use of RFID and sensor technology, allowing computers to observe, identify, and comprehend the environment. Sensors are specifically designed for various scenarios, such as temperature and humidity monitoring, fire alarms, and buzzers. To enable wireless access, physical objects must be assigned unique identities. IPv4, the most commonly deployed internet protocol, is used to connect devices to the internet, while IPv6, which offers a 128-bit address space, serves as its successor. This digital identity enables tracking of each object and collection of their data.

The IoT has emerged from conventional internet technology with sizeable competencies to establish a strong interconnection among human beings and machines with the aid of making use of numerous sensing and actuating devices. The intelligence in the IoT is made possible through the integration of advanced technologies such as wireless sensor networks, big data analytics, data science or edge and fog computing. Additionally, significant advancements in wireless information and communication technology and the decreasing cost of sensor nodes have greatly expanded the scope of the IoT [10, 11]. Objects in IoT environments interact with each other autonomously and are governed by predefined communication protocols, without human intervention [12]. The efficient coordination of connected sensors and systems results in significant savings of human effort and time. However, as the IoT network grows, its management and control becomes increasingly complex.

2.1.2 Applications of IoT

The IoT technology has a broad range of applications, from domestic uses such as home security and lighting, to industrial uses in manufacturing and defense. These applications can be broadly categorized into four main areas: infrastructure, industrial, commercial, and consumer. The major beneficiaries and design specifications of this rapidly developing technology will be discussed in more detail in the following sections.

2.1.2.1 Military Applications

The IoT has crucial applications in the military field, particularly in the delivery of battlefield data through reconnaissance and surveillance. The use of wireless network technologies such as Zigbee and GSM networks allows for tracking and monitoring of the health of armed personnel. IoT deployment in the battlefield can improve situational awareness, risk assessment, and response times for military authorities. IoT-based systems can aid the military in tracking enemies, monitoring the wellbeing of the armed forces, and coordinating with defense systems [13]. The use of military gear, such as helmets and uniforms with embedded sensor devices, enables the command center to quickly act and save the lives of armed personnel. Some of the sensors that can be used to create intelligent military gear include temperature, pulse rate, oxygen level, accelerometer, ECG, and mobility sensors [14].

2.1.2.2 Consumer Applications

The IoT technology has a diverse range of consumer applications, including connected cars, connected health, and home automation. Personal IoT devices, such as smart watches, and smartphones, are designed for individual use. These devices, which include smart shirts and other wearables, are also commonly used in the smart home application [15, 16]. With their ability to communicate and interact with other connected devices, these personal IoT devices offer a wide range of possibilities for individuals to improve their daily lives and increase convenience.

2.1.2.3 Smart Home Applications

An IoT-enabled home has completely redesigned the way an electronic appliance is controlled in a home environment. By utilizing a combination of relay switches, microcontrollers, and network devices, all appliances, including lights, air conditioners, media players, security systems, refrigerators, and ovens, can be connected to the internet. This enables users to remotely manage their appliances using a central platform or hub that connects to smart devices and appliances. To implement an IoT-based home automation system, a wide range of sensors have been developed, including temperature sensors, light sensors, water level sensors, air composition sensors, and humidity sensors. These smart home devices can be controlled through a smartphone, tablet, or other device, often without the need for a Wi-Fi bridge. They can also be connected to independent platforms such as Amazon Echo [17] or Apple HomePod [18], or an open source ecosystem like Home Assistant or OpenHAB [19].

2.1.2.4 Medical and Healthcare Applications

The healthcare sector is a crucial area where the IoT is being leveraged to improve patient care and reduce costs. IoT technology allows for the collection and analysis of data for research and patient monitoring. It also enables users to communicate with medical professionals more quickly and efficiently over the internet. By connecting resources and services, IoT aims to create a digitized healthcare system that can monitor health and emergency notification systems for patients with chronic conditions such as blood pressure and heart rate monitors, heart diseases, neurological diseases, and diabetes [20, 21]. Internet-connected wearables allow doctors and caregivers to monitor patients remotely, reducing the burden on healthcare facilities and addressing issues such as bed shortages and overworked medical professionals [22]. Smart beds, which can recognize when a patient is attempting to get up and adjust support accordingly, are also being implemented in medical facilities. Sensors and devices such as accelerometers, respiration rate sensors [23], Kinect cameras [24], wireless body sensors [25], t-shirts with embedded sensors, AMPED sensors [26], pedometers, pulsometers [27], defibrillator devices, and textile-based autonomous nervous systems can be used to collect vital signals, which are then processed and transmitted via a communication network [28].

IoT is also being applied to the health insurance sector, where sensor-based tools such as wearables, connected health devices, and mobile apps are being used to track customer behavior and produce more precise underwriting and pricing models. The transformation of hospitals into smart facilities is heavily dependent on IoT, with mobile applications for inquiry, test result reporting, and appointment scheduling being developed based on doctor availability [29].

2.1.2.5 Transport Applications

Transportation applications for the Internet of Things include inter- and intra-vehicle communication, intelligent traffic control, intelligent parking, toll collection, logistics, fleet management, vehicle control, safety, and road assistance. IoT also open ups new directions of vehicular communications: vehicle-to-everything (V2X), vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-pedestrian (V2P) communication, which connects vehicles with the transportation infrastructure. V2V, V2I infrastructure, and V2X communications aim to reduce traffic delays, improve fuel efficiency, and improve safety. V2X can help drivers, for instance, with intersection movement, weather alerts, road hazards, notification of emergency brake lights, and forward collision warning. In Figure 2.2, these last two scenarios are illustrated. In the first, the black car suddenly stops, and the bus avoids collision. In the second, the driver of the green car behind the bus cannot see the sudden stop, but the car is alerted and takes the appropriate safety measures to avoid a possible accident.

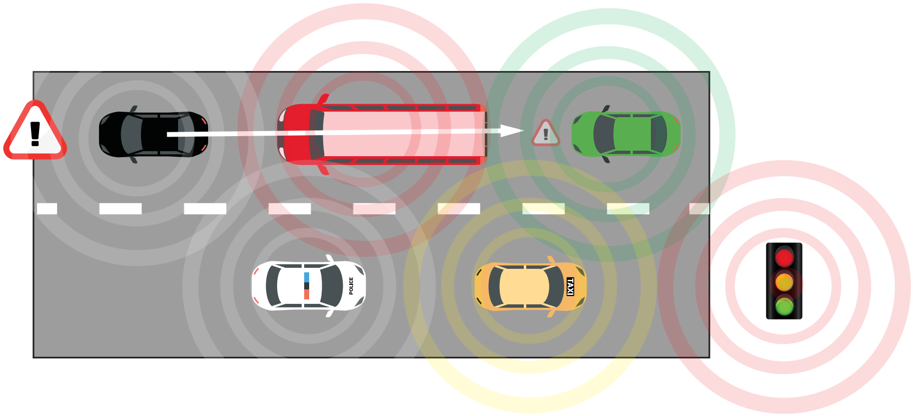


Figure 2.2: IoT can help to alert vehicles prior to visual confirmation of dangers. the black car suddenly stops, and the bus avoids collision and green car received the alert thanks to the V2V communication. Vehicles receive alert of traffic lights via V2I.

Intra vehicle communication systems consist of a network of sensors connected to the Electrical Control Unit (ECU) to obtain On-board diagnostics (OBD) to monitor drivers fatigue, road conditions, tyre pressure and water temperature in the cooling system etc [30]. The topology, deployment of the sensor systems, and connectivity to the ECU can be established with the traditional short-range protocols because the sensors are stationary and powered by the vehicle's power system. Vehicles can communicate with each other to avoid collisions, inform one another when a lane is changing, and other uses of inter-vehicle connectivity [31]. By properly designing the architecture and selecting lightweight communication protocols to establish a vehicle to vehicle communication, IoT can offer an easy transition from conventional vehicles to smart vehicles. Finally, a connected road infrastructure and autonomous driving are being made possible by these IoT communication systems [32]. In the case that diversions are needed, the smart infrastructure is capable of communicating the incident's details to traffic management systems.

2.1.2.6 Industrial Applications

Industrial Internet of Things (IIoT), includes businesses engaged in production and manufacturing, and it is a significant area that has already benefited from IoT. "Industry 4.0" a term used to denote the fourth industrial revolution is being used to include IoT [33]. IIoT leverages the vast amount of data generated by sensors and other connected devices to optimize processes, reduce costs, and minimize accidents. An example of this is how Amazon utilizes autonomous robots to manage inventory and fulfill customer orders, thus increasing shipping efficiency [34]. IIoT also enables automated monitoring and maintenance of assets, preventing costly downtime and repairs. In the future, IIoT will enable geographically dispersed sites to communicate more effectively about production lines, leading to lower inventory costs and real-time information sharing about problems or delays. The interconnected nature of IoT devices allows for constant exchange of information throughout the entire manufacturing and production cycle. By collecting and analyzing data from equipment, technologies, and locations, IIoT devices provide valuable insights to optimize processes, supply chains, and products, as well as respond to market demands. Predictive maintenance, statistical analysis, and advanced measurements are some of the ways IIoT can enhance safety and reliability. However, the rapidly expanding scalability of IoT devices may pose challenges for unprepared system administrators, and the collection of massive amounts of data may create vulnerabilities that could be exploited. To overcome these challenges, the IoT can connect industrial equipment to enable network control and management, delivering intelligent manufacturing processes.

2.1.2.7 Infrastructure Applications

IoT has the potential to change the way we monitor and manage sustainable urban and rural infrastructure. For example, IoT-enabled sensors can be placed on bridges, railroad tracks, and wind farms to collect data on structural conditions. This information can then be used to make safety and productivity improvements, reduce time and costs, and minimize risk. Additionally, real-time analytics can aid in scheduling maintenance and repairs, further increasing the efficiency and longevity of these infrastructure assets. Overall, IoT has the ability to enhance the sustainability and reliability of urban and rural infrastructures [35, 36].

2.1.2.8 Metropolitan Applications

IoT can play a vital role in the development of smart cities by connecting various infrastructure and systems to optimize their performance and improve the quality of life for residents. By integrating IoT sensors, devices, and networks, cities can collect and analyze data to make informed decisions and take proactive measures for managing various aspects such as traffic flow, environmental monitoring, public safety, and more. This can lead to a number of benefits such as reducing congestion, improving energy efficiency, enhancing public services, and creating a more sustainable and livable environment. Additionally, IoT-enabled smart city solutions such as digital signage, smart parking, public Wi-Fi, and paperless ticketing can make daily tasks more convenient and efficient for residents [37].

2.1.2.9 Energy Management Applications

The integration of IoT technology in various devices and assets, such as lamps, home appliances, and industrial equipment, allows for improved energy management and conservation. By connecting these devices to the internet, they can be remotely controlled and optimized for energy efficiency. Additionally, data on energy usage can be collected and analyzed through smart grid systems, enabling improved distribution and overall efficiency in energy consumption [38, 39].

2.1.2.10 Environmental Monitoring Applications

IoT-enabled sensors can revolutionize the way we monitor air and water quality. By collecting data on wildlife movements, soil condition, and more, we can gain a deeper understanding of the environment. Additionally, IoT sensors can aid in monitoring for natural disasters such as tsunamis and earthquakes, thus streamlining emergency response and minimizing damage. One example of this is the "Ocean of Things" project [40], which utilizes IoT technology to collect, monitor, and analyze environmental and vessel activity in the seas [41].

2.1.2.11 Agriculture Applications

Another way IoT-enabled sensors can alter our world is by monitoring the quality of the air or water. The IoT makes it possible to gather information on the movements of wildlife, the state of the soil, and other topics. Smart Agriculture uses IoT technologies to intelligently control the agricultural production process [42]. In a smart agriculture environment, various information technology and intelligent technology, such as AI, big data, and cloud computing, are used to integrate with agricultural technology to achieve effective tracking and control of crop growth environment, provide intelligent detection, prediction, analysis, and guidance services, aid in more accurate agricultural activities, and provide more convenient and efficient management support [43]. The initial development of smart agriculture will support ongoing advancements in agricultural production effectiveness and financial gains.

2.1.3 Requirements and Challenges in IoT

There are several requirements and challenges that need to be considered when developing and deploying IoT systems. Five significant challenges that pose the greatest threat to IoT security were prioritized and described below. These challenges were selected based on their potential impact on IoT security.

1. **Standardization:** In the rapidly-growing field of IoT, device and system manufacturers are often focused on being the first to bring new products to market, which can sometimes lead to security being a lower priority. As a result, there is a lack of standardization across many sectors of IoT, with different vendors following different design recommendations and deployment of heterogeneous devices into a common environment often requiring deactivation of some security features [44]. This lack of standardization can create a sense of mistrust among IoT devices and a lack of trustworthiness within the industry. In a 2017 IoT security survey, 96% of businesses believed there should be regulation for IoT security [45]. However, self-regulation is still needed as more devices are being introduced without proper security measures in place. The National Institute of Standards and Technology (NIST) and other organizations such as Institute of Electrical and Electronics Engineers (IEEE) are working to establish standards for IoT operability across various domains [46] with the aim of protecting the future of IoT devices and networks. Until a set of defined standards are agreed upon, there is a risk that companies that do not follow good security practices may put others at risk when their devices are integrated into heterogeneous networks.

2. **Cost, Size, Weight, and Power:** Implementing an IoT system can be expensive due to the costs of infrastructure, updates, maintenance, design, replacing outdated devices, and the technical skillsets required. These hidden costs can add up quickly and surprise those who are unprepared for them. In order to extend the lifetime of an IoT device, manufacturers often focus on minimizing the size and weight of the device, as well as the processing power, memory, and battery size. However, in order to ensure effective security,

manufacturers must also find a balance between size reduction, cost, and security. While size and weight may be important considerations for portable or easily integrated devices, such as wearable fitness trackers or smart home sensors, they may not be as relevant for other types of IoT devices.

3. **Trust and Authentication:** Trust and authentication are major challenges in the IoT due to the vast number of connected devices and the potential for unauthorized access or misuse. Ensuring trust and authentication in an IoT system involves verifying the identity of devices, users, and services, and only allowing authorized parties to access the system. Therefore, authentication is a crucial aspect of network security to ensure that only trusted devices can communicate on the network. Most authentication protocols used in IoT systems rely on non-physical data inspection, such as Data Encryption Standard (DES) [47], WiFi Protected Access (WPA) [48], WPA2 [49], or Elliptic Curve Cryptography (ECC) [50], which may have latent defects. The security of IoT devices can be a concern due to their small size, low cost, and potential lack of security compared to traditional computing devices [51]. This makes them more susceptible to attacks or compromise, which can damage trust in the entire system. To address these challenges, it is necessary to implement strong authentication and access control measures that verify the identity of devices, users, and services before granting access. This may involve using secure protocols like Transport Layer Security (TLS) or implementing device- or user-specific authentication methods such as biometrics or one-time passwords. Keeping IoT devices and software up to date with the latest security patches and updates can also help reduce vulnerabilities [52].

4. **Privacy:** Many IoT devices, such as smart home devices, wearable fitness trackers, and connected vehicles, collect and transmit data about the people who use them, including location, activity, and health information. While this data can be valuable to individuals and organizations, it also has the potential to be misused or mishandled if it is not properly protected. To address these privacy challenges, it is important to implement strong privacy controls and data protection measures that ensure personal data are collected, used, and shared in a transparent, secure, and respectful manner. This may involve implementing secure communication protocols, using encryption to protect data in transit, implementing access controls to prevent unauthorized access, implementing blockchain technology for a decentralized data storage, and ensuring that personal data is only collected and used for legitimate purposes.

It is also important to provide individuals with clear information about what data are being collected, how it will be used, and who it will be shared with, and to give them the ability to control their own data and privacy settings [53].

5. **Latency:** Latency, or the delay between the transmission and reception of a signal, can be a significant challenge in IoT as it can impact the performance and reliability of IoT systems. There are several factors that can contribute to latency in an IoT system, including the distance between the sender and receiver, network topology, protocol overhead, and device limitations. To address these challenges, it is essential to optimize the network infrastructure, select more efficient protocols, and choose devices with sufficient processing power and memory [54].

6. **Scalability:** IoT is expected to consist of billions of connected devices globally, making scalability a crucial aspect in the development of IoT-enabled applications. For example, if each parking spot is equipped with an occupancy sensor, the application would need to communicate with each sensor to check its status (empty or occupied) and then count the empty spots. While this approach may be manageable for a small system with only a few sensors covering a single street, it would not be scalable for millions of sensors potentially deployed throughout a city like Berlin due to the excessive delay and energy cost required for the communication between the application and all the sensors [55]. To build scalable systems, research efforts, such as the development of caching mechanisms, parallel computations, hierarchical architectures, and scalable web monitoring application, will be essential.

2.2 Wireless Sensor Networks (WSN)

In discussions about IoT, the term (WSNs) is often heard. WSN stands for Wireless Sensor Networks, which are networks of interconnected sensors that communicate wirelessly with each other and can be utilized for real-time data collection and transmission in various applications within the IoT ecosystem. These sensors, commonly known as sensor nodes or end nodes, have the capability to sense, measure and gather information from their environment, then use local decision-making processes to transmit the data to a central location or cloud-based server for analysis and decision-making. Also, they are characterized by the small size, low-power, and cost-efficient, and their wireless communication capabilities.

2.2.1 Wireless Sensor Networks: An Overview

WSNs have become increasingly popular in recent years, thanks in part to the advancements in Micro-Electro-Mechanical Systems (MEMS) technology, which has made it possible to produce small, inexpensive sensors with limited processing and computing resources [56]. WSNs can be applied in a variety of fields such as environmental monitoring, industrial automation, healthcare, agriculture, and military. They offer several advantages over traditional wired sensor networks, including flexibility, ease of deployment, and cost-effectiveness. However, they also face challenges such as limited power and transmission range, interference, security, and reliability.

WSNs can be either structured or unstructured. Structured WSNs have sensor nodes that are deployed in a pre-planned manner, providing coverage over a specific area. This allows for fewer nodes to be used, reducing network maintenance and management costs. In contrast, unstructured WSNs consist of a dense collection of sensor nodes that are deployed in an ad-hoc manner, often resulting in uncovered regions. These networks can be more difficult to maintain and manage due to the large number of nodes. Both types of WSNs can be used for a variety of applications, including environmental monitoring, industrial automation, healthcare, agriculture, and military.

As illustrated in Figure 2.3, WSNs rely on sensor technologies to enable a range of tasks, which can be broadly classified into three categories: systems, communication protocols, and services.

- **Systems:** Each sensor node in a WSN is an individual system that requires the development of platforms, operating systems, and storage schemes to support different application software.

- **Communication protocols:** These enable communication between the application and sensors, as well as between the sensor nodes themselves.

- **Services:** These are developed to enhance the application and improve system performance and network efficiency.

WSN are able to self-organize and efficiently control and manage themselves [57]. This requires the development of new communication protocols and management services that take into account the limited power, processing capacity, and storage of the sensor nodes. Self-organization allows the sensor nodes to form a network and work together to carry out the tasks required by the application, such as monitoring the environment or controlling industrial processes. It also helps to optimize the use of resources and improve the efficiency of the WSN. However, WSNs can face

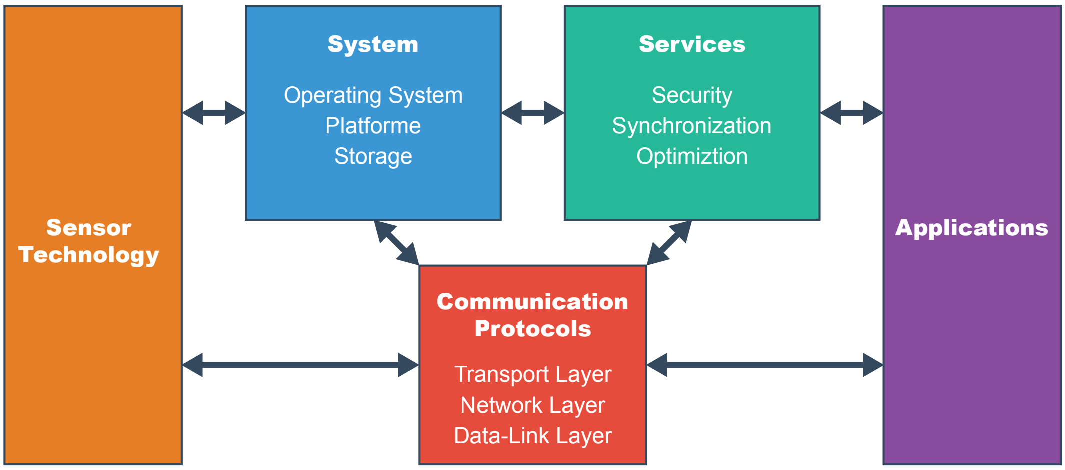


Figure 2.3: Broad classification of technologies in a WSN.

challenges such as limited power and communication range, interference, security, and reliability [58].

The communication protocol for WSNs consists of five standard layers: the application layer, transport layer, network layer, data-link layer, and physical layer. In addition to these standard layers, WSNs also explore functions such as localization, coverage, storage, synchronization, security, and data aggregation and compression as sensor network services [59]. It is crucial to optimize communication and minimize energy usage in WSNs, as the implementation of protocols at different layers in the protocol stack can significantly impact energy consumption, end-to-end delay, and system efficiency. However, traditional networking protocols are not well-suited for WSNs because they are not designed to meet the specific requirements of these networks. As a result, new energy-efficient protocols have been proposed for all layers of the protocol stack in WSNs. These protocols employ cross-layer optimization, which involves sharing protocol state information across all layers in order to meet the specific requirements of the WSN. This approach allows for more efficient communication and better resource management in the network.

2.2.2 Routing protocols of Wireless Sensor Networks

Routing protocols in WSNs determine how nodes communicate with each other and how information is disseminated throughout the network. There are various methods of classifying these routing protocols. Figure 2.4 illustrate the basic classification of routing protocols.

1. **Node centric:**
   In node-centric protocols, the destination node is specified using numeric identifiers, which is not a common method of communication in WSNs. An example of a node-centric protocol is Low Energy Adaptive Clustering

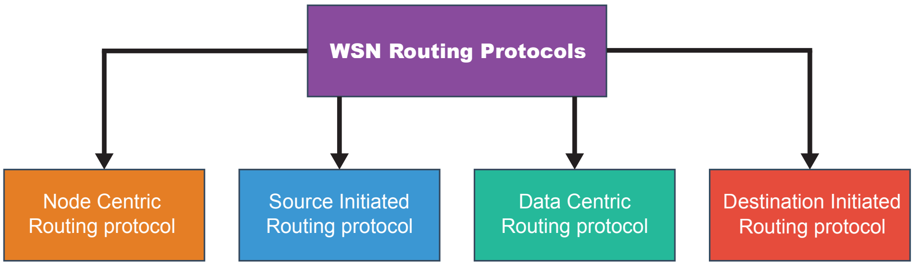

WSN Routing Protocols
Node Centric Routing protocol
Source Initiated Routing protocol
Data Centric Routing protocol
Destination Initiated Routing protocol

Figure 2.4: Classification of routing protocols of WSN

Hierarchy (LEACH), a routing protocol that aims to distribute the energy used by sensor nodes evenly across the network by organizing them into clusters. In LEACH, one node in each cluster is designated as the cluster head and acts as a routing node for all other nodes in the cluster. The cluster heads are selected through a randomization process, with sensor nodes electing themselves as cluster head with a probability defined by the protocol and announcing this to the other nodes. Node-centric protocols can be used to improve the efficiency and resource utilization of WSNs, but they may also encounter challenges such as interference, security and reliability [60].

2. **Destination-initiated (Dst-initiated):**
   The destination node initiates communication with the source node, rather than the other way around. In other words, the destination node initiates a request or query for data or information, and the source node responds with the requested data [61].

3. **Data-centric:**
   In WSNs, the data or information collected by the sensor nodes is often more valuable than the nodes themselves. Data-centric routing techniques prioritize the transmission of information based on specific attributes, rather than collecting data from specific nodes. In these techniques, the sink node sends queries to specific regions to gather data with specific characteristics. Thus, it is essential to use a naming scheme based on attributes to describe the characteristics of the data. This allows the sink node to efficiently gather the specific data it needs from the network, rather than indiscriminately collecting data from all the nodes. Data-centric routing can help optimize the use of resources in WSNs and improve the efficiency of data collection and transmission [60].

4. **Source-initiated (Src-initiated):**
   The source node initiates the transmission of data or information to the destination node, rather than waiting for an explicit request. This means

that the source node actively sends data to the destination node, rather than waiting for the destination node to initiate the communication [62].

2.3 Short-Range Wireless Sensor Network

Short-range wireless communication refers to wireless communication over relatively short distances, such as those covered by wireless personal area networks (WPANs) and wireless local area networks (WLANs). In recent years, there has been an increase in the use of wide-range wireless communication technologies, such as field area networks (FANs), which utilize multi-hop technology to extend their range. FANs are an example of a wireless communication technology that falls outside the traditional definition of short-range communication [63].

2.3.1 Short-Range communication protocols

There are several wireless technologies designed for communication over short distances, typically within a few meters. These technologies are known as short-range wireless communication. In contrast, medium-range wireless communication allows for communication over distances up to 100 meters, while wide-area wireless communication can reach distances ranging from several kilometers to thousands of kilometers. Some examples of short-range wireless communication include Bluetooth, Infrared, Near Field Communication, Ultra-Wideband, WiFi, and ZigBee. This section focus on five of these technologies: Wi-Fi, Bluetooth, ZigBee, UWB and BLE which are all part of the WPANs family.

2.3.1.1 Wi-Fi

Wi-Fi is a wireless networking technology that allows devices to connect to the Internet or to each other. It is based on the IEEE 802.11 family of standards, including 802.11abg, and it uses radio waves to transmit data over the air. When connected to an access point, users can surf the Internet using a WLAN (Wireless Local Area Network). The Wi-Fi architecture consists of various components that work together to provide WLAN capability [64]. The basic unit of a Wi-Fi LAN is called a basic service set (BSS), which consists of fixed and mobile stations. When a station moves outside of its BSS, it is unable to communicate directly with other members of the BSS. There are two types of network configurations based on BSS: independent basic service set (IBSS) and extended service set (ESS). IBSS networks are ad-hoc networks that are formed without pre-planning, while ESS networks are formed by combining multiple BSSs using a distribution system and access points. ESS networks can be of any size and complexity [65].

2.3.1.2 ZigBee

ZigBee is a wireless technology that operates based on the IEEE 802.15.4 standard for WPAN. It enables low-cost, low-data-rate, and long-battery-life networks that allow devices to communicate with one another, regardless of their manufacturer. This protocol is often used for devices that require low power consumption and has a range of about 10-20 meters [66]. The ZigBee standard was developed by the ZigBee Alliance [67], a collaboration of companies dedicated to creating reliable, cost-effective, and low-power wirelessly networked products based on an open global standard. The Zigbee Alliance, a nonprofit organization, which was founded in 2002 and is open to all interested parties, has hundreds of member companies ranging from semiconductor and software developers to Original Equipment Manufacturers (OEMs) and installers.

2.3.1.3 Ultra-wideband (UWB)

UWB technologies, which use short-pulse signals, have been utilized in radar systems since the 1960s and have gained attention for their communication applications since the 1990s. UWB technology has gained popularity due to its high speed of indoor wireless communication [68]. The UWB frequency range is between 3.1 and 10.6 GHz. UWB can determine the relative position of other devices within 200 meters in its line of sight. With a bandwidth ranging from 110 to 480 Mbps, UWB is capable of handling multimedia applications, such as audio and video delivery, in home networking, making it a suitable replacement for high-speed cables such as USB 2.0 [69]. UWB uses pulse position or time modulation, and its ability to regulate the time of flight at different frequencies allows it to overcome multipath propagation.

2.3.1.4 Bluetooth and BLE

Bluetooth technology is a short-range wireless communication system that operates according to the IEEE 802.15.1 standard [70]. It was initially developed as a replacement for cabled RS-232 connections, but is now used to transfer data between personal area networks and various types of devices, including fixed and mobile devices. Bluetooth uses a master/slave architecture, where devices can take on either role and can switch between them by mutual agreement. One master device can communicate with up to seven slave devices in a single piconet. In order to use Bluetooth technology, a device must be able to interpret certain Bluetooth profiles, which are predefined sets of applications and behaviors that allow Bluetooth-enabled devices to communicate with each other. These profiles include settings that establish and control the communication from the outset, saving the time and effort of transmitting parameters separately before the connection is established [71].

Adhering to these profiles helps ensure compatibility and interoperability between devices.

BLE is designed to provide reduced power consumption and cost, while maintaining a similar communication range to classic Bluetooth. Its ultra-low power requirements make it ideal for small devices, such as wearable technologies, where minimal battery life and small form factor are crucial design considerations. BLE is commonly used in a wide range of devices, including heart rate monitors and smart watches, which require small data updates, like current heart rate, every few seconds [72]. It is also used for health and fitness wearables, and for other small devices that need to communicate with other devices. Bluetooth, on the other hand, is mainly used for streaming audio and for connecting devices such as mouse, keyboard, and headphones.

2.3.2 Comparative Analysis of Short-Range Communication Protocols

In this section, Five short-range wireless communication technologies used for WPANs are compared, which are Bluetooth, BLE, ZigBee, Ultra-wideband, and Wi-Fi. The performance of a WPAN can be evaluated based on three factors: data coding efficiency, transmission time, and power handling capabilities.

2.3.2.1 Data coding efficiency

Data coding efficiency refers to the performance and accuracy of a telecommunication system. It is calculated as the ratio of the data size to the message size, or the number of bytes used to transmit the data. The formula for calculating efficiency is described in Equation 2.1:

$$P_{codeEff} = \frac{N_{data}}{N_{data} + [\frac{Ndata}{NMax}] \times N_{Over}} \times 100. \tag{2.1}$$

Where N_{data} is the total data size, N_{Max} represents the maximum data size and N_{Over} represents overhead data size.

The data coding efficiency of the five technologies varies with respect to the data size. The efficiency generally increases as the data size increases. When dealing with small data sizes, ZigBee, BLE and Bluetooth tend to offer the best results. However, for large data sizes, UWB and Wi-Fi are more preferable choices. The data in this graph was obtained by using the typical parameters listed in Table 2.1 for the five short-range wireless technologies [73].

Figure 2.5 demonstrates that among the five technologies, ZigBee and BLE have the lowest efficiency, while the others (Wi-Fi, UWB, and Bluetooth) have approximately 94% efficiency for larger payload data sizes. The fluctuations in the

Wireless technology	Bluetooth	UWB	Wi-Fi	ZigBee	BLE
Time of bits (μs)	1.39	0.0091	0.0185	4	1
Max Data rate (Mbit/s)	0.72	110	600	0.25	2
Maximum data payload (bytes)	27	2048	2304	100	251
Coding efficiency %	94.41	97.94	97.18	76.52	78.68

Table 2.1: Typical parameters of short-range wireless protocols

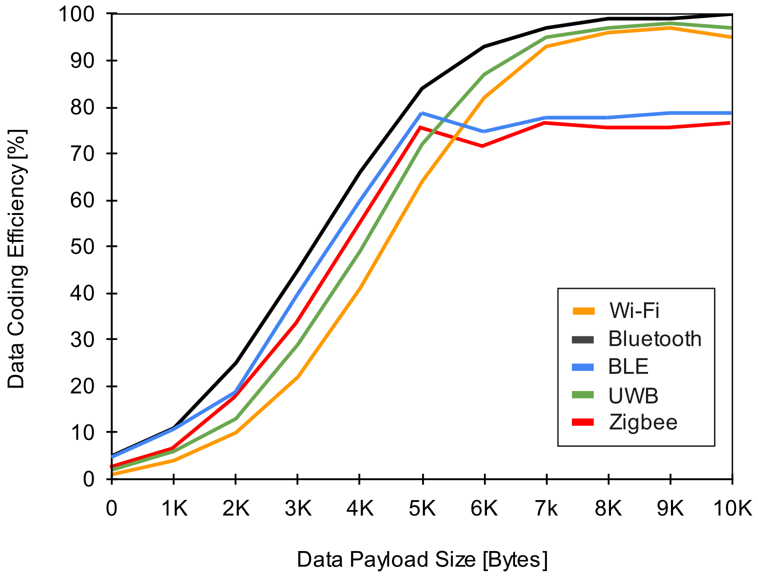


Figure 2.5: Comparison between data size and data coding efficiency in short-range communication protocols

graph are likely due to data fragmentation. In terms of data rate, Wi-Fi and UWB outperform BLE and ZigBee.

2.3.2.2 Transmission time

The transmission time can be obtained using Equation 2.2:

$$T_{tx} = N_{data} + (\frac{N_{data}}{N_{Max} \times N_{Over}}) \times T_{bit} + T_{prop}. \tag{2.2}$$

Where N_{data}, N_{Max} and N_{Over} represents data, maximum payload and overhead size, respectively. T_{bit} and T_{prop} represents the bit time, and the propagation time between two nodes, respectively.

As shown in Figure 2.6, the transmission time of the five technologies varies based on their data coding efficiency and data size. ZigBee has a lower data rate (i.e., 250 kbps) compared to the other three protocols, resulting in a longer transmission time. On the other hand, Ultra-wideband (UWB) has the highest data rate (i.e., 110 Mbit/s), making it the fastest in terms of transmission time among the five technologies [74]. It is clear that the transmission time is directly proportional to the data payload size and inversely proportional to the data rate of the WPAN protocol [75]. According to Figure 2.6, UWB has the shortest transmission time among the remaining four protocols

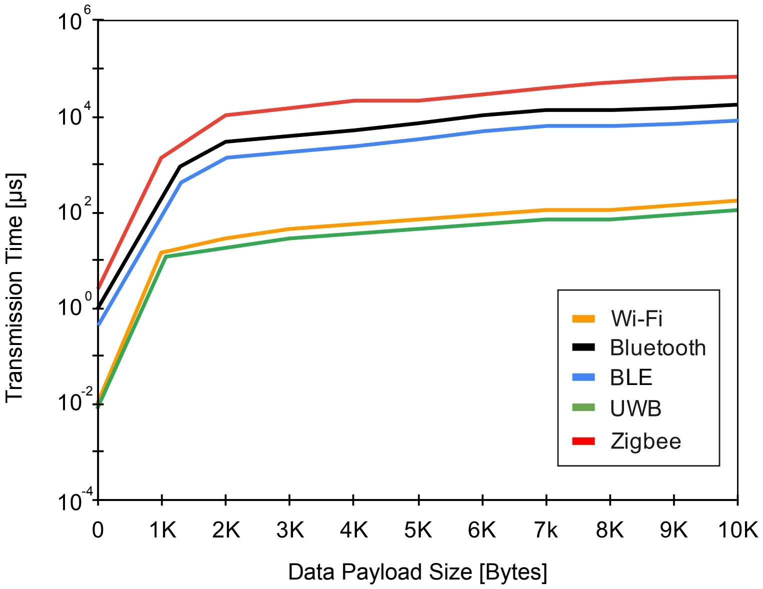


Figure 2.6: Comparison between transmission time and data size in short-range communication protocols

2.3.2.3 Transmission range

The transmission range of a WPAN plays a crucial role in determining its overall performance. The distance over which data can be transmitted is directly impacted by the transmission power of the network, making it essential to carefully consider this factor during the design process. This includes assessing the power level required to effectively cover the intended area of operation, and ensuring that the network's transmission power is optimized to support the desired range while also minimizing energy consumption. [76]. In wireless transmissions, the relationship between the received power and the transmitted power is given by the Friis equation [77–79] as follows (Equation 2.3):

$$\frac{P_r}{P_t} = G_t G_r (\frac{\lambda}{4\pi D})^2. \tag{2.3}$$

where G_t and G_r are transmitted and received gains of the antenna, λ is the wavelength, and D is the distance between the receiver and the transmitter.

From Equation 2.3, D can be derived as follows:

$$D = \frac{1}{\frac{4\pi}{\lambda}\sqrt{\frac{P_r}{P_t G_t G_r}}}. \tag{2.4}$$

From Equation 2.4, we can note that, as the frequency increases, the range of the signal tends to decrease. This relationship is demonstrated in Figure 2.7, which shows the variation of the signal range based on the transmission frequency for a fixed power. Ultra-wideband (UWB) has the smallest signal propagation range of 3.1 GHz among the five protocols.

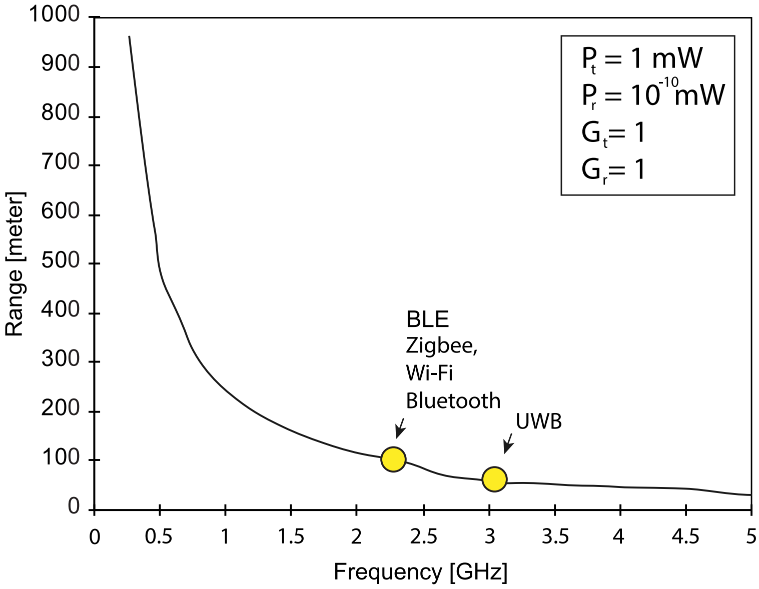


Figure 2.7: Comparison between range and frequency transmission in short-range communication protocols

2.3.2.4 Power consumption

To compare the power consumption of different protocols, Table 2.2 presents a representative characteristics for specific chipsets of each protocol [80]. Figure 2.8 shows the power consumption in milliwatts (mW) for each protocol. As depicted in this figure, it can be observed that the power consumption of UWB and Wi-Fi is approximately 8 times higher compared to that of Bluetooth, BLE and Zigbee.

Protocol	**Chipset**	V_{DD} **(Volt)**	I_{Tx} **(mA)**	I_{Rx} **(mA)**	**Bit rate (Mb/s)**
Wi-Fi	CX53111	3.3	219	215	54
Bluetooth	BlueCore2	1.8	57	47	0.72
BLE	CC2540	3.0	24	19.6	2
Zigbee	CC2430	3.0	24.7	27	0.25
UWB	XS110	3.3	227.3	227.3	114

Table 2.2: Power consumption characteristics of some chipsets in short-range communication protocols

When choosing a wireless protocol for an intelligent sensing application, it is essential to weigh the trade-offs between energy consumption, quality of service, and real-time performance. By evaluating various factors, such as network reliability, link capacity, security, chipset cost, compliance, and installation cost, robust sensing

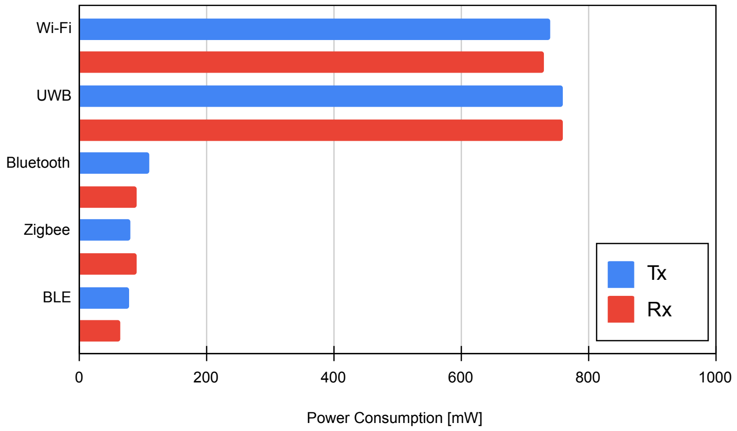


Figure 2.8: Comparison of chipset power consumption for each short-range communication protocol

quantitative indicators can assist in determining the most suitable protocol for the specific application. A significant challenge in this process is developing a gateway that can facilitate data exchange between different infrastructures with a high level of quality of service, despite the use of unlicensed frequency bands, such as those used by Bluetooth and Wi-Fi, that are commonly employed in short-range communication technologies.

2.4 BLE protocol

The Bluetooth Low Energy (BLE) is frequently the preferred option for numerous IoT applications due to its low power consumption as highlighted in the previous section, and compatibility with various platforms, including smartphones and tablets, render it ideal for IoT applications that necessitate connectivity with these devices. As illustrated in Figure 2.9, the BLE protocol stack is divided into two main parts: the Controller and the Host. The Controller handles the Physical Layer and Link Layer, which are responsible for managing physical layer packets and their associated timing. It is typically implemented as a small System-on-Chip (SoC) with an integrated Bluetooth radio. The Host, on the other hand, contains the upper layer of the stack, including profiles and applications. It typically runs on the application processor along with the user's application [81]. The communication between the Host and the Controller is standardized through the Host Controller Interface (HCI). The purpose of HCI is to interface the Controller with the Host, allowing a wide range of Hosts to communicate with the Controller.

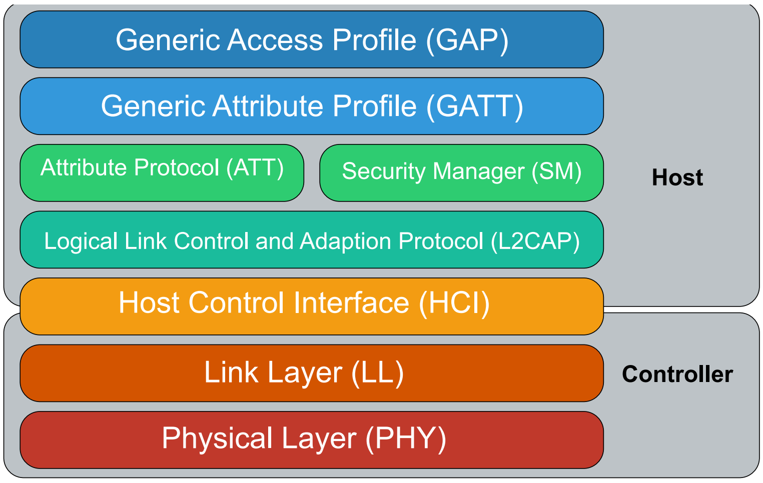

Generic Access Profile (GAP)
Generic Attribute Profile (GATT)
Attribute Protocol (ATT)
Security Manager (SM)
Logical Link Control and Adaption Protocol (L2CAP)
Host Control Interface (HCI)
Link Layer (LL)
Physical Layer (PHY)
Host
Controller

Figure 2.9: The BLE protocol stack.

2.4.1 Physical Layer

The Physical Layer of BLE describes how a BLE device transmits and receives data wirelessly. BLE uses the 2.4 GHz Industrial, Scientific, Medical (ISM) band, which is commonly used because it is unlicensed. This band ranges from 2400 MHz to 2483.5 MHz and is divided into 40 Radio Frequency (RF) channels with a 2 MHz channel spacing as illustrated in Figure 2.10. Among these channels, three are designated as "advertising" channels and are used by devices to broadcast information about themselves so that other BLE devices can connect. The remaining channels are called "data" channels and are used for bidirectional communication between connected devices. The advertising channels were chosen in the lower, upper and middle portions of the band to minimize interference with other channels. For example, if Channel 38 and its surrounding channels are being interfered with by WiFi, the advertising channels 37 and 39 will not be affected [82].

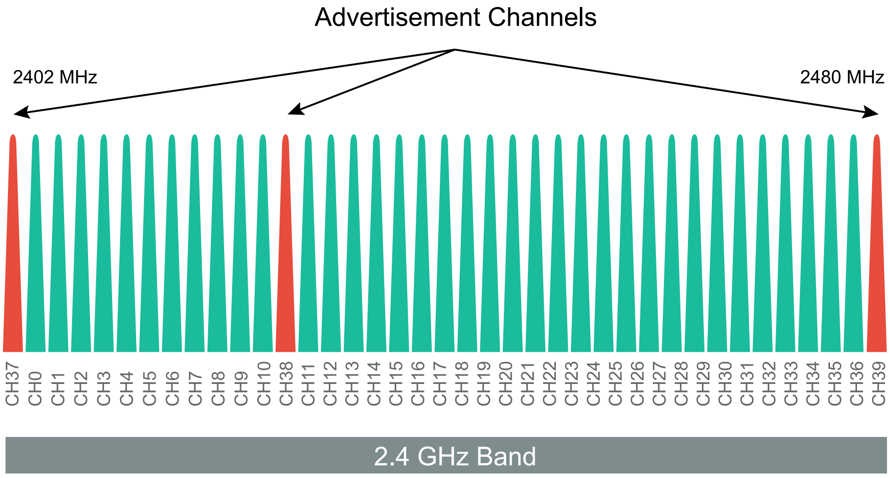


Figure 2.10: BLE Frequency Band

2.4.2 Link Layer

BLE technology uses two types of devices: advertisers and scanners. Advertisers transmit advertising packages, while scanners only receive data via advertising channels. These transmissions occur during intervals called advertising events. In each event, the advertiser rotates between advertising channels for packet transmission. To establish bidirectional communication, the advertiser must announce its connectability through advertising channels, and the initiator device listens for these advertisements. Once the initiator finds the advertiser, it can initiate a connection by sending a connection request message. This creates a point-to-point connection between the two devices, enabling them to communicate through physical data channels. The communication is identified by a 32-bit randomly generated access code, which ensures the security of the connection. With this code, the devices can send and receive data packets seamlessly and securely [83].

BLE defines two device roles in a created connection: Master and Slave. During the connection creation process, some devices act as initiators while others act as advertisers. A Master can manage multiple connections with different Slaves, while each Slave can only connect to one Master. The network composed of a Master and its Slaves is called a piconet and follows a star topology. A BLE device can only belong to one piconet at a time. Slaves are usually in sleep mode by default to conserve energy, waking up periodically to listen for packets from the Master. The Master coordinates medium access through a Time Division Multiple Access (TDMA) scheme, determining when Slaves should listen and providing frequency hopping information.

Once a connection is established between a Master and a Slave, connection management parameters are transmitted, dividing the physical channel into non-overlapping time units called connection events. All packets within a connection use the same data channel frequency. The Master transmits a packet at the start of each connection event, and the Slave should respond with a packet if it receives the Master's packet. A minimum of 150 μs should pass between the end of one transmission and the start of the next. Each new connection event uses a different data channel frequency, computed using the frequency hopping algorithm [84].

2.4.3 L2CAP

The Logical Link Control and Adaptation Protocol (L2CAP) is a protocol for Bluetooth Low Energy that supports the generic access profile (GAP) by defining the procedures for discovering BLE devices and managing links with other LE devices. The purpose of L2CAP is to multiplex data from three higher layer protocols, including Attribute protocol (ATT), Security Manager (SM), and Link Layer control signaling, over a Link Layer connection [85].

2.4.4 BLE Profile

A BLE profile is a specification in Bluetooth technology that outlines the set of actions and behaviors for devices to communicate with each other. It ensures compatibility when multiple devices use the same profile. For instance, keyboards utilize the Human Interface Device (HID) profile and heart rate monitors use the Human resource management (HRM) profile [85].

2.4.5 GAP and Application Profiles

The BLE Generic Attribute Profile (GAP) outlines the procedures for device discovery, connection, and communication between BLE devices. The GAP defines four device roles: Broadcaster, Observer, Peripheral, and Central [86].

- Broadcaster: A device that only broadcasts data through advertising channels and does not support connections with other devices.
- Peripheral: A device that connects to a Central device, such as a fitness monitor connecting to a mobile phone.
- Central: A device that connects to a Peripheral device, such as a mobile phone connecting to a fitness monitor.
- Observer: A device that listens for broadcasts from Broadcaster devices.

A device may support multiple roles, but can only adopt one role at a time. The GAP requires the device's controller to support either the slave (Peripheral) or master (Central) role, depending on the device's role. Figure 2.11 shows the three steps to establish a connection between a BLE master and slave.

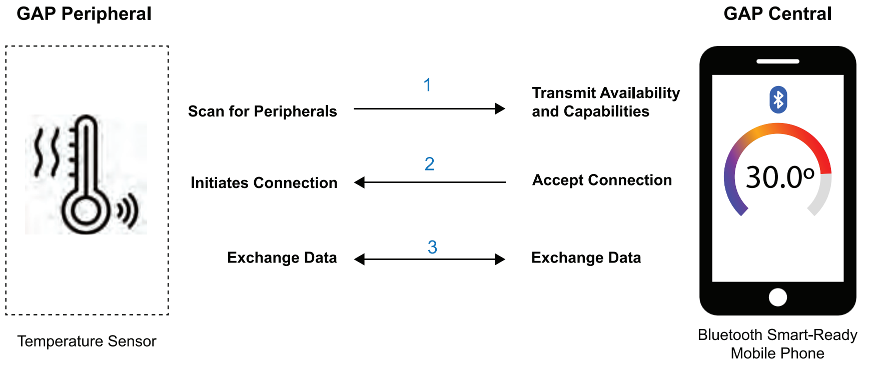


Figure 2.11: The three steps to establish a BLE Connection between master and slave

2.4.6 ATT and GATT

The Attribute Protocol (ATT) defines the communication between two BLE devices, where one device acts as the server and the other as the client. The server holds a collection of attributes, and the client can request access to these attributes by sending requests to the server. In response, the server sends back the requested information.

Generic Attribute Profile (GATT) is a framework that uses the ATT to discover services, and exchange characteristics from one device to another. A BLE device can operate in two GATT roles, GATT server and GATT Client. The device serving as the GATT Server maintains the attributes and receives requests and data, while the GATT Client is responsible for requesting and receiving data. An attribute is a data structure that stores information managed by the GATT protocol, which also determines the client or server role. This role is separate from the slave or master role assigned in the BLE link layer. A characteristic is a set of data which includes a value and properties. The data related to services and characteristics are stored in attributes. For example, a server that runs a "Humidity sensor" service may account with a "Humidity" characteristic that uses an attribute to describe the sensor and another attribute to store measurement values. The GATT Database stores and provides data. Runs in a GAP Peripheral and responds to read and write requests from both GAP Central and the GAP Peripheral itself. Figure 2.12 describe the BLE Communication via GATT Database, where GATT server is the temperature sensor and GATT client is the mobile phone. In order to modify an attribute value, the client sends commands to the server. The communication between the server and client occurs over a dedicated L2CAP channel, ensuring efficient and secure transfer of data.

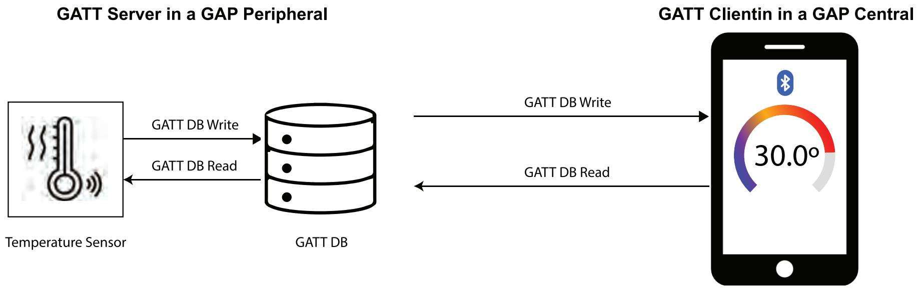


Figure 2.12: BLE communication via GATT database.

2.4.7 Security

BLE provides robust security services to safeguard the information exchange between connected devices. It supports two main security modes: LE Security Mode 1 and LE Security Mode 2. LE Security Mode 1 provides security at the Link Layer while LE Security Mode 2 provides security at the ATT layer. Encryption in BLE uses AES-CCM cryptography and the encryption process is handled by the LE Controller. The AES-128-bit block cipher, as specified in FIPS-1971, is used to generate 128-bit encrypted data from 128-bit plaintext data and a 128-bit key [87].

In addition, BLE also supports the privacy feature, which allows a device to frequently change its private addresses, reducing the risk of tracking. These private addresses are generated by encrypting the public address of the device, and can be resolved by a trusted device that has been provided with the corresponding encryption key.

2.5 Long Range Wireless Sensor Network

Long-range wireless communication refers to the use of wireless radio technologies to enable communication between devices over large distances, typically spanning tens of kilometers. These technologies, known as Low-Power Wide-Area Networks (LPWAN), have gained significant attention in both academia and industry, with early examples such as Sigfox and LoRa. With the recent emergence of technologies like Long-Term Evolution (LTE-M) and Narrowband-IoT (NB-IoT), and the impending rollout of 5G, the IoT connectivity landscape is rapidly changing. It is crucial to understand the role of LPWAN in this landscape, as well as how to evaluate the costs and benefits of different LPWAN technologies in order to make informed decisions about connectivity options.

2.5.1 Long Range communication protocols

LPWAN technologies have gained significant attention in recent years for their ability to enable communication over large distances, typically spanning tens of kilometers. These technologies come in a variety of forms, including open-standards and proprietary options, as well as those that operate in unlicensed ISM band and those that use global system for mobile (GSM) frequency bands. Additionally, LPWAN can be deployed through user-based or operator-based models. It is important to understand the different characteristics and capabilities of LPWAN technologies in order to make informed decisions about connectivity options. As described in Figure 2.13, LPWANs can be divided into two categories: 3GPP-based technologies and non-3GPP-based technologies; 3GPP-based technologies, also known as licensed technologies, are standardized by the 3GPP standards body and have the capability to support existing cellular networks, while non-3GPP-based technologies, also known as unlicensed technologies, do not fall under the 3GPP standards.

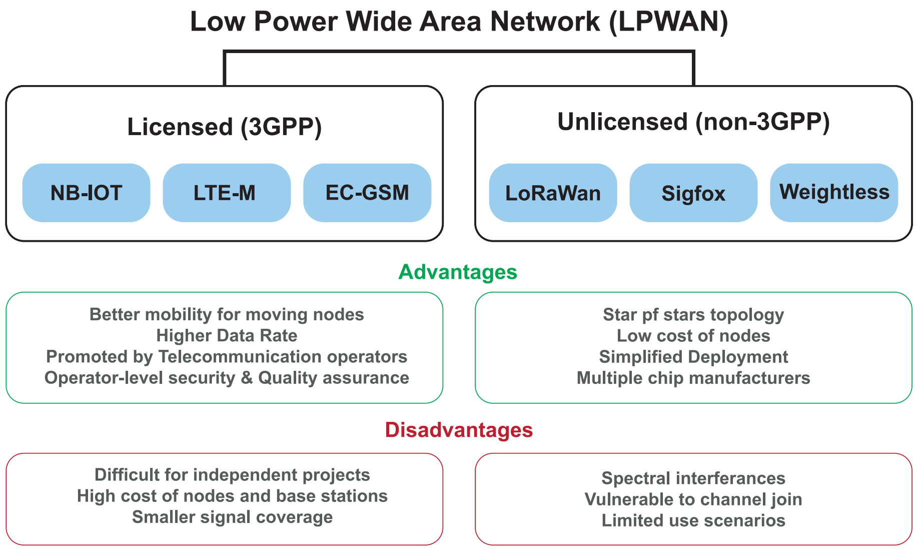

Low Power Wide Area Network (LPWAN)
Licensed (3GPP)
NB-IOT
LTE-M
EC-GSM
Unlicensed (non-3GPP)
LoRaWan
Sigfox
Weightless
Advantages
Better mobility for moving nodes
Higher Data Rate
Promoted by Telecommunication operators
Operator-level security & Quality assurance
Star pf stars topology
Low cost of nodes
Simplified Deployment
Multiple chip manufacturers
Disadvantages
Difficult for independent projects
High cost of nodes and base stations
Smaller signal coverage
Spectral interferances
Vulnerable to channel join
Limited use scenarios

Figure 2.13: The classification of LPWAN technologies with their advantages and disadvantages.

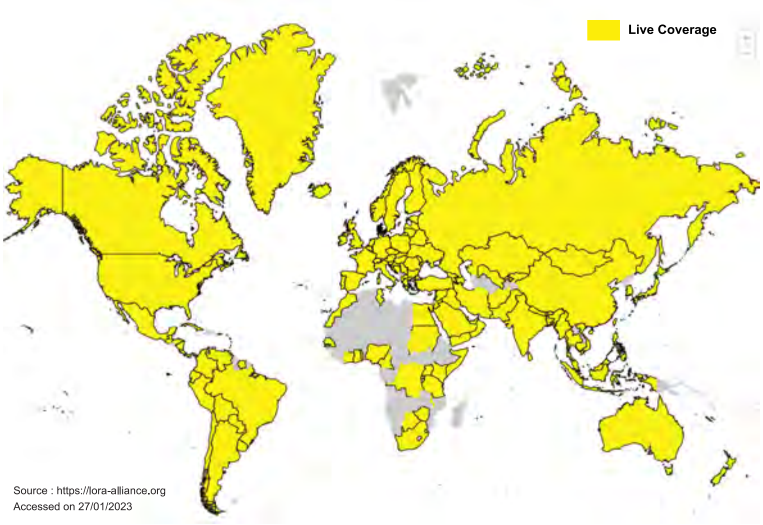
In this section, we will delve into the characteristics and capabilities of three pioneer LPWAN technologies: LoRa, Sigfox and NB-IoT.

2.5.1.1 LoRa

LoRa is a proprietary technology developed by Semtech [88]. It uses Chirp Spread Spectrum (CSS) modulation and can operate in various bands of the ISM sub-GHz spectrum, depending on the region: 868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia. LoRa communications are resistant to detection and jamming and are immune to Doppler deviation [89]. The technology offers several adjustable parameters that allow for a trade-off between range and data rate (from 0.3 to 50 kbps), such as the spreading factor. LoRa uses six spreading factors (SF7 to SF12) to adjust the trade-off between range and data rate. Higher spreading factors allow for longer range at the cost of lower data rates, while lower spreading factors increase data rates but reduce range. Additionally, LoRa base stations are able to receive messages transmitted using different spreading factors simultaneously [90].

While LoRa is the physical layer technology, LoRaWAN [91], supported by the LoRa Alliance, is an open protocol for the MAC and network layers. LoRaWAN defines three classes of devices: Class A for highly energy-constrained devices, Class B for moderately energy-constrained devices, and Class C for always-on devices.

