UNIVERSIDAD POLITÉCNICA DE MADRID
Escuela Técnica Superior de Ingenieros de Telecomunicación

On the Trade-Offs Between Energy Harvesting & Wireless Communications for Stand-Alone IoT Devices

DOCTORAL THESIS

Submitted for the degree of Doctor by:

Edgar Saavedra Darriba
Telecommunications Engineer

Madrid, 2024

UNIVERSIDAD POLITÉCNICA DE MADRID
Escuela Técnica Superior de
Ingenieros de Telecomunicación

Doctoral Degree in
Communication Technologies and Systems

On the Trade-Offs Between Energy Harvesting & Wireless Communications for Stand-Alone IoT Devices

DOCTORAL THESIS

Submitted for the degree of Doctor by:

Edgar Saavedra Darriba
Telecommunications Engineer

Under the supervision of:
Dr. Asunción Santamaría Galdón

Madrid, 2024

Title: On the Trade-Offs Between Energy Harvesting & Wireless Communications for Stand-Alone IoT Devices

Author: Edgar Saavedra Darriba

Doctoral Programme: Communication Technologies and Systems

Thesis Supervision:

Dr. Asunción Santamaría Galdón, Full Professor, UPM (Supervisor)

External Reviewers:

Thesis Defense Committee:

Thesis Defense Date:

This thesis has been partially supported by the project 'Context-Aware and Veracious Big Data Analytics for Industrial IoT' (ABIDI), within the framework of the CHIST-ERA ERA-NET Call 2017 for the topic 'Big Data and Process Modelling for Smart Industry' (BDSI), funded by Spain's State Research Agency (AEI) under the Ministry of Science and Innovation (MICINN) with reference PCI2019-103762.

Abstract

The proliferation of the Internet of Things has driven significant advancements in energy harvesting and wireless communications, enabling the deployment of autonomous devices in diverse, resource-constrained environments. This thesis investigates the trade-offs between energy harvesting techniques and IoT wireless communication protocols to design stand-alone IoT devices capable of sustained operation without human intervention.

By addressing critical gaps, a systematic framework to evaluate and integrate energy harvesting systems with low-power communication technologies is established. This matter requires a tailored configuration of the whole IoT system for the specific use case, do that a virtually infinite operation without intervention be feasible.

The research adopts a multi-phase methodology encompassing analysis of energy harvesting techniques, energy requirements of IoT protocols, use case's requisites evaluation, and the development of a universal testbed to verify results, evaluating latency, error rate and stability across various protocols and hardware platforms. offering

Outcomes demonstrate the feasibility of developing self-powered IoT networks in a variety of scenarios, ranging from remote environmental monitoring to industrial automation, what leverages significant improvements in maintenance, operational costs, sustainability and scalability.

Key findings reveal that the synergy between energy harvesting and protocol optimization enhances energy efficiency, ease of deployment, scalability and reliability. Thus, this thesis aims to help pave the way for elevating the connected society.

Resumen

El crecimiento del Internet de las Cosas (IoT) ha impulsado avances significativos en *energy harvesting* y las comunicaciones inalámbricas, permitiendo el despliegue de dispositivos autónomos en entornos diversos y con recursos limitados. Esta Tesis investiga los compromisos entre las técnicas de *energy harvesting* y los protocolos de comunicación inalámbrica para IoT, de forma que se puedan diseñar dispositivos autónomos capaces de operar de forma sostenida sin intervención humana.

Se establece un marco sistemático para evaluar e integrar sistemas de *energy harvesting* con tecnologías de comunicación de bajo consumo. Este enfoque requiere una configuración adaptada de todo el sistema IoT según el caso de uso específico, haciendo posible una operación virtualmente infinita en el tiempo sin intervención.

La investigación adopta una metodología en varias fases que incluye el análisis de técnicas de *energy harvesting*, los requerimientos energéticos de los protocolos IoT, la evaluación de los requisitos del caso de uso y el desarrollo de un banco de pruebas universal para verificar los resultados, evaluando latencia, tasa de error y la estabilidad en diversos protocolos y plataformas de hardware.

Los resultados demuestran la viabilidad de desarrollar redes IoT autosuficientes en una variedad de escenarios, desde el monitoreo ambiental en ubicaciones remotas hasta la automatización industrial, logrando mejoras significativas en mantenimiento, costos operativos, sostenibilidad y escalabilidad.

Los hallazgos clave revelan que la sinergia entre el *energy harvesting* y la optimización de protocolos mejora la eficiencia energética, la facilidad de despliegue, la escalabilidad y la confiabilidad. Con ello, esta Tesis busca contribuir al avance sostenible y eficaz hacia una sociedad más conectada.

Contents

ABSTRACT iii
RESUMEN iv
FIGURES & TABLES vi

1. INTRODUCTION 1
1.1. FOUNDATION 2
1.2. ABIDI 5
1.3. HYPOTHESIS 7
1.4. OBJECTIVES 8

2. STATE OF THE ART 11
2.1. SMART METERING 11
2.1.1. Varying Needs Lead to Distinct Approaches 11
2.1.2. Current and Future Directions 13
2.2. ENERGY HARVESTING 14
2.2.1. Modern IoT Will Need Energy Harvesting 14
2.2.2. Specific Energy Harvesting Techniques 15
2.2.3. Realizing Harvested Energy 18
2.3. WIRELESS COMMUNICATIONS 19
2.4. INTEROPERABILITY 24
2.5. SECURITY & AI 28

3. METHODOLOGY 29
PHASE I – RESEARCH ON ENERGY HARVESTING SYSTEMS 29
PHASE II – ANALYSIS OF ENERGY REQUIREMENTS FOR IOT 30
PHASE III – DEVELOPING A TESTBED FOR IOT NETWORKS 31
PHASE IV – INTEGRATION AND SYNTHESIS 32
PHASE V – REPORTING, DISSEMINATION 32

4. RESULTS 35
4.1. MILESTONES 35
4.2. COMPENDIUM OF PUBLICATIONS FOR THIS THESIS 37
I. DOI: 10.3390/s20247133 38
II. DOI: 10.3390/s21227433 65
III. DOI: 10.3390/s22114159 90
IV. DOI: 10.3390/app14083411 114

5. DISCUSSION 135
5.1. HARVESTING & WIRELESS — TAILORING 137
5.2. SCALABILITY & INTEROPERABILITY 140
5.3. BROADER IMPLICATIONS 142

6. CONCLUSION 145
6.1. FUTURE RESEARCH 145

REFERENCES 149
ANNEXES 155

Figures & Tables

Figure 1. Global IoT market forecast from 2019 to 2030 (real data until Q4/2023). 1

Figure 2. Left: front side of the prototype, where the LoPy4 and the electronic subsystems can be seen; right: back side, where the battery, antenna and clamp inductor are shown. 2

Figure 3. A high-level representation of the ABIDI Framework. 5

Figure 4. Screenshot from an ABIDI's web application detecting HVAC usage inside CeDInt's building, utilizing multiple data streams. 7

Figure 5. Overview on global CO2 emissions [Ritchie 2020]. 13

Figure 6. Google Trends for 'energy harvesting', 'internet of things', 'smart meters'; period 2010-2024 15

Figure 7. High-level schematic of the smart meter's EH subsystem. 18

Figure 8. General diagram of the solution presented in [Saavedra 2024]. 25

Figure 9. Latency: abstract definition and message paths for different wireless IoT topologies. Paths are, for i) 6LoWPAN, Zigbee, LoRaWAN; ii) Sigfox, NB-IoT; iii) Wi-Fi, BLE; as follows: i) A-B-E-F; ii) A-D-H; iii) A-C-G. 26

Table 1. Energy consumption of a message transmission for different IoT wireless technologies within the smart meter use case. 20

Table 2. Summary of IoT wireless technologies' features. 21

Table 3. Smart meter average consumption (mW) depending on buffer size—message payload—, metering period and wireless technology; where italics mean that magnetic induction EH complies, so does PV; underline means that only PV complies; grey text means that no EH technique would comply. 139

1. Introduction

The rapid proliferation of the Internet of Things (IoT) in recent years has heralded an era of unprecedented connectivity, enabling devices across diverse sectors to communicate, interact, and exchange data over expansive networks. IoT is revolutionizing industries ranging from healthcare and agriculture to industrial automation and urban development, fundamentally redefining how data—irrespective of its nature—is collected, processed, and harnessed to enhance efficiency, sustainability, and generate transformative insights.

IoT's influence extends across multiple domains of modern society—and continues to expand—showcasing the profound potential of connected devices. Nonetheless, this vast diversity of devices, stakeholders, and applications also presents significant challenges to IoT interoperability, democratization, and scalability.

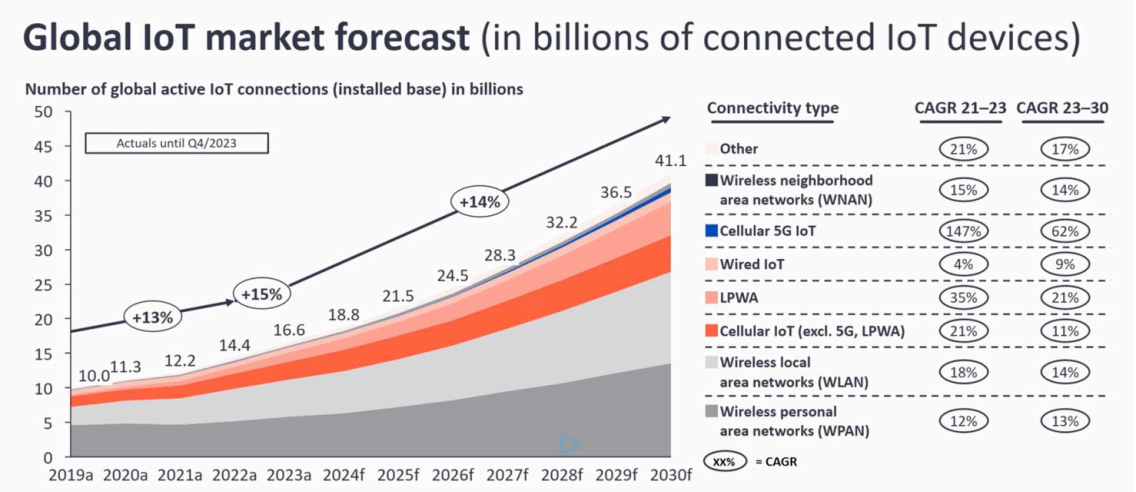


Figure 1. Global IoT market forecast from 2019 to 2030 (real data until Q4/2023)*.

As the IoT continues to proliferate (Figure 1), their reliance on traditional power sources and wireless communication infrastructures raises critical challenges, particularly for stand-alone systems operating in remote or resource-constrained environments. Energy harvesting has emerged as a promising solution to address these limitations, enabling devices to harness energy from their surroundings—such as solar, thermal, or kinetic sources—to sustain their operation. However, this paradigm introduces trade-offs between energy availability, efficiency, and the performance of wireless communications, requiring a careful balance to ensure reliability, scalability, and long-term viability in a diverse range of IoT applications.

* This graph was obtained from [Sinha 2024], where periodic projections on IoT-related numbers and insights on previous data are published.

1.1. Foundation

The genesis of this thesis is closely intertwined with my personal journey as a researcher at CeDInt-UPM. I began my professional path at CeDInt in 2016, during my Master studies in Telecommunication Engineering, joining the Energy Efficiency and Internet of Things Department. CeDInt, a renowned R&D center, has established itself as a benchmark in key areas such as Wireless Sensor Networks—particularly for applications in energy efficiency, home automation, smart cities, virtual reality, and advanced data visualization.

My early involvement in diverse research projects expanded my perspective, solidified my technical foundation, and deepened my understanding of emerging technologies and market dynamics. These experiences allowed me to witness firsthand the transformative potential of IoT across various domains. At the same time, the rapid evolution of the IoT landscape revealed its complexities, with competing players often proposing conflicting solutions, adding layers of ambiguity to an already intricate field.

The seeds of this thesis were sown during my Master thesis, where my curiosity about energy harvesting took shape. My work focused on autonomous smart metering, exploring magnetic induction energy harvesting and comparing it to more established techniques. Certainly, this work ultimately succeeded in building a fully functional prototype (Figure 2) that was presented at the international congress IE2020 [Saavedra 2020]. This experimentation sparked a deeper interest in the interplay between energy harvesting methods and IoT devices' autonomy.

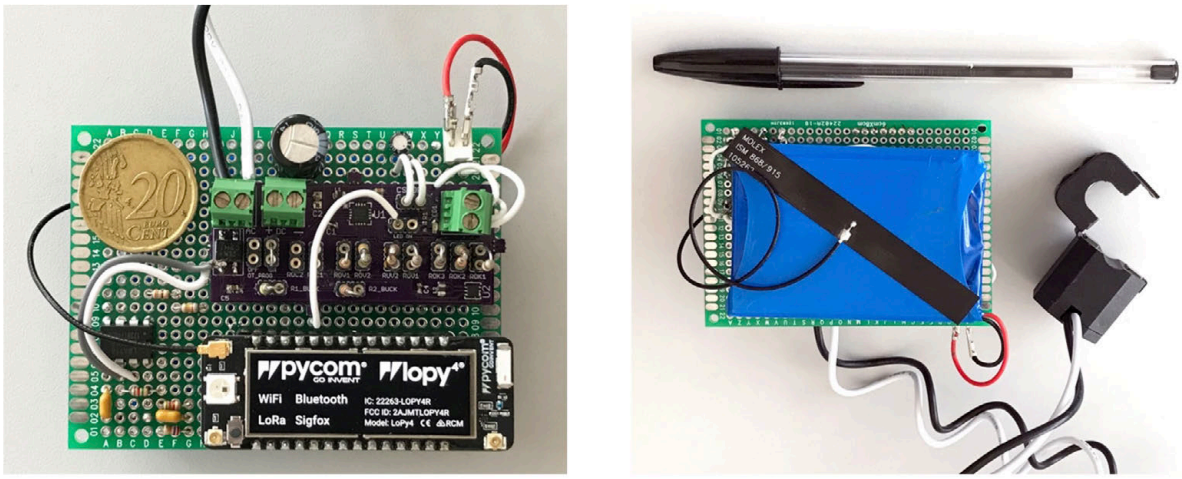


Figure 2. Left: front side of the prototype, where the LoPy4 and the electronic subsystems can be seen; right: back side, where the battery, antenna and clamp inductor are shown.

These formative experiences laid the foundation for this thesis, which seeks to address the crucial challenge of selecting the most suitable combination of wireless communication technologies and energy harvesting techniques. The goal is to provide a comprehensive framework for designing stand-alone IoT devices tailored to specific domains, considering their requirements for data transmission, energy consumption, and operational contexts*.

Key IoT Domains

* CeDInt | Self-powered system. https://www.cedint.upm.es/en/project/self-powered-system

The IoT is reshaping industries and redefining how we interact with the world and society. With its ability to connect devices, gather data, and enable intelligent decision-making, IoT has become a cornerstone for innovation across a wide range of domains. From enhancing operational efficiency in industries to addressing global challenges like urban sustainability and environmental conservation, IoT's applications are as diverse as they are impactful. Each domain not only benefits from IoT's capabilities but also drives further advancements, making IoT a truly dynamic field.

By leveraging connected devices, real-time data and automation, these domains showcase the potential of IoT to improve efficiency, sustainability, and quality of life. Whether revolutionizing healthcare with wearable technology, optimizing resource use in agriculture, or transforming transportation through connected vehicles, these use cases highlight IoT's versatility and far-reaching implications. Understanding these domains provides a comprehensive view of IoT's role as a critical enabler of progress in the modern world.

Health

IoT-enabled devices in healthcare are revolutionizing patient monitoring and care. Wearable devices, such as smartwatches and fitness trackers, continuously gather and analyze data on vital signs and physical activity. This real-time information allows healthcare providers to monitor patient health remotely, facilitating early intervention and preventive care. For instance, wearable devices can alert providers to irregular heart rates or other health indicators, reducing hospital readmissions and enhancing overall healthcare efficiency. IoT technology is also improving healthcare logistics, such as tracking critical medical supplies, further supporting streamlined operations.

Agriculture

In agriculture, IoT has given rise to "smart farming," where sensors monitor field conditions such as soil moisture, nutrient levels, and ambient temperature. This data enables farmers to optimize water and fertilizer use, maximizing crop yields while conserving resources and reducing environmental impact. IoT-enabled machinery, such as autonomous tractors and drones, further enhances efficiency by streamlining planting, fertilizing, and harvesting processes. This data-driven approach to farming supports greater resilience and sustainability in agricultural practices, crucial for meeting the global demand for food.

Industry

IoT is a key component of Industry 4.0, where connected devices enhance operational efficiency in manufacturing and logistics. IoT sensors in smart factories monitor machinery, facilitating predictive maintenance that minimizes downtime and extends equipment life. Additionally, IoT optimizes supply chain management by improving inventory tracking, real-time shipment monitoring, and logistics planning, ultimately reducing operational costs and enhancing productivity. This interconnected approach is transforming industries, enabling more responsive and adaptive production processes.

City

Urban environments are leveraging IoT to improve residents' quality of life and the efficiency of municipal services. For example, smart traffic management systems use real-time data from sensors and cameras to adjust traffic signals, easing congestion, reducing emissions, and enhancing road safety. IoT-enabled street lighting systems adjust brightness based on foot traffic and vehicle

movement, reducing energy consumption. Moreover, smart waste management systems with IoT sensors monitor bin levels, optimizing waste collection routes to reduce costs and environmental impact. These applications illustrate the potential of IoT to support sustainable urban growth.

Energy

IoT is transforming energy management by enabling smarter and more sustainable practices. Smart grids, equipped with IoT-enabled sensors, allow for real-time monitoring and control of energy distribution, improving efficiency and reducing energy losses. IoT devices in homes and businesses, such as smart meters and connected appliances, provide granular insights into energy consumption patterns, empowering users to optimize their usage and lower costs. Additionally, IoT-based demand response systems dynamically adjust energy supply based on real-time demand, contributing to grid stability. Renewable energy sources, like solar and wind, are also being integrated into IoT-powered energy management systems, ensuring their optimal utilization while supporting global sustainability goals.

Vehicle

The automotive sector is harnessing IoT to revolutionize transportation through connected vehicles. IoT-enabled systems facilitate vehicle-to-everything (V2X) communication, allowing cars to interact with each other, infrastructure, and even pedestrians to enhance safety and reduce accidents. Autonomous driving technologies rely heavily on IoT sensors and data to navigate roads and respond to environmental changes. For example, real-time data from cameras, LiDAR, and radar systems enable precise decision-making for self-driving cars. Additionally, IoT integration improves user experiences with advanced infotainment systems, predictive maintenance alerts, and personalized driving features. These innovations are paving the way for smarter, safer, and more efficient mobility solutions.

Retail

IoT is reshaping the retail industry by optimizing operations and enhancing customer experiences. Smart shelves, equipped with weight sensors and RFID tags, monitor inventory in real-time, ensuring stock availability and reducing waste. IoT-enabled beacons personalize the shopping experience by delivering tailored promotions and product recommendations to customers' smartphones. In warehouses and logistics, IoT devices provide real-time tracking of shipments and optimize supply chain operations, ensuring timely delivery and reducing costs. These innovations not only streamline backend processes but also elevate the shopping experience, positioning IoT as a cornerstone of modern retail practices.

Environment

IoT is playing a crucial role in environmental conservation and monitoring. IoT-enabled sensors are deployed in natural ecosystems to collect real-time data on air quality, water levels, temperature, and other environmental parameters. For instance, connected devices in rivers and lakes monitor water quality, detecting pollutants and ensuring compliance with environmental regulations. Similarly, IoT networks track deforestation rates, wildlife movement, and soil degradation, providing actionable insights to researchers and policymakers. These systems enable early detection of environmental threats, support disaster prevention efforts, and contribute to a more sustainable relationship between human activities and the planet. By leveraging IoT for environmental

monitoring, we are taking significant strides toward preserving natural resources for future generations.

1.2. ABIDI

This thesis is framed within the ABIDI (Context-Aware and Veracious Big Data Analytics for Industrial IoT) projects' scope*. The project ABIDI is a European multidisciplinary initiative funded by CHIST-ERA†. Its overarching goal is to develop solutions that address key challenges in industrial IoT (IIoT) environments by leveraging cutting-edge technologies in big data analytics, machine learning, edge computing, context-aware systems and the very IoT networks themselves. By improving data veracity, contextualization, and knowledge discovery, ABIDI aims to enable reliable, efficient, and autonomous IIoT systems capable of supporting fully automated industrial processes.

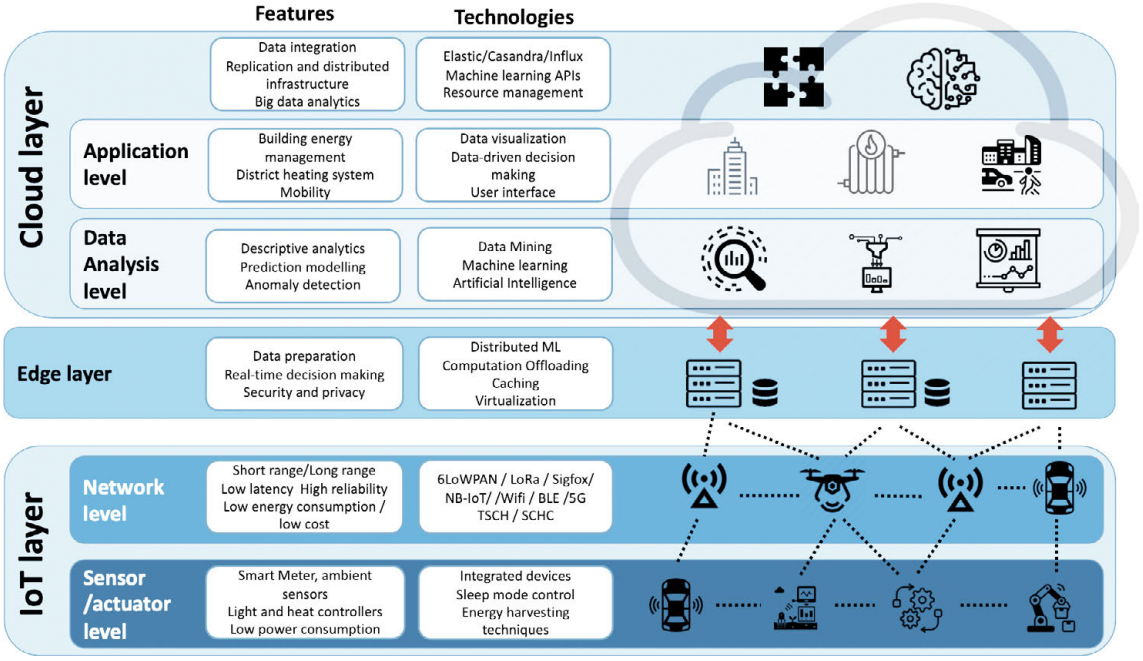


Figure 3. A high-level representation of the ABIDI Framework.

The project focuses on several interconnected aspects: building reliable IIoT networks, designing intelligent edge computing infrastructures, developing scalable big data processing systems, and creating adaptive machine learning models for handling complex data streams (Figure 3). These components are integrated and validated through a comprehensive use case centered on energy consumption prediction in a smart building environment at UPM‡.

Objectives and Key Innovations of ABIDI

ABIDI aims to address four primary challenges inherent to IIoT environments, be they:

- **Reliable IIoT Networks.** IIoT systems demand high reliability in data communication, even in noisy, harsh industrial environments. ABIDI focuses on enhancing wireless protocols,

* Context-Aware and Veracious Big Data Analytics for Industrial IoT. https://www.chistera.eu/projects/abidi
† CHIST-ERA ERA-NET | Our Mission. https://www.chistera.eu/mission
‡ CeDInt | ABIDI. https://www.cedint.upm.es/en/project/abidi

such as IEEE 802.15.4, to achieve low latency, minimal jitter, and high packet delivery rates in industrial applications.

- **Edge Computing Infrastructure.** To reduce latency and improve decision-making, ABIDI emphasizes shifting computation from centralized cloud systems to edge devices. This includes deploying machine learning models and semantic reasoning capabilities directly on IoT gateways and nodes.
- **Big Data Processing and Scalability.** ABIDI addresses the challenges of managing the variety, velocity, and volume of IIoT data streams. The project evaluates and optimizes NoSQL solutions to balance computational workloads between edge devices and centralized big data infrastructures.
- **Adaptive Machine Learning Models.** ABIDI develops prediction models that adapt to the dynamic nature of IIoT systems, accounting for sensor malfunctions, data uncertainty, and changing environmental conditions.

ABIDI's connection to this thesis is directly related to the first challenge—reliable IIoT networks. Key outcomes from the project are, in fact, published within the compendium of papers of this thesis.

Use Case: Energy Efficiency in Smart Buildings

ABIDI's research outcomes are validated through a real-world application at UPM's CeDInt laboratory, where IoT systems are deployed to optimize energy consumption and HVAC control in a three-story smart building*. The setup includes:

- **Energy Meters.** Monitoring 560 electrical lines with 30 IoT devices.
- **Ambient Sensors.** Capturing temperature, humidity, luminosity, and occupancy data using 40 IoT devices.
- **HVAC Controllers.** Managing temperature, fan speed, and operational states through 30 devices.

Primary objectives of this use case are to improve energy efficiency through detailed, context-aware analysis of energy usage patterns, and to automate HVAC control by learning from user behavior and environmental factors. An exemplification of this matter can be seen in Figure 4.

* CeDInt's IoT pilots, tests and proof of concepts deployed within their facilities and UPM's Montegancedo Campus are detailed in https://www.cedint.upm.es/en/project/batnet

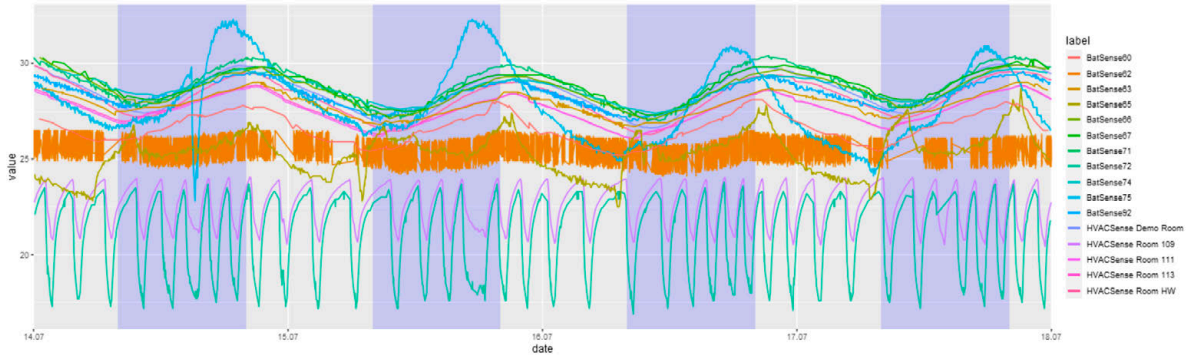


Figure 4. Screenshot from an ABIDI's web application detecting HVAC usage inside CeDInt's building, utilizing multiple data streams.

This environment serves as a testbed for validating the project's advancements in data veracity, predictive modeling, and edge-based decision-making.

Synergy's Implications

The outcomes of ABIDI and this thesis have significant implications for the broader IoT ecosystem:

- **Industry Impact.** By enhancing the efficiency and reliability of IIoT systems, the research contributes to the development of smarter, more autonomous industrial processes. Energy harvesting systems, as explored in the thesis, reduce the operational costs and environmental impact of large-scale IoT deployments.
- **Societal Benefits.** Improved energy efficiency and predictive maintenance reduce resource consumption and promote sustainable practices. The integration of ABIDI's frameworks with energy harvesting technologies paves the way for eco-friendly smart cities and industrial systems.
- **Technological Advancements**. The combination of advanced data analytics, machine learning, and energy harvesting technologies accelerates the evolution of IoT architectures. This synergy enhances the scalability, adaptability, and sustainability of IoT systems in various domains.

The combined research contributed to addressing critical challenges in IIoT environments. The alignment of goals, methodologies, and outcomes highlights the complementary nature of both initiatives, underscoring their collective impact on advancing sustainable and intelligent IoT systems. As ABIDI progresses toward its objectives, the findings and innovations from this thesis may help shape the future of industrial IoT.

1.3. Hypothesis

The starting situation is that the rapid proliferation of Internet of Things (IoT) devices has introduced a diverse and diffuse landscape of technologies, particularly in the domains of energy harvesting and wireless communication.

Despite the wealth of options available, the lack of a unified approach to selecting appropriate technologies for specific use cases poses a significant challenge. Years of research have highlighted the need for a systematic framework—a blueprint or set of guiding principles—to aid in making informed decisions when designing fully autonomous IoT devices.

There is a need for self-sufficient, non-intrusive IoT electronic devices capable of operating for extended periods without human intervention.

This type of device is essential in scenarios where modifications to existing infrastructure are not feasible, such as industrial environments, factories, and production lines. The lack of adequate solutions currently limits the deployment of these systems.