Figure 2.14 displays the global deployment of LoRaWAN technology, which is currently present in 173 countries around the world [91].



Source : https://lora-alliance.org
Accessed on 27/01/2023

Figure 2.14: LoRaWAN deployment around the world

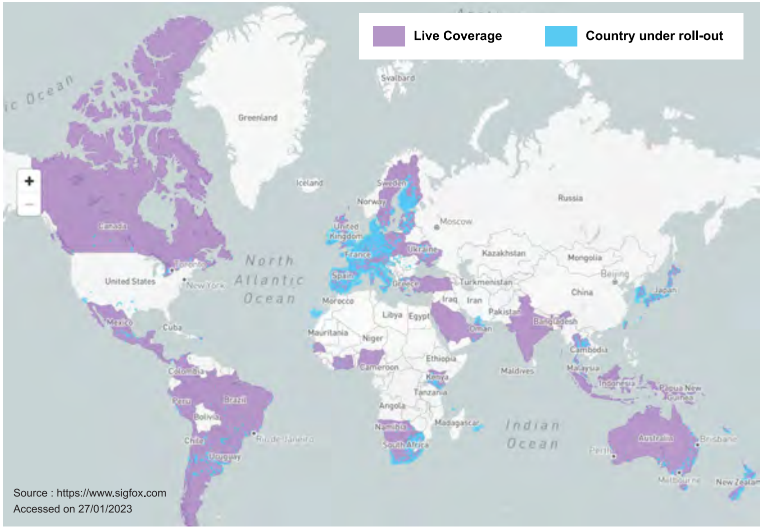
2.5.1.2 Sigfox

Sigfox [92] is a proprietary IoT connectivity solution that operates as an alternative network operator by deploying base stations globally. It uses Binary Phase Shift Keying (BPSK) modulation over an Ultra-Narrow-Band (UNB) carrier in the sub-GHz ISM bands, which allows for a long communication range but low data rate of 100 bits per second. To comply with duty cycle regulations in the sub-GHz bands, Sigfox limits up-link communications to 140 transmissions of 12 bytes payload and down-link to 4 transmissions of 8 bytes payload per day and per device. Additionally, the sensitivity of Sigfox base stations varies depending on the transmission bit rate; for example, a bit rate of 100 bps has a receiver sensitivity of -142 dBm, while a rate of 600 bps has a sensitivity of -134 dBm.

The Sigfox network is available in several countries and operates as a single, unified network, eliminating the need for roaming when using it in different countries. Figure 2.15 illustrates the Sigfox coverage around the world [92].

2.5.1.3 NB-IoT

Long-Term Evolution (LTE) is a standard from the 3GPP. LTE Cat M1, also known as LTE-M or Enhanced Machine-Type Communication (eMTC), is derived from the LTE standard and specified in 3GPP release 13. It is designed for Machine-to-Machine (M2M) communications, such as those used in the IoT. eMTC is a simplified version of LTE that is designed to use less battery power and extend its range. In contrast to classic LTE, eMTC reduces the data rate to one-tenth of LTE



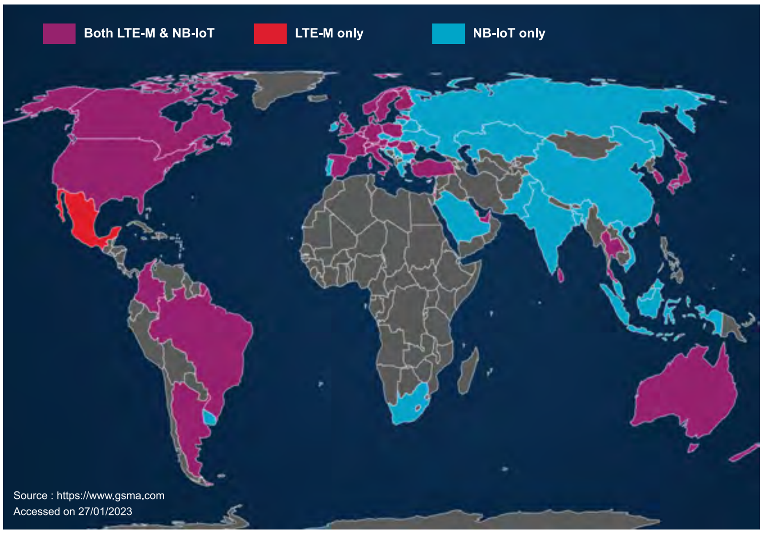
Source : https://www.sigfox.com
Accessed on 27/01/2023

Figure 2.15: Sigfox coverage estimation based on computer prediction

(up to 1 megabit per second) and reduces the bandwidth from 20 MHz to 1.4 MHz. eMTC supports full-duplex communications and optional half-duplex operations to reduce power consumption. It's worth noting that Voice over LTE (VoLTE) is also possible on LTE-M communications. eMTC includes two new features: extended Discontinuous Reception (eDRX) and Power Saving Mode (PSM). The eDRX feature allows for longer paging cycles, while the PSM feature allows nodes to be inactive for an indefinite period of time, both with the goal of reducing power consumption. eMTC also supports handover, making it suitable for mobile IoT applications. eMTC has already been deployed in numerous countries worldwide and is relatively easy for Mobile Network Operators (MNOs) to deploy, as it only requires a software upgrade without any physical hardware modifications.

NB-IoT is also known as LTE Cat NB1 and is a technology that allows for the efficient and secure connection of numerous devices using established mobile networks. It transmits data in both uplink and downlink directions and is known for its long battery life, large coverage area, low cost, and network security [93, 94]. NB-IoT requires a minimum of 180 kHz of bandwidth to operate, which is equal to the smallest LTE Physical Resource Block (PRB). The availability of spectrum in the existing LTE network determines the mode of operation for NB-IoT, which can be divided into three categories: stand-alone, guard band, and in-band. Stand-alone operation involves deploying NB-IoT on its own or using existing GSM low bands (700 MHz, 800 MHz, and 900 MHz). Guard band operation involves using the guard carries of already existing LTE spectrum. In-band operation involves replacing PRBs in the existing LTE spectrum.

NB-IoT uses Single Carrier Frequency Division Multiple Access (SC-FDMA) for uplink data transmission and Orthogonal Frequency Division Multiplexing (OFDM) for downlink transmission. The downlink includes four physical layer channels: a synchronization channel, a broadcast channel, a control channel, and a data channel. The uplink has two channels: the Narrowband Random Access Channel (NPRACH) and the Narrowband Uplink Shared Channel (NPUSCH). While NB-IoT is already available in some regions, it is still being deployed in other countries. However, its deployment is not as straightforward as eMTC because it requires a hardware upgrade to the existing LTE infrastructure. Figure 2.16 illustrate the worldwide deployment of the LTE-M and NB-IoT technologies.



Source : https://www.gsma.com
Accessed on 27/01/2023

Figure 2.16: Countries with LTE-M and NB-IoT deployment

2.5.2 Comparative Analysis of Long-Range Communication Protocols

When selecting an LPWAN technology for an IoT application, it is important to consider various factors such as quality of service, battery life, latency, scalability, payload length, coverage, range, deployment, and cost. In this section, the proprietary technologies Sigfox, LoRa, and NB-IoT are compared in terms of these characteristics and discuss their technical differences. By understanding the strengths and limitations of each technology, an informed decision can be made on which one is best suited for a specific IoT project. Table 2.3 summarizes the main specifications of the three LPWAN technologies based on [95–99].

2.5.2.1 Spectrum, Quality of Service and Spectrum Cost

LoRa and Sigfox operate in unlicensed frequency bands below 1 GHz, while NB-IoT and cellular technology use licensed frequency bands in the same range. NB-IoT and cellular technologies, which are based on time-slotted and LTE synchronous protocols, offer higher quality of service (QoS) compared to the asynchronous LoRa and Sigfox. However, the use of unlicensed spectrum can significantly reduce the cost

	Sigfox	**LoRaWAN**	**NB-IoT**
Modulation	BPSK	CSS	QPSK
Frequency	Unlicensed ISM bands (868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia)	Unlicensed ISM bands (868 MHz in Europe, 902 Mhz in North America, and 920 MHz in South America)	Licensed LTE frequency bands
Bandwidth	100 Hz	250 kHz and 125 kHz	200 kHz
Maximum data rate	100 bps	50 kbps	200 kbps
Modulation	DBPSK and GFSK	CSS	Downlink: QPSK+OFMDA Uplink: BPSK/QPSK + SC-FDMA
Bidirectional	Limited / Half-duplex	Yes / Half-duplex	Yes / Half-duplex
Maximum messages/day	140 (UL), 4 (DL)	Unlimited	Unlimited
Maximum payload length	12 bytes (UL), 8 bytes (DL)	243 bytes	1600 bytes
Range	10 km (urban), 40 km (rural)	5 km (urban), 20 km (rural)	1 km (urban), 10 km (rural)
Interference immunity	Very high	Very high	Low
Authentication & encryption	Not supported	Yes (AES 128b)	Yes (LTE encryption)
Adaptive data rate	No	Yes	No
Handover	End-devices do not join a single base station	End-devices do not join a single base station	End-devices join a single base station
Localization	Yes (RSSI)	Yes (TDOA)	No (under specification)
Allow private network	No	Yes	No
Standardization	Sigfox with ETSI	LoRa-Alliance	3GPP
Architecture	Star Network	Star-of-stars topology	Cellular
Spectrum cost	Free	Free	>500 M€ /MHz
Deployment cost	>4000€/base station	>100€/gateway >1000€/base station	>15.000€/base station
End-device cost	<2€	3–5€	>20€
Battery life time 2000 mAH	150 months	105 months	90 months

Table 2.3: Overview of the main technical specifications of LPWAN technologies: Sigfox, LoRa, and NB-IoT.

of implementing LoRa and Sigfox in an IoT application, compared to the licensed NB-IoT and cellular technologies, which can cost a significant amount of money [95].

2.5.2.2 Data Rate, Range and Payload

NB-IoT offers a high data rate of 200 kbps, making it suitable for applications that require high throughput. LoRa has a maximum data rate of 50 kbps, while Sigfox offers a lower rate of 100 bps. Sigfox has a longer transmission range of up to 10 km in urban areas and 40 km in rural areas, it has a smaller payload of only 12 bytes. LoRa has a shorter range of 5 km in urban areas and 20 km in rural areas, but can transmit larger payloads of up to 243 bytes. NB-IoT has the shortest range, reaching up to 1 km in urban areas and 10 km in rural areas, but can transmit larger payloads of up to 1600 bytes.

2.5.2.3 Scalability & Payload length

Sigfox, LoRa, and NB-IoT are all able to support a large number of connected devices, making them suitable for use in IoT applications with increasing numbers and densities of devices. These technologies use various techniques to achieve scalability, such as exploiting diversity in channels, time, and space. However, NB-IoT stands out in terms of scalability, with the ability to connect up to 100,000 end devices per cell, compared to 50,000 per cell for Sigfox and LoRa [100]. NB-IoT also offers the advantage of a larger maximum payload length, allowing the transmission of up to 1600 bytes of data. LoRa has a maximum payload length of 243 bytes, while Sigfox has the smallest payload length of only 12 bytes, which limits its use in applications that require the transmission of large amounts of data.

2.5.2.4 Latency

NB-IoT is a good choice for application with low latency and frequent communication requirements. Sigfox has high latency in communication, while LoRaWAN Class A devices have high latency in downlink communication. However, LoRaWAN Classes B and C are designed to reduce downlink latency. Keep in mind that the appropriate technology for an application will depend on the latency and communication requirements of the IoT network.

In summary, Sigfox, LoRa, and NB-IoT each has their respective advantages in terms of different IoT factors as shown in Figure 2.17. LoRa and LoRaWAN Classes A and B are well-suited for applications that require long battery life and low data rates, such as smart agriculture and intelligent building systems. LoRaWAN Class C is ideal for low latency and low power applications, like smart water systems. On the other hand, NB-IoT technology is best for high data rate, low latency, and guaranteed QoS applications like smart meters and point of sale systems.

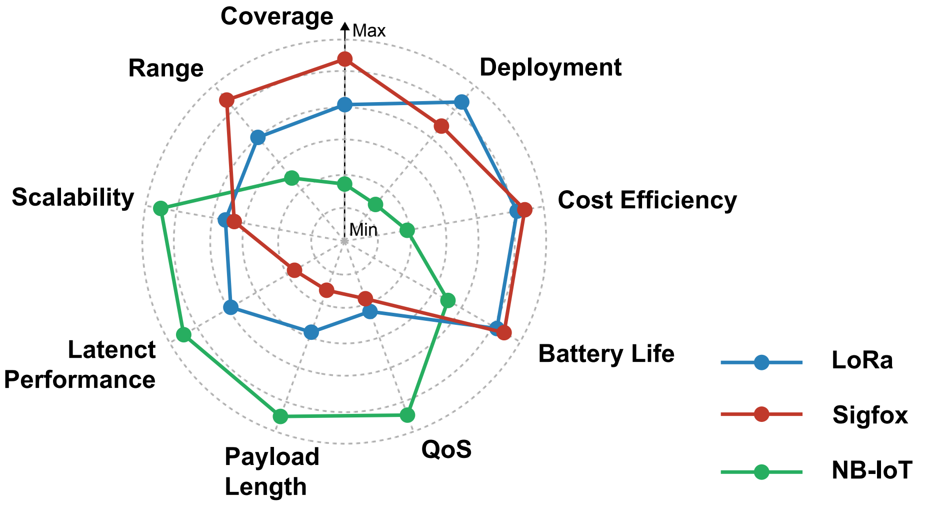


Figure 2.17: Respective advantages of Sigfox, LoRa, and NB-IoT in terms of IoT factors

2.6 LoRa and LoRaWan Overview

LoRa technology comprises two layers: the Physical layer and the MAC layer. As depicted in Figure 2.18, The Physical layer is patented by Semtech [88] and is based on CSS modulation, providing high receiver sensitivity and improved resistance to noise through the use of forward error correction messages [101]. The MAC layer protocol and system architecture, known as LoRaWAN, ensures seamless communication and compatibility between devices. LoRa utilizes unlicensed radio spectrum in the ISM band, providing broad reach and accessibility.

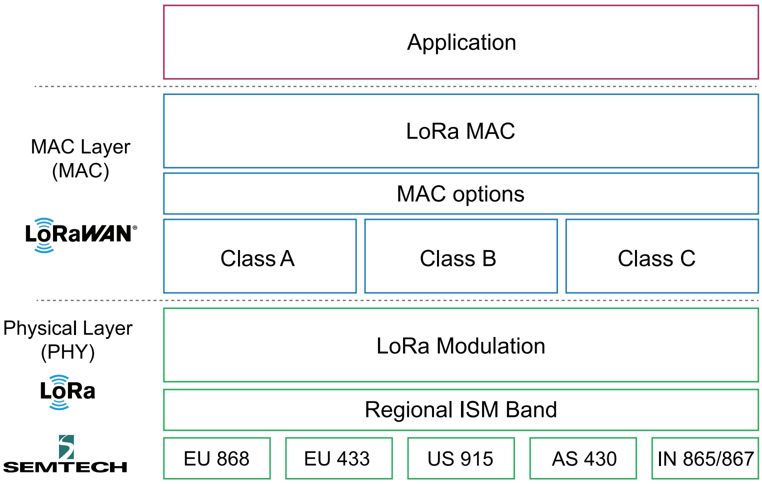


Figure 2.18: LoRa Technology Protocol Stack.

2.6.1 LoRa Physical Layer

In Europe, the LoRa technology utilizes the frequency band of 863-870 MHz and operates in two distinct sub-bands at 868 MHz and 867 MHz. The 868 MHz sub-band comprises three 125 kHz LoRa channels, while the 867 MHz sub-band has five 125 kHz channels. According to regulations in Europe, the LoRaWan duty cycle should not exceed 1% for each sub-band, as specified in the EU regulations [102].

The duty cycle refers to the time interval between successive transmissions on the same channel by a device and can range from 0.1% to 10%. The payload size of each transmission can vary between 2 and 25 octets, and the data rate can reach up to 50 Kbps, depending on the Spreading Factor (SF). The SF, expressed as a base-2 logarithm, represents the number of chips per symbol, where a symbol represents a change in frequency [103]. LoRa uses six different SF values ranging from 7 to 12, with increasing SF resulting in increased receiver sensitivity but decreased bit rate. A relationship between the bit rate, SF, and receiver sensitivity can be found in Table 2.4.

SF	Bit rate [kbps]	Rx sensitivity [dBm]
12	0,25	-137
11	0,44	-135
10	0,98	-133
9	1,7	-130
8	3,1	-129
7	5,4	-124

Table 2.4: Relationship between Spreading Factor (SF), Bit rate and receiver (Rx) sensitivity.

2.6.2 LoRa Modulation Characteristics

The LoRaWAN Regional Parameters document, available from the LoRa Alliance, outlines the specific modulation characteristics for each region. Carrier grade macro gateways, which are used specifically for outdoor applications, can have up to 64 uplink channels of 125 kHz as well as eight 500 kHz uplink and downlink channels [104].

The LoRa physical layer is designed for low data rate, low throughput, and long-range communication. The spreading factor, which determines the processing gain, has a direct impact on the sensitivity and link budget. The higher the spreading factor, the greater the sensitivity and link budget, but the longer the transmission time. LoRa allows for multiple transmissions on the same channel frequency and in the same time-slot through the orthogonality of its spreading factors. Narrower bandwidths result in higher sensitivity at a fixed spreading factor due to reduced bit rates. LoRaWAN utilizes 125 kHz uplink channels and 500 kHz uplink and downlink channels. The Code Rate, set at 4/5 in the LoRaWAN protocol, provides error correction through forward error correction [103].

2.6.3 Data Collisions and Spreading Factor Orthogonality

With LoRa, packets utilizing different spreading factors are orthogonal, meaning they do not interfere with each other and are treated as noise. As a result, packets arriving simultaneously on the same receive channel but with different SF will not collide and can be successfully demodulated by the gateway modem chip. However, packets with the same SF arriving at the same time on the same channel may experience a collision, unless one of the packets is stronger by 6 dB, in which case it will dominate [105].

The capacity of a LoRaWAN network is dependent on its gateway density, and maximizing this capacity requires the use of an adaptive data rate (ADR) mechanism. The main objective of ADR is to conserve the battery power of LoRaWAN end-nodes

[106]. By having end-nodes closest to a gateway transmit with the lowest spreading factor, their transmission time is reduced, extending their battery life. On the other hand, more distant sensors transmit at higher spreading factors to maintain connectivity. A balance must be struck between battery power and range, as a higher spreading factor allows the gateway to connect to devices at greater distances.

2.6.4 LoRa MAC Layer

LoRaWAN is a cloud-based, open protocol developed and maintained by the LoRa Alliance [91] that enables wireless communication between devices using LoRa technology. It's provides the means for communication between LoRa devices and the LoRaWAN receiver gateway. LoRaWAN has a star network architecture, where end-devices can only communicate with the receiver gateway and not with each other. However, multiple gateways can be connected to a central LoRaWAN server and the end-node can send the information to multiple gateways.

The LoRa Alliance is an open, non-profit association that was created to standardize LPWAN technology for IoT applications and machine-to-machine (M2M) communications. The alliance is dedicated to promoting and advancing the use of LoRa wireless technology, which is a proprietary wireless communication technology that enables low-power, wide-area networks with long-range connectivity. The alliance works to standardize the technology, promote its adoption and interoperability, and provide education and support to its members and the wider community. The members of the alliance include companies, universities, and organizations from various industries, including telecommunications, electronics, and IoT.

A LoRaWAN network typically consists of several components, including end devices (sensors or actuators), gateways, and a network server (LNS). The end devices are responsible for collecting data from the physical environment and transmitting it to the gateways. The gateways receive the LoRa-modulated RF messages from the end devices and forward them to the network server, which is connected to the Internet through an IP backbone. The network server performs tasks such as data de-duplication, payload interpretation, and routing of downlink messages to the end devices [107]. The communication between the end devices and gateways is achieved using LoRa technology, while the backhaul of IP traffic from the gateway to the network server can be through Wi-Fi, Ethernet, or cellular connections. Figure 2.19 describes a typical LoRaWAN network implementation from end to end.

2.6.5 LoRa-based End Devices

A LoRaWAN-enabled end device refers to a sensor or actuator that connects wirelessly to a LoRaWAN network through radio gateways using the LoRa radio frequency modulation technology. In most cases, an end device is an autonomous and battery-

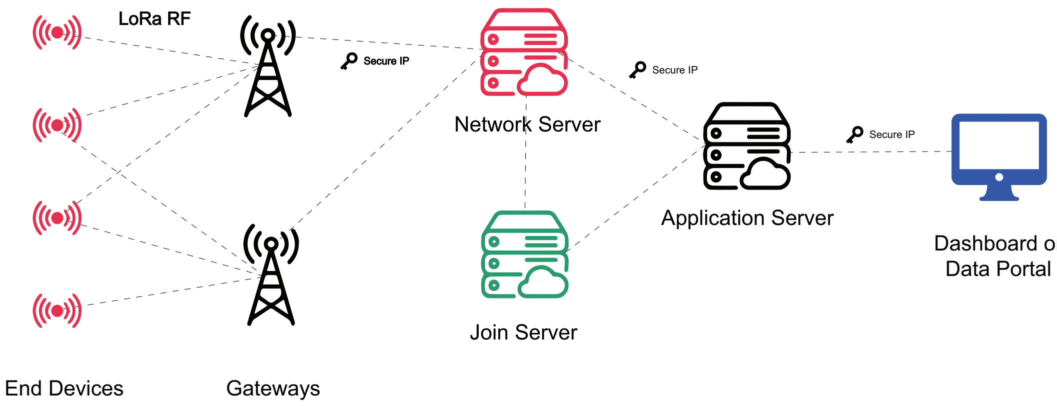


Figure 2.19: Typial LoRaWAN network implementation

powered sensor that converts physical conditions and environmental events into digital data. Some examples of actuators include street lighting systems, wireless locks, water valve shut-off systems, and leak prevention devices. When manufactured, LoRa-based devices are assigned unique identifiers that serve several purposes. These identifiers secure the activation and administration of the device, ensure the safe transmission of packets over private or public networks, and facilitate the delivery of encrypted data to the cloud [98].

2.6.6 LoRaWAN Gateways

The LoRaWAN gateway is designed to receive LoRa modulated radio frequency messages from end devices within its range and forward them to the LoRaWAN network server (LNS). The end devices are not associated with a specific gateway, allowing for greater flexibility and reduced packet error rate. With multiple gateways in the area, it increases the chances of receiving the message and reduces battery consumption for mobile sensors [108]. The gateways only verify the data integrity of each incoming message and if it is incorrect, the message is dropped. If the message is accurate, it is forwarded to the LNS, along with metadata such as the RSSI (Received Signal Strength Indicator) and an optional timestamp.

For LoRaWAN downlinks, the gateway executes transmission requests from the LNS without interpreting the payload. The LNS performs data de-duplication and removes duplicates to ensure efficient communication. The network server selects the gateway with the best RSSI level to transmit downlink messages to ensure that the message reaches the closest gateway to the end device.

In terms of cost and scalability, LoRa provides options for gateway implementation that cater to different deployment objectives. The number of channels in a gateway varies and determines its cost. Gateways with 8, 16, and 64 channels are available. The 8-channel gateways are the most affordable, while 16-channel gateways are a good balance of cost and capability. Both 8- and 16-channel gateways are designed for indoor and outdoor use. For large-scale deployment, such as on cell towers or tall building rooftops, the 64-channel carrier-grade gateway is the best option [109].

2.6.7 Network Server (LNS)

The LoRaWAN Network Server (LNS) serves as the backbone of the entire LoRaWAN network, providing dynamic control over network parameters and ensuring secure end-to-end data transmission with 128-bit AES encryption. It manages the authenticity of all devices on the network, as well as the integrity of every message. However, the network server does not have access to the application data [110]. The LNS is equipped with various features to ensure efficient network management, including:

- Verifying the device addresses
- Authenticating and managing frame counters
- Acknowledging received messages
- Adapting data rates using the ADR protocol
- Responding to MAC layer requests from devices
- Forwarding uplink application payloads to the appropriate application servers
- Queuing downlink payloads from application servers for delivery to any device connected to the network
- Forwarding Join-request and Join-accept messages between devices and the join server.

2.6.8 Application Servers

The application servers act as a mediator between the LNS and the cloud-based applications, forwarding uplink data from the end devices to the applications and vice versa. The application server is responsible for managing the payloads of data that are sent between the end devices and the cloud-based applications. It also performs tasks such as payload decryption, data processing, and message queuing to ensure that the data is properly transmitted and received by the intended recipients. By serving as the intermediary between the end devices and the cloud-based applications, the application server plays a crucial role in enabling the seamless communication and data exchange that is required for effective IoT deployment in a LoRaWAN network [110].

2.6.9 Join Server

The Join Server in a LoRaWAN network is a component responsible for managing the device activation process. This includes verifying the authenticity of new devices attempting to join the network, assigning network keys and session keys to the devices, and registering the devices in the network. In the initial stage of device activation, a new device sends a Join Request to the Join Server. The Join Server verifies the device's identity and if the device is authorized, it generates a unique network key and session key for the device. The Join Server then sends a Join Accept message back to the device with the network key and session key. Once the device has received the Join Accept message, it can securely communicate with the network. The role of the Join Server is important for ensuring the security and privacy of the LoRaWAN network by verifying the identity of new devices and controlling access to the network [111].

The Join Server in LoRaWAN must maintain important information for each connected end-device, including:

- DevEUI (end-device serial unique identifier)
- AppKey (application encryption key)
- NwkKey (network encryption key)
- Application Server identifier
- End-Device Service Profile

2.6.10 Device Commissioning

In order to ensure security, quality of service, billing accuracy, and other important considerations, it is necessary to commission and activate each device on the LoRaWAN network before it can begin operating. The commissioning process securely establishes the necessary parameters and aligns each device with the network, including important information such as device and network identifiers, encryption keys, and server locations.

The LoRaWAN specification provides two methods for activation: Over-the-Air Activation (OTAA) and Activation by Personalization (ABP):

- **OTAA** is a preferred activation method that offers several benefits for device security and flexibility. With OTAA, device manufacturers can autonomously generate essential provisioning parameters, including secure session-long and derived keys, which can be regularly renewed for added security. Additionally, devices equipped with OTAA can store multiple identities, allowing them to dynamically and securely switch between networks and operators throughout their lifetime. Advanced tamper-proof security options are also available to enhance the security of the device [112].

- **ABP** requires pre-provisioning of the device with static network session keys and device addresses. Unlike OTAA, where the device autonomously generates essential provisioning parameters, ABP activation is typically used in cases where the network operator or system integrator has direct physical access to the device and can provision it in a secure manner. The pre-provisioned parameters remain fixed throughout the device's lifetime and are used for secure communication with the network server. ABP activation provides a simple and straightforward approach for commissioning devices, but it lacks the dynamic key exchange and network switching capabilities provided by OTAA [113].

2.6.11 LoRaWan Security

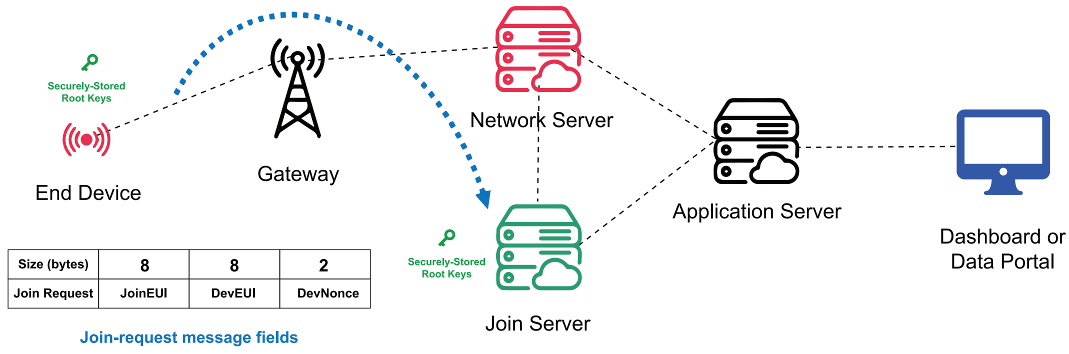
The security of a LoRaWAN network is ensured by the combination of a secure join procedure and message authentication. The join procedure ensures that only authorized devices can join the network, while the message authentication secures the communication between the end device and the application server by providing origin authentication, integrity protection, and end-to-end encryption [114]. These security measures guarantee that the network traffic remains unaltered, only legitimate devices can connect to the network, eavesdropping and capture-replay of network traffic is prevented, and overall confidentiality and privacy are maintained. With this strong foundation, the LoRaWAN security measures offer a high level of security for the IoT network.

2.6.11.1 The Join Procedure

The join procedure in LoRaWAN is the process by which a device connects to a network and is able to communicate with it. The join procedure involves several steps. First, the root keys, unique to each device, are kept secure on the end devices, while the matching keys are kept safe on the join server as shown in Figure 2.20.

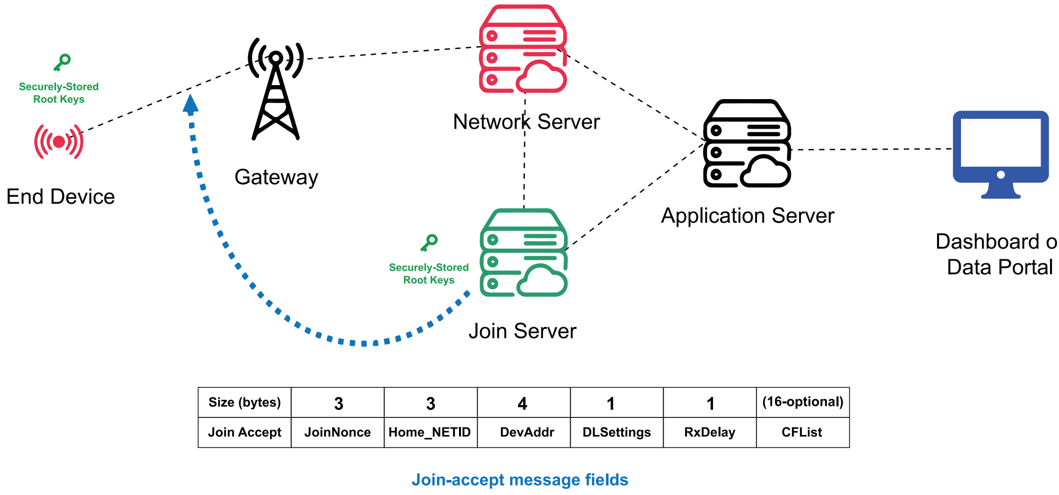
Once the join server has successfully authenticated the device's request to join the network, it sends back a join accept message, as depicted in Figure 2.21.

Following this, the end device generates session keys locally, utilizing the DevEUI, Join EUI, DevNonce, root keys and information present in the join request and join accept messages. Meanwhile, the join server also derives session keys based on the serial IDs, root keys and fields found in the join requests and join accept messages. In the end, the join server distributes the session keys to the network and



Size (bytes)	8	8	2
Join Request	JoinEUI	DevEUI	DevNonce

Figure 2.20: Sending a join request message to the join server



Size (bytes)	3	3	4	1	1	(16-optional)
Join Accept	JoinNonce	Home_NETID	DevAddr	DLSettings	RxDelay	CFList

Figure 2.21: Sending a join accept message to an end device

application servers, as shown in Figure 2.22. The communication between the end device and the network server for control purposes is protected using a 128-bit AES Network Session Key (NwkSKey). The data transmission from the end device to the application server is secured using a 128-bit Application Session Key (AppSKey). This approach guarantees that neither the gateway nor the network server has the capability to access the user data.

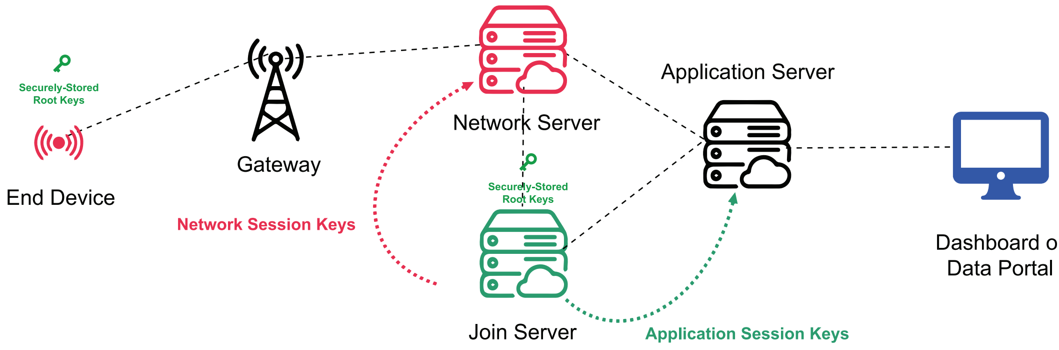


Figure 2.22: Session keys are shared with the network server and the application server

2.6.12 LoRaWan Classes

End devices that are based on LoRa technology can function in one of three modes, which is determined by their device class. All such devices must have the capability to operate in Class A mode. Devices of Class B must be capable of both Class A and Class B modes, while Class C devices must be equipped to work in all three modes. These modes dictate the way the devices communicate with the network [114].

2.6.12.1 Class A Devices

The end-devices in this class support bidirectional communication and have an active/sleep interval duty cycle. The end-device initiates communication by sending an uplink packet and waiting for a potential data reception within the specified intervals. The server remains active during the entire communication process. This class of devices is suitable for applications that require two-way communication and have limited power resources [114].

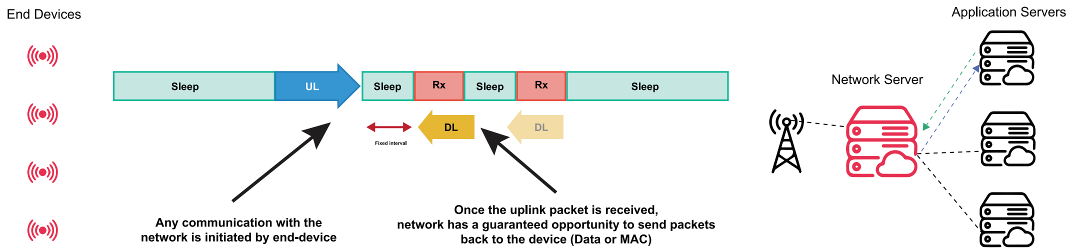

End Devices
Sleep
UL
Sleep
Rx
Sleep
Rx
Sleep
DL
DL
Fixed interval
Any communication with the network is initiated by end-device
Once the uplink packet is received, network has a guaranteed opportunity to send packets back to the device (Data or MAC)
Network Server
Application Servers

Figure 2.23: LoRaWan Class A operation

As described in Figure 2.23, the end device in this scenario primarily stays in an inactive state, which is referred to as sleep mode. When there is a change in the environment being monitored by the device, it wakes up and initiates an uplink transmission to send data about the changed state back to the network (Tx). It then listens for a response from the network, usually for a duration of one second (however, this time frame can be adjusted). If there is no downlink received during the first receive window (Rx1), the device returns to sleep briefly before waking up again to listen for a response (Rx2). If there is still no response during the second Rx window, the device goes back to sleep until it has new data to transmit. The interval between Rx1 and Rx2 is set based on the time elapsed from the end of the uplink transmission [114]. The communication patterns are depicted in Figures 2.24, 2.25 and 2.26.

It is important to note that a device will only attempt to send another uplink message after either of the following conditions have been met: It has received a downlink message during the first receive window (Rx1), or The second receive window (Rx2) after its last transmission has finished.

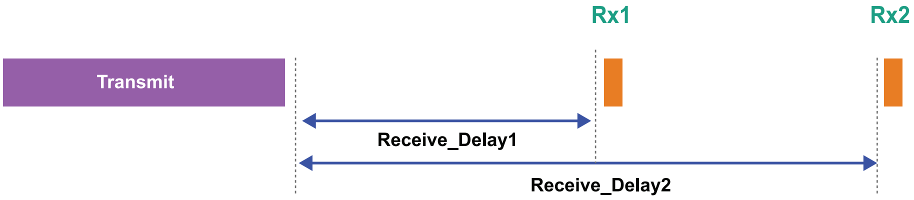


Figure 2.24: LoRaWan Class A operation when nothing is received

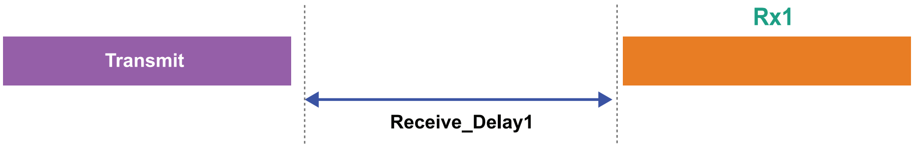


Figure 2.25: LoRaWan Class A operation when a data packet is received in the first receive window

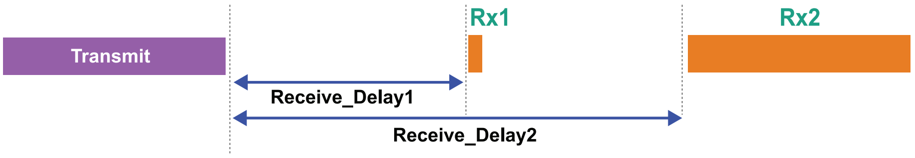


Figure 2.26: LoRaWan Class A operation when a data packet is received in the second receive window

2.6.12.2 Class B Devices

The end-devices are synchronized with the network through periodic beacons. These devices regulate their transmission windows and schedule receiver slots in a periodic manner, with the speed and cycle of data transmission controlled by the server. This allows for more efficient communication and reduces the power consumption of the end-devices. Class B devices are suitable for applications that require more frequent communication and have more stringent latency requirements than Class A devices, but still need to conserve power. Class B mode, which is an enhancement of Class A in LoRaWAN, offers regularly scheduled, fixed time windows for end devices to receive downlinks from the network, making it suitable for both sensor monitoring and actuator applications. All LoRa-based end devices start in Class A mode, however, devices that are manufactured with a Class B stack can be switched to Class B mode by the application layer. In addition to the receive windows that open whenever a Class A-style uplink is sent, Class B end devices provide regularly scheduled receive windows for better communication with the network.

The Class B mode of communication in LoRaWAN requires a process called beaconing. During this process, the network periodically broadcasts time-synchronized beacons via the gateways, as shown in Figure 2.27. End devices must regularly receive one of these network beacons to align their internal timing reference with the network. Beacons are used to derive and synchronize the internal clocks of the end devices with the network. If the device's internal clock is already aligned, it does not have to process every beacon received. In most cases, realigning several times a day has a minimal impact on battery life and is sufficient [114].

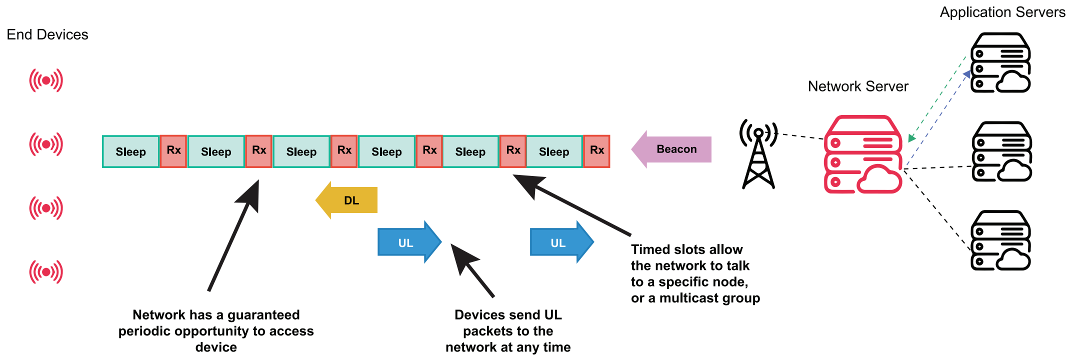

End Devices
Application Servers
Network Server
Sleep
Rx
Beacon
DL
UL
Timed slots allow the network to talk to a specific node, or a multicast group
Network has a guaranteed periodic opportunity to access device
Devices send UL packets to the network at any time

Figure 2.27: LoRaWan Class B beaconing operations

The end devices can open periodic receive windows (ping slots) based on the timing reference from the beacons. The network infrastructure can use any of these ping slots to initiate a downlink communication, as illustrated in Figure 2.28. For a LoRaWAN network to support Class B devices, all the gateways in the network must be equipped with a built-in GPS timing source to ensure exact synchronization with the beacon timing [114].

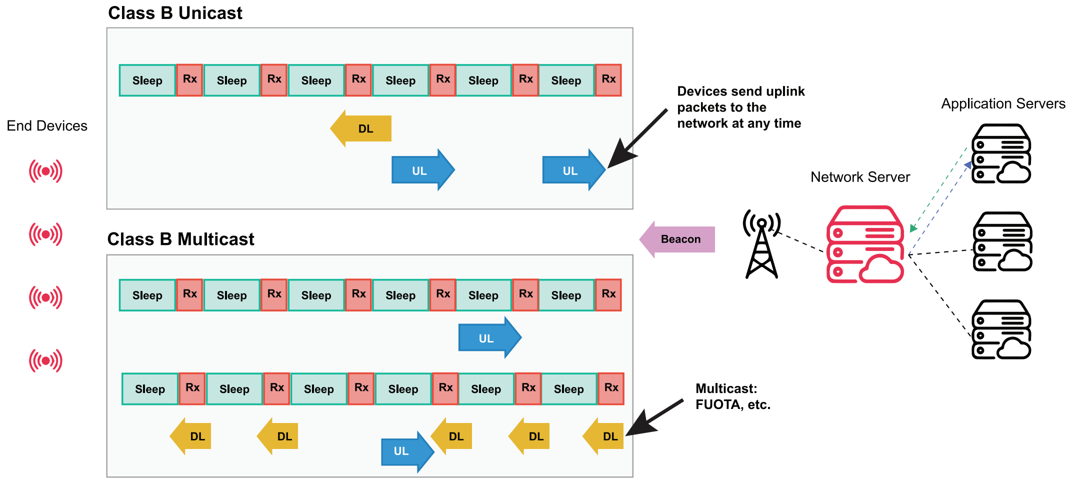


Figure 2.28: LoRaWan Class B ping slots

2.6.12.3 Class C Devices

The end-devices are designed for continuous communication and have almost no sleep time. They can continuously receive data, except when transmitting, which reduces latency and makes them ideal for applications that require low latency and have a constant power source available. These devices have a smaller duty cycle compared to Class A and Class B devices, and are typically used in applications where power consumption is not a concern and real-time communication is critical.

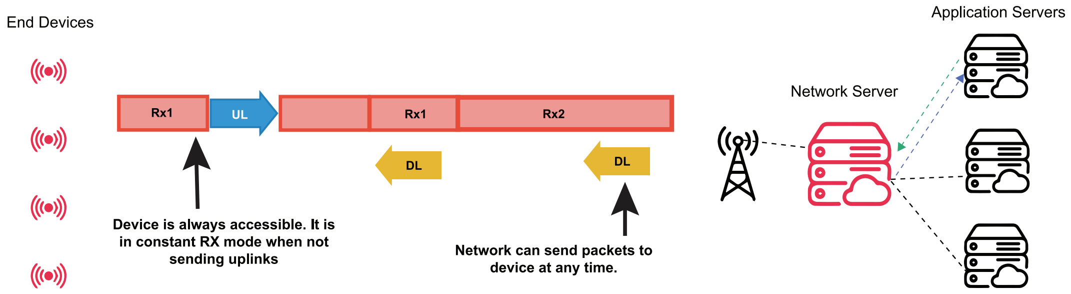

End Devices
Rx1
UL
Rx1
Rx2
DL
DL
Device is always accessible. It is in constant RX mode when not sending uplinks
Network can send packets to device at any time.
Network Server
Application Servers

Figure 2.29: LoRaWan Class C operation

As described in Figure 2.29, Class C devices are always connected and do not rely on battery power, such as street lights and electrical meters. They are constantly listening for downlink messages from the network, except during the times when they are transmitting an uplink. This results in the lowest latency for communication from the network server to the end device. Class C end devices utilize the same two receive windows as Class A devices, however, they do not close the Rx2 window until they initiate the next transmission back to the network [114]. This allows for almost constant reception of downlink messages in the Rx2 window, and a short receive window is also opened between the end of a transmission and the start of the Rx1 receive window .

2.7 IoT Web Monitoring Application

In the IoT ecosystem, web applications represents a critical component that play a vital role in managing and analyzing the data collected from the end-nodes, and allow users to interact with their IoT systems in real-time, providing access from anywhere in the world. These applications enable users to remotely monitor and control IoT devices, making it possible to adjust settings, analyze performance, and receive alerts if something goes wrong. Web applications provide a platform for analyzing the data collected by IoT devices to help users to identify trends, detect anomalies, and make informed decisions by using data visualization tools. These insights can be used to optimize the performance of IoT systems, reduce energy consumption, and improve the overall user experience (UX). Moreover, web applications make it easier to scale IoT systems as they grow. As more devices are added to the network, they can be used to manage the increased volume of data and provide users with a streamlined interface for accessing critical information. This scalability is essential for ensuring that IoT systems can continue to provide value as they expand.

Numerous technologies are available for developers to choose from when building an IoT web applications. JavaScript is a versatile programming language that is widely used for creating dynamic and interactive user interface (UI), with frameworks such as Angular, React, and Vue. Node.js provides a powerful and scalable platform for building web applications, while REST APIs are used for integrating IoT devices with web applications. For back-end development, Hypertext Preprocessor (PHP) is one of the most popular and efficient dynamic scripting languages [115] and it gives high performance using little system resources during the image processing of active web pages [116]. The PHP Laravel framework is a particularly popular choice for building secure and reliable IoT web applications. With its robust features and developer-friendly approach, the Laravel framework provides a valuable asset for building high-performance and scalable applications.

2.7.1 PHP Laravel

Laravel is a free and open-source PHP framework used for developing web applications following the model-view-controller (MVC) architectural pattern. The framework was first released in 2011 and has since gained immense popularity in the PHP developer community due to its simplicity, flexibility, and extensive features. Laravel is built with the principle of "convention over configuration" which means it provides default configurations and conventions for common development tasks, making it easier for developers to get started quickly without having to spend time configuring settings. However, it also provides a lot of flexibility to customize the settings and configurations as per the developer's requirements.

One of the key features of Laravel is its elegant syntax and powerful tools that help developers write clean, reusable, and maintainable code. It includes a range of tools such as Artisan, a command-line interface for performing common tasks, Eloquent object relational mapping (ORM), a powerful and intuitive database query builder, and Blade, a templating engine for building dynamic, data-driven views. Laravel also has a strong focus on security, providing built-in features such as protection against cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. It also provides robust authentication and authorization mechanisms to secure user data and prevent unauthorized access.

In addition, Laravel has a large and active community that provides support, tutorials, and packages to extend the functionality of the framework. This community-driven approach has helped Laravel become one of the most widely used PHP frameworks in the world. Overall, Laravel is a powerful and versatile framework that can be used to develop a wide range of web applications, from small-scale personal projects to large-scale enterprise applications. Its simplicity, flexibility, and extensive features make it a popular choice for PHP developers looking to build robust and scalable web applications.

2.7.1.1 MVC architecture

MVC is a popular software architectural pattern used in the development of user interfaces in computer applications [117]. As described in Figure 2.30, the MVC pattern divides the application into three interconnected components: the model, the view, and the controller.

- **The model** represents the data and the business logic of the application. It interacts with the database, retrieves and stores data, and performs all the necessary calculations and operations required by the application. The model is responsible for maintaining the state of the application and ensuring data integrity.
- **The view** is responsible for displaying the data to the user. It presents the data in a user-friendly and interactive manner, making it easy for the user to interact with the application. The view can be a graphical user interface, a web page, or any other type of user interface.
- **The controller** acts as an intermediary between the model and the view. It receives user inputs and sends them to the model for processing. It then receives the processed data from the model and sends it to the view for display. The controller is responsible for maintaining the flow of data and ensuring that the data is correctly processed and displayed to the user.

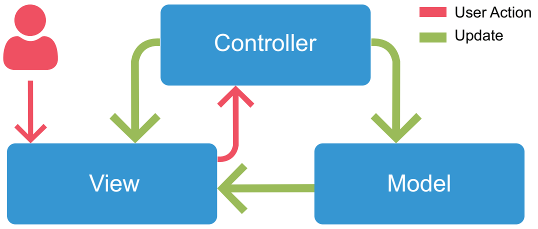


Figure 2.30: Outline view of the MVC architecture pattern

The MVC pattern has many benefits, including separation of concerns, code reusability, and testability. Separating the application into distinct components makes it easier to manage and maintain the code, as each component is responsible for a specific set of tasks. This makes it easier to add new features or modify existing ones without affecting the other components. MVC pattern is a widely used architectural pattern in software development that separates the application into three components: the model, the view, and the controller. The model handles the data and the business logic, the view displays the data to the user, and the controller acts as an intermediary between the model and the view, managing the flow of data between them.

2.7.1.2 Laravel Security

Laravel is a secure web application framework that includes several built-in security features to protect applications from common security threats. Here are some of the key security features of Laravel:

1. CSRF Protection: Laravel includes built-in CSRF protection that generates a token for each user session to prevent malicious requests from being executed by unauthorized users [118].

2. Secure Authentication: Laravel offers a built-in authentication system that uses secure hashed passwords, as well as two-factor authentication and email verification to enhance security.

3. Protection from Structured Query Language (SQL) Injection Attacks: Laravel's database query builder uses prepared statements to prevent SQL injection attacks.

4. Encrypted Cookies: Laravel encrypts session and authentication cookies to prevent unauthorized access and tampering.

5. Role-Based Access Control: Laravel allows developers to easily implement role-based access control, which allows access to be restricted based on the user's role and permissions.

6. Form Input Validation: Laravel includes a built-in form input validation feature that automatically validates user input to prevent malicious input from being executed.

7. Protection from XSS Attacks: Laravel's Blade template engine automatically escapes user input to prevent XSS attacks [118].

8. Password Hashing: Laravel uses the bcrypt algorithm to securely hash passwords, making them difficult to crack.

9. Encryption and Decryption: Laravel includes a built-in encryption and decryption feature, which can be used to encrypt sensitive data such as credit card information or personal information.

Generally, Laravel provides a comprehensive set of security features that help to protect web applications from common security threats. Developers can use these features to enhance the security of their applications and minimize the risk of data breaches or other security incidents.

2.7.2 Development of the Web Application

Developing a web application is a complex process that requires careful planning and execution. The process involves a series of steps, each of which is essential for the successful development of a web application. These steps include setting up the development environment, designing the database schema, building the user interface, creating the database migration files, seeding the database, testing the application, and deploying it to a production server. In the context of this thesis, these steps were followed to develop a range of different IoT web applications, each with its unique set of requirements and challenges. By following a structured approach to development and incorporating industry best practices, the resulting applications were robust, scalable, and secure, meeting the needs of their respective users.

2.7.2.1 Setting up the development environment:

The first step is to set up the development environment by installing and configuring the required software. A virtual private server (VPS) is a powerful tool that allows for the creation of a dedicated instance of an operating system with superuser-level access. With this level of control, it is possible to install almost any software required for a given project and build applications within that OS. A VPS is often functionally equivalent to a dedicated physical server, making it an attractive option for software developers. Thus, to host the web applications, *DigitalOcean* [119] was used. It is a cloud computing vendor that offers infrastructure as a service platform for software developers. One of the benefits of *DigitalOcean* is that developers can easily resize their droplets after creation, allowing for greater flexibility and efficiency in virtualization.

After creating the droplet, the next step was installing the LAMP stack, which is a group of open-source software (Linux, Apache, MySQL, PHP) typically installed together to enable a server to host dynamic websites and web apps. The lowest-level layer is the Linux operating system. The Apache web server is responsible for delivering web pages to users and is stable and mission-critical capable, running more than 65 percent of all web sites on the internet. PHP sits inside Apache and its installation is mandatory to use the Laravel framework. MySQL is a capable database suitable for running large and complex sites, and all the data, products, accounts, and other types of information in the web application reside in this database in a format that can be easily queried with the SQL language. MySQL database that gives high performance for small data and simple queries [120]. Additionally, it is fast, reliable and it provides strong data protection [121].

2.7.2.2 Designing the Database Schema:

After the development environment is established, the subsequent step is to plan the database schema. This process encompasses outlining the tables, columns, and connections between them, along with specifying any restrictions or rules for validation. Each web application is unique and has different requirements, which means that the database used for each application will also be different. A database serves as the foundation for storing and managing data within a web application, and the type of data and the way in which it is accessed and manipulated will vary depending on the application's specific needs. For example, an e-commerce application may require a database capable of handling large amounts of data related to products, orders, and customer information, while a social media platform may require a database optimized for quickly retrieving and displaying user-generated content. In addition to the type of data being stored, the scalability, security, and performance requirements of the application will also influence the choice of database. Therefore, selecting the right database for a web application is a critical decision that can impact the application's functionality, performance, and ultimately, its success.

Designing a database schema involves several steps and tools. The first step is to identify the entities, attributes, and relationships that will be represented in the database. This can be done by analyzing the requirements of the application and the domain it belongs to. The next step is to create an Entity-Relationship (ER) model, which is a graphical representation of the entities and their relationships. This model can be created using tools such as ERDPlus, Lucidchart, or Visual Paradigm [122–124]. Once the ER model is complete, it is transformed into a database schema. This involves defining the tables, columns, and relationships between them, as well as defining any constraints or validation rules. This can be done using tools such as MySQL Workbench or phpMyAdmin [125, 126]. It's important to ensure the schema is optimized for performance, scalability, and security. Regularly reviewing and refining the schema is also necessary to ensure it remains effective and efficient over time.

2.7.2.3 Creating the Laravel application:

After designing the database schema, the next step is to create the Laravel application. This involves setting up the routes, controllers, models, and views that will be used to create a functional and user-friendly application:

1. **Routes**: We define the routes with the associated controller of each, theses

routes will be responsible for directing users to specific pages or functionalities within the application.

2. **Controllers**: After defining the routes, we create the controllers that will handle the business logic of the application. Controllers are responsible for receiving user input, processing data, and rendering views. A controller is required for each route in the application and define the methods that will handle each specific request.

3. **Models**: Models are responsible for communicating with the database and retrieving or modifying data as required. It is required the creation of model for each data entity in the application and define the relationships between them.

4. **Views**: Views are responsible for presenting data to the user in a readable and visually appealing format. Each page require the creation of view in the application. These views represents the user interface.

2.7.2.4 Building the user interface:

The next step is to build the user interface using Bootstrap [127]. This involves designing and coding the HTML, CSS, and JavaScript that will be used to create the user interface. Bootstrap is a widely used front-end framework that provides developers with a collection of pre-built CSS and JavaScript components to create responsive and visually attractive web pages. Laravel enables developers to integrate Bootstrap into their projects and make use of its components.

When using Laravel's blade templating engine in combination with the Bootstrap framework, it becomes easier to create reusable UI components that can be used throughout the application. The first step to using Bootstrap in Laravel blades involves installing Bootstrap and its dependencies via a package manager like *npm* or *yarn* [128]. Once this is done, the necessary CSS and JavaScript files can be included in the blade template by referencing them in the head and footer sections of the layout file. By integrating Laravel's powerful backend capabilities with Bootstrap's front-end framework, a robust and visually appealing web applications can be created, providing an excellent user experience. Whether developing a small web app or a complex enterprise solution, Bootstrap and Laravel blades can help create the desired look and feel.

2.7.2.5 Creating the database migration files:

After building the user interface, the next step is to create the database migration files. This involves using Laravel's migration feature to create the database tables and columns that were defined in the database schema.

2.7.2.6 Testing the application:

After the application has been built, the next step is to test it to ensure that it is working correctly. This involves testing the user interface, as well as the database functionality and any other features that were added to the application.

2.7.2.7 Deployment:

The final step is to deploy the application to the production server and link a domain name to this server. Linking a domain name to a server involves adding a Domain Name System (DNS) record that maps the domain name to the server's IP address. This process enables users to access the website by typing in the domain name, which resolves to the server's IP address, allowing the server to respond with the content associated with that domain name. Figure 2.31 shows the general architecture of a Laravel application.

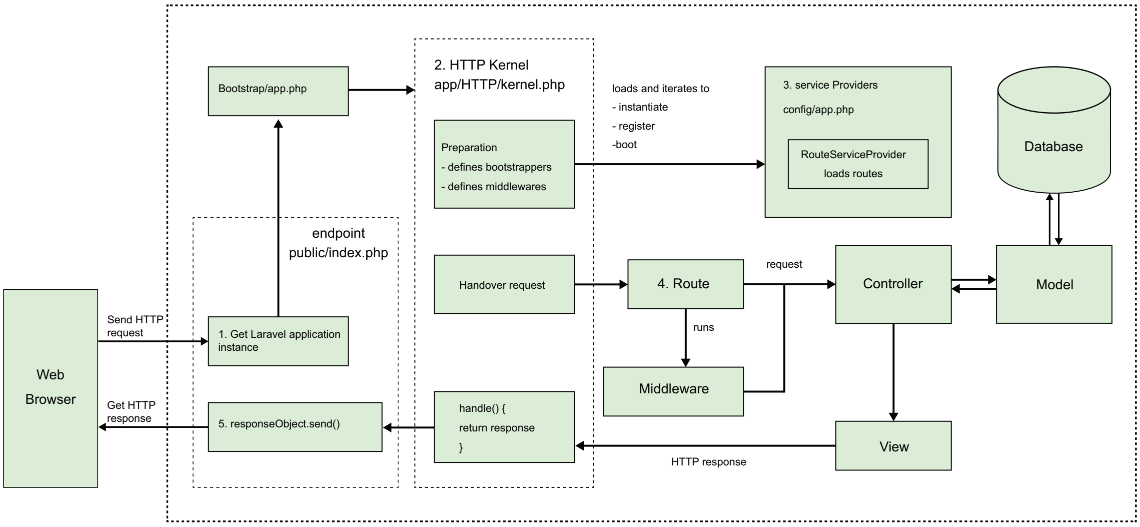


Figure 2.31: Laravel architecture showing the process of sending and receiving a request from the end users

The process from sending a request to receiving the response typically involves the following steps:

1. The user sends a request to the server via their web browser or other HTTP client.
2. The server receives the request and passes it to the Laravel router, which determines which controller and method should handle the request based on the URL and HTTP method.