The success of energy harvesting systems depends not only on the technology used but also on the communication protocols implemented by IoT devices. Therefore, for the design of viable energy harvesting solutions, it is essential to understand the energy consumption requirements associated with the different protocols used in the IoT networks. Additionally, it is necessary to have a tool for selecting the most suitable wireless IoT technology for the needs of each use case.

The central hypothesis of this work posits that

> *Advanced energy harvesting solutions can be developed for non-intrusive IoT devices so as to address the current gap in efficacious, viable alternatives. This realization may require a custom, perhaps unique design approach and implementation process, which rigorously account for those devices' specific energy requirements, as dictated by the communication protocols they employ, as well as other use case's requisites to comply.*

1.4. Objectives

The main objective of this thesis is to achieve the deployment of IoT networks in environments where an adequate power supply is unavailable, either because it does not exist or cannot be utilized. In these cases, self-powered IoT devices are essential to ensure the sustainability, scalability, and effectiveness of IoT networks in such environments, while reducing maintenance requirements and improving energy efficiency. Some examples of these environments are the following:

- Remote areas and rural zones with **no access to the electrical grid** where IoT networks need to be deployed for environmental monitoring, precision agriculture infrastructure, or water resource management.
- **Densely developed urban areas** where installing electrical wiring can be expensive or disruptive, yet systems for air quality monitoring, traffic sensors, or smart parking are needed.
- **Industrial environments** where IoT devices must be installed guaranteeing not to interfere with existing infrastructure. In these environments devices operate under extreme conditions—high temperatures, humidity, vibrations)—and maintenance access is difficult, as seen in deployments for machinery monitoring.
- Applications with IoT devices **embedded in vehicles** or mobile systems, where energy must be independent, such as fleet trackers, autonomous drones, and agricultural robots.
- Installations in **natural ecosystems**, such as protected areas where wiring or human intervention could damage the environment. This is the case with biodiversity monitoring systems, forest fire management, and climate sensors.
- Monitoring of **critical infrastructures**, where continuous monitoring is required, and conventional energy sources may be unreliable, such as in bridges, dams, and power grids.

- IoT applications for **smart buildings**, aiming to reduce energy consumption through sustainable solutions like smart lighting systems, climate control, or presence monitoring.
- **Temporary** or emergency applications that require rapid, autonomous installation of IoT devices, such as the monitoring of massive events or temporary deployments.

These scenarios illustrate the importance of self-powered IoT networks in enabling efficient, sustainable, and scalable solutions across a wide range of challenging environments. To achieve the main objective, the following partial objectives were proposed:

A. Design and implementation of viable EH systems for IoT devices

This objective focuses on the identification, evaluation, and development of energy harvesting (EH) systems capable of powering low-consumption IoT devices. It involves a thorough analysis of the various energy harvesting techniques available, evaluating their capacity to meet the specific energy requirements of such devices. Once the most suitable EH techniques are identified, experimental validation will be carried out through the design, implementation, and testing of prototypes. This approach will demonstrate the technical feasibility of the selected EH systems, evaluating their performance in real operational scenarios and their effective integration with IoT devices.

B. Analysis of the energy requirements of various IoT protocols

This objective focuses on a detailed study of the energy demands associated with the main communication protocols used in IoT networks. The aim is to identify those protocols that can be efficiently implemented in self-powered devices using energy harvesting (EH) techniques. The analysis will include the evaluation of energy consumption characteristics for each protocol and the determination of optimal configurations to maximize energy efficiency. This step is critical to facilitate the implementation of self-powered IoT systems. Once the most suitable protocols are selected, experimental work will be conducted for their practical implementation. This process will identify optimal combinations of IoT protocols and EH techniques, ensuring the viability of IoT devices with optimal performance and energy sustainability.

C. Development of a testbed to evaluate key IoT network parameters

The objective is to design and build a technical testbed to measure and analyze the critical performance parameters of IoT networks, such as latency, error rate, and stability. Currently, no standardized or accessible tools exist to objectively compare different IoT technologies. This limits the ability to select the most suitable technology to meet the specific requirements of a system or use case. The implementation of this platform will provide a valuable technical resource for comparative evaluation, enabling informed decisions regarding the selection of optimal IoT solutions tailored to operational and deployment needs.

The proposed objectives provide a comprehensive and well-founded framework to address the key challenges associated with the development of self-powered IoT networks. Each of them tackles critical aspects essential to ensuring the technical feasibility, energy efficiency, and functionality of these systems in diverse operational scenarios—almost bijectivity:

Design and implementation of EH systems

This objective establishes the technological foundation needed to provide energy autonomy to IoT devices by leveraging environmental energy sources. The identification, analysis, and validation

of EH techniques ensure that the developed systems are viable, efficient, and capable of integrating into real-world environments.

Analysis of the energy requirements of IoT protocols

This objective complements the previous one by ensuring that the communication protocols used in IoT networks are compatible with the energy constraints inherent to self-powered systems. By identifying optimal configurations and conducting experimental tests, efficient and sustainable implementation is ensured.

Development of a testbed to evaluate key parameters

This objective provides a critical tool to measure and analyze the performance of IoT networks, enabling the objective comparison of technologies and protocols. This facilitates the selection of optimal combinations of EH, protocols, and configurations, maximizing system efficiency and performance.

Together, these objectives not only address energy autonomy and protocol design but also ensure that the solutions developed are rigorously evaluated in terms of performance, scalability, and suitability for specific needs. This establishes a clear and robust path toward the implementation of efficient, sustainable, and adaptable self-powered IoT networks that meet current technological challenges.

2. State of the Art

The rapid development and deployment of Internet of Things (IoT) technologies have fundamentally altered numerous industries by introducing an unparalleled level of connectivity and data exchange. As the IoT landscape continues to evolve, several key technologies and methodologies have emerged, each contributing to the diverse and dynamic ecosystem that defines modern IoT applications. This section explores the current state of the art in IoT, focusing on significant technological advancements, existing challenges, and the role of various communication protocols and energy harvesting techniques in advancing IoT deployments.

The foundation of IoT is built upon a complex array of sensors, actuators, communication protocols, and data processing systems. These components collectively enable the creation of smart environments where devices can communicate, process data, and make autonomous decisions.

At the heart of IoT are low-power wireless communication technologies, which facilitate the seamless transmission of data between devices and centralized systems. Key protocols such as Zigbee, Bluetooth Low Energy (BLE), LoRaWAN, and 6LoWPAN have been instrumental in enabling low-power, wide-area communications suitable for various IoT applications.

Since this thesis is presented by a compendium of publications—as detailed in Section 0 hereof—its SoA reflects the knowledge investigated, studied, required to perform, understand and elevate the research. Central to this work are the interrelated domains of smart meters, energy harvesting techniques, wireless communication technologies, and the interoperability of IoT systems. These thematic pillars form the foundation upon which the contributions of this thesis are built. Following subsections review the SoA in these areas, emphasizing the innovations, methodologies, and technical advancements ineludible to the course of the thesis.

2.1. Smart Metering

Smart metering has become a pivotal technology in the modernization of energy management systems, particularly in the context of IoT-enabled solutions. These devices offer real-time monitoring and control of energy consumption, improving efficiency, reducing waste, and fostering sustainable practices. However, the design and implementation of smart meters face multiple challenges, including energy autonomy, cost-effectiveness, communication reliability, and ease of deployment.

2.1.1. Varying Needs Lead to Distinct Approaches

Several smart meter technologies are currently in use, each with unique operational characteristics. In fact, they may be split by their installation method: i) utility grid, ii) electrical panel, and iii) stand-alone.

Utility Grid

A primary category includes those smart meters installed by utility companies to remotely collect consumption data for accurate billing purposes [Sendin 2012, 2014]. These meters often play a role in the broader context of the smart grid, enabling dynamic demand response mechanisms, which adjust energy consumption based on real-time data and grid condition [Chren 2016]. They

are not manageable and consumption is usually metered as a whole per residential/industrial unit—without splitting into circuits.

Electrical Panel

In this group fall most commercial smart meters. They are powered directly from the electrical mains through a transformer, as seen in systems discussed in [Reinhardt 2011]. As they are directly attached to the line under observation, they can sample both voltage and current, allowing for the calculation of power factor. However, this specific *pro* is their major *con*, as their installation often requires power supply interruption and professional installation—even administrative paperwork—which increase costs and limit deployment in certain environments [Praktiknjo 2011; Woo 2014].

Additionally, in developing regions or rural areas, the infrastructure of electrical panel boards often presents challenges such as limited space, difficult access, or non-standard configurations. This makes it impractical to install traditional smart meters in these settings, where non-intrusive and cost-effective solutions become crucial factors in the selection of appropriate devices.

Stand-Alone

Let us differentiate between self-powered smart meters, and (literally) plug-and-play ones. The latter are the most established, they usually are plugs with both a plug itself and a receptacle; they are plugged into the wall, and the load of interest eventually plugged into the smart meter's receptacle. This load would be subject to observation and consumption reckoning. Sometimes they also come in the form of plastic boxes with electrical terminals, where a power cord is interrupted.

In contrast, self-powered ones have been gaining interest and even place in the last years. Since these systems do not rely on an external power supply, they are more suitable for diverse, unexpected environments. Various self-powered meter designs have emerged, each with distinct measurement capabilities, electronic configurations, and installation methods. For instance, in [Moghe 2010], a self-adhesive current and temperature sensor was developed using Zigbee for wireless communication, designed to measure currents in the range of 60–1000 A. This type of solution is advantageous for its easy installation and flexibility.

In another example, [Cai 2012] describes the integration of a GPS receiver within a smart meter to ensure time synchronization with the data, a useful feature for maintaining accurate readings across distributed systems. Furthermore, [Porcarelli 2013] shows a smart meter that complies with IEEE 802.15.4, incorporating a backup battery and designed for consumption measurements ranging from 10 W to 10 kW, with a reported maximum measurement error of 1.6%. This system illustrates a reliable solution for varying consumption profiles while ensuring robustness in energy monitoring.

A further advancement in self-powered smart meters is presented in [Han 2015], where a piezoelectric cantilever, excited by the magnetic coupling of AC, is used to harvest energy from the surrounding environment to power the device. This method allows for continuous operation without the need for an external power supply, offering a sustainable solution for remote monitoring. Additionally, [Paprotny 2010] outlines the development of microelectromechanical systems that integrate self-powered current sensors with the capability to also measure voltage, marking a promising direction for the next generation of smart meters that are both compact and highly efficient.

Self-powered smart meters are still a significant innovation in the field, overcoming many of the limitations of traditional systems by providing energy-efficient, cost-effective, and flexible solutions. Their development continues to evolve, with new technologies and prototypes in the literature, aiming to expand their capabilities and improve performance across diverse operating environments. This ongoing research is critical to addressing the growing demand for smart metering solutions in both developed and developing regions, particularly where infrastructure limitations hinder the widespread adoption of conventional devices.

2.1.2. Current and Future Directions

Being electricity ubiquitous across society, the need for electricity meters in all spots where human beings may be is undeniable. Therefore, their significance leaves a lasting impact, both in the present and for the future. This topic could be the subject of extensive discussion, especially when considering the non-stopping transformation society is—was and will—be suffering towards greater connectivity.

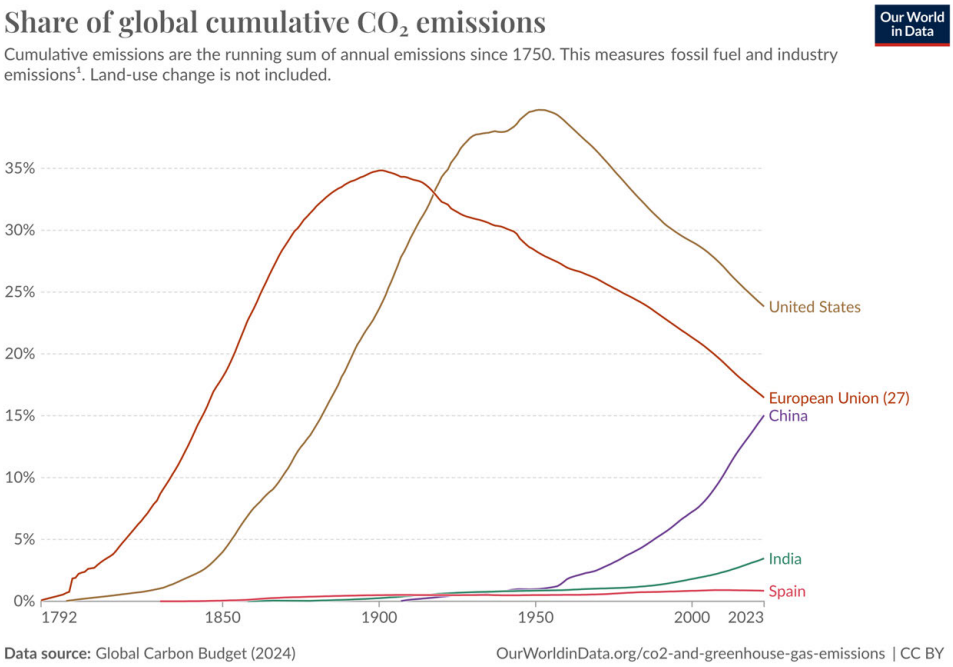


Figure 5. Overview on global CO2 emissions [Ritchie 2020].

Yet, given the increasing consciousness for efficiency and sustainability—at least in certain parts of the globe (Figure 4)—exploring the current and future directions of smart meter technology could be essential for meeting both regulatory requirements and well-being expectations, ultimately helping drive the evolution of energy management systems.

The impact of smart metering extends beyond energy management. By enabling precise, real-time monitoring, these devices contribute to the development of smart grids and support initiatives such as demand response policies, where energy consumption is adjusted dynamically based on supply conditions. In emerging economies, the deployment of low-cost smart meters facilitates equitable energy distribution, reduces theft, and enhances billing accuracy.

Despite these advancements, smart metering keeps on facing persistent challenges. Achieving consistent energy autonomy in diverse environmental conditions remains a critical goal, as does

enhancing the security of communication protocols to protect against cyber threats. Additionally, the scalability of smart meter networks in heterogeneous environments demands further research to address issues such as signal interference, network congestion, and data integrity.

Future research shall explore hybrid energy harvesting systems that combine multiple techniques to optimize energy availability. The integration of machine learning algorithms for predictive analytics and anomaly detection could further enhance the capabilities of smart metering systems. Finally, developing standardized frameworks for interoperability across IoT platforms and protocols will be essential for ensuring the widespread adoption and impact of smart metering technologies.

2.2. Energy Harvesting

As IoT technology advances, the reliance on batteries to power devices presents a significant challenge, particularly in remote or hard-to-access environments where replacing or recharging batteries is logistically and economically unfeasible. To address this, energy harvesting technologies have emerged as a pivotal solution, enabling IoT devices to generate power autonomously from ambient energy sources. These technologies utilize already-existing energy flows such as solar radiation, temperature gradients, mechanical vibrations, and radio frequency (RF) signals to sustain device operations without the need for traditional power sources.

The integration of energy harvesting with wireless communication protocols is at the core of this thesis, as it enables the development of self-sustaining IoT systems capable of functioning independently over extended periods. By leveraging diverse energy harvesting mechanisms, this research seeks to tailor solutions for applications ranging from environmental monitoring to industrial automation, where reliable power supply is critical.

To ensure energy harvesting systems meet the demands of IoT applications, this research examines advanced power management techniques. These include the use of energy storage systems such as rechargeable batteries or supercapacitors to buffer harvested energy and the optimization of communication protocols to reduce power consumption. By aligning energy harvesting technologies with efficient data transmission methods, the goal is to enhance both the reliability and sustainability of IoT deployments.

2.2.1. Modern IoT *Will* Need Energy Harvesting

IoT devices are predominantly wireless, often deployed in environments ranging from urban centers and industrial complexes to rural and remote areas. Many of these deployments necessitate prolonged operation without physical intervention, making traditional power sources such as batteries unsuitable. The periodic replacement of batteries in large-scale IoT networks poses a logistical and financial burden, often exceeding the cost of the devices themselves. Moreover, the environmental impact of battery disposal contributes to the growing issue of electronic waste.

Energy harvesting technologies address these limitations by offering devices the capability to generate power directly from ambient sources. This autonomy significantly reduces maintenance requirements, enabling IoT systems to operate reliably in challenging conditions. Furthermore, energy harvesting aligns with the principles of green technology by minimizing the reliance on non-renewable resources and fostering the development of sustainable IoT ecosystems.

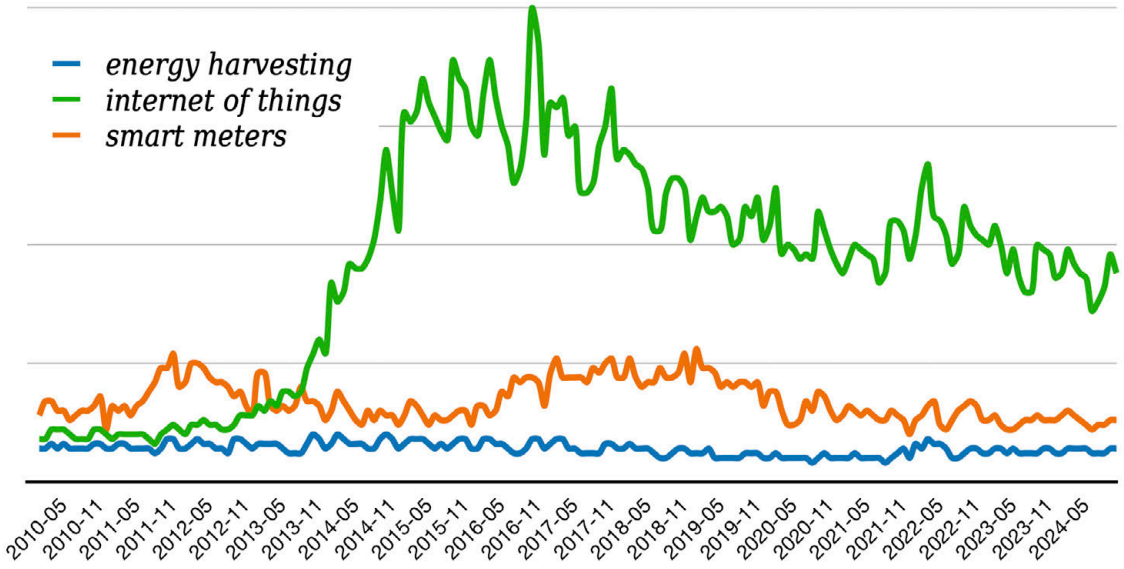


Figure 6. Google Trends for 'energy harvesting', 'internet of things', 'smart meters'; period 2010-2024

The integration of EH technologies with low-power communication protocols, advanced energy storage solutions, and optimized system architectures is critical to unlocking their full potential. By tailoring energy harvesting mechanisms to the specific demands of IoT applications, this research seeks to enhance the efficiency, reliability, and scalability of these systems, ensuring their suitability for both current and future applications.

2.2.2. Specific Energy Harvesting Techniques

This subsection delves into specific energy harvesting technologies, be they photovoltaic, magnetic induction and radio-frequency, as they present the most suitable sources for IoT use cases, and they are the ones that best fitted during this research development. Each of them offers unique advantages and challenges in powering IoT devices. Yet, by understanding the interplay between these energy sources and IoT system requirements, the aim is to unlock innovative solutions for sustainable IoT applications.

Photovoltaic

Solar energy harvesting is one of the most extensively utilized methods for powering IoT devices, particularly in outdoor environments. Photovoltaic (PV) cells convert sunlight into electrical energy, making them ideal for applications such as agricultural monitoring, environmental sensors, and smart city infrastructure. The abundance of sunlight and the mature technology behind PV systems make solar energy a reliable source for IoT devices deployed in open areas where light availability is high.

Outdoor

Outdoor PV systems are ideally suited for applications such as agricultural monitoring, environmental sensing, and smart city infrastructure. The abundance of sunlight in outdoor environments enables high energy generation, with state-of-the-art PV cells achieving efficiencies of up to 40% under ideal conditions. These systems often incorporate energy storage elements, such as lithium-ion batteries or supercapacitors, to store excess energy during peak sunlight hours. This stored

energy ensures uninterrupted operation during periods of low irradiance, such as nighttime or overcast conditions.

Indoor

Indoor PV systems face distinct challenges due to lower light intensities and intermittent artificial lighting. However, advancements in materials and cell design have significantly improved the efficiency of PV systems under these conditions. Compact PV cells, typically measuring around 30 cm^2, achieve conversion efficiencies of 9% under fluorescent lighting at 100 lux. New-generation materials, such as gallium arsenide (GaAs) and organic photovoltaics (OPVs), offer even higher efficiencies, with GaAs cells capable of powering devices with energy requirements up to 10 mW in low-light environments.

However, the variability of solar energy presents a significant challenge to device stability. Factors such as time of day, weather conditions, and geographic location cause fluctuations in solar intensity, potentially disrupting the power supply for IoT devices. This thesis explores the use of advanced energy storage solutions, such as lithium-ion batteries or supercapacitors, to store excess solar energy during periods of high intensity, ensuring uninterrupted operation during low-light conditions.

In addition to energy storage, the integration of photovoltaic systems with energy-efficient communication protocols is critical. By employing low-power wireless technologies, such as LoRaWAN or Zigbee, the overall energy demand of IoT devices is reduced, enabling extended autonomy even in environments with inconsistent sunlight. This approach balances energy generation and consumption, ensuring that devices remain operational in diverse environmental conditions.

Magnetic Induction

Magnetic induction is a widely employed energy harvesting technique that leverages the principles of electromagnetic induction to generate electrical energy from varying magnetic fields. This phenomenon, described by Faraday’s law of electromagnetic induction, occurs when a conductor is exposed to a changing magnetic flux, inducing an electric current. In the context of IoT, magnetic induction serves as a robust and efficient method for harvesting energy, particularly in environments where magnetic fields are naturally present or generated, such as in power systems and industrial applications.

One notable implementation of magnetic induction for energy harvesting is through current transformers (CTs), commonly used in smart meters to measure electrical current. CTs function by coupling energy from the magnetic field surrounding a conductor carrying an alternating current (AC). The magnetic flux generated by the AC flow induces a proportional voltage in the transformer’s secondary winding, which can then be used to power the associated circuitry of the meter or other IoT devices. This approach is particularly advantageous in smart meters, as it allows the device to draw energy passively from the same power line it monitors, eliminating the need for an external power source.

The integration of magnetic induction in smart meters not only supports energy-efficient operation but also facilitates continuous, real-time monitoring of electricity usage. This capability is critical for modern power grids, enabling advanced features such as demand response, dynamic pricing, and anomaly detection. Additionally, this method ensures minimal disruption to the electrical network, as CTs can be installed non-invasively around conductors without requiring physical disconnection or modification of the power lines.

This research explores magnetic induction-based energy harvesting as the source for IoT applications, also considering the challenges of scaling this technology, particularly in scenarios with fluctuating current levels or low-power environments, to further expand its potential applications in the IoT ecosystem.

Radio-Frequency

RF energy harvesting is a promising technology that captures electromagnetic waves from ambient sources like Wi-Fi, cellular signals, or broadcast radio. These signals are ubiquitous in urban and indoor environments, providing a near-constant source of energy for low-power IoT devices. RF harvesting is particularly useful in scenarios where physical access to devices is limited, such as smart homes, healthcare monitoring, or densely populated urban areas.

This thesis examines the feasibility of RF energy harvesting for powering IoT devices, focusing on its advantages in communication-dense settings. RF harvesting is well-suited for devices with minimal energy requirements, such as passive sensors or small-scale actuators. By utilizing ambient RF signals, IoT systems can achieve extended operational lifespans without the need for battery replacements or recharging.

A critical aspect of RF energy harvesting is the integration of highly efficient communication protocols that minimize power demands. Protocols like NB-IoT or BLE, which prioritize energy efficiency, are explored in conjunction with RF systems to ensure that harvested energy supports reliable data transmission. This approach enables IoT devices to remain operational even in environments with fluctuating RF signal strength.

While RF harvesting shows great promise, challenges such as low power density and interference from competing signals must be addressed. This research investigates strategies to optimize energy capture and mitigate these issues, paving the way for the practical deployment of RF-powered IoT devices in a wide range of applications.

Other Techniques

As IoT expands into increasingly diverse and demanding environments, traditional energy harvesting techniques, while effective, are sometimes insufficient to meet the growing requirements for efficiency, adaptability, and sustainability. To address these challenges, incipient energy harvesting techniques are emerging as innovative solutions capable of harnessing unconventional or untapped energy sources. These methods aim to complement or enhance existing energy harvesting technologies, offering greater versatility and opening new possibilities for self-sustaining IoT systems.

Triboelectricity

One promising area of exploration is triboelectric energy harvesting, which leverages the triboelectric effect to generate electricity from contact and separation between materials with differing electrical charges. This technique is particularly suitable for dynamic environments, such as wearable devices, where regular physical interaction can produce usable energy. Triboelectric systems are being studied for their potential to generate power in scenarios like human motion, textile friction, or mechanical vibrations, offering a scalable and environmentally friendly alternative for powering IoT devices in motion-rich settings. Advances in nanomaterial coatings and flexible substrates further enhance the efficiency and adaptability of these systems. [Zhu 2012; Wang 2014].

Bioenergy

Another burgeoning field is bioenergy harvesting, which explores the use of biological processes or organic materials to produce energy. Microbial fuel cells (MFCs), for example, utilize bacteria to convert organic matter into electricity, presenting an exciting opportunity for powering IoT devices in agricultural, environmental, or wastewater management contexts. Similarly, bio-piezoelectric systems harness the natural mechanical properties of biological materials, such as collagen or bone, to generate electricity in applications where biological integration is key. Energy derived from human metabolic processes, including heat, glucose, or motion, is also being researched for wearable IoT devices, particularly in healthcare, offering a harmonious interface between technology and the human body. [Logan 2012, 2012].

Quantum

Lastly, quantum energy harvesting represents a futuristic frontier in energy research. Quantum phenomena such as zero-point energy, thermoelectric quantum dots, and tunneling effects offer theoretical possibilities for ultra-efficient energy generation. While still experimental, quantum energy harvesting could revolutionize IoT power solutions by enabling devices to operate at micro- and nanoscale levels with minimal environmental impact. Similarly, kinetic microfluidic systems, which use the movement of liquid within small-scale channels to generate electricity, are being studied for their potential to power IoT devices in biomedical or environmental monitoring scenarios, leveraging natural fluid flows in compact environments. [Sothmann 2015; Thierschmann 2015; Hildebrandt 2017; Mitchison 2019]

2.2.3. Realizing Harvested Energy

Energy harvesting has been a trending topic during the last years, becoming a feasible solution when very-low-power electronic devices were achievable—from the 2010s. Providing energy harvesting capability to wireless devices enables them to continuously acquire energy, therefore eliminating the concern of their lifetime being dependent on the energy storage system capacity [Gunathilaka 2012; Ulukus 2015]. Nonetheless, achieving this integration still presents several challenges and making strategic trade-offs to balance energy availability, conversion, and utilization, as every new application may require a different approach in its energy harvesting system design. As exemplification, **Figure 7** depicts the circuit blocks that conformed the EH subsystem developed to make the smart meter from Section 1.1 hereof perform.

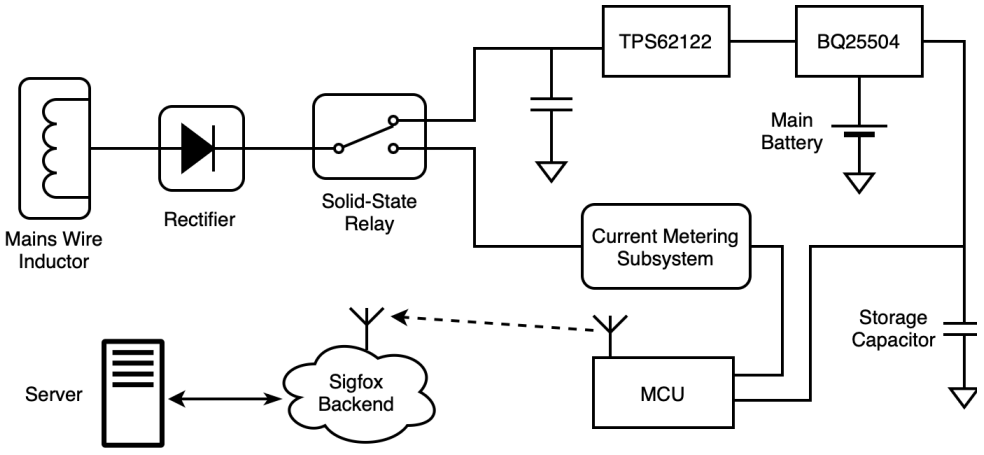


Figure 7. High-level schematic of the smart meter's EH subsystem.

One of the most critical challenges is the variability and intermittency of ambient energy sources, which directly impacts the reliability and performance of IoT devices. For instance, solar energy fluctuates with weather and daylight, thermal gradients may vary with operational conditions, and mechanical vibrations depend on specific environmental activities. This inherent unpredictability necessitates the development of robust strategies to manage energy availability effectively.

To address these issues, researchers are focusing on advanced power management algorithms that dynamically optimize the device's operation based on real-time energy availability. These algorithms monitor the energy harvesting input and adjust the device's functionality to prioritize critical tasks while deferring non-essential or energy-intensive operations during periods of low energy. For example, an environmental monitoring sensor might reduce its sampling rate or delay data transmission until sufficient energy is available. These dynamic adjustments not only improve the reliability of IoT devices but also ensure optimal utilization of the harvested energy, extending device operational lifespans even under fluctuating conditions.