3. The controller method receives the request and any data that was submitted with it. It may perform some validation or processing on the data before passing it to the appropriate service or model to perform the necessary business logic.

4. The service or model performs the necessary business logic, which may involve accessing a database, interacting with external APIs, or performing some other task.

5. The service or model returns the results of the business logic back to the controller.

6. The controller takes the results returned by the service or model and prepares a response to send back to the client. This may involve rendering a view, returning a JSON response, or redirecting the user to a different page.

7. The server sends the response back to the client via HTTP.

8. The client receives the response and displays it to the user in their web browser or other HTTP client.

Throughout this process, Laravel provides a number of features and tools to make it easier to build robust, secure, and efficient web applications, including middleware for handling authentication and other common tasks, routing for mapping uniform resource locator (URLs) to controller methods, and views for rendering HTML templates.

2.8 Blockchain technology: Technical overview

The concept of a blockchain can be traced back to the early 1990s, but the first successful implementation of a blockchain was the Bitcoin blockchain, which was created by "Satoshi Nakamoto" and introduced to the world in the Bitcoin whitepaper published in 2008 [129]. This enabled the creation of a system that did not require third-party trust. Along with the blockchain, Nakamoto also introduced Bitcoin (BTC) as the native cryptocurrency for the network. The Bitcoin blockchain is a decentralized, distributed ledger that allows for the secure and transparent transfer of value (BTC) without the need for a third-party intermediary. It was the first time that such a system had been created and it opened up a world of possibilities for the use of blockchain technology.

Decentralized architecture has received ample acceptance in the past few years because of its need in many fields [130, 131]. It is also of utility for IoT to solve their open problems, such as, security.

2.8.1 Definitions of Blockchain

A blockchain is a digital, decentralized, distributed ledger that records transactions on multiple computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. This allows for a secure and transparent record of transactions. Each block in a blockchain contains a list of transactions, and once a block is added to the chain it is very difficult to alter the information contained within it [132]. In a blockchain, a block contains several pieces of information, including:

- A unique identifier, called a "block hash," that distinguishes it from other blocks in the chain.
- A timestamp that records when the block was created.
- A set of transactions or data that are being added to the blockchain.
- A reference to the previous block in the chain, creating a link between the blocks.
- A nonce, which is a random number used in the process of mining to solve the cryptographic puzzle and add the block to the blockchain.

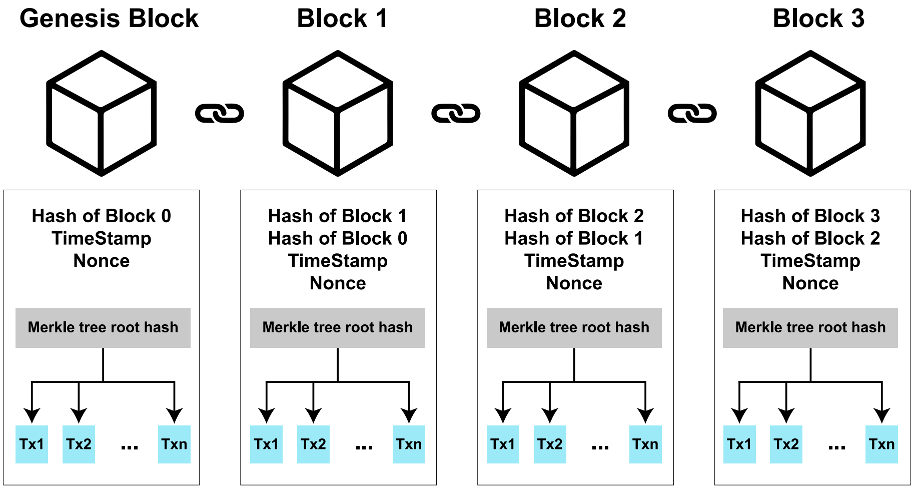


Figure 2.32: Blockchain structure showing the genesis block and the rest of the blocks. Each block contains a nonce, timestamp, a hash and the hash of the previous block.

Figure 2.32 shows the structure of the blockchain, these blocks are linked together in a chronological order, forming a chain of blocks, hence the name "blockchain." The first block of a blockchain is called Genesis block. It is a special block that is created when a new blockchain is launched, and it serves as the foundation for all subsequent blocks in the chain. The genesis block typically contains a message or a block of data that is chosen by the creator of the blockchain. This message is intended to convey the purpose or mission of the blockchain to those who will use it. In general, the genesis block is an important part of a blockchain because it marks the beginning of the chain and serves as the foundation for all subsequent blocks which are linked to it through the cryptographic hash of the previous block [133].

The decentralized nature of a blockchain makes it resistant to tampering and censorship, as there is no single point of control. The use of blockchain technology is not limited to just financial transactions, and it has the potential to be applied to a wide range of applications beyond crypto-currencies. Blockchain allows for the completion of payments without the need for banks or intermediaries, making it useful for various financial services such as digital asset management, remittances, and online payments [134]. The blockchain has already been integrated into a variety of sectors, including, healthcare, government, manufacturing, and distribution [135]. It has the potential to revolutionize industries including supply chain management, the sale of digital media such as art, travel and tourism, and distributed computing.

Other potential applications of blockchain include distributed energy generation and distribution, crowdfunding, electronic voting, identity management, and public record keeping [136].

2.8.2 Types of Blockchains

There are various types of blockchain networks, including public, private and hybrid. Each with its own unique characteristics and uses. These different types of blockchain can be customized to meet the specific needs and requirements of different organizations and use cases.

2.8.2.1 Public Blockchain

Public blockchain is a type of decentralized ledger that is open to anyone and allows for the conduct of transactions. It is a non-restrictive system in which every participant has a copy of the ledger and can access it with an internet connection. Users of a public blockchain have access to both historical and current records and have the ability to perform mining operations, which are complex computations used to verify transactions and add them to the ledger. One of the key features of a public blockchain is that once a record or transaction has been added to the network, it cannot be altered, and the source code is often open, allowing anyone to review the transactions and identify any issues or potential improvements.

One of the primary uses of public blockchain is for the mining and exchange of cryptocurrencies, with Bitcoin and Ethereum being the most well-known examples. While public blockchains are generally considered secure, it is important for users to strictly follow security protocols and practices to ensure the integrity of their transactions and protect against potential threats [133]. By adhering to proper security measures, users of public blockchain can help to further enhance the security of these networks and ensure that they are used effectively and efficiently.

However, public blockchain has some disadvantages that can impact its performance and scalability. One of these is a low number of transactions per second (TPS), due to the large size of the network and the time it takes for transactions to be verified and proof-of-work to be completed. This can also lead to scalability issues, as the larger the network becomes, the slower the processing and completion of transactions will be [137]. In addition, most of public blockchain relies on a proof-of-work (PoW) system, which can be expensive and consume a large amount of energy. As a result, there is a need for the development of more energy-efficient consensus methods to address these issues and improve the effectiveness of public blockchain technology.

2.8.2.2 Private Blockchain

Private blockchain is a type of decentralized ledger system that is only accessible within a restricted network or is controlled by a single entity. It operates in a similar way to a public blockchain, with a peer-to-peer connection and decentralized structure, but it is typically smaller in scale and is only available to a select group of users within a specific organization or firm. It is typically used within an enterprise or organization, and access to the network is restricted to members. In a private blockchain, the level of security, authorization, and access is controlled by the managing organization, making it a more secure and private alternative to a public blockchain network [138]. Private blockchain is often used for applications such as voting systems, supply chain management, digital identity verification, and asset ownership tracking, among others.

Private blockchain has several advantages over public blockchain, including increased speed and scalability. One of the primary benefits of private blockchain is the faster transaction speed, as the smaller network size and fewer number of nodes result in a shorter verification time for transactions. Private blockchain is also highly scalable, as it allows companies to easily adjust the size of their network to meet their specific needs and requirements [139]. Nevertheless, private blockchains have some disadvantages that can impact their effectiveness and security. One of the main challenges of private blockchains is building trust among a smaller number of participants, as there are fewer nodes on the network compared to a public blockchain, which makes it more vulnerable to security breaches. Additionally, private blockchain is centralized, as it relies on a central Identity and Access Management (IAM) system to function [140]. This system provides full administrative and monitoring capabilities, but it also means that the network is not fully decentralized like a public blockchain.

2.8.2.3 Hybrid Blockchain

Hybrid blockchain is a type of decentralized ledger system that combines the characteristics of both private and public blockchain networks as illustrated in Figure 2.33. It allows organizations to create a private, permission-based network that is connected to a public, permissionless network, giving them the ability to choose which data is made public and who has access to it. The hybrid system is flexible, allowing users to easily connect a private blockchain to multiple public blockchains, and transactions on a private network can be verified within that network or released to a public blockchain for additional security and transparency [141].

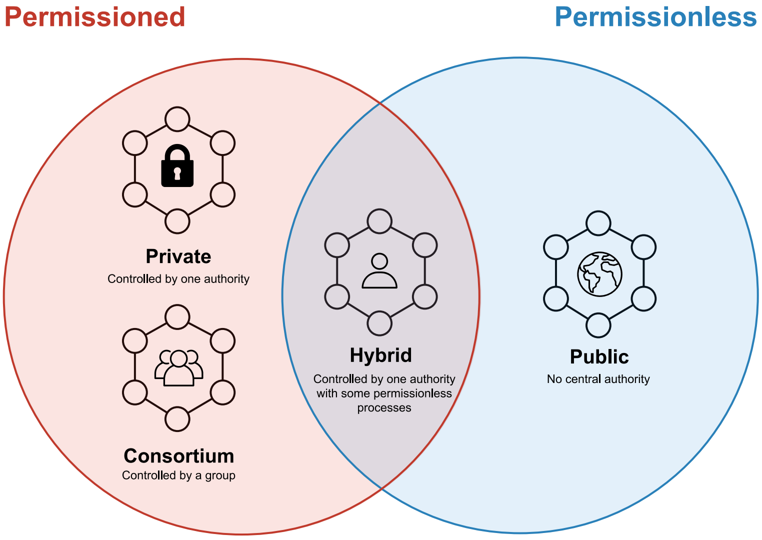


Figure 2.33: Hybrid Blockchain permissions

Hybrid blockchain technology has a number of potential use cases in various industries. In the real estate industry, it can be utilized to manage and make public important information related to properties. Retail businesses can benefit from the streamlining of processes through the use of a hybrid network. Additionally, hybrid blockchains can be particularly useful in heavily regulated markets such as the banking sector, as they offer a balance of security and flexibility. Hybrid blockchain also offers cost-effective transactions that are fast and scale well, as it allows for third-party contact while still preserving privacy [142]. However, one of the main challenges of hybrid blockchain is a lack of transparency, as it allows for the hiding of certain information. This can make it less transparent compared to a public blockchain network. Additionally, upgrading a hybrid blockchain network can be difficult, and users may not have an incentive to participate in or contribute to the network, which can limit its adoption and growth in cases where transparency and participation are important considerations.

2.8.3 Security and Distributed Consensus

At the heart of blockchain systems are distributed consensus protocols, which enable decentralization by ensuring that all participants agree on a single transaction ledger without the need for a central authority. These protocols involve message passing and decision-making at each node, and the specific design choices made in the protocol can greatly impact the performance of the blockchain system in terms of transaction capacity, scalability, and fault tolerance [143]. A consensus algorithm is a mechanism used in computer science to ensure that distributed systems or processes agree on a single value or course of action. The consensus problem, which consensus algorithms aim to solve, is especially important in distributed computing systems and blockchain networks used in cryptocurrency [144]. By enabling multiple nodes to reach a consensus on the data or actions within a network, these algorithms ensure the integrity and consistency of the system.

Consensus mechanisms require a minimum percentage of responding nodes to achieve consensus on a data value or network state. For example, an algorithm may require at least 51% of nodes to agree in order to reach consensus [145]. This approach allows for the achievement of consensus with minimal resources, even when other resources are unavailable or faulty. It also helps to maintain the integrity of decisions made by the agreeing nodes within the fault-tolerant system. Blockchain networks rely on consensus algorithms to achieve agreement among the various distributed nodes. These mechanisms secure the network and prevent unauthorized users from submitting invalid transactions. They also enable the network to reach agreement on its state even when no single node has complete control [146]. Currently, the most used consensus mechanisms are proof of work (PoW) and proof of stake (PoS).

2.8.3.1 Proof of Work (PoW)

PoW mechanism is a method used by nodes in a blockchain network to reach consensus on the state of the blockchain. It was first introduced in 1993 and was later adopted by the Bitcoin blockchain in 2008. In PoW, nodes, also known as miners or validators, compete to solve complex mathematical puzzles in order to earn the right to add new transactions to the blockchain. This is done by taking data from a block header, applying a cryptographic hash function to it, and making small changes to the input data by adding a nonce [147]. When a node finds a solution that leads to consensus, it is rewarded in cryptocurrency. While PoW is effective in maintaining network security and is resistant to Denial-of-service attack (DDoS) attacks [148], it is also relatively inefficient due to the high amount of computational power required for the multiple iterations involved. Despite this, it remains a popular choice for blockchains due to its proven track record of security and reliability. Figure 2.34 illustrate the PoW algorithm.

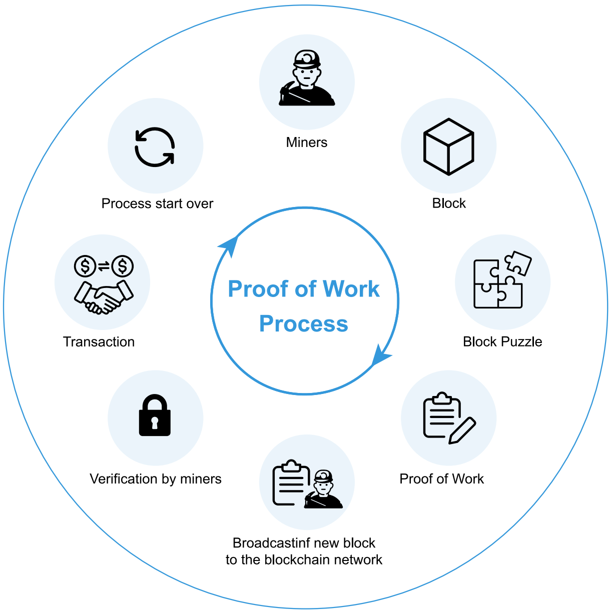


Figure 2.34: Proof of Work (PoW) consensus mechanism process.

2.8.3.2 Proof of Stake (PoS)

PoS is a type of consensus mechanism used by some blockchain networks to achieve distributed consensus. PoS is an alternative to PoW that is designed to be more energy efficient. In PoS, as described in Figure 2.35, instead of using specialized equipment to perform resource-intensive calculations to mine for new blocks, as is the case in PoW, nodes can earn the right to create new blocks by holding and staking a certain amount of the cryptocurrency.

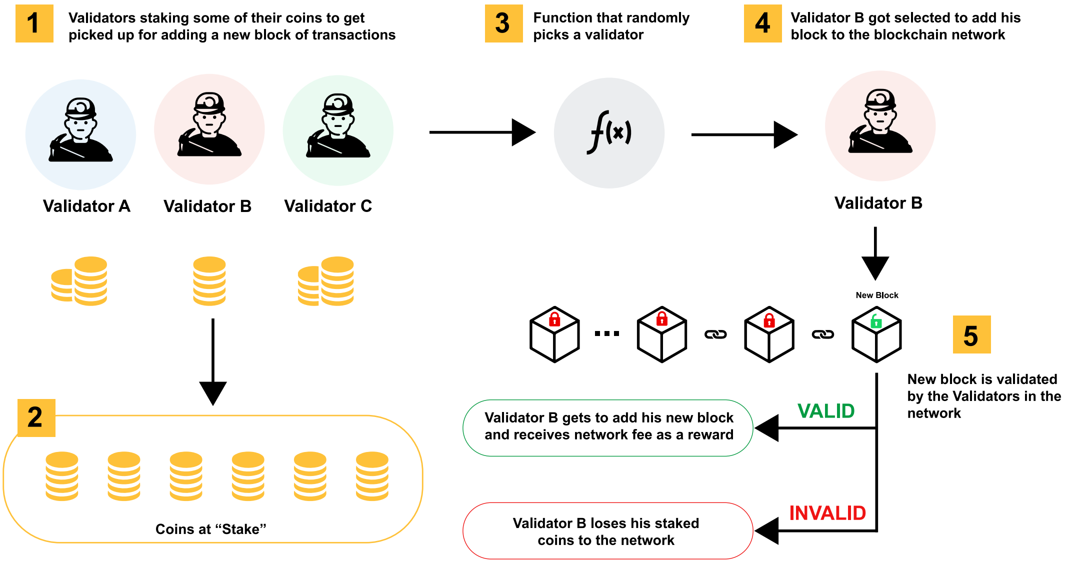

1
Validators staking some of their coins to get picked up for adding a new block of transactions
3
Function that randomly picks a validator
4
Validator B got selected to add his block to the blockchain network
Validator A
Validator B
Validator C
f(x)
Validator B
New Block
5
New block is validated by the Validators in the network
2
Coins at "Stake"
VALID
Validator B gets to add his new block and receives network fee as a reward
INVALID
Validator B loses his staked coins to the network

Figure 2.35: Proof of Stake consensus algorithm

This process of staking one's cryptocurrency to participate in the block creation process can be thought of as buying chances of block creation in the blockchain. PoS aims to reduce the power consumption associated with PoW mining, as it does not require the same level of computational resources. Instead, nodes are selected to create new blocks based on the amount of cryptocurrency they hold and are willing to stake, which can provide a financial incentive for nodes to hold and maintain their stake in the network [149, 150]. One advantage of PoS over PoW is that it is generally more energy efficient, as it does not require miners to perform resource-intensive calculations in order to create new blocks. Additionally, because the probability of creating a new block is proportional to the amount of coins held by a node, there is a financial incentive for node operators to hold and maintain their stake in the network, which can contribute to the overall security of the blockchain.

2.9 Blockchain and IoT Integration

Blockchain technology holds an immense potential in revolutionizing the IoT. By incorporating blockchain, IoT can be enhanced with a trusted sharing service that ensures reliable and traceable information. This means that data sources can be identified at any time and data remains immutable, significantly increasing its security. In particular, this integration of blockchain technology would be a game-changer in situations where IoT information needs to be securely shared among multiple participants. Moreover, the integration of blockchain and IoT has enormous potential to enhance the functionality and development of current IoT technologies. However, there are still many research challenges and open issues that need to be addressed in order to seamlessly integrate these two technologies. This research topic is still in its early stages.

The integration of blockchain with IoT can provide several improvements, including:

- **Decentralization and scalability:** The shift from a centralized architecture to a peer-to-peer distributed one can remove central points of failure and bottlenecks [151]. This can help prevent scenarios where a few powerful companies control the processing and storage of the information of a large number of people. Decentralized architecture can also improve fault tolerance IoT scalability.

- **Identity:** Participants in the system can identify every single device using a common blockchain system. Data fed into the system is immutable and uniquely identifies the actual data provided by a device. Additionally, blockchain can provide trusted distributed authentication and authorization of devices for IoT applications [152].

- **Autonomy:** Blockchain technology can empower next-generation application features, making it possible to develop smart autonomous assets and hardware as a service. With blockchain, devices can interact with each other without the involvement of any servers [153, 154]. IoT applications can benefit from this functionality to provide device-agnostic and decoupled applications.

- **Security:** Information and communications can be secured if they are stored as transactions of the blockchain. Blockchain can treat device message exchanges as transactions validated by smart contracts, thus securing communications between devices. Current secure standard protocols used in the IoT can also be optimized with the application of blockchain [155].

- **Reliability:** IoT information can remain immutable and distributed over time in blockchain. Participants in the system can verify the authenticity of the data and have the certainty that it has not been tampered with. Additionally, the technology enables sensor data traceability and accountability. Reliability is a key aspect of blockchain that can be beneficial for the IoT [156].

- **Market of services:** Blockchain can accelerate the creation of an IoT ecosystem of services and data marketplaces where transactions between peers are possible without authorities. Microservices can be easily deployed, and micro-payments can be made safely in a trustless environment [157–159]. This can improve IoT interconnection and the access of IoT data in blockchain.

- **Secure code deployment:** Taking advantage of blockchain secure-immutable storage, code can be safely and securely pushed into devices. Manufacturers can track states and updates with the highest confidence. IoT middlewares can use this functionality to securely update IoT devices [151, 160].

The integration of blockchain and IoT has the potential to enhance security, reliability, autonomy, and scalability of IoT technologies. Further research and development are necessary to address the challenges and open issues in integrating these two technologies seamlessly. However, the potential benefits of this integration are enormous and can revolutionize the IoT industry. The most important Blockchain nodes include the following types.

- Mining node: special nodes trying to add a new block of transactions to the blockchain and run the consensus algorithms to transmit information to all the nodes. This process in cryptocurrency generates a financial reward to the miners. [129, 161].

- Full node: these nodes download the entire blockchain and verify the integrity of all transactions continuously, which makes the infrastructure trustful and decentralized.

- Lightweight node: these nodes download the block headers that contain the hashes of the transactions. They require minimal storage and computing processors to interact with the blockchain, with minimal storage and computing requirements.

The integration of IoT devices to a blockchain infrastructure can be done in many different ways, depending on power requirements and the capabilities of the end nodes and gateways. The most common method is to use gateways as full nodes that route the data to the network and verify the integrity at the same time. The end devices act as lightweight nodes that interact with the network without any storage or computational requirements. This method connects the IoT network directly with the blockchain network in order to store the collected data.

In the literature, the Ethereum blockchain is mostly integrated with IoT networks such as the proposed systems in [162] and [163]. Ethereum extended the scripting capabilities of transactions to have a fully programming language to create a programming environment. Ethereum is a global blockchain-based decentralized platform allowing the users to deploy decentralized applications in the form of "Smart Contracts" [164]. The difference between a normal contract and the Ethereum smart contract is described in Figure 2.36.

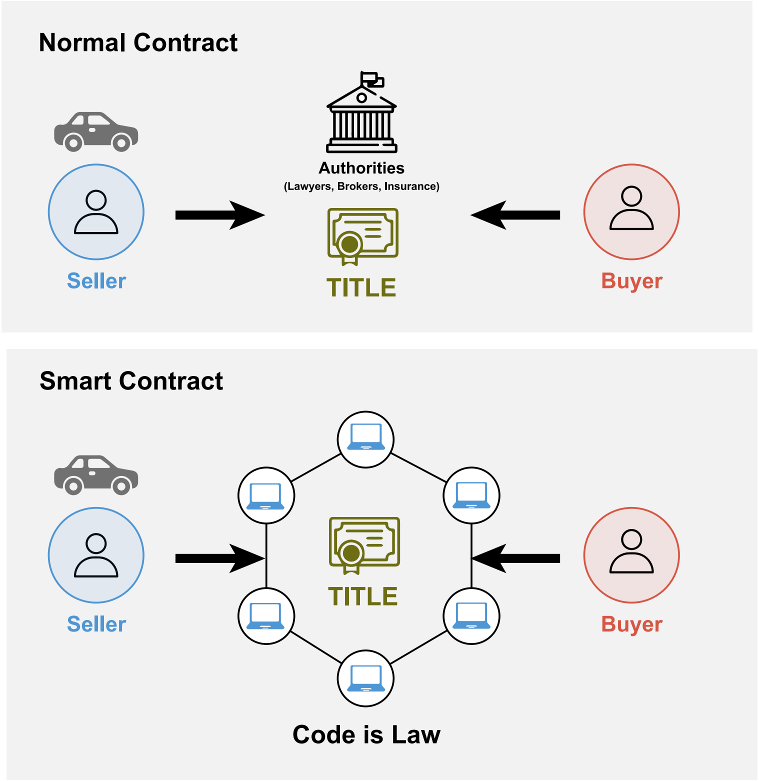


Figure 2.36: Smart Contract are associated with blockchain technology, the intervention of third parties such as lawyers and brokers is not required.

A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist on the blockchain network. It is a set of pre-defined rules that are enforced automatically, without the need for intermediaries. Smart contracts allow for the automation of a wide range of processes, including the transfer of assets, verification of identity, and the execution of agreements. Smart contracts have the potential to revolutionize the way that contracts are created and enforced. They can be used to automate a wide range of processes and reduce the need for intermediaries, which can save time and money. They also offer increased security and transparency, as the terms of the contract are recorded on the blockchain and are immutable. Ethereum Virtual Machine (EVM) is used to run smart contracts on Ethereum blockchain. Smart contracts are programmed with Solidity programming language and compiled by the EVM [165]. This contracts are self executed, immutable and distributed.

Ethereum uses the PoW consensus mechanism, in order to execute the smart contracts, payment is required for transactions that will apply changes in the blockchain as the costs effort for miners to incorporate the transactions. The digital currency used in Ethereum is Ether, each transaction consumes a certain amount of gas, which is priced in Gwei and paid in Ether through a crypto-wallet like MetaMask [166] where 10^8 Gwei = 1 Ether [164]. The gas price varies depending on the number of transactions executed in the Ethereum blockchain. The number of transactions that can be executed in the Ethereum blockchain is only 15 transactions per second, which makes the gas prices too high, and sometimes, during rush hours, the gas prices can be even higher than the transaction amount, because miners will process firstly those who pay higher amount of gas. Therefore, using the main Ethereum blockchain to store the IoT data will cost a lot due to the augmenting price of Ether and the gas fees. Storing data in the Ethereum blockchain is not recommended because their role in the distributed technology stack is intended for computation rather than storage.

Whereas, Ethereum created the Swarm protocol [167] that aims to a distributed storage built-in incentives to guarantee uploaded data persistence due to high coupling with the Ethereum network layer. Swarm is a P2P storage service that rely on the PoS consensus mechanism and it is integrated with Ethereum. Swarm provides a decentralized and redundant store for Decentralized Applications (DApps) code, user data, blockchain and state data. Swarm has opted to use xDAI which is an EVM compatible blockchain bridged to the Ethereum blockchain. In the Swarm network, nodes use a TCP-based transport protocol used for P2P communication among Ethereum nodes. The Swarm nodes directly connect to the Ethereum network and has the cryptographic hash associated with their account address. Figure 2.37 shows the Swarm distributed storage architecture.

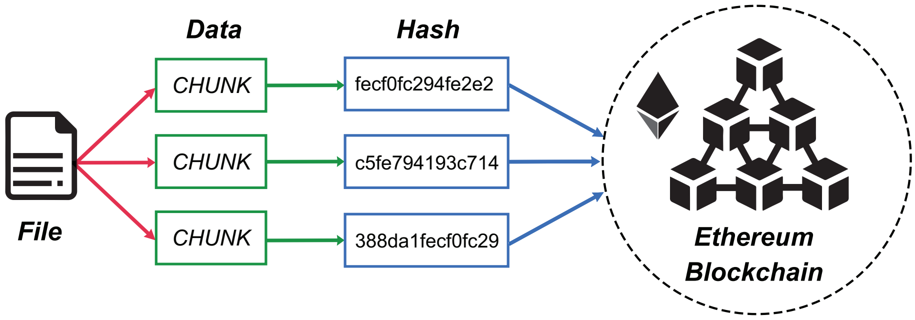


Figure 2.37: Swarm distributed storage architecture.

Swarm has a distributed chunk store with a basic unit of storage (currently, the maximum size is fixed to 4KB hash). The chunk store is derived from its addressed content in a deterministic manner. When data (images, videos, files, etc.) are uploaded to a Swarm network, the Swarm API layer chop this data into chunks with fixed size. Each chunk is hashed with a unique cryptographic hash. The hashes of these chunks will be used to generate another hash for a new chunk. Currently, a new chunk is made with 128 hashes, so the content gets mapped to a chunk tree which gathers a Merkle tree. To retrieve the uploaded files, the address used is the root hash of this tree [168].

In this thesis, the Swarm Ethereum is selected to be integrated with the LoRaWAN network because it provides a scalable and self-sustaining infrastructure for a supply-chain economy of data, unlike the Ethereum blockchain. Also, the transaction time is faster and cheaper. The LoRa network is extended by storing the received data in the Swarm Ethereum storage service, and defining a clear way to store, access and retrieve the data using Swarm and Ethereum smart contracts. The integration of a public blockchain in LoRaWan network will secure the transmitted data for safe and immutable data storage.

Chapter 3

Development of Short-Range BLE IoT Sensor

"Knowledge is the conformity of the object and the intellect."

- Ibn Rushd (Averroes)

This chapter introduces a compact moisture sensor that utilizes a resistance measurement method accurate for a broad range of resistance values. The sensor is cost-effective and low in power consumption, features digital control via a BLE-enabled micro-controller.

3.1 Moisture measurement

The characteristics of materials can be assessed through their impedance. Various measuring instruments and electronic circuits have been developed to determine the impedance of a material or group of similar materials. For instance, the impedance value can give insights into liquid conductivity or biological cell suspensions [169], analysis of meat or fish composition, determination of food freshness [170], bioimpedance measurements in food processing [171], evaluation of soil [172], sapphire [173], wood [174], and semiconductors [175]. However, it is important to note that these impedance measurement methods are limited to specific applications and may not be suitable for use in other fields.

Contact electrodes are a widely used method for measuring material impedance by inserting them into the material and making it a part of the electronic measurement circuit. The accuracy of the impedance measurement depends on various factors, including the electrode impedances, which are in series with the material being measured, and parasitic impedances between the electrodes, material, and surroundings [176]. The use of four electrodes, with separate potential and current electrodes, can reduce electrode impedance effects, but it increases circuit complexity.

Multiple measurement systems have been developed to achieve accurate impedance measurement, such as a combination of commercial equipment and custom electronic circuits, or a combination of commercial instruments and specialized systems [177]. However, accurately measuring resistive impedance over a wide range and with high accuracy remains a challenge, requiring complex laboratory setups with specialized commercial instruments. The electronic components used in the measurement circuit must be carefully selected and evaluated, as their ideal behavior can differ from their actual behavior, especially under varying conditions like different measurement values, temperature ranges, humidity, etc. Commercial instruments take these factors into account, but they can be bulky, expensive, power-hungry, and not portable [178]. Therefore, a new simple, low-power, low cost and accurate device is proposed in this chapter to overcome these limitations.

3.2 Electronic Circuit Development

Accurate measurement of high resistance values above GΩ typically requires the use of specialized instruments like electrometers or megohmmeters/picoammeters [179]. These instruments, however, are not practical for portable use due to their size and weight. They employ either constant-voltage or constant-current measurement methods, with constant-voltage (the more commonly used method) measuring the unknown resistance by connecting it in series with the electronic circuit and measuring the circulating current, then determining the resistance value using Ohm's law. However, this process is not straightforward as a single electronic circuit may not provide accurate results for a wide range of resistance values, especially for materials such as building materials, textiles, and biological tissues. With the goal of creating a precise and versatile measurement device that is lightweight and compact, we propose utilizing the latest technology to design an electronic circuit that overcomes current limitations.

In measuring resistances above 1 GΩ, various factors in the circuit can cause deviations from the actual value. Some of the main sources of unwanted effects are offset voltage, polarization currents in operational amplifiers, leakage currents, noise, etc. It is therefore crucial to assess the circuit to account for these effects and compensate for them based on the measurement conditions (resistance value and temperature) and the characteristics of the circuit. There are several circuit configurations that can be used in electrical resistance measurement. The appropriate configuration depends on the range of resistance to be measured. Figure 3.1 illustrates three possible configurations.

The circuit in Figure 3.3(a) shows uses a Wheatstone bridge, where the unknown resistance R_x is one of the resistors in the bridge. The differential voltage (V_2 - V_1)

is measured and amplified by a variable gain stage. An instrumentation amplifier with fA polarization current is required to avoid load effects, resulting in the need for a discrete instrumentation amplifier designed using electrometer-grade discrete operational amplifiers, further increasing complexity. Figure 3.3(b) shows a second option that uses a current source, where the voltage V_x is amplified and measured. However, this configuration is not optimal for low voltage and wide resistance range measurements, as the current source may not be stable for precise pA generation, and the amplification section must be programmable, increasing complexity without precision guarantees.

The chosen option was an inverter circuit as illustrated in Figure 3.3(c), which offers simplicity, affordability, and effectiveness, with the sole requirement of using an electrometer-grade operational amplifier to avoid load effects due to polarization currents. The amplification section of the circuit applies a fixed voltage V_i and the unknown resistance value R_x. Equation 3.1 relates all values involved in the measurement circuit, including the input voltage V_i, output voltage V_o, feedback resistor R_f, and measured resistance R_x. With knowledge of V_i, R_f, and V_o, the value of R_x can be calculated.

$$V_o = -\frac{R_f}{R_x} V_i \tag{3.1}$$

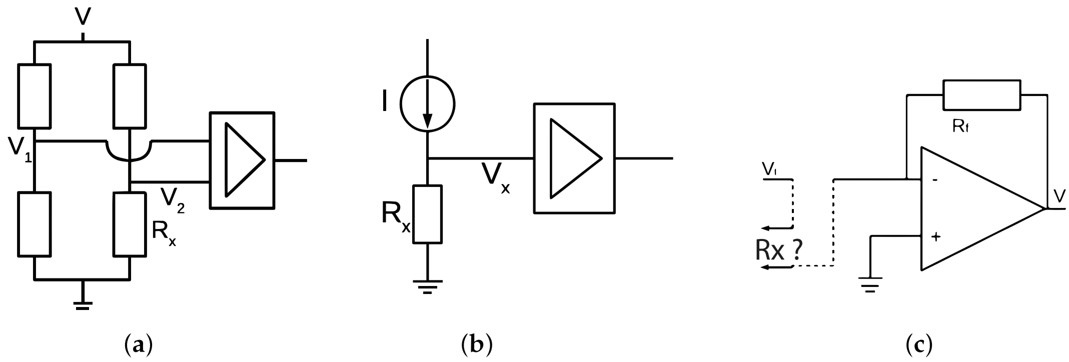


Figure 3.1: Three methods for measuring resistance: (a) utilizing a Wheatstone bridge, (b) using a current source, and (c) employing an inverter circuit with an ideal amplification stage. Out of these options, the inverter circuit with ideal amplification stage was selected for the measurement, and the unknown resistance value, referred to as R_x, of the material to be measured was determined using this circuit [180]

The proposed circuit employs a multiplexer in the feedback loop of the operational amplifier to prevent saturation and achieve the maximum output voltage (Vo). The multiplexer modulates the gain by adjusting the R_f value in accordance with R_x. Three different R_f values have been included and the multiplexer is controlled by the digital part. For R_x values in the range [1,50] MΩ,R_f is set to 680 KΩ; for R_x values in the range [50 MΩ, 3 GΩ], R_f is set to 33 MΩ, and for R_x values in the range [1.5, 100] GΩ, R_f is set to 1 GΩ. An automatic undervoltage detection procedure is used to automatically select R_f, where the voltage from the amplifier falls in the range [0.6, 3.5] V. It is important to choose the multiplexer carefully, as its actual performance can deviate significantly from the ideal working mode [181], as will be discussed later. After amplification, a Sallen-Key low-pass filter is included to eliminate noise contribution.

Figure 3.2 describes the real model of the input amplifier is simplified for three different feedback resistor values (R_{f1}, R_{f2}, R_{f3}). Both the alternating current (AC) and direct current (DC) models of the multiplexer are taken into account. C_D represents the output pin capacitance of the multiplexer, C_S is the associated capacitance for the input pin in each internal switch of the multiplexer, C_{DS} is the capacitance between multiplexer pins, C_{SS} is the parasitic capacitance between multiplexer channels, I_S is the leakage current in the multiplexer pins, and I_L is the leakage current at the multiplexer output terminal.

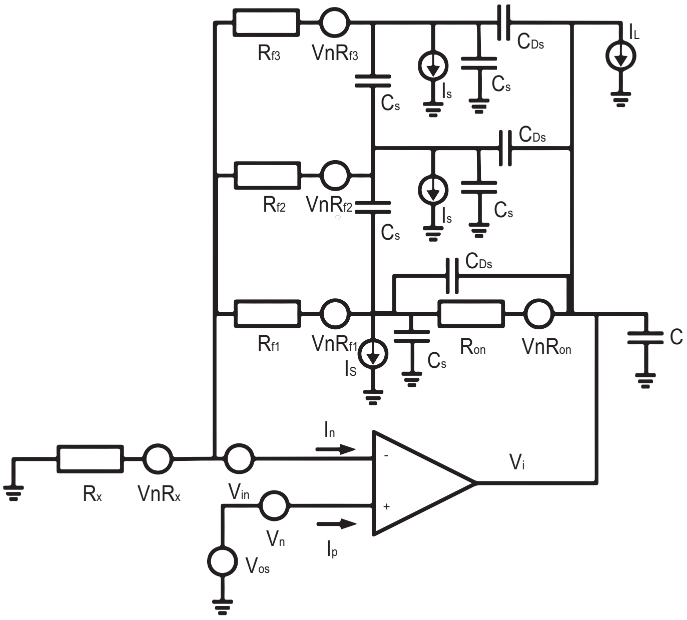


Figure 3.2: Model of the input amplifier section considering real effects of electronic components used [180]

However, due to real-world effects such as thermal noise in resistors ($V_{nR_{fi}}$), operational amplifier noise (V_n), offset voltage between input pins (V_{os}), and polarization currents (I_p, I_n), Equation (3.1) becomes inadequate, particularly for certain values of R_x and R_f. These effects include:

- Increased thermal noise in resistors ($V_{nR_{fi}}$) with rising temperature, which becomes more pronounced as resistor values increase [182].
- Operational amplifier noise (V_n) due to offset voltage between input pins (Vos), and noise (V_{in}) due to polarization currents (I_p, I_n) [183].

- Leakage currents in the multiplexer (I_L, I_S), parasitic capacitances (C_{DS}, C_D, C_S), and resistance in the multiplexer (R_{on}) [181].

As depicted in Figures 3.2 and 3.3, the real model deviates from the ideal circuit. Hence, the circuit response must be evaluated based on the actual circuit, particularly in cases where the error currents are similar in magnitude to the currents to be measured (e.g. when measuring values in GΩ, the current to be measured is in the *pA* range). To ensure accuracy in the analog circuit, it is crucial to evaluate potential sources of error. By applying the superposition theorem, we can isolate the AC and DC models in the circuit and make an informed choice of electronic components to minimize errors. Table 3.1 displays the selected characteristics (at 25°C) of the resistors, multiplexer, and operational amplifier.

R_f	Operational Amplifier	MUX
Tolerance $\leq 1\%$ TC(R_f) $\leq 100\ ppm/$°C	$I_b \leq 30\ fA$ $I_{os} \leq 30 fA$ $V_{os} \leq 2$ mV $TC(V_{os}) \leq 10\ \mu$V / °C $\gamma_n \leq 85$ nV / $Hz^{1/2}$ $\sigma_n \leq 0.1\ fA\ /\ Hz^{1/2}$	$R_{on} = 5\Omega \ll R_f$ $I_s \leq 10pA$ $C_D < 30\ pF$ $C_S < 5\ pF$ $C_{DS} < 0.2\ pF$

Table 3.1: Technical data of components used in the input amplifier for the theoretical characterization and experimental verification [180]

However, the input amplifier can be affected by noise and the output voltage (V_o) supplied to the filter section can become saturated. To counter this, a ±5 V power supply has been added to the analog board, with the supply voltage being 3.3 V from the digital board. As a result, the maximum theoretical output voltage is limited to ±3.5 V due to saturation in the operational amplifier. For resistance values above 10 GΩ, the maximum output voltage is significantly reduced due to noise, and the gain must be decreased to prevent signal saturation. To rectify this, the filter circuit following the amplification stage enables obtaining a suitable output voltage after filtering.

3.2.1 Electronic Board of the BLE Device:

The circuit of the developed BLE device is composed of two boards, digital and analog in order to reduce interference. The interface between the analog and digital boards consists of 8 pins, including 2 ground pins, an I2C bus interface for the A/D converter, 3 control lines for the analog multiplexer to regulate gain, and a single analog power shutdown line for power optimization by enabling and disabling the analog power supply. All lines of this interface operate at 3V. Figure 3.3 illustrates the circuit.

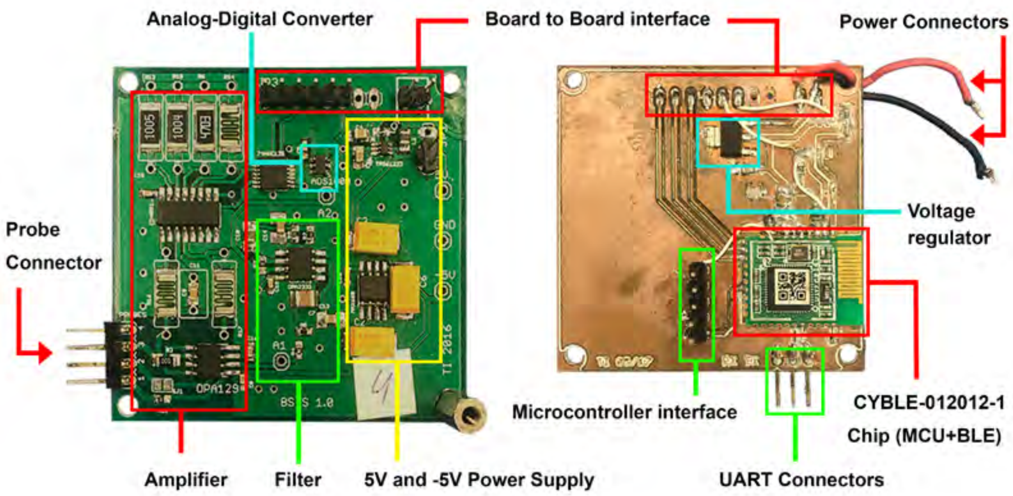


Figure 3.3: BLE moisture device circuit: analog and digital boards. The size of the circuit when the boards are connected: 5.7 cm × 5.3 cm × 1.5 cm [184]

3.2.1.1 Analog board:

The moisture device measures the DC electrical resistance of the wood to calculate the moisture content. The regression model used to obtain the moisture value from the resistance is described by Equation 3.2, where a, b, and c are variables that depend on the type of wood and the can be obtained from the average electrical resistance at different moisture content level [185]. Figure 3.4 illustrates the resistance as a function of moisture for various species of wood.

$$M = a \times R_x^b + c \tag{3.2}$$

3.2.2 Digital board:

The digital board can be adapted to different requirements while maintaining the analog board. The interface between the two boards consists of 8 pins: two ground pins, three analog multiplexer control lines for gain control, an I2C bus interface for the A/D converter, and an analog power shutdown line for power efficiency by switching on and off the analog power supply. All lines of the interface operate at 3.3V.

The core component of the digital board is the CYBLE-012012-1 SoC from Cypress. This module boasts a 32-bit processor with a clock speed of up to 48 MHz and an impressive performance of 0.9 DMIPS/MHz. It was selected due to its

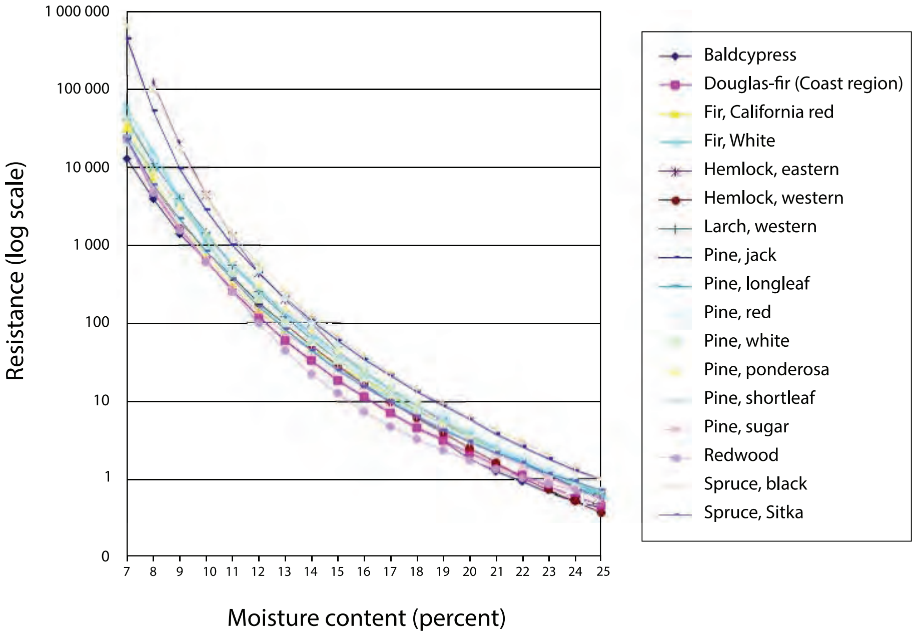


Figure 3.4: Resistance as function of moisture for multiple wood species [186]

compact size of 14.52 mm x 19.20 mm x 2.00 mm and the ability to connect to up to 23 configurable General Purpose Input/Outputs (GPIOs), allowing for the integration of additional electronic boards. Additionally, it features a Bluetooth 4.1 qualified single-mode module. The power consumption and transmission specifications of the module are detailed in the accompanying table 3.2.

TX output power	–18 dbm to +3 dbm
R_x output power	–18 dbm to +3 dbm
TX current consumption	15.6 mA (radio only, 0 dbm)
R_x current consumption	16.4 mA (radio only)
Low-power mode support (Deep Sleep)	1.3 μA with watch crystal oscillator (WCO) on
Low-power mode support (Stop)	60 nA with GPIO (P2.2) or XRES wakeup

Table 3.2: Power consumption characteristics of the module CYBLE-012012-1

The BLE SoC is powered by the AMS1117 low-drop voltage regulator, which provides a stable 3V voltage to its components. This SoC is a comprehensive RF solution for Bluetooth Low Energy data sharing and offers a complete communication stack. It supports various peripheral functions, such as Analog-to-digital converter (ADC), timers, counters, I2C, (UART), and SPI, through its programmable architecture. The device was designed to measure resistance values from analog parts, process the information, and send notifications to another device via BLE. The instant resistance value is obtained by averaging the last 50 measurements (over a sliding window) and determining the physicochemical value of the material using pre-calculated property-resistance.

The BLE sensor was made portable by integrating additional circuitry for a battery power supply, as shown in Figure 3.5 (a). It runs on three AAA batteries providing 4.5V. The compact size of the circuit is 5.7 cm x 5.3 cm x 3 cm. A protective casing made of epoxy material was designed to encase the sensor, with stainless steel probes to prevent corrosion due to continuous use. The final product prototype is depicted in Figure 3.5 (b).

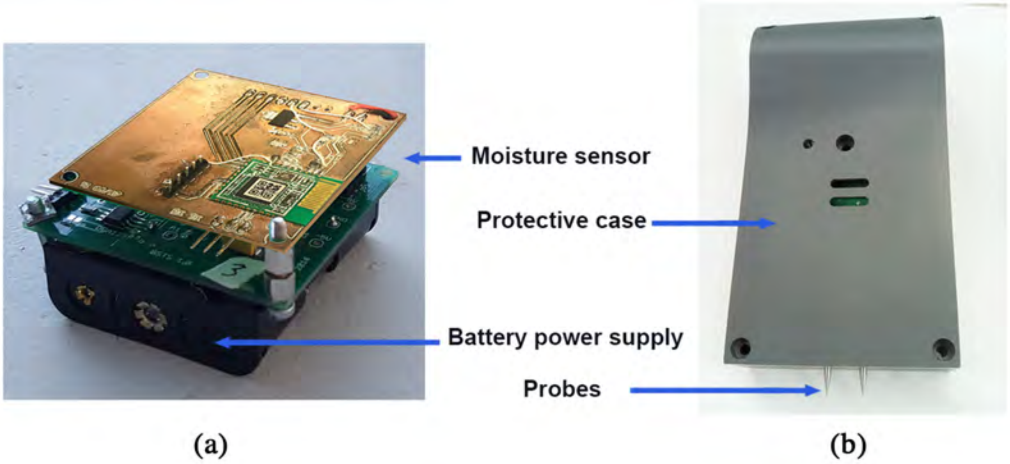


Figure 3.5: The BLE sensor node prototype; (**a**): the BLE sensor circuit with battery power supply, (**b**): the protective case of the BLE sensor with the measurements probe. [184]

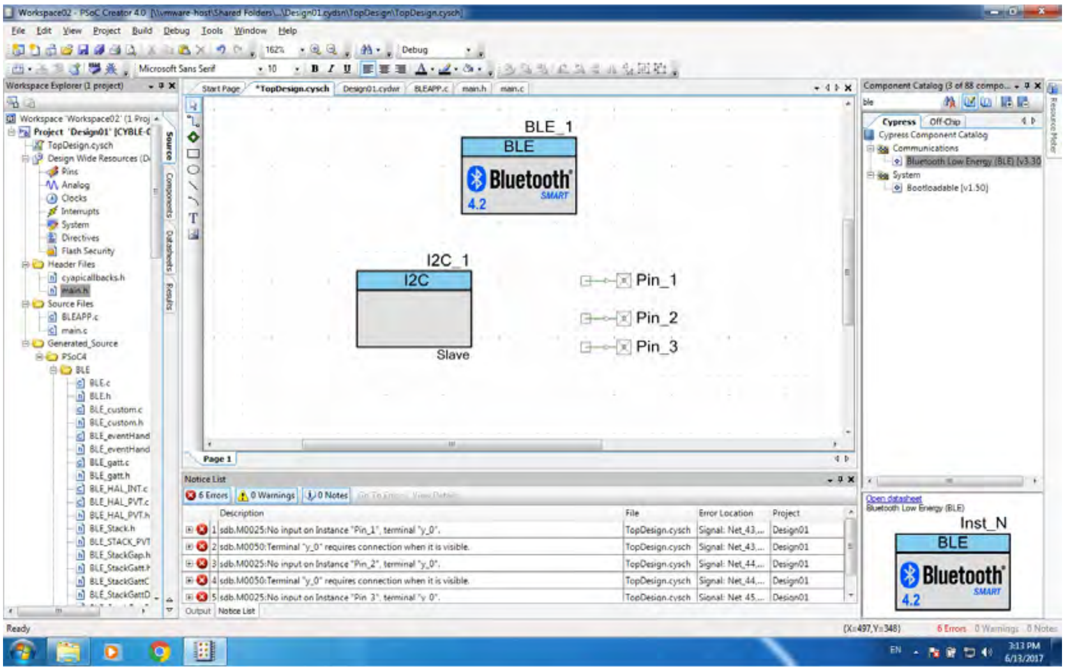
3.3 Programming the BLE device

The accompanying software, "PSoC Creator IDE", simplifies the development and programming of BLE applications. Figure 3.6 displays a block diagram of the components activated from the PSoC Creator software.

The component used to program the BLE device are: an I2C block reads ADC, a BLE block manages BLE communication, three pins for the multiplexer, and a timer block that controls the data sample rate and wake-up/standby. By incorporating these components, their functions can be utilized in the main code.

In the BLE component configuration tab, the "Profile" is changed to "Custom" in order to create a new profile from scratch. The profile role is set as "**GATT Server**" as in order to store the data transported over ATT and accept ATT requests, commands, and confirmations from the GATT client. The Gap role is changed to "**Peripheral**" so that the device monitor the environment. In the "Gap Settings" tab, the device was given the name "**Humidity Sensor**" and a unique 48-bit Bluetooth address used to identify the device UUID was generated.

The device will transmit two data points: resistance value and calculated moisture value. To achieve greater precision, these values will be divided into two parts: the



	Description	File	Error Location	Project
1	sdb.M0025:No input on Instance "Pin_1", terminal "y_0".	TopDesign.cysch	Signal: Net_43,...	Design01
2	sdb.M0050:Terminal "y_0" requires connection when it is visible.	TopDesign.cysch	Signal: Net_43,...	Design01
3	sdb.M0025:No input on Instance "Pin_2", terminal "y_0".	TopDesign.cysch	Signal: Net_44,...	Design01
4	sdb.M0050:Terminal "y_0" requires connection when it is visible.	TopDesign.cysch	Signal: Net_44,...	Design01
5	sdb.M0025:No input on Instance "Pin_3", terminal "y_0".	TopDesign.cysch	Signal: Net_45,...	Design01

Figure 3.6: Screenshot from PSoC Creator IDE software showing the final BLE application schematic.

decimal and fractional parts. To accomplish this, four characteristics were defined in the GAP Settings tab: $ResInt$ and $ResDec$ to respectively retrieve the integer and fractional parts of the resistance value stored in the GATT database, and $MoisInt$ and $MoisDec$ to respectively retrieve the integer and fractional parts of the moisture value stored in the GATT database. The size of $MoisInt$ and $ResInt$ is 4 bytes while $MoisDes$ and $ResDec$ is 1 byte.

The main code is initialized by defining five global variables:

- $BleConnected$**:** denote the connection state.

- $connectionHandle$**:** Represents the identifier handle for the connection of the first characteristic $ResInt$.

- $connectionHandle2$**:** Represents the identifier handle for the connection of the second characteristic $ResDec$.

- $connectionHandle3$**:** Represents the identifier handle for the connection of the third characteristic $MoisInt$.

- $connectionHandle4$**:** Represents the identifier handle for the connection of the fourth characteristic $MoisDec$.

To handle Gap and GATT database access events, a method called "$Stack\_Handler$" was created. This method acts as a switch statement, handling events as they occur.

For example, when a connection is established, the global variable *BleConnected* is assigned and the event is handled accordingly within the *Stack_Handler* method. The function $CyBle_GappStartAdvertisement$ is utilized to initiate the advertisement process. This function employs the advertisement data specified in the GUI of the component customizer. Upon executing this API, the device becomes accessible for connection by other devices configured as GAP central role.

The GATT client's data will be stored in the GATT server database using the following functions:

- *Cyble_GattWriteRsp* (*connectionHandle*) stores the integer part of the resistance value.
- *Cyble_GattWriteRsp* (*connectionHandle*2) stores the fractional part of the resistance value.
- *Cyble_GattWriteRsp* (*connectionHandle*3) stores the integer part of the moisture value.
- *Cyble_GattWriteRsp* (*connectionHandle*4) stores the fractional part of the moisture value.

The structure of the handles is "*CYBLE_ GATTS_ HANDLE_ VALUE_ NTF_ T*". For each of the four handlers, the following inputs are added: "*handleValuePair.attrHandle*" to specify the value to be written, "*handleValuePair.value.len*" for the length of the written data, and "*handleValuePair.value.val*" for the data buffer.
The "*CyBle_ GattsWriteAttributeValue*" function writes to the value field of a specified attribute in the GATT database of a GATT server. It is a blocking function that does not generate an event. If a connected peer device initiates a write operation, this function is executed on the GATT server and checks the attribute permissions (flags).

The two methods, "*Setmux*" and "*SetmuxGain*", are defined in addition to the main loop. The *Setmux* method takes three boolean inputs (A, B, and C) and sets the outputs (MUXA, MUXB, and MUXC) of the multiplexer in the device to 0 or 1. The "*SetmuxGain*" method adjusts the values of A, B, and C and adjusts the feedback resistor when the gain changes, these values corresponds to the variable a,b and c of Equation 3.2.

The method "*SetMaterial*" has three floating-point variables a, b, and c, which depend on the type of wood used. The program retrieves the material value from the GATT database and uses it to calculate the moisture content.

The I2C bus is started and the measured value is read using the following functions:

- $I2C\_I2CMasterClearStatus()$: Clears all status flags and returns the master status.
- $I2C\_I2CMasterSendStart(uint32slaveAddress, uint32bitRnW)$: Generates a start condition and sends the slave address with the read/write bit.
- $I2C\_I2CMasterWriteByte(uint32theByte)$: Sends one byte to a slave.
- $I2C\_I2CMasterSendRestart()$: Generates a restart condition and sends the slave address with the read/write bit.
- $I2C\_I2CMasterReadByte(I2C_I2C_ACK_DATA)$: Reads the I2C slave address byte from the ADS, ACKs and the transfer.
- $I2C\_I2CMasterSendStop()$: Generates an I2C stop condition on the bus.

The developed BLE moisture sensor is battery-operated. A long battery life is a crucial requirement for such devices. The device is programmed with a low-power solution, as shown in the flow diagram represented in Figure 3.7: the device sends the data to the gateway and enters deep sleep mode, waking up on the next notification from the gateway. This deep sleep mode allows the BLE device to minimize energy consumption and extend battery life.

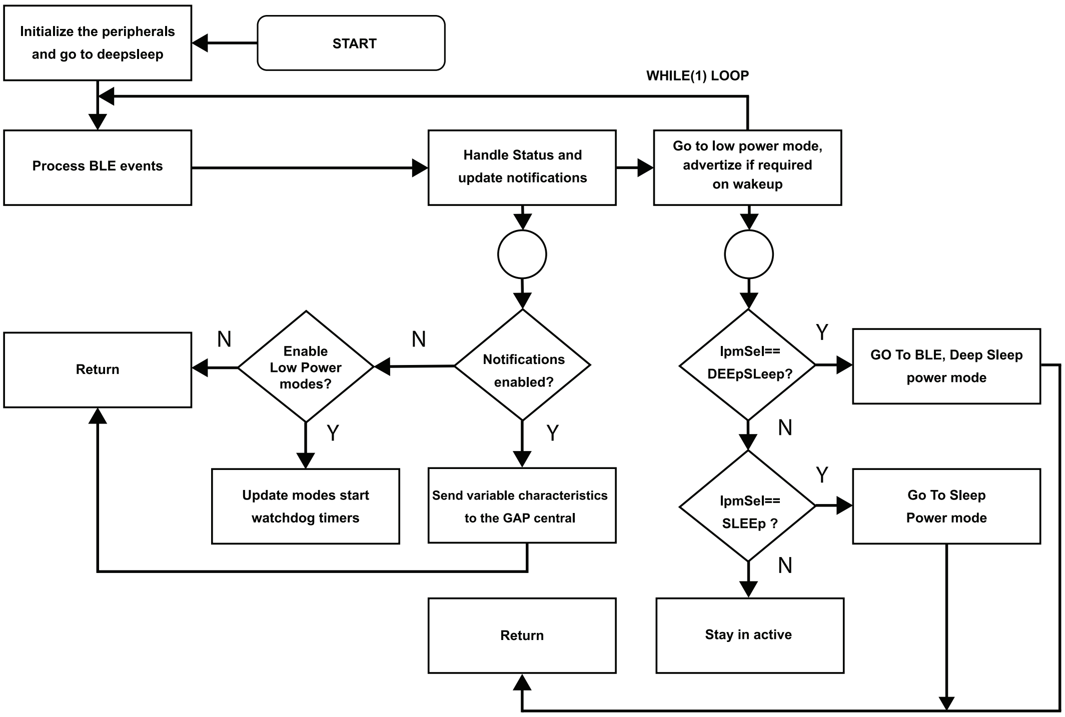
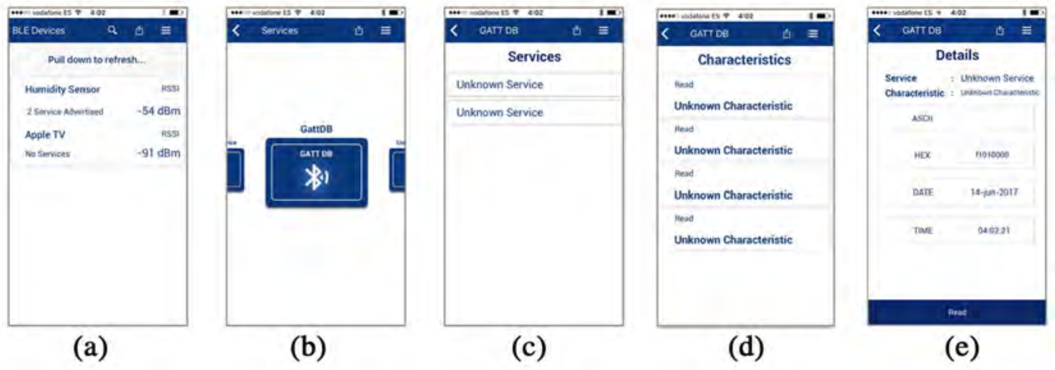

Initialize the peripherals and go to deepsleep
START
WHILE(1) LOOP
Process BLE events
Handle Status and update notifications
Go to low power mode, advertize if required on wakeup
Return
N
Enable Low Power modes?
N
Notifications enabled?
IpmSel== DEEpSLeep?
Y
GO To BLE, Deep Sleep power mode
Y
Y
N
Update modes start watchdog timers
Send variable characteristics to the GAP central
Y
IpmSel== SLEEp ?
Go To Sleep Power mode
N
Return
Stay in active

Figure 3.7: The simplified diagram flow of the deep sleeping mode process configuration of the BLE sensor node. [184]

3.4 Experimental tests and Results

This section assesses the performance of the developed BLE device in regards to energy consumption an latency. The CySmart iOS app is used for in the experimental test, which is a BLE tool developed by Cypress Semiconductor Corporation. It's important to note that a slave typically has limited energy supply, while a master may not have the same limitations. The study considers two methods of obtaining sensor readings from the slave, acting as an attribute server, which are referred to as one-way ATT communication and round-trip ATT dialogue. In the one-way ATT communication, the slave sends a notification upon receiving a poll from the master. In the round-trip ATT dialogue, the master sends a request, which prompts the slave to transmit a response, triggering Link Layer acknowledgements in both the request and response. The first packet transmission from the master occurs at the start of each connection event for both methods.



Service : Unknown Service
Characteristic : Unknown Characteristic
ASCII
HEX f1010000
DATE 14-jun-2017
TIME 04:02:21

Figure 3.8: Mobile Screenshots of *CYSmart* mobile app

After connecting the BLE device's connectors to a 500 MΩ resistor. The the *CySmart* app is launched, As shown in Figure 3.8 (a), The device can be located as "**Humidity Sensor**". Once it is selected, the *GattDB* option allow to read the measured values (Figure 3.8 (b)). It is important to note that since custom services and characteristics were used in the program, these services may not be recognized by the app and appear under the name "Unknown" as shown in Figure 3.8 (c), and the same thing for the characteristics as shown in Figure 3.8 (d). Figure 3.8(e) shows the value read of this first characteristic which is $MoisInt$ (0d00 equals 13 in decimal).

3.4.1 Characterization Test Bench

The setup of the test bench is illustrated in Figure 3.9(a) where the device is powered and connected to the *CySmart* app via Bluetooth for data transfer. Figure 3.9(b) illustrates the climate chamber used to evaluate the circuit performance, for this aim, a resistance decade box is used as a reference pattern.

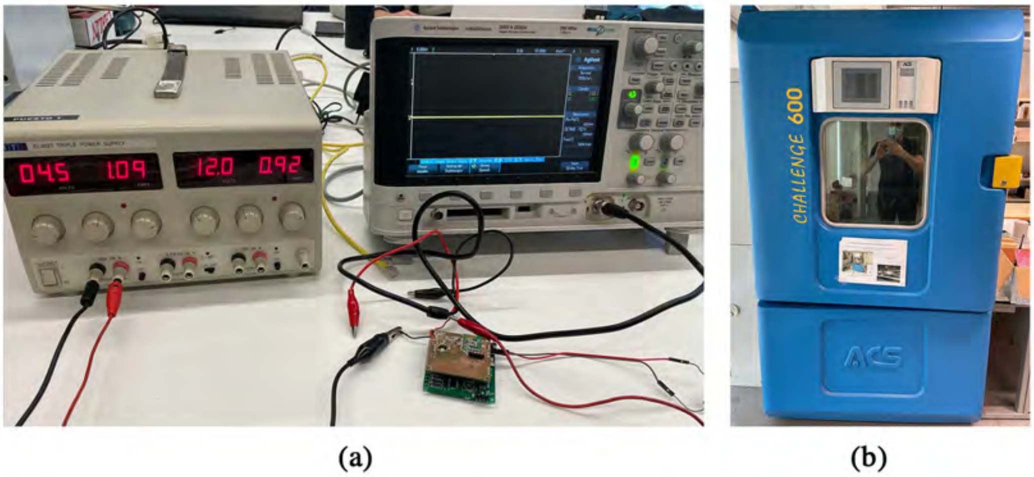


Figure 3.9: Test bench: (a)The circuit is powered and connected to a PC for monitoring and data analysis using Bluetooth. (b) the climate chamber used for characterization

3.4.2 Latency and Energy Consumption

To determine the power consumption and estimated operational period of sensor devices, the InfiniiVision DSO-X 2022A oscilloscope is used along with a setup that included a resistor and a mobile phone with the CySmart app to receive the measured values. This setup was used to measure the power consumption profile of BLE environmental beacons during various activities. The energy consumption during the transmission of a single advertisement packet was analyzed. The findings, presented in Figure 3.10, demonstrate that each transmission completes in 2 milliseconds and consumes 0.018 Joules of energy with a one-second advertising interval.

The normal operation power profile of the device is depicted in Figure 3.11. This device performs a measurement of resistance and moisture content and transmits advertisement packets during a 7-second active interval, leading to an energy consumption of 0.64 J. The device operates with two AAA batteries, which typically have a nominal voltage of 1.5V and a capacity of 600-1200 milliampere-hours (mAh).

In the case of measuring the moisture content of wood, two to three measurements per day are sufficient. If the device is programmed to take two measurements per day, the total time required for advertising, measuring, and transmitting the data would be around 8 seconds. The average current consumption during this time, as seen in Figure 3.11, is approximately 18.23 mA.

The device enters a stand-by mode, where it consumes an average of 13.36 mA, for 30 seconds. During this time, the device wakes up 10 seconds before taking a measurement and remains awake for 5 seconds after. The deep sleeping mode

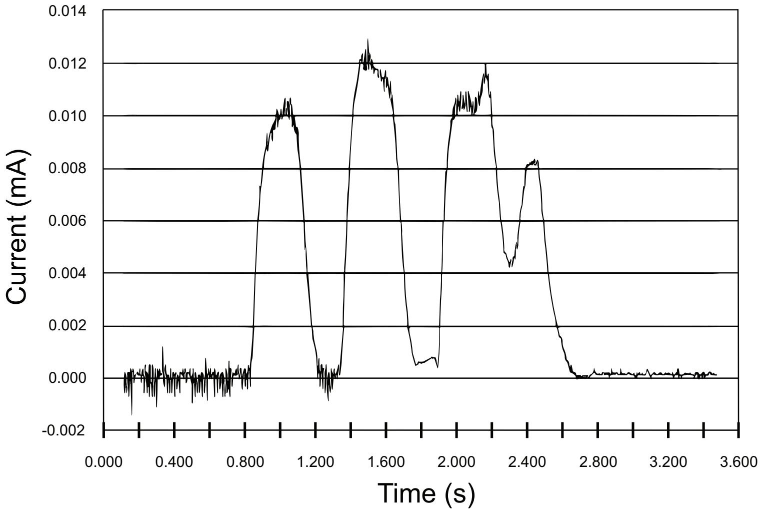


Figure 3.10: Consumption profile during advertising.

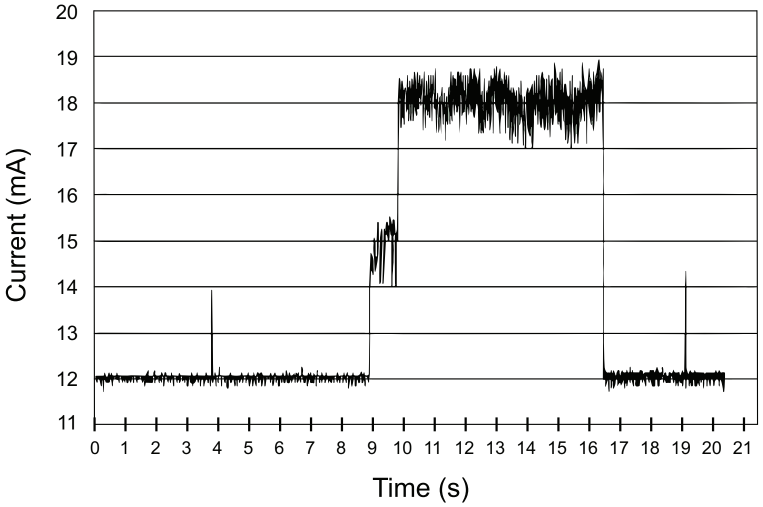


Figure 3.11: Consumption profile during advertizing and measurement.

consumes only 1.3 μA, and the device remains in this mode for the rest of the day. The total daily energy consumption for the three modes is 0.001317 J. Therefore, considering that the capacity of a typical AAA battery is 600 - 1200 mAh, the batteries can last for about 125 to 250 days if the device is in stand-by mode for 30 seconds, active for 16 seconds, and sleeping for the rest of the day.

3.4.3 Evaluation of Accuracy

To evaluate the long-term accuracy, the Type A extended uncertainty [187] is obtained by taking 32 independent measurements from a calibrated decade box, at a rate of two measurements per day (every 12 hours) for 16 days in our laboratory. The relative humidity at this time was between 43 and 55 percent, while the temperature was between 23 and 25 °C. The average of 100 readings taken over the course of two minutes was used to create each observation.

R_{nom}	R_{cal}	Accuracy (%)	R_m	σ_{ext}	$\epsilon r(\%)$
1 MΩ	1.0000057 MΩ	± 0.00002	1.0049 MΩ	±0.0004	0.5
10 MΩ	10.000028 MΩ	± 0.0005	10.083 MΩ	±0.045	0.8
100 MΩ	100.00173 MΩ	± 0.01	100.4211 MΩ	±0.0001	0.4
1 GΩ	1.000183 GΩ	± 0.005	1.0042 GΩ	±0.0001	0.4
10 GΩ	10.016717 GΩ	± 0.005	10.0436 GΩ	±0.0012	0.3
100 GΩ	99.89014 GΩ	± 1	99.235 GΩ	±1.010	0.7

Table 3.3: The results of the measurement of resistance (R_{nom}) include the nominal value, the calibrated value (R_{cal}) with its tolerance, the value obtained through the measurement circuit (R_m), and the extended uncertainty (σ_{ext}) and relative error (ϵ_r) when compared to the calibrated value (Rcal).

The results are shown in Table 3.3, along with the resistance measurement's nominal value (R_{nom}), calibrated value (R_{cal}) and its tolerance, measured value (R_m), extended uncertainty (σ_{ext}), and relative error (ϵ_r) when compared to calibrated value (R_{cal}). As shown in this table, accurate results acheived even for resistances as high as 100 GΩ, with a relative error of 0.7% and an extended accuracy of ±1 GΩ. This is particularly impressive given that a low voltage of 5 V was used.

3.4.4 Thermal Characterization

Temperature fluctuations can affect not only the resistance of a material, but also the response of the circuit due to electronic component effects. To assess the impact of temperature on the electronic components of the circuit, a climate chamber was used, as high resistance measurements deal with low values and small temperature variations must be taken into account. The temperature analysis was conducted at 10°C, 20°C, 30°C, 40°C, and 50°C with a constant relative humidity of 50%. After the climate chamber reached thermal equilibrium, data was acquired every three seconds and averaged over five minutes (100 samples). For each temperature and calibrated resistance (R_{cal}) value, measurements were taken for 30 minutes. The measurement circuit and calibrated resistance decade box were placed inside the climate chamber and the measured values were transmitted wirelessly to a computer (as shown in Figure 3.11(b)). Table 3.4 presents the accuracy and extended uncertainty results for resistance values ranging from 1 MΩ to 10 GΩ. The maximum error observed was 0.4% for the 10 GΩ resistance value.

Table 3.4 shows that the measurement error is less than 0.5% for resistance values under 10 GΩ. However, for ultra-high resistance values, the measurement is significantly impacted by temperature. The circuit is stable for temperatures

T(°C)	R_{cal}	1.0000057 MΩ	10.000028 MΩ	100.00173 MΩ	1.000183 GΩ	10.016717 GΩ
10	R_m	0.9968	10.0119	99.7234	0.99723	9.9723
	σext	0.0002	0.0053	0	0	0
	ϵ_r (%)	0.3	0.1	0.3	0.3	0.4
20	Rm	0.9971	10.015	99.7234	0.997234	9.9723
	σext	0.0006	0	0	0	0
	ϵ_r (%)	0.3	0.1	0.3	0.3	0.4
30	Rm	0.9981	10.0058	99.7234	0.997234	9.9723
	σext	0	0.0181	0	0	0
	ϵ_r (%)	0.2	0.06	0.3	0.3	0.4
40	Rm	0.9981	10.008	99.7234	0.997277	10.015
	σext	0	0.0159	0	0.004305	0
	ϵ_r (%)	0.2	0.08	0.3	0.3	0.02
50	Rm	0.9981	9.9779	99.7234	0.997277	10.015
	σext	0	0.0145	0	0.0004283	0
	ϵ_r (%)	0.2	0.2	0.3	0.3	0.2

Table 3.4: Measurements of resistance values were taken in a climate chamber at temperatures ranging from 10°C to 50°C for resistance values of R_x ranging from 1 MΩ to 10 GΩ using a power supply of 5 V.

below 30°C for all analyzed power supply values (V_i). However, for temperatures above 30°C, a growing discrepancy with respect to the actual resistance value occurs. These results highlight the need for a correction factor to account for high resistance and temperature, especially when using a power supply of 5 V. The correction factor is implemented in the digital portion by the micro-controller as the variation is systematic.

3.4.5 Moisture Content Measurement

The BLE device underwent a benchmark experiment to assess its functionality in terms of flexibility, performance and compatibility with devices. The experiment involved connecting a BLE device powered at 5V to Computer. As illustrated in Figure 3.12, to validate the results, the Lutron MS-7000 moisture meter is used. This digital meter boasts 9 material species groups in memory and utilizes 2 pins electrodes to accurately measure the moisture content of wood. The test was conducted using multiple types of wood, and the results obtained from the Lutron MS-7000 moisture meter were found to be consistent with those obtained from the BLE device. The test was performed at a temperature of 25 °C. The results are summarized in Table 3.5.

The results indicate that the values obtained from the BLE device are comparable to those obtained from the Lutron MS-7000 moisture meter. This deviation is acceptable due to the difference in calculation methods between the two devices. Additionally, the Lutron MS-7000 only supports 9 registered wood materials while the BLE device supports 36 different materials, allowing users to add more materials through the settings page on the web application. This versatility makes the BLE

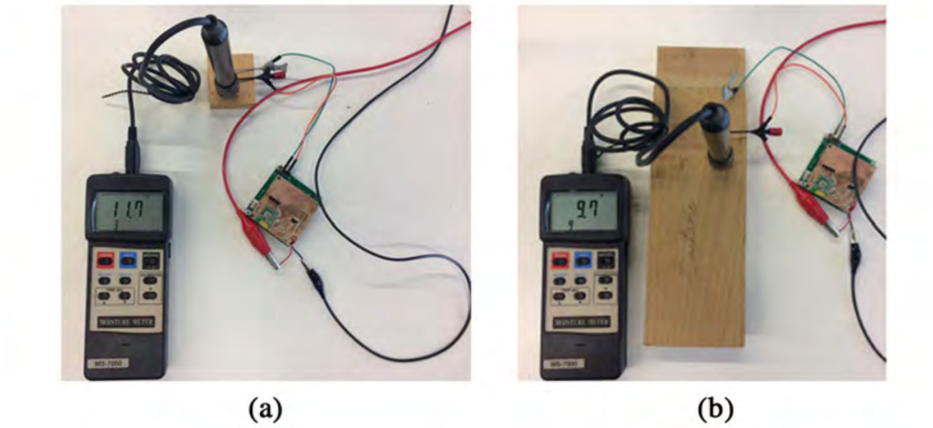


Figure 3.12: Test bench to compare the measurement of the BLE device and the Moisture meter 'MS-7000' of two different wood species: (a) Larch Western, (b): Pine, Red

Wood	Resistance (BLE) MΩ	Moisture (BLE) %	Moisture Meter Value %
Pine, Shortleaf	11,730	8.43	8.6
Larch, Western	3980	9.71	9.7
Pine, Red	1570	11.47	11.7
Pine, Ponderosa	39,800	7.23	7.1
Redwood	22,450	7.91	7.7

Table 3.5: Result of test with 5 different wood: Resistance BLE and Moisture BLE are the values transmitted from the device and Moisture meter value is the value read by the MS-7000.

device a more versatile option compared to the moisture meter used in this test.

3.5 Discussion

This chapter presented a novel resistance measurement BLE device, capable of measuring a wide range of resistance values, including ultra high resistance values up to 100 GΩ. The device demonstrates accurate results for resistance values below 10 GΩ and systematic deviations for higher values, which can be digitally compensated. The circuit design is thoroughly analyzed, taking into consideration possible sources of error when measuring resistance, and experimental tests were conducted to validate the circuit's performance under long-term measurement, temperature variations, and different timber materials. This circuit opens up new opportunities for IoT applications such as detecting the actual moisture content of processed wood and building monitoring where timber materials are used. The developed device is a critical component in the deployment of the IoT system based on BLE technology described in Chapter 5. The system will be thoroughly described, showcasing the potential for the device to be utilized in an IoT application.

Chapter 4

Development of Long-Range LoRa IoT Sensor

> *"The only way to do Great Work is to love what you do."*
>
> - Steve Jobs

This chapter introduces a compact and cost-effective moisture sensor that utilizes a LoRa-enabled micro-controller, which allows for digital control of the device, making it highly versatile and flexible. The moisture sensor itself is designed with a novel resistance measurement method, which offers accurate readings across a broad range of high resistance values.

4.1 Circuit development

The moisture device presented in this section is specifically designed for use in Cultural Heritage buildings. The moisture content (MC) in wood refers to the percentage of the mass of water present in wood relative to the mass of dry wood. According to the EN 16682 standard [188], the resistance measurement method is favored for continuous monitoring of MC in wooden heritage structures and buildings [189].

4.1.1 Resistance method

The resistance parameter can be measured using either direct or indirect methods [189–191]. Regarding indirect measurement methods, electrical resistance measurement is a widely used technique to estimate the MC in wood. This method is favored for its quick and non-destructive nature, as well as the direct relationship between resistivity σ and MC in wood that can be appropriately adjusted based on the type of wood and temperature [192–194]. The electrical resistance measurement process involves applying a voltage between two electrodes inserted into the wood, creating an electric current path and enabling the measurement of resistance R. The resistance depends on several factors, including the geometry of the wood piece, the position and material of the electrodes, the insertion depth, the species and density of the wood, and temperature and MC [195–197].

Standard measurement protocols, such as the European Norm EN 13183-2:2002 for sawn timber and EN 16682:2018 for resistive measurement in wood and cultural heritage conservation, can be utilized to control or adjust these factors for more accurate results in laboratory settings using high precision instruments [198, 199]. However, practical measurement in the field using commercial instruments can result in less accurate values due to non-controlled environment conditions [200]. The electrical resistance measurement in wood is impacted by two main groups of factors: those related to the internal wood characteristics and those related to the experimental measurement procedure. The latter can be set prior to measurement, while the former must be accurately measured [198, 199].

In terms of resistive measurement methods, both direct current (DC) [179, 193, 194, 201] and alternating current (AC) [202, 203] can be used to determine the equivalent resistance (R) of the electrodes. However, DC measurement methods are susceptible to polarization effects, which cause a temporary change in the measured resistance [204, 205]. In contrast, AC measurement methods effectively minimize these effects by alternating the polarity of the voltage applied to the electrodes [205–207]. The procedure involves applying a positive polarization voltage, measuring the current after a specified time period (which varies depending on the wood species), repeating the same process with a negative polarization voltage, and repeating these steps until equal and stable values are obtained. The resistance is then calculated by averaging the last ten values. The main challenge in this procedure lies in determining the appropriate AC frequency required to reach stability, which must be estimated through a prior analysis specific to the type of wood. The AC method used in the developed sensor, for measuring the electrical resistance of wood, eliminates the need for prior analysis to determine the optimal AC frequency. This method also minimizes polarization effects during transient measurements, providing an effective solution to the problem at hand.

4.1.2 Electronic board

The resistance measurement method involves applying an electric current path between a pair of electrodes inserted into the wood, which measures its electrical resistance R. The wood's moisture content is directly proportional to its resistivity (ρ), which can be determined through the electrical resistance (R) according to Equation 4.1:

$$R = \frac{\rho L}{A} \tag{4.1}$$

where L is the distance between the electrodes and A is the transversal area of the current path.

The presented device uses a novel AC resistance measurement method, which eliminates the need for prior frequency analysis. The method is based on a simple and efficient relaxation oscillator, as depicted in Figure 4.1. Unlike other AC methods [205, 207] which require prior study to fix the frequency, this method automatically adjusts its frequency f based on the equivalent electrical resistance of the wood (R_w in Figure 4.1). The capacitor C_2 is charged and discharged through the voltage V_0 and resistance R_w, producing a square signal that oscillates between $+V_{sat}$ and -V_{sat} when V_t reaches the threshold values V_{tmax} and V_{tmin}, respectively, as shown in Figure 4.1.

$$\begin{aligned} V_{tmax} &= \tfrac{R_1}{R_1+R_3}V_{sat}. \\ V_{tmin} &= -\tfrac{R_1}{R_1+R_3}V_{sat}. \end{aligned} \tag{4.2}$$

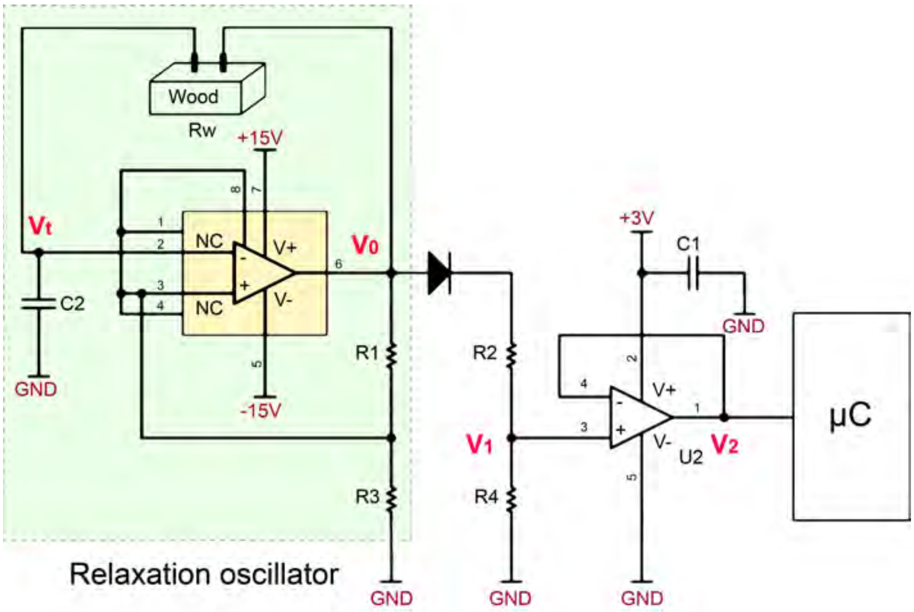


Figure 4.1: Electronic circuit for MC conversion using an AC resistance measurement method.

The oscillation period T is linearly proportional to the equivalent wood electrical resistance (R_w), given the symmetry of the saturation voltages $+V_{sat}$ and -V_{sat} in the operational amplifier U_1, as follows:

$$T = 2\ln(\frac{R_1 + 2R_3}{R_1})R_w C_2. \tag{4.3}$$

The resistance of the wood, R_w, can be determined indirectly by measuring the time period, T, of the oscillation. This period is measured using a microcontroller and converted into the wood resistance through a program that adjusts the voltage levels in the circuit (as seen in Figure 4.1). This method, which was previously presented by the authors in [206], eliminates the need for a prior study to estimate the optimal AC frequency, allowing for a more efficient and streamlined process.

The operational amplifier U_1 in Figure 4.1 requires a ±15 V power supply, which is generated by the low-input boost converter TPS61093DSK. This regulator is designed with an enable pin that allows the microcontroller to turn on the circuit only when the wood resistance is being measured, thereby conserving battery power. Once the measurements have been taken, the device sends the average value to the gateway and enters sleep mode for a configurable period of time that can be set by the user through the web monitoring platform.

The sensing node, also includes a LM335DT temperature sensor, since the moisture content conversion from the R_w measurement depends on temperature as well [208–210]. The LM335DT boasts an impressive accuracy of ±1 °C.

4.1.3 Description of LoRa Moisture Sensor

The newly developed end-node sensor for measuring the MC in wood has a compact design that integrates the sensing and LoRa communication components into a single board. The components of the moisture sensor are illustrated in Figure 4.2.

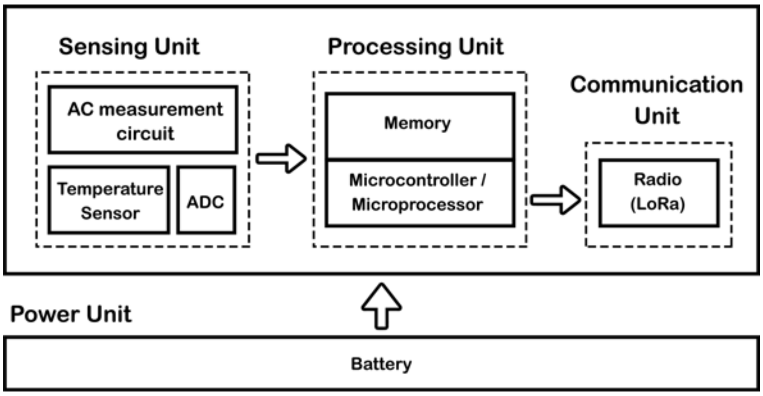


Figure 4.2: Components of the LoRa end-node MC sensor.

The sensor can be divided into four main components:

- **The Sensing Unit**: This section contains a novel AC measurement circuit designed to measure the MC in wood, as well as a temperature sensor. These components provide the necessary data to be read by the Processing Unit.

- **The Processing Unit**: This section is equipped with a programmable micro-controller that has been programmed to manage the sensing and LoRa communication functions. The firmware also has power management features to conserve energy.
- **The Communication Unit**: This section enables data exchange between the sensor node and the LoRa gateway using the LoRa communication protocol.
- **The Power Unit**: The sensor is powered by two standard 1.5 V AAA batteries. This section regulates the power supply to provide a constant 3.3 V output for the Processing and Communication Units, as well as generates a symmetrical ±15 V DC power supply for the Sensing Unit.

The processing and communication capabilities of the end-node sensor are integrated into the WiMOD iM881-XL module from IMST [211]. The iM881-XL is equipped with a programmable STM32L081 microcontroller that is optimized for battery-driven applications. The specific firmware for the sensor will reside in this unit. Key features of the iM881-XL include:

- Operating voltage: 1.8 V to 3.6 V.
- MCU operation frequency: 32 MHz.
- Sensitivity: -138 dBm.
- Operating frequency: ISM 868 MHz.
- Operating temperature range: -40 °C to +85 °C.
- Low Power mode current: 1.4 μA.
- Receiving current: 11.2 mA.
- Transmitting current: 25 mA to 38 mA.

This commercial module boasts ultra-long range spread spectrum communication and exceptional immunity to interference. Operating within the 868 MHz ISM band, the iM881A-XL has a wide operating voltage range of 1.8 V to 3.6 V, and employs Semtech's patented LoRa modulation technique, which combines spread spectrum modulation with forward error correction. It is pre-certified according to the European guideline EN 300 220 and can be directly soldered as a surface mount device (SMD) component.

The resulting board has a size of 81 × 83 mm, it offers versatility in terms of antenna connectivity with the option of using either an internal antenna for reduced size or an external antenna for enhanced range. A switch is conveniently located on the board to allow for switching between the two options. Figure 4.3 illustrate the electronic board of the device which includes the following components:

1. Sliding switch to power up the device.
2. Power supply regulation components.
3. LED to inform about different operation modes according to blinking codes.
4. MC measurement circuit.
5. Wood probes connector.
6. Battery holder type AAA.
7. Programming connector for firmware update and debugging.
8. Wireless LoRa Module.
9. Switch between integrated and external antennas.
10. External SMA antenna connector.
11. Temperature sensor LM335DT.
12. Integrated PCB Antenna W3136.

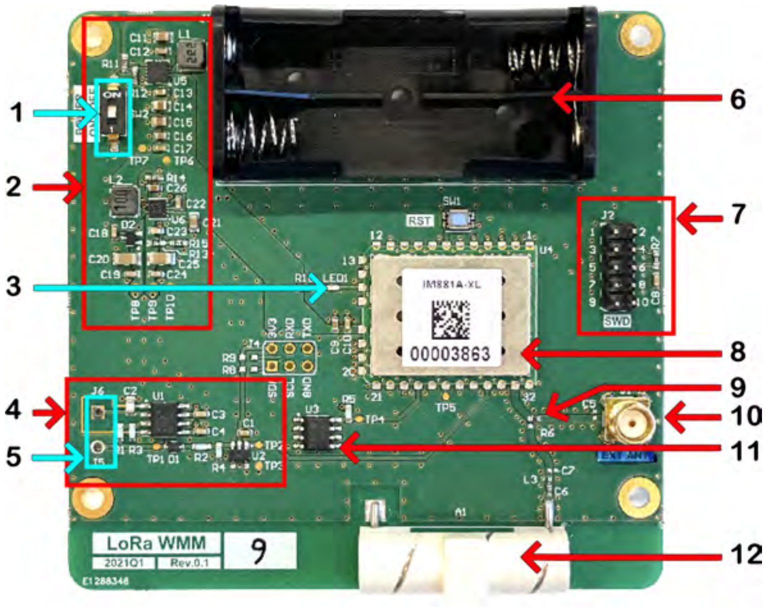


Figure 4.3: LoRa end-node MC sensor board.

4.1.4 Moisture Sensor Final Prototype

To protect the electronic circuit from dust and other environmental factors, a custom plastic box was designed using 3D printing technology. The box was designed to perfectly fit the dimensions of the circuit board that effectively shielded the electronic components from potential damage. Figures 4.4(a) and 4.4(b) illustrate the front and back sides of the moisture device prototype, respectively. The blue component, as depicted in Figure 4.4(b), featuring two 0.7 mm diameter stainless nails is affixed to the wooden roof and then connected to the device. The moisture device is powered by two 1.5 V AAA batteries.

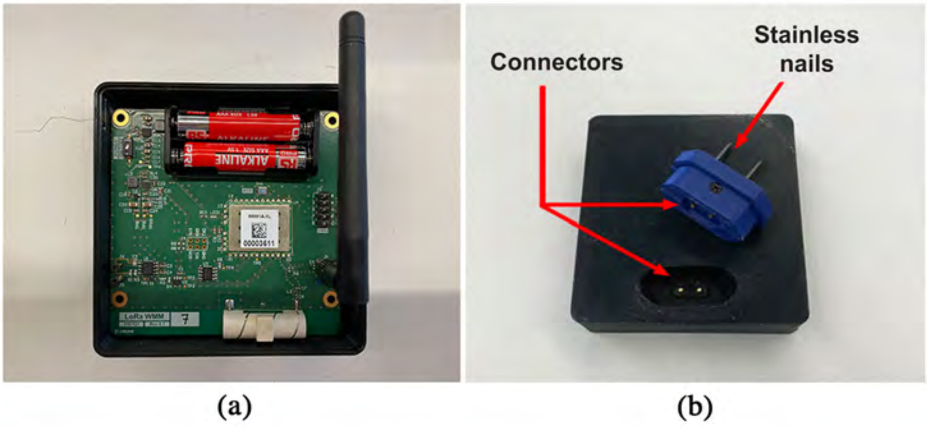


Figure 4.4: LoRa moisture device : (a) Front side of the moisture device, (b) back side of the moisture device showing the detached nail pieces.

4.2 Programming the LoRa Device

In order to program the LoRa sensor, the open-source project available at GitHub in [212] is used. It is an open-source code repository developed by the LoRa Alliance that provides a software foundation for LoRa devices and includes drivers for the LoRa radio module, including the "$IM880 - XL$", along with a communication protocol implementation that adheres to the LoRaWAN standard. After preparing the development environment and cloning the repository from GitHub, the first step was to secure communications between LoRa end-nodes and gateways. The project supports 3 different secure-elements "$soft - se$", "$lr1110 - se$" and "$atecc608a - tnglora - se$" implementations. The "$soft - se$" tool was chosen to commission and personalize the LoRa device as it provides flexibility and low resources. It is a small, tamper-resistant chip that is embedded in the LoRaWAN device, and it is used to store sensitive security information such as keys and certificates. The DevEUI, JoinEUI and AES128 keys may be stored on a non-volatile memory through dedicated APIs.

In order to update the end-device identity, one must update the "$se-identity.h$" file located under ./src/peripherals/soft-se/ directory. Listing 4.2 presents the code that define the different identification elements including the device EUI, the Koin EUI and the device address, and also the network key and the application key.

```c
#ifndef __SOFT_SE_IDENTITY_H__
#define __SOFT_SE_IDENTITY_H__

#ifdef __cplusplus
extern "C" {
#endif
#define STATIC_DEVICE_EUI        1

#define LORAWAN_DEVICE_EUI       { 0x70, 0xB3, 0xD5, 0x8F, 0xF1, 0x01, 0x50, 0xF8 }

#define LORAWAN_JOIN_EUI         { 0x70, 0xB3, 0xD5, 0x7E, 0xD0, 0x03, 0x85, 0xC4 }

#define SECURE_ELEMENT_PIN       { 0x00, 0x00, 0x00, 0x00 }

#define STATIC_DEVICE_ADDRESS    1

#define LORAWAN_DEVICE_ADDRESS   ( uint32_t )0x26011DE5

#define SOFT_SE_KEY_LIST
    {
        {
            .KeyID    = APP_KEY,
            .KeyValue = { 0xFA, 0x30, 0x05, 0xD0, 0xBF, 0x88, 0x32, 0x36, 0x13, 0x03, 0x6E, 0xA7, 0x1E, 0xD6, 0x79, 0x1A },
        },
        {
            .KeyID    = NWK_KEY,
            .KeyValue = { 0xFA, 0x30, 0x05, 0xD0, 0xBF, 0x88, 0x32, 0x36, 0x13, 0x03, 0x6E, 0xA7, 0x1E, 0xD6, 0x79, 0x1A },
        },
        {
            .KeyID    = APP_S_KEY,
            .KeyValue = { 0x65, 0xA8, 0xF4, 0x3B, 0xC0, 0xF5, 0xFB, 0x57, 0x1D, 0x30, 0xC9, 0x60, 0x5F, 0x22, 0xE2, 0x5D },
        },
#ifdef __cplusplus
}
#endif
```

Listing 4.1: Code of the "se-identify" file that defines the device and the network identification.

The different pins of the LoRa module chip can be defined in the file $board-config.h$. The different functions of the board are added in the $board.c$ file. In addition to the several function for LoRa communication defined in the main code, the following functions are added in order to get the moisture measurement:

- $BoardBatteryMeasureVoltage()$: this function is used to measure the battery voltage and return the battery level.

- $ActiveMeasuringCircuit()$: This function turn on the 15V measurement circuit in order to measure the moisture of wood.
- $BoardMeasurePeriod()$: this function uses a timer $OnOsc4TimerEvent()$ to measure the period of frequency of the relaxation oscillator described in Figure 4.1. The analog input of the micro-controller connected to the oscillator is triggered when there is a positive voltage, this way the frequency period T can be obtained to measure the resistance of wood.
- $GetMoisture()$: This function uses the average period value T of ten measurements obtained by the function $BoardMeasurePeriod()$. Then, the resistance of the wood R_w is obtained using Equation 4.3.
- $BoardSleepMode()$: This function turn off the 15V circuit and put the device in sleeping mode.

In addition to these functions, other timers and functions to are defined to control the LED of the board and the sleeping mode and the waking up process, in addition to the control of transmission and the reception of packets from the LoRaWan gateway. The LoRaWan class, the duty cycle and the data-rate are also defined in the main code. The simplified flow diagram of the developed program to compute the period T for the STM32L081 microcontroller is shown in Figure 4.5.

As described in Figure 4.6, the "ST-LINK/V2" is used in order to debug the program into the device board. The single-wire interface module (SWIM) and JTAG/serial wire debugging (SWD) interfaces are used to communicate with STM32 microcontroller located on the target application board.

The Things Network (TTN), which is a globally accessible, open-source infrastructure based on LoRaWAN standards [213] is used for LoRaWan communication. After creating an account on TTN's website. A new application was created so the devices can be registered under that application. Figure 4.7 shows the TTN dashboard while registering the moisture device. Information such as the device's EUI (Extended Unique Identifier) and the network session key will need to be provided during the registration process. After the device has been registered, the appropriate parameters such as the device's data rate, frequency plan, and activation method can be set up to enable it to communicate with TTN. Once the device has been configured, data can be transmitted to TTN where it can be monitored and managed through the TTN Console or using TTN's APIs.

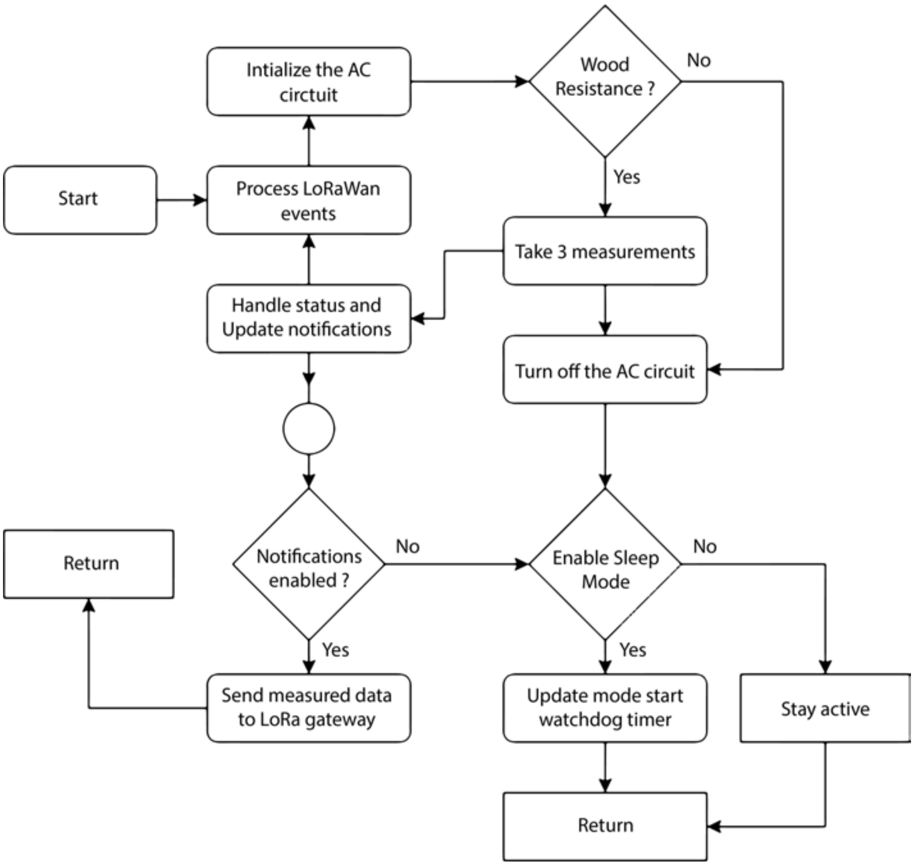
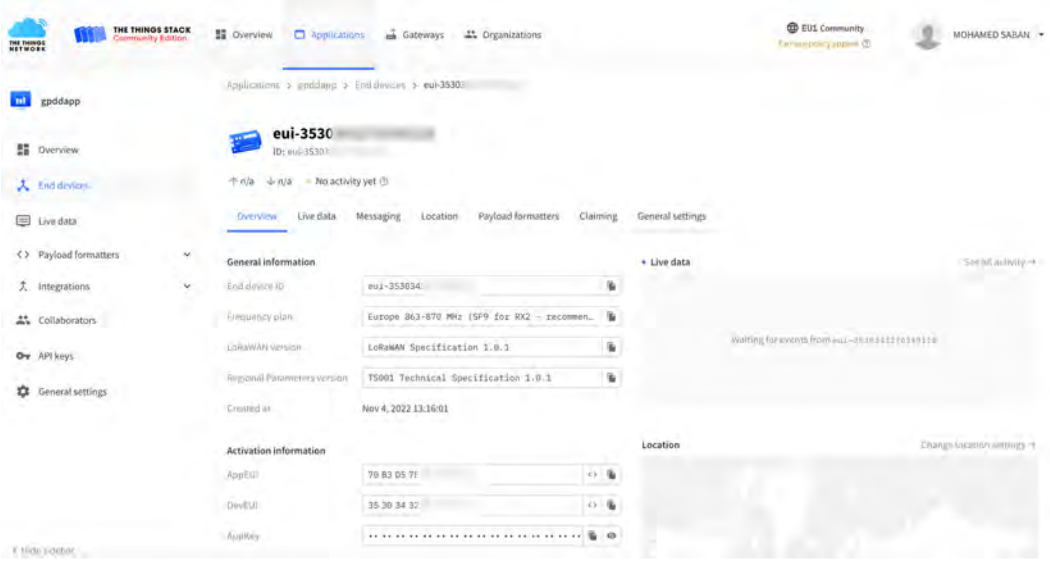


Figure 4.5: Simplified flow diagram used in the MC device.



Applications > gpddapp > End devices > eui-3530[redacted]

eui-3530[redacted]

ID: eui-3530[redacted]

↑ n/a ↓ n/a • No activity yet

General information

End device ID	eui-353034[redacted]
Frequency plan	Europe 863-870 MHz (SF9 for RX2 - recommen…
LoRaWAN version	LoRaWAN Specification 1.0.1
Regional Parameters version	TS001 Technical Specification 1.0.1
Created at	Nov 4, 2022 13:16:01

Activation information

AppEUI	70 B3 D5 7E[redacted]
DevEUI	35 30 34 32[redacted]
AppKey	•• •• •• •• •• •• •• •• •• •• •• •• •• •• •• ••

• Live data

See all activity →

Waiting for events from eui-3530341[illegible]

Location

Change location settings →

Figure 4.7: Screenshot from the TTN platfrom showing the process of registering a new device in the TTN LoRaWan network.

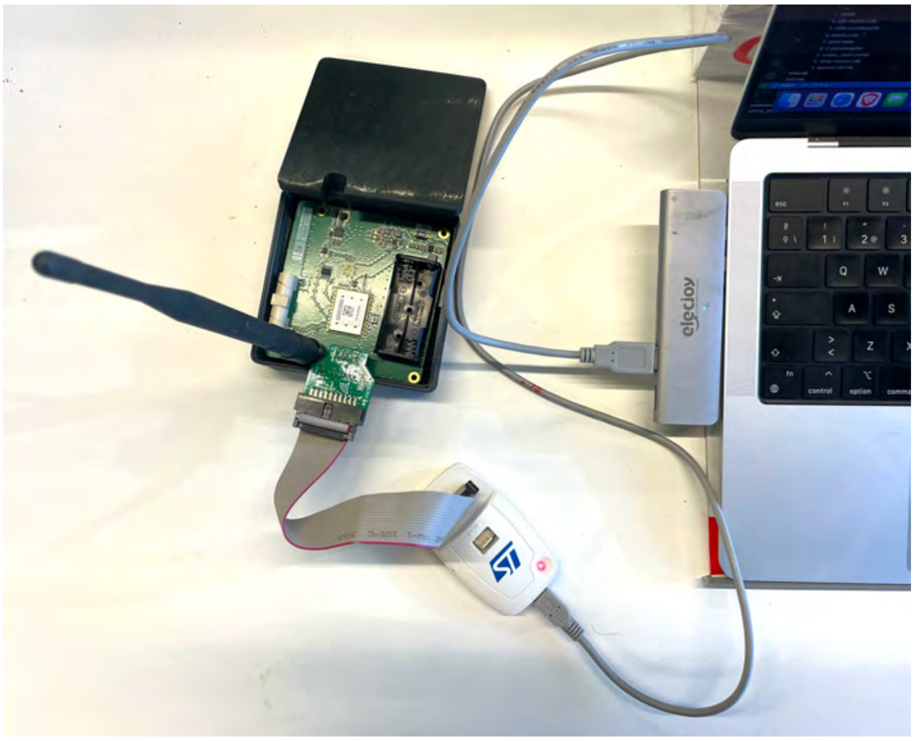


Figure 4.6: ST-Link/v2 debugger device used to upload the code to the developed board

4.3 Experimental Tests and Results

Two separate analyses were conducted to fully evaluate the MC LoRa end-node. The first analysis consisted of characterizing the end-node through a calibration process at a constant temperature of 25 °C. This calibration helped determine the accuracy of resistance measurement. The thermal analysis was also included to assess its impact on accuracy. The correlation between wood resistance and the MC was established, and the results were compared with previous studies using the oven-drying method [189–191]. The second analysis focused on analyzing the LoRa communication to determine the real-world capabilities of the end-node, including range, data transmission, and communication link stability between end-nodes and the LoRa gateway. To accurately study the capabilities of the proposed monitoring system, a real-world scenario was employed

4.3.0.1 MC Measurement Circuit: Functional Test

The MC LoRa end-node was calibrated in a laboratory environment at a controlled temperature of 25 °C. The calibration process involved measuring the oscillation period, T, of the circuit in Figure 4.1, for different values of R_w. A calibrated resistance decade box (IET model VRS-100) was utilized to provide a fixed value of R_w ranging from 10 $M\Omega$ to 10 $G\Omega$, which are typical values for wood resistance as it changes from humid to dry. A total of 30 measurements were performed for each value of R_w, and a linear fit was applied as a linear correlation was observed between the measured period T and R_w. The resistance value R_w can be estimated using equation (4.4), where K is equal to 322.9 Ω/s.

$$R_w = K \cdot T. \tag{4.4}$$

The results of the analysis of the three PCBs are displayed in Table 4.1. R_d represents the resistance values fixed by the calibrated decade box, expressed in $M\Omega$, T is the period obtained using the measurement circuit, R_w is the resistance estimated by the MCU using the obtained period T, and ϵ_r indicates the relative error.

Table 4.1: Accuracy Evaluation of Resistance Measurement: The accuracy of the resistance measurement was analyzed by comparing the calibrated resistance value (R_d), the obtained period (T), the measured resistance (R_w) calculated using equation (4.4), and the relative error (ϵ_r) for three MC LoRa end-node boards (PCB1, PCB2, and PCB3).

PCB	R_d (**MΩ**)	***T(s)***	R_w *(MΩ)*	ϵ_r(%)
1	10.000028	0.0309	9.935975	0.2
	100.001730	0.3046	98.463497	1.6
	1000.183000	3.0620	995.092578	1.1
	10016.717000	30.8620	10083.190000	0.5
2	10.000028	0.0311	10.042190	0.4
	100.001730	0.3101	100.115145	0.1
	1000.183000	3.0913	998.180770	0.2
	10016.717000	31.2502	10090.689601	0.7
3	10.000028	0.0309	9.990526	0.1
	100.001730	0.3090	99.759955	0.3
	1000.183000	3.1121	1004.906780	0.5
	10016.717000	30.9608	9997.245550	0.2

The results indicate that the accuracy of the R_w measurement is within 2 %. This confirms that the resistance value can be precisely determined from the measured period (T) by the sensing circuit in the MC LoRa end-node.

According to Samuelson's equation [208], the Moisture content in wood is related with its resistance R_w as:

$$MC = \frac{log[log(R_w) + 1] - b}{a} \tag{4.5}$$

where MC is given in %, R_w in $M\Omega$; a and b are model coefficients which values depend on the wood species [209, 210].
Using (4.5), the analytic MC relative error is given by:

$$\epsilon_{MC} = \frac{\epsilon_r}{ln10^2 \times [log(R_w) + 1] \times [log(log(R_w) + 1) - b]}. \tag{4.6}$$

From (4.6), it can be interpreted that $\epsilon_r < 2$ % in R_w typically implies $\epsilon_{MC} < 0.2$ % in the MC value (slightly dependent on the wood species).

4.3.0.2 Thermal Characterization of the Sensing Unit

The MC LoRa end-node features a highly sensitive sensing unit that operates with minimal current levels (pA). However, these low-level currents may be impacted by the leakage currents that occur in the circuitry components at high temperatures, leading to significant measurement errors [214, 215].
To ensure the functionality of the MC LoRa end-node in outdoor environments, it was important to conduct a thermal characterization. The behavior of the MC LoRa end-node at varying temperatures was assessed using a climate chamber. The temperature was adjusted from 25 °C to 50 °C, incrementing by 5 °C, while four different resistance values were fixed using a calibrated resistance decade box. The results of the thermal characterization exhibited a consistent pattern for each temperature, in accordance with Equation (4.4). The maximum relative error was less than 3 %, resulting in an error of less than 0.3 % in the MC value. This implies that the developed MC LoRa end-node can be used over a broad temperature range without requiring thermal compensation.

4.3.0.3 MC measurement in different wood species

The accuracy of the resistance measurement was verified using calibrated values, and a resistance range between 300 kΩ and 100 GΩ was experimentally measured with an accuracy of less than 2 %. As discussed in (4.5), and based on the parameters a and b obtained in (Table 4.2) [209, 210, 216, 217], this resistance range corresponds to a moisture content (MC) range of 6 % to 30 % for the species of Douglas Fir (Pseudotsuga Menziesii), European Ash (Fraxinus Excelsior), and Chestnut Tree (Castanea Sativa). After this experiment, the MC LoRa end-node board was tested on these three species of wood. The dimensions of each timber sample were 90 × 35 × 45 mm. Two 0.7 mm diameter nails were used as electrodes, inserted 10 mm deep into the center of each sample with a separation of 20 mm, as shown in Figure 4.8(a).
The test was conducted over a period of three days, with slight variations in environmental conditions, including a temperature range of 23 °C to 27 °C and a relative humidity range of 55 % to 63 %. During the test, each MC LoRa end-node

Table 4.2: Parameters a and b of (4.5) associated to each wood species.

Wood species	a	b
Oregon pine (Pseudotsuga Menziesii)	-0.045000	1.14700
European ash (Fraxinus Excelsior)	-0.051567	1.13545
Chestnut tree (Castanea Sativa)	-0.039347	1.02940

was set to send 10 measurements per hour. However, for practical use in real-world scenarios, sending 2 to 4 measurements per day is sufficient. A web platform (Figure 4.8(b)) was created for data storage, visualization, and analysis.

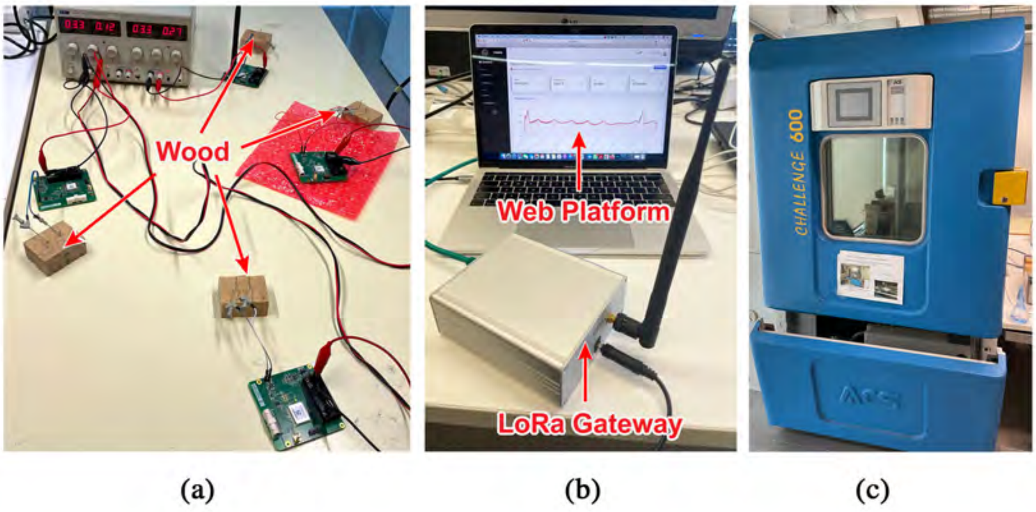


Figure 4.8: A test bench is utilized for circuit characterization, which involves (a) measuring the resistance of three timber samples from various wood species, including Douglas Fir, Ash, and Chestnut. These measurements were taken using an MC LoRa end-node board, (b) LoRaWAN gateway and a custom-developed web platform and (c) Climatic chamber.

Equation (4.5) and coefficients a and b for each of the different wood species are integrated into the platform to calculate the MC values. The resulting MC measurements over time are displayed in Figure 4.9, exhibiting values lower than 10 %, as expected given that the wood was stored in the laboratory for two years.

4.3.0.4 Verification of the developed MC LoRa-based monitoring system.

In order to validate the accuracy of the developed MC measurement system, it was compared against the results obtained using the traditional oven-drying method.

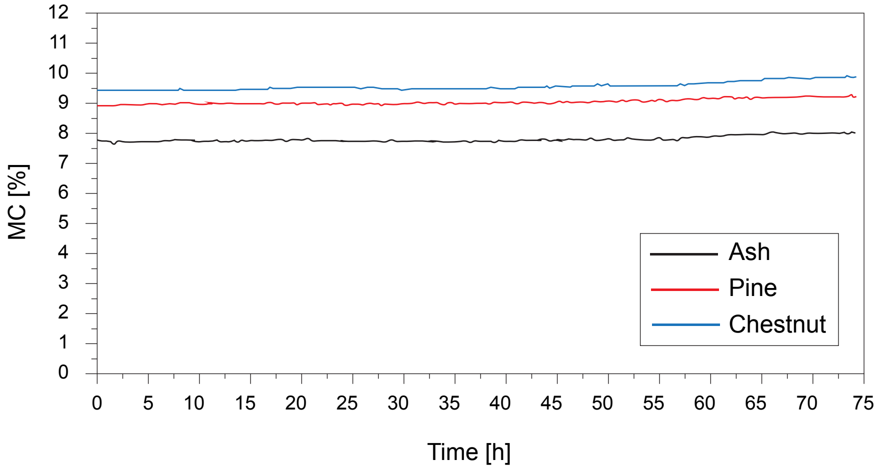


Figure 4.9: MC measured during 3 days under ambient conditions for pine, ash and chestnut wood species.

Nine timber pieces from three different species were tested: three pieces of Oregon Pine (Pseudotsuga Menziesii), three pieces of European Ash (Fraxinus Excelsior), and three pieces of Chestnut Tree (Castanea Sativa). To ensure that the timber pieces had varying MC levels, they were soaked in water for 24 hours and then stored in the laboratory for 2 days to allow the MC to stabilize. Four measurements were then taken, with a two-day interval between each measurement, to observe the gradual reduction of the MC. Before each measurement, the weight of the timber pieces (m_w) was recorded. The MC measurement was then taken using the developed system. Finally, the timber pieces were dried in an oven for five days at $103 \pm 2\ °C$ and their final weight (m_0) was recorded. The MC value obtained through this process (MC_{OD}) was calculated as follows:

$$MC_{OD}(\%) = \frac{m_w - m_0}{m_0} \times 100 \tag{4.7}$$

A Mettler AE200 precision balance was used to weigh the timber pieces and a Memmert UFP400 oven was utilized in the testing process. The results obtained are summarized in Table 4.3, where MC_{OD} (%) represents the MC obtained through the oven-drying method, while MC_E (%) represents the MC obtained using the LoRa-based monitoring system. The difference in MC between the two methods, represented by ε_{abs}, is also indicated in the table. The results show that ε_{abs} ranges from 0.1 to 1.7, demonstrating the accuracy of the proposed LoRa-based monitoring system.

Table 4.3: Experimental MC measurement comparison using the oven-drying method (MC_{OD}) and the LoRa-based monitoring system (MC_E) and its MC absolute error (ε_{abs}).

	MC_{OD}(%)	MC_E(%)	ε_{abs}	MC_{OD}(%)	MC_E(%)	ε_{abs}	MC_{OD}(%)	MC_E(%)	ε_{abs}	MC_{OD}(%)	MC_E(%)	ε_{abs}
1 Ash	21,3	19,8	1,5	10,9	11,4	1,0	10,6	12,0	0,7	10,6	11,1	0,5
2 Ash	20,6	20,1	0,4	11,8	12,0	0,8	11,1	12,6	0,8	11,0	11,6	0,6
3 Ash	21,3	20,0	1,3	10,9	11,6	1,5	10,6	12,5	1,0	10,6	11,4	0,9
1 Pine	19,2	19,7	0,5	12,0	12,9	1,5	11,9	13,5	1,0	11,9	12,6	0,7
2 Pine	19,8	19,6	0,1	12,2	12,9	1,3	12,0	13,5	0,9	12,0	12,5	0,5
3 Pine	19,9	19,8	0,1	12,6	13,3	1,3	12,3	13,8	0,9	12,3	12,8	0,5
1 Chestnut	25,6	24,0	1,6	12,9	13,7	1,7	12,1	14,6	1,6	15,5	13,8	1,7
2 Chestnut	26,1	24,4	1,7	13,1	13,5	1,5	12,5	14,7	1,0	12,4	13,1	0,6
3 Chestnut	25,8	24,4	1,4	13,4	14,0	1,5	12,9	14,9	1,1	12,7	13,5	0,7
	Day 1			Day 3			Day 5			Day 7		

4.4 Path-Loss Evaluation in LoRa communication

The proposed moisture device leverages the capabilities of LoRaWAN wireless protocols, with a focus on its ability to transmit data over long distances. Extensive research has been conducted on the performance of LoRa and LoRaWAN in both outdoor and indoor environments [218–220], including studies that have explored the propagation of LoRa signals inside buildings. The following configuration was employed for the end-node devices:

1. LoRa Class: Class A.
2. Transmitting Antenna gain: +2 dB.
3. Receiving Antenna gain: +2 dB.
4. Frequency: 867.1–868.5 MHz.
5. Bandwidth size: 125 kHz.
6. Spreading Factor (SF): 7.
7. Coding Rate: fixed = 4/5.
8. Transmitting Power: +14 dB.