Another significant challenge lies in the efficiency of energy conversion and storage systems. Ambient energy sources typically provide low power, often in the milliwatt or microwatt range, necessitating highly efficient energy conversion mechanisms to maximize the usable power. For instance, thermoelectric generators must efficiently convert thermal gradients into electricity while minimizing losses, and piezoelectric systems must effectively capture and convert kinetic energy from vibrations. Innovations in materials science, such as the use of nanostructured materials or advanced semiconductors, are driving improvements in conversion efficiency, enabling greater energy yield from limited sources.

Equally important are advancements in energy storage technologies, which play a crucial role in maintaining a consistent power supply for IoT devices. Supercapacitors, with their rapid charge-discharge cycles and high durability, are increasingly being used to buffer short-term energy variations. Meanwhile, rechargeable batteries with high energy density and low self-discharge rates are employed to store larger amounts of energy for long-term use. Research is also exploring hybrid storage solutions that combine the strengths of supercapacitors and batteries, providing both immediate power delivery and sustained energy reserves. By integrating these advanced storage solutions with energy harvesting systems, IoT devices can achieve a higher degree of autonomy and resilience, even in energy-scarce environments.

In conclusion, the exploitation of energy harvesting for IoT devices requires a holistic approach that addresses the interplay between energy sources, conversion efficiency, storage solutions, and power management. By tackling these challenges, this research aims to unlock the full potential of energy harvesting, enabling IoT systems that are not only self-sustaining but also adaptable to diverse and dynamic environmental conditions. This integration is a cornerstone of future IoT deployments, fostering innovation in areas such as smart cities, industrial automation, and environmental conservation.

2.3. Wireless Communications

Since the IoT has been established as one of the most acknowledged paradigms, the amount of related research and emerging technologies and services [Evans 2021; Wegner 2021] has increased, both regarding IoT devices themselves—35 billion ($\times 10^9$) devices connected in 2021

[Maayan 2020] and 75 billion devices expected by 2025 [Newman 2019]—, yet also monetary spending—more than EUR 1200 billion by 2027*.

The wireless paradigm for IoT allows medium and large coverage areas with relatively low energy consumption by providing small processing power requirements for devices as well as low transmission data rates [S. Farrell 2018; Chaudhari 2020], factors inherent in the IoT field itself. Focusing on this thesis' domain, **Table 1** shows detailed energy consumption for the smart meter use case, as it was profoundly carried out and further explained in one of this thesis' compendium papers [Saavedra 2021].

Table 1. Energy consumption† of a message transmission for different IoT wireless technologies within the smart meter use case.

Technology	MTC ‡ (mA)	ETC § (mA)	Establishment Consumption (mAs)	Transmission Consumption (mAs)	Total Consumption (mAs)
Sigfox	<59,4	53,1	0	804,80	804,80
LoRaWAN	<59,4	62,5	256,73	6,33	263,06
NB-IoT	<277,2	141,2	4.341,9	8,88	4.350,8
Wi-Fi	118,8	109,9	198,46	3,40	201,86
BLE	85,8	95,9	51,98	1,01	52,99

Despite the wide variety in wireless IoT technologies, some actors widely dominate the current picture of IoT communications, although this has always depended on the specific use case. Medium-range communications such as Bluetooth and Zigbee may have ac-counted for up to 28% of the wireless IoT chips in 2021. For long-range communications technologies, only four accounted for over 96% of global, installed active devices in 2021: NB-IoT, LoRa, LTE-M and Sigfox. NB-IoT leads this ranking with 47% of the global share, followed by LoRa with 36% [Pasqua 2021]. In fact, low-power wide-area network (LPWAN) protocols that rely on licensed bands (NB-IoT, LTE-M) have surpassed those relying on non-licensed ones (LoRa, Sigfox) in 2021**.

However, different technologies provide different levels of performance and need different infrastructure requirements. Choosing one over another widely depends on the specific use case and it is not always clear how to compare their performance. The very specific use case will set the requirements for wireless technology. Requirements may be divided into technical factors (data rate, latency, range), implementation factors (cost, documentation, available coverage) and functional factors (energy consumption, location services, over-the-air upgrade) [Al-Kashoash 2016; Hedi 2017; Moraes 2019; del Campo 2020]. **Table 2** presents a comprehensive, coarse approach thereof.

* Fortune Business Insights. https://www.fortunebusinessinsights.com
† Energy consumption values are shown in milliampere-second (*mAs*) for ease of reading.
‡ MTC stands for *Manufacturer* Transmission Current, which is the maximum current consumption during transmission that the manufacturer claims in the datasheet—normalized to a 5 V DC power supply.
§ ETC stands for *Experimental* Transmission Current, which is the current consumption measured in the laboratory during transmission—also at 5 V.
** IoT Analytics 2021. https://iot-analytics.com/number-connected-iot-devices

Table 2. Summary of IoT wireless technologies' features.

Technology	Data rate[1]	Latency[2]	Range[3]	Duplex	Reliability	Consumption	Cost
BLE	Mbps	30 ms	100 m	half	low	low	low
ZigBee	kbps	40 ms	100 m	half	high	low	low
WiFi	Mbps	30 ms	100 m	half	med	med	low
WirelessHart	kbps	10 ms	200 m	half	high	med	high
LoRaWAN	kbps	300 ms	10 km	half	med	med	med
Sigfox	bps	4 s	50 km	limited[4]	high	high	med
6LoWPAN	kbps	20 ms	100 m	half	med	low	low
NB-IoT	kbps	2 s	10 km	half	high	high	high
LTE Cat-M1	kbps	2 s	10 km	half	high	high	high
5G	Gbps	10 ms	10 km	half	high	high	high

[1,2,3] Approximate values—in the order of magnitude.
[4] Sigfox provides limited bidirectional capacity: the IoT device can upload up to 140 12-byte messages a day, but it can only receive four 8-byte messages.

The literature offers resources aimed to evaluate and compare specific IoT characteristics, though they often focus on a limited subset of IoT technologies. For example, [Pereira 2017] present an experimental characterization of mobile IoT latency, while [Mroue 2018] analyze LoRa, Sigfox, and NB-IoT using a MAC layer-based approach. Furthermore, comprehensive studies targeting specific IoT technologies also exist, covering a broad range of aspects. Examples include this survey on LoRa and NB-IoT [Sinha 2017], as well as [Alsukayti 2020], which examines quality, transmission range, power consumption, and data rates across various scenarios and technologies. In addition, other studies address challenges related to achieving low-latency or high-reliability IoT communication networks, as seen in [Schulz 2017; Ma 2019; Atutxa 2021].

However, there remains a lack of research focused on a universal, ubiquitous approach. This gap likely stems from the immense diversity of the IoT field. This issue is tackled in [Hossain 2017] by proposing a large-scale IoT testbed-as-a-service. Developing testbeds capable of integrating diverse systems, interfaces, and technologies is challenging but necessary for a domain with growing complexity and prevalence. This need is emphasized [Rana 2021], where the authors highlight the interoperability issues among IoT platforms and devices.

Hereon, the most relevant technologies for this thesis development are briefly presented to the reader. These technologies are selected due to their being the most common, commercially available ones for IoT devices—both in residential and industrial scenarios.

6LoWPAN

6LoWPAN is a transformative technology that bridges the gap between the vast ecosystem of the Internet and the world of resource-constrained devices. Based on the IEEE 802.15.4 standard, 6LoWPAN enables the efficient communication of IPv6 packets over low-power networks, ensuring seamless integration with existing Internet infrastructures. This is achieved through mechanisms like header compression and packet fragmentation, which reduce the size of IPv6 packets to fit the limited payload of low-power wireless links. Furthermore, the protocol supports mesh networking, allowing multi-hop communications that extend the range and flexibility of deployments.

The significance of 6LoWPAN lies in its ability to bring the benefits of IPv6—such as a virtually unlimited address space and enhanced security—to IoT devices, enabling scalable and interoperable solutions. This makes 6LoWPAN a key enabler in smart home automation, industrial IoT, and environmental monitoring, where the need to connect vast numbers of small, battery-powered devices is paramount. By lowering the barriers to integrating low-power devices into IP-based networks,

6LoWPAN sets the stage for a truly interconnected IoT ecosystem. [Gee 2010; Jiménez 2016; Al-Kashoash 2016; del Campo 2018; Yang 2019; Al-Amiedy 2022].

Bluetooth—Low Energy

Bluetooth Low Energy (BLE) is a widely adopted technology that addresses the need for short-range, energy-efficient wireless communication. It is designed for applications requiring minimal power consumption, such as wearable devices, healthcare monitoring systems, and smart home solutions. BLE operates using advertising and scanning mechanisms, where devices broadcast small data packets over specific channels, and nearby devices listen for these packets to initiate connections. With a typical connection range of up to 100 meters and data rates ranging from 125 kbps to 2 Mbps, BLE offers flexibility for diverse use cases while maintaining a compact and cost-effective implementation.

BLE network topology supports both star and mesh configurations, enhancing its versatility in IoT systems. Its connection setup time is optimized to be quick, though it can vary depending on the network's density and advertising intervals. This capability makes BLE an ideal choice for scenarios where rapid interactions and energy conservation are critical. Furthermore, the technology's low cost and widespread adoption ensure that it remains a cornerstone for developing innovative IoT applications across industries such as fitness, healthcare, and entertainment. [Gregori 2002; Duflot 2006; Drula 2007; Cho 2014].

Cellular: NB-IoT & LTE-M

Cellular IoT technologies such as Narrowband IoT (NB-IoT) and LTE-M have emerged to address the unique requirements of IoT applications by building on the extensive global LTE infrastructure. Unlike conventional cellular networks, which were originally designed for high-speed data transmission, NB-IoT and LTE-M optimize connectivity for low-power devices that require infrequent, small-packet data exchanges. NB-IoT, for instance, operates on a narrowband spectrum, providing deep indoor coverage and supporting devices with ultra-low data rates. LTE-M, on the other hand, offers slightly higher data rates while maintaining energy efficiency, making it suitable for use cases like asset tracking and connected wearables.

Both technologies have made cellular connectivity more accessible to the IoT market by reducing device complexity, power consumption, and costs. NB-IoT's ability to use narrowband carriers within LTE or GSM frequencies simplifies deployment and enhances compatibility. Meanwhile, LTE-M's reliance on standard LTE bands ensures seamless integration with existing cellular networks. Together, these technologies enable scalable and secure IoT applications, with Spain achieving near-total population coverage for NB-IoT by 2024, highlighting the widespread adoption and potential of cellular IoT solutions. [Ratasuk 2016, 2016; Beyene 2017; Salva-Garcia 2018; Ayoub 2019; Jia 2019; Sánchez 2019; Gbadamosi 2020].

Sigfox

Sigfox represents a minimalist yet highly effective approach to IoT connectivity, focusing on simplicity and energy efficiency. The technology operates on ultra-narrowband (UNB) radio modulation, which allows devices to transmit small amounts of data reliably over long distances while avoiding interference. Unlike traditional networks, Sigfox does not require devices to establish or maintain a continuous connection. Instead, devices send messages directly to the network using a

lightweight protocol, and these messages are received by multiple base stations, implementing spatial diversity to enhance reliability.

Sigfox is tailored for applications where uplink communication is prioritized, such as sensor networks for environmental monitoring, utility metering, or asset tracking. The protocol's bidirectional capabilities are limited, allowing only a few downlink messages per day, but this trade-off ensures ultra-low power consumption and extended battery life for devices. With its managed network infrastructure and global reach, Sigfox simplifies IoT deployments by eliminating the need for complex network configurations, making it an attractive option for massive-scale, low-bandwidth IoT applications. [Gomez 2019; Lavric 2019, 2019; DeutscheTelekom 2021; Putra 2022].

LoRaWAN

LoRaWAN is a flexible and scalable wireless communication protocol that operates on the LoRa modulation technique. Its network architecture employs a star-of-stars topology, where gateways relay data between end devices and a central server. LoRaWAN is known for its long-range capabilities, with devices communicating over distances of several kilometers using the 868 MHz ISM band. Its adaptive data rate mechanism optimizes network performance by adjusting the data rate and transmission power based on signal quality, ensuring efficient use of energy and bandwidth.

LoRaWAN's appeal lies in its openness and community-driven development. While there is no commercial LoRaWAN network in Spain, public initiatives like The Things Network enable individuals and organizations to deploy their own gateways and participate in a shared infrastructure. The protocol supports data rates from 250 bps to 50 kbps, catering to a range of IoT applications from simple environmental sensors to more complex industrial automation systems. With end-to-end AES encryption, LoRaWAN ensures secure communications, making it a compelling choice for privacy-conscious IoT deployments in smart cities, agriculture, and beyond. [de Carvalho 2017; Haxhibeqiri 2018; Ayoub 2019; Ertürk 2019; Alenezi 2020; Mane 2021].

Zigbee

Zigbee is a well-established low-power, low-data-rate wireless communication protocol designed for simple, reliable, and secure communication over short distances. Built on the IEEE 802.15.4 standard, Zigbee excels in creating mesh networks, allowing devices to route data through multiple nodes and ensuring robust connectivity in dynamic environments. This capability makes it ideal for smart home applications, industrial automation, and healthcare systems, where the network must adapt to changing conditions or node failures.

One of Zigbee's strengths is its interoperability through adherence to the Zigbee Alliance standards, which define device communication profiles. Zigbee's ability to support thousands of nodes within a single network, combined with its low energy consumption, makes it particularly suitable for large-scale IoT deployments. However, its limited data rate of up to 250 kbps restricts its use to applications where bandwidth demands are minimal, such as sensor monitoring and basic control systems. Despite this, Zigbee's maturity, extensive ecosystem, and wide adoption make it a cornerstone technology for IoT development. [Ergen 2004; Pan 2007; Farahani 2011; Ramya 2011, 2011; Alobaidy 2020; Zohourian 2023].

Wi-Fi

Wi-Fi is perhaps the most ubiquitous wireless technology, providing high-speed communication for devices in a wide range of environments. While traditionally focused on high-bandwidth applications like video streaming and internet access, recent advancements such as Wi-Fi HaLow (IEEE 802.11ah) and Wi-Fi 6 (802.11ax) have expanded its capabilities to support IoT use cases. Wi-Fi HaLow, for instance, operates in the sub-GHz spectrum, offering extended range and lower power consumption, which are critical for IoT sensors and devices.

Despite its advantages in speed and widespread availability, Wi-Fi's high-power consumption compared to other IoT-focused protocols can be a limitation for battery-operated devices. However, its robust infrastructure, ease of deployment, and ability to support large amounts of data make Wi-Fi indispensable for applications where power is less of a concern, such as video surveillance, industrial IoT, and smart appliances. With the emergence of IoT-specific optimizations, Wi-Fi continues to play a vital role in enabling connectivity for both consumer and industrial applications. [Tozlu 2012; Camps-Mur 2013; Khairy 2019; Chen 2021].

Thread*

Thread is a relatively new wireless protocol that also builds on the IEEE 802.15.4 standard, but with a focus on IPv6 support and enhanced security. Unlike Zigbee, Thread employs 6LoWPAN to enable direct IP communication, eliminating the need for a proprietary application layer and fostering seamless integration with other Internet-connected systems. Thread networks are inherently mesh-based, self-healing, and scalable, with no single point of failure, making them robust and efficient for smart home and building automation.

Thread's key advantage lies in its low-latency, low-power operation, allowing devices to remain operational for extended periods without frequent battery replacement. It is designed to coexist with other wireless technologies, minimizing interference in environments where multiple protocols operate simultaneously. The protocol's adoption by the Connected Home over IP (CHIP) initiative, now branded as Matter, further solidifies Thread's role as a foundational technology for future smart home ecosystems, ensuring interoperability and future-proof connectivity. [Unwala 2018a, 2018b; Rzepecki 2019].

2.4. Interoperability

Interoperability is a cornerstone of the Internet of Things (IoT), as it enables seamless communication and integration across diverse devices, platforms, and networks. However, achieving interoperability is a persistent challenge, given the heterogeneity of IoT devices, the coexistence of legacy systems, and the multiplicity of communication protocols. This section explores key advancements in IoT interoperability, with a focus on bridging the divide between incompatible networks and achieving cohesive systems.

* It is worth noting that Thread is not further analyzed in the compendium papers of this thesis. This is primarily due to the absence of a finalized Matter standard during the early years of this investigation. Nonetheless, given its shared foundations with 6LoWPAN and Zigbee, Thread is expected to demonstrate similar performance figures.

Challenges of Interoperability in IoT

The IoT landscape is characterized by a vast array of devices, each operating on different communication standards, protocols, and architectures. This heterogeneity complicates integration efforts, particularly in large-scale deployments where devices from multiple manufacturers must coexist. For instance, the widespread adoption of IPv6 in modern IoT devices contrasts with the dominance of IPv4 in legacy networks, creating barriers to seamless communication. [Ziegler 2013; Jara 2013; Hyun 2015].

This divide is further exacerbated by proprietary platforms and protocols, which hinder cross-vendor compatibility. IoT manufacturers often design systems that are optimized for specific applications but lack the flexibility to interface with third-party devices or platforms. Consequently, these silos limit the scalability and usability of IoT ecosystems. [Grosse 2003; Samad 2018; Kumar 2018]

Bridging IPv4 and IPv6 Networks

One of the most critical challenges in IoT interoperability is bridging the gap between IPv4 and IPv6 networks. IPv6 offers significant advantages, including a vastly expanded address space and enhanced support for mobile and IoT devices. However, the transition to IPv6 has been slow, with many networks and devices still reliant on IPv4 infrastructure. This coexistence presents a major obstacle to unified IoT systems. [Sabir 2009; Savolainen 2013; Lencse 2018, 2019; Ghumman 2019].

Aiming to fade this structural gap, this thesis presents a novel and simple solution to connect and expose data from IPv6-based IoT sensors to the legacy, IPv4-based Internet. This solution is deeply described in [Saavedra 2024], yet a coarse scheme thereof can be depicted in **Figure 8**.

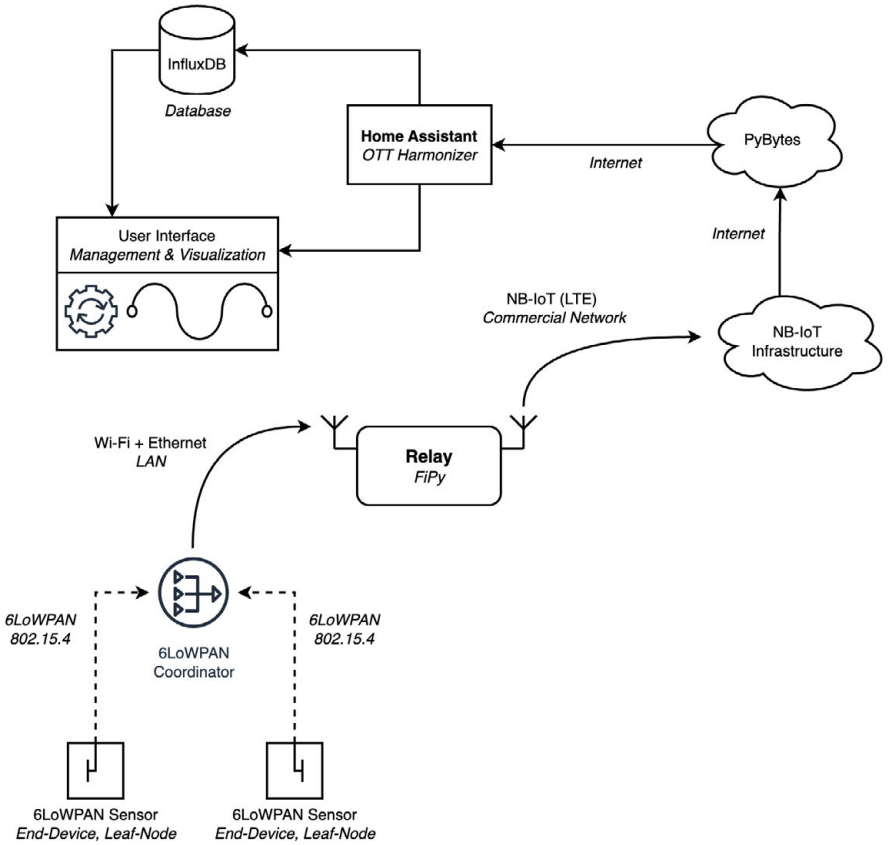


Figure 8. General diagram of the solution presented in [Saavedra 2024].

Harmonizing Protocols and Standards

IoT systems employ a wide range of communication protocols, each tailored to specific use cases and performance requirements. For instance, low-power wide-area network (LPWAN) protocols such as Sigfox and LoRaWAN are optimized for long-range, low-bandwidth communication, while protocols like BLE and Zigbee are better suited for short-range, high-density networks. The diversity of these protocols creates significant challenges in achieving seamless interoperability. Efforts to harmonize protocols have included the development of gateways and middleware solutions that abstract protocol-specific details within certain boundaries and applications. [Grosse 2003; Arzo 2021; Kitamura, H.].

Proof of IoT wireless communications great diversity is properly explained in [Saavedra 2022]. In this thesis' compendium paper, key differences among IoT wireless technologies are faced and normalized to some extent. **Figure 9** depicts this enormous variety issue and its coming with strings attached, to the point that a novel, normalized definition for *latency*—which is such a basic communications concept—had to be settle, aiming for a common framework in which different wireless technologies—which may have distinct components, routes, architectures—could be properly compared.

> **Latency:** *The time a message takes from the moment when the transmitting device is called to send a message until this message is ready for utilisation at the other end (user-side).*

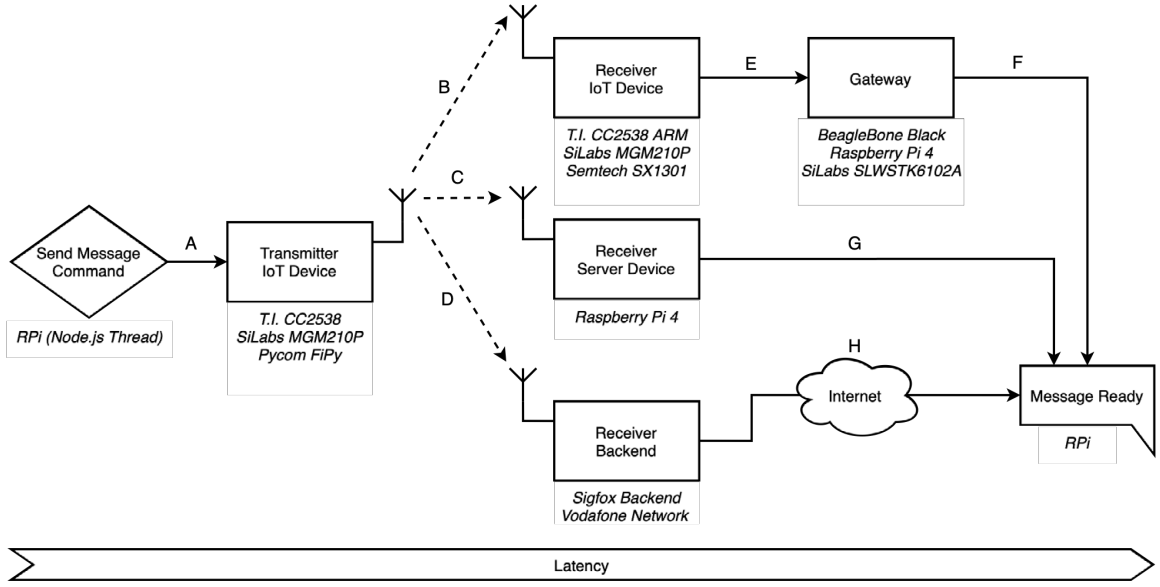


Figure 9. *Latency*: abstract definition and message paths for different wireless IoT topologies. Paths are, for i) 6LoWPAN, Zigbee, LoRaWAN; ii) Sigfox, NB-IoT; iii) Wi-Fi, BLE; as follows: i) A-B-E-F; ii) A-D-H; iii) A-C-G.

Interoperability Through Open Platforms

The growing number of IoT devices connected also means more players in the ground, therefore more manufacturers, service providers and third-party platforms. To make IoT devices interoperable, overlaying platforms must be able to *speak* one another, and open-source initiatives realize as the only ones capable of such a tough task. The role of the open-source community in fostering IoT interoperability and breaking access barriers cannot be overstated.

Should one harmonizer-platform be highlighted, this is Home Assistant, which provides a centralized interface for managing and integrating IoT devices from thousands of different vendors and devices (only rising), with a great community of developers and users aiming to improve and enjoy the platform. These kinds of platforms enable users to seamlessly connect and control devices—that might otherwise be incompatible—by abstracting device-specific complexities, presenting all of them in a systematic, structured manner. [Cujilema 2023].

Emerging Solutions for IoT Interoperability

As IoT systems continue to evolve, new approaches to interoperability are emerging. One promising avenue is the adoption of semantic interoperability frameworks, which use standardized data models to enable meaningful data exchange between devices and platforms. These frameworks ensure that data generated by one device can be correctly interpreted and utilized by another, regardless of differences in their underlying architectures. [Rana 2021; Del Campo 2024]

In addition, advances in edge computing and AI-driven middleware offer the potential to dynamically adapt and translate protocols in real time, further reducing the barriers to integration. For example, edge devices equipped with protocol translation capabilities can act as intermediaries between incompatible networks, ensuring seamless data flow without requiring centralized processing. [Tandon 2016]

Applications and Broader Implications

The benefits of interoperability extend far beyond individual IoT deployments. In the context of smart cities, for example, interoperable IoT systems enable the integration of transportation, energy, and public safety networks, creating a cohesive urban infrastructure. Similarly, in industrial IoT (IIoT), seamless communication between machines, sensors, and control systems enhances operational efficiency and reduces downtime.

Moreover, achieving interoperability is essential for the scalability of IoT ecosystems. As the number of connected devices continues to grow, standardized frameworks and interoperable technologies will be critical to managing the complexity of large-scale networks. The development of universal testbeds and open-source platforms represents a significant step toward this goal, providing the tools and frameworks necessary for widespread adoption.

Future Directions

Despite these advancements, significant challenges remain. The lack of universally accepted standards for IoT protocols and architectures continues to hinder interoperability efforts. Security and privacy concerns also complicate integration, as ensuring the safe exchange of data across heterogeneous systems requires robust encryption and authentication mechanisms.

Future research should focus on the development of lightweight, scalable solutions for protocol translation and integration. The use of blockchain for decentralized device authentication and trust management is another promising avenue for enhancing security in interoperable systems. Additionally, fostering collaboration between industry stakeholders and standardization bodies will be essential for achieving the global harmonization of IoT protocols and architectures.

2.5. Security & AI

As IoT devices generate vast amounts of data, there is a growing need for real-time data processing and analysis to derive actionable insights. Therefore, this field offers as a perfect fit into the Big Data *cloud*, reason why machine learning and artificial intelligence (AI) are increasingly being integrated into IoT systems to enable predictive analytics, anomaly detection, and autonomous decision-making. These technologies enhance the intelligence of IoT devices, allowing them to learn from data patterns and adapt their behavior accordingly. For instance, AI-powered IoT systems can predict equipment failures in industrial settings, optimize energy consumption in smart buildings, and improve traffic management in smart cities. Although complex AI computation is usually made in the cloud, sometimes smaller calculations are brought to the Edge to reduce latency and spread resources. [Sabir 2009; Lencse 2019].

Data comes along with privacy, so security and privacy remain paramount concerns in the IoT ecosystem. The widespread deployment of IoT devices expands the attack surface for cyber threats, necessitating robust security measures to protect data and ensure the integrity of IoT systems. End-to-end encryption, secure boot mechanisms, and hardware-based security modules are some of the strategies employed to safeguard IoT devices and networks. Additionally, compliance with data privacy regulations, such as the General Data Protection Regulation (GDPR), is crucial to ensure that personal data collected by IoT devices is handled responsibly. There is a number of papers regarding these concerns, such as the research presented in [Anand 2020] and that presented in [Malhotra 2021] which might serve as great references regarding the security challenges in the IoT field. Nevertheless, it is a never-enough research topic considering its pace of growth and its more-than-ever quasi-omnipresent presence in our lives, with more applications and devices emerging constantly.

3. Methodology

This Section of presents the systematic approach taken to address the main matter. This section is crafted to provide a clear and replicable outline of the processes used throughout the thesis, establishing a framework that reflects rigor, consistency, and the structured integration of theory and experimentation.

The foundational approach underpinning each phase of this research has been marked by uniformity and rigor. This consistency extends across all preliminary studies and published papers contributing to the final body of work.

Initial stages involved rigorous theoretical exploration, including literature review and conceptual modeling of energy harvesting techniques suitable for IoT devices. This groundwork established a clear understanding of the various energy sources—such as photovoltaic, radiofrequency, and thermoelectric—examining their feasibility in environments with different energy availability. These insights informed the design of experimental setups that would later validate theoretical assumptions through practical testing.