In the subsequent experimental test, the Spreading Factor (SF) was fixed at 7 and the bandwidth at 125 kHz in order to assess the farthest distances the MC device could reach while transmitting packets with the minimum possible energy. However, in similar applications, it is advisable not to fix the SF and instead utilize the Adaptive Data Rate (ADR) mechanism to optimize data rates, airtime, and power consumption, thus enhancing the range and network capacity within different structures.

The Path Loss parameter (PL) characterizes the Large-Scale Fading (LSF). Modeling signal propagation is a crucial aspect in certain applications, such as a Wireless Sensor Network location system. The ratio of the received power (P_r) to the transmitted power (P_t) in a free space environment is given by the Friis law, which represents the relationship between these values

$$\frac{P_r}{P_t} = G_t G_r (\frac{\lambda}{4\pi d})^2. \tag{4.8}$$

where G_t and G_r are the gains of the transmitter and the receiver, respectively; λ is the wave length, and d is the distance between the transmitter and the receiver.
For non-free space environment, a path loss exponent γ and a reference distance are introduced. Then, (4.8) becomes:

$$\frac{P_r}{P_t} = G_t G_r (\frac{\lambda}{4\pi})^2 \times \frac{1}{d_0^\gamma} \times (\frac{d_0}{d})^\gamma. \tag{4.9}$$

The Path Loss (PL) can be estimated through a first-order fit [221] by modeling the experimental PL. The Estimated Path Loss (EPL) can then be obtained as follows:

$$EPL = PL_0 + 10 \times \gamma \times log_{10}(\frac{d}{d_0}). \tag{4.10}$$

Where PL_0 is the PL intercept at the reference distance d_0, which is determined through measurements in microcellular systems and typically ranges between 1 m and 100 m. In this study, we set d_0 to 1 m. The PL exponent, represented by γ, indicates the nature of the propagation environment and can be estimated from measurement results. There are several algorithms available in the literature to estimate the exponent value, such as the one presented by Wojcicki [222]. In a free-space environment, γ is typically equal to 2. In urban environments, γ varies between 2.7 and 3.5, while in building environments, it varies between 1.6 and 6, depending on factors such as the building structure, construction material, and obstacles [223].
The difference between the actual Path Loss (PL) and the Estimated Path Loss (EPL) arises due to shadow fading deviation.

$$\sigma_{SF} = std(PL - EPL). \tag{4.11}$$

The Path Loss (PL) has been evaluated in both outdoor and indoor environments based on the measured Received Signal Strength (RSSI) and signal-to-noise ratio (SNR) using equation (4.12) [224], where P_{Tx} is the transmission power, G_{Tx} and G_{Rx} are the gains of the transmitting and receiving antennas respectively.

$$PL = P_{Tx} + G_{Tx} + G_{Rx} + 10 \times \log_{10}(1 + \frac{1}{SNR}) - RSSI. \tag{4.12}$$

The Received Packet Percentage (RPP) was calculated at each location using equation (4.13), where NACK represents the number of packets acknowledged and NAP represents the total number of transmitted packets:

$$RPP[\%] = 100 \times \frac{NACK}{NAP}. \tag{4.13}$$

In this experiment, measurement points with an RPP below 50% were disregarded. The collected data, along with the superimposed Path Loss (PL) measurements and the model parameters in equation (4.10), were compared to the Free-Space Path Loss (FSPL). This experiment was carried out in the center of Valencia, Spain. As depicted in Figure 4.10 (b), the LoRa gateway receiver was located on the roof of a ten-floor building (approximately 40 meters above ground level). The gateway was powered and connected to the internet through an Ethernet cable.

Figure 4.10(a) is a screenshot from the TTN website that shows the active gateways at the time of the test. In order to minimize interference from other LoRa gateways in the area, all measurement points were positioned in the southeast to ensure that the packets would be received by our gateway. The measurement points are represented by the letter "P" in Figure 4.10(c), and the red point "G" refers to the gateway. At each location, ten messages were sent that included the temperature value and period T, with 2 bytes reserved for the temperature and 6 bytes for the period in the payload. Table 4.4 describes the distance between the LoRa gateway and the measurement locations and the RPP rate. Figure 4.11 respresents the RSSI and SNR values.

The collected data with superimposed Path Loss (PL) measurements, calculated using equation (4.12), are presented in Figure 4.12. The parameters of the Estimated Path Loss (EPL) model are outlined in Table 4.5. The results are compared with the Free-Space Path Loss (FSPL) model. As the distance increases, the proposed EPL model appears to be more accurate. At distances shorter than 60 m, the model may not be reliable due to the influence of shadow fading, which can impact the propagation of signals at smaller distances, depending on the position of the end-node relative to the transmitter [224].

The significance of studying Path Loss (PL) lies in its ability to shed light on how the strength of a LoRa signal decreases as it travels through different environments. This knowledge is essential for accurately predicting the range of a LoRa network and for designing effective communication systems. The reduction in the strength of a signal as it travels through a medium can be attributed to various factors, such as the type of environment, the distance between the transmitter and receiver, and the frequency of the signal. Modeling the PL helps in understanding the impact of these factors on the signal strength and in turn enables better placement of end-nodes

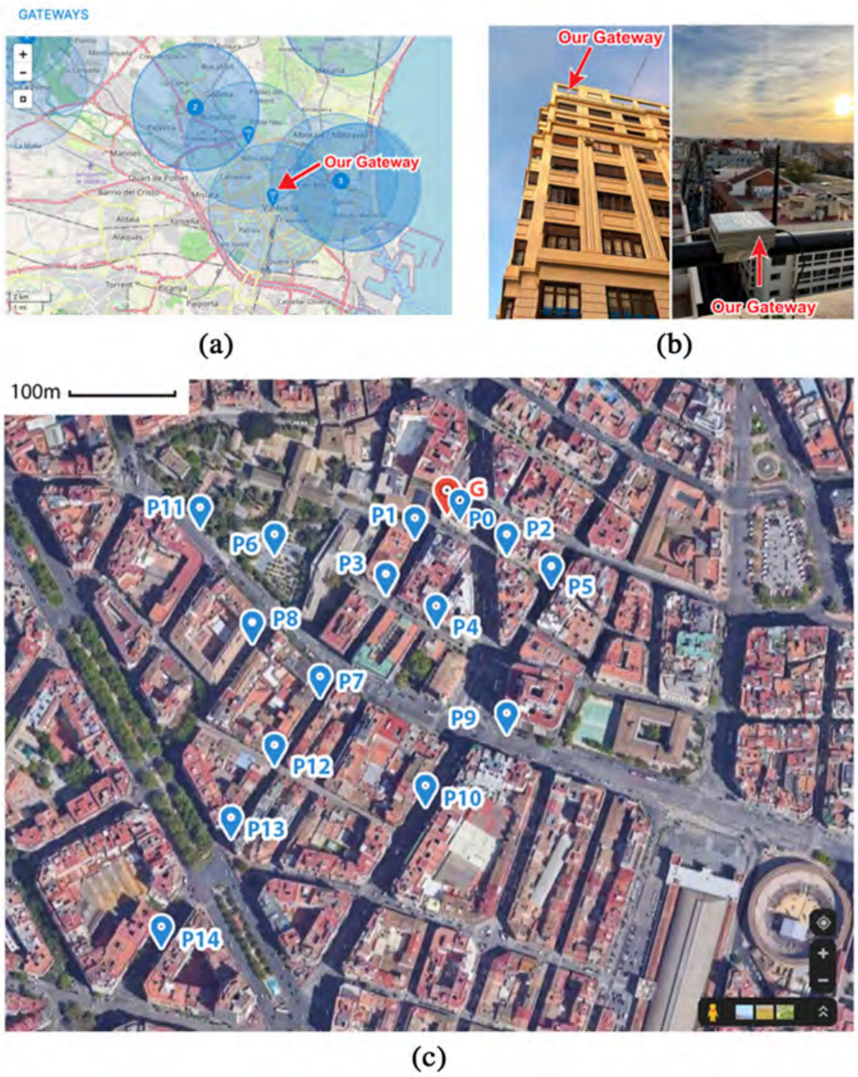


Figure 4.10: Experimental setup for outdoor LoRa communication tests. (a): Screenshot from the TTN website showing the location of the active gateways in the test area. (b): LoRa gateway setup in a highly populated area. (c): P0 to P14 represent the measurement locations, G represent the gateway location.

Table 4.4: Percentage of received packets RPP from each measurement point in the outdoor LoRa communication test

Point	Distance (m)	RPP (%)
PR	1	100
P0	5	100
P1	52	100
P2	72	100
P3	89	100
P4	117	90
P5	127	100
P6	160	90
P7	196	100
P8	202	100
P9	212	80
P10	265	60
P11	287	60
P12	290	70
P13	390	60
P14	503	60

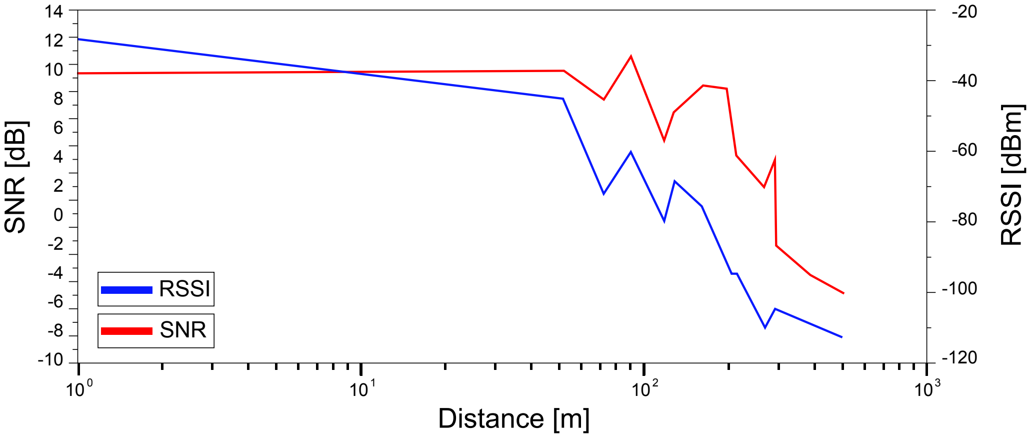


Figure 4.11: LoRa communication parameter values: Average RSSI [dBm] and Average SNR [dB] as a function of distance [m].

and identification of potential issues with a LoRa network, thereby facilitating ways to enhance its performance.

4.5 Discussion

This chapter presented the development of a wood moisture content (MC) IoT device. The MC LoRa device features a novel, battery-operated electronic board

Table 4.5: Lognormal PL Model parameters in the outdoor environment.

EPL exponent (γ)	3.2
EPL intercept (PL(d_0))	40.82 dB
Standard deviation (σ_{SF})	5.6

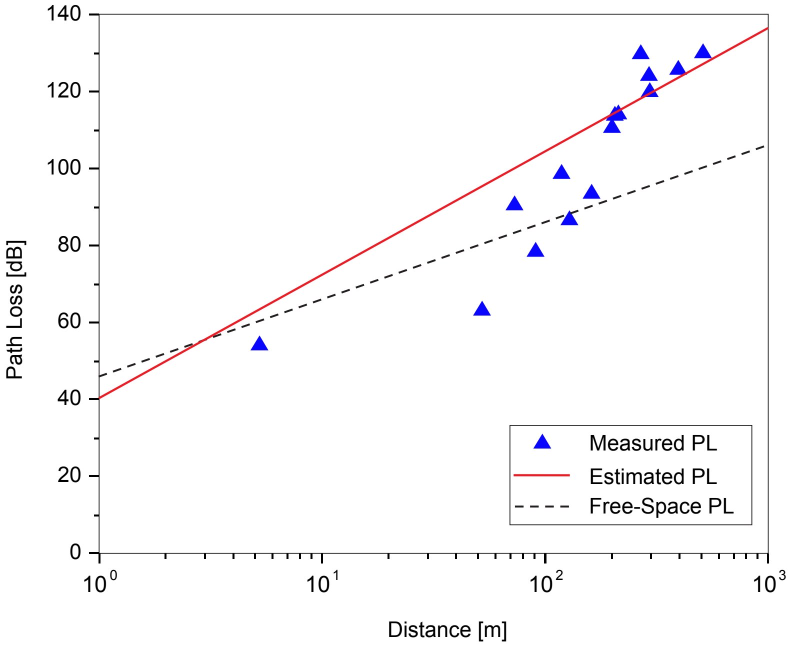


Figure 4.12: Estimated and measured PL compared with the FS model in urban environment.

with an AC-based measurement method that utilizes a relaxation oscillator. The frequency of the oscillator is automatically tuned based on the resistance of the wood, which is directly correlated to the MC. The results of the experiments indicate that the developed system has a maximum MC difference of ±1.7 compared to the oven-drying method. The LoRa end-node is capable of functioning in a temperature range of 0 °C to 50 °C with different types of wood, and has stable measurements over extended periods of time. The device can transmit data up to 430 meters. The micro-controller on the end-node is programmed to wake up the device, activate the MC sensing circuitry, take the average of ten measurement values, and send the data to the gateway. The device then enters sleep mode until the next measurement time. This operation mode minimizes power consumption and ensures long battery life.

The developed sensor will play a crucial role in deploying an IoT system for moisture content monitoring inside cultural heritage wooden buildings. The system is described in the next chapter and is aimed to serve as a support tool for building maintenance services, specifically for those made of timber. The IoT system will utilize the LoRa and LoRaWAN wireless protocols to cover all aspects of the sensing process, from the end-nodes to a newly developed web application. The system is capable of providing accurate and stable measurements.

Chapter 5

Deployment of IoT Applications and Blockchain Integration

> *"It is always seems impossible until it's done."*
>
> - Nelson Mandela

This chapter describes the deployment of four different IoT monitoring systems done in this thesis.

5.1 Application 1: Wood Moisture monitoring system based on BLE

Wood is a common material used in the construction of buildings, furniture, and many other applications. One of the most important factors affecting its properties is moisture content. The amount of water contained within wood can significantly impact its weight and strength, making it weaker and more susceptible to biological attacks [225]. Therefore, monitoring the moisture content of wood is crucial for forecasting and preventing damages, particularly in old buildings where timber has been exposed to changing environmental conditions over time. Traditionally, measurements of moisture content have been done manually using large devices that require human interaction. However, a monitoring IoT system based on Bluetooth Low Energy (BLE) represents a good solution for early detection of wood moisture due to heavy rain, leaks, and other factors. This section presents an IoT system based on BLE for detecting moisture content, which could greatly improve the accuracy and efficiency of monitoring wood in various applications.

To implement the proposed IoT system for detecting moisture content in wood, the previously developed BLE moisture sensor is used as an end-node, which was described in section 3. The sensor will be placed in various locations throughout the building to provide continuous and accurate measurements of moisture content.

5.1.1 Architecture of the Monitoring System

Figure 5.1 illustrates the proposed monitoring system. It consists of a cloud server hosting a monitoring web application for data visualization and control. The cloud server will receive data from the sensors through a raspberry pi acting as the gateway between the BLE end nodes and the cloud server database.

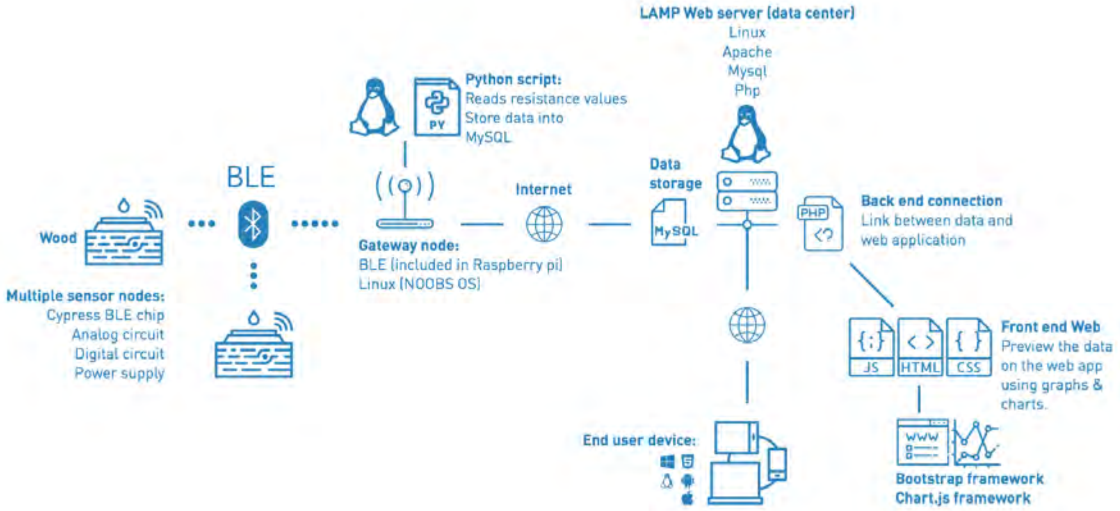


Figure 5.1: Project diagram: sensors transmit moisture measurements via BLE to the gateway, which then sends the data to a remote server via the internet for storage in its database. The user interface is connected to the database, enabling users to monitor and control the sensor nodes easily.

This architecture will ensure that the data is transmitted securely and efficiently to the cloud server, where it can be analyzed and interpreted to provide insights on the moisture content of the wood. With this IoT system, it will be possible to detect and prevent moisture-related damages, preserving the structural integrity of buildings and other wooden structures. The gateway is equipped with Python scripting for BLE communication, data analysis, and Ethernet data exchange with the server. To host the web application, a remote server was configured with LAMP (Linux, Apache, MySQL, and PHP) software. This ensures reliable and efficient data management and allows for easy updates to the system as needed.

The diagram can be divided into two main sections. The first section comprises the BLE sensor nodes and the gateway. A Raspberry Pi 3 is used as the gateway, which sends system commands to the sensor nodes and receives data from them. The gateway then converts the data into float values and writes it into the server's database via the HTTP protocol. A Python script is used in the gateway to wake up each BLE device and send new values according to the user-defined time period, which is set in the configuration page of the web application. This script also performs error detection on the data before sending it to the cloud server and checks the connection between the gateway and the sensor nodes. If the connection is lost, an error message is sent to the server and the user is notified. As the developed system is intended for indoor use, it is capable of handling a small number of devices due to the limited range of communication. The actual gateways have a RAM memory of 1GB LPDDR2 (900 MHz), which is sufficient to handle the connected sensor nodes in the local network, taking into consideration that the sensor nodes do not send data continuously. Therefore, there are no expected memory limitations. The second section of the diagram consists of the cloud server and the web application. The cloud server is built on the Apache web server environment, which uses MySQL database management. This environment is based on a multi-process (MP) architecture that spawns several processes to support multiple clients [226]. The web application is developed using Laravel PHP framework. Users can access the data without any limitations and use it anytime, anywhere.

5.1.2 Monitoring Web Application

5.1.2.1 UML diagram

To represent the web application, an object-oriented modeling diagram will be utilized. Modeling is an essential component of the software development process, and the Unified Modeling Language (UML) was chosen as the modeling tool to describe the system's structure, as shown in Figure 5.2.
In the system, the user assumes the role of a parent administrator. The user has the ability to create a new network and add, update, or remove gateways and devices from it. The user can also monitor the data and export it into an Excel or CSV file, which simplifies data analysis. In contrast, the administrator role can add, update, and delete users, as well as manage their networks.

5.1.2.2 Database

The database design is represented by the EER (Enhanced Entity-Relationship) diagram in Figure 5.3. The database consists of six tables: 'Users', 'Devices', 'Notifications', 'Roles', 'Datos', 'Password_reset', and two pivot tables: 'Role_user' and 'Device_user'. The 'Users' table contains user roles, such as administrator or user. Each user has associated gateways and devices, and the data received from each device is stored in the 'Datos' table. The 'Notifications' table stores the notifications generated by the application when a device receives a value outside the range specified by the user.

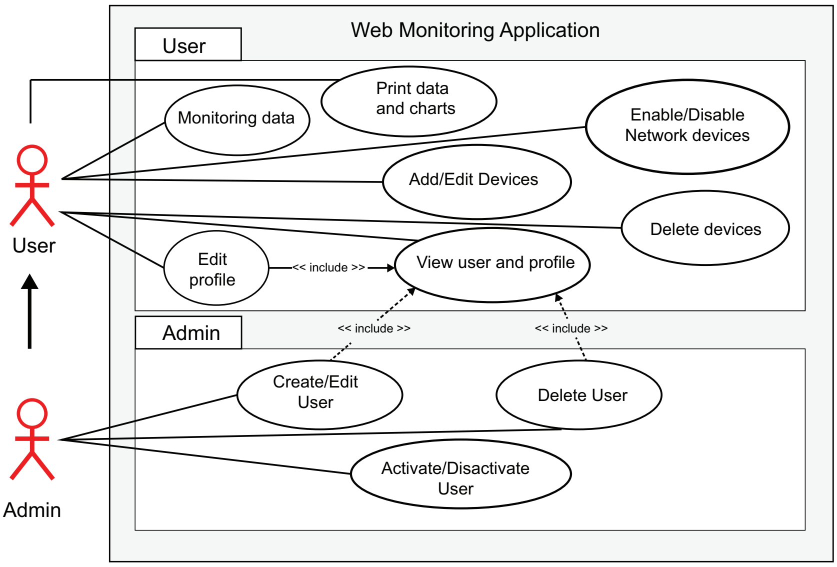


Figure 5.2: Project diagram: sensors transmit moisture measurements via BLE to the gateway, which then sends the data to a remote server via the internet for storage in its database. The user interface is connected to the database, enabling users to monitor and control the sensor nodes easily.

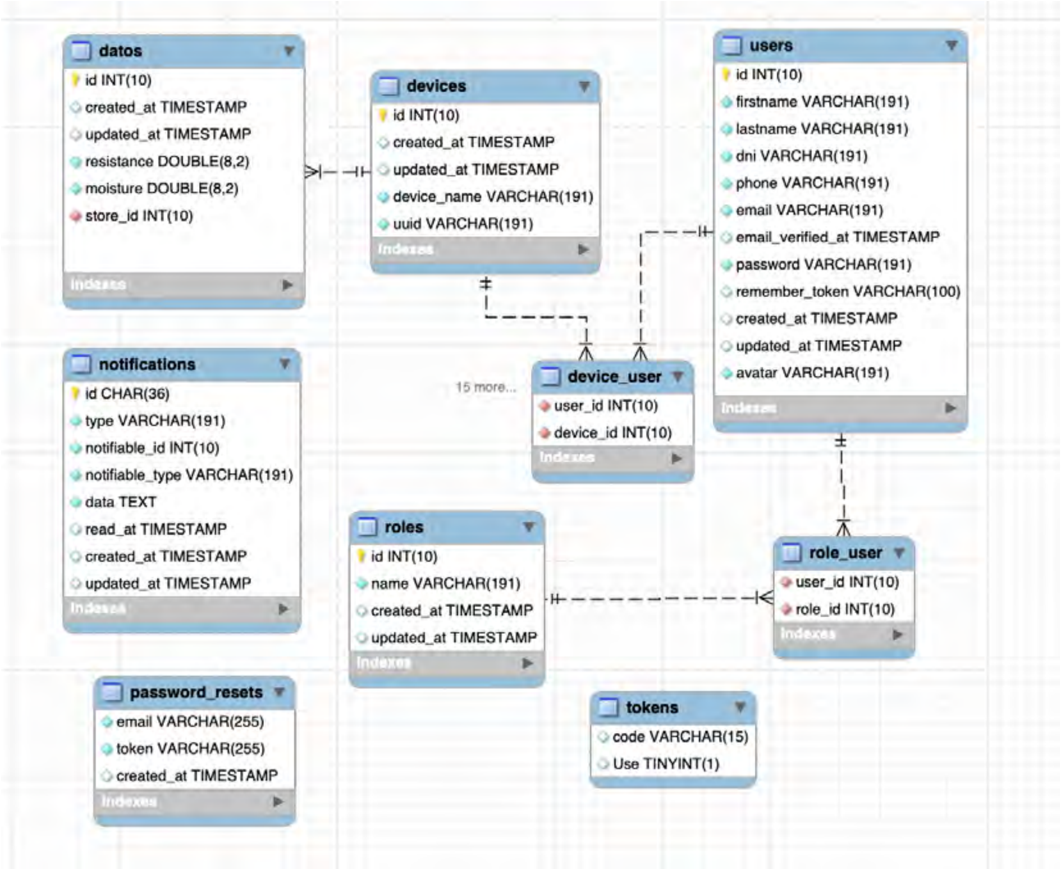
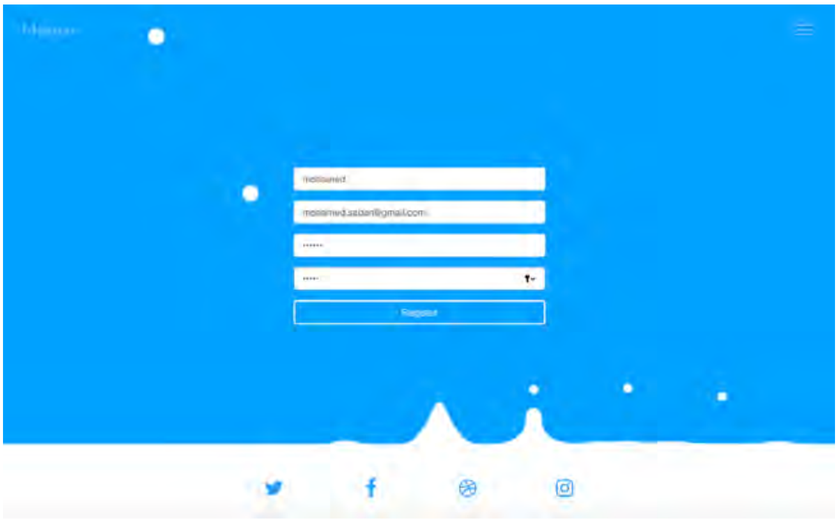


Figure 5.3: Web application Database design represented by EER diagram.

5.1.2.3 User Interface

The Twitter Bootstrap framework was used to develop the web application's front-end. This framework provides a set of JavaScript functions and CSS classes that simplify the front-end development process. Additionally, this framework provides a responsive design that supports a variety of mobile devices, as well as tablet and desktop interfaces [227]. Figure 5.4 illustrates the Register page where the user can create his account by entering his name, email and password. More fields can be added for the registration process if needed. Figure 5.5presents a screenshot of the dashboard user interface of the web application.



mohamed

mohamed.saban@gmail.com

••••••

•••••

Figure 5.4: Web application register page, the new user should fill the name, email and password labels.

The web application consists of five menus: 'Home', 'Setting', 'Dashboard', 'Profile', and 'Notifications'. The home page displays the user's networks and associated devices, including gateways and sensor nodes. Clicking on a device redirects the user to its dashboard page, where they can view data charts and export them. The setting page allows users to add new devices, edit, delete, and activate or deactivate devices. Additionally, users can set limit values for each device, and the application will generate a notification if the received data falls out of the specified range. Notifications are shown on the user profile page and sent via email using the simple mail transfer protocol (SMTP) protocol [228]. The profile page enables users to update their data, and the notifications page displays all notifications received.

5.1.3 Experimental test

In order to ensure the system's functionality, a benchmark experiment was conducted with two primary objectives: testing the flexibility, performance, and speed of the web application, as well as assessing its ability to adapt to the BLE device. As

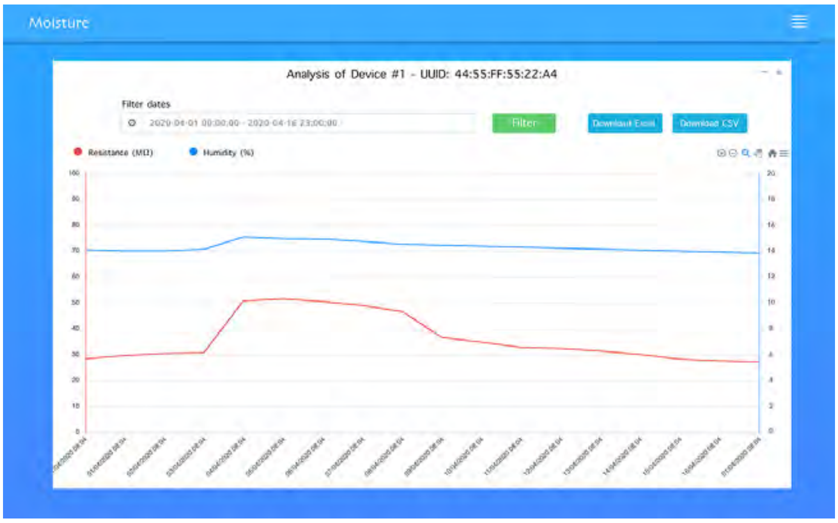


Figure 5.5: Web application device dashboard page showing the chart of moisture and resistance in function of time, the user can filter data by date and download it as Excel or CSV file.

described in Figure 5.6 The BLE device is powered at 5 V and connected to the gateway via Bluetooth Low Energy. Once received, the gateway converts the values and writes them to the cloud server database. To compare results, the moisture meter 'Lutron MS-7000' was used to simultaneously measure moisture content. The moisture content of the wood is measured using a 2-pin electrode.

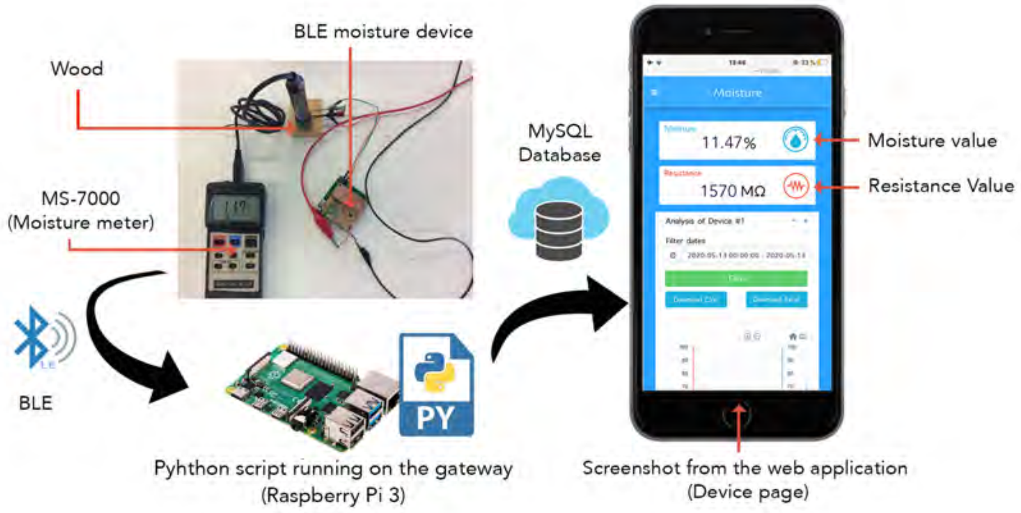


Figure 5.6: Test bench used to check the functionality of the system. The BLE device is connected to a Raspberry Pi 3 through BLE. The Raspberry receives the values, convert them to float and write them into the server database. The user can check the last stored values through the web application.

In order to measure the maximum transmission distance allowing the BLE sensor to send and receive data corrrectly from the gateway in an indoor environment, the sensor was placed in different position along the pathway of the department of Electronic Engineering at the engineering school ETSE in Valencia. Figure 5.7 illustrate the department plan where the gateway was located within our laboratory while the BLE sensor is positioned at various locations denoted as P1 to P5. The distance between the measurement positions of the BLE node and the gateway, the received signal strength indication (RSSI), and the signal quality are provided in Table 5.1. The results presented in this table were obtained using the 'CYSMART BLE Test and Debug Utility' software developed by Cypress, which was utilized to transmit data and obtain the aforementioned results.

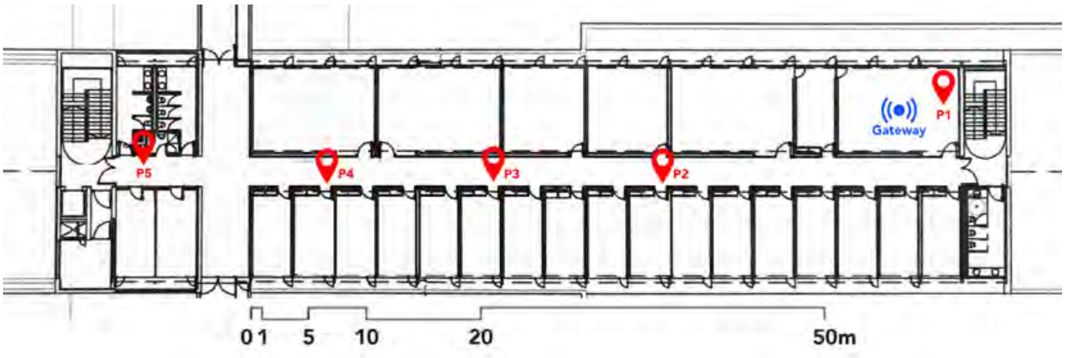


Figure 5.7: Test bench used to check the functionality of the system. The BLE device is connected to a Raspberry Pi 3 through BLE. The Raspberry receives the values, convert them to float and write them into the server database. The user can check the last stored values through the web application.

Table 5.1: The distances between the measurement positions and the gateway, the average RSSI [dBm], and the signal quality.

Measurement Positions	Distance (m)	RSSI (dBm)	Signal Quality (%)
P1	4	-34	100
P2	22.2	-55	87
P3	38.5	-72	56
P4	53.6	-80	43
P5	71	-92	13

Based on the results of our test, it has been demonstrated that the BLE sensor node is capable of transmitting data up to a distance of 71 meters, without the need for any additional power amplification. However, it should be noted that low signal quality may lead to a lack of data reception, as seen at position P5 which represents the furthest point where data could be transmitted and received accurately. In fact, any signal that exceeds -92 dBm is considered unusable.

It is important to take into account the blocking effects of walls and obstacles between the gateway and sensor nodes, as these may impact the performance of the system. As such, it is recommended to evaluate the blocking effects prior to deployment, in order to determine the optimal placement of sensor nodes and ensure reliable and robust coverage for the IoT network. By doing so, a more efficient and effective system can be achieved.

5.1.4 Conclusion

The presented BLE monitoring system is highly versatile and can be implemented in a variety of settings and it offers a more energy-efficient and practical solution for wood moisture measurement. This system offers numerous strengths, which include:

- Cost-effectiveness: The fabrication of the BLE sensor circuit is not expensive, resulting in a significantly cheaper final product compared to manual alternatives. The gateway employed is a Raspberry Pi, which is also affordable at around 30€.
- Central topology: The use of a central server to manage all transmitted data enables a lower hardware and support cost. This architecture is faster to deploy and easier to manage due to the simplified messaging structure, eliminating the need for coordination among distant sites. This topology allows for the deployment of a large number of BLE devices and gateways, thereby enabling a high volume of users to access the same server and web application.
- Local data storage: Data is stored locally in the gateway's internal memory before being sent to the cloud server. This feature ensures that measured values are not lost in case of connection failure between the gateway and the server.
- Notifications: Users receive notifications if the measured moisture value falls outside of the previously specified range. They are also notified of any connection failures between the devices, the gateway, or the server.
- Authentication system: The system ensures the security of user data by protecting all routes that lead to it. Only authorized personnel can access their accounts to add or remove devices and monitor their data.
- UI/UX design: The web application boasts a beautiful and easy-to-use user interface design that prioritizes the user experience (UX). The design is responsive and functions seamlessly across all devices and web browsers.

The presented sensor exhibited outstanding performance in accurately measuring resistance values, converting it to moisture content and sending them to the cloud server for visualization. However, during testing, it was observed that the maximum transmission distance achieved was only 71 meters. This presents a challenge for larger buildings, as additional gateways would be required for successful transmission of data. To address this issue, selecting a long-range protocol can be an effective solution, particularly in historical buildings such as old churches and museums.

5.2 Application 2: Wood Moisture system based on LoRa

The previous application discussed an IoT system based on BLE for monitoring moisture content in wood, which demonstrated excellent performance in detecting and transmitting data. However, its limited transmission range of only 70 meters makes it less practical for larger wooden structures such as heritage buildings, where moisture control is crucial. To address this issue, the present system implements a new monitoring system using long-range LoRa technology.

Cultural heritage sites hold immeasurable value throughout the world, serving as vital links to the past and important sources of inspiration for future generations. However, the preservation of cultural heritage structures, including historical buildings, poses significant challenges due to their exposure to numerous natural and human-made risks. Timber has been a common construction material for centuries, and as such, monitoring its Moisture Content (MC) is essential for preventing potential damages, particularly in older buildings that have been subjected to environmental changes over time. Accurately monitoring the moisture content of wood in historical buildings can help to identify potential risks and enable timely action to preserve their structural integrity, safeguarding these important cultural artifacts for future generations.

The new LoRa system is composed of the previously developed moisture sensor in Section 4, one LoRaWAN gateway, and a cloud server hosting a web monitoring application. A new web application was developed from scratch using the Laravel framework and HTML, as well as Vue JS software.

5.2.1 System architecture

The proposed LoRa system architecture for moisture wood sensors typically consists of the moisture wood sensors, LoRaWAN gateway, and a cloud server hosting a web application for data analysis and visualization as illustrated in Figure 5.8.

The system uses the WiMOD LoRa Lite Gateway, which is composed basically of a Raspberry Pi and an iC880A connector. The Things Network (TTN) is used as platform for LoRaWAN communication. TTN V3 uses Join Servers that securely store LoRaWAN keys and issue session keys to both the Network Server

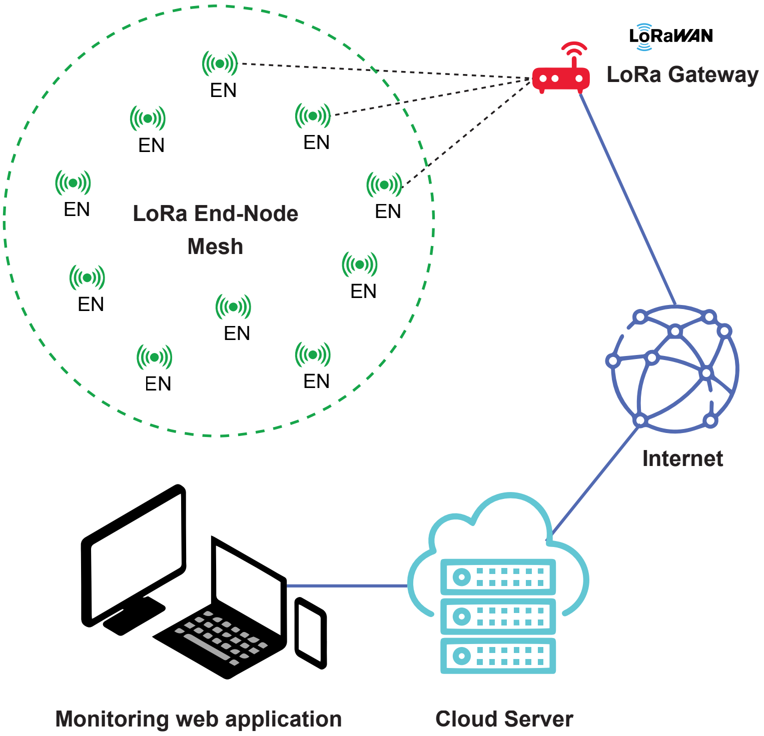


Figure 5.8: The LoRa monitoring system consists of a Cloud server hosting the monitoring web-page, a LoRaWan gateway and the LoRa moisture sensors

and Application Server. This approach separates secure storage from packet routing, enabling users to host Join Servers on-premises and use hardware secure modules (HSMs) to have full control over security keys [229, 230].

The wood moisture devices are responsible for sensing moisture levels in the wood and transmitting this data wirelessly to the LoRaWAN gateway. The LoRaWAN gateway acts as a bridge between the sensors and the TTN network, which receives and processes the data from multiple gateways. TTN will forward the received data directly to the cloud server. The end-node devices were configured as follows:

- LoRa Class: Class A
- Bandwidth size: 125 kHz
- Frequency: 867.1–868.5 MHz
- Spreading Factor (SF): 7
- Transmitting Power: +14 dB
- Coding Rate: Fixed at 4/5
- Transmitting Antenna gain: +2 dB
- Receiving Antenna gain: +2 dB

The proposed LoRa system architecture provides a reliable, low-power, and long-range communication solution for moisture wood sensors, enabling efficient monitoring and management of wood moisture levels in various applications.

5.2.2 Application in the field: Indoor test in a heritage building

This experimental test was carried out at the Cultural Centre 'La Nau', a historically significant building that has served as the University of Valencia's headquarters since its establishment in the 15th century until the first half of the 20th century.

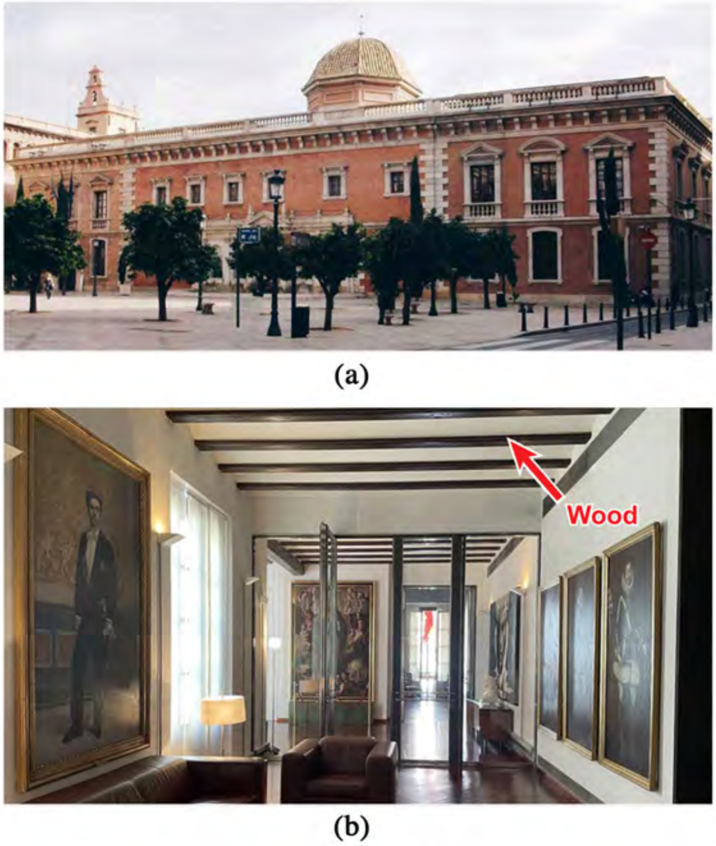


Figure 5.9: Cultural Centre 'La Nau' where the LoRa monitoring system was installed: (a) outside view of the building, (b) roofs inside the building are made of wood.

With its last significant restoration completed in 1830 and its declaration as an Asset of Cultural Interest in 1981, the building stands as a testament to the region's rich cultural heritage [231]. The external facade of the building is depicted in Figure 5.9(a). The building has a constructed area of 2900 m^2, with most of its roofs made of wood, making it essential to monitor wood conditions, particularly moisture content, as shown in Figure 5.9(b). This monitoring helps to ensure the preservation of the building, preventing problems such as water leaks and biological attacks. In order to study the connectivity and the path loss inside the historical building, one LoRa moisture device was connected to 100 MΩ ±1 % resistor to read the resistance value, and it was placed in 15 distinct locations, both inside and outside the building. The LoRa gateway was situated in a fixed indoor position Figure 5.10 illustrates the floor plan of the La Nau building, including the gateway and measurement point locations. P0 signifies the gateway location on the ground floor. The red points indicate measurement locations on the ground floor, blue points signify measurement locations on the first floor, and orange points depict outdoor measurement locations on the ground floor.

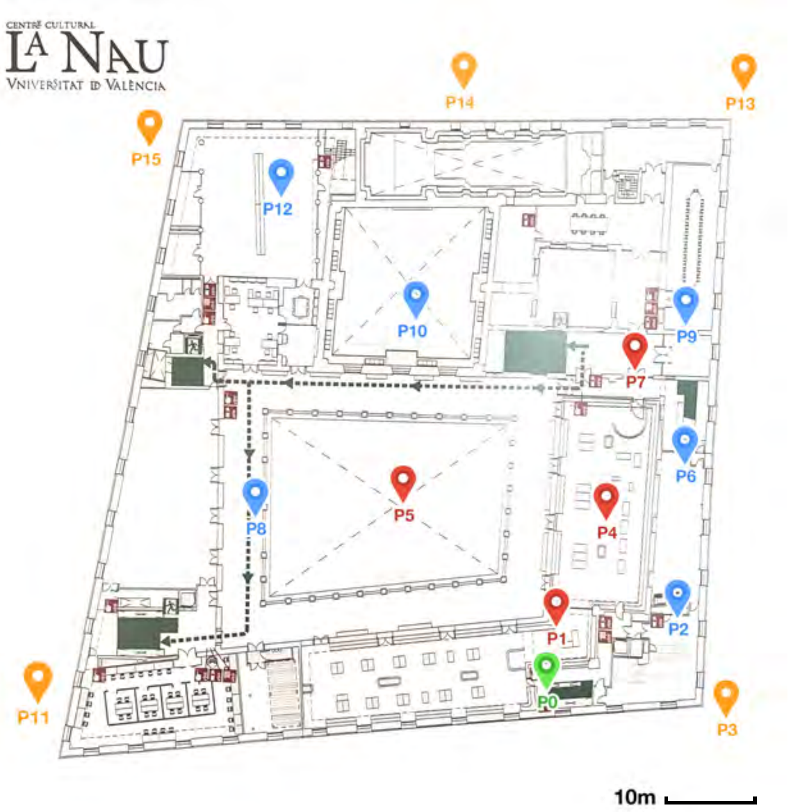


Figure 5.10: Plan of the cultural Centre La Nau showing the position of the gateway (P0) and the location of different measurement points (P1 to P15) where the LoRa MC end-nodes were located. Red, blue and orange colors refer to the ground floor, first floor and grand floor, but outdoors, respectively.

Ten messages were sent containing the temperature value and the corresponding wood resistance period. When the gateway receives the payload, it transmits the following information to the cloud server: transmitting time, end-node device EUI (identification number), base station EUI, decrypted payload, temperature value, wood oscillation period T, frequency band, data rate spreading factor, bandwidth.

In Figure 5.11, the average RSSI and SNR values are shown for each measurement point. The LoRa SNR values typically range from -20 dB to +10 dB, with a value closer to +10 dB indicating less signal corruption. The SNR values in all measurement points ranged from 6.8 dB to 12 dB and were positive, while the RSSI values did not follow a similar trend. The RSSI decreased to -101 dBm at P12, where the first packet loss occurred, due to the high density of the building materials that hindered the propagation of LoRa radio waves when the end-node and gateway were indoors. This had a significant impact on RSSI, emphasizing the importance of using an external end-node antenna in such cases.

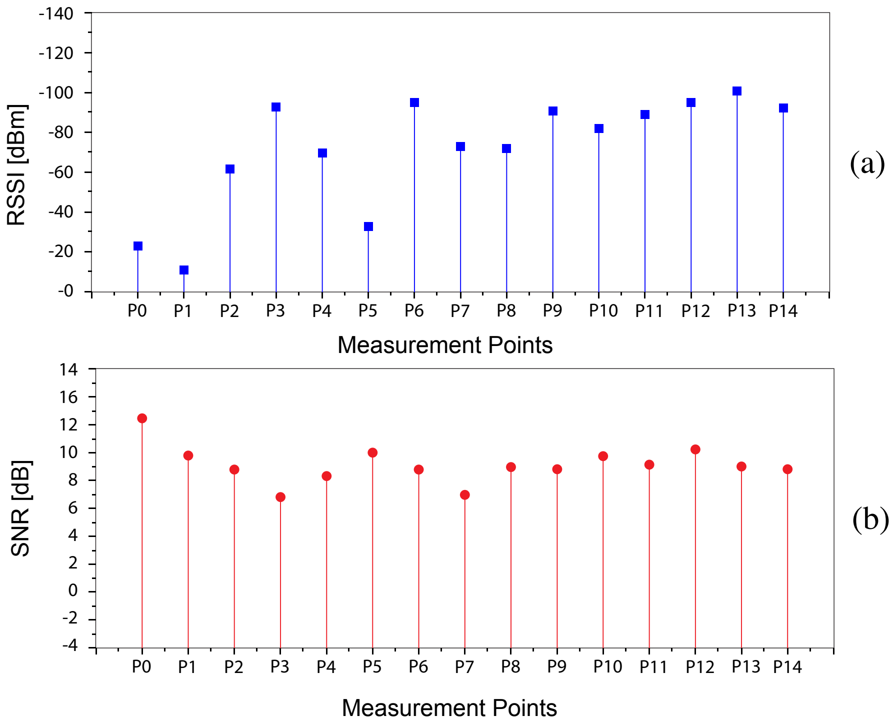


Figure 5.11: LoRa communication analysis results in the heritage building: average RSSI [dBm] (a) and average SNR [dB](b) measured in 15 points in the building.

When dealing with indoor propagation of LoRa signals, there are typically obstacles such as walls, soft partitions, and floors that obstruct the path between the gateway and end-nodes. To create a more accurate model, it is necessary to consider the path loss effects of these obstructions. Previous works such as [232] and [233] have achieved this by incorporating the attenuation factors of floors, soft partitions, and walls into their prediction models. In this approach, the model is simplified by considering any obstacle that partially or totally blocks the direct path between the gateway and end-node as a concrete wall. The path loss predicted by the attenuation factor model can be estimated as follows:

$$EPL = PL_0 + 10 \times \gamma \times log_{10}(\frac{d}{d_0}) + a \times FAF + b \times WAF. \tag{5.1}$$

where FAF is the floor attenuation factor, WAF is the attenuation factor of a concrete wall, a is the number of floors and b represents the number of walls. The distance between the gateway and each measurement point, along with the number of walls and floors in the path are presented in Table 5.2. Results shows that 100 % of packets were received from all the measurement points.

Table 5.2: Distance, number of walls, number of floors and RPP corresponding to each measurement point inside the historical building

Point	**Distance (m)**	**Walls**	**Floors**	**RPP (%)**
P0	1.00	0	0	100
P1	4.90	1	0	100
P2	14.95	2	1	100
P3	19.55	1	0	100
P4	21.40	2	0	100
P5	25.40	2	0	100
P6	29.70	3	1	100
P7	35.25	3	0	100
P8	39.00	2	1	100
P9	40.50	3	1	100
P10	45.90	3	1	100
P11	54.10	3	0	100
P12	61.40	4	1	90
P13	67.25	4	0	100
P14	70.60	4	0	100
P15	77.00	4	0	100

To calculate the attenuation factors, a drive test was conducted where the PL was measured with a wall or floor separating the gateway and end-node, and then again without the obstruction while keeping the same separation distance. The difference in PL between these measurements represents the attenuation factor of the obstruction. This process was repeated at various locations in the building, and the final results were obtained by calculating the mean of these tests. The EPL parameters of the indoor environment, FAF, and WAF are shown in Table 5.3.
Figure 5.12 depicts the collected data with superimposed path loss (PL) measurements calculated using equation (4.12), as well as the estimated PL calculated using Equation 5.1. These results are compared with the free-space path loss (FSPL) model.

Figure 5.12 demonstrates that the measured PL at the gateway aligns closely with the proposed model. Thus, the Equation 5.1 is an adequate representation of LoRa

Table 5.3: Lognormal PL Model parameters in the indoor environment.

EPL exponent (γ)	2.9
EPL intercept (PL(d_0))	41.34 dB
Standard deviation (σ_{SF})	6.7
FAF	20 dB
WAF	2 dB

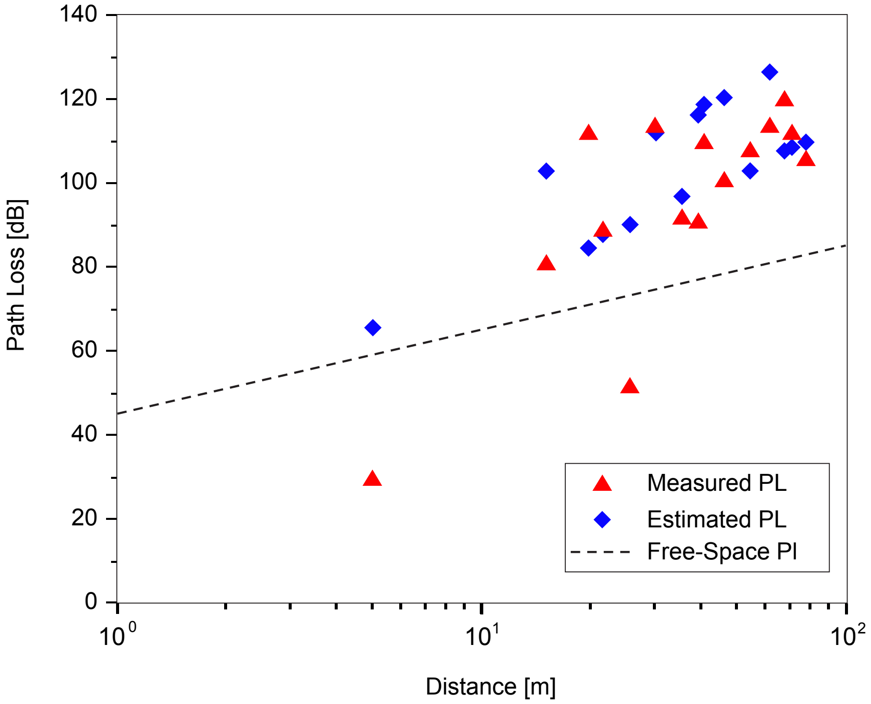


Figure 5.12: LoRa communication analysis results in the heritage building: estimated and measured PL compared with the FS model.

radio propagation inside the building. Through the analysis of variables such as the separation between the sender and the recipient, the frequency of the transmitted signal, and the surrounding environment, it is possible to determine the underlying reasons behind the loss of signal strength in LoRa technology. Predicting the reduction in signal power as it travels through a medium by modeling the path loss can aid in optimizing the placement of end-nodes and identifying any potential problems that may arise in a LoRa network. Additionally, this approach can provide valuable insights and recommendations for improving network performance.

5.2.3 Web monitoring platform 'TimberCare'

The current system utilizes The Things Network (TTN) for LoRaWAN communication, which provides a web platform for reading data from LoRa end-nodes and simple data management. However, for specific purposes, a personalized platform is required to customize user control, data analysis, and additional functionalities such as receiving alerts via email or mobile phone, specific data visualization options, user access control privileges, and more. To address this need, a custom web interface called "Timbercare" was developed using the Model-View-Controller (MVC) approach based on the Laravel framework [117] and implemented with a MySQL database. The front-end of the web application was built using the Bootstrap framework, which ensures responsive design and compatibility with mobile devices, tablets, and desktops.

To complete the system infrastructure, the Timbercare web application was hosted on a remote cloud server configured with LAMP (Linux, Apache, MySQL, and PHP) software. In this system, the LoRa gateway collects data from the MC LoRa end-node devices and sends it to the TTN server. Once the data is received by the TTN server, it is forwarded to the Timbercare remote cloud server and stored in the database. The database tables are represented in in Figure 5.13.

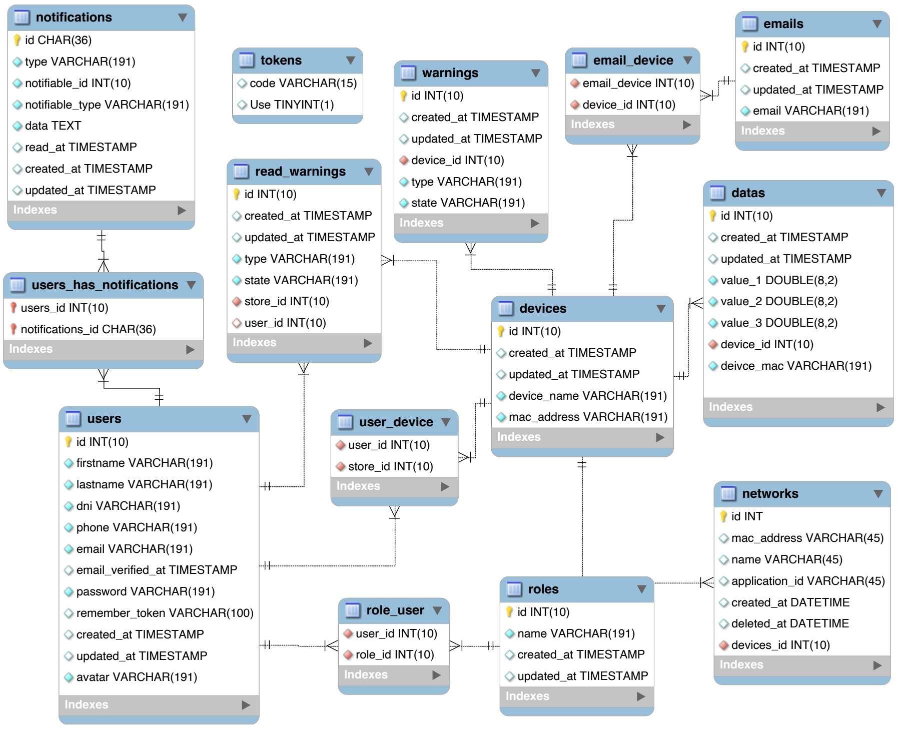


Figure 5.13: EER diagram of the MySQL database.