Experimental phases were characterized by a systematic evaluation of each energy harvesting source in conjunction with wireless communication protocols like NB-IoT, LoRa, Sigfox, and BLE. Each experimental setup was designed to replicate real-world conditions as closely as possible, ensuring that the results would be applicable to actual IoT deployments. Performance metrics, such as energy consumption, latency, throughput, and error rate, were meticulously recorded and analyzed, providing the data necessary to assess the feasibility and efficiency of various protocol and energy source combinations.

In summary, the methodology of this thesis reflects a rigorous approach to IoT research, following a structured, yet natural approach to address the main matter, therefore achieving research objectives. The steps undertaken were as follows:

Phase I – *Research on Energy Harvesting Systems*

Literature Review

This task involves conducting an in-depth analysis of existing energy harvesting (EH) technologies, including photovoltaic, piezoelectric, thermoelectric, and RF harvesting methods. The review will focus on understanding the underlying operational principles, energy conversion efficiencies, and feasibility of these technologies for integration into IoT applications. Additionally, the review aims to identify state-of-the-art advancements, current limitations, and knowledge gaps within the domain, providing a foundation for innovation and targeted research.

Requirements Specification

This phase involves defining the energy requirements of low-power IoT devices across diverse use cases, considering operational scenarios and device functionalities. Evaluation criteria for energy harvesting (EH) systems will be established, emphasizing critical parameters such as power

output, environmental adaptability, and integration feasibility. These criteria will serve as benchmarks to assess the suitability and performance of EH technologies in meeting the specific demands of IoT applications.

Simulation & Design

This stage involves the simulation of identified energy harvesting (EH) systems to model and predict their performance under various environmental conditions, such as light intensity, thermal gradients, or mechanical vibrations. Using these simulations, prototypes of the most promising EH systems will be designed, with a focus on ensuring compatibility with the power requirements and operational constraints of IoT devices. This process will validate theoretical models and guide the development of functional EH solutions tailored to IoT applications.

Experimental Validation

Prototypes of the energy harvesting (EH) systems will be constructed and rigorously tested in controlled environments to evaluate key performance metrics, including energy output, reliability, and efficiency under standardized conditions. Following laboratory validation, the prototypes will be deployed in real-world scenarios to assess their operational feasibility, environmental adaptability, and seamless integration with IoT devices. This phase aims to validate the practical applicability and robustness of the EH systems in diverse operational contexts.

Phase II – *Analysis of Energy Requirements for IoT*

Protocol Selection

This task involves identifying and selecting key IoT communication protocols, such as 6LowPan, LoRaWAN and Sigfox, based on their prevalence, technical specifications, and suitability for low-power IoT applications. Emphasis will be placed on protocols widely utilized in IoT networks that incorporate self-powered devices, ensuring their compatibility with energy harvesting systems and their potential for efficient integration into resource-constrained environments.

Energy Profiling

This phase involves a detailed analysis of the energy consumption characteristics of each selected IoT communication protocol under varying configurations. Key parameters such as message size, transmission frequency, and security settings will be systematically evaluated to quantify their impact on power consumption. Specialized measurement tools and hardware, such as power analyzers and energy monitoring devices, will be employed to capture precise power usage data during communication processes. This profiling will provide critical insights into the energy efficiency of each protocol in the context of self-powered IoT applications.

Optimization

This phase focuses on developing energy-efficient configurations for each selected IoT communication protocol. Adjustments will be made to parameters such as data packet size, transmission intervals, and security protocols to minimize power consumption while preserving optimal perfor-

mance. Simulations will then be conducted to evaluate the behavior of these optimized configurations within self-powered IoT scenarios, ensuring that they meet the operational and energy constraints of devices relying on energy harvesting systems. This process aims to identify the most effective configurations for sustainable and reliable communication.

Experimental Implementation

The selected IoT communication protocols will be deployed on devices powered by energy harvesting systems so as to assess their practical applicability. Performance metrics such as latency, communication reliability, and energy efficiency will be rigorously evaluated under controlled and real-world conditions. This experimental phase aims to identify optimal combinations of protocols and EH techniques, ensuring seamless integration, robust operation, and energy sustainability in self-powered IoT networks.

Phase III – *Developing a Testbed for IoT Networks*

Design of the Testbed Architecture

The architecture of the testbed will be designed systematically to support comprehensive evaluation of IoT networks. This includes specifying the hardware components, such as IoT nodes, probing equipment and the like, as well as developing not only the software that runs the system, but also the software, procedures and hardware characterizing the testbed itself, so that statistically correct data and veracity thereof can be stated. Key performance parameters to be measured will be clearly defined, encompassing latency, error rate and network stability. The design will ensure modularity and scalability to accommodate various IoT technologies and configurations for rigorous testing and evaluation.

Implementation of the Testbed

The testbed will be assembled utilizing modular and scalable hardware components to support flexibility in testing various IoT configurations. Open-source software platforms will be employed to ensure cost-effectiveness and ease of customization. Automation tools will be integrated into the testbed to streamline data collection, processing, and analysis, enabling efficient and consistent evaluation of performance metrics across diverse IoT technologies and scenarios.

Validation and Calibration

Calibration tests will be performed to ensure the precision and reliability of the testbed’s measurement capabilities, with a focus on key parameters such as latency, error rate, stability, and energy consumption. The platform will be rigorously tested across a range of IoT technologies to validate its robustness, adaptability, and versatility. This process will ensure the testbed's effectiveness as a standardized tool for evaluating and comparing IoT systems under various configurations and operational conditions.

Comparative Evaluation

The testbed will be utilized to systematically evaluate and compare the performance of various IoT technologies and configurations, outcoming key performance indicators such as latency, error

rate, stability, and energy consumption. Detailed technical reports will be generated to document the strengths, limitations, and potential applications of each technology, providing actionable insights for the selection and deployment of optimal IoT solutions in energy-constrained environments.

Phase IV – *Integration and Synthesis*

Synthesis of Results

The insights gathered from the evaluation of energy harvesting (EH) systems, analysis of protocol energy consumption, and testbed performance metrics will be integrated. This synthesis will enable the identification of optimal combinations of EH techniques, IoT communication protocols, and configurations that maximize energy efficiency, reliability, and performance. The results will provide a comprehensive framework for designing and deploying self-powered IoT networks tailored to specific operational requirements.

Implementation Guidelines

A detailed set of guidelines will be developed to support the deployment of self-powered IoT networks, customized to meet specific operational requirements. These guidelines will encompass best practices for selecting EH techniques, configuring IoT protocols, and integrating hardware and software components. The recommendations will ensure optimal performance, energy efficiency, and scalability in diverse application scenarios.

Scalability and Future Directions

Evaluate the scalability of the developed solutions by testing their performance and reliability in larger-scale and more heterogeneous IoT deployments. The assessment will focus on maintaining energy efficiency, communication reliability, and operational stability as the network size and complexity increase.

This task also includes the development of a tool for deployment facilitation. This adaptive tool will allow the deployment of IoT networks within existing IPv4-based infrastructures. This tool will bridge compatibility gaps and optimize integration with legacy systems, ensuring seamless operation and efficient resource utilization.

Proposed Enhancements based on experimental results and Future Research will be identified, including advancements in energy harvesting technologies, protocol optimizations, and enhanced interoperability for hybrid network environments.

Phase V – *Reporting, Dissemination*

The research findings shall be disseminated through publication in high-impact, peer-reviewed journals to ensure rigorous evaluation and recognition within the scientific community. Additionally, selected results might be presented at relevant technical conferences, fostering knowledge exchange and contributing to the advancement on the field of self-powered IoT networks and energy-efficient communication technologies.

This methodology ensures a systematic and rigorous approach to addressing the challenges of developing efficient, sustainable, and scalable self-powered IoT networks, ultimately meeting the main and partial objectives of this work.

4. Results

The synthesis of research findings reveals significant insights into the interactions between different energy harvesting sources and communication protocols, each combination offering unique trade-offs and advantages. This integrated approach highlights several critical dimensions for IoT deployment.

4.1. Milestones

The research carried out in this thesis is structured around the three objectives initially proposed. The progress of the research conducted has led to results that have been published throughout the four years of investigation, marking the evolution from the initial theoretical analyses outlined in the methodology to the development and refinement of innovative solutions.

As a result, four main milestones have been achieved, each of which led to a publication in a top-tier (Q1/Q2) scientific journal. The evolution of the work carried out up to the achievement of the publications that constitute the compendium of this thesis is presented below.

Theoretical Analysis

The research began with a theoretical analysis to establish a comprehensive understanding of the technical and practical challenges in deploying autonomous IoT devices. This analysis focused on identifying barriers such as the complexity of installation, the limitations of existing energy harvesting methods, and the challenges of ensuring interoperability between IoT devices and networks.

Key areas of study included energy harvesting techniques, wireless communication protocols, and the requirements for scalable and interoperable IoT architectures. This foundational work informed the design of the subsequent practical implementations and provided a clear framework for the research.

Development of a Self-Powered Smart Meter

Building on the theoretical groundwork, the next phase involved the design and development of a self-powered smart meter, as presented in the first publication. This device aimed to address the initial barriers to IoT adoption, particularly the need for simple, non-intrusive installation in industrial and rural environments. Utilizing energy harvested through magnetic induction and the low-power communication capabilities of Sigfox, the smart meter was capable of operating autonomously, requiring no modifications to existing electrical infrastructure.

This stage demonstrated the feasibility of deploying energy-efficient IoT devices in constrained environments. However, the device’s reliance on Sigfox and its limited features highlighted the need for more versatile and adaptable solutions. These limitations shaped the direction of subsequent research, leading to an exploration of diverse energy harvesting techniques and communication protocols.

Exploration of Wireless and Energy Harvesting Options

Recognizing the constraints of the initial device, the third phase focused on the evaluation of energy harvesting and wireless communication technologies to develop solutions tailored to a wider range of scenarios. This stage, detailed in the second publication, analyzed various energy harvesting methods, including photovoltaic, magnetic induction, and radiofrequency, assessing their compatibility with different IoT deployment environments.

In parallel, the research examined low-power communication protocols such as LoRa, NB-IoT, and BLE, comparing their performance across different energy sources and use cases. This analysis provided valuable insights into the trade-offs between energy efficiency, communication range, and data throughput, enabling the selection of optimal configurations for specific applications. The findings emphasized the importance of aligning energy sources and protocols to ensure the sustainability and reliability of IoT devices.

Standardization Through a Universal Test Bench

The lack of a standardized framework for evaluating the performance of IoT devices motivated the development of a universal test bench, as described in the third publication. This test bench was designed to provide a consistent and objective method for comparing the efficiency and reliability of IoT systems across various configurations.

The test bench allowed researchers to measure KPIs such as energy consumption, communication latency, and data transmission reliability under controlled conditions. By enabling normalized comparisons, this tool addressed a critical gap in the field, fostering innovation and guiding the optimization of IoT deployments. This stage marked a significant step toward standardizing the evaluation of IoT technologies, ensuring their scalability and interoperability.

Enhancing Interoperability Through an NB-IoT Relay

The final phase focused on addressing the challenge of interoperability between diverse IoT networks. This work, presented in the fourth publication, involved the development of an NB-IoT relay capable of bridging 6LoWPAN-based devices with legacy IPv4 internet infrastructures. The relay translated CoAP messages into standard REST requests, enabling seamless communication between low-power IoT devices and traditional networks.

This solution prioritized simplicity and energy efficiency, leveraging the multi-protocol capabilities of the FiPy microcontroller to support a range of IoT applications. By enhancing compatibility between emerging and established technologies, the relay facilitated the integration of IoT systems into broader network architectures, promoting scalability and reducing deployment complexity.

4.2. Compendium of Publications for this thesis

I. DOI: 10.3390/s20247133

Smart Metering for Challenging Scenarios: A Low-Cost, Self-Powered and Non-Intrusive IoT Device

Sensors 2020, 20, 7133

https://doi.org/10.3390/s20247133

Pages 39–64 present the original manuscript as published

sensors

MDPI

Article

Smart Metering for Challenging Scenarios: A Low-Cost, Self-Powered and Non-Intrusive IoT Device †

Edgar Saavedra *, Guillermo del Campo and Asuncion Santamaria

CeDInt-UPM, Universidad Politécnica de Madrid, Campus de Montegancedo, Pozuelo de Alarcón, 28223 Madrid, Spain; gcampo@cedint.upm.es (G.d.C.); asun.santamaria@upm.es (A.S.)

* Correspondence: e.saavedra@upm.es

† This paper is an extended version of the conference paper: Saavedra, E.; del Campo, G.; Santamaria, A. A Novel, Self-Powered, Non-Intrusive, Sigfox-Enabled Smart Meter for Challenging Scenarios. In Proceedings of the 2020 16th International Conference on Intelligent Environments (IE), Madrid, Spain, 20–23 July 2020; pp. 115–118.

Received: 27 October 2020; Accepted: 9 December 2020; Published: 12 December 2020

Abstract: In this work, a novel current metering device was presented. This device was intended to bring current metering capabilities to a wide variety of scenarios: Developing countries, rural areas, or any situation with technological constraints. The device was designed to provide a straightforward installation with no intrusion in the electrical panels. This was achieved by applying energy harvesting techniques and wireless communication technology for data transmission. The device was able to exploit the magnetic field inducted around a wire carrying electricity as energy harvesting, thus acquiring the power it needed to work. Since very low power was harvested, an efficient treatment for the incoming power and a minimal power consumption system were essential. Although exploiting the magnetic fields inducted around a wire has been used for years, the combination of this technology for both energy harvesting and current metering in an end-user device was off-center. To work in a wide variety of scenarios, it used Sigfox for communications as this brought wide coverage and out-of-the-box functioning. The theoretical design of the device was validated by verification assessments for the joint performance of the individual parts compounding the device, including metering capabilities and wireless communication test-bench. Finally, the metering device was tested under three distinct real-world scenarios that demonstrated the viability of the system. Results show that, depending on the metering period and the average current value in the mains line, the device could work forever acquiring and sending electricity consumption data. Perpetual working was achieved with an average current of 3.1 A to meter every 15 min, and an average current of 5 A for a 5-min metering period.

Keywords: energy harvesting; smart meter; Sigfox; self-powering; autonomous device; energy saving; internet of things

1. Introduction

Worldwide electricity consumption is constantly growing: The global increase from 2017 to 2018 was 3.5%, and it has more than doubled from 1990 [1]. Although more trust is put on renewable energies, fuel fossil-dependant energy generation is still a crucial contributor to global pollution, being more than 60% globally in 2018 [2]. Whereas USA and EU have been reducing carbon emissions since the 2000s—both for energy and goods production—emerging economies such as China and India present an increasing CO_2 contribution trend [3]. To overcome this global issue, there are different strategies such as the use of renewable energies, smart energy consumption analysis to reduce

usage, ambient-aware systems, smart grids, or on-demand response policies [4–6]. Among them, and focusing on emerging and developing countries, smart metering seems to be the most suitable approach [7]. Apart from being less cost-demanding, it may help to learn about inhabitants' energy habits, hence possibly reducing consumption and targeting on energy drains [8].

Regarding the smart meters' market, there are several options working in different ways. Some smart meters are those installed by electric companies to remotely acquire consumption data, and therefore bill accordingly [9,10]. Occasionally, they can even be used as part of the smart grid infrastructure and implement demand response mechanisms [11]. On the other hand, most of the available commercial systems are powered directly by the mains line with a transformer, such as those encountered in [12,13]. Although they have the advantage of also metering voltage (thus, reckoning power factor), this sort of device requires electrical supply, meaning that a specialist is needed for installation and the building power supply might be interrupted temporally, increasing costs and preventing actual deployments [14,15]. Further, in many cases—especially in developing countries or rural areas—electrical board panels face different challenges (location, access, configuration, size, and shape), not allowing the installation of intrusive smart meters. Hence, low cost, easy-to-install solutions may be a crucial factor in the decision for smart meters' installation. In the literature, there can be found various examples of self-powered electricity meters. Each of them faces a different measure range, electronic configuration, shape, and installation type.

In [16], a stick-on current and temperature sensor was presented, using Zigbee as a wireless technology and for currents in the range of 60–1000 A. Another example can be found in [17], where the authors cleverly implemented a GPS receiver in order to keep time synchronization with the data. Porcarelli et al. implemented an IEEE 802.15.4 compliant smart meter with a back-up battery for consumptions between 10 W and 10 kW, with a maximum measurement error of 1.6% [18]. In [19], a self-powering method based on the vibration of a piezoelectric cantilever excited by the magnetic coupling of AC was presented. A novel development of self-powered microelectromechanical systems (MEMS) current sensor modules was explained in [20], aiming to achieve voltage sensors as well.

However, none of them either used Sigfox as wireless technology or was targeted to ubiquitous, rural, developing areas, as some of them were difficult to install, lacking the aim of being non-intrusive.

This paper is an extension of the work originally presented in the 16th International Conference on Intelligent Environments (IE2020), titled "A Novel, Self-Powered, Non-Intrusive, Sigfox-Enabled Smart Meter for Challenging Scenarios" [21]. In comparison with the IE2020 manuscript, this paper assessed important improvements in the back-end part of the system, changed in the device's firmware to adapt it to different scenarios, and offered a more detailed analysis and validation of the device. This work presented a novel device that was able to measure current at 230 V single-phase mains lines, with no intrusion in the existing electrical installations, which may be crucial to be deployed in emerging countries or rural areas. Neither wired data connection nor power lines were required to make the system work. All the components of the device, from communications to firmware, were designed to minimize energy consumption and assure perpetual working.

The rest of the paper is organized as follows: Section 2 presents system description, including component selection and design decisions to meet working constraints. In Section 3, the reliability of the device is shown, including results from real-world implementations. Insights coming from results and experimental validation are discussed in Section 4.

2. System Design

The aim of the proposed device was measuring currents at mains electrical lines periodically. The general block for the system can be plotted out as in Figure 1. Energy was harvested with a clamp inductor, i.e., a current transformer, which generated an AC current. This current passed through a rectifier, where it was converted to DC before attacking one of the two following circuits: (a) The energy harvesting one, or (b) the current metering one. These two circuits were switched depending on the working state.

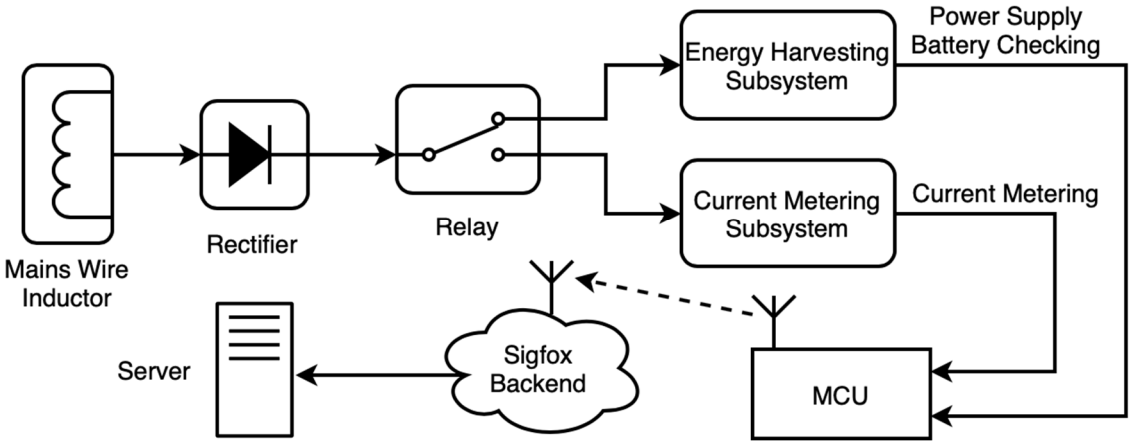


Figure 1. General block-diagram for the complete system, including the metering device itself and the communication to the server.

If the system was in sleep/stand-by mode, the energy harvesting subsystem was working, supplying power to the microcontroller (MCU) and storing the remaining energy in a battery. Otherwise, the MCU was in charge of reckoning the current value in the mains wire by using the current metering subsystem. Current measurements were stored in the MCU's RAM (buffer) until a sending event was triggered, when data were parsed and transmitted via Sigfox. The Sigfox backend received these data and then forwarded them to an ad-hoc server, where data were stored and prepared for visualization and analysis.

Sigfox was the selected communication technology, although it presented some drawbacks in terms of packet size (12-byte messages), bandwidth (100 bps), or messages per day (140). Still, it was the most suitable one concerning the smart metering application in different scenarios: Rural environments, crowded buildings, developing countries, etc. Sigfox works out-of-the-box with its own network, providing end-to-end encryption and ultra-narrow band modulation (UNB) [22]. Thus, there was no need to deploy a wireless infrastructure (as with 6LoWPAN or LoRaWAN), which could be ineffective in rural or developing areas with a few smart meters. Cellular technologies such as NB-IoT or LTE-M were also discarded since they were relatively new in the market and they were not really established [23].

The measure range was set to 0–25 A since it seemed to be a fair-minded span for most metering scenarios. Moreover, it allowed each current measurement to be enocoded with just one byte, providing 0.1 A precision—since one byte could represent integers from 0 to 255. This was important to note since Sigfox's message payload was 12 bytes and measures were sent in groups of 12 to reduce energy consumption. This meant an overall relative encoding precision of 0.4%.

Since the device was meant for a wide variety of non-critical scenarios, such as rural areas or developing countries, where main constraints appear in terms of cost, power consumption, and simplicity, its design was not thought against harsh environments such as industrial facilities or weather hazards. For usage under these conditions, a specific casing should be designed and tested. In any case, using Sigfox assured a high quality of wireless communications, as it was very tough against interferences due to its UNB modulation and receiving antennas' infrastructure.

2.1. Energy Harvesting

Energy harvesting has been a trending topic during the last years, becoming a feasible solution when very-low-power electronic devices were achievable from the 2010s. Providing energy harvesting capability to wireless devices enables them to continuously acquire energy, therefore eliminating the concern of their lifetime being dependant on the energy storage system capacity or battery exchange [24]. Every energy harvesting device is compounded, at least, of three main blocks: The harvester itself, the signal conditioning block, and the storage element.

There are many energy harvesting technologies and new ones may appear in the near future. The most relevant for smart meters and similar applications might be:

- Ambient radiation: This is based on exploiting the large amount of radio frequency (RF) energy available in the ambient at different frequencies; an example can be seen in [25];
- Photovoltaic (PV): Transforming light radiation into current; it is virtually inexhaustible and probably the one from which greatest energy can be obtained [26];
- Piezoelectric: Using the piezoelectric effect, which converts mechanical strain or ambient vibration into electrical energy; an example can be seen in [27];
- Magnetic induction: Electrical energy is obtained by moving magnets—or changing magnetic fields, as in [28]—near or inside a coil;
- Vibration: Vibration energy harvesting may be fitted into the magnetic energy harvesting field, as it usually relies on varying magnetic fields created due to vibrations to generate energy, as designed in [29];
- Pyroelectric and thermoelectric: These are intended to exploit heat in order to obtain electrical energy, whether relying on temperature gradients or time-variant temperatures, as described in [30].

The device proposed in this work was power supplied by means of magnetic induction energy harvesting (MIEH). When magnets teeter through a coil, they create a variable magnetic field. This magnetic field happens to generate an electromotive force (EMF) into the coil. This phenomenon is described in Faraday's Law of Induction [31,32], which explains the EMF (**E**) created when a time-variant (dt) magnetic field (**B**) is present (1, 2). As Faraday's Law is reciprocal, every conductor carrying a certain amount of current creates a surrounding magnetic field. If this is the magnetic field time-variant, it may be able to be exploited. Thus, some amount of electrical energy might be drawn.

$$\oint_{\partial\Sigma} \mathbf{E}\, \mathrm{d}l = -\frac{\mathrm{d}}{\mathrm{d}t} \iint_{\Sigma} \mathbf{B}\, \mathrm{d}\mathbf{S} \tag{1}$$

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \tag{2}$$

MIEH seemed to be the best choice for this device considering its own nature, in which a wire carrying electricity had to always be present for metering current. The device needed the existence of a current, and therefore power to perform its current metering function. This device took advantage of the magnetic field happened around a conductor carrying electricity—which was a time-variant as mains electricity was AC—to produce an EMF in a coil. This is the principle used in most current probes for current metering, notwithstanding with the fact that in this work it was also proven to be the power supply for the system. If other methods of energy harvesting were used, a different component would be needed for energy harvesting and metering, increasing the complexity and cost of the device and its functioning. Moreover, depending on the meter location, different types of EH techniques might have been chosen, which counteracted the universal aim of the device.

This approach to MIEH has not been used widely, yet the device proposed in this work and [28] used a similar configuration for the main blocks of the system, but different wireless and switching technologies. It used IEEE 802.15.4 as wireless technology instead of Sigfox, and a MOSFET-based switch system, whilst we relied on a solid-state relay for switching. The device proposed in [28] was proven to self-power itself for a metering period of 60 s when a load of 300 W was connected. In this work, several conditions of the metering period and current consumption were discussed and demonstrated.

2.2. Harvester

The harvester itself was a clamp inductor—a current transformer—with a current ratio of 1500:1. This meant that the current outgoing the inductor was 1500 times lower—the secondary coil—than that being carried in the mains wire—the primary coil. The inductor was characterized, including measurements for the short-circuit (SC) current and open-circuit (OC) voltage in the secondary coil. Table 1 shows these measurements, in which the 1500 times relation can be seen—SC current vs. the current through primary. The SC current and OC voltage were the absolute maximum values that the harvester could provide, which were not those really exploited when a load was connected—both of them being lower. In Section 3.1 hereof, actual charging currents are depicted, the top limit being restricted to 1.13 mA.

Table 1. Measurement samples on the harvester characterization.

Current through Primary (A_{rms})	SC Current (mA_{rms})	OC Voltage (V_{rms})
0.80	0.5	0.7
1.60	1.0	1.5
3.20	2.1	3.7
6.35	4.4	6.8
12.70	8.7	9.5
19.05	13.1	10.8
25.60	17.5	12.4

A worth-noting, non-linear effect occurred in the harvester when it was excited by high currents. The inductor's iron core magnetic hysteresis altered the sinusoidal shape of the mains wire signal, resulting in a disturbed alternating signal [33]. This effect altered efficiency and dimensioning of the device due to the loss of power capability, thus limiting the harvesting capabilities of the device. Cutting out peak voltage plus sinusoidal shape loss—signal area loss resulted in less usable energy to harvest. It also affected the calibration process since linearity was lost. This anomaly arose when a high intensity magnetic field was inducted into the iron core and it changed, as the material remained magnetized. An example of the signal out of the harvester is shown in Figure 2.

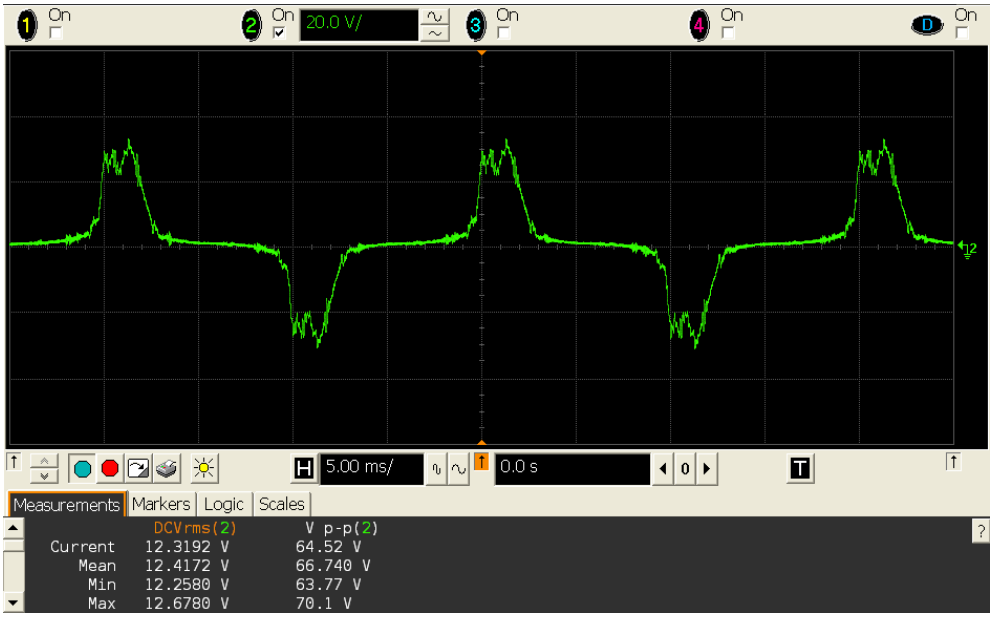


Figure 2. Oscilloscope screenshot where the disturbance occurred due to the inductor's iron core magnetic hysteresis is depicted.

2.3. Microcontroller

The MCU had to comply with different requisites that could be summarized in: (i) Very low stand-by power consumption, (ii) Sigfox-compliant, (iii) fast and wide firmware development.

After a market research on Sigfox-compliant development boards, Pycom devices came to court bringing a wide community for development and a MicroPython environment to run the program code. MicroPython is an efficient implementation of Python 3 with a subset of the standard Python library. Further, it is optimized to run on microcontrollers [34]. This leads to a fast, lean, and interactive building process by using Python rather than C, which is the typical language used for microcontroller programming.

Pycom provides several devices depending on the wireless communication. They are all based on the well-known ESP32 [35]. LoPy4 [36] is the one used in this work, which provides Wi-Fi, Bluetooth, LoRa, and Sigfox—although only Sigfox was used so far.