As illustrated in Figure 5.13, the web application database comprises eight main tables: 'Users', 'Roles', 'Devices', 'Networks', 'Datas', 'Notifications', 'Warnings',

and 'Emails':
Users: This table stores information about users registered in Timbercare, such as their name, email, address, password, and more.
Roles: This table records the access level of users, such as Administrator, Moderator, and so on. This work utilizes 'administrator' and 'user' roles, with the former being able to define other roles in the dashboard. The 'Role_user' pivot table links users to their roles.
Devices: This table stores user devices and their corresponding identifiers.
Networks: This table registers the LoRa network.
Datas: This table stores data received from sensors connected to the LoRa network. The 'Device_data' table links the sensors to their data.
Notifications: This table stores multiple notifications generated by the platform.
Warnings: Whenever the platform receives a value outside the user-defined range from an MC LoRa end-device, a warning message is generated and stored in this table, which is then sent to the user (the owner of the device).
Emails: The user can define multiple email addresses to which warnings and notifications related to the sensors are sent.
The authentication system implemented in the platform protects all data, ensuring that only authorized users can access their specific dashboard according to the MC LoRa end-nodes assigned to them. Depending on the user's role (administrator or user), they can add/remove devices, view notifications, monitor data, and export it. Figure 5.14 (a) displays the login fields on the homepage, and Figure 5.14 (b) describes the register page, enabling users to create a new account.

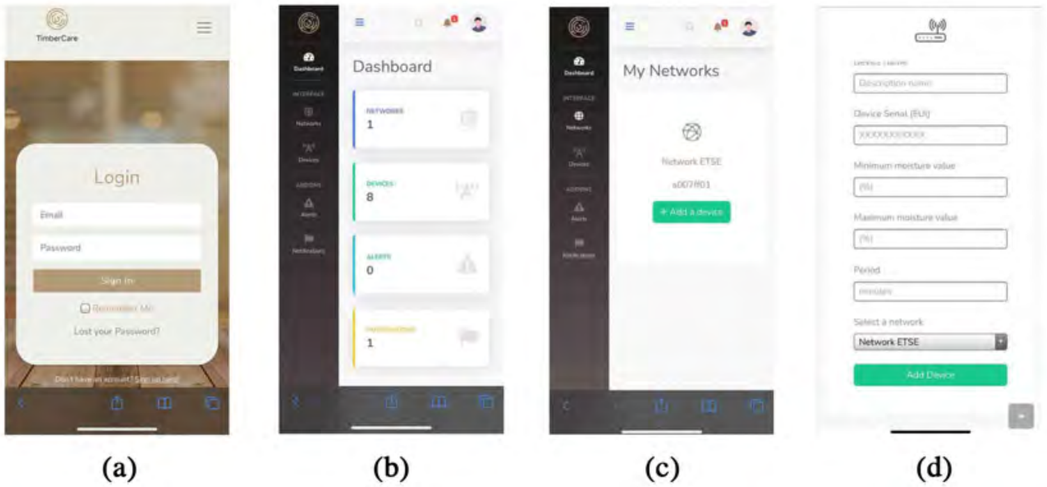


Figure 5.14: Screenshots from the 'Timbercare' monitoring and management platform for MC. (a) Home page with login fields, (b) user dashboard page, (c) network settings page, and (d) register new device screens.

The web interface for Timbercare platform offers easy navigation through five main menus: 'Dashboard', 'Device', 'Network', 'Notifications', and 'Profile'. Here is a detailed description of each menu:

Dashboard: Once the user logs in, they are redirected to the 'Dashboard' page, which displays an overview of all the devices associated with the network, including gateways and end-nodes. By clicking on a device name, the user can view its data charts and analyze sensor readings. The dashboard provides users with a high-level view of the data and allows them to explore it in more detail by clicking on specific devices.

Device: The 'Device' page shows detailed information about an MC LoRa end-node, including the received data presented in the form of charts. Users can filter data by defining a time range and export it in CSV or EXCEL formats. The user can also add, edit, delete, activate, or deactivate devices, including gateways and end-nodes. Users can set the measurement limits for each sensor node, and the platform generates an alert message via email and on the platform when the sensor readings are out of the defined range.

Network: The 'Network' page allows users to add new LoRa networks or update existing ones. Every device added to the platform must belong to a network.

Notifications and Alerts: This page displays all the messages generated by the platform, including messages related to out-of-range MC measured values, connection lost with end-nodes or gateways, and other system messages. Two classes of messages are defined: 'notifications' and 'alerts,' depending on the priority level.

Profile: Users can update their information, including avatar, email, password, and other details in the 'Profile' page.

The platform's authentication system protects all data, and only authorized users have access to their specific dashboard. Depending on the user's role, such as administrator or user, users can add/remove devices, view notifications, monitor the data, and export them.

5.2.4 Installation of System in a Heritage Building

After analyzing the path loss inside the heritage building "La Nau", three moisture devices were installed at locations P4, P9, and P12 (as shown in Figure 5.10). The gateway was placed at position P0. The front and back side of the moisture device prototype are shown in Figure 5.15(a) and 5.15(b) respectively. Figure 5.15(c) illustrates the installation process of the moisture device on a wooden roof.

The blue piece (depicted in Figure 5.15(b)) contains two stainless nails with a diameter of 0.7 mm that are hammered onto the wooden roof and then connected to the device. The moisture device is powered by two standard 1.5 V AAA batteries

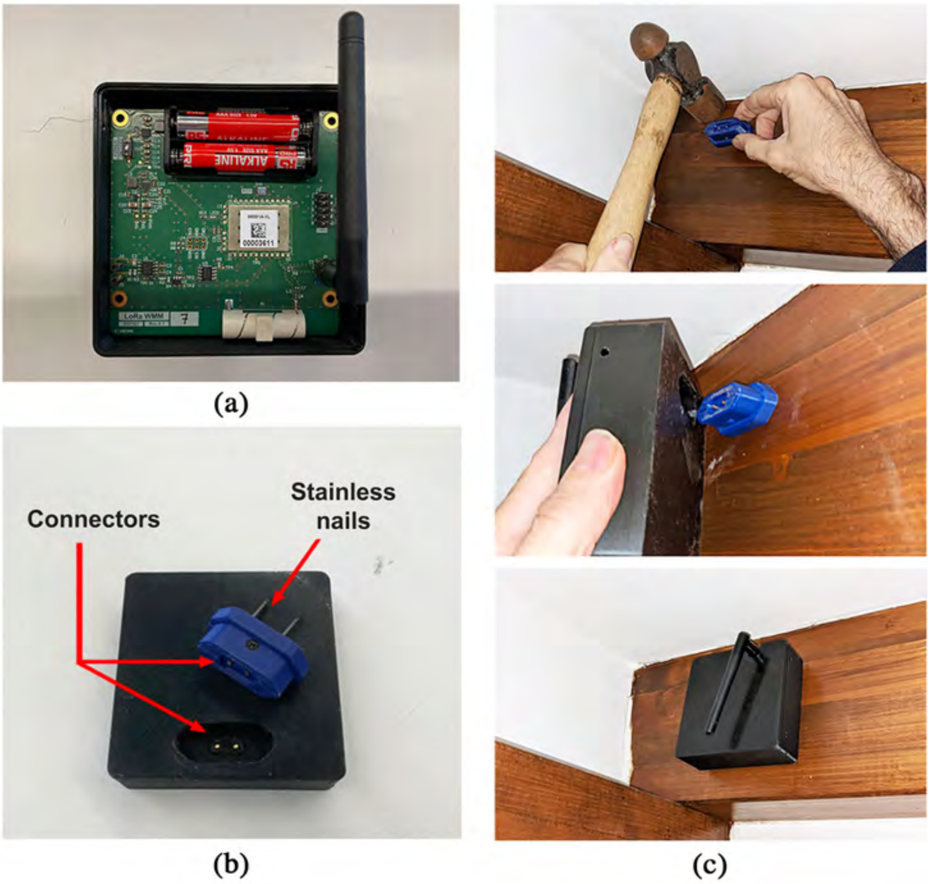
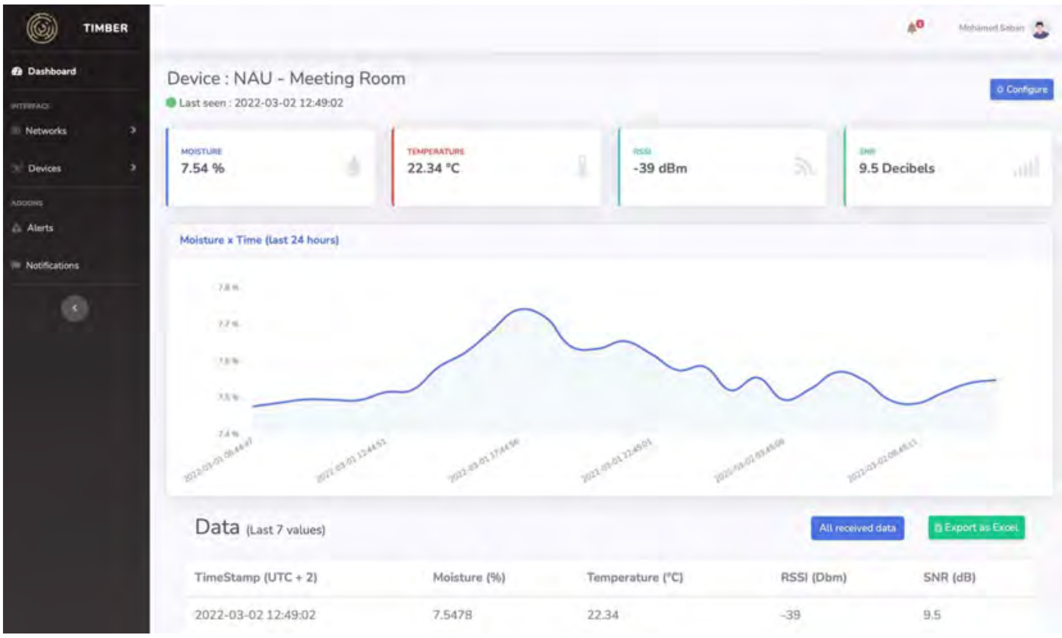


Figure 5.15: Installation of moisture device : (a) Front side of the moisture device, (b) back side of the moisture device showing the detached nail pieces, (c) steps of installing the device inside a wooden building.

and programmed to transmit the measured values of resistance frequency period T and ambient temperature four times a day. Each end-node is programmed to send four measurements per day, and the data is collected in the cloud server's database. The developed web monitoring application allows for monitoring and analysis of the measured moisture content values, as well as reporting on any abnormalities.

The installed moisture devices were left inside the heritage building 'La Nau' for a period of one month. During this period, the devices successfully transmitted the measured values of resistance frequency period T and ambient temperature four times a day to the gateway, which in turn was connected to the cloud server. The data was stored in the database of the 'TimberCare' web monitoring application, and the system was able to monitor and analyze the measured values of moisture content. The system was able to detect and report any abnormalities in the moisture content during the monitoring period as described in Figure 5.16. Overall, the successful transmission and monitoring of the measured values over the course of one month demonstrates the effectiveness and reliability of the installed system in tracking the moisture content of the heritage building.



Device : NAU - Meeting Room

Last seen : 2022-03-02 12:49:02

MOISTURE 7.54 %

TEMPERATURE 22.34 °C

RSSI -39 dBm

SNR 9.5 Decibels

Moisture x Time (last 24 hours)

Data (Last 7 values)

TimeStamp (UTC + 2)	Moisture (%)	Temperature (°C)	RSSI (Dbm)	SNR (dB)
2022-03-02 12:49:02	7.5478	22.34	-39	9.5

Figure 5.16: Screenshots of the device page showing the latest received information from a LoRa end-node device placed in the heritage building 'La Nau'. The user can visualize the temperature and MC in the form of charts and also can download the data as an excel table.

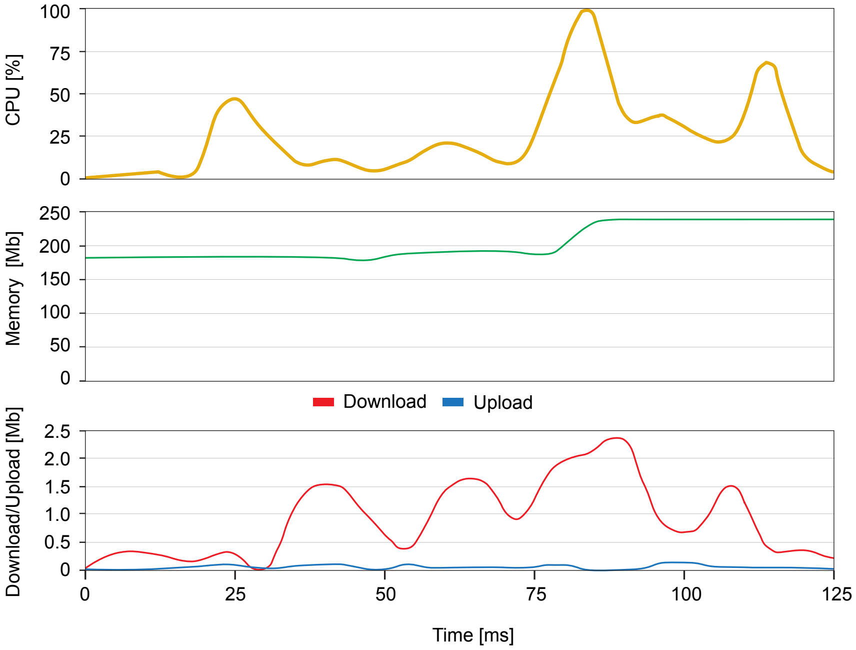


Figure 5.17: CPU usage, allocated memory and data download/upload as a function of time during multiple user interface visualization requests.

The resource usage of the server is an important aspect of any web application. The resource usage of 'Timbercare' on user operations was evaluated and the results are presented in Figure 5.17. The figure shows the CPU consumption, memory usage, and downloaded data size when the system receives user requests. On average, the response time is 125 ms, indicating the high performance and optimization of the platform. The CPU usage slightly increases after receiving a user request and then decreases, but remains low and stable even with multiple concurrent requests. The occupied memory remains lower than 200 Mb in all cases, which demonstrates the efficient memory management of the application. Moreover, all the pictures and icons used in the platform are vectorial SVG files, which increase the speed of the platform and consume low resources. As a result, the size of the downloaded data from the server does not exceed 2.5 Mb for each user request, as shown in the figure. In summary, the test results demonstrate the efficient resource usage of 'Timbercare' web application, with low CPU and memory usage and small data size downloads.

5.3 Application 3: Smart Farm system based on PLC and LoRa

Industry 4.0 can be defined as an umbrella term for a new industrial paradigm that includes different technologies that have a crucial role in the process of increasing the productivity and reducing the costs in the modern industry such as the Artificial Intelligence (AI), Augmented Reality (AR), big data, remote sensing and the Internet of Things (IoT) [234–236]. Recently, Industry 4.0 has become one of the main topics of research and discussion by industry and academia in the field of management and engineering [237, 238].

The integration of Industry 4.0 in the field of agriculture introduced the concept of smart agricultural and farming systems. IoT and other communication models have led to the automation of agricultural farms in a collaborative and intelligent manner in order to improve the reliability of crop production management. The significant advances in healthcare and medical technologies, and the growing consciousness about health [239, 240] has increased the population during the past century, which has raised the demand for food around the world. Thus, relying on the old ways of agriculture does not fill the world's needs for food.

Agricultural practices such as planting, sowing, reaping, irrigation, and cultivation heavily rely on the climatic conditions, particularly the air temperature, humidity, and precipitation intensity, as these factors can affect the spread of pests and diseases that can cause significant loss to global food production, which accounts for 40% of the total loss [234, 241]. Additionally, agronomic activities consume about 20% of the world's water reserve, where line losses, leakages, and over-irrigation are the primary reasons for water wastage [242]. Smart farming systems provide an automated solution to monitor and control the farm's natural resources and planting conditions without human intervention. By gathering data from multiple sensors and processing the information through a decision-making system, smart farm systems can improve production while reducing manual labor.

This application demonstrates the integration of LoRaWAN communication with the existing Programmable Logic Controllers (PLCs) that have been utilized in agriculture for decades to regulate multiple processes and machinery. As a result, previous automated processes can be employed in smart farms without replacing old control systems. The Simatic $IOT2040$, which is equipped with a LoRa shield, is used to integrate LoRa connectivity with these PLCs. The communication between the PLC and the $IOT2040$ is facilitated through the Modbus-TCP protocol. The proposed system employs the PLC to control the functions of farming machines, such as water pumps, and receive data from various sensor nodes distributed across the farm. Data processing is performed on a cloud server, which employs a secure, flexible, and scalable web-based platform to offer a user interface that enables remote management of all the devices employed in the proposed smart farm system.

5.3.1 Smart Farm architecture

The term "smart farm" refers to a modernized agricultural system that utilizes IoT infrastructure to automate farming processes. The proposed system comprises four key components: end-node sensors, an IoT LoRaWAN gateway, control equipment, a cloud server that hosts a web-based platform for control and monitoring, and a Telegram bot for mobile devices. As depicted in Figure 5.18, the proposed smart farm system is comprised of two main networks:

- The monitoring network (Farm): This wireless network comprises various LoRa sensors that are distributed across the farm to gather vital information such as moisture and airflow levels.
- The control network (Warehouse): The harvested fruits and vegetables are stored in the warehouse, and it is crucial to maintain optimal climatic conditions. Therefore, this network is equipped with environmental sensors, including temperature sensors, and it houses all the control equipment such as air conditioners and irrigation water pumps, which are managed by a PLC.

The LoRa sensors situated throughout the farm transmit the collected data (pH, moisture, air flow, temperature, etc.) to the LoRa gateway, which is connected to the internet. The gateway is responsible for relaying the sensor data to the cloud server, where it is analyzed and stored in the database. The gateway is also responsible for receiving control commands from the server and forwarding them to the PLC located in the warehouse. These commands can be manually instructed by the user via the web-based platform or automatically executed if the received sensor data require an action (e.g., the PLC will activate the water pump if the soil requires more water). The user can configure these automatic commands in the web platform by defining the target device and the threshold values that trigger the actuating device. To ensure efficient communication coverage, the LoRa gateway should be placed at a high altitude, and all the LoRa end-nodes must be distributed appropriately.

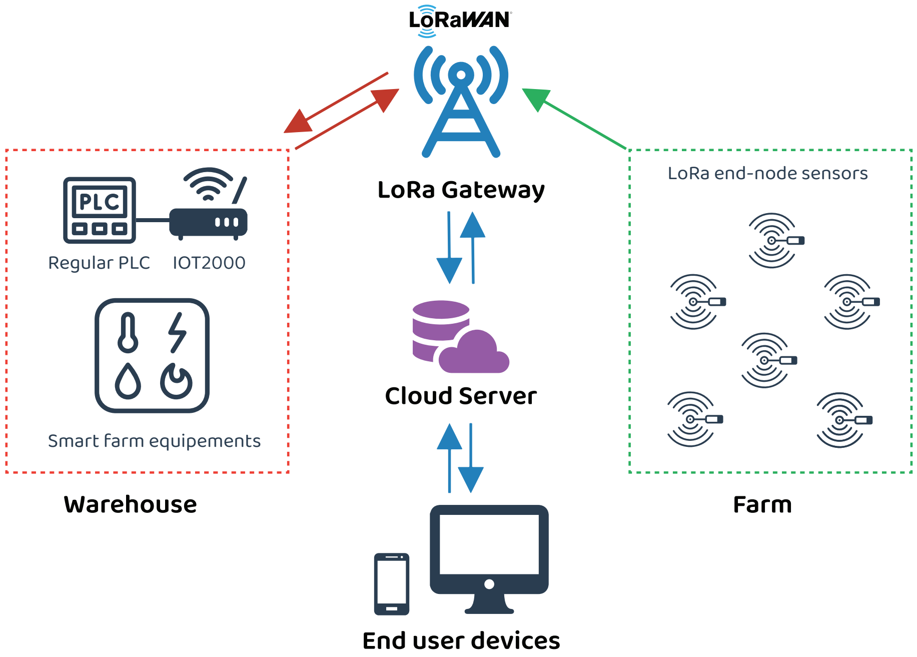


Figure 5.18: Smart farm system architecture overview. The farm is connected to a LoRa gateway which exchanges data with users via a cloud server.

5.3.2 Materials and Methods

To establish LoRa communication within our system, the "WiMOD LoRa Lite Gateway" from IMST is used. The warehouse contains a PLC that manages devices on the farm, such as the water pump. For this PLC to wirelessly connect through LoRa, it must establish a connection with the gateway to receive commands from the cloud server. To achieve this, the Simatic $IOT2040$ from Siemens [243] was connected to a regular S7 Siemens PLC via Modbus TCP. The LoRa Wimod Arduino shield board from IMST is inserted into the Simatic $IOT2040$ as an additional communication board, enabling it to function as a LoRa end-node in the same way as other LoRa end-node sensors on the farm. This solution allows us to connect existing PLCs to the LoRa network. Figure 5.19 depicts the devices used in our test bench. The farm device's inputs/outputs are simulated using the SIMATIC Step7 software and controlled using the S7 Siemens PLC.

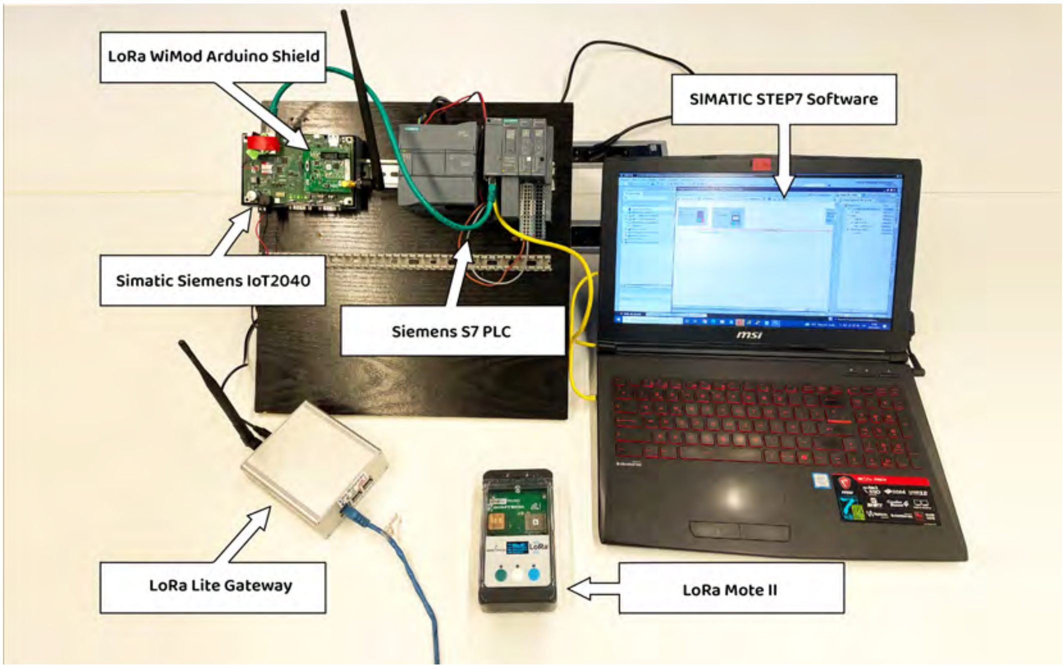
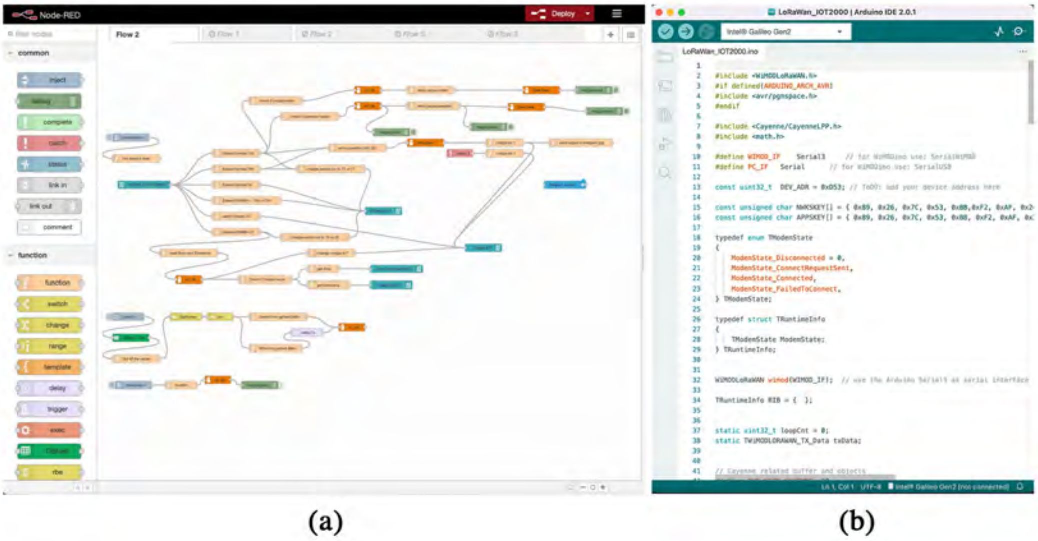


Figure 5.19: Siemens S7 PLC connected to Siemens Simatic $IOT2040$ incorporating the Wimod LoRa shield. The LoRa gateway is powered and connected to the internet. The inputs/outputs of the different devices in the farm are simulated with the Simatic Step7 software and controlled with the S7 Siemens PLC [244].

The Siemens Simatic $IOT2040$ has a compact industrial design that operates with Yocto Linux and can be easily expanded with Arduino shields. It allows for simple programming of applications using the Node-Red visual programming tool, as shown in Figure 5.20(a). To enable the use of WiMOD radio modules based on LoRa, we added the WiMOD Shield, which is an expansion board that includes everything necessary to connect a WiMOD module to an Arduino board using the "$WiMODLoRAWAN$" library. The shield offers two UART connections that communicate with the IOT2040 main board. To program the LoRa communication shield, we used the Arduino IDE software, as depicted in Figure 5.20(b), and then wrote the code directly to the IOT2040 using a USB cable. This was possible thanks to the Intel Galileo firmware, which must first be added to the Arduino IDE.

In the NodeRed dashboard, the "*node-red-node-arduino*" package is added to read the LoRa payloads exchanged between the IOT2040 and the gateway through the LoRa shield board. We also used the "*node-red-contrib-s7*" package to read and write commands to the Siemens S7 PLC via Modbus-TCP, although any other PLC could also be connected using standard Modbus-TCP wired communication. Figure 5.20 provides a glimpse of the Arduino code and the NodeRed scheme of the smart farm.

The PLC in the warehouse controls the following elements:



```

#include <WiMODLoRaWAN.h>
#if defined(ARDUINO_ARCH_AVR)
#include <avr/pgmspace.h>
#endif

#include <Cayenne/CayenneLPP.h>
#include <math.h>

#define WIMOD_IF    Serial3     // for WiMODino use: SerialWiMOD
#define PC_IF   Serial      // for WiMODino use: SerialUSB

const uint32_t  DEV_ADR = 0x053; // ToDO: add your device address here

const unsigned char NWKSKEY[] = { 0x89, 0x26, 0x7C, 0x53, 0x88,0xF2, 0xAF, 0x2
const unsigned char APPSKEY[] = { 0x89, 0x26, 0x7C, 0x53, 0x88, 0xF2, 0xAF, 0x

typedef enum TModemState
{
    ModemState_Disconnected = 0,
    ModemState_ConnectRequestSent,
    ModemState_Connected,
    ModemState_FailedToConnect,
} TModemState;

typedef struct TRuntimeInfo
{
    TModemState ModemState;
} TRuntimeInfo;


WiMODLoRaWAN wimod(WIMOD_IF);  // use the Arduino Serial3 as serial interface

TRuntimeInfo RIB = {  };


static uint32_t loopCnt = 0;
static TWiMODLORAWAN_TX_Data txData;


// Cayenne related buffer and objects
```

Figure 5.20: (a):NodeRed dashboard, it provides a browser-based editor that makes it easy to wire together flows using the nodes. (b): a part of the code used to program the LoRaWan communication of the SIMATIC IoT2040 [244].

- Water pump and associated valves: controls the amount of water needed for irrigation.
- Air conditioner and fans for ventilation and air quality, maintaining an adequate level of temperature and humidity to preserve food products.
- Intrusion alarms.
- Lighting: on/off programming for presence simulation and night activity.
- LoRa Temperature sensor.
- LoRa Humidity sensor.

The communication between the Siemens S7 PLC and the LoRa gateway in our system is established through Modbus-TCP. The remaining sensors installed in the farm act as LoRa end-nodes and directly communicate with the LoRa gateway.
To enable Telegram instant messaging in our system, we integrated a bot using the Telegram Bot API both in the $IOT2040$ and the web application. The bot was created by registering with "$@botfather$" and completing several steps such as defining a bot name, username, and commands using the */newbot* command. The bot token obtained after creation was used to communicate with our system via Telegram. To integrate the Telegram bot with the $IOT2040$, the NodeRed package "*node-red-contrib-telegrambot*" was installed and programmed the Telegram node with JSON code to define commands and their corresponding actions. The aim of this integration is to receive direct control commands from users via Telegram, such

as turning on lights. The $IOT2040$ analyses the request, executes the command, and sends a confirmation message to the user.
In the second integration of the Telegram bot with the web application, the same bot token as the $IOT2040$ was integrated using the "*Telegram Bot API - PHP SDK*" [245]. This integration enables the analysis of user requests related to the database (e.g. requesting the last irrigation water usage or the time when the lights were switched off) or requests related to sensor nodes to receive instant measured values without waiting for the duty cycle time needed to send the last measured value to the database.

5.3.3 Experimental Tests and Results

The experimental test took place in a farmland situated in Valencia city, Spain. For this test, we utilized a LoRa Mote II from IMST as the end-node, which consisted of an accelerometer, an altimeter, a temperature sensor, and a GPS module. The LoRa gateway was positioned on the balcony of a 6th-floor apartment, with an altitude of approximately 24 meters.
The configuration used for the LoRa end-node device was:

- LoRa Class: Class A
- Frequency: 867.1–868.5 MHz
- Bandwidth size: 125 kHz
- Spreading Factor (SF): 7
- Coding Rate: fixed = 4/5
- Transmitting Power: +14 dB

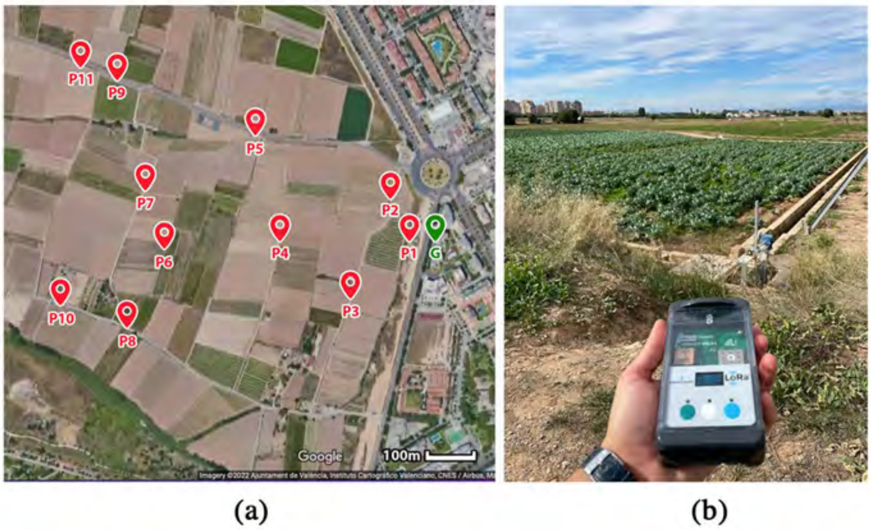


Figure 5.21: Experimental setup for outdoor LoRa communication test. (a): P1 to P14 represent the measurement locations, G represent the gateway location. (b): LoRa Mote II used as LoRa end-node [244].

To conduct the experimental test, the LoRa end-node was placed at various locations with varying distances from the gateway. Ten messages were exchanged between the end-node and the gateway from each transmit location. The location of the LoRa gateway and the different measurement positions (P1 to P11) are shown in a situation map in Figure 5.21. To reach the maximum distance, the Spreading Factor (SF) was fixed at 7. However, in similar applications, it is recommended to use the Adaptive Data Rate (ADR) mechanism instead of fixing the SF. This will optimize data rates, airtime, and power consumption, ultimately improving the range and capacity of the network.

The percentage of received packets (RPP) was computed at each location anc only the measurement points with an RPP of 50% or higher were considered. Table 5.4 displays the Received Signal Strength Indicator (RSSI), signal-to-noise ratio (SNR), and percentage of received packets (RPP) for each measurement point. The RSSI and SNR were plotted against distance in Figure 5.22. As expected, the RSSI decreased with distance, and the first packet loss occurred at position P6 (550 m). At position P5 and beyond, the RSSI dropped below -90 dBm. The SNR remained above 0 dB until P9 (720 m), after which it dropped to -4 dB at P11 (795 m). The lowest SNR value was recorded at P8 (640 m), whereas the highest RPP was achieved at P11 (795 m), with a value of 60%. These results indicate that communication between end-nodes and the gateway can be successfully achieved within distances under 500 meters.

Table 5.4: SNR, RSSI and RPP of received packets from each measurement point

Locations	Distance (m)	RSSI (dBm)	SNR (dB)	RPP (%)
P1	50	-36	9	100
P2	120	-80	5.2	100
P3	200	-70	7.4	100
P4	290	-76	9	100
P5	415	-90	5	100
P6	550	-100	6	90
P7	580	-95	4	80
P8	640	-110	2	50
P9	720	-105	-2	60
P10	755	-98	-2	70
P11	795	-109	-4	60

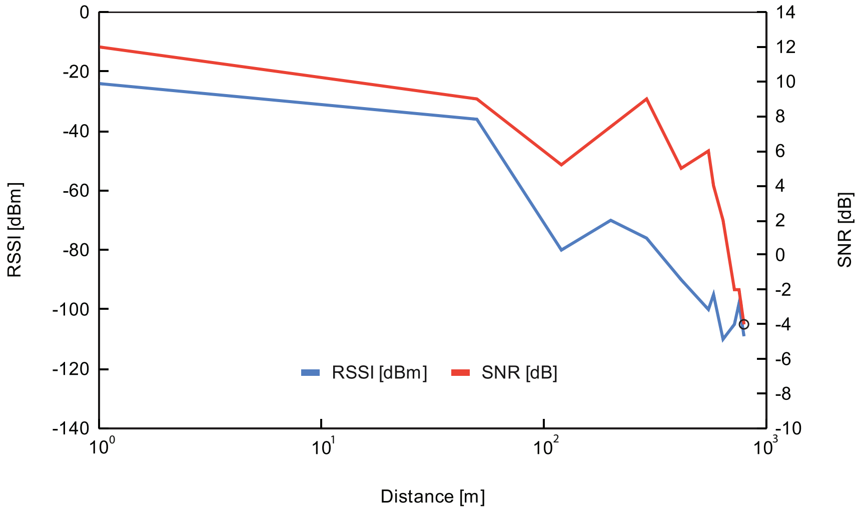


Figure 5.22: LoRa communication values in outdoor testing: Average RSSI[dBm] and Average SNR[dB] as a function of distance[m] [244].

Understanding Path Loss (PL) is crucial as it provides insights into the weakening of LoRa signals as they traverse the environment. This knowledge can aid in predicting the range of a LoRa network and designing effective communication systems. By examining factors like the distance between the transmitter and receiver, the frequency of the signal, and the type of environment, we can identify what causes LoRa path loss. By modeling PL, we can anticipate the signal power reduction as it moves through a medium, which can facilitate the proper distribution of end-nodes and detection of potential issues with a LoRa network. It can also offer suggestions for enhancing network performance.

Using the data collected from the experiment and the EPL parameters described in

Table 5.5: Lognormal PL Model parameters and statistical measures in the outdoor environment.

EPL exponent (γ)	2.9
EPL intercept (PL(d_0))	36.34 dB
Standard deviation (σ_{SF})	6
Standard error of the mean (SEM)	1.81
Range	71.29 dB

Table 5.5, the PL was calculated using the same method described in the previous section. The results are presented in Figure 5.23. Understanding path loss is crucial for predicting the range of a LoRa network and designing efficient communication systems. The proposed model appears to be more accurate as distance increases. However, for distances shorter than 70m, the proposed model exhibits instability, mainly due to shadowing effects [224]. Received packets with a PL lower than 126 dB are possible. As expected, the free space model FSPL shows the lowest level of attenuation.

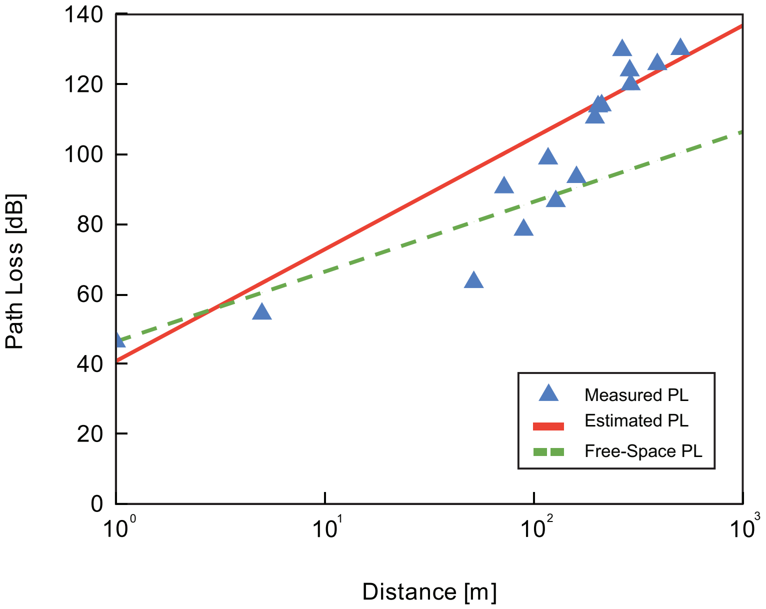


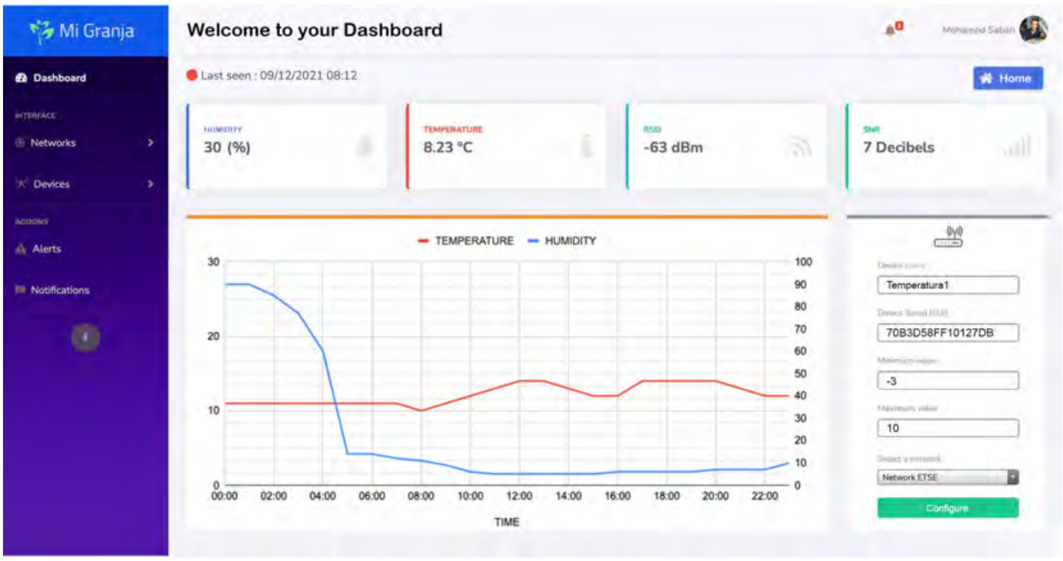
Figure 5.23: Estimated and measured PL compared with the FS model in the farm environment [244].

The environment, the distance between the transmitter and receiver, and the height of the transmit and receive antennas all have an impact on PL. As a result, the PL model parameters are typically only valid in specific environments, frequency ranges, and antenna configurations. Thus, for similar condition to our experimental test, the proposed PL estimation model can be applied in the design of a LoRa mesh network in a farm to improve the energy efficiency and reliability over existing LoRa systems.

The presented smart farm system requires a tailored application to customize the control and analysis of data and provide more flexibility in its management. To meet this need, we have developed a personalized web application called 'Mi granja' (My Farm), using the Laravel framework [117] for back-end operations and a MySQL database. The front-end of the web application is developed using the Bootstrap framework, which implements a responsive design that is supported by multiple screen sizes. The web application allows users to easily access and analyze the data collected by the sensor nodes, as well as remotely control the machines connected to the PLC. It also provides a user-friendly interface for configuring the system settings and defining custom alerts and notifications. The web application is hosted on a cloud server, enabling users to access it from anywhere with an internet connection. The LoRa gateway communicates with the TTN server, which will forward the received payloads directly to our cloud server to be stored in the database, so that it can be visualized and monitored from the user interface. The user commands also take the same path: they are transmitted to the TTN server and then forwarded to the LoRa gateway, which will finally communicate with the LoRa end-node. The web application allows different users to create their accounts, each user can register several networks corresponding to his associated farms (multiples farms can be managed from the same web interface), and each network (each farm, in fact) contains a number of connected devices. In order to register a device in the network, the user should register this device in the TTN server first, and then register it in the dashboard page of the web application using its identifier, because all the data go through the TTN LoRaWan network before receiving/sending it to our cloud server.

Figure 5.24 shows the home page and dashboard of the web application. On the dashboard, the user can define multiple parameters related to each LoRa end-node, such as maximum and minimum values for specific devices. If the received value is outside the defined range, the user will receive an alert notification via email and Telegram. These notification and alert messages can be customized in the dashboard. The data collected by the sensor nodes can be viewed in the form of tables and charts and can be downloaded as an Excel or CSV file for manual and advanced analysis if needed. The web application also has the flexibility to easily add additional features thanks to its MVC design based on the Laravel framework. Overall, the web application provides a comprehensive and user-friendly interface for managing and analyzing the data collected by the smart farm system.

The web application is hosted in a cloud server and its main features are:



Welcome to your Dashboard

Last seen : 09/12/2021 08:12

HUMIDITY 30 (%)

TEMPERATURE 8.23 °C

RSSI -63 dBm

SNR 7 Decibels

Device name: Temperatura1

Device Serial (EUI): 70B3D58FF10127DB

Minimum value: -3

Maximum value: 10

Select a network: Network ETSE

Figure 5.24: Screenshot from the web application "Mi Granja" showing the dashboard page and relevant data [244].

- Scalable design, light weight and fast response.
- Strong security thanks to the MVC design and authentication system.
- Multi-device experience: users can access to the web application from various devices.
- Instant messaging: users receive notifications via email and Telegram.
- Different charts and graphs for Data visualisation.
- Organized data storage and easy searching.
- Export data for advanced analyses as Excel and CSV files.

Figure 5.25 [234] describes the general illustration of the presented system.
The smart agricultural system utilizes LoRa end-node sensors scattered throughout the farm to collect data about the environment. The sensors transmit this data to a LoRaWAN gateway, which then sends it to a cloud server for analysis. The system also includes a PLC that is connected to various machines in the warehouse, such as water pumps and lights. The IoT2040 is connected to the PLC via Modbus-TCP and programmed with Node-RED. Users can access the system through a web-based monitoring application, which allows for remote control of the warehouse machines through the IoT2040. Additionally, users can send commands and requests via a Telegram bot. The cloud server analyzes the received information and stores useful data.

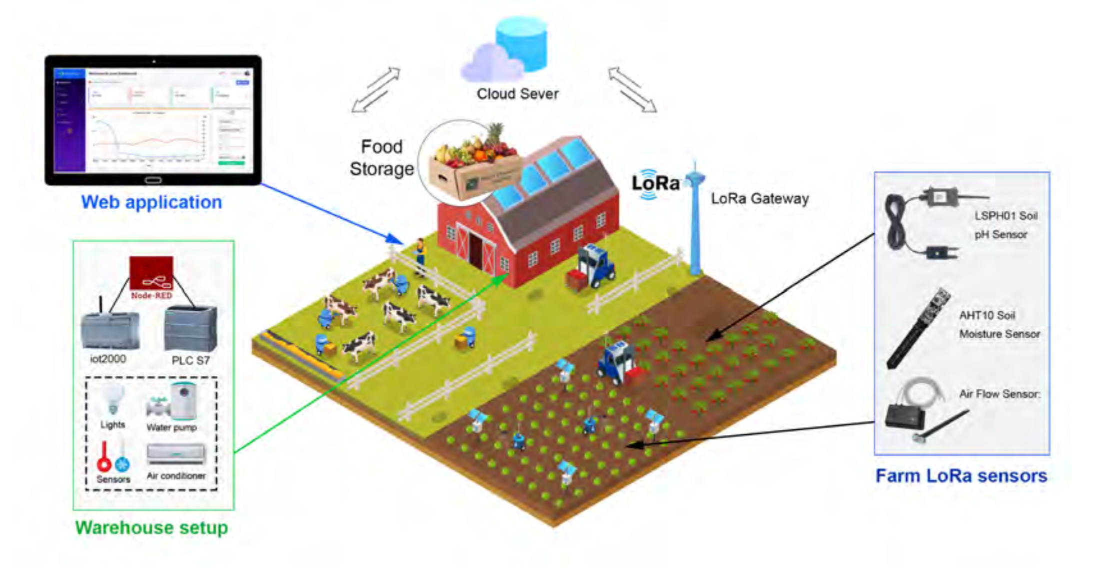


Figure 5.25: Illustration of the smart farming application. The proposed IoT system integrates different devices and technologies: PLC controllers and LoRa nodes connected via a gateway [244].

To conclude, the proposed infrastructure represents a smart solution for farmers to integrate the IoT in their already existed farming systems which mainly are relying on a regular PLC.

5.4 Application 4: Blockchain-Integrated LoRa System for Monitoring the Well-being of Elderly

The average life span has increased during the past decades due to the significant advances in healthcare and medical technologies, sanitation, nutrition, and the growing consciousness about health [239, 240, 246]. Thus, the proportion of elderly population relative to the total population continues to increase. According to the United Nations Population Fund (UNFPA), the global number of people aged 60 or older will reach 2 billion by 2050 [247]. Most of the elderly relies on other persons such as family members and volunteers, while the ones who can afford the expenses may go to elderly care centers [248]. On the other hand, a large fraction of elderly are living alone making their life susceptible to many dangers, and, in the worst cases, some of them can die alone in their homes [249]. It is important to ensure the wellness of the elderly who live alone, especially in rural areas due to the far distance from hospitals. In Spain, more than 2 million people over the age of 65 were living alone in 2020 according to the National Statistics Institute (INE), taking into account that 16,2% of the Spanish population are living in rural areas [250]. However, many of these people cannot continue their independent life due to the physical or mental issues such as Alzheimer's disease, dementia, cardiovascular, diabetes, osteoarthritis, lung diseases, or other chronic diseases.

The recent advances in communications and computing technologies, together with the decrease in the cost of sensor based devices, have driven the implementation of health monitoring and human activity detection systems [251, 252]. Remote monitoring systems in primary healthcare and well-being shows great promise as they are easy to perform, especially for elderly and housebound patients [253, 254]. On the other hand, implementing home monitoring systems becomes more difficult in far villages and rural areas, especially in underdeveloped countries, where not all houses are provided with internet services. Nevertheless, the use of LPWAN technologies such as LoRa can be a good solution. The main advantages of LoRa CSS modulation are the low transmission power, the wide communication range and the inherent robustness from channel degradation mechanisms such as fading and multi-path. Thus, one LoRa gateway can cover a wide area, which means that, e.g. in a village, all LoRa devices installed in the houses can transmit and receive data to this LoRa gateway.

However, home monitoring systems should maximize the privacy of patients while still providing information regarding deviations from their normal habits or health problems. For example, motion-detection sensors are favored to invasive technologies such as video recording [255, 256]. Also, data collection in home monitoring should respect the privacy of the patients, and transmitted information should be encrypted and protected.

In the present work, an intelligent home monitoring LoRa-based system is designed to monitor the activities of elderly living alone in rural areas and evaluate their well-being. A new low-cost LoRa smart plug to monitor the usage of the domestic appliances is proposed. This smart plug is used to recognize the daily activities of the elderly in order to determine their well being. In addition, multiple commercial LoRa sensors can be added to the proposed system.

To secure the transmitted data, the Swarm Ethereum public blockchain is integrate for safe and immutable data storage. The remote monitoring and control of the different LoRa devices of this system is done through a newly developed web-based platform, providing a user interface accessible through a web browser allowing the user to configure the devices of his network and analyse the received data under different operating systems and screen sizes. Also, it implements an authentication system to secure the access and a notification system to alert the patient family or his healthcare center in emergency cases.

5.4.1 Monitoring the activity behaviour of elderly

The main objective of elderly wellness systems is to provide care for them, no matter where they live. Elderly people who do not require daily care can live alone, they are reluctant to move to another place apart from their home, and do not like to use wearable sensors. Thus, a 'transparent' monitoring system is a good option. Wellness determination and activity recognition are two important functions to forecast and help the elderly thanks to the analysis of data. One of the indications about the wellness of elderly while living alone is the use of electrical appliances at home. They typically repeat activities everyday: preparing food, watching TV, turning on/off different room lights (kitchen, bathroom, etc.). Then, monitoring the use of electric appliances can be a good indication of wellness. If a deviation in the use of appliances is detected, a warning can be triggered.

5.4.1.1 LoRa smart plug

In order to monitor the use of electric appliances, we propose a smart LoRa plug that aims on sensing the use of the electrical appliances in the house. This smart plug will notify the LoRa system when a device is turned on/off. The data are collected and analysed in the cloud server, in the case of an odd behavior, the system will generate an alert message and send it to the person or entity concerned. Figure 5.26 describes the electronic circuit of the LoRa smart plug.

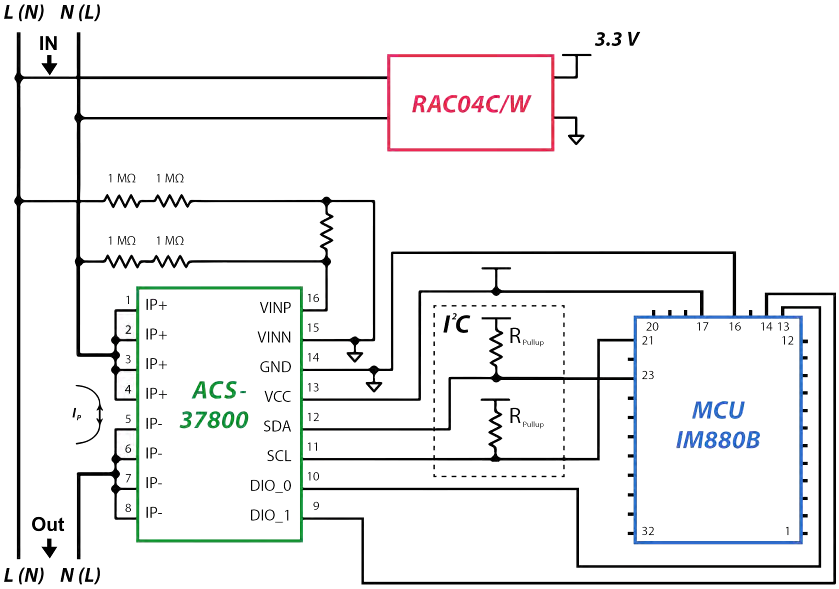


Figure 5.26: LoRa smart plug simplified electronic circuit: the power monitoring sensor $ACS - 37800$ transmits the sensed values to the LoRa module $IM880B$ through the I^2C communication protocol. The LoRa module will send the measured values to the LoRaWAN servers via the LoRa gateway.

The proposed smart plug consists of three main components:

1. $ACS37800$: power monitoring sensor, it can easily be accessed through its SPI or I2C digital protocol interfaces.

2. $RAC04C/W$: AC/DC converter to generate a constant voltage of 3.3 V from AC mains.
3. $IM880B$: processing and LoRa communication module from IMST [**IMST_2021**], this module is equipped with a programmable $STM32L081$ microcontroller unit with a frequency of 32 MHz where our specific firmware applications reside. This module has a sensitivity of -138 dBm.

An external transmitting antenna with a gain of +2 dB will be implemented in the final smart plug PCB in order to increase the signal strength, extend the range of transmission and improve the signal quality.

Before the fabrication of the printed circuit board (PCB) for the LoRa Smart plug, the functionality of the device was tested by building a prototype that consisted of a normal plug, a WiMOD Demo Board, and an ACS37800 power monitoring sensor. The WiMOD Demo Board was selected for its wireless communication capabilities, which are essential for the LoRa Smart plug's operation, and the ACS37800 power monitoring sensor was used to measure the electrical parameters of the plug, such as voltage, current, and power consumption. As described in Figure 5.27,the prototype was constructed by connecting the WiMOD Demo Board and the ACS37800 power monitoring sensor to the normal plug, with the WiMOD Demo Board being connected to the plug's control circuitry, and the ACS37800 connected to the plug's power supply. The data from the power monitoring sensor was then transmitted wirelessly to a nearby computer for analysis through the WiMOD Demo Board.

The functionality and performance of the prototype were extensively tested, including tests to measure the plug's power consumption under different load conditions, its wireless communication capabilities, and its ability to operate reliably over extended periods. Compatibility tests were also conducted to ensure the plug's versatility and ease of use with different devices, such as smartphones and laptops. The successful testing of the prototype gave us confidence that the design was reliable and feasible for the intended application. With this assurance, we proceeded with the fabrication of the PCB for the LoRa Smart plug, which will be used in future work for real-world applications. The PCB will allow for a more compact and efficient design, enabling the device to be easily integrated into various appliances and systems. The knowledge and experience gained during the prototype testing phase will also aid in future improvements and modifications to the design. Ultimately, the successful fabrication of the PCB for the LoRa Smart plug will pave the way for the deployment of the device in real-world scenarios, where it can make a positive impact by providing efficient and cost-effective power monitoring and control capabilities.

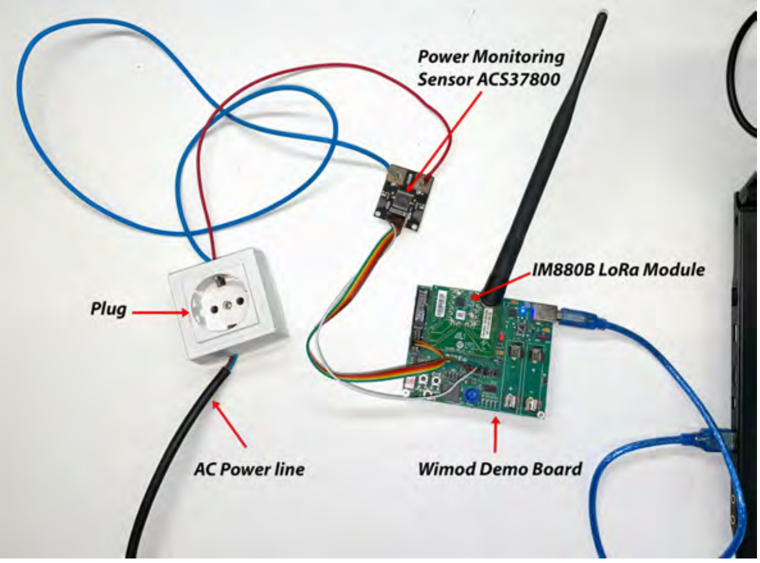


Figure 5.27: Test bench of the LoRa smart plug: The power monitoring sensor ACS37800 is connected to the LoRa Wimod Demo board and to AC power line through a normal plug.

5.4.1.2 Wellness Determination of Elderly

The monitored activities of the elderly can provide a more comprehensive and longitudinal evaluation than the annual physical examination. There are various wellness concepts suggested by experts from multiple domains. Wellness have multiple dimensions or levels that can be influenced by different factors such as culture, religion and experiences [257, 258]. In this work, Wellness means how the elderly living alone is able to perform his daily activities in a *normal* way. As done in [259], the wellness of the elderly will be determined using two functions. The first function (5.2) is determined from the inactive time of different sensors. The second function (5.3) is determined from the overuse of a specific appliance (e.g. oven), or under-use (e.g. bathroom light).

$$W_1 = 1 - \frac{t_{off}}{T_{off}}. \tag{5.2}$$

where t_{off} is time duration where all the sensors and appliances are inactive (No electrical device is used, and the motions sensors are not detecting any movement) T_{off} is the maximum inactive duration when no appliance is active. When W_1 goes below 0, that indicates unusual situation due to the excess usage of the appliance.

$$W_2 = 1 + (1 - \frac{t_{on}}{T_{on}}). \tag{5.3}$$

Where t_{on} is the actual usage duration of an appliance and T_{on} is the maximum usage duration use of this appliances in a normal situation. If W_2 goes below 0.5 that indicates unusual situation.

The maximum inactive duration T_{off} and the maximum usage duration T_{on} for each device in the house can be obtained during the trial period of the system deployment. These values vary from one person to another and they cannot be initially predefined. The developed web application allows the concerned person to add and change T_{on} and T_{off} corresponding to each LoRa end-device existing in the elder's house, through the user interface. Furthermore, an AI (Artificial Intelligence) algorithm can be used to adapt the timing and define the regular activities for each user.

In addition to monitoring electrical appliances' activities, motion sensors are important to detect the elderly moving among the different rooms in the house. Since the use of cameras is not preferred in such applications because of people privacy, the commercial LoRa motion sensor $TBMS100$ was chosen in this work. This sensor operates in the frequency of 868 MHz and has a motion sensitivity distance of 7 meters, with a transmission power of +17 dBm with a sensitivity of -135 dBm.

The monitoring system is scalable and other additional LoRa sensors such as room presence, temperature, humidity, etc. can be installed inside the house in order to obtain more information. Even personal health monitoring sensors as cardiac pulse, blood pressure could also be included. However, in order to reduce the use of personal wearing devices which reduces the comfort of the user and forces them to follow some instructions, we opted for using 'invisible' activity detection to avoid misuse.