This board provided a deep-sleep consumption of just 25 µA, supporting wake-up from an external interruption and from a timer, which was the one used in this work. Moreover, the integrated 12-bit analog-to-digital converter (ADC) provided 4096 measure points, meaning a theoretical overall precision of 6.1 mA within the 0–25 A measurable range—enough for this purpose and above the 100-mA precision set by the encoding format.

2.4. Switching and Conditioning Subsystem

Since the same clamp was acting as harvester and current probe, it was necessary to have a proper conditioning stage to get the signal ready for either energy harvesting or current measurement (see Figure 3). Considering that this power meter was intended for measuring only active power, and that electronic circuitry worked on DC, the incoming AC signal was rectified from the very beginning to simplify electronic design and procedures. Working with DC allowed us to use a single pole switch—since the other pole is ground—whilst AC would require dual pole switches. Thus, a full-wave rectifier was implemented: CBRHDSH1-40L [37]. Although every component added to the system came with a certain amount of power losses, those resulting from an efficient, full-wave rectifier could be considered negligible.

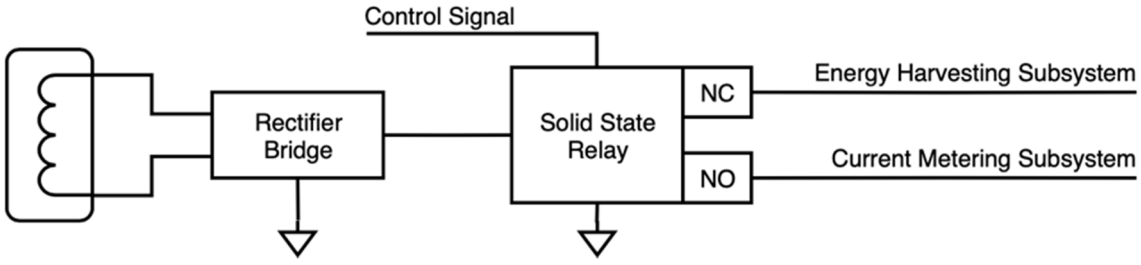


Figure 3. Conceptual schematic of the switching and conditioning circuit, including the harvester, the rectifier, and the solid-state relay.

Once the signal was rectified, it had to go either to the energy harvesting circuit or to the current measurement one. For this switching to be performed, a solid-state relay was chosen: LBA710 [38]. Reduced energy consumption in operation and stand-by was crucial, and a relay guaranteed a non-consuming default state (normally open, NO). Furthermore, using a solid-state relay instead of a magnetoelectric one meant less energy consumption and faster switching.

2.5. Energy Harvesting Subsystem

The harvester subsystem was intended to be as efficient and simple as possible in order to maximize energy harvesting capabilities (see Figure 4). The main element of this block was a power management IC intended for low-power energy harvesting applications: BQ25504 [39]. The BQ25504

is a boost converter that manages the energy storage: The charge of a battery as main storage element and a capacitor as first-stage, instantaneous storage element. The main characteristics of BQ25504 are summarized in Table 2.

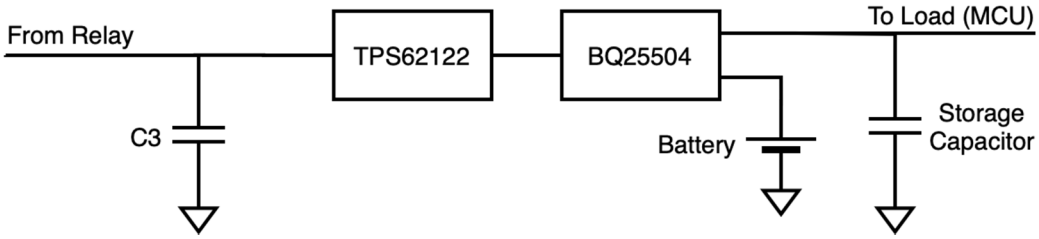


Figure 4. Conceptual schematic of the energy harvesting subsystem.

Table 2. Summary of BQ25504 characteristics.

Parameter	Value
Input voltage (V_{IN})	0.12–3 V
Battery voltage ($VBAT$)	2.5–5.25 V
Storage capacitance (C_{STOR})	4.7 µF
Input power (P_{IN})	0.01–300 mW
Cold-start voltage ($V_{IN(CS)}$)	300 mV
Min. cold-start input power ($P_{IN(CS)}$)	15 µW
Switching frequency (f_{SW})	1 MHz

The BQ25504 has a restricted input voltage of up to 3 V, but the incoming signal may be higher. Therefore, it is necessary to limit input voltage. Due to efficiency reasons, the buck converter TPS62122 [40] is selected, providing an output of 2.8 V, which is set by means of external resistors. The main characteristics of TPS62122 are summarized in Table 3.

Table 3. Summary of TPS62122 characteristics.

Parameter	Value
Input voltage (V_{IN})	2–15 V
Output current capability (I_{OUT})	> 75 mA
Output voltage (V_{OUT})	1.2–5.5 V
Switching frequency (f_{SW})	800 kHz

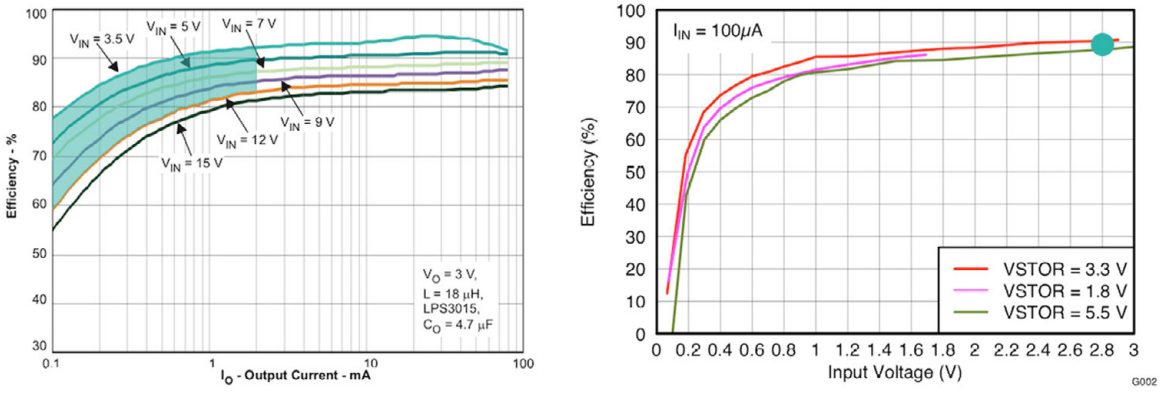
The BQ25504 was configured for an output working range of 3.5–4.2 V, corresponding to the common range of battery (3.4–4.2 V) and MCU (3.5–5.5 V) specifications. These thresholds were set by means of configuration resistors following datasheet instructions.

Figure 5 depicts the behavior of BQ25504 when a partially charged battery was attached. The VSTOR signal represents the voltage in the terminal where the first-stage storage element, as well as the load, i.e., the boost converter output, are connected. $VBAT_{OK}$ is a logical signal indicating whether the battery has a reliable level of charge, as determined in the configuration thresholds. The yellow signal was a 2.8 V DC voltage used as the boost converter input.

Figure 5. Behavior of BQ25504 when a partially charged battery is attached.

In instant (**O**), the power source was turned on and therefore the capacitor at VSTOR began charging. The first stage (**O**-**A**) corresponded to the switching of the internal PFET between VSTOR and VBAT, with a duration of ~45 ms. This was the reason why the voltage at point (**A**) was the voltage at the battery, approximately 3.6 V. Then, the charger was disabled for ~32 ms (**A**-**B**), after an internal procedure to reset feedback voltages. Next, VIN_{DC} was used as the power source, being the voltage risen up to nearly 4.2 V ($VBAT_{OV}$) after ~5 ms. Lastly, another ~32 ms later, a normal charging process took place (**C**); thus, the VSTOR voltage dropped to 3.77 V as it was charging the second-stage storage element, and VSTOR and VBAT were short-circuited. The $VBAT_{OK}$ signal switched just when the first feedback sampling was done: Point (**C**), approximately 100 ms after the power source was turned on.

Regarding harvesting efficiency, the two main contributors were buck and boost converters. Figure 6 shows efficiency curves for the buck converter (a) and boost converter (b) for different voltage configurations. In our design, the buck converter was set to provide an output of 2.8 V, which was the input voltage of the boost converter. Output current values were in the range 0.1–1.1 mA, as it will be described in Section 3.1 hereof, and buck input voltages were below 12.4 V, as in Table 1. With these data, energy harvesting theoretical efficiency could be reckoned to be in the range 50–80% (60–90% and 90% for the buck and boost converter, respectively), depending on the working characteristics. However, experimental results showed that real efficiency was lower, resulting in the range of 30–55%.



(**a**) (**b**)

Figure 6. (**a**) Buck converter efficiency curve [40]; (**b**) boost converter efficiency curve [39].

The power consumption of the energy harvesting subsystem without battery and load was measured and it is depicted in Figure A3 of the Appendix A. It corresponded to an average current consumption of 0.38 µA.

2.6. Current Metering Subsystem

The current metering subsystem was in charge of measuring the current carried by the mains wire. A measurement resistor was needed for converting the proportional current signal of the probe into a voltage signal for the ADC (MCU) to be read (see Figure 7). Two series resistors were implemented—i.e., a voltage divider (R1-R2)—sampling the voltage in the second resistor of the branch (R2).

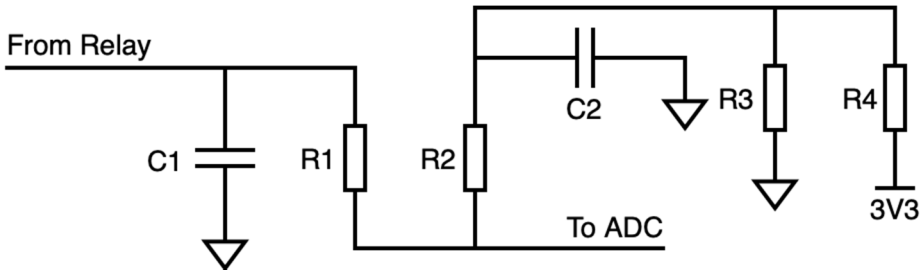


Figure 7. Conceptual schematic for the current metering subsystem.

The resulting signal was full-wave rectified, yet a capacitor was still to be set in this block. The ripple was desired to be as negligible as possible; but the smaller the ripple was, the longer the stabilization time became. A long stabilization time was not wished as more time would be spent in measuring instead of harvesting; hence, more energy would be wasted. Be that as it may, a perfectly constant signal was not needed as the signal was sampled 1100 times, then averaged, so the ripple was overcome.

It is worth noting that, for voltages under 50 mV (0.98 A), the ADC did not work properly, and measurements were very inaccurate, often returning negligible values. To overcome this issue, an offset was set to the signal read by the ADC: A pretend reference was introduced and soared up from ground (GND). This was solved with a voltage divider (R3-R4), using the 3.3 V coming out from LoPy4's general-purpose input/output (GPIO) pin when the relay was toggled, and stabilized with C2. With a capacitor value of 2.2 µF (C1), a convergence time of 200 ms was obtained, and the ripple reached 15.5 mV in the worst-case scenario, which was that corresponding to the greater current in the mains wire (see Figure 8). The mean value for the ADC signal plus the ripple (green signal, 940.7 mV) remained lower than the ADC limit (1.1 V).

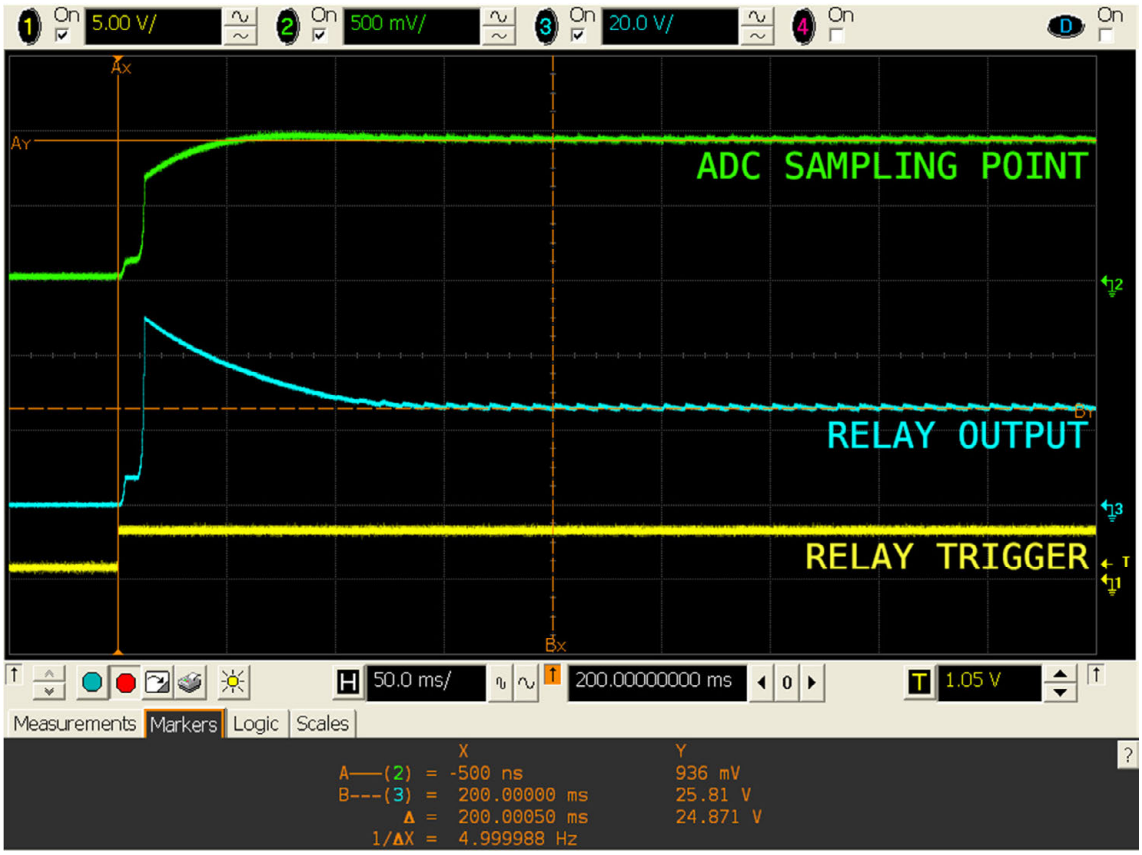


Figure 8. Oscilloscope screenshot: 200 ms convergence time for the metering system.

A calibration process was performed by reading the values returned by the ADC when 48 known currents were sampled (see Figure 9), with an average value of 10,000 samples for each current value. This led to obtaining the quadratic approximation for the current by means of ADC readings with an $R^2 = 1$; i.e., a greater order would not necessarily enhance formula's performance. Note the adjusting of ADC voltages to overcome readings <50 mV: 0 A corresponds to a >50 mV ADC reading. This formula was then programmed in the MCU's firmware to reckon the current in the mains wire.

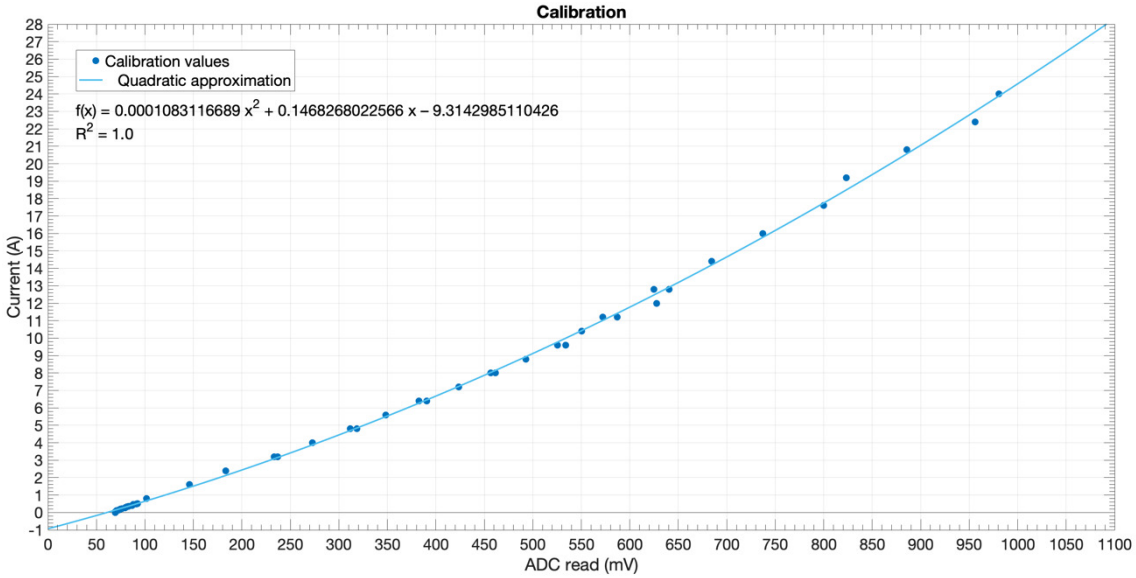


Figure 9. Calibration curve and quadratic approximation.

2.7. Switching between the Energy Harvesting Mode and the Current Metering Mode

As aforementioned, this metering device had two modes of operation: The default one—for energy harvesting—and the periodically triggered mode—to meter the current at the mains wire. The change between states happened when the MCU toggled the solid-state relay. Figure 10 shows the most relevant signals in order to illustrate this phenomenon. Note that there was no battery attached and the process was slowed down in order to see the effect on $VBAT_{OK}$.

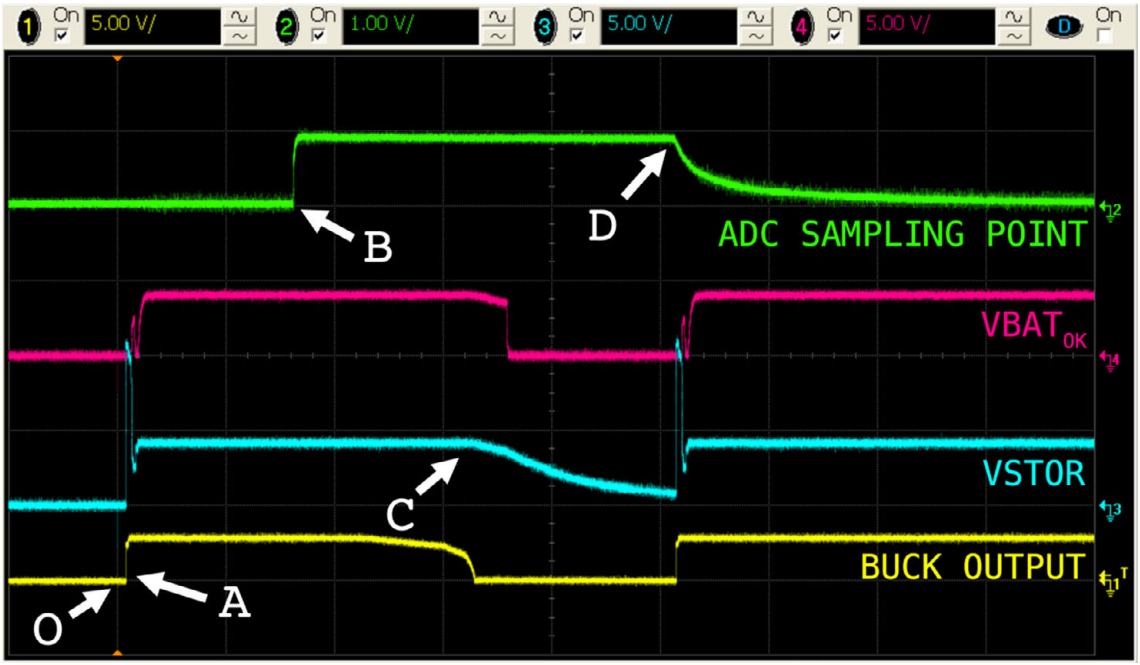


Figure 10. Oscilloscope screenshot: Switching between modes of operation.

In instant (**O**) the load was connected. However, it was not until event (**A**) when there was enough energy in the input capacitor C_{DCIN} so that the buck converter could start working. The switching mode phenomenon occurred at point (**B**), where the relay was toggled. Thus, C_{DCIN} started discharging until occurrence (**C**), where there was not sufficient energy to drive the buck converter and therefore the VSTOR capacitor started discharging. At point (**D**), the relay was toggled, starting the harvesting process anew. As expected, the $VBAT_{OK}$ signal changed its state according to the voltage at the VSTOR and designated thresholds.

2.8. Device's Firmware

The MCU's firmware was written in MicroPython, intended to be as straightforward and short as possible to make the processes fast and stable. The behavior was event-driven, based on a 15-min timer to take measurements. Its working principle may be summarized as follows (see Figure 11 for clarification):

1. When the device woke up from sleep mode, it checked the charge level of the battery ($VBAT_{OK}$ signal). If it was above the required threshold, it continued running. Otherwise, error was handled, then it returned to sleep. If this error code provoked the buffer to be full, the buffer would be erased in order not to lose time reference, as it was not sent alongside the message but using Sigfox's backend timestamp;
2. If the battery health was good, the metering process began. The relay was toggled, then stabilization time was waited. Next, 1100 samples of the signal were collected, averaged, and converted into a current value. If the current reading was out of boundaries, an error message was encoded;

3. The new measurement was buffered and, if the buffer became full (12 measurements), the Sigfox sending process was performed to begin anew.

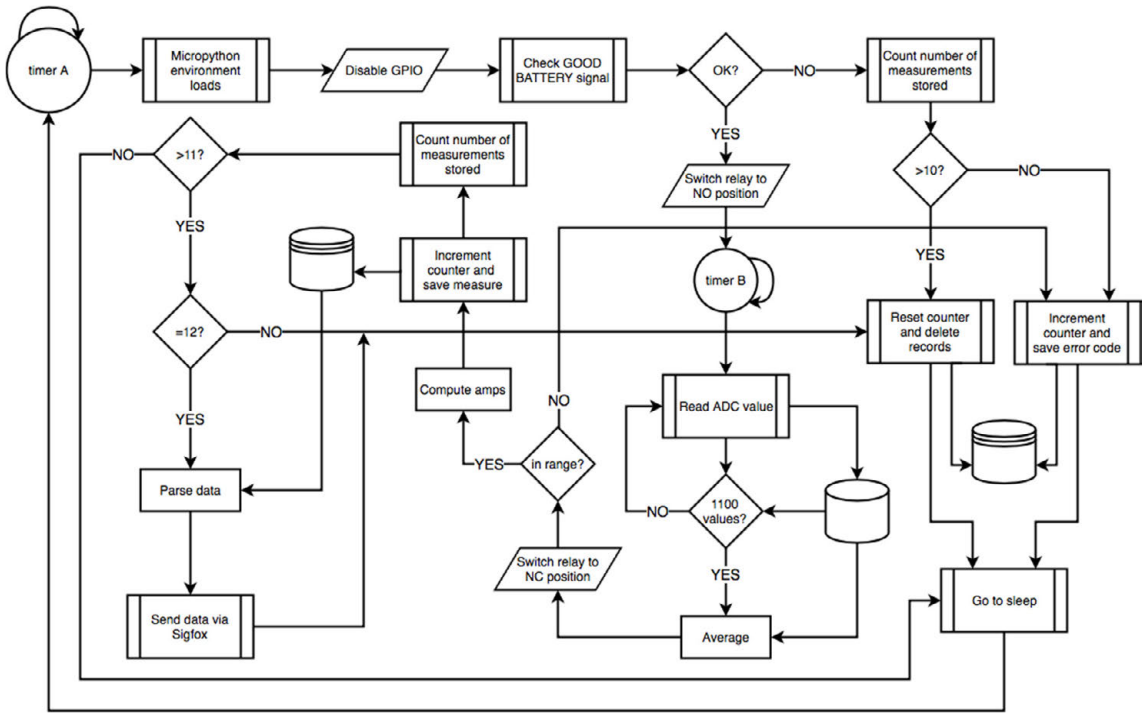


Figure 11. Flowchart for the microcontroller's (MCU) firmware.

In order to keep time synchronization, the time the device went to deep sleep and was slightly modified depending on what it did before. Every behavior (metering, metering and sending, low battery level, etc.) took a different amount of time. They all were characterized and taken into account when commanding the device to sleep.

The encoding format, one byte for every measure, is the following:

- [0, 250]: Current reading in tenths of ampere;
- [251, 255]: Reserved for error codes:
    - 251: Measure under range;
    - 252: Measure over range;
    - 253: Future use;
    - 254: Handled firmware exception;
    - 255: Energy fault, bad battery status.

2.9. Server-Side Software

When the device sent a Sigfox message, this was received by the Sigfox backend, where call-backs were set up. In this case, an HTTPS POST request was performed to an ad-hoc server every time a message is received. The usage of HTTPS was crucial in order to send requests encrypted, being only readable by the receiver: A server located at university facilities. The call-back was set to send a header with an authentication token and a JavaScript Object Notation (JSON) body containing the following parameters:

{"payload":{"device":"{device}","time":"{time}","data":"{data}","seqNumber":"{seqNumber}"}}

The server was written in Node.js [41], using the Express [42] framework on a Raspberry Pi 4 [43]. For communicating with the Sigfox backend, the POST resource was available at https://SERVER-IP:

1784/insert. When receiving a request, the server checked the authentication token to prove the request was legitimate. Then it parsed the data, applying the temporal shifting to every measurement and storing them into an InfluxDB [44] database.

InfluxDB was the selected database technology as it is a very powerful yet fast, emerging temporal-series database. Moreover, it is part of the TICK [45] stack, which provides Chronograf as a straight-forward way of visualizing InfluxDB data, and it is also compatible with the well-known Grafana. In Figure 12, one can see an example of a Sigfox message (12 measures) in the database, where timestamps are stored in nanoseconds referred to as the epoch, data are current measurements in amperes, and seqN is the Sigfox message sequence number.

```
> select * from "4D380B" where "seqN" = 65
name: 4D380B
time                data seqN
----                ---- ----
1598925301000000000 4.9  65
1598926201000000000 4.8  65
1598927101000000000 5.1  65
1598928001000000000 4.9  65
1598928901000000000 4.7  65
1598929801000000000 5    65
1598930701000000000 5.1  65
1598931601000000000 4.7  65
1598932501000000000 4.7  65
1598933401000000000 4.9  65
1598934301000000000 4.9  65
1598935201000000000 4.8  65
1598939635000000000 5    65
```

Figure 12. Example of a Sigfox message in the InfluxDB database.

2.10. In-Situ Wireless Communication Latency Test

We developed a test-bench (see Figure 13) to measure the time elapsed since the device was commanded to send a message until it was received at our server. To do this, we used a Raspberry Pi in which a dedicated Node.js server to measure the latency was deployed. This server rose a GPIO signal to trigger an interruption on the LoPy4 (rising edge). In this moment, the MCU began the Sigfox sending process with a 12-byte payload message and the server timestamps starting time. When the message was received back from the Sigfox backend to the server, the latter measured the time elapsed since the start.

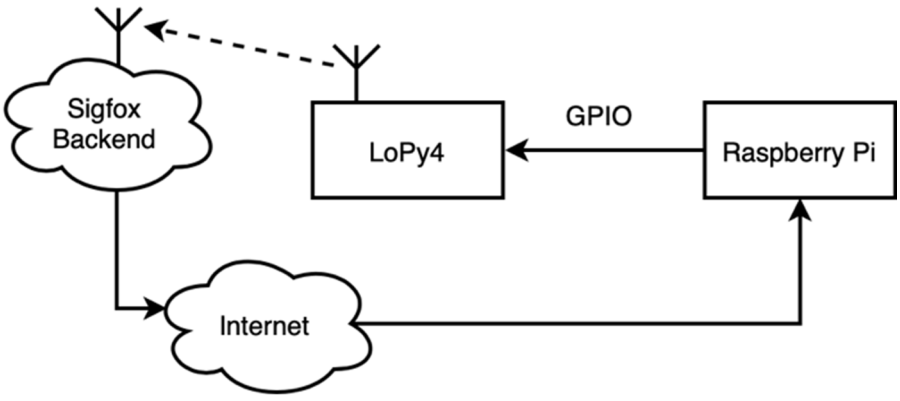


Figure 13. Conceptual diagram of the test-bench deployed for metering Sigfox latency.

After different tests, the resulting measured latency was about 3.6 s (values between 3.5–3.7 s were measured). From these values, we could extract that a base station was receiving messages in the first Sigfox iteration, since a Sigfox iteration took about 2 s on air for a 12-byte payload message. Sigfox sent messages thrice in three different carriers to ensure delivery. In other geographical zones with worse coverage, this might not be the case, and two or even three iterations could be needed for delivery.

Taking a look into the call-back information, messages were received by four different base stations with identifiers 086A, 080D, 7DC7, and 0663. This meant that the tests were performed in a high coverage area, covered by at least four base stations.

3. Results and Validation

In order to verify the proper functioning of the device, three main validation steps were conducted: (i) Power budget validation, (ii) current metering certainty verification, and (iii) real-world application final testing.

3.1. Power Budget

The first-proposed metering period is 15 min, thus sending data every 3 h—when 12 measures were collected. In order to guarantee a perpetual working, i.e., no change of battery, for the metering period to be 15 min, a mean current of 3.1 A was needed in the mains line that was being monitored. For shorter metering periods, the average current in the mains line would be greater, as it is explained later.

An Agilent 34,410A multimeter was used to measure and record the device's working current consumption. There were five main behaviors for the MCU depending on the buffer state and battery level. These were:

1. Sleep mode (15 min, 21.56 µA);
2. Standard measuring process (2.26 s, 59.61 mA);
3. $VBAT_{OK}$ was low, so an error code was saved (1.85 s, 60.55 mA);
4. $VBAT_{OK}$ was low, and this error code saving made the buffer full; thus, it had to be erased and the counter reset (1.81 s, 60.54 mA);
5. A measurement that made the buffer be full was taken, so the Sigfox sending process was launched (12.69 s, 70.57 mA).

Appendix A presents detailed consumption measurements for processes #2 (see Figure A1) and #5 (see Figure A2), which are the most relevant in energy consuming terms.

Afterwards, the actual energy injected into the battery was characterized, checking the battery life of the device. The energy stored into the battery depended, as previously stated, on the mains wire current. Measured charging currents—for a half-charged battery—are presented in Figure 14.

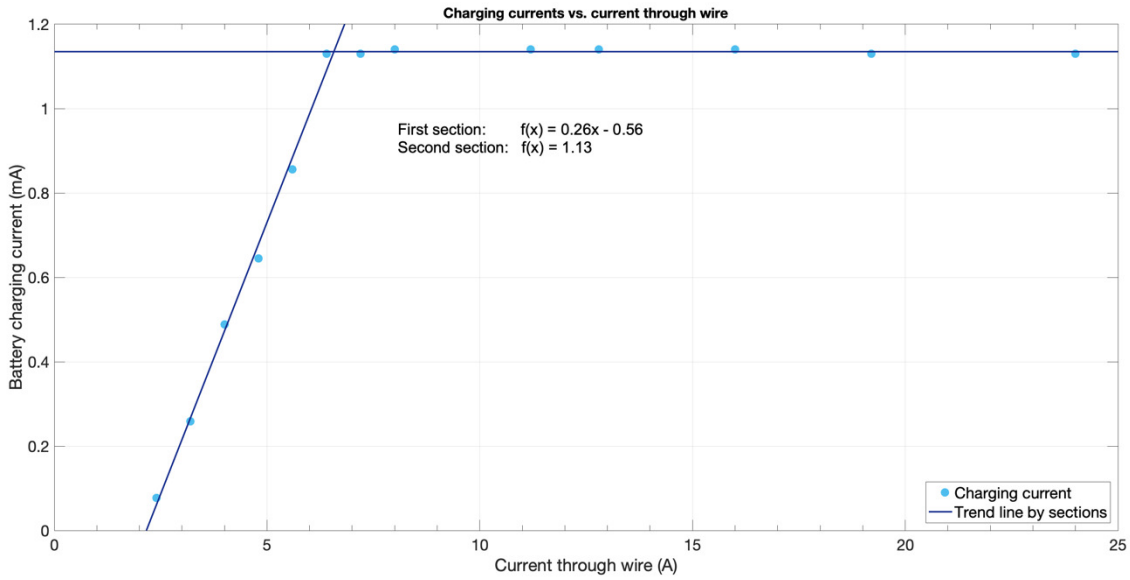


Figure 14. Charging currents for different currents in the mains wire.

As it can be observed, the charging current followed a linear pattern until it reached the maximum current that the boost converter was able to inject into the battery. In fact, the charging current behaved as a PWM signal with a top current of approximately 1.13 mA, which increased its duty cycle as the mains wire current increased until 6.4 A (see Figure A4 of the Appendix A for exemplification). This was the reason why once the charging current provided a 100% duty cycle, it could not become higher as the top limit was imposed by the charging circuit itself. Further, for mains wire currents lower than 2.2 A, there was not enough input voltage for the buck converter to start working, therefore stepping down the signal to 2.8 V. This issue might have been solved by using a more complex buck/boost converter or by bypassing the input signal directly to the boost converter if the voltage remained lower than that of the needed threshold.

This issue led to an effective current harvesting range (2.2–6.4 A) different to the whole metering range (0–25 A). This was the reason why, in order to calculate and check power budget, metered currents were assumed to be in the effective current harvesting range. In the upcoming sections, when consumptions were above or below these effective limits, we would be referring to them as the "effective average current" when the average calculation was made, taking into account this limitation—i.e., currents greater than 6.4 A computed as 6.4 A and currents lesser than 2.2 A computed as 0 A. On the other hand, the "average current" referred to the pure mean calculation of the average current.

With both the consumption and generation characterizations, battery life could now be determined. For this calculation, the most energy-demanding scenario was used, which was also the most feasible one: That where 12 complete measures were done, sending the buffer in the last one via Sigfox (see Figure 15). This energy could be computed following Equation (3):

$$\begin{gathered} \Psi_1 = 11{\cdot}2.26 \text{ s}{\cdot}59.61 \text{ mA} = 1481.9 \text{ mAs} \\ \Psi_2 = 1{\cdot}12.69 \text{ s}{\cdot}70.57 \text{ mA} = 895.53 \text{ mAs} \\ \Psi_3 = 12{\cdot}900 \text{ s}{\cdot}21.56 \text{ µA} = 232.85 \text{ mAs} \\ \Psi = \Psi_1 + \Psi_2 + \Psi_3 = 2610.28 \text{ mAs} \end{gathered} \tag{3}$$

where:

- Ψ_1 is the energy required for the 11 standard metering processes;
- Ψ_2 is the energy required for the last metering process which also sends the buffer via Sigfox;
- Ψ_3 is the energy required for the 12 deep-sleep periods compounding a whole metering cycle.

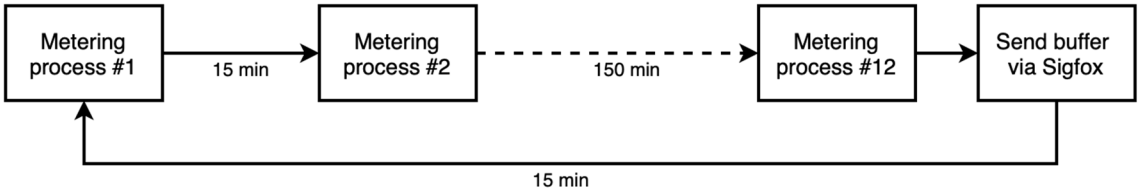


Figure 15. Graphical representation of the standard metering cycle.

The aim of this device was being able to work for a lifetime, so the energy harvested into the battery had to compensate for the energy consumed in the process. Taking into account the measured consumptions for every iteration, the necessary current to be injected into the battery happens to be:

$$\begin{gathered} \Gamma = \frac{\Psi}{t} = \frac{2610.28 \text{ mAs}}{12{\cdot}900 \text{ s} - (11{\cdot}2.26 \text{ s} + 12.69 \text{ s})} = 242.5 \text{ µA} \\ 242.5 \text{ µA} \underset{\text{harvested when}}{\Longleftarrow} \sim 3.08 \text{ A} \end{gathered} \tag{4}$$

If an effective average current of 3.1 A (713 W, e.g., a workstation) was being carried by the mains line wire, an infinite battery lifetime could be guaranteed for a 15-min measuring period. This average current would increase if shorter periods were wished.

Figure 16 represents the relation between a metering period and efficient average mains wire current. The metering period was a factor from Equation (5)—generalized Equation (4), where T is the metering period in seconds—and the mains wire current came from Equation (6), which is derived from Figure 14.

$$\Gamma\,(\mathrm{mA}) = \frac{\Psi}{t} = \frac{2610.28\ \mathrm{mAs}}{12{\cdot}T\,(\mathrm{s}) - (11{\cdot}2.26\ \mathrm{s} + 12.69\ \mathrm{s})} \tag{5}$$

$$\Gamma\,(\mathrm{mA}) = 0.26{\cdot}I\,(\mathrm{A}) - 0.56 \tag{6}$$

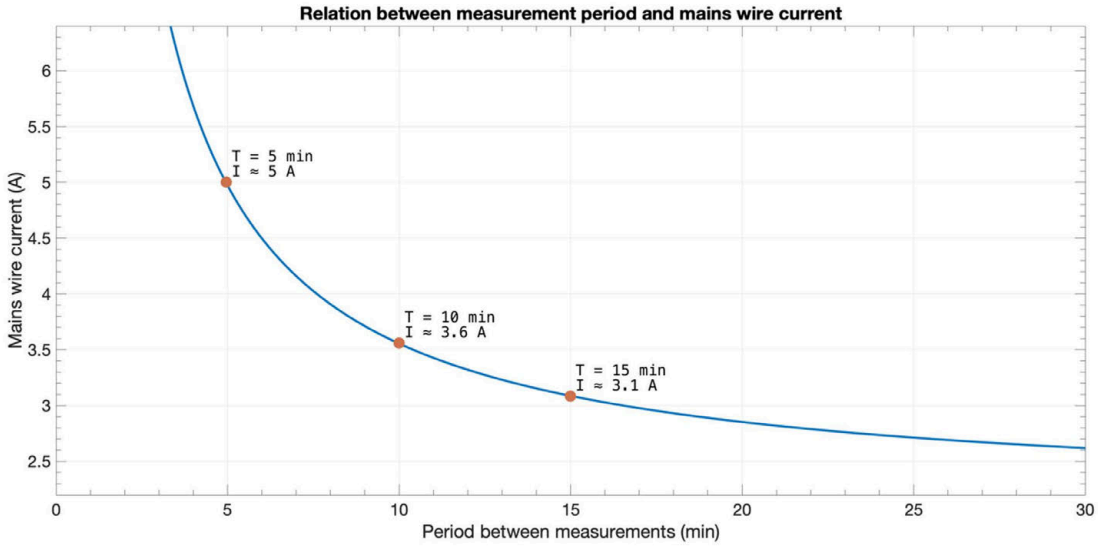


Figure 16. Effective average current needed in the mains wire vs. metering period.

Working conditions for perpetual work depended on the effective average mains current and the metering period. For instance, for a metering period of 5 min, the effective average current needed would be nearly 5 A. It is worth noting that, due to the 1.13 mA upper limit of the charging circuit, the minimum feasible period was 3.4 min. Further, due to the lower limit from which the circuit began charging (2.2 A), the maximum theoretical period was about 5 h.

Considering that the prototype was equipped with a 2200-mAh battery, battery life could be summarized as in Figure 17; where the metering period was depicted on the horizontal axis, average current in the mains line on the vertical axis, and the bubble size showed the estimated battery life for such conditions. As shown in Figure 16, from a certain value and above, battery life would become virtually infinite as the device's energy consumption became counterbalanced with the energy harvested from the mains (colored area). No bubbles were plotted out for currents less than 2.5 A since the device needed a minimum current of 2.2 A for energy harvesting—as stated in Section 3.1 hereof.

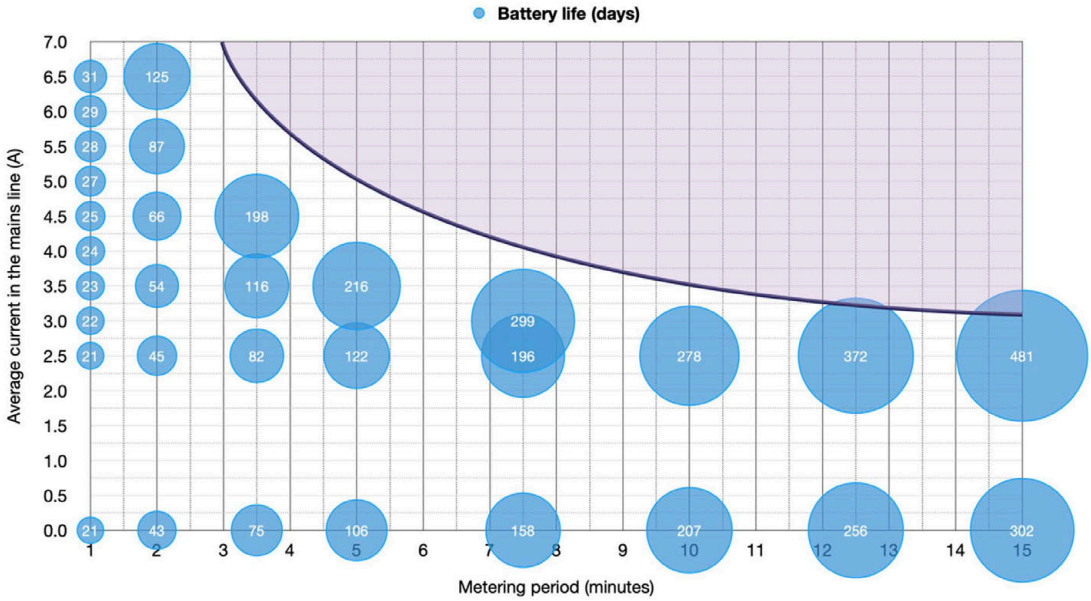


Figure 17. Graphical summary of battery life depending on metering period and effective average current in the mains electrical line.

3.2. Current Metering

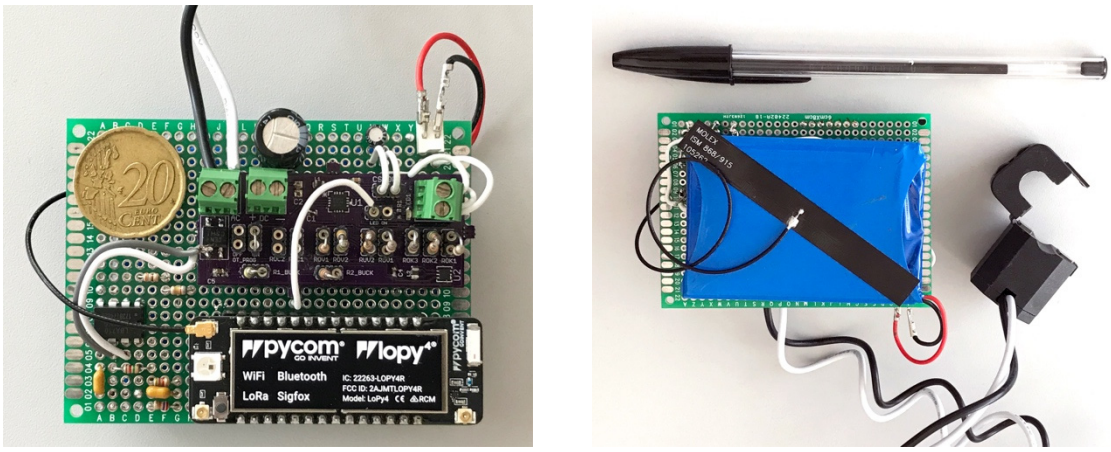
For metering veracity, 15 different current values were probed; composed of 10 consecutive measurements each (see Table 4). Standard deviation was 0.032 A, while the relative error was 3.28% in the whole range of measurement. This relative error was suitable for most cases. Still, it was important to note that it was greatly increased due to the first current values in the lowest range. If measurements below 0.5 A were dismissed, the relative error would result in just about 0.8%. Regarding the standard deviation, it was in fact below the encoding format precision limit (0.1 A), so it was not be noticed. Comparing with the work in [28], they obtained a relative peak error of 1.6%.

Table 4. Measurements corresponding to the metering validation (all values in amperes).

Multim. Reading	1	2	3	4	5	6	7	8	9	10	Avg.	Std. Dev.	Rel. Err. (%)
0.14	0.1	0.1	0.2	0.1	0.1	0.1	0.1	0.1	0.0	0.1	0.10	0.0471	28.57
0.28	0.2	0.3	0.2	0.3	0.3	0.2	0.2	0.2	0.2	0.2	0.23	0.0316	3.57
0.42	0.4	0.4	0.4	0.4	0.3	0.4	0.4	0.4	0.3	0.4	0.38	0.0316	7.14
0.56	0.5	0.6	0.6	0.5	0.6	0.6	0.6	0.6	0.6	0.6	0.58	0.0316	5.36
0.80	0.8	0.7	0.7	0.8	0.8	0.8	0.8	0.8	0.7	0.8	0.77	0.0316	1.25
1.60	1.6	1.5	1.6	1.6	1.6	1.6	1.6	1.6	1.6	1.6	1.59	0.0316	0.63
2.40	2.3	2.4	2.4	2.4	2.4	2.4	2.4	2.4	2.4	2.4	2.39	0.0000	0.00
3.20	3.2	3.2	3.3	3.2	3.3	3.3	3.2	3.2	3.3	3.2	3.24	0.0316	0.31
4.80	4.8	4.8	4.8	4.9	4.8	4.8	4.8	4.8	4.8	4.9	4.82	0.0422	0.42
6.35	6.4	6.5	6.4	6.4	6.5	6.4	6.3	6.4	6.4	6.4	6.41	0.0316	0.63
9.53	9.5	9.6	9.7	9.6	9.5	9.6	9.6	9.5	9.6	9.6	9.58	0.0422	0.52
12.70	12.8	12.8	12.6	12.7	12.7	12.7	12.8	12.8	12.7	12.8	12.74	0.0483	0.24
15.88	15.9	15.9	15.8	15.8	15.8	15.8	15.9	16	15.9	15.9	15.87	0.0316	0.06
19.05	19.0	18.9	18.9	19.0	18.9	19.0	19.1	19.0	19.0	19.1	18.99	0.0422	0.16
23.81	23.9	23.9	23.8	23.9	24.0	23.9	23.9	23.8	23.9	23.9	23.89	0.0316	0.34
MEAN RESULTS												**0.0338**	**3.28**

3.3. Real-World Tests

The prototype (see Figure 18) was put under real-world conditions measuring electrical lines connected to different systems in various environments: A kitchen within the university facilities, an electric water heater, and the main line within a household.



(**a**) (**b**)

Figure 18. Picture of the prototype: (**a**) Front, where the LoPy4 and the electronic subsystems can be seen; (**b**) back, where the battery, antenna, and clamp inductor are shown.

3.3.1. Test #1: 15-Minute Period in a Kitchen

The device monitored an electrical line providing power to a kitchen inside a university building (refrigerator, microwave ovens, water heater, coffee machines, and lighting). During a week period, there were no error messages and the battery level increased from 3.78 to 3.81 V. The effective average current measured during the test was nearly 4 A (920 W). With these energy consumption conditions, the system could work perpetually, and even the metering period could be reduced to around 8 min (see Figure 16).

3.3.2. Test #2: 5-Minute Period for an Electric Water Heater

The device was set to measure the electrical consumption of a water heater. This test was planned because the water heater might be considered as a pure resistive load. Further, its active consumption had to always be the same—which was 1.25 kW according to specifications. The metering period was set to 5 min in order to get more detailed information about the heater's active timing—having in mind that in this use case, the device would not be able to power itself.

In Figure 19, it can be observed that the consumption when the heater was working was similar to that of the specifications (5.5 A, equivalent to 1265 W at 230 V). The stand-by consumption, when resistors were not heating, was 0.1 A. Note that the stand-by consumption could be lower than that as 0.1 A was the metering resolution, as well as the smallest reading value the device could provide.

During the metering period shown in Figure 19 (48 h), the average consumption was around 0.52 A, far from the required ~5 A to ensure perpetual functioning as depicted in Figure 16. In fact, for this consumption behavior, it was not possible to assure a lifetime working condition even though the metering period was enormously stretched.

Taking this 48-h behavior as a permanent, repetitive pattern, we would have:

- 220 min of active consumption (5.5 A), which led to a harvested current of 0.86 mA according to Figure 14, providing 3.15 mAh every 48 h;
- 2660 min of stand-by consumption (0.1 A), which could not provide a harvested current.

The energy required for the device happened to be the same as that of Equation (3), but the stand-by time changed from 900 to 300 s:

$$\begin{gathered} \Psi'_1 = 11{\cdot}2.26 \text{ s}{\cdot}59.61 \text{ mA} = 1481.9 \text{ mAs} \\ \Psi'_2 = 1{\cdot}12.69 \text{ s}{\cdot}70.57 \text{ mA} = 895.53 \text{ mAs} \\ \Psi'_3 = 12{\cdot}300 \text{ s}{\cdot}21.56 \text{ µA} = 77.62 \text{ mAs} \\ \Psi' = \Psi'_1 + \Psi'_2 + \Psi'_3 = 2455.05 \text{ mAs} \end{gathered} \tag{7}$$

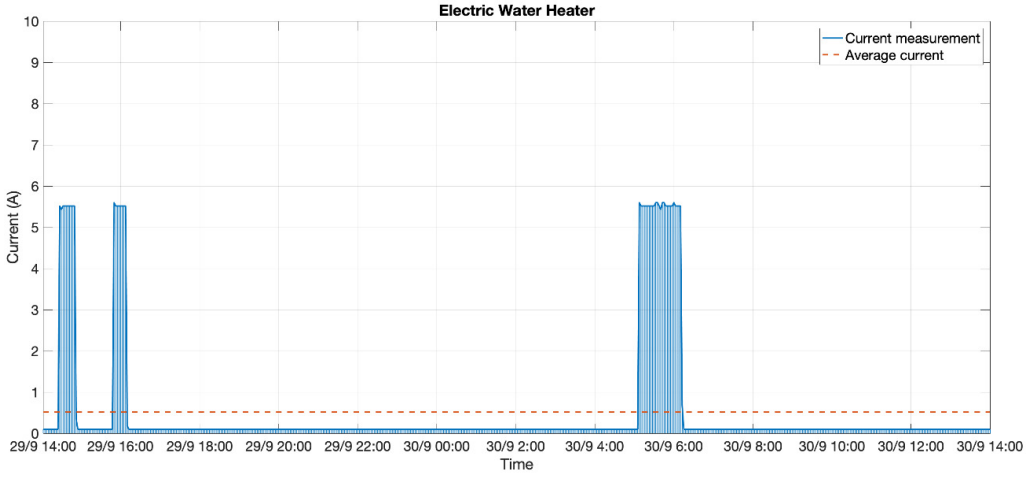


Figure 19. Electrical consumption of the water heater.

Energy computed from Equation (7) was required for each complete cycle, which occurred every hour. Hence, for 48 h, the energy required would be 117,842.40 mAs—32.73 mAh. This energy consumption was countervailed with the 3.15 mAh harvested in the same period, letting 29.58 mAh of net energy consumption every 48 h, which was equivalent to an average current of 0.62 mA.

Therefore, with the 2200-mAh battery used in the prototype—and assuming that a Li-ion battery would provide at least 3.5 V when the discharge capacity was 80%—the device could be autonomously running for 118 days as reckoned in Equation (8):

$$\text{T} = 0.8{\cdot}\frac{2200 \text{ mAh}}{0.62 \text{ mA}} = 2838.71 \text{ h} \cong 118 \text{ days} \tag{8}$$

3.3.3. Test #3: 5-Minute Period in a Household

In order to validate the system in other conditions, the device was put under test in an apartment monitoring its main electrical line. This apartment had a nominal power of 5.75 kW (25 A at 230 V), so it fit perfectly within the measure range of the prototype. After a 7-day electrical consumption dimension test, we assured the mean household consumption was above the designated 3.1 A. In fact, it was around 5.5 A (1265 W).

As the higher average current allowed for shorter metering/sending periods, both the firmware of the device and server parts were modified to collect measurements every 5 min. The device was installed and working as expected for two weeks. During this period, 4000+ current measures were taken and 330+ Sigfox messages sent.

As an example, a graph corresponding to a 24-h interval was depicted in Figure 20. It could be seen how the 5-min period allowed the detection of electrical consumption peaks, like those appearing around lunch and dinner hours. Even though the average consumption during this period was almost 6.1 A (green line), considering the effective harvesting range, the effective average consumption got to be 5.4 A (orange line)—also satisfying the 5 A lower limit for perpetual working measuring the current every 5 min.

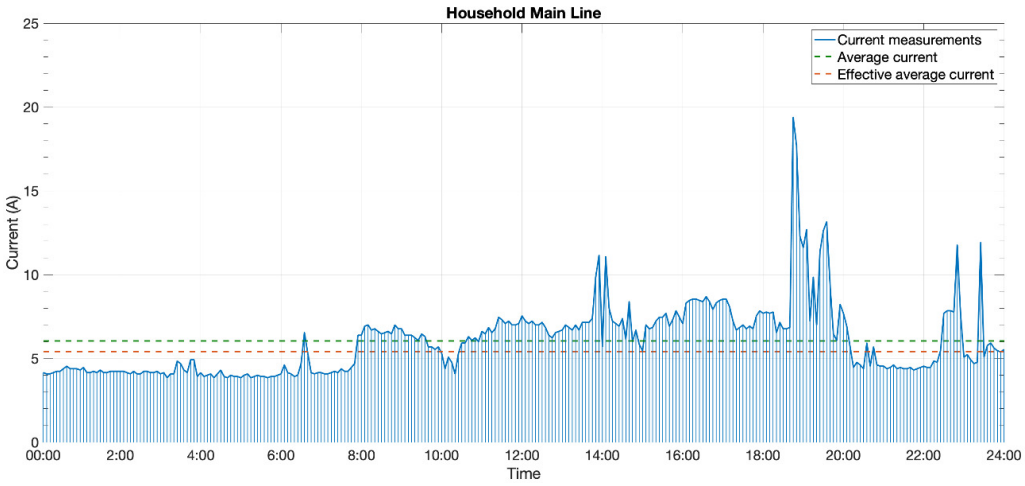


Figure 20. A day of current consumption in the third test scenario.

Figure 21 shows the prototype installed at the electrical panel board, where it was clamped to the house main switch. The power control switch (PCS)—left hand side—shows the 5.75 kW nominal power contracted for the house. The installation process did not require powering out, as the only necessary action was adjusting the clamp around the electrical wire.

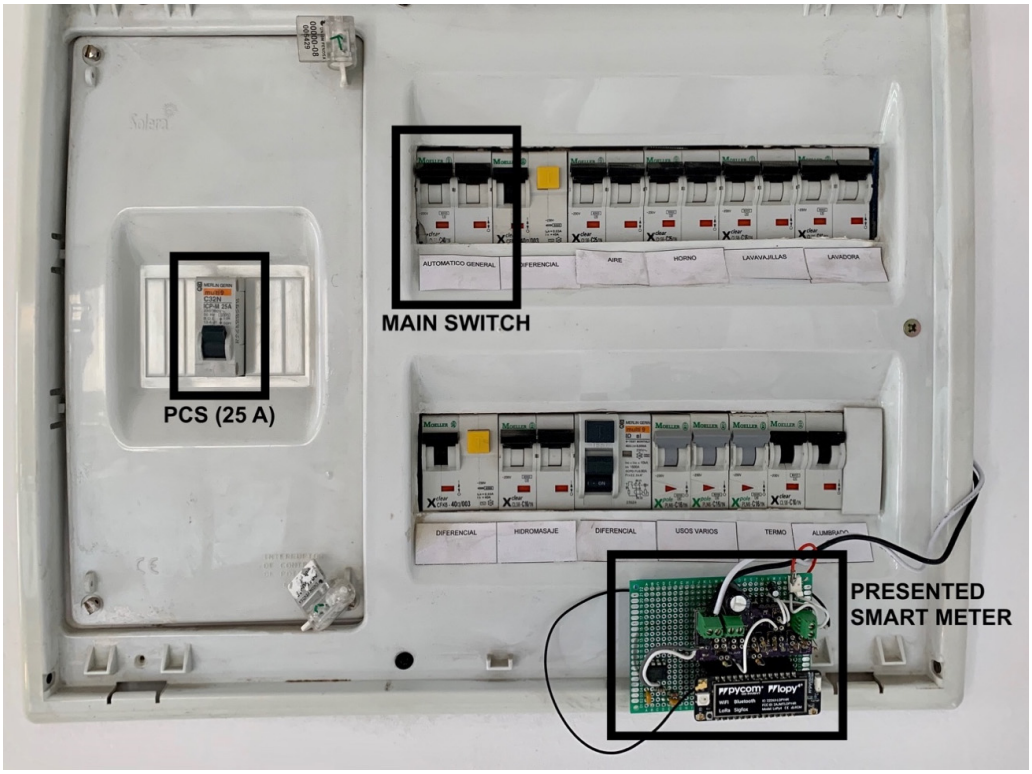


Figure 21. Installation of the device in the electrical panel of a household.

4. Conclusions

Bringing an easy way of metering power consumption was a crucial pillar to counteract the increase of energy consumption and CO_2 emissions. Having a record on consumptions, people's consumption patterns, and electricity flows, among other aspects, is essential to detect energy sinks, failures, and irresponsible habits. Such measures are especially relevant in rural areas and developing countries, where access to more advanced strategies, such as smart grids or demand response, are not feasible.

In this paper, a self-powered, Sigfox-compliant smart meter was presented. A fully functional design was demonstrated to work. From the theoretical analysis and real-world tests, we can assure that the device was able to properly meter current and, as long as conditions are complied, work perpetually acquiring current consumption data.

Its electronic design was developed in order to pursue an efficient, simple design, and meet three main requisites: Non-intrusive (easy installation), perpetual working (unending battery lifetime), and global accessibility (scenario versatility and low cost: About 80 € for the prototype, which would be lowered to 20–30 € for a chain-produced device).