5.4.1.3 Blockchain Integration

In this work, the Swarm Ethereum is integrated with the LoRaWAN network in order to provides a scalable, secure and self-sustaining infrastructure for data. The LoRa network is extended by storing the received data in the Swarm Ethereum storage service and defining a clear approach to store, access, and retrieve data using Swarm and Ethereum smart contracts.

To achieve this integration, a Swarm node is set up on the cloud server. For Laravel applications, the "web3.php" is should be installed in order to connect to the Ethereum network. The smart contract described in Listing 5.4.1.3 is created which the logic for storing and retrieving data on the Swarm network and deployed on the Ethereum network.

```

pragma solidity ^0.8.0;
```

```

contract SwarmFileStorage {
    struct File {
        string swarmHash;
        string description;
        uint256 timestamp;
    }

    mapping(uint256 => File) private files;
    uint256 private latestIndex = 0;

    function storeFile(string memory _hash, string memory _description) public {
        files[latestIndex] = File(_hash, _description, block.timestamp);
        latestIndex++;
    }

    function getFile(uint256 _index) public view returns (string memory, string memory, uint256) {
        File memory file = files[_index];
        return (file.swarmHash, file.description, file.timestamp);
    }
}
```

Listing 5.1: Smart Contract that stores Swarm hashes for files along with timestamps and descriptions

This smart contract defines a struct called *File* that stores a Swarm hash, a description, and a timestamp for a file. It also defines a mapping called *files* that maps indices to File structs, and a counter called *latestIndex* that keeps track of the latest index used. The *storeFile* function takes a Swarm hash and a description as input, creates a new *File* struct with the current timestamp, and adds it to the files mapping using the latest index. The *getFile* function takes an index as input and returns the Swarm hash, description, and timestamp for the corresponding *File*. The private Ethereum network of this project has a default gas limit of 4,712,000 gas per block. Given that the average gas price is 21,000 gas, a block can accommodate up to 224 transactions. The average block time is 15s, which implies that our private network can handle around 1000 transactions per minute. Although this number may seem low to support the deployment of thousands of LoRa-devices, in our case, data is filtered and grouped in the cloud server before being uploaded to the Swarm storage network. As a result, only a few transactions are carried out each day. The useful data from each monitored house is collected in a temporary database. Each day, the relevant data is exported automatically and pushed into the Swarm network, where it is encrypted and saved. Once the data is successfully uploaded to the blockchain network, it is deleted from the temporary database. This process reduces gas fees and establishes a clear path for retrieving data in future applications. Figure 5.28 shows the data processing workflow for this system.

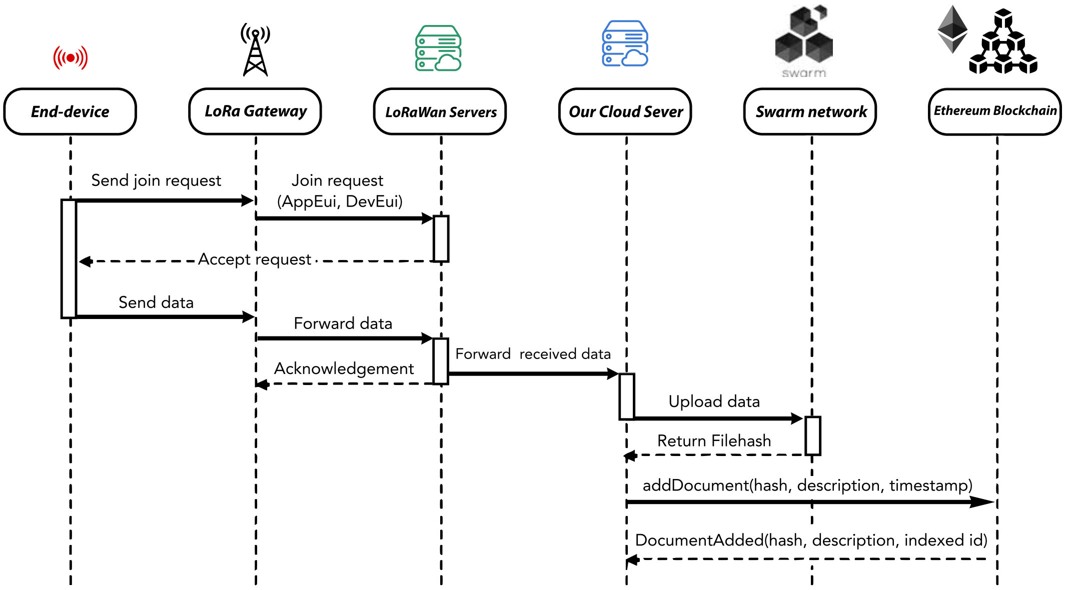


Figure 5.28: Data processing and storage Workflow: The data collected by the LoRa end-devices is transmitted to the LoRaWAN server and forwarded to our cloud server, The useful data is pushed into the Swarm network and their hashes is stored into the Ethereum blockchain.

The LoRa end-devices collect data and transmit it to the LoRa gateway, which forwards it to the LoRaWAN servers. Once the data arrives at the LoRaWAN server, it is automatically forwarded to our cloud server where it is analyzed and filtered. After that, it is pushed into the Swarm Ethereum blockchain network.

The collected data from the end-devices are forwarded by the LoRa gateway to the cloud server where they are filtered and analyzed. Once this process is complete, the data is pushed to the Swarm network via HTTPS. A unique cryptographic hash is generated for the uploaded file, which serves as the address for retrieving data from the Swarm network. To facilitate the interaction of the Swarm storage network with the Ethereum blockchain, an Ethereum smart contract is deployed. The uploaded data is deleted from the cloud server once it has been successfully uploaded to the blockchain.

A personalized Laravel platform is developed which enables users to control and analyze collected data and includes other features such as receiving alert messages via email or mobile phone using instant messaging applications like WhatsApp and Telegram. Additionally, it offers control over user access privileges and the ability to push data to the Swarm network. The user interface was developed using the Bootstrap framework, providing a responsive design that supports multiple screen sizes. To improve server resource utilization and speed, we used vectorial SVG pictures and icons. Figures 5.29(a) and 5.29(b) show the dashboard page and setting page to configure a specific LoRa device respectively.

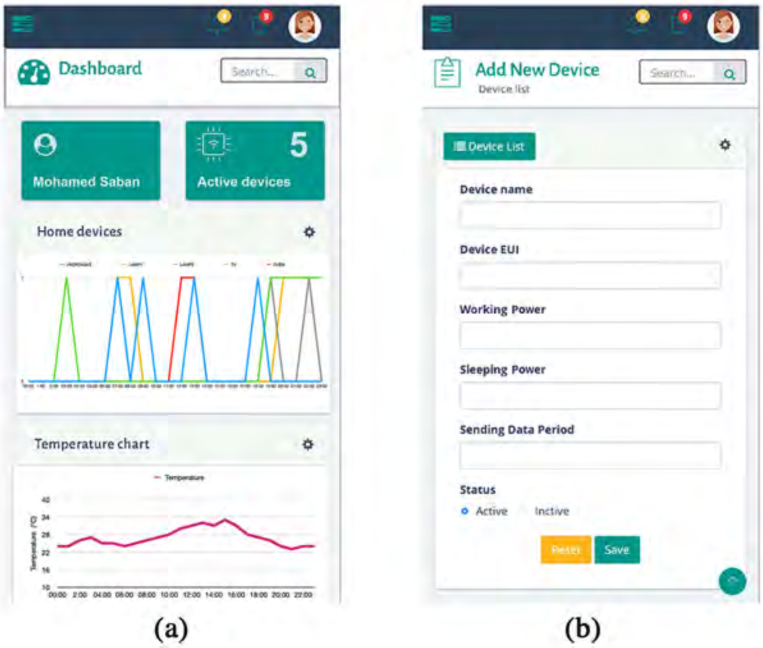


Figure 5.29: Screenshots from the monitoring and web application. (a) Dashboard page, (b) register new device.

The web application developed in this work is intended to be used by either the elderly person's family or the healthcare entity responsible for their wellbeing, such as their family doctor or healthcare center. To ensure timely response in emergency situations, the web application has been integrated with instant messaging applications such as WhatsApp and Telegram, facilitating rapid communication.

5.4.2 Discussion

This project presented a novel, cost-effective, and versatile system to monitor and evaluate the activities of the elderly who live alone. Figure 5.30 illustrates the whole monitoring system in a village where different devices in multiple houses can transmit their data to one gateway.

The system does not require the elderly to wear any sensors or have access to the internet since communication is achieved through wireless LoRa communication. This makes it particularly useful in remote locations where regular supervision of the elderly is difficult to achieve. The proposed LoRa system can be implemented in any location but is intended for areas with limited internet access, utilizing LoRa as the communication channel. Experimental tests revealed that the proposed smart plug

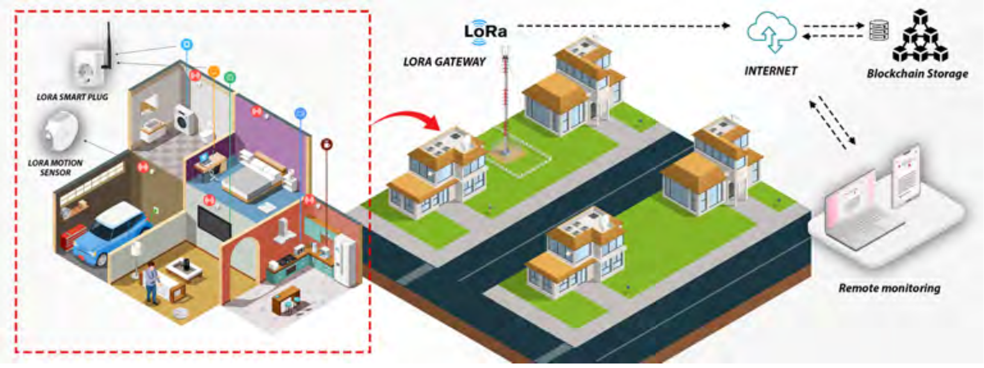


Figure 5.30: General scheme of the LoRa monitoring system

can transmit information to a gateway located within a 500-meter radius, which can cover multiple houses in a wide area.

This study introduced a new LoRa smart plug in addition to other commercial LoRa sensors such as temperature, humidity, and presence. The smart plug plays a crucial role in the proposed system, as it provides valuable information about the usage of electrical appliances and lights in the house. Any unusual or inappropriate use of certain appliances may indicate a wellness issue for the resident. In the event of an alert, the plug can be remotely disconnected. All sensor data are securely stored using Blockchain technology to safeguard users' privacy. The combination of Proof-of-Steak (PoS) with LoRa is a novel and effective way to provide decentralized and secure data storage.

The developed web application provides the ability to define users, homes, and appliances associated with each house. Users can manage all alarm options, monitor and analyze data collected, and define instant messaging via WhatsApp and Telegram for communication with responsible parties. The MVC design of the web application makes it easy to update for future changes and responsive for multiple platforms.

Chapter 6

Conclusions and Future work

"When you want something, all the universe conspires in helping you to acheive it."

- Paulo Coelho

6.1 Summary of obtained results

The main objective of this thesis has been to conduct a thorough study and analysis of various communication protocols and technologies used to build complete IoT infrastructures. The key features of these protocols was studied, including their message formats, packet sizes, data rates, and energy consumption. These protocols were compared to determine their advantages and disadvantages, in order to identify the most suitable communication protocols for each IoT application. The aim was to explore the strengths and weaknesses of different communication protocols, including their reliability, efficiency, and scalability.

Sensors are the backbone of any IoT systems and play a crucial role in collecting data from the environment. Delving into lower layers of IoT systems by developing new sensors allow to understand better the technology, customize the programming for specific tasks, optimize power consumption, and build robust systems. In this thesis, three different IoT sensors were developed to demonstrate the importance of sensor development in understanding and optimizing IoT systems, and to ensure that the IoT system meets those requirements and overcomes the challenges.

The first sensor developed was a short-range Bluetooth Low Energy (BLE) moisture sensor. This sensor was designed to measure the moisture content in wood and transmit the data to a central server for further analysis. The sensor was optimized for low power consumption to ensure long battery life, making it suitable for use in remote areas where access to power is limited. The second and third sensors were based on Long-Range (LoRa) technology, which allows for wide communication range with low power consumption. The second sensor was a wood moisture sensor suitable for use in large-scale buildings specially cultural heritage buildings, such as museums and old churches, where the rood and walls were made typically of wood, while the third sensor was a smart plug that aims to measure the power consumption of home appliances and notify when a device is turned on/off. This smart plug uses LoRa to transmit the data to a cloud server, where it can be analyzed to provide insights into energy consumption patterns. This device can be used in homes and it was developed specifically to build an IoT system for home monitoring of elderly who live alone in villages. The use of LoRa technology helps to transmit data over large distance which make it suitable in rural areas, where not all houses have internet coverage.

Web applications represent an important component of IoT systems as they provide an interface for users to interact with the system and access the data collected by the IoT devices, in addition to monitor and control these devices remotely. Various technologies can be used to develop a web monitoring application for IoT systems, including PHP Laravel which is a powerful and flexible PHP framework that simplifies the development of web applications and it is widely used in web development. This thesis showcased the development of web applications based on Laravel for each IoT system presented. These web applications were customized to offer users a remote interface to monitor and control the IoT devices. The customizations ensured that each web application met some specific requirements and challenges.

In order to integrate a decentralized infrastructure with IoT systems, the Blockchain technology was used. It provides a secure and transparent method of storing data. Decentralization is critical in saving data, particularly sensitive information, it eliminates a central point of failure, making it difficult for hackers to access, and it can improve system performance, reduce the cost of data storage, and increase system reliability. The integration of Blockchain with IoT can bring several benefits to the system. For instance, it can improve the security and privacy of sensitive data, reduce the cost of data storage, and increase system scalability. With Blockchain, data is stored in a tamper-proof manner, making it difficult for hackers to alter or manipulate it. This feature is especially important for IoT systems that handle sensitive data, such as healthcare and financial data. Moreover, By using smart contracts, access to data can be restricted based on pre-defined conditions, such as user identity and device location. This feature can help prevent unauthorized access to data, improve system security, and protect user privacy.

In this thesis, the integration of the Swarm Ethereum blockchain into an IoT system was achieved. The extension of the LoRaWAN system was accomplished by integrating the Swarm network, which provided a secure and decentralized method of managing data storage, access control, and authentication. The integration of the Swarm network enhanced the security and privacy of data in the IoT system, as well as increased the scalability of the system. Overall, the integration of the Swarm network demonstrated the potential of blockchain technology to improve the performance and security of IoT systems.

6.2 Conclusions

The general objective of this thesis is to explore the vast and growing field of the IoT. The aim is to study various aspects of IoT technology, including the communication protocols, the development of novel sensors and web monitoring applications in order to provide insights into how to build robust and reliable IoT systems across various fields such as healthcare, transportation, and smart cities.
The specific objectives that were raised at the beginning of the thesis were:

- Experimental analysis of IoT communication protocols including the development, design and implementation of new low-cost IoT sensors that can be used in several IoT applications.

- Optimization of the low level embedded program of the developed IoT node for better communication and low power consumption, especially in the stand-by mode.

- Development of new IoT web applications that can display real-time data using a dynamic User Interface (UI) in order to provide valuable insights to users by enabling the display of constantly changing data.

- Enhancing the security of the IoT network, by leveraging decentralized databases using Blockchain technology in order to ensure the privacy of collected data.

The thesis has successfully achieved its objectives by employing novel analysis methodologies and introducing several innovative designs that have practical applications in the latest communication standards.

6.3 Future Work

The PhD thesis has shed new light on the potential of IoT systems and opened up exciting new avenues for research and innovation. However, there are some unresolved issues that are considered to be of strategic importance for future research.
The topics to be investigated are as follows:

- Artificial Intelligent (AI): AI can provide the necessary intelligence and decision-making capabilities and predictive analytics to IoT systems, making them more efficient and effective. By analyzing the massive amounts of data generated by IoT devices, AI can help identify patterns and insights that can be used to optimize operations and improve overall performance.

- Edge computing: Edge computing is a promising technology that can address some of the challenges of IoT, such as latency, scalability, and security. Future research could explore the potential of edge computing for IoT systems, including how it can be used to improve performance and reduce data transfer.

- Energy harvesting: Energy harvesting technologies can enable IoT devices to generate their own power, reducing the need for batteries and improving their lifespan. Future research could explore the potential of energy harvesting for IoT, including how it can be used to power low-power IoT devices.

- Analyze and evaluate the effectiveness of Thread and 5G NR communication protocols for deploying new IoT systems. Thread is a wireless mesh networking protocol designed specifically for low-power IoT devices in homes, which utilizes IPv6 and is optimized for low-power devices and networks, making it an ideal choice for smart homes and other IoT applications. On the other hand, 5G NR is the latest cellular networking standard that provides high-speed, low-latency communication for various applications, including IoT. With better coverage, lower latency, and higher bandwidth than previous cellular standards, 5G NR is suitable for a wide range of IoT applications, such as industrial automation and smart transportation.

Appendix 1

Resumen Amplio

1 Introducción

En los últimos años se han producido rápidos avances en diversos ámbitos tecnológicos, como la informática integrada, la miniaturización del hardware, la detección y las redes inalámbricas. Esto ha permitido que internet se extienda más allá del mundo virtual y conecte objetos físicos, como puertas, coches y árboles, dotándolos de identificadores únicos y de la capacidad de percibir, procesar información y responder a su entorno, creando un mundo inteligente. La conexión de estos objetos inteligentes a Internet para interactuar con ellos de forma inalámbrica nos introduce en el concepto de Internet de las Cosas (IoT). Esta tesis doctoral está dedicada al enrutamiento y búsqueda de sensores en el IoT, analizando las tecnologías de comunicación y la seguridad de los sistemas IoT.

1.1 Motivación

Las aplicaciones basadas en IoT ofrecen muchas soluciones para facilitar nuestra vida cotidiana. Actualmente, la IoT está evolucionando en muchos sistemas domésticos e industriales [1]. La International Data Corporation (IDC) prevé que el número de dispositivos conectados a IoT alcance los 41.600 millones en 2025 [2]. Estos dispositivos están conectados a servidores en la nube que procesan los datos recogidos, lo que permite a los usuarios controlarlos y supervisarlos a distancia a través de aplicaciones web y móviles. Los avances en el campo de las redes inalámbricas han llevado a la creación de importantes tecnologías de comunicación e identificación inalámbricas como IEEE 802.15.4, Bluetooth, Bluetooth Low Energy (BLE), Ultra-Wide Bandwidth (UWB), IPv6, Radio Frequency Identification (RFID), Near-Field Communication (NFC) y Low Power Wide Area Network (LPWAN).

La selección del protocolo de comunicación IoT adecuado es crucial y depende del tipo específico de aplicación IoT. Cada protocolo tiene sus propias ventajas, desventajas y condiciones de despliegue. A la hora de elegir la mejor opción para un proyecto IoT, se deben considerar detenidamente los siguientes criterios para garantizar que el protocolo elegido se alinea con las necesidades y limitaciones específicas de cada proyecto:

- **Capacidades de los dispositivos.** Los dispositivos IoT admiten un protocolo de comunicación específico. La selección de un dispositivo está relacionada con el protocolo que se va a utilizar.
- **Consumo de energía.** Este problema sale a la luz cuando la red IoT se despliega en un entorno exterior, cuando los dispositivos funcionan con baterías y no con una línea eléctrica directa, como los dispositivos domésticos inteligentes.
- **Requisitos de respuesta sincrónica.** Si el sistema IoT requiere una respuesta inmediata a las acciones, debe seleccionarse un patrón de comunicación síncrono.
- **Conectividad.** Factores como la velocidad de transmisión de datos, el alcance de la comunicación y la latencia deben tenerse en cuenta en función del tipo de conexión.
- **Seguridad.** La seguridad de los protocolos de comunicación también debe tenerse en cuenta en función del objetivo del sistema y de la información intercambiada.
- **Presupuesto asignado.** Los costes de instalación dependen de múltiples factores, como la banda de frecuencia, el coste de los dispositivos finales y el coste de las estaciones base.

Otro elemento importante en los sistemas IoT son las aplicaciones web. Estas aplicaciones se utilizan ampliamente para simplificar la gestión de los dispositivos IoT y mejorar el valor que las organizaciones pueden extraer de sus despliegues IoT. Desarrollar una aplicación web robusta para IoT es una tarea compleja que requiere una cuidadosa consideración de varios factores, incluida la elección de la tecnología. La tecnología elegida debe tener la capacidad de manejar grandes volúmenes de datos de manera eficiente y sin sacrificar el rendimiento. Además, debe contar con sólidas funciones de seguridad, como autenticación, cifrado y controles de acceso, para impedir el acceso no autorizado a la aplicación y los datos. La Web actual está pasando a la siguiente generación, conocida como Web 3.0, uno de cuyos aspectos fundamentales son la propiedad y la descentralización. El uso de bases de datos descentralizadas impulsadas por la tecnología Blockchain podría resolver algunos de los retos más críticos a los que se enfrenta el IoT. Con blockchain, cualquier dato puede registrarse de forma inmutable y distribuida, a diferencia de la actual infraestructura de IoT, que depende de intermediarios y entidades centralizadas para validar los datos. En la Web 3.0 IoT, blockchain transformaría la estructura de IoT de cliente-servidor a peer-to-peer. Los mecanismos de consenso pueden utilizarse para verificar las transformaciones y abordar la fiabilidad, convirtiendo IoT en un sistema sin confianza que permite la comunicación directa entre dispositivos sin intermediación.

En esta Tesis doctoral se estudian y analizan los protocolos de comunicaciones IoT en diferentes circunstancias con el fin de comparar los resultados teóricos y los experimentales. Este análisis ayuda a verificar el rendimiento y los límites de cada tecnología que conducirá a una buena distribución de los nodos finales de la red. Además, se han desarrollado y probado sensores específicos. El desarrollo de nuevos sensores IoT también forma parte del estudio y tiene diferentes intereses que deben tenerse en cuenta, como los costes, la calidad y el plazo de entrega. En esta tesis también se presenta un enfoque para asegurar el IoT utilizando la tecnología Blockchain que proporciona un almacenamiento descentralizado de datos. A través de este enfoque, el procesamiento de datos de las aplicaciones IoT será seguro y rápido.

1.2 Objetivos

El objetivo de esta tesis es abordar diferentes temas relacionados con el desarrollo, el diseño y la implementación de nodos sensores para múltiples redes IoT. Se han formulado cuatro objetivos:

- **Objetivo 1:** Análisis experimental de protocolos de comunicación IoT. Este objetivo incluye el desarrollo, diseño e implementación de nuevos sensores IoT de bajo coste que puedan ser utilizados en diversas aplicaciones IoT.

- **Objetivo 2:** Optimización del programa embebido de bajo nivel del nodo IoT desarrollado para una mejor comunicación y un bajo consumo de energía, especialmente en el modo stand-by. Este objetivo implica el análisis, caracterización y evaluación de los nodos sensores en diferentes entornos. Se han realizado múltiples pruebas para este objetivo.

- **Objetivo 3:** Desarrollo de nuevas aplicaciones web IoT que puedan mostrar datos en tiempo real utilizando una Interfaz de Usuario dinámica (UI) que está diseñada teniendo en cuenta la facilidad de uso para proporcionar una experiencia intuitiva. Este objetivo pretende proporcionar información valiosa a los usuarios al permitir la visualización de datos en constante cambio.

- **Objetivo 4:** Mejorar la seguridad de la red IoT, aprovechando las bases de datos descentralizadas que utilizan la tecnología Blockchain, que reforzará la seguridad de la comunicación de los datos gracias a los robustos protocolos criptográficos.

1.3 Contribución

Los siguientes puntos pretenden contribuir al ecosistema IoT a través de esta tesis:

- Se proponen nuevos sensores IoT. Se han desarrollado y probado tres nodos finales IoT diferentes de bajo coste, controlados digitalmente y energéticamente eficientes, tal y como se propone en esta tesis. El primer sensor es un sensor de humedad de la madera, que utiliza conectividad inalámbrica BLE. Se ha desarrollado un segundo sensor de humedad de la madera utilizando un método de resistencia avanzado y conectividad inalámbrica LoRa de largo alcance. El tercer sensor es un enchufe inteligente que utiliza tecnología LoRa. El objetivo de este dispositivo es controlar el uso de los aparatos eléctricos en los hogares.

- Como parte de esta tesis doctoral se han desarrollado nuevas aplicaciones web basadas en el framework PHP Laravel para la gestión de los sistemas IoT.

- Un nuevo sistema basado en tecnología BLE para monitorizar el contenido de humedad de la madera en casas de madera. El sistema incluye el desarrollo de un dispositivo de humedad BLE y una nueva aplicación web.

- Un novedoso sistema IoT basado en tecnología LoRa para la monitorización del contenido de humedad de la madera en edificios de madera patrimoniales e históricos. El sistema incluye el desarrollo de un dispositivo de humedad LoRa y una nueva aplicación web.

- Un novedoso sistema para determinar el bienestar de las personas mayores que viven solas en pueblos basado en la tecnología LoRa. Incluye el desarrollo de un dispositivo de monitorización basado en LoRa para controlar el uso de electrodomésticos.

- Un sistema de agricultura inteligente basado en la tecnología LoRa mediante la adición de la conectividad inalámbrica LoRa a un controlador lógico programable (PLC) regular que ya se utilizan en las granjas, junto con el desarrollo de una nueva aplicación web para la supervisión y gestión.

- Un modelo de seguridad para redes LoRaWan basado en la tecnología Blockchain para disponer de un almacenamiento distribuido de los datos recogidos. Para ello se utilizó la red blockchain Swarm Ethereum.

2 Estado del arte

En los debates sobre IoT se oye a menudo el término (abreviado: WSN). WSN son las siglas de Wireless Sensor Networks (redes de sensores inalámbricos), que son redes de sensores interconectados que se comunican entre sí de forma inalámbrica y pueden utilizarse para la recopilación y transmisión de datos en tiempo real en diversas aplicaciones dentro del ecosistema IoT. Estos sensores, comúnmente conocidos como nodos sensores o nodos finales, tienen la capacidad de percibir, medir y recopilar información de su entorno, y luego utilizar procesos locales de toma de decisiones para transmitir los datos a una ubicación central o a un servidor basado en la nube para su análisis y toma de decisiones. Además, se caracterizan por su pequeño tamaño, bajo consumo y rentabilidad, y por sus capacidades de comunicación inalámbrica.

Es crucial optimizar la comunicación y minimizar el uso de energía en las WSN, ya que la implementación de protocolos en diferentes capas de la pila de protocolos puede afectar significativamente al consumo de energía, al retardo de extremo a extremo y a la eficiencia del sistema. Sin embargo, los protocolos de red tradicionales no se adaptan bien a las WSN porque no están diseñados para satisfacer los requisitos específicos de estas redes. Por ello, se han propuesto nuevos protocolos energéticamente eficientes para todas las capas de la pila de protocolos de las WSN. Estos protocolos emplean la optimización entre capas, que implica compartir la información de estado del protocolo entre todas las capas para cumplir los requisitos específicos de la WSN. Este enfoque permite una comunicación más eficiente y una mejor gestión de los recursos de la red.

2.1 Red de sensores inalámbricos de corto alcance

Existen varias tecnologías inalámbricas diseñadas para la comunicación en distancias cortas, normalmente de unos pocos metros. Estas tecnologías se conocen como comunicación inalámbrica de corto alcance. Por el contrario, la comunicación inalámbrica de medio alcance permite la comunicación a distancias de hasta 100 metros, mientras que la comunicación inalámbrica de área amplia puede alcanzar distancias que van desde varios kilómetros hasta miles de kilómetros. Algunos ejemplos de comunicación inalámbrica de corto alcance son Bluetooth, infrarrojos, comunicación de campo cercano, UWB, WiFi y ZigBee.

Bluetooth Low Energy (BLE) es con frecuencia la opción preferida para numerosas aplicaciones IoT debido a su bajo consumo de energía, como se destacó en la sección anterior, y la compatibilidad con diversas plataformas, incluyendo teléfonos inteligentes y tabletas, lo hacen ideal para aplicaciones IoT que requieren conectividad con estos dispositivos. BLE proporciona sólidos servicios de seguridad para salvaguardar el intercambio de información entre los dispositivos conectados. En esta Tesis se ha elegido la tecnología BLE para desarrollar un novedoso sensor IoT.

2.2 Red de sensores inalámbricos de largo alcance

La comunicación inalámbrica de largo alcance se refiere al uso de tecnologías de radio inalámbricas para permitir la comunicación entre dispositivos a grandes distancias, normalmente decenas de kilómetros. Estas tecnologías, conocidas como redes de área extensa de baja potencia (Low-Power Wide-Area Networks, LPWAN), han atraído una gran atención tanto en el mundo académico como en la industria, con ejemplos tempranos como Sigfox y LoRa. Con la reciente aparición de tecnologías como la evolución a largo plazo (Long-Term Evolution, lte-M) y Narrowband-IoT (Narrowband-IoT, NBIoT), y el inminente despliegue de 5G, el panorama de la conectividad IoT está cambiando rápidamente. Es crucial comprender el papel de la LPWAN en este panorama, así como la forma de evaluar los costes y beneficios de las diferentes tecnologías LPWAN con el fin de tomar decisiones informadas sobre las opciones de conectividad.

En esta tesis se ha elegido la tecnología LoRa de largo alcance para desarrollar un nuevo sensor IoT. LoRa consta de dos capas: la capa física y la capa MAC. Como se muestra en la figura 2.18, La capa física está patentada por Semtech [88] y se basa en Chirp Spread Spectrum (CSS), proporcionando una alta sensibilidad del receptor y una mayor resistencia al ruido mediante el uso de mensajes de corrección de errores hacia adelante [101]. El protocolo de capa MAC y la arquitectura del sistema, conocidos como LoRaWAN, están estandarizados por la LoRa Alliance [260] para garantizar una comunicación fluida y la compatibilidad entre dispositivos. LoRa utiliza el espectro radioeléctrico sin licencia en la banda de ISM, lo que proporciona un amplio alcance y accesibilidad.

2.3 Aplicación de supervisión web de IoT

En el ecosistema IoT, las aplicaciones web representan un componente crítico que desempeña un papel vital en la gestión y el análisis de los datos recogidos de los nodos finales, y permiten a los usuarios interactuar con los sistemas IoT en tiempo real, proporcionando acceso a datos críticos desde cualquier parte del mundo. Estas aplicaciones permiten a los usuarios supervisar y controlar a distancia los dispositivos IoT, haciendo posible ajustar la configuración, analizar el rendimiento y recibir alertas si algo va mal. Las aplicaciones web también proporcionan una plataforma para analizar los datos recogidos por los dispositivos IoT para ayudar a los usuarios a identificar tendencias, detectar anomalías y tomar decisiones informadas mediante el uso de herramientas de visualización de datos.

Laravel fue elegido para desarrollar las diversas aplicaciones web utilizadas en esta

Tesis. Se trata de un framework PHP utilizado para el desarrollo de aplicaciones web siguiendo el patrón arquitectónico modelo-vista-controlador (acrshortmvc). Proporciona mucha flexibilidad para personalizar los ajustes y configuraciones según los requisitos del desarrollador. En general, Laravel proporciona un amplio conjunto de características de seguridad que ayudan a proteger las aplicaciones web de las amenazas de seguridad comunes. Los desarrolladores pueden utilizar estas características para mejorar la seguridad de sus aplicaciones y minimizar el riesgo de violación de datos u otros incidentes de seguridad.

2.4 Tecnología Blockchain

Un blockchain es un libro de contabilidad digital, descentralizado y distribuido que registra las transacciones en múltiples ordenadores, de modo que el registro no puede alterarse retroactivamente sin la alteración de todos los bloques posteriores y el consenso de la red. Esto permite un registro seguro y transparente de las transacciones. Como se describe en la figura 2.32, cada bloque de una cadena de bloques contiene una lista de transacciones, y una vez que un bloque se añade a la cadena es muy difícil alterar la información que contiene [132]. En una cadena de bloques, un bloque contiene varios elementos de información, entre ellos

Un identificador único, llamado "hash del bloque", que lo distingue de otros bloques de la cadena. Una marca de tiempo que registra cuándo se creó el bloque. Un conjunto de transacciones o datos que se añaden a la cadena de bloques. Una referencia al bloque anterior de la cadena, que crea un vínculo entre los bloques. Un nonce, que es un número aleatorio utilizado en el proceso de minería para resolver el rompecabezas criptográfico y añadir el bloque a la cadena de bloques.

La naturaleza descentralizada de una cadena de bloques la hace resistente a la manipulación y la censura, ya que no existe un único punto de control. El uso de la tecnología blockchain no se limita sólo a las transacciones financieras, y tiene potencial para aplicarse a una amplia gama de aplicaciones más allá de las criptomonedas.

La tecnología blockchain tiene un inmenso potencial para revolucionar el IoT. Al incorporar blockchain, IoT puede mejorarse con un servicio de intercambio de confianza que garantice una información fiable y rastreable. Esto significa que las fuentes de datos pueden identificarse en cualquier momento y que los datos permanecen inmutables, lo que aumenta significativamente su seguridad.

En esta tesis, se selecciona la Blockchain de Ethereum Swarm para integrarla con la red LoRaWAN porque proporciona una infraestructura escalable y autosostenible para una economía de cadena de suministro de datos, a diferencia de la blockchain de Ethereum. Además, el tiempo de transacción es más rápido y barato. La red LoRa se amplía almacenando los datos recibidos en el servicio de almacenamiento

Swarm Ethereum, y definiendo una forma clara de almacenar, acceder y recuperar los datos mediante contratos inteligentes Swarm y Ethereum. La integración de una blockchain pública en la red LoRaWan asegurará los datos transmitidos para un almacenamiento de datos seguro e inmutable.

3 Desarrollo de un sensor IoT BLE de corto alcance

Esta sección presenta un sensor de humedad rentable y compacto. Este sensor utiliza un método de medición de resistencia que es preciso para un amplio rango de valores de resistencia. Cuenta con control digital a través de un micro-controlador habilitado para BLE que es pequeño en tamaño y bajo en consumo de energía, lo que garantiza una larga duración de la batería.

3.1 Medición de la humedad

Las características de los materiales pueden evaluarse a través de su impedancia. Se han desarrollado diversos instrumentos de medida y circuitos electrónicos para determinar la impedancia de un material o grupo de materiales similares. La medición precisa de valores de resistencia elevados por encima de GΩ suele requerir el uso de instrumentos especializados como electrómetros o megóhmetros/picoamperímetros [179]. Estos instrumentos, sin embargo, no son prácticos para uso portátil debido a su tamaño y peso. Emplean métodos de medición de tensión constante o de corriente constante, siendo el de tensión constante (el método más utilizado) el que mide la resistencia desconocida conectándola en serie con el circuito electrónico y midiendo la corriente circulante, para luego determinar el valor de la resistencia mediante la ley de Ohm. Sin embargo, este proceso no es sencillo, ya que un único circuito electrónico puede no ofrecer resultados precisos para una amplia gama de valores de resistencia, especialmente en el caso de materiales como los de construcción, los textiles y los tejidos biológicos. Con el objetivo de crear un dispositivo de medición preciso y versátil que sea ligero y compacto, proponemos utilizar la tecnología más avanzada para diseñar un circuito electrónico que supere las limitaciones actuales.

3.2 Circuito electrónico

El circuito propuesto emplea un multiplexor en el bucle de realimentación del amplificador operacional para evitar la saturación y alcanzar la máxima tensión de salida (Vo). El multiplexor modula la ganancia ajustando el valor de R_f en función de R_x. Se han incluido tres valores diferentes de R_f y el multiplexor está controlado por la parte digital. Para valores de R_x en el rango [1,50] MΩ, R_f se ajusta a 680 KΩ; para valores de R_x en el rango [50 MΩ, 3 GΩ], R_f se ajusta a 33 MΩ, y para valores de R_x en el rango [1,5, 100] GΩ, R_f se ajusta a 1 GΩ. Un procedimiento automático de detección de subtensión se utiliza para seleccionar automáticamente Rf, donde la tensión del amplificador cae en el rango [0,6, 3,5] V. Es importante elegir cuidadosamente el multiplexor, ya que su rendimiento real puede desviarse significativamente del modo de trabajo ideal [181], como se discutirá más adelante. Tras la amplificación, se incluye un filtro de paso bajo Sallen-Key para eliminar la contribución de ruido.

El circuito del dispositivo BLE desarrollado se compone de dos placas, digital y analógica, para reducir las interferencias. La interfaz entre las placas analógica y digital consta de 8 pines, incluyendo 2 pines de tierra, una interfaz de bus I2C para el convertidor A/D, 3 líneas de control para el multiplexor analógico para regular la ganancia, y una única línea de apagado analógico para la optimización de la alimentación mediante la activación y desactivación de la fuente de alimentación analógica. Todas las líneas de esta interfaz funcionan a 3V. La figura 3.3 ilustra el circuito.

El dispositivo BLE mide la resistencia eléctrica de corriente continua (CC) de la madera para calcular el contenido de humedad. El modelo de regresión utilizado para obtener el valor de humedad a partir de la resistencia se describe mediante la ecuación 3.2, donde a, b, y c son variables que dependen del tipo de madera y la se puede obtener a partir de la resistencia eléctrica media a diferente nivel de contenido de humedad [185]. La figura 3.4 ilustra la resistencia en función de la humedad para varias especies de madera.

El componente central de la placa digital es el SoC CYBLE-012012-1 de Cypress. Este módulo cuenta con un procesador de 32 bits con una velocidad de reloj de hasta 48 MHz y un impresionante rendimiento de 0,9 DMIPS/MHz. Fue seleccionado por su tamaño compacto de 14,52 mm x 19,20 mm x 2,00 mm y la capacidad de conectarse a hasta 23 entradas/salidas de propósito general configurables (GPIOs), lo que permite la integración de placas electrónicas adicionales. Además, incorpora un módulo monomodo cualificado para Bluetooth 4.1. Las especificaciones de consumo y transmisión del módulo se detallan en la tabla adjunta 3.2. El valor de resistencia instantánea se obtiene promediando las últimas 50 mediciones (a lo largo de una ventana deslizante) y determinando el valor fisicoquímico del material mediante propiedades de resistencia precalculadas.

3.3 Conclusión

El sensor BLE se hizo portátil mediante la integración de circuitos adicionales para una fuente de alimentación por batería, como se muestra en la figura (a). Funciona con tres pilas AAA que proporcionan 4,5 V. El tamaño compacto del circuito es de 5,7 cm x 5,3 cm x 3 cm. Se diseñó una carcasa protectora de material epoxi para encerrar el sensor, con sondas de acero inoxidable para evitar la corrosión debida al uso continuo. El prototipo del producto final se muestra en la figura (b). El sensor de humedad BLE desarrollado funciona con batería. Una batería de larga duración es un requisito crucial para este tipo de dispositivos. El dispositivo está programado con una solución de bajo consumo, como se muestra en el diagrama de flujo representado en la Figura 3.7: el dispositivo envía los datos a la pasarela y entra en modo de sueño profundo, despertando en la siguiente notificación de la pasarela. Este modo de sueño profundo permite al dispositivo BLE minimizar el consumo de energía y prolongar la duración de la batería. El dispositivo desarrollado es un componente crítico en el despliegue de un sistema IoT de vanguardia basado en la tecnología BLE. Este sistema aprovechará las capacidades de BLE para proporcionar una gran comunicación y transferencia de datos entre los dispositivos conectados.

4 Desarrollo de un sensor IoT LoRa de largo alcance

Esta sección presenta un sensor de humedad compacto y rentable que utiliza un microcontrolador habilitado para LoRa, que permite el control digital del dispositivo, lo que lo hace altamente versátil y flexible. El propio sensor de humedad está diseñado con un novedoso método de medición de resistencia, que ofrece lecturas precisas en un amplio rango de valores de alta resistencia.

4.1 Medición de la humedad

El dispositivo de medición de la humedad que se presenta en esta sección está diseñado específicamente para su uso en edificios del Patrimonio Cultural. El contenido de humedad (MC) en la madera se refiere al porcentaje de la masa de agua presente en la madera con respecto a la masa de madera seca. Según la norma EN 16682 [188], se favorece el método de medición de la resistencia para la monitorización continua del MC en estructuras y edificios de patrimonio de madera [189].

Para este dispositivo, se propone un novedoso método de medición de resistencia de corriente alternativa (CA), que elimina la necesidad de un análisis de frecuencia previo. El método se basa en un oscilador de relajación simple y eficiente, como se representa en la Figura 4.1. A diferencia de otros métodos de CA [205, 207] que requieren un estudio previo para fijar la frecuencia, este método ajusta automáticamente su frecuencia f en función de la resistencia eléctrica equivalente de la madera (R_w en la Figura 4.1). El condensador C_2 se carga y descarga a través de la tensión V_0 y la resistencia R_w, produciendo una señal cuadrada que oscila entre $+V_{sat}$ y -V_{sat} cuando V_t alcanza los valores umbral V_{tmax} y V_{tmin}, respectivamente, como se muestra en la Figura 4.1. El periodo de oscilación T es linealmente proporcional a la resistencia eléctrica equivalente de la madera (R_w), dada la simetría de las tensiones de saturación $+V_{sat}$ y -V_{sat} en el amplificador operacional U_1, como Ecuación 4.3. La resistencia de la madera, R_w, puede determinarse indirectamente midiendo el período de tiempo, T, de la oscilación. Este período se mide utilizando un microcontrolador y se convierte en la resistencia de la madera a través de un programa que ajusta los niveles de tensión en el circuito (como se ve en la Figura 4.1). Este método, que fue presentado previamente por los autores en [206], elimina la necesidad de un estudio previo para estimar la frecuencia óptima de CA, permitiendo un proceso más eficiente y ágil.

El amplificador operacional U_1 de la figura 4.1 requiere una alimentación de ±15 V, que es generada por el convertidor elevador de baja entrada TPS61093DSK. Este regulador está diseñado con un pin de habilitación que permite al microcontrolador encender el circuito sólo cuando se está midiendo la resistencia de la madera, conservando así la energía de la batería. Una vez realizadas las mediciones, el dispositivo envía el valor medio a la pasarela y entra en modo reposo durante un periodo de tiempo configurable por el usuario a través de la plataforma web de monitorización. El nodo sensor, también incluye un sensor de temperatura LM335DT, ya que la conversión del contenido de humedad a partir de la medida R_w depende también de la temperatura [208–210]. El LM335DT presume de una impresionante precisión de ±1 °C.

4.2 Circuito electrónico

El nuevo sensor desarrollado para medir la MC en la madera tiene un diseño compacto y puede dividirse en cuatro componentes principales como descrito en la figura 4.2:

- La unidad de Detección: Esta sección contiene un novedoso circuito de medición de CA diseñado para medir la MC de la madera, así como un sensor de temperatura.
- La Unidad de Procesado: Esta sección está equipada con un microcontrolador programable que ha sido programado para gestionar las funciones de detección y comunicación LoRa. El firmware también dispone de funciones de gestión de la alimentación para ahorrar energía.
- La Unidad de Comunicación: Esta sección permite el intercambio de datos entre el nodo sensor y la pasarela LoRa utilizando el protocolo de comunicación LoRa.
- La unidad de alimentación: El sensor se alimenta con dos pilas AAA estándar de 1,5 V. Esta sección regula la fuente de alimentación para proporcionar una salida constante de 3,3 V para las Unidades de Procesamiento y Comunicación,

así como genera una fuente de alimentación simétrica de ±15 V CC para la Unidad de Detección.

Las capacidades de procesamiento y comunicación del sensor de nodo final están integradas en el módulo WiMOD iM881-XL de IMST [211]. El iM881-XL está equipado con un microcontrolador programable STM32L081 optimizado para aplicaciones alimentadas por batería. El firmware específico para el sensor residirá en esta unidad. La placa resultante tiene un tamaño de 81 × 83 mm, ofrece versatilidad en términos de conectividad de antena con la opción de utilizar una antena interna para reducir el tamaño o una antena externa para mejorar el alcance. En la placa hay un interruptor que permite alternar entre ambas opciones. La figura 4.3 ilustra la placa electrónica del dispositivo.

Para proteger el circuito electrónico del polvo y otros factores ambientales, se diseñó una caja de plástico a medida utilizando tecnología de impresión 3D. La caja se diseñó para ajustarse perfectamente a las dimensiones de la placa de circuitos que protegía eficazmente los componentes electrónicos de posibles daños. Las figuras 4.4(a) y 4.4(b) ilustran las caras frontal y posterior del prototipo de dispositivo de humedad, respectivamente. El componente azul, como se muestra en la Figura 4.4(b), con dos clavos inoxidables de 0,7 mm de diámetro, se fija al techo de madera y luego se conecta al dispositivo. El dispositivo de humedad funciona con dos pilas AAA de 1,5 V.

4.3 Conclusion

El dispositivo MC LoRa se diseñó desde cero y cuenta con una novedosa placa electrónica que funciona con pilas y con un método de medición basado en CA que utiliza un oscilador de relajación. La frecuencia del oscilador se ajusta automáticamente en función de la resistencia de la madera, que está directamente correlacionada con la MC. Los resultados de los experimentos indican que el sistema desarrollado tiene una diferencia máxima de MC de $\pm 1,7$ en comparación con el método de secado al horno. El nodo final LoRa es capaz de funcionar en un rango de temperatura de 0 °C a 50 °C con diferentes tipos de madera, y tiene mediciones estables durante largos períodos de tiempo. El dispositivo puede transmitir datos hasta 430 metros. El microcontrolador del nodo final está programado para despertar el dispositivo, activar los circuitos de detección MC, tomar la media de tres valores de medición y enviar los datos a la pasarela. A continuación, el dispositivo entra en modo de reposo hasta la siguiente hora de medición, que determina el usuario a través de la interfaz web Timbercare. Este modo de funcionamiento minimiza el consumo de energía y garantiza una larga duración de la batería. El sensor desarrollado desempeñará un papel crucial en el despliegue de un sistema IoT para la monitorización del contenido de humedad en el interior de edificios de madera del patrimonio cultural.

5 Despliegue de aplicaciones IoT e integración de Blockchain

Esta sección describe el despliegue de cuatro sistemas de monitorización IoT diferentes realizado en esta tesis.

5.1 Aplicación 1: Sistema de monitorización de la humedad de la madera basado en BLE.

Uno de los factores más importantes que afectan a sus propiedades es el contenido de humedad. La cantidad de agua contenida en la madera puede afectar significativamente a su peso y resistencia, haciéndola más débil y más susceptible a los ataques biológicos [225]. Por lo tanto, controlar el contenido de humedad de la madera es crucial para prever y prevenir daños, especialmente en edificios antiguos donde la madera ha estado expuesta a condiciones ambientales cambiantes a lo largo del tiempo.

Un sistema IoT de monitorización basado en Bluetooth Low Energy (BLE) representa una buena solución para la detección temprana de la humedad de la madera debido a fuertes lluvias, fugas y otros factores. Para implementar el sistema IoT propuesto para detectar el contenido de humedad en la madera, se utiliza el sensor de humedad BLE desarrollado anteriormente como nodo final. El sensor se colocará en varios lugares del edificio para proporcionar mediciones continuas y precisas del contenido de humedad.

El sistema propuesto consiste en un servidor en la nube que aloja una aplicación web de monitorización para la visualización y el control de los datos. El servidor en la nube recibirá los datos de los sensores a través de una Raspberry Pi que actuará como pasarela entre los nodos finales BLE y la base de datos del servidor en la nube. Esta arquitectura garantizará que los datos se transmitan de forma segura y eficiente al servidor en la nube, donde podrán ser analizados e interpretados para proporcionar información sobre el contenido de humedad de la madera. Con este sistema IoT, será posible detectar y prevenir los daños relacionados con la humedad, preservando la integridad estructural de los edificios y otras estructuras de madera.

La figura 5.1 ilustra el sistema de monitorización propuesto, que es muy flexible y puede adaptarse a diferentes funcionalidades en función de las necesidades del operador. La pasarela está equipada con secuencias de comandos Python para la comunicación BLE, el análisis de datos y el intercambio de datos Ethernet con el servidor.

Basándose en los resultados de las pruebas experimentales, se ha demostrado que el nodo sensor BLE es capaz de transmitir datos hasta una distancia de 71 metros, sin necesidad de ninguna amplificación de potencia adicional. Sin embargo, cabe señalar que una baja calidad de la señal puede provocar una falta de recepción de datos, como se observa en la posición P5, que representa el punto más lejano en el que se pudieron transmitir y recibir datos con precisión. De hecho, cualquier señal que supere los 92 dBm se considera inutilizable. Es importante tener en cuenta los efectos de bloqueo de paredes y obstáculos entre la pasarela y los nodos sensores, ya que pueden afectar al rendimiento del sistema. Por ello, se recomienda evaluar los efectos de bloqueo antes del despliegue, con el fin de determinar la ubicación óptima de los nodos sensores y garantizar una cobertura fiable y robusta para la red IoT.
El sistema de monitorización BLE presentado es muy versátil y puede implementarse en una gran variedad de entornos, incluidas iglesias antiguas en las que predominan las paredes y los tejados de madera, así como edificios de madera en los que la monitorización del contenido de humedad es esencial para prevenir ataques biológicos.

5.2 Aplicación 2: Sistema de humedad de la madera basado en LoRa

La aplicación anterior analizó un sistema IoT basado en BLE para controlar el contenido de humedad en la madera, que demostró un excelente rendimiento en la detección y transmisión de datos. Sin embargo, su limitado alcance de transmisión de solo 70 metros lo hace menos práctico para estructuras de madera más grandes, como edificios patrimoniales, donde el control de la humedad es crucial. Para resolver este problema, el presente sistema implementa un nuevo sistema de monitorización que utiliza la tecnología LoRa de largo alcance.
La arquitectura del sistema LoRa propuesta para los sensores de humedad de la madera consiste normalmente en los sensores de humedad de la madera, la pasarela LoRaWAN y un servidor en la nube que aloja una aplicación web para el análisis y la visualización de datos, como se ilustra en la Figura 5.8. El sistema utiliza el sensor de humedad LoRa desarrollado previamente y la pasarela WiMOD LoRa Lite, compuesta básicamente por una Raspberry Pi y un conector iC880A. The Things Network (TTN) se utiliza como plataforma para la comunicación LoRaWAN. Se desarrolló una interfaz web personalizada llamada "Timbercare" utilizando el enfoque Modelo-Vista-Controlador (MVC) basado en el framework Laravel e implementado con una base de datos MySQL. El front-end de la aplicación web se construyó utilizando el framework Bootstrap, que garantiza un diseño responsivo y la compatibilidad con dispositivos móviles, tabletas y ordenadores de sobremesa. El sistema de autenticación de la plataforma protege todos los datos, y sólo los usuarios autorizados tienen acceso a su panel de control específico.
Se ha realizado una prueba experimental en el Centro Cultural 'La Nau', un edificio de

importancia histórica que ha servido como sede de la Universidad de Valencia desde su fundación en el siglo XV hasta la primera mitad del siglo XX. Los resultados muestran que se recibieron el 100 % de los paquetes desde todos los puntos de medición. La Pérdida de Trayecto PL se estudió en el interior de este edificio y la Figura 5.12 demuestra que el PL medido en la entrada se alinea estrechamente con el modelo propuesto. Por lo tanto, la ecuación 5.1 es una representación adecuada de la propagación de radio LoRa en el interior del edificio.

Los sitios del patrimonio cultural tienen un valor incalculable en todo el mundo, ya que sirven como vínculos vitales con el pasado e importantes fuentes de inspiración para las generaciones futuras. La madera ha sido un material de construcción común durante siglos y, como tal, la monitorización de su contenido de humedad (MC) es esencial para prevenir posibles daños, especialmente en edificios antiguos que han estado sometidos a cambios ambientales a lo largo del tiempo. El sistema IoT presentado ayudará a monitorizar con precisión el contenido de humedad de la madera en edificios históricos puede ayudar a identificar posibles riesgos.

5.3 Aplicación 3: Sistema agrícola inteligente basado en PLC y LoRa

Las prácticas agrícolas como la plantación, la siembra, la cosecha, el riego y el cultivo dependen en gran medida de las condiciones climáticas, en particular la temperatura del aire, la humedad y la intensidad de las precipitaciones, ya que estos factores pueden afectar a la propagación de plagas y enfermedades que pueden causar pérdidas significativas en la producción mundial de alimentos, lo que representa el 40% de la pérdida total [234, 241]. Además, las actividades agronómicas consumen alrededor del 20% de la reserva mundial de agua, donde las pérdidas en las líneas, las fugas y el exceso de riego son las principales razones del despilfarro de agua [242]. Los sistemas de agricultura inteligente ofrecen una solución automatizada para supervisar y controlar los recursos naturales de la explotación y las condiciones de siembra sin intervención humana.

En este trabajo se presenta un sistema de agricultura inteligente que demuestra la integración de la comunicación LoRaWAN con los controladores lógicos programables existentes (PLCs) que se han utilizado en la agricultura durante décadas para regular múltiples procesos y maquinaria. Como resultado, los procesos automatizados anteriores pueden emplearse en granjas inteligentes sin sustituir los antiguos sistemas de control. El Simatic $IOT2040$, equipado con un escudo LoRa, se utiliza para integrar la conectividad LoRa con estos PLC. La comunicación entre el PLC y el $IOT2040$ se facilita a través del protocolo Modbus-TCP. El sistema propuesto emplea el PLC para controlar las funciones de las máquinas agrícolas, como las bombas de agua, y recibir datos de varios nodos sensores distribuidos por la granja. El procesamiento de los datos se realiza en un servidor en la nube, que emplea una

plataforma web segura, flexible y escalable para ofrecer una interfaz de usuario que permite la gestión remota de todos los dispositivos empleados en el sistema de granja inteligente propuesto.
El sistema propuesto se compone de dos redes principales:

- La red de monitorización (Granja): Esta red inalámbrica comprende varios sensores LoRa que se distribuyen por la granja para recopilar información vital como los niveles de humedad y flujo de aire.
- La red de control (Almacén): Las frutas y verduras cosechadas se almacenan en el almacén, y es crucial mantener unas condiciones climáticas óptimas. Por ello, esta red está equipada con sensores ambientales, incluidos sensores de temperatura, y alberga todos los equipos de control, como los acondicionadores de aire y las bombas de agua de riego, gestionados por un PLC.

Se desarrolló una nueva aplicación web Laravel para este sistema. El Siemens Simatic $IOT2040$ se puede ampliar fácilmente con escudos Arduino. Permite la programación sencilla de aplicaciones utilizando la herramienta de programación visual Node-Red, como se muestra en la Figura 5.20(a). Para permitir el uso de módulos de radio WiMOD basados en LoRa, se añade el WiMOD Shield, que es una placa de expansión que incluye todo lo necesario para conectar un módulo WiMOD a una placa Arduino utilizando la librería $WiMODLoRAWAN$. La comunicación entre el PLC Siemens S7 y la pasarela LoRa en nuestro sistema se establece a través de Modbus-TCP. Para habilitar la mensajería instantánea Telegram en nuestro sistema, integramos un bot utilizando la API Telegram Bot tanto en el $IOT2040$ como en la aplicación web.
Figura 5.25 la ilustración general del sistema presentado. El sistema agrícola inteligente utiliza sensores LoRa de nodo final repartidos por toda la granja para recopilar datos sobre el entorno. Los sensores transmiten estos datos a una pasarela LoRaWAN, que a su vez los envía a un servidor en la nube para su análisis. El sistema también incluye un PLC que está conectado a varias máquinas del almacén, como bombas de agua y luces. El IoT2040 se conecta al PLC mediante Modbus-TCP y se programa con Node-RED. Los usuarios pueden acceder al sistema a través de una aplicación de supervisión basada en web, que permite el control remoto de las máquinas del almacén a través del IoT2040. Además, los usuarios pueden enviar comandos y peticiones a través de un bot de Telegram. El servidor en la nube analiza la información recibida y almacena los datos útiles.

5.4 Sistema LoRa integrado en Blockchain para monitorizar el bienestar de las personas mayores

Este trabajo presenta un sistema inteligente basado en LoRa para monitorizar las actividades de las personas mayores que viven solas en zonas rurales y evaluar su bienestar. Se propone un nuevo enchufe inteligente LoRa de bajo coste para monitorizar el uso de los electrodomésticos. Este enchufe inteligente se utiliza para reconocer las actividades diarias de los ancianos con el fin de determinar su bienestar. Además, se pueden añadir múltiples sensores LoRa comerciales al sistema propuesto. Para asegurar los datos transmitidos, se integra la blockchain pública Swarm Ethereum para el almacenamiento seguro e inmutable de los datos. Para lograr esta integración, se instala un nodo Swarm en el servidor en la nube. Para las aplicaciones Laravel, el "web3.php" se debe instalar con el fin de conectarse a la red Ethereum. Se crea un contrato inteligente con la lógica para almacenar y recuperar datos en la red Swarm. Figura 5.28 muestra el flujo de trabajo de procesamiento de datos para este sistema. La monitorización y control remoto de los diferentes dispositivos LoRa de este sistema se realiza a través de una plataforma web de nuevo desarrollo, proporcionando una interfaz de usuario accesible a través de un navegador web que permite al usuario configurar los dispositivos de su red y analizar los datos recibidos bajo diferentes sistemas operativos y tamaños de pantalla. Además, implementa un sistema de autenticación para asegurar el acceso y un sistema de notificación para alertar a la familia del paciente o a su centro sanitario en casos de emergencia.

El principal objetivo de los sistemas de bienestar para personas mayores es proporcionarles atención, independientemente de dónde vivan. Las personas mayores que no requieren cuidados diarios pueden vivir solas, son reacias a trasladarse a otro lugar distinto de su domicilio y no les gusta utilizar sensores portátiles. Por eso, un sistema de monitorización "transparente" es una buena opción. La determinación del bienestar y el reconocimiento de la actividad son dos funciones importantes para prever y ayudar a las personas mayores gracias al análisis de datos. Uno de los indicios sobre el bienestar de las personas mayores que viven solas es el uso de electrodomésticos en casa. Suelen repetir actividades todos los días: preparar la comida, ver la televisión, encender y apagar las luces de distintas habitaciones (cocina, baño, etc.). Entonces, vigilar el uso de los aparatos eléctricos puede ser un buen indicador de bienestar. Si se detecta una desviación en el uso de los electrodomésticos, puede activarse una alerta.