However, this device was not a feasible solution for critical scenarios where either very accurate measures or a very short metering period were needed, due to both the energy harvesting technique and Sigfox limitations. Other wireless technologies or power sources would need to be evaluated and tested for such applications. For instance, 6LoWPAN for short distances or LoRaWAN for longer distances could be used if shorter metering periods were wished. Regarding the power supply, PV or vibration energy harvesting could be used together with MIEH if conditions helped it to achieve more usable power.

Regarding metering accuracy, although the overall error rate was about 3.3%, it was lowered to just around 0.8% if the range 0.5–25 A was considered. It is worth noting that, although 0–25 A was the whole metering range, the effective energy harvesting range was 2.2–6.4 A, so the line being metered had to comply with working conditions taking these limits into account, as detailed in Section 3.1 hereof. This range seemed fair for the most common residential scenarios, as it represented a usual current consumption range for a household. However, these limits might be modified, making circuital changes and redesigning the energy harvesting subsystem.

Future Adaptative Behavior of the Device

Taking into account that the device was intended for a variety of scenarios—average current, consumption peaks, periods with limited current like night-time, energy sampling frequency, etc.—we were interested in applying an adaptive algorithm to the system. The device could be aware of the current measures itself, hence varying the metering period accordingly without the need of a dedicated configuration for every scenario.

For instance, if during a period of time the consumption was almost constant and there was no need for much precision, some current measures could be missed, and the metering period extended. In this manner, energy consumption would be reduced, hence the battery saved. On the other hand, for periods where consumption was higher and variant, more measures could be taken provided that the battery level would recover as well.

Varying the metering period periodically came with strings attached regarding timestamps. With the current firmware, no timestamp was recorded along measurements. A time reference—be it a timestamp, period between measures, or whatsoever—is needed for proper time scheduling if the metering period is wished to be dynamic. This led to not always being able to send 12 measures per Sigfox message, since some payload were needed for time recording.

The device could also be aware of the precise battery level instead of only a $VBAT_{OK}$ threshold. This way, it could be prepared for recovering the battery level when the current is high enough, although it might lose battery charge in other moments when there is less current; however, a short metering period is necessary.

Author Contributions: Conceptualization, E.S., G.d.C., and A.S.; methodology, E.S. and G.d.C.; software and hardware, E.S.; validation, E.S. and G.d.C.; formal analysis, writing—original draft preparation, E.S; writing—review and editing, supervision, G.d.C.; project administration, funding acquisition, A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work is part of the CHIST-ERA research project "ABIDI: Context-aware and Veracious Big Data Analytics for Industrial IoT" and was funded by the State Research Agency (AEI) from the Ministerio de Ciencia e Innovación (MICINN) of Spain, grant number PCI2019-103762.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

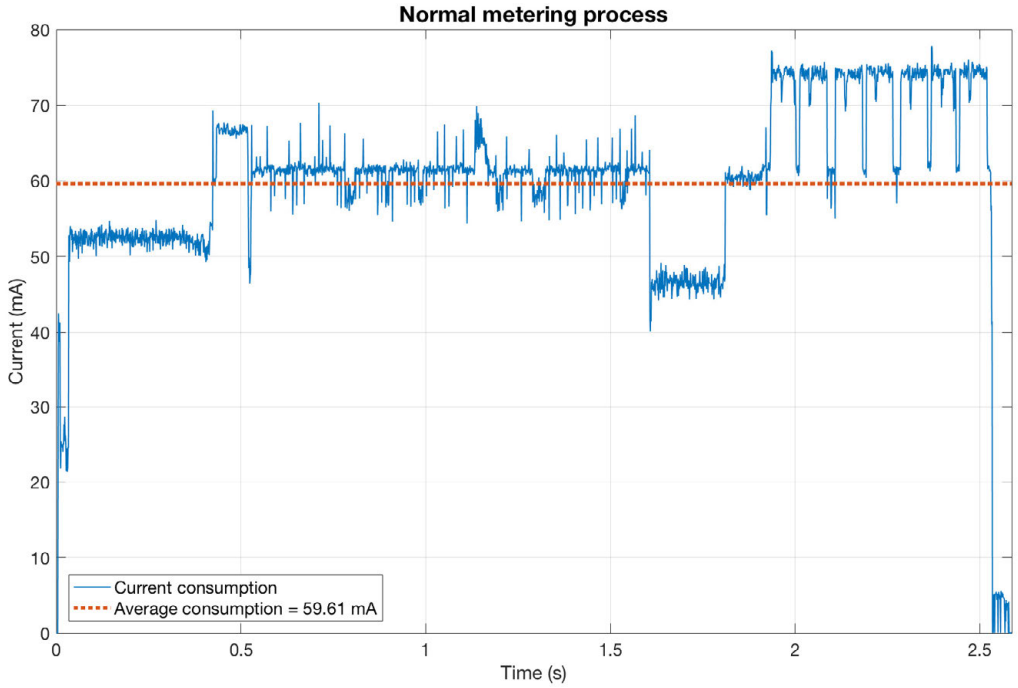


Figure A1. Detailed consumption for the device when a normal metering process occurs.

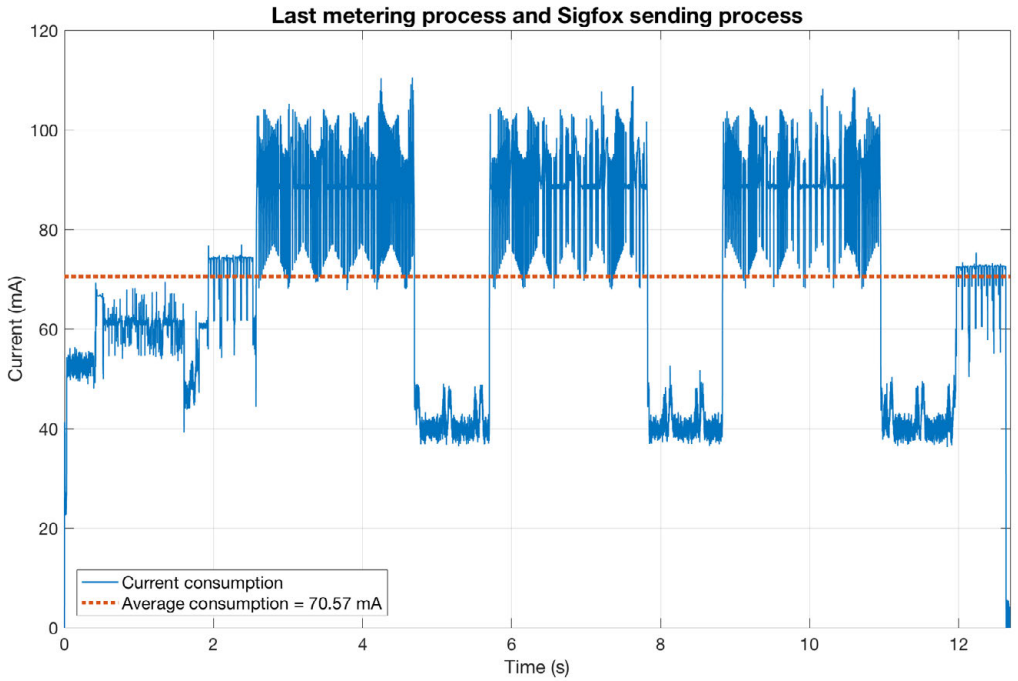


Figure A2. Detailed consumption for the device when a metering process makes the buffer full and the Sigfox message is sent. Notice the three big consumption peaks corresponding to the Sigfox transceiver sending the message thrice—approx. from 2.5 to 12 s.

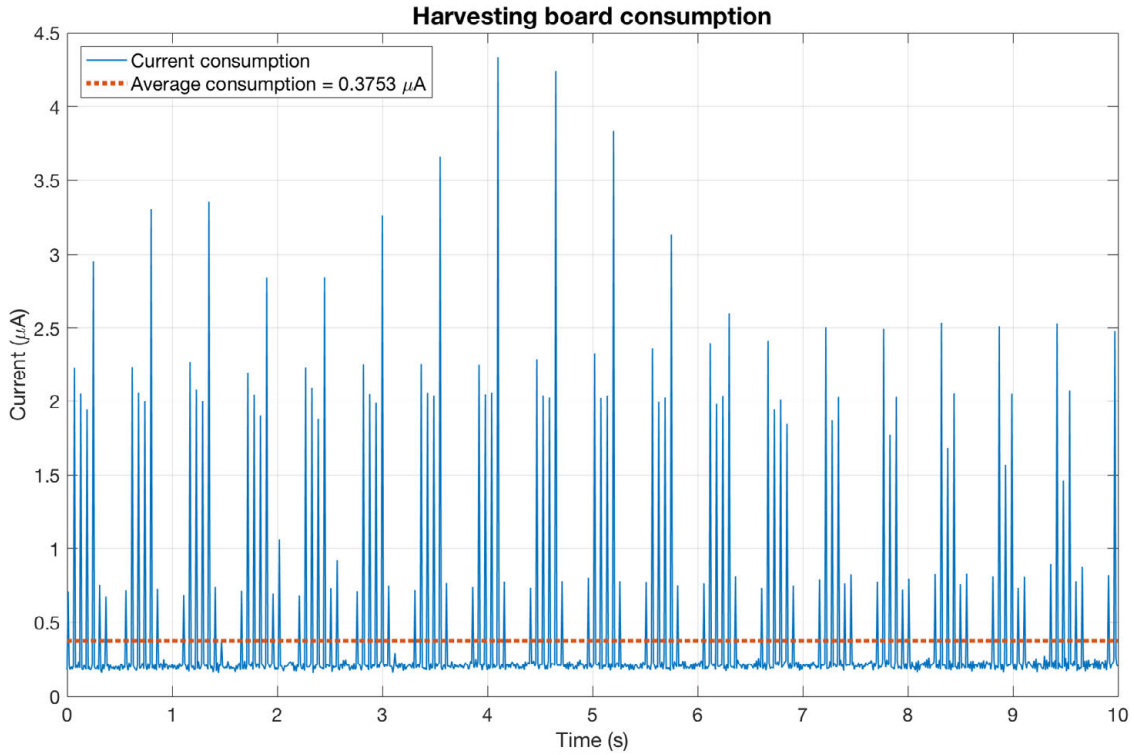


Figure A3. Detailed consumption for the energy harvesting subsystem.

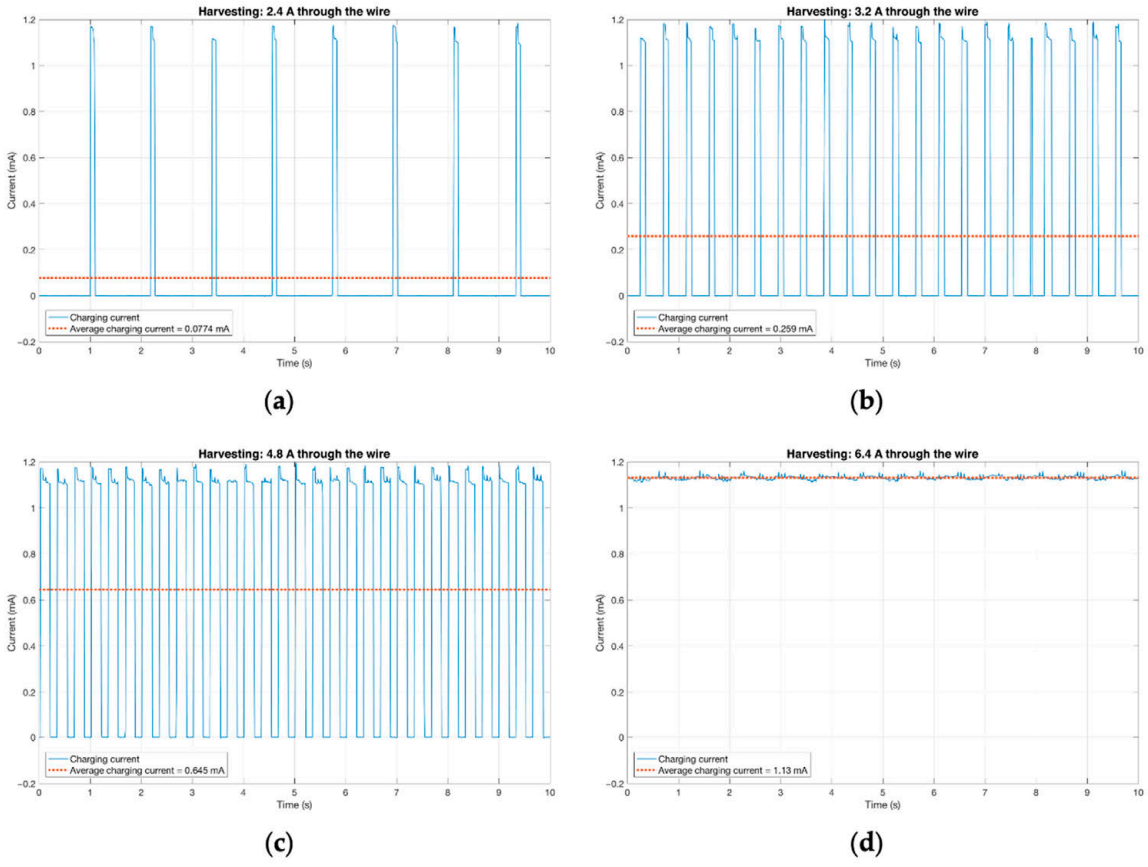


Figure A4. Current injected into the battery: (**a**) 2.4 A in the mains wire; (**b**) 3.2 A in the mains wire; (**c**) 4.8 A in the mains wire; (**d**) 6.4 A in the mains wire.

References

1. World Power Consumption|Electricity Consumption|Enerdata. Available online: https://yearbook.enerdata.net/electricity/electricity-domestic-consumption-data.html (accessed on 15 September 2020).
2. International Energy Agency Key World Energy Statistics 2020. 2020. Available online: https://www.iea.org/reports/key-world-energy-statistics-2020 (accessed on 15 September 2020).
3. European Comission, Joint Research Centre and Netherlands Environmental Assessment Agency EDGAR v4.3.2. 2017. Available online: https://edgar.jrc.ec.europa.eu/overview.php?v=432_GHG (accessed on 15 September 2020).
4. Benzi, F.; Anglani, N.; Bassi, E.; Frosini, L. Electricity Smart Meters Interfacing the Households. *IEEE Trans. Ind. Electron.* **2011**, *58*, 4487–4494. [CrossRef]
5. Depuru, S.S.S.R.; Wang, L.; Devabhaktuni, V.; Gudi, N. Smart meters for power grid—Challenges, issues, advantages and status. In Proceedings of the 2011 IEEE/PES Power Systems Conference and Exposition, Phoenix, AZ, USA, 20–23 March 2011; pp. 1–7.
6. Zheng, J.; Gao, D.W.; Li, L. Smart Meters in Smart Grid: An Overview. In Proceedings of the 2013 IEEE Green Technologies Conference (GreenTech), Denver, CO, USA, 4–5 April 2013; pp. 57–64.
7. Rámila, P.; Rudnick, H. Assessment of the Introduction of Smart Metering in a Developing Country. 10. Available online: http://hrudnick.sitios.ing.uc.cl/paperspdf/RamilaRudnick.pdf (accessed on 15 September 2020).
8. Janardhana, S.; Deekshit Shashikala, M.S. Challenges of smart meter systems. In Proceedings of the 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), Mysuru, India, 9–10 December 2016; pp. 78–82.
9. Sendin, A.; Simon, J.; Urrutia, I.; Berganza, I. PLC deployment and architecture for Smart Grid applications in Iberdrola. In Proceedings of the 18th IEEE International Symposium on Power Line Communications and Its Applications, Glasgow, UK, 30 March–2 April 2014; pp. 173–178.
10. Sendin, A.; Berganza, I.; Arzuaga, A.; Pulkkinen, A.; Kim, I.H. Performance results from 100,000+ PRIME smart meters deployment in Spain. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 145–150.
11. Chren, S.; Rossi, B.; Pitner, T. Smart grids deployments within EU projects: The role of smart meters. In Proceedings of the 2016 Smart Cities Symposium Prague (SCSP), Prague, Czech Republic, 26–27 May 2016; pp. 1–5.
12. Reinhardt, A.; Burkhardt, D.; Mogre, P.S.; Zaheer, M.; Steinmetz, R. SmartMeter.KOM: A low-cost wireless sensor for distributed power metering. In Proceedings of the 2011 IEEE 36th Conference on Local Computer Networks, Bonn, Germany, 4–7 October 2011; pp. 1032–1039.
13. CeDInt-UPM Industrial IoT IP Open Solution for Smart Production 2017. Available online: https://www.cedint.upm.es/en/infrastructure/industry-40-lab (accessed on 15 September 2020).
14. Woo, C.K.; Ho, T.; Shiu, A.; Cheng, Y.S.; Horowitz, I.; Wang, J. Residential outage cost estimation: Hong Kong. *Energy Policy* **2014**, *72*, 204–210. [CrossRef]
15. Praktiknjo, A.J.; Hähnel, A.; Erdmann, G. Assessing energy supply security: Outage costs in private households. *Energy Policy* **2011**, *39*, 7825–7833. [CrossRef]
16. Moghe, R.; Yang, Y.; Lambert, F.; Divan, D. Design of a low cost self powered "Stick-on" current and temperature wireless sensor for utility assets. In Proceedings of the 2010 IEEE Energy Conversion Congress and Exposition, Atlanta, GA, USA, 12–16 September 2010; pp. 4453–4460.
17. Cai, F.; Farantatos, E.; Huang, R.; Meliopoulos, A.P.S.; Papapolymerou, J. Self-powered smart meter with synchronized data. In Proceedings of the 2012 IEEE Radio and Wireless Symposium, Santa Clara, CA, USA, 15–18 January 2012; pp. 395–398.
18. Porcarelli, D.; Balsamo, D.; Brunelli, D.; Paci, G. Perpetual and Low-cost Power Meter for Monitoring Residential and Industrial Appliances. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 18–22 March 2013; pp. 1155–1160.
19. Han, J.; Hu, J.; Yang, Y.; Wang, Z.; Wang, S.X.; He, J. A Nonintrusive Power Supply Design for Self-Powered Sensor Networks in the Smart Grid by Scavenging Energy From AC Power Line. *IEEE Trans. Ind. Electron.* **2015**, *62*, 4398–4407. [CrossRef]

20. Paprotny, I.; Leland, E.; Sherman, C.; White, R.M.; Wright, P.K. Self-powered MEMS sensor module for measuring electrical quantities in residential, commercial, distribution and transmission power systems. In Proceedings of the 2010 IEEE Energy Conversion Congress and Exposition, Atlanta, GA, USA, 12–16 September 2010; pp. 4159–4164.
21. Saavedra, E.; del Campo, G.; Santamaria, A. A Novel, Self-Powered, Non-Intrusive, Sigfox-Enabled Smart Meter for Challenging Scenarios. In Proceedings of the 2020 16th International Conference on Intelligent Environments (IE), Madrid, Spain, 20–23 July 2020; pp. 115–118.
22. Technology|Sigfox. Available online: https://www.sigfox.com/en/what-sigfox/technology (accessed on 15 September 2020).
23. Del Campo, G.; Gomez, I.; Cañada, G.; Piovano, L.; Santamaria, A. Guidelines and criteria for selecting the optimal low-power wide-area network technology. In *LPWAN Technologies for IoT and M2M Applications*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 281–305. ISBN 978-0-12-818880-4.
24. Ulukus, S.; Yener, A.; Erkip, E.; Simeone, O.; Zorzi, M.; Grover, P.; Huang, K. Energy Harvesting Wireless Communications: A Review of Recent Advances. *IEEE J. Sel. Areas Commun.* **2015**, *33*, 360–381. [CrossRef]
25. Gunathilaka, W.M.D.R.; Dinesh, H.G.C.P.; Gunasekara, G.G.C.M.; Narampanawe, K.M.M.W.N.B.; Wijayakulasooriya, J.V. Ambient Radio Frequency energy harvesting. In Proceedings of the 2012 IEEE 7th International Conference on Industrial and Information Systems (ICIIS), Chennai, India, 6–9 August 2012; pp. 1–5.
26. Bourgoine, N. Linear Technology—Journal of Analog Innovation. 2011. Available online: https://www.analog.com/media/en/technical-documentation/lt-journal-article/LTJournal-V21N1-2011-04.pdf (accessed on 15 September 2020).
27. Howells, C.A. Piezoelectric energy harvesting. *Energy Convers. Manag.* **2009**, *50*, 1847–1850. [CrossRef]
28. Porcarelli, D.; Brunelli, D.; Benini, L. Clamp-and-measure forever: A MOSFET-based circuit for energy harvesting and measurement targeted for power meters. In Proceedings of the 5th IEEE International Workshop on Advances in Sensors and Interfaces IWASI, Bari, Italy, 13–14 June 2013; pp. 205–210.
29. Drezet, C.; Kacem, N.; Bouhaddi, N. Design of a nonlinear energy harvester based on high static low dynamic stiffness for low frequency random vibrations. *Sens. Actuators Phys.* **2018**, *283*, 54–64. [CrossRef]
30. Ravindran, S.K.T.; Huesgen, T.; Kroener, M.; Woias, P. A self-sustaining pyroelectric energy harvester utilizing spatial thermal gradients. In Proceedings of the 2011 16th International Solid-State Sensors, Actuators and Microsystems Conference, Beijing, China, 5–9 June 2011; pp. 657–660.
31. Jordan, E.C.; Balmain, K.G. *Electromagnetic Waves and Radiating Systems*; Prentice-Hall: Upper Saddle River, NJ, USA, 1968.
32. Hayt, W. *Engineering Electromagnetics*; McGraw-Hill: New York, NY, USA, 1989.
33. Magnetic Hysteresis. Wikipedia 2020. Available online: https://en.wikipedia.org/wiki/Magnetic_hysteresis (accessed on 15 September 2020).
34. MicroPython—Python for Microcontrollers. Available online: http://micropython.org/ (accessed on 15 September 2020).
35. ESP32 Datasheet. Available online: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf (accessed on 15 September 2020).
36. LoPy4 Datasheet. Available online: https://docs.pycom.io/gitbook/assets/specsheets/Pycom_002_Specsheets_LoPy4_v2.pdf (accessed on 15 September 2020).
37. CBRHDSH1-40L Datasheet. Available online: https://my.centralsemi.com/datasheets/CBRHDSH1-40L.PDF (accessed on 15 September 2020).
38. LBA710 Datasheet. Available online: https://www.ixysic.com/home/pdfs.nsf/www/LBA710.pdf/$file/LBA710.pdf (accessed on 15 September 2020).
39. BQ25504 Datasheet. Available online: https://www.ti.com/lit/ds/symlink/bq25504.pdf (accessed on 15 September 2020).
40. TPS62122 Datasheet. Available online: https://www.ti.com/lit/ds/symlink/tps62122.pdf (accessed on 15 September 2020).
41. Node.js Node.js. Available online: https://nodejs.org/en/about/ (accessed on 15 September 2020).
42. Express—Node.js Web Application Framework. Available online: https://expressjs.com/ (accessed on 15 September 2020).

43. Raspberry Pi 4 Product Brief. Available online: https://static.raspberrypi.org/files/product-briefs/200521+Raspberry+Pi+4+Product+Brief.pdf (accessed on 15 September 2020).
44. InfluxDB: Purpose-Built Open Source Time Series Database. Available online: https://www.influxdata.com/ (accessed on 15 September 2020).
45. InfluxDB 1.X: Open Source Time Series Platform. Available online: https://www.influxdata.com/time-series-platform/ (accessed on 15 September 2020).

II. DOI: 10.3390/s21227433

The Smart Meter Challenge: Feasibility of Autonomous Indoor IoT Devices Depending on Its Energy Harvesting Source and IoT Wireless Technology

Sensors 2021, 21, 7433

https://doi.org/10.3390/ s21227433

Pages 66–89 present the original manuscript as published

sensors

MDPI

Article

The Smart Meter Challenge: Feasibility of Autonomous Indoor IoT Devices Depending on Its Energy Harvesting Source and IoT Wireless Technology

Edgar Saavedra *, Laura Mascaraque, Gonzalo Calderon, Guillermo del Campo and Asuncion Santamaria

CeDInt-UPM, Universidad Politécnica de Madrid, Campus de Montegancedo, Pozuelo de Alarcón, 28223 Madrid, Spain; lmascaraque@cedint.upm.es (L.M.); gcalderon@cedint.upm.es (G.C.); gcampo@cedint.upm.es (G.d.C.); asun.santamaria@upm.es (A.S.)

* Correspondence: e.saavedra@upm.es

Abstract: Most smart meters are connected and powered by the electric mains, requiring the service interruption and qualified personnel for their installation. Wireless technologies and energy harvesting techniques have been proved as alternatives for communications and power supply, respectively. In this work, we analyse the energy consumption of the most used IoT wireless technologies nowadays: Sigfox, LoRaWAN, NB-IoT, Wi-Fi, BLE. Smart meters' energy consumption accounts for metering, standby and communication processes. Experimental measurements show that communication consumption may vary upon the specific characteristics of each wireless communication technology—payload, connection establishment, transmission time. Results show that the selection of a specific technology will depend on the application requirements (message payload, metering period) and location constraints (communication range, infrastructure availability). Besides, we compare the performance of the most suitable energy harvesting (EH) techniques for smart meters: photovoltaic (PV), radiofrequency (RF) and magnetic induction (MIEH). Thus, EH technique selection will depend on the availability of each source at the smart meter's location. The most appropriate combination of IoT wireless technology and EH technique must be selected accordingly to the very use case requirements and constraints.

Keywords: smart meter; Internet of Things; energy harvesting; energy efficiency; LPWAN; Sigfox; LoRaWAN; NB-IoT; Wi-Fi; BLE; IoT; IIoT

Citation: Saavedra, E.; Mascaraque, L.; Calderon, G.; del Campo, G.; Santamaria, A. The Smart Meter Challenge: Feasibility of Autonomous Indoor IoT Devices Depending on Its Energy Harvesting Source and IoT Wireless Technology. *Sensors* **2021**, *21*, 7433. https://doi.org/10.3390/s21227433

Academic Editors: Carlo Trigona, Olfa Kanoun and Slim Naifar

Received: 20 October 2021
Accepted: 6 November 2021
Published: 9 November 2021

1. Introduction

In the last few years, the number of IoT devices has grown significantly, so does the spending in IoT-related fields, which is expected to increase by 24% in 2021 [1]. Moreover, the global IoT market will be worth more than 1200 billion ($\times 10^9$) euros by 2027 [2]. It is estimated that the IoT was born in 2008, with the things-to-people ratio growing from 0.08 in 2003 to 1.84 in 2010 [3], and leading to almost 4.5 in 2021, with 35 billion devices connected [4], currently adding more than 120 new devices per second.

IoT devices may be used for a wide range of applications: healthcare, ambient conditions monitoring, workout tracking, infrastructures monitoring, failure prevention, smart metering, etc. The latter is the one we focus on in this work. Following our research presented in [5], in which an autonomous Sigfox smart meter was presented, in this paper, we analyse the feasibility of indoor IoT nodes. Specifically, we focus on smart meters with different energy harvesting (EH) sources and wireless technologies—although it might be extrapolated to any kind of indoor sensor.

Regarding the smart meter field, most of them are directly connected to the mains—such as those installed by electric companies—[6–8], so an intrusion in the electrical panel is required for installation, which leads to the requirement of a specialist and a temporary interruption in power supply. All these cons increase costs and prevent new deployments [9,10].

Considering the great growth in the IoT industry, the ability to keep smart meters autonomous, adapting their working conditions by their scenario necessities is crucial to encourage companies—and people—to adopt smart meters. Thus, we are about to compare the main trendy wireless communication technologies workable in smart meters—Sigfox, LoRaWAN, NB-IoT, Wi-Fi, BLE—for an extensive variety of scenarios. At the same time, we compare the most adequate EH sources for indoor wireless sensors: photovoltaic (PV), radiofrequency (RF); and specifically for smart meters: magnetic induction (MIEH). Based on metering application requisites and smart meter location constraints, this work aims to help smart meters' developers and adopters with a roadmap to select the most suitable wireless communication technologies and energy harvesting techniques.

The rest of the paper is organised as follows: Section 2 describes the smart meter under consideration for this review, characterising both its consumption and working principle. Section 3 assesses the actual electrical consumption for each wireless technology in the spotlight. In Section 4, we sum up the existing literature to provide data on EH generations for every technique. Finally, in Section 5, the feasibility of different combinations between IoT technologies and EH sources are discussed, supported by a brief conclusion in Section 6.

2. Targeted Smart Meter

The smart meter used in the development of this work is inspired by the one we developed in [5], except for the EH Subsystem (see Figure 1), which is removed and characterised accordingly as EH source in Section 4. In this section, we will briefly explain the main characteristics of the smart meter.

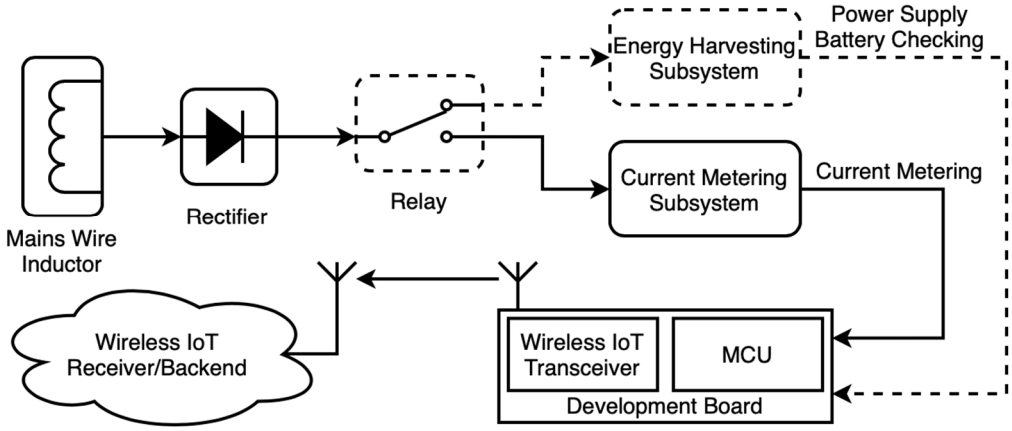


Figure 1. General block-diagram of the smart meter under consideration.

2.1. Working Principle

The working principle of the smart meter is that it is event-driven, with a variable metering period (*A* minutes) depending on the working conditions. Current measurements are stored in a buffer (sized to *N* measurements) and then sent when the buffer is full—see Figure 2. One measurement is 1 byte in size, as it is encoded in tenths on amperes (dA) with 1 dA (0.1 A) precision, which would allow measurements between 0 and 255 dA (0–25.5 A).

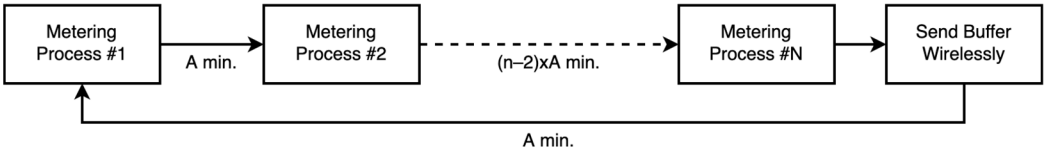


Figure 2. Graphical representation of the main behaviour of the smart meter.

This buffer is sent to the corresponding wireless receiver depending on the wireless technology that we are testing. It may be a base station that sends the data to a backend

(Sigfox, NB-IoT), an ad-hoc wireless gateway/host (LoRaWAN, Wi-Fi), or a receiver device scanning messages (BLE).

As well as the metering period may be changed based on the scenario conditions, so is the buffer. In the original design, the buffer was stated to 12 measurements due to Sigfox constrains [5], and the metering period was 15 min first, with latter tests of 5-min periods.

In this work, as other wireless technologies are used, the buffer size and the period may vary and adapt to the characteristics of each wireless technology.

2.2. Development Board

The development used for the smart meter is a FiPy [11]. This board provides Sigfox, LoRaWAN, NB-IoT, Wi-Fi and BLE in the same device, thus making the comparison between wireless technologies easier, as the basal consumption of the board is the same with no regard to the wireless technology under study. The microcontroller (MCU) is an Xtensa dual-core 32-bit LX6, which is programmed in MicroPython.

Figure 3 shows the basic layout for the five different wireless technologies embedded into the development board. Being the smart meter workable across different technologies makes the server ubiquitous and interoperable between smart metering instances—be they any of the aforementioned wireless technologies.

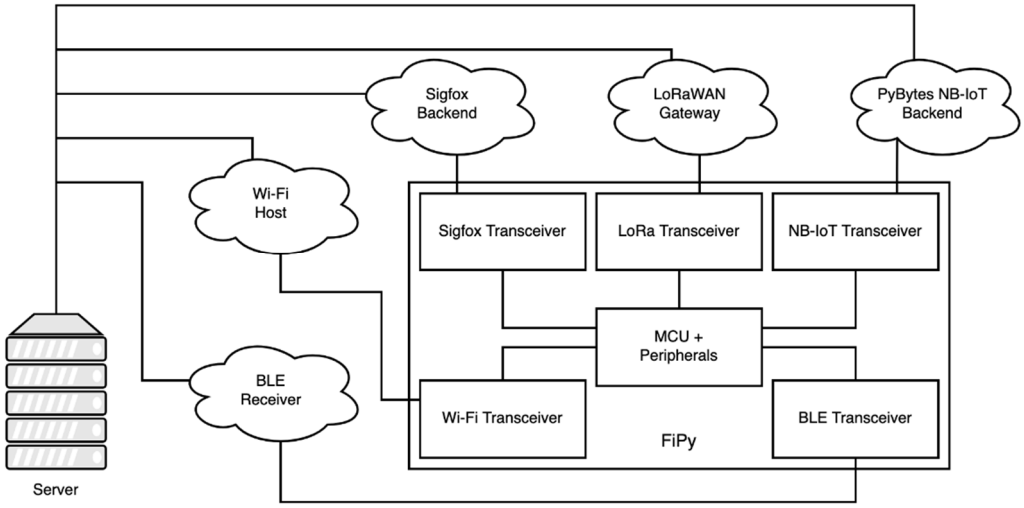


Figure 3. Layout for the five different wireless technologies under consideration.

2.3. Current Metering

The metering range is 0–25 A as it is an adequate range for most domestic scenarios. However, this range is easily adjusted by making small changes in the current metering subsystem [5], and it is not crucial in the object of this paper.

The Metering Subsystem is made as one can see in Figure 4. It is based on a voltage divider to convert the incoming current-proportional signal from the current probe into an ADC-measurable voltage signal. As depicted in Figure 2, the signal outcoming the current probe is first rectified. This allows a simpler circuit design for both current metering and energy harvesting (MIEH).

Resistors were adjusted accordingly to set the proper metering range within the ADC input range.

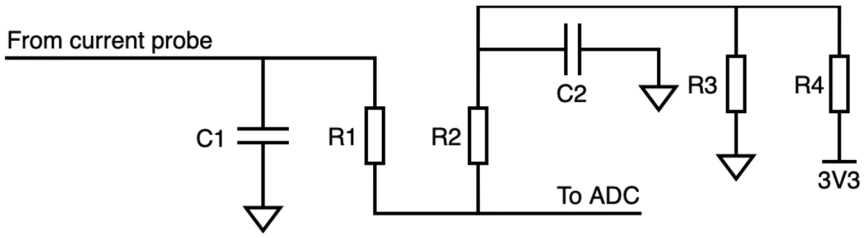


Figure 4. Conceptual schematic of the current metering subsystem.

2.4. Metering Consumption

Considering the functioning principle described in Section 2.1 hereof, the specific metering—data communication apart—consumption may be: (1) that coming from every metering process, and (2) stand-by time between metering processes:

1. The consumption due to the metering process will be the same indistinctively to the wireless technology used, as no wireless transceiver is turned on for current metering and the device is always the same: 44.16 mA during 2.55 s, i.e., 112.77 mAs—see Figure A1.
2. The stand-by consumption is a constant current value that is demanded during the deep-sleep period of the device, i.e., when the device is waiting for the timer to expire, and another current measurement is about to be done—this time is A minutes in Figure 2: 16.28 µA during A min, i.e., $A \times 1.29$ mAs. Datasheet [11] claims a deep-sleep current consumption of 25 µA at 3.3 V, fact that agrees with our 16.28 µA at 5 V.

These two different consumptions will compute for the energy consumption of the very smart meter. Measurements taken with the aid of a Keysight/Agilent 34410A multimeter [12] at 5 V.

In this manner, we split apart the consumption due to the wireless IoT technology—which is evaluated in Section 3 and will vary across protocols. The consumption of the wireless transmission happens eventually when the measurements buffer is full—corresponding to #N in Figure 2.

3. IoT Wireless Technologies Characterisation

In this section, the five IoT wireless technologies under study are evaluated. As the main objective of this work is to evaluate the feasibility of different wireless technologies according to their energy consumption, current consumption measurements are taken for each technology: Sigfox, LoRaWAN, NB-IoT, Wi-Fi and BLE.

We have selected these technologies as they tend to be the most used, supported, and well-known IoT wireless technologies nowadays. Furthermore, they represent a wide range of characteristics: some of them need to deploy a dedicated infrastructure (LoRaWAN, Wi-Fi, BLE) and others provide their own network for receiving messages (Sigfox, NB-IoT); Wi-Fi and BLE provide a short range whilst the others provide a very long range; they differ as well in data rate, payload, or the necessity of a handshake to send messages. These facts make the energy consumption comparison tougher as their behaviour is not equivalent. This will be discussed in Section 5.

For consumption portrayal, message payloads from 12 bytes (Sigfox limitation) up to 768 bytes will be considered—double-fold increments. Furthermore, the consumption of the handshake or communication establishment for those technologies requiring it is considered apart from that of the transmission itself.

Then, we will evaluate the choice of using larger messages with the technologies supporting that. Several protocols provide very high data rates, which may lead to an increase in energy efficiency provided that larger messages are used, as they will deliver fast, avoiding headers and eventual handshakes. Table 1 [13–15] summarises some critical points for the wireless technologies under consideration—for the transceivers embedded in our development board.

Table 1. Summary for some critical characteristics of the IoT Wireless technologies.

Technology	Data Rate	Payload [1]	Handshake
Sigfox	100 bps	12 B	No
LoRaWAN	5470 bps	222 B	Yes
NB-IoT	250 kbps	768+ B	Yes
Wi-Fi	16 Mbps	768+ B	Yes
BLE	1 Mbps	25 B	No

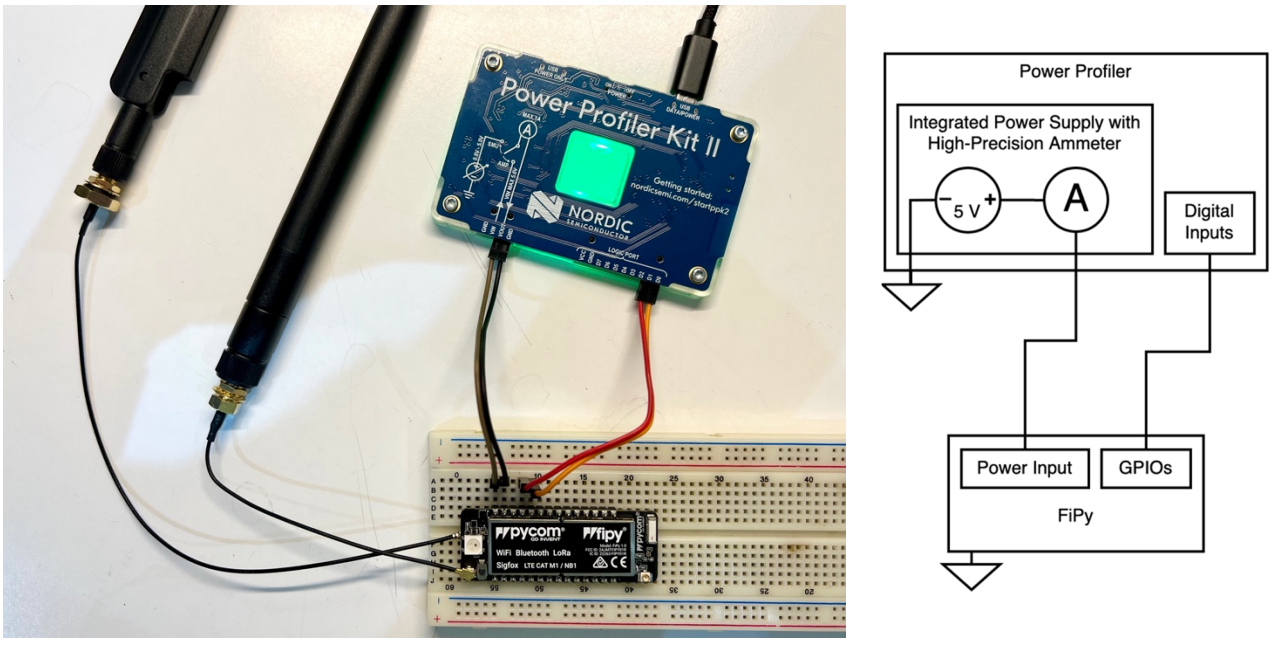
[1] User-available payload per message/packet.

Depending on the message size, a different number of transmissions will be needed, due to the maximum payload allowed by each technology for a single message. Hence, the consumptions required for each technology would be determined by the consumption of the connection establishment plus X times that of the message transmission, depending on the number of messages required—see Table 2.

Table 2. Number of transmissions needed for each wireless technology for different payloads.

Technology	24-Byte	48-Byte	96-Byte	192-Byte	384-Byte	768-Byte
Sigfox	2	4	8	16	32	64
LoRaWAN	1	1	1	1	2	4
NB-IoT	1	1	1	1	1	1
Wi-Fi	1	1	1	1	1	1
BLE	1	2	4	8	16	31

For current consumption characterisation, the equipment we used is a Nordic Semiconductor Power Profiler Kit II [16], which provides current sample rates of up to 100 kS/s (thousand-samples per second) with a resolution of up to 200 nA. Every current measurement is made with just the development board attached to the Power Profiler, using its embedded power source and high-precision ammeter, and only the essential peripherals turned on (see Figure 5).



(**a**) (**b**)

Figure 5. Current measurement setup: (**a**) Real picture of the Power Profiler Kit II measuring current consumption of the development board; (**b**) Block-diagram of the current measurement setup.

So as to evaluate the actual accuracy of the Power Profiler, we set a test bed as described in Appendix B, Figure A11. The set was excited with a 100 Hz sinusoidal wave, characterised at the same time by the Power Profiler and a Keysight/Agilent 34410A multimeter—device taken as reference. Readings from the multimeter claim:

- I_{DC} = 92.825 mA
- I_{AC} = 20.539 mA_{RMS}

Considering that we are working with a sinusoidal wave, its peak value—which is that happened at 100 Hz—can be calculated as in Equation (1):

$$I_{100\ Hz} = I_{AC_{RMS}} \times \sqrt{2} = 20.539 \times \sqrt{2} = 29.05\ mA \quad (1)$$

The signal measured by the Power Profiler for 10 periods is depicted in Figure A12, as well as its Fast Fourier Transform (FFT)—performed with the aid of Matlab. In the FFT plot, we can see that there are only noticeable current values for 0 Hz (DC) and 100 Hz. These values are, with their relative errors (ε):

- $I_{0\ Hz}$ = 90.61 mA; ($\varepsilon_{0\ Hz}$ = 2.4%)
- $I_{100\ Hz}$ = 28.71 mA; ($\varepsilon_{100\ Hz}$ = 1.3%)

Besides, we extracted the value of the signal in 1000 same-phase sampling points (0 radians, which corresponds to a sine wave's nulls). For this set of values, the standard deviation was reckoned, happening to be 0.2492 mA for a mean value of 90.61 mA (0.3%).

Table 3 sums up the consumption for every technology characterised, which can be seen in detail in the following subsections and Appendix A. For the consumption characterisation, we measured the current demand for each wireless technology synchronously with the FiPy's firmware. This was made by triggering a digital signal during the transmission process. The consumption appearing in Table 3 corresponds to an average of a cluster of 100 current measurements for each technology. Range for different measurements is less than 5%, which is an acceptable tolerance value for characterisation taking into account the accuracy of the Power Profiler.

Table 3. Summary of energy consumptions for IoT wireless technologies (12-byte messages).

Technology	MTC (mA)	ETC (mA)	Establishment Consumption (mAs)	Transmission Consumption (mAs)	Total Consumption (mAs)
Sigfox [1]	<59.4	53.1	0	804.80	804.80
LoRaWAN	<59.4	62.5	256.73	6.33	263.06
NB-IoT	<277.2	141.2	4341.9	8.88	4350.8
Wi-Fi	118.8	109.9	198.46	3.40	201.86
BLE	85.8	95.9	51.98	1.01	52.99

[1] Sigfox's ETC is not calculated with the average consumption of the transmission process (Appendix A), but with the average current demand of one of the three transmissions occurred in Sigfox (90.1 mA), so as to not include the period between transmissions in the calculus.

In this table, we also depict the current demand of the development board's transceivers for each technology according to the manufacturer (Wi-Fi/BLE [17], LoRa/Sigfox [18], NB-IoT [11]), converted to 5 V (MTC). The current demands provided by the manufacturers do not always comply with our specific working characteristics, reason why they are shown as an upper limit—nevertheless, these data are useful to check that measured consumptions are in a reasonable margin within those of the manufacturer:

- Sigfox/LoRa transceiver's current demand is specified for +17 dBm, but not for +14 dBm, which is our case.
- NB-IoT transceiver's current demand is only specified for a possible maximum 1.5 W power, but actual power profile would depend upon network conditions.

The idle consumption of the board was also characterised and happened to be around 37 mA. This current must be subtracted to that measured for the whole board when transmitting (Appendix A) in order to isolate the specific experimental consumption of

the transceiver's transmission (ETC), since idle current demand is due to the development board's MCU and peripherals before wireless transceivers are activated. However, this is not the case for Wi-Fi and BLE as the transceiver is embedded into the MCU, and the consumption data provided by the manufacturer take the whole board into consideration.

The consumption coming from connection establishment (or just modem initialisation) is also depicted in Table 3. This consumption is relevant, as the device will need to do this process when waking up from deep sleep for the technologies requiring it.

In the upcoming subsections, each technology will be deeply analysed. First, the consumption for the initial 12-byte-payload message is explained; then, a table shows the measured consumptions for larger payload sizes for each technology. Detailed consumption figures are attached in Appendix A.

3.1. Sigfox

The Sigfox 12-byte transmission process lasts 10.6 s with an average current consumption of 75.93 mA, which leads to an energy consumption of 804.80 mAs. Sigfox does not need a handshake for the connection to be established, so this energy is the only needed when sending a message.

In the consumption plot (Figure A2), it is clearly noticeable the three transmissions in three different carriers that Sigfox performs to ensure delivery: the three big waves that last about two seconds, which is the time on air of a 12-byte Sigfox message.

For larger payloads, check Table 4.

Table 4. Summary of energy consumptions (mAs) for Sigfox.

Sigfox Payload (Bytes)	12	24	48	96	192	384	768
Establishment consumption	0	0	0	0	0	0	0
Number of transmissions	1	2	4	8	16	32	64
Transmission consumption	804.80	804.80	804.80	804.80	804.80	804.80	804.80
Total consumption	804.80	1609.6	3219.2	6438.4	12,876.8	25,753.6	51,507.2

3.2. LoRaWAN

LoRaWAN allows different configurations regarding spreading factor (SF) and bandwidth. In this work, we assume the most used in the LoRa field is the proper one to use, with corresponds to using an SF7 with 125 kHz. Other SF could be used if messages were lost, but this configuration works well for us whilst providing the fastest data rates, which means less time on air, thus less energy spent.

With this set, the LoRaWAN 12-byte transmission process lasts for 63.63 ms, with an average consumption of 99.51 mA, which leads to an energy consumption of 6.33 mAs for the LoRaWAN process (see Figure A3). However, it is important to note that after transmission, the LoRa transceiver may keep activated for a while to be able to receive messages. We will not consider that phenomenon here as we truly think that it is not necessary for message transmission—the main purpose of this work is comparing only the uplink channel.

LoRaWAN needs connection establishment before sending messages. When the device is put in a deep sleep mode, the connection needs to be done again as the device loses its previous state. The consumption for the connection establishment can be seen in Figure A4. This process lasts 5.2 s with an average consumption of 49.42 mA, which leads to an energy consumption of 256.73 mAs.

Thus, the full energy consumption for a LoRaWAN 12-byte message is 263.06 mAs—considering both the establishment and the transmission. For larger payloads, check Table 5.

Table 5. Summary of energy consumptions (mAs) for LoRaWAN.

LoRaWAN Payload (Bytes)	12	24	48	96	192	384	768
Establishment consumption	256.73	256.73	256.73	256.73	256.73	256.73	256.73
Number of transmissions	1	1	1	1	1	2	4
Transmission consumption	6.33	9.34	12.75	20.79	36.81	36.81	36.81
Total consumption	263.06	266.07	269.48	277.52	293.54	330.35	403.97

3.3. NB-IoT

The NB-IoT 12-byte transmission process lasts for 49.8 ms, with an average current of 178.2 mA, which leads to an energy consumption of 8.88 mAs (see Figure A5). The consumption for NB-IoT does not increase much as message payload increases—as measured in Table 6. This wireless technology provides very high data rates which makes the time spent not definitely increase when we use small byte-sized increases.

Table 6. Summary of energy consumptions (mAs) for NB-IoT.

NB-IoT Payload (Bytes)	12	24	48	96	192	384	768
Establishment consumption	4341.9	4341.9	4341.9	4341.9	4341.9	4341.9	4341.9
Number of transmissions	1	1	1	1	1	1	1
Transmission consumption	8.88	8.88	8.88	9.13	9.37	9.87	11.15
Total consumption	4350.8	4350.8	4350.8	4351.0	4351.3	4351.8	4353.1

NB-IoT takes a long time to establish the connection. The modem first needs to be initialised, then attach to the network, then connect to the service. The time needed for attaching and connecting to the network can vary depending on the NB-IoT network conditions (Vodafone Spain), so will the energy consumption. An average process is shown in Figure A6, with an energy consumption of 4342 mAs.

We can see that the consumption coming from the transmission is negligible considering that from the connection establishment (8.88 mAs vs. 4341.9 mAs), with a total of 4350.8 mAs for a 12-byte message. For larger payloads, check Table 6.

3.4. Wi-Fi

The Wi-Fi transmission process lasts for 30.98 ms, with an average current of 109.0 mA, which leads to an energy consumption of 3.4 mAs. The Wi-Fi consumption does not depend on the packet size, as it is meant for larger messages. The time it takes for the transmission to be made is not consistent, however, as it depends on the current network traffic and network characteristics. For illustration, let us consider an average transmission as in Figure A7.

Wi-Fi needs to establish a connection before sending messages. The modem needs to be reinitialised every time the device wakes from a sleep mode as well. This time will vary depending on real working conditions as the Wi-Fi connection time is not only dependant on the IoT device. In Figure A8, the consumption for modem initialisation and connection establishment can be seen.

Thus, the whole consumption required to send a Wi-Fi message is that coming from the establishment and the transmission per se, which is 201.86 mAs. For larger payloads, check Table 7.

Table 7. Summary of energy consumptions (mAs) for Wi-Fi.

Wi-Fi Payload (Bytes)	12	24	48	96	192	384	768
Establishment consumption	198.46	198.46	198.46	198.46	198.46	198.46	198.46
Number of transmissions	1	1	1	1	1	1	1
Transmission consumption	3.40	3.40	3.40	3.40	3.40	3.40	3.40
Total consumption	201.86	201.86	201.86	201.86	201.86	201.86	201.86

3.5. BLE

For the case of BLE, the FiPy board still provides a limited support of the protocol. Only advertisements are supported, and no security can be implemented. Thus, we implement transmissions over BLE as advertisements that are received by another BLE device.

Moreover, the size of message does not matter as the driver always fill the user datagram with dumb bytes. We have checked in the lab that the time and current waveform—i.e., the energy consumed—for the advertisement transmission is the same either with one user byte or the maximum 25 user bytes.

In Figure A9, the current consumption for the BLE transmission process (12-byte message) can be seen.

Since the BLE advertisement is set until the transmission finishes, the time spent is 10.52 ms, with an average consumption of 95.99 mA, which leads to an energy consumption of 1.01 mAs for the transmission of a 12-byte BLE message.

BLE does not need a connection establishment per se, but when the device wakes up from a sleep mode, the modem needs to be reinitialised. This consumption (see Figure A10) must be taken into consideration every time the device sends a message: 51.98 mAs.

Thus, the full energy consumption for a 12-byte BLE transmission—considering both the modem initialisation and the message transmission—gets to be 52.99 mAs. For larger payloads, check Table 8.

Table 8. Summary of energy consumptions (mAs) for BLE.

BLE Payload (Bytes)	12	24	48	96	192	384	768
Establishment consumption	51.98	51.98	51.98	51.98	51.98	51.98	51.98
Number of transmissions	1	1	2	4	8	16	31
Transmission consumption	1.01	1.01	1.01	1.01	1.01	1.01	1.01
Total consumption	52.99	52.99	54.00	56.02	60.06	68.14	83.29

4. Energy Harvesting Generation

The global increase in IoT nodes, and especially indoor ones, has led to the search for new ways of providing power supply to them. IoT devices are usually wireless, which means they need a battery (or other storage element) to operate. This battery needs to be replaced occasionally, which increase costs—in fact, the cost of replacing the battery can be greater than the IoT device itself. For exemplification, the device explained in Section 2 hereof has an average consumption of about 1 mW [5]. This device was wisely designed to be very power efficient, so it can run autonomously by means of MIEH.

Energy harvesting technology provides a green, carbon-free, sustainable, and virtually infinite power supply to wireless devices, obtaining the available energy from the environment to reduce—or even eliminate—the need for storage elements and wired power supply. Some of the most relevant EH methods for IoT devices are ambient radiation (RF), photovoltaic, piezoelectric, magnetic induction, vibration, pyroelectric and thermoelectric [5].

This paper is focused on the development and possibilities of what we consider the three main sources for indoor smart meters: photovoltaic (transforming light radiation into electrical current), radiofrequency (using the already-present electromagnetic waves) and magnetic induction (exploiting the changing magnetic fields that occurred in AC wires).

The nature of these three technologies entails a complex comparative study. In the literature, one can find different results for a bunch of designs, configurations and sets. Power generations depend widely on the real characteristics of the ambient energy availability, device's design, system's requisites, and implementation. However, it is crucial to compare these techniques with one another. Hence, for this work, we are using data from similar use cases found in the literature—comparing them by magnitude order instead of concrete values as they tend to be specific for each case. Be they:

- Photovoltaic: tens of milliwatts (10–20 mW)
- Radiofrequency: tenths of milliwatts (0.1–0.2 mW)
- Magnetic induction: milliwatts (1–2 mW)

4.1. Photovoltaic

Photovoltaic cells are used to power a multitude of sensors and other IoT systems. In [19], Xicai Yue et al. developed a PV EH model for a CO_2 sensor, which produces an output of 4.2 V and a pulse current of 100 mA for 600 ms. They also determined that the best average storage efficiency is obtained at 200 lux. This is remarkable because, if a storage element is added to the PV harvester, the device could achieve its self-sustainability. Abhiman Hande et al. depicted in [20] the use of several ultracapacitors as energy storage devices. This leads to a compact and robust system with fewer solar panels in a series-parallel combination.

The values of the indoor photovoltaic technique depend mainly on two criteria: light and material. Regarding the nature of light it usually would be artificial for inside use cases; in terms of material, the efficiency of new generation cells compared to commercial silicon is more than twice [21]. Nonetheless, it is important to note that real-world working conditions may drop theoretical efficiencies of PV panels to half [22].

Indoor lighting conditions are more complex than the exterior ones, since spaces are smaller, and the light levels are lower and intermittent. Indoor PV cells have a small size of around 30 cm^2 [23]. A polymer-based silicon cell has a conversion power efficiency of 9% for F12 fluorescent lamps (100 lux). The light resource comes from natural outdoor light and artificial light from luminaires—fluorescent, LED. Solar cells require an irradiance of around 7 mW/m^2 to work properly.

On the one hand, the non-constant presence of people reduces the daylight hours of the surroundings. On the other hand, average consumption is much lower than active consumption, saving energy and enabling this technology. The most common outdoor solar cells are made of silicon, a cheap material highly studied that produces 0.1 mW/lm. However, for indoor conditions where size requirements are tougher, researchers are studying new materials with larger bandgap energy, higher efficiency and smaller dark currents [24].

In [25], Lin Xie et al. use an organic photovoltaic cell for high intensity indoor environments, such as hospitals, with a theoretical efficiency of 60%. In the same way, the interest in gallium cells for indoor EH is also growing thanks to the lack of transparency losses, leading to a 40% energy conversion [22]. A small GaAs cell that is one-third of an office paper can power devices of up to 10 mW [26].

PV could be mixed with other technologies. For example, in [27] Yen Kheng Tan et al. create a hybrid of solar photovoltaic and thermal energy. The goal of this system is to extend the lifetime of the wireless sensor nodes. For a solar irradiance of 1010 lux and a thermal gradient of 10 K, an average of 621 W is obtained—three times more than just thermal.

Indoor and outdoor uses can also be combined, for example for smart building applications. This is described in [28], where a PV EH generates an average of 0.5 W, getting to be a maximum of 2.3 W with 130 lux.

4.2. Radiofrequency

Radio signals, mobile phones or Wi-Fi are some of the examples that originate these electromagnetic waves which are available almost everywhere. In addition, the fluctuations it presents are usually caused by human factor, not by weather conditions.

It is essential to consider the frequency, the modulation, and the power transmission to properly design the circuit of indoor devices. The key element is known as rectenna. Its main components are a rectifier and an antenna. In order to optimise energy conversion, a DC-DC boost converter can be added [29]. Many rectennas have been created, achieving different efficiencies depending on the design characteristics.

The study of radiofrequency EH is related to the dBm value of the incident signal and the conversion efficiency. For –20 dBm, equivalent to 10 μW, the average efficiency may be around 10%, while if it is goes up to 0 dBm (1 mW), the efficiency could increase up to 50% [30].

In [31], a paper substrate rectenna designed