Con el fin de controlar el uso de los aparatos eléctricos, se propone un enchufe inteligente LoRa cuyo objetivo es detectar el uso de los aparatos eléctricos de la casa. Este enchufe inteligente notificará al sistema LoRa cuando se encienda o apague un aparato. Los datos son recogidos y analizados en el servidor en la nube, en el caso de un comportamiento extraño, el sistema generará un mensaje de alerta y lo enviará a la persona o entidad afectada. La Figura 5.26 describe el circuito electrónico del enchufe inteligente LoRa.

La figura 5.30 ilustra todo el sistema de vigilancia de un pueblo, en el que distintos dispositivos de varias casas pueden transmitir sus datos a una pasarela. Este proyecto presentó un sistema novedoso, rentable y versátil para supervisar y evaluar las actividades de las personas mayores que viven solas. El sistema no requiere que los ancianos lleven ningún sensor ni tengan acceso a Internet, ya que la comunicación se consigue mediante la comunicación inalámbrica LoRa. Además, el sistema puede implantarse en cualquier lugar, pero está pensado para zonas con acceso limitado a internet, utilizando LoRa como canal de comunicación.

6 Conclusiones y trabajo futuro

El objetivo general de esta tesis es explorar el vasto y creciente campo del IoT. El objetivo es estudiar diversos aspectos de la tecnología IoT, incluidos los protocolos de comunicación, el desarrollo de sensores novedosos y las aplicaciones de monitorización web, con el fin de aportar ideas sobre cómo construir sistemas IoT robustos y fiables en diversos campos como la sanidad, el transporte y las ciudades inteligentes. La tesis ha logrado con éxito sus objetivos empleando novedosas metodologías de análisis e introduciendo varios diseños innovadores que tienen aplicaciones prácticas en los últimos estándares de comunicación.

La tesis doctoral ha arrojado nueva luz sobre el potencial de los sistemas IoT y ha abierto nuevas e interesantes vías de investigación e innovación. Sin embargo, quedan algunas cuestiones sin resolver que se consideran de importancia estratégica para futuras investigaciones. Los temas que se investigarán son los siguientes:

- Inteligencia Artificial (IA): La IA puede proporcionar la inteligencia necesaria y las capacidades de toma de decisiones y análisis predictivo a los sistemas IoT, haciéndolos más eficientes y eficaces. Al analizar las cantidades masivas de datos generados por los dispositivos IoT, la IA puede ayudar a identificar patrones y perspectivas que pueden utilizarse para optimizar las operaciones y mejorar el rendimiento general.

- Edge computing: La computación de borde es una tecnología prometedora que puede abordar algunos de los retos de la IO, como la latencia, la escalabilidad y la seguridad. La investigación futura podría explorar el potencial de la computación de borde para los sistemas IoT, incluyendo cómo puede utilizarse para mejorar el rendimiento y reducir la transferencia de datos.

- Captación de energía: Las tecnologías de captación de energía pueden permitir a los dispositivos IoT generar su propia energía, reduciendo la necesidad de baterías y mejorando su vida útil. La investigación futura podría explorar el potencial de la captación de energía para IoT, incluyendo cómo puede utilizarse para alimentar dispositivos IoT de baja potencia.

- Analizar y evaluar la eficacia de los protocolos de comunicación Thread y 5G NR para desplegar nuevos sistemas IoT. Thread es un protocolo de red de malla inalámbrica diseñado específicamente para dispositivos IoT de bajo consumo en hogares, que utiliza IPv6 y está optimizado para dispositivos y redes de bajo consumo, lo que lo convierte en una opción ideal para hogares inteligentes y otras aplicaciones IoT. Por otro lado, 5G NR es el último estándar de redes celulares que proporciona comunicación de alta velocidad y baja latencia para diversas aplicaciones, entre ellas IoT.

Appendix 2

List of Publications

1 Related publications

- Saban M, Aghzout O, Rosado-Muñoz A,. A Blockchain-Enabled Home Monitoring System Based on LoRa for Wellness Determination of Elderly. DCN. 2023; (submitted).

- Saban M, Bekkour M, Amdaouch I, El Gueri J, Ait Ahmed B, Chaari MZ, Ruiz-Alzola J, Rosado-Muñoz A, & Aghzout O. A Smart Agricultural System Based on PLC and a Cloud Computing Web Application Using LoRa and LoRaWan. Sensors. 2023; 23(5):2725. DOI: `https://doi.org/10.3390/s23052725`

- Saban, M., Casans-Berga, S., García-Gil, R., Navarro-Antón, A. E., Aghzout, O., Rosado-Muñoz, A. (2022). Sensing Wood Moisture in Heritage and Wooden Buildings: A New Sensing Unit With an Integrated LoRa-Based Monitoring System. IEEE Internet of Things Journal, 9(24), 25409-25423. DOI: `https://doi.org/10.1109/JIOT.2022.3196740`

- Saban, M., Aghzout, O., Medus, L. D., Rosado, A. (2021). Experimental Analysis of IoT Networks Based on LoRa/LoRaWAN under Indoor and Outdoor Environments: Performance and Limitations. IFAC-PapersOnLine, 54(4), 159-164. DOI:`https://doi.org/10.1016/j.ifacol.2021.10.027`

- Saban, M., Medus, L. D., Casans, S., Aghzout, O., & Rosado, A. (2021). Sensor Node Network for Remote Moisture Measurement in Timber Based on Bluetooth Low Energy and Web-Based Monitoring System. Sensors, 21(2), 491. DOI: `https://doi.org/10.3390/s21020491`

- Saban, M., Aghzout, O., & Rosado-Muñoz, A. (2022, June). Deployment of a LoRa-based Network and Web Monitoring Application for a Smart Farm. In 2022 IEEE International Workshop on Metrology for Industry 4.0 & IoT

(MetroInd4. 0&IoT) (pp. 424-427). IEEE. DOI: https://doi.org/10.1109/MetroInd4.0IoT54413.2022.9831521

2 Other publications

- Amdaouch, I., Saban, M., El Gueri, J., Chaari, M. Z., Alejos, A. V., Alzola, J. R., Rosado, A. & Aghzout, O. (2022). A Novel Approach of a Low-Cost UWB Microwave Imaging System with High Resolution Based on SAR and a New Fast Reconstruction Algorithm for Early-Stage Breast Cancer Detection. Journal of Imaging, 8(10), 264. DOI: https://doi.org/10.3390/jimaging8100264

- Medus, L. D., Saban, M., Frances-Villora, J. V., Bataller-Mompean, M., & Rosado-Muñoz, A. (2021). Hyperspectral image classification using CNN: Application to industrial food packaging. Food Control, 125, 107962. DOI: https://doi.org/10.1016/j.foodcont.2021.107962

- Benouis, M., Medus, L. D., Saban, M., Ghemougui, A., & Rosado-Muñoz, A. (2021). Food Tray Sealing Fault Detection in Multi-Spectral Images Using Data Fusion and Deep Learning Techniques. Journal of Imaging, 7(9), 186. DOI: https://doi.org/10.3390/jimaging7090186

- Benouis, M., Medus, L. D., Saban, M., Łabiak, G., & Rosado-Muñoz, A. (2020). Food tray sealing fault detection using hyperspectral imaging and PCANet. IFAC-PapersOnLine, 53(2), 7845-7850. DOI: https://doi.org/10.1016/j.ifacol.2020.12.1955

- Bekkour, M., Alaoui, N., Saban, M., Chaari MZ, Ruiz-Alzola J, Aghzout, O., (2023, March).A New Encoding Method to Enhance the Transmission Integrity and Overcome the Noisy environment in the WBAN Networks . In ISAECT 2022 (Casablanca, Morocco, 15-17 March 2023). Accepted on March 2023. (Accepted)

Bibliography

[1] Andrew Whitmore, Anurag Agarwal, and Li Da Xu. "The Internet of Things—A survey of topics and trends". In: *Information systems frontiers* 17.2 (2015), pp. 261–274.

[2] Armin Wasicek. "The future of 5G smart home network security is micro-segmentation". In: *Network Security* 2020.11 (2020), pp. 11–13.

[3] Bhagya Nathali Silva, Murad Khan, and Kijun Han. "Internet of things: A comprehensive review of enabling technologies, architecture, and challenges". In: *IETE Technical review* 35.2 (2018), pp. 205–220.

[4] Ana Reyna et al. "On blockchain and its integration with IoT. Challenges and opportunities". In: *Future generation computer systems* 88 (2018), pp. 173–190.

[5] Pedro M Reyes, John K Visich, and Patrick Jaska. "Managing the dynamics of new technologies in the global supply chain". In: *IEEE Engineering Management Review* 48.1 (2020), pp. 156–162.

[6] Mark Weiser. "The Computer for the 21 st Century". In: *Scientific american* 265.3 (1991), pp. 94–105.

[7] Kevin Ashton et al. "That 'internet of things' thing". In: *RFID journal* 22.7 (2009), pp. 97–114.

[8] Karen Rose, Scott Eldridge, and Lyman Chapin. "The internet of things: An overview". In: *The internet society (ISOC)* 80 (2015), pp. 1–50.

[9] Tai-hoon Kim, Carlos Ramos, and Sabah Mohammed. *Smart city and IoT*. 2017.

[10] Behrouz Pourghebleh, Karzan Wakil, and Nima Jafari Navimipour. "A comprehensive study on the trust management techniques in the Internet of Things". In: *IEEE Internet of Things Journal* 6.6 (2019), pp. 9326–9337.

[11] Sheng-Joue Young and Chia-Lin Chiou. "Synthesis and optoelectronic properties of Ga-doped ZnO nanorods by hydrothermal method". In: *Microsystem Technologies* 24.1 (2018), pp. 103–107.

[12] Lijun Wei, Jing Wu, and Chengnian Long. “Blockchain-enabled trust management in service-oriented internet of things: opportunities and challenges”. In: *2021 The 3rd international conference on blockchain technology*. 2021, pp. 90–95.

[13] Aniello Castiglione et al. “Context aware ubiquitous biometrics in edge of military things”. In: *IEEE Cloud Computing* 4.6 (2017), pp. 16–20.

[14] Brijesh Iyer and Niket Patil. “IoT enabled tracking and monitoring sensor for military applications”. In: *International Journal of System Assurance Engineering and Management* 9.6 (2018), pp. 1294–1301.

[15] Gobinath Aroganam, Nadarajah Manivannan, and David Harrison. “Review on wearable technology sensors used in consumer sport applications”. In: *Sensors* 19.9 (2019), p. 1983.

[16] Giuseppe Boriani et al. “Consumer-led screening for atrial fibrillation using consumer-facing wearables, devices and apps: a survey of health care professionals by AF-SCREEN international collaboration”. In: *European journal of internal medicine* 82 (2020), pp. 97–104.

[17] Amazon. *Echo*. `https://www.amazon.com/echo/`. Accessed: February 28, 2023.

[18] Apple. *HomePod*. `https://www.apple.com/homepod/`. Accessed: February 28, 2023.

[19] openHAB Foundation. *openHAB - a vendor and technology agnostic open source automation software for your home*. Accessed: February 28, 2023. 2022. URL: `https://www.openhab.org/`.

[20] Lakmini P Malasinghe, Naeem Ramzan, and Keshav Dahal. “Remote patient monitoring: a comprehensive study”. In: *Journal of Ambient Intelligence and Humanized Computing* 10.1 (2019), pp. 57–76.

[21] SR Ramson and D Jackuline Moni. “A case study on different wireless networking technologies for remote health care”. In: *Intelligent Decision Technologies* 10.4 (2016), pp. 353–364.

[22] Stephanie B Baker, Wei Xiang, and Ian Atkinson. “Internet of things for smart healthcare: Technologies, challenges, and opportunities”. In: *Ieee Access* 5 (2017), pp. 26521–26544.

[23] Giovanna Sannino, Ivanoe De Falco, and Giuseppe De Pietro. “A supervised approach to automatically extract a set of rules to support fall detection in an mHealth system”. In: *Applied Soft Computing* 34 (2015), pp. 205–216.

[24] Paolo Casacci et al. “Alzheimer patient’s home rehabilitation through ICT advanced technologies: the ALTRUISM project”. In: *Ambient Assisted Living*. Springer, 2015, pp. 377–385.

[25] Maneesha V Ramesh, Sruthy Anand, and P Rekha. “A mobile software for health professionals to monitor remote patients”. In: *2012 Ninth international conference on wireless and optical communications networks (WOCN)*. IEEE. 2012, pp. 1–4.

[26] Ahmed Fawzi Otoom et al. “Effective diagnosis and monitoring of heart disease”. In: *International Journal of Software Engineering and Its Applications* 9.1 (2015), pp. 143–156.

[27] Tomasz Szydło and Marek Konieczny. “Mobile devices in the open and universal system for remote patient monitoring”. In: *IFAC-PapersOnLine* 48.4 (2015), pp. 296–301.

[28] M Kozlovszky, L Kovacs, and K Karoczkai. “Cardiovascular and diabetes focused remote patient monitoring”. In: *VI Latin American Congress on Biomedical Engineering CLAIB 2014, Paraná, Argentina 29, 30 & 31 October 2014*. Springer. 2015, pp. 568–571.

[29] A Spender et al. “Wearables and the internet of things: Considerations for the life and health insurance industry”. In: *British Actuarial Journal* 24 (2019), e22.

[30] Paul Baltusis. *On board vehicle diagnostics*. Tech. rep. SAE Technical Paper, 2004.

[31] Fan Bai and Bhaskar Krishnamachari. “Exploiting the wisdom of the crowd: localized, distributed information-centric VANETs [Topics in Automotive Networking]”. In: *IEEE communications magazine* 48.5 (2010), pp. 138–146.

[32] Yuyan Liu et al. “A systematic review: Road infrastructure requirement for Connected and Autonomous Vehicles (CAVs)”. In: *Journal of Physics: Conference Series*. Vol. 1187. 4. IOP Publishing. 2019, p. 042073.

[33] M Hermann, T Pentek, and B Otto. “Design principles for Industrie 4.0 scenarios (Vol. 2016)”. In: *IEEE Computer Society* (2016).

[34] AARON BROWN FOR MAILONLINE. *Rise of the machines? Amazon’s army of more than 100,000 warehouse robots still can’t replace humans because they lack ’common sense’*. URL: `https://www.dailymail.co.uk/sciencetech/article-5808319/Amazon-100-000-warehouse-robots-company-insists-replace-humans.html`. (accessed: 27.12.2022).

[35] Simon Elias Bibri. "The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability". In: *Sustainable cities and society* 38 (2018), pp. 230–253.

[36] Mina Nasiri, Nina Tura, and Ville Ojanen. "Developing disruptive innovations for sustainability: A review on Impact of Internet of Things (IOT)". In: *2017 Portland International Conference on Management of Engineering and Technology (PICMET)*. IEEE. 2017, pp. 1–10.

[37] Luca Foschini et al. "M2M-based metropolitan platform for IMS-enabled road traffic management in IoT". In: *IEEE Communications Magazine* 49.11 (2011), pp. 50–57.

[38] Sana Benhamaid, Abdelmadjid Bouabdallah, and Hicham Lakhlef. "Recent advances in energy management for Green-IoT: An up-to-date and comprehensive survey". In: *Journal of Network and Computer Applications* 198 (2022), p. 103257.

[39] Fadi Shrouf and Giovanni Miragliotta. "Energy management based on Internet of Things: practices and framework for adoption in production management". In: *Journal of Cleaner Production* 100 (2015), pp. 235–246.

[40] D Menaka and Sabitha Gauni. "Ocean of things: Marine environment monitoring using discriminatory model". In: *Journal of Physics: Conference Series*. Vol. 1964. 7. IOP Publishing. 2021, p. 072015.

[41] Mihai T Lazarescu. "Design of a WSN platform for long-term environmental monitoring for IoT applications". In: *IEEE Journal on emerging and selected topics in circuits and systems* 3.1 (2013), pp. 45–54.

[42] Mohamed Rawidean Mohd Kassim. "Iot applications in smart agriculture: Issues and challenges". In: *2020 IEEE conference on open systems (ICOS)*. IEEE. 2020, pp. 19–24.

[43] Jinyuan Xu, Baoxing Gu, and Guangzhao Tian. "Review of agricultural IoT technology". In: *Artificial Intelligence in Agriculture* (2022).

[44] Antonio Joao Schuhmann Dos Santos. "How does the collection and use of private data slow the development of eHealth solutions and which are the recommendations that can speed up innovation of eHealth solutions?" In: (2018).

[45] Henry Vargas et al. "Detection of Security Attacks in Industrial IoT Networks: A Blockchain and Machine Learning Approach". In: *Electronics* 10.21 (2021), p. 2662.

[46] Michael Hogan, Ben Piccarreta, Interagency International Cybersecurity Standardization Working Group, et al. *Interagency report on status of international cybersecurity standardization for the Internet of Things (IoT).* Tech. rep. National Institute of Standards and Technology, 2018.

[47] Eli Biham and Adi Shamir. *Differential cryptanalysis of the data encryption standard.* Springer Science & Business Media, 2012.

[48] Mathy Vanhoef and Frank Piessens. "Practical verification of WPA-TKIP vulnerabilities". In: *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security.* 2013, pp. 427–436.

[49] Mathy Vanhoef and Frank Piessens. "Key reinstallation attacks: Forcing nonce reuse in WPA2". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.* 2017, pp. 1313–1328.

[50] Neal Koblitz and Alfred Menezes. "A riddle wrapped in an enigma". In: *IEEE Security & Privacy* 14.6 (2016), pp. 34–42.

[51] Wei Wei et al. "Security in internet of things: Opportunities and challenges". In: *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI).* IEEE. 2016, pp. 512–518.

[52] Hannes Tschofenig and Thomas Fossati. *Transport layer security (tls)/datagram transport layer security (dtls) profiles for the internet of things.* Tech. rep. 2016.

[53] Yong Ho Hwang. "Iot security & privacy: threats and challenges". In: *Proceedings of the 1st ACM workshop on IoT privacy, trust, and security.* 2015, pp. 1–1.

[54] Paolo Ferrari et al. "Evaluation of communication latency in industrial IoT applications". In: *2017 IEEE International Workshop on Measurement and Networking (M&N).* IEEE. 2017, pp. 1–6.

[55] Anisha Gupta, Rivana Christie, and R Manjula. "Scalability in internet of things: features, techniques and research challenges". In: *Int. J. Comput. Intell. Res* 13.7 (2017), pp. 1617–1627.

[56] "Wireless sensor network survey". In: *Computer Networks* 52.12 (2008), pp. 2292–2330. ISSN: 1389-1286. DOI: `https://doi.org/10.1016/j.comnet.2008.04.002`. URL: `https://www.sciencedirect.com/science/article/pii/S138912860800125`.

[57] Robert E Van Dyck. "Detection performance in self-organized wireless sensor networks". In: *Proceedings IEEE International Symposium on Information Theory,* IEEE. 2002, p. 13.

[58] Raghavendra V Kulkarni and Ganesh Kumar Venayagamoorthy. “Particle swarm optimization in wireless-sensor networks: A brief survey”. In: *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 41.2 (2010), pp. 262–267.

[59] Hossam Mahmoud Ahmad Fahmy and Hossam Mahmoud Ahmad Fahmy. “Protocol stack of WSNs”. In: *Concepts, Applications, Experimentation and Analysis of Wireless Sensor Networks* (2021), pp. 53–66.

[60] Rajashree V Biradar et al. “Classification and comparison of routing protocols in wireless sensor networks”. In: *Special Issue on Ubiquitous Computing Security Systems* 4.2 (2009), pp. 704–711.

[61] Noman Shabbir and Syed Rizwan Hassan. “Routing protocols for wireless sensor networks (WSNs)”. In: *Wireless Sensor Networks-Insights and Innovations* (2017), pp. 36–40.

[62] Arun Jain and Ramesh Bharti. “Simulation and performance analysis of throughput and delay on varying time and number of nodes in MANET”. In: *International Journal of Recent Research and Review* 7 (2014), pp. 113–117.

[63] Peter Palensky and Thilo Sauter. “Security considerations for FAN-Internet connections”. In: *2000 IEEE International Workshop on Factory Communication Systems. Proceedings (Cat. No. 00TH8531)*. IEEE. 2000, pp. 27–35.

[64] Jon Edney, William A Arbaugh, and William Arbaugh. *Real 802.11 security: Wi-Fi protected access and 802.11 i.* Addison-Wesley Professional, 2004.

[65] Zoran Hadzi-Velkov and Boris Spasenovski. “Capture effect in IEEE 802.11 basic service area under influence of Rayleigh fading and near/far effect”. In: *The 13th IEEE international symposium on personal, indoor and mobile radio communications.* Vol. 1. IEEE. 2002, pp. 172–176.

[66] C Muthu Ramya, M Shanmugaraj, and R Prabakaran. “Study on ZigBee technology”. In: *2011 3rd international conference on electronics computer technology.* Vol. 6. IEEE. 2011, pp. 297–301.

[67] ZigBee Alliance. *IEEE 802.15. 4, ZigBee standard.* 2009.

[68] Khushbu Meena, Manoj Gupta, and Arun Kumar. “Analysis of UWB indoor and outdoor channel propagation”. In: *2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE).* IEEE. 2020, pp. 352–355.

[69] Ian Oppermann, Matti Hämäläinen, and Jari Iinatti. *UWB: theory and applications.* John Wiley & Sons, 2004.

[70] S Ahmad Salehi et al. “IEEE 802.15. 6 standard in wireless body area networks from a healthcare point of view”. In: *2016 22nd Asia-Pacific Conference on Communications (APCC)*. IEEE. 2016, pp. 523–528.

[71] Elke Mackensen, Matthias Lai, and Thomas M Wendt. “Bluetooth Low Energy (BLE) based wireless sensors”. In: *SENSORS, 2012 IEEE*. IEEE. 2012, pp. 1–4.

[72] Andreina Liendo et al. “BLE parameter optimization for IoT applications”. In: *2018 IEEE International Conference on Communications (ICC)*. IEEE. 2018, pp. 1–7.

[73] Jin-Shyan Lee, Ming-Feng Dong, and Yuan-Heng Sun. “A preliminary study of low power wireless technologies: ZigBee and Bluetooth Low Energy”. In: *2015 IEEE 10th Conference on Industrial Electronics and Applications (ICIEA)*. 2015, pp. 135–139. DOI: 10.1109/ICIEA.2015.7334098.

[74] Muhammad Tariq Sadiq, Xiaojun Yu, and Zhaohui Yuan. “Exploiting dimensionality reduction and neural network techniques for the development of expert brain–computer interfaces”. In: *Expert Systems with Applications* 164 (2021), p. 114031.

[75] Hesam Akbari and Muhammad Tariq Sadiq. “Detection of focal and non-focal EEG signals using non-linear features derived from empirical wavelet transform rhythms”. In: *Physical and Engineering Sciences in Medicine* 44.1 (2021), pp. 157–171.

[76] Waqar Hussain et al. “Epileptic seizure detection using 1 D-convolutional long short-term memory neural networks”. In: *Applied Acoustics* 177 (2021), p. 107941.

[77] Jean-Paul Linnartz. *Wireless communication: the interactive multimedia CD-ROM*. Springer, 2001.

[78] Joseph Ho, Yixin Zhu, and Seshu Madhavapeddy. “Throughput and buffer analysis for GSM general packet radio service (GPRS)”. In: *WCNC. 1999 IEEE Wireless Communications and Networking Conference (Cat. No. 99TH8466)*. Vol. 3. IEEE. 1999, pp. 1427–1431.

[79] Kamilo Feher. *Wireless digital communications: modulation & spread spectrum applications*. Prentice-Hall, Inc., 1995.

[80] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen. “A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi”. In: *IECON 2007-33rd Annual Conference of the IEEE Industrial Electronics Society*. Ieee. 2007, pp. 46–51.

[81] F John Dian, Amirhossein Yousefi, and Sungjoon Lim. “A practical study on Bluetooth Low Energy (BLE) throughput”. In: *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE. 2018, pp. 768–771.

[82] Hadi Givehchian et al. “Evaluating physical-layer ble location tracking attacks on mobile devices”. In: *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2022, pp. 1690–1704.

[83] Hyung-Sin Kim et al. “System architecture directions for post-soc/32-bit networked sensors”. In: *Proceedings of the 16th ACM conference on embedded networked sensor systems*. 2018, pp. 264–277.

[84] Bin Yu, Lisheng Xu, and Yongxu Li. “Bluetooth Low Energy (BLE) based mobile electrocardiogram monitoring system”. In: *2012 IEEE International Conference on Information and Automation*. IEEE. 2012, pp. 763–767.

[85] Carles Gomez, Joaquim Oller, and Josep Paradells. “Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology”. In: *sensors* 12.9 (2012), pp. 11734–11753.

[86] Surthineni Ashok and RV Krishnaiah. “Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology”. In: *International Journal* 3.9 (2013), pp. 11734–11753.

[87] RB Salikhov, V Kh Abdrakhmanov, and TT Yumalin. “Experience of Using Bluetooth Low Energy to Develop a Sensor Data Exchange System Based on the NRF52832 Microcontroller”. In: *2021 International Ural Conference on Electrical Power Engineering (UralCon)*. IEEE. 2021, pp. 229–233.

[88] Jetmir Haxhibeqiri et al. “LoRa indoor coverage and performance in an industrial environment: Case study”. In: *2017 22nd IEEE international conference on emerging technologies and factory automation (ETFA)*. IEEE. 2017, pp. 1–8.

[89] Hussein Mroue et al. “MAC layer-based evaluation of IoT technologies: LoRa, SigFox and NB-IoT”. In: *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)*. IEEE. 2018, pp. 1–5.

[90] Congduc Pham et al. “Radio channel access challenges in LoRa low-power wide-area networks”. In: *LPWAN Technologies for IoT and M2M Applications*. Elsevier, 2020, pp. 65–102.

[91] LoRa Alliance. *LoRaWAN*. URL: `https://lora-alliance.org/`. (accessed: 03.01.2023).

[92] SigFox. *SigFox Coverage*. URL: `https://www.sigfox.com/coverage/`. (accessed: 03.01.2023).

[93] Ansuman Adhikary, Xingqin Lin, and Y-P Eric Wang. “Performance evaluation of NB-IoT coverage”. In: *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*. IEEE. 2016, pp. 1–5.

[94] Rubbens Boisguene et al. “A survey on NB-IoT downlink scheduling: Issues and potential solutions”. In: *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE. 2017, pp. 547–551.

[95] Sarath Chandu Gaddam and Mritunjay Kumar Rai. “A comparative study on various LPWAN and cellular communication technologies for IoT based smart applications”. In: *2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR)*. IEEE. 2018, pp. 1–8.

[96] Kais Mekki et al. “Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT”. In: *2018 ieee international conference on pervasive computing and communications workshops (percom workshops)*. IEEE. 2018, pp. 197–202.

[97] Luiz Oliveira et al. “MAC layer protocols for Internet of Things: A survey”. In: *Future Internet* 11.1 (2019), p. 16.

[98] Rashmi Sharan Sinha, Yiqiao Wei, and Seung-Hoon Hwang. “A survey on LPWA technology: LoRa and NB-IoT”. In: *Ict Express* 3.1 (2017), pp. 14–21.

[99] Samir Dawaliby, Abbas Bradai, and Yannis Pousset. “In depth performance evaluation of LTE-M for M2M communications”. In: *2016 IEEE 12th international conference on wireless and mobile computing, networking and communications (WiMob)*. IEEE. 2016, pp. 1–8.

[100] Konstantin Mikhaylov, Juha Petaejaejaervi, and Tuomo Haenninen. “Analysis of capacity and scalability of the LoRa low power wide area network technology”. In: *European Wireless 2016; 22th European Wireless Conference*. VDE. 2016, pp. 1–6.

[101] Wael Guibene et al. “Evaluation of LPWAN technologies for smart cities: River monitoring use-case”. In: *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE. 2017, pp. 1–5.

[102] ERM TG28 ETSI. “Electromagnetic compatibility and radio spectrum matters (erm); short range devices (srd); radio equipment to be used in the 25 mhz to 1 000 mhz frequency range with power levels ranging up to 500 mw”. In: *European harmonized standard EN* 300.220 (2012), p. v2.

[103] Mohamed Saban et al. “Sensing Wood Moisture in Heritage and Wooden Buildings: A New Sensing Unit With an Integrated LoRa-Based Monitoring System”. In: *IEEE Internet of Things Journal* 9.24 (2022), pp. 25409–25423. DOI: 10.1109/JIOT.2022.3196740.

[104] Phoebe Edward et al. “On the Coexistence of LoRa- and Interleaved Chirp Spreading LoRa-Based Modulations”. In: *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 2019, pp. 1–6. DOI: 10.1109/WiMOB.2019.8923211.

[105] Fatma Benkhelifa, Zhijin Qin, and Julie A. McCann. “User Fairness in Energy Harvesting-Based LoRa Networks With Imperfect SF Orthogonality”. In: *IEEE Transactions on Communications* 69.7 (2021), pp. 4319–4334. DOI: 10.1109/TCOMM.2021.3068304.

[106] Yousef A. Al-Gumaei et al. “Optimizing Power Allocation in LoRaWAN IoT Applications”. In: *IEEE Internet of Things Journal* 9.5 (2022), pp. 3429–3442. DOI: 10.1109/JIOT.2021.3098477.

[107] Dania Eridani et al. “Monitoring System in Lora Network Architecture using Smart Gateway in Simple LoRa Protocol”. In: *2019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*. 2019, pp. 200–204. DOI: 10.1109/ISRITI48646.2019.9034612.

[108] Adrian I Petrariu, Alexandru Lavric, and Eugen Coca. “Lorawan gateway: Design, implementation and testing in real environment”. In: *2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME)*. IEEE. 2019, pp. 49–53.

[109] Jean Moraes et al. “Evaluation of an adaptive resource allocation for lorawan”. In: *Journal of Signal Processing Systems* 94.1 (2022), pp. 65–79.

[110] Jonathan de Carvalho Silva et al. “LoRaWAN—A low power WAN protocol for Internet of Things: A review and opportunities”. In: *2017 2nd International multidisciplinary conference on computer and energy science (SpliTech)*. IEEE. 2017, pp. 1–6.

[111] Stefano Tomasin, Simone Zulian, and Lorenzo Vangelista. “Security analysis of lorawan join procedure for internet of things networks”. In: *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE. 2017, pp. 1–6.

[112] SeungJae Na et al. “Scenario and countermeasure for replay attack using join request messages in LoRaWAN”. In: *2017 international conference on information networking (ICOIN)*. IEEE. 2017, pp. 718–720.

[113] Erik Gresak and Miroslav Voznak. "Protecting gateway from abp replay attack on lorawan". In: *AETA 2018-Recent Advances in Electrical Engineering and Related Sciences: Theory and Application*. Springer. 2020, pp. 400–408.

[114] Semtech Corporation. *LoRa and LoRaWAN*. 2021. URL: https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/.

[115] Stenly Ibrahim Adam and Stevani Andolo. "A New PHP Web Application Development Framework Based on MVC Architectural Pattern and Ajax Technology". In: *2019 1st International Conference on Cybernetics and Intelligent System (ICORIS)*. Vol. 1. IEEE. 2019, pp. 45–50.

[116] Lei Chen et al. "The online education platform using Proxmox and noVNC technology based on Laravel framework". In: *2017 IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS)*. IEEE. 2017, pp. 487–491.

[117] Rashidah F Olanrewaju, Thouhedul Islam, and Nor'ashikin Ali. "An empirical study of the evolution of PHP MVC framework". In: *Advanced Computer and Communication Engineering Technology*. Springer, 2015, pp. 399–410. DOI: 10.1007/978-3-319-07674-4_40.

[118] Jibril Adamu, Raseeda Hamzah, and Marshima Mohd Rosli. "Security issues and framework of electronic medical record: A review". In: *Bulletin of Electrical Engineering and Informatics* 9.2 (2020), pp. 565–572.

[119] *DigitalOcean*. https://www.digitalocean.com/. Accessed on: February 15, 2023.

[120] Sayed Md Fahim Fahad and Mohammad Shorif Uddin. "Cloud-based solution for improvement of response time of MySQL RDBMS". In: *2016 International Workshop on Computational Intelligence (IWCI)*. IEEE. 2016, pp. 7–10.

[121] Sergio Aguilar, Rafael Vidal, and Carles Gomez. "Opportunistic sensor data collection with bluetooth low energy". In: *Sensors* 17.1 (2017), p. 159.

[122] *ERDPlus*. https://erdplus.com. Accessed: March 2, 2023.

[123] *Lucidchart*. https://www.lucidchart.com/. Accessed: March 2, 2023.

[124] *Visual Paradigm*. https://www.visual-paradigm.com. Accessed: March 2, 2023.

[125] *MySQL Workbench*. https://www.mysql.com/products/workbench/. Accessed: March 2, 2023.

[126] *phpMyAdmin*. https://www.phpmyadmin.net. Accessed: March 2, 2023.

[127] *Bootstrap*. https://getbootstrap.com. Accessed: March 2, 2023.

[128] Alex Banks and Eve Porcello. *Learning React: functional web development with React and Redux.* " O'Reilly Media, Inc.", 2017.

[129] Satoshi Nakamoto. "Bitcoin whitepaper". In: *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)* (2008).

[130] Xiao Yue et al. "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control". In: *Journal of medical systems* 40.10 (2016), pp. 1–8.

[131] Ingo Weber et al. "Untrusted business process monitoring and execution using blockchain". In: *International conference on business process management.* Springer. 2016, pp. 329–347.

[132] Imran Bashir. *Mastering blockchain.* Packt Publishing Ltd, 2017.

[133] Joseph J Bambara and Paul R Allen. "Blockchain". In: *A practical guide to developing business, law and technology solutions. New York City: McGraw-Hill Professional* (2018).

[134] Gareth W Peters, Efstathios Panayi, and Ariane Chapelle. "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective". In: *arXiv preprint arXiv:1508.04364* (2015).

[135] Jameela Al-Jaroodi and Nader Mohamed. "Blockchain in industries: A survey". In: *IEEE Access* 7 (2019), pp. 36500–36515.

[136] Fran Casino, Thomas K Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: Current status, classification and open issues". In: *Telematics and informatics* 36 (2019), pp. 55–81.

[137] Evangelos Georgiadis. "How many transactions per second can bitcoin really handle? Theoretically." In: *Cryptology ePrint Archive* (2019).

[138] Rebecca Yang et al. "Public and private blockchain in construction business process and information integration". In: *Automation in construction* 118 (2020), p. 103276.

[139] Dominique Guegan. "Public blockchain versus private blockhain". In: (2017).

[140] Tomas Mikula and Rune Hylsberg Jacobsen. "Identity and access management with blockchain in electronic healthcare records". In: *2018 21st Euromicro conference on digital system design (DSD).* IEEE. 2018, pp. 699–706.

[141] Zhihua Cui et al. "A hybrid blockchain-based identity authentication scheme for multi-WSN". In: *IEEE Transactions on Services Computing* 13.2 (2020), pp. 241–251.

[142] Heru Susanto et al. "Securing Financial Inclusiveness Adoption of Blockchain FinTech Compliance". In: *FinTech Development for Financial Inclusiveness*. IGI Global, 2022, pp. 168–196.

[143] Manpreet Kaur et al. "MBCP: Performance analysis of large scale mainstream blockchain consensus protocols". In: *IEEE Access* 9 (2021), pp. 80931–80944.

[144] Imran Bashir. *Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more*. Packt Publishing Ltd, 2020.

[145] Sarwar Sayeed and Hector Marco-Gisbert. "Assessing blockchain consensus and security mechanisms against the 51% attack". In: *Applied sciences* 9.9 (2019), p. 1788.

[146] Matthias Baudlet et al. "The best of both worlds: A new composite framework leveraging pos and pow for blockchain security and governance". In: *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE. 2020, pp. 17–24.

[147] Leo Maxim Bach, Branko Mihaljevic, and Mario Zagar. "Comparative analysis of blockchain consensus algorithms". In: *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. Ieee. 2018, pp. 1545–1550.

[148] Christoph L Schuba et al. "Analysis of a denial of service attack on TCP". In: *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097)*. IEEE. 1997, pp. 208–223.

[149] Andrew Poelstra et al. "Distributed consensus from proof of stake is impossible". In: *Self-published Paper* (2014).

[150] Aggelos Kiayias et al. "Ouroboros: A provably secure proof-of-stake blockchain protocol". In: *Annual international cryptology conference*. Springer. 2017, pp. 357–388.

[151] Pureswaran Veena et al. "Empowering the edge-practical insights on a decentralized internet of things". In: *IBM Institute for Business Value* 17 (2015), p. 21.

[152] Saptarshi Gan. "An IoT simulator in NS3 and a key-based authentication architecture for IoT devices using blockchain". In: *Indian Institute of Technology Kanpur* (2017).

[153] *Chain of things*. Available online: `https://www.blockchainofthings.com/`. Accessed 2 March 2023. 2017.

[154] *Filament*. Available online: `https://filament.com/`. Accessed 2 March 2023. 2017.

[155] M.A. Khan and K. Salah. "IoT security: review, blockchain solutions, and open challenges". In: *Future Gener. Comput. Syst.* (2017).

[156] *Modum.* Available online: `https://modum.io/`. Accessed 2 March 2023. 2017.

[157] *LO3ENERGY.* Available online: `https://lo3energy.com/`. Accessed 2 March 2023. 2017.

[158] *Aigang.* Available online: `https://aigang.network/`. Accessed 2 March 2023. 2017.

[159] *My Bit.* Available online: `https://mybit.io/`. Accessed 2 March 2023. 2017.

[160] M. Samaniego and R. Deters. "Hosting virtual iot resources on edge-hosts with blockchain". In: *Computer and Information Technology (CIT), 2016 IEEE International Conference on.* Yanuca Island, Fiji: IEEE, 2016, pp. 116–119.

[161] Ittay Eyal and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable". In: *International conference on financial cryptography and data security.* Springer. 2014, pp. 436–454.

[162] Michail Sidorov et al. "A public blockchain-enabled wireless LoRa sensor node for easy continuous unattended health monitoring of bolted joints: Implementation and evaluation". In: *IEEE Sensors Journal* 20.21 (2020), pp. 13057–13065.

[163] Stephen Kirkman and Richard Newman. "A cloud data movement policy architecture based on smart contracts and the ethereum blockchain". In: *2018 IEEE International Conference on Cloud Engineering (IC2E).* IEEE. 2018, pp. 371–377.

[164] Vitalik Buterin et al. "A next-generation smart contract and decentralized application platform". In: *white paper* 3.37 (2014), pp. 2–1.

[165] Chris Dannen. *Introducing Ethereum and solidity.* Vol. 1. Springer, 2017.

[166] MetaMask. *The crypto wallet for defi, Web3 Dapps and nfts. https://metamask.io/, (accessed 20 September 2022).*

[167] Swarm. *Swarm Ethereum web3 stack. https://www.ethswarm.org, (accessed 20 September 2022).*

[168] WEG2G Group. *How to Work with Ethereum Swarm Storage. https://www.coding-bootcamps.com/blog/how-to-work-with-ethereum-swarm-storage.html, (accessed 20 September 2022).*

[169] Koji Asami. "Design of a measurement cell for low-frequency dielectric spectroscopy of biological cell suspensions". In: *Measurement Science and Technology* 22.8 (2011), p. 085801.

[170] Anna Nakonieczna et al. “Electrical impedance measurements for detecting artificial chemical additives in liquid food products”. In: *Food Control* 66 (2016), pp. 116–129.

[171] Uwe Pliquett. “Bioimpedance: a review for food processing”. In: *Food engineering reviews* 2 (2010), pp. 74–94.

[172] Myounghak Oh, Yongsung Kim, and Junboum Park. “Factors affecting the complex permittivity spectrum of soil at a low frequency range of 1 kHz–10 MHz”. In: *Environmental geology* 51 (2007), pp. 821–833.

[173] J Fleig et al. “Inductive loops in impedance spectroscopy caused by electrical shielding”. In: *Journal of the Electrochemical Society* 143.11 (1996), p. 3636.

[174] Christian Brischke, Andreas Otto Rapp, and Rolf Bayerbach. “Measurement system for long-term recording of wood moisture content with internal conductively glued electrodes”. In: *Building and Environment* 43.10 (2008), pp. 1566–1574.

[175] Sverre Grimnes and Ørjan G Martinsen. “Sources of error in tetrapolar impedance measurements on biomaterials and other ionic conductors”. In: *Journal of Physics D: Applied Physics* 40.1 (2006), p. 9.

[176] BP Kibble et al. “A guide to measuring resistance and impedance below 1 MHz.” In: (1999).

[177] Sunil Putta, Vijay Vaidyanathan, and Jaycee Chung. “Development and testing of a nodal resistance measurement (NRM) system for composite structures”. In: *Measurement* 41.7 (2008), pp. 763–773.

[178] JI Fernandez-Golfin et al. “Curves for the estimation of the moisture content of ten hardwoods by means of electrical resistance measurements”. In: *Forest Systems* 21.1 (2012), pp. 121–127.

[179] S. Casans, A. Rosado-Munoz, and T. Iakymchuk. “Novel Resistance Measurement Method: Analysis of Accuracy and Thermal Dependence with Applications in Fiber Materials”. In: *Sensors* 16 (2016), p. 2129. DOI: 10.3390/s16122129. URL: https://doi.org/10.3390/s16122129.

[180] Silvia Casans, Alfredo Rosado-Muñoz, and Taras Iakymchuk. “Novel Resistance Measurement Method: Analysis of Accuracy and Thermal Dependence with Applications in Fiber Materials”. In: *Sensors* 16.12 (2016). ISSN: 1424-8220. DOI: 10.3390/s16122129. URL: https://www.mdpi.com/1424-8220/16/12/2129.

[181] RAMÓN Pallas and J Webster. *Analog signal processing.* 1999.

[182] Low Level Measurements Handbook. “Keithley Instruments”. In: *Inc., Cleveland, OH* (2004), pp. 2–42.

[183] Sergio Franco. *Design with operational amplifiers and analog integrated circuits*. Vol. 1988. McGraw-Hill New York, 2002.

[184] Mohamed Saban et al. "Sensor Node Network for Remote Moisture Measurement in Timber Based on Bluetooth Low Energy and Web-Based Monitoring System". In: *Sensors* 21.2 (2021). ISSN: 1424-8220. DOI: 10.3390/s21020491. URL: https://www.mdpi.com/1424-8220/21/2/491.

[185] William Lanpheer James. *Electric moisture meters for wood*. Vol. 8. US Department of Agriculture, Forest Service, Forest Products Laboratory, 1963.

[186] *Moisture Meter*. https://woodgears.ca/lumber/moisture_meter.html.

[187] Stella Regina Reis da Costa et al. "EA-4/02 Expression of the Uncertainty of Measurement in Calibration". In: (1999).

[188] BS EN 16682. *Conservation of Cultural Heritage - Methods of Measurement of Moisture Content, or Water Content, in Materials Constituting Immovable Cultural Heritage*. 2017.

[189] Dario Camuffo. "Standardization activity in the evaluation of moisture content". In: *Journal of Cultural Heritage* 31 (2018). MODIHMA 2018 Innovative Techniques for Moisture Detection in Historical Masonry, S10–S14. ISSN: 1296-2074. DOI: https://doi.org/10.1016/j.culher.2018.03.021. URL: https://www.sciencedirect.com/science/article/pii/S1296207418300633.

[190] Robert J Ross et al. "Wood handbook: wood as an engineering material. USDA Forest Service, Forest Products Laboratory". In: *General Technical Report FPL-GTR-190* 509.5 (2010).

[191] Philipp Dietsch et al. "Methods to determine wood moisture content and their applicability in monitoring concepts". In: *Journal of Civil Structural Health Monitoring* 5.2 (2015), pp. 115–127.

[192] G.T. Kirker, A.B. Bishell, and S.L. Zelinka. "Electrical properties of wood colonized by Gloeophyllum trabeum". In: *Int. Biodeterior. Biodegrad.* 114 (2016), pp. 110–115. DOI: 10.1016/j.ibiod.2016.05.023. URL: https://doi.org/10.1016/j.ibiod.2016.05.023.

[193] A. J. Stamm. "The Electrical Resistance of Wood as a Measure of Its Moisture Content". In: *Ind. Eng. Chem.* 19 (1927), pp. 1021–1025. DOI: 10.1021/ie50266a014. URL: https://doi.org/10.1021/ie50266a014.

[194] C. Brischke and S. C. Lampen. "Resistance based moisture content measurements on native, modified and preservative treated wood". In: *Eur. J. Wood Wood Prod.* 72 (2014), pp. 289–292. DOI: 10.1007/s00107-013-0727-6. URL: https://doi.org/10.1007/s00107-013-0727-6.

[195] J. Johansson, O. Hagman, and B. A. Fjellner. “Predicting moisture content and density distribution of Scots pine by microwave scanning of sawn timber”. In: *J. Wood Sci.* 49 (2003), pp. 312–316. DOI: 10.1007/s10086-003-0456-y. URL: https://doi.org/10.1007/s10086-003-0456-y.

[196] V. Tamme et al. “Experimental study of electrode effects of resistance type electrodes for monitoring wood drying process above fibre saturation point”. In: *For. Stud.* 56 (2012), pp. 42–55.

[197] V. Tamme, P. Muiste, and H. Tamme. “Experimental study of resistance type wood moisture sensors for monitoring wood drying process above fibre saturation point”. In: *For. Stud.* 59 (2013), pp. 28–44.

[198] *Conservation of Cultural Heritage—Methods of Measurement of Moisture Content or Water Content, in Materials Constituting Immovable Cultural Heritage.* 2017. URL: https://www.cen.eu/standards/publications/Pages/default.aspx.

[199] *Moisture Content of a Piece of Sawn Timber—Part 2: Estimation by Electrical Resistance Method.* 2002. URL: https://www.cen.eu/standards/publications/Pages/default.aspx.

[200] H. Forsen and V. Tarvainen. *Accuracy and functionality of hand held wood moisture content meters.* Tech. rep. VTT Technical Research Centre of Finland, 2000, pp. 79–17. URL: https://www.vtt.fi/inf/pdf/publications/2000/P379.pdf.

[201] S. Casans, T. Iakymchuk, and A. Rosado-Muñoz. “High resistance measurement circuit for fiber materials: Application to moisture content estimation”. In: *Measurement* 119 (2018), pp. 167–174. DOI: 10.1016/j.measurement.2017.11.013. URL: https://doi.org/10.1016/j.measurement.2017.11.013.

[202] G. Dai, K. Ahmet, and P.I. Morris. “A review of wood moisture content measurement techniques”. In: *Materials* 13.2 (2020), p. 300. DOI: 10.3390/ma13020300. URL: https://www.mdpi.com/1996-1944/13/2/300.

[203] S. Gao et al. “Comparison of voltammetry and digital bridge methods for electrical resistance measurements in wood”. In: *Comput. Electron. Agric.* 145 (2018), pp. 161–168. DOI: 10.1016/j.compag.2018.03.016. URL: https://doi.org/10.1016/j.compag.2018.03.016.

[204] Valdek Tamme, Peeter Muiste, and Hannes Tamme. “Experimental study of resistance type wood moisture sensors for monitoring wood drying process above fibre saturation point”. In: *Forestry Studies/Metsanduslikud Uurimused* 59.1 (2013).

[205] G Dai and K Ahmet. “Long-term monitoring of timber moisture content below the fiber saturation point using wood resistance sensors”. In: *Forest Products Journal* 51.5 (2001), p. 52.

[206] Silvia Casans Berga et al. “Novel wood resistance measurement method reducing the initial transient instabilities arising in DC methods due to polarization effects”. In: *Electronics* 8.11 (2019), p. 1253.

[207] Shan Gao et al. “Comparison of voltammetry and digital bridge methods for electrical resistance measurements in wood”. In: *Computers and Electronics in Agriculture* 145 (2018), pp. 161–168.

[208] A. Samuelson. *Resistanksurvor für elektriska fuktkvotsmätare. TräteknikCentrum.* Rapport L 9006029, Stockholm, 37pp, 1990.

[209] Holger Forsén, Veikko Tarvainen, et al. *Accuracy and functionality of hand held wood moisture content meters.* Technical Research Centre of Finland Espoo,, Finland, 2000.

[210] J Fernandez Golfin et al. “Curves for the estimation of the moisture content of ten hardwoods by means of electrical resistance measurements”. In: *Forest Systems* 21.1 (2012), pp. 121–127.

[211] IMST. *iM881A-XL LoRa® Radio Module - Wireless Solutions Application.* 2021. URL: `https://wireless-solutions.de/products/lora-solutions-by-imst/radio-modules/im881a-xl/`.

[212] LoRa Alliance. *LoRaMac-node.* `https://github.com/Lora-net/LoRaMac-node/blob/master/src/CMakeLists.txt`. accessed on 3 March 2023.

[213] Pape Abdoulaye Barro, Marco Zennaro, and Ermanno Pietrosemoli. “TLTN - The local things network: on the design of a LoRaWAN gateway with autonomous servers for disconnected communities”. In: *2019 Wireless Days (WD).* IEEE. 2019, pp. 1–4.

[214] A.R. Hambley. *Electronics.* Prentice Hall, 2000. ISBN: 9780136919827. URL: `https://books.google.es/books?id=0et7QgAACAAJ`.

[215] A.S. Sedra and K.C. Smith. *Microelectronic Circuits.* Oxford Series in Electrical and Computer Engineering. Oxford University Press, 2004. ISBN: 9780195142525. URL: `https://books.google.es/books?id=9UujQgAACAAJ`.

[216] P Garrahan. “Moisture Meter Correction Factors. Forintek Canada Corp”. In: *Proceedings of a seminar on “In-grade testing of structural lumber”, held at uSDA Forest Products laboratory, Madison WI.* 1988.

[217] Donald M Onysko, Christopher Schumacher, and Peter Garrahan. “Field measurements of moisture in building materials and assemblies: pitfalls and error assessment”. In: *Best 1 Conference–Building Enclosure Science & Technology*. 2008.

[218] Norbert Blenn and Fernando Kuipers. “LoRaWAN in the wild: Measurements from the things network”. In: *arXiv preprint arXiv:1706.03086* (2017).

[219] Juha Petajajarvi et al. “On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology”. In: *2015 14th International Conference on its Telecommunications (itst)*. IEEE. 2015, pp. 55–59.

[220] Johnny Gaelens et al. “LoRa mobile-to-base-station channel characterization in the Antarctic”. In: *Sensors* 17.8 (2017), p. 1903.

[221] Thomas Ameloot, Patrick Van Torre, and Hendrik Rogier. “Indoor body-to-body LoRa link characterization”. In: *2019 IEEE-APS Topical Conference on Antennas and Propagation in Wireless Communications (APWC)*. IEEE. 2019, pp. 042–047.

[222] Piotr Wojcicki et al. “Estimation of the Path-Loss Exponent by Bayesian Filtering Method”. In: *Sensors* 21.6 (2021), p. 1934.

[223] Theodore S Rappaport et al. *Wireless communications: principles and practice*. Vol. 2. prentice hall PTR New Jersey, 1996.

[224] Giulio Maria Bianco et al. “LoRa System for Search and Rescue: Path-Loss Models and Procedures in Mountain Scenarios”. In: *IEEE Internet of Things Journal* 8.3 (2020), pp. 1985–1999.

[225] Veli-Matti O Törmänen and Anssi J Mäkynen. “Determination of wood moisture content using angularly, spatially and spectrally resolved reflectance”. In: *2011 IEEE International Instrumentation and Measurement Technology Conference*. IEEE. 2011, pp. 1–5.

[226] Takashi Shinozaki et al. “Performance anomalies of advanced web server architectures in realistic environments”. In: *2006 8th International Conference Advanced Communication Technology*. Vol. 1. IEEE. 2006, pp. 169–174.

[227] Viknes Balasubramanee et al. “Twitter bootstrap and AngularJS: Frontend frameworks to expedite science gateway development”. In: *2013 IEEE International Conference on Cluster Computing (CLUSTER)*. IEEE Computer Society. 2013, pp. 1–1.

[228] R Sureswaran et al. “Active e-mail system SMTP protocol monitoring algorithm”. In: *2009 2nd IEEE International Conference on Broadband Network & Multimedia Technology*. IEEE. 2009, pp. 257–260.

[229] Charat Khamsaeng and Sophon Mongkolluksamee. “Providing an End-to-End Privacy Preservation over LoRa WanPlatforms”. In: *2020 - 5th International Conference on Information Technology (InCIT)*. 2020, pp. 56–60. DOI: 10.1109/InCIT50588.2020.9310934.

[230] The Things Network. *TTN Technology stack*. Last accessed 22 August 2022. 2020. URL: https://www.thethingsnetwork.org/tech-stack#section2.

[231] University of Valencia. *La NAU*. Last accessed 22 August 2022. URL: https://www.uv.es/uvweb/culture/en/la-nau/la-nau-cultural-centre/presentation-1285866274374.html.

[232] Scott Y Seidel and Theodore S Rappaport. “914 MHz path loss prediction models for indoor wireless communications in multifloored buildings”. In: *IEEE Transactions on Antennas and Propagation* 40.2 (1992), pp. 207–217.

[233] Weitao Xu et al. “Measurement, characterization, and modeling of LoRa technology in multi-floor buildings”. In: *IEEE Internet of Things Journal* 7.1 (2019), pp. 298–310.

[234] Mohamed Saban, Otman Aghzout, and Alfredo Rosado-Muñoz. “Deployment of a LoRa-based Network and Web Monitoring Application for a Smart Farm”. In: *2022 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0IoT)*. 2022, pp. 424–427. DOI: 10.1109/MetroInd4.0IoT54413.2022.9831521.

[235] Emanuele Cardillo and Alina Caddemi. “Feasibility study to preserve the health of an industry 4.0 worker: A radar system for monitoring the sitting-time”. In: *2019 II Workshop on Metrology for Industry 4.0 and IoT*. IEEE. 2019, pp. 254–258.

[236] Pasquale Pace et al. “An edge-based architecture to support efficient applications for healthcare industry 4.0”. In: *IEEE Transactions on Industrial Informatics* 15.1 (2018), pp. 481–489.

[237] B Wang. *The future of manufacturing: A new perspective. Engineering, 4 (5), 722–728*. 2018.

[238] Sachin S Kamble, Angappa Gunasekaran, and Shradha A Gawankar. “Sustainable Industry 4.0 framework: A systematic literature review identifying the current trends and future perspectives”. In: *Process safety and environmental protection* 117 (2018), pp. 408–425.

[239] Vince Salazar Thomas et al. “Estimating the prevalence of dementia in elderly people: a comparison of the Canadian Study of Health and Aging and National Population Health Survey approaches”. In: *International Psychogeriatrics* 13.S1 (2001), pp. 169–175.

[240] Carol T Kulik et al. *Aging populations and management.* 2014.

[241] Leonor Varandas et al. “Low-cost IoT remote sensor mesh for large-scale orchard monitorization”. In: *Journal of Sensor and Actuator Networks* 9.3 (2020), p. 44.

[242] Nikesh Gondchawar, RS Kawitkar, et al. “IoT based smart agriculture”. In: *International Journal of advanced research in Computer and Communication Engineering* 5.6 (2016), pp. 838–842.

[243] Siemens. *SIMATIC IOT2000. `https://new.siemens.com/global/en/products/automation/pc-based/iot-gateways/iot2000.html`, (accessed 10 November 2022).*

[244] Mohamed Saban et al. “A Smart Agricultural System Based on PLC and a Cloud Computing Web Application Using LoRa and LoRaWan”. In: *Sensors* 23.5 (2023). ISSN: 1424-8220. DOI: `10.3390/s23052725`. URL: `https://www.mdpi.com/1424-8220/23/5/2725`.

[245] Telegram BoT API. *Telegram Bot SDK. `https://telegram-bot-sdk.readme.io/docs`, (accessed 29 December 2022).*

[246] Alexandre Kalache and Arianna Gatti. “Active ageing: a policy framework.” In: *Advances in gerontology= Uspekhi gerontologii* 11 (2003), pp. 7–18.

[247] HelpAge International UNFPA. *Ageing in the twenty-first century: a celebration and a challenge.* 2012.

[248] Gerard Anderson and James R Knickman. “Changing the chronic care system to meet people’s needs”. In: *Health Affairs* 20.6 (2001), pp. 146–160.

[249] R Jan Gurley et al. “Persons found in their homes helpless or dead”. In: *New England Journal of Medicine* 334.26 (1996), pp. 1710–1716.

[250] Instituto Nacional de Estadística INE. *Encuesta Continua de Hogares (ECH).* 2020.

[251] Liang Cao et al. “GCHAR: An efficient Group-based Context—Aware human activity recognition on smartphone”. In: *Journal of Parallel and Distributed Computing* 118 (2018), pp. 67–80.

[252] Raffaele Gravina et al. “Cloud-based Activity-aaService cyber–physical framework for human activity monitoring in mobility”. In: *Future Generation Computer Systems* 75 (2017), pp. 158–171.

[253] Clare Liddy et al. “Telehomecare for patients with multiple chronic illnesses: Pilot study”. In: *Canadian Family Physician* 54.1 (2008), pp. 58–65.

[254] “Remote health monitoring for older adults and those with heart failure: adherence and system usability”. In: 22.6 (2016), pp. 480–488.

[255] Zhongna Zhou et al. “Activity analysis, summarization, and visualization for indoor human activity monitoring”. In: *IEEE transactions on circuits and systems for video technology* 18.11 (2008), pp. 1489–1498.

[256] Emmanuel Munguia Tapia, Stephen S Intille, and Kent Larson. “Activity recognition in the home using simple and ubiquitous sensors”. In: *International conference on pervasive computing*. Springer. 2004, pp. 158–175.

[257] Chitsutha Soomlek and Luigi Benedicenti. “Operational wellness model: A wellness model designed for an agent-based wellness visualization system”. In: *2010 Second International Conference on eHealth, Telemedicine, and Social Medicine*. IEEE. 2010, pp. 45–50.

[258] Majd Alwan. “Passive in-home health and wellness monitoring: Overview, value and examples”. In: *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE. 2009, pp. 4307–4310.

[259] NK Suryadevara et al. “Wellness determination of inhabitant based on daily activity behaviour in real-time monitoring using sensor networks”. In: *2011 Fifth International Conference on Sensing Technology*. IEEE. 2011, pp. 474–481.

[260] Lorenzo Vangelista12, Andrea Zanella, and Michele Zorzi12. “Long-range IoT technologies: the dawn of LoRa TM”. In: *2015 1st EAI International Conference on Future access enablers of ubiquitous and intelligent infrastructures (EAI)*. 2015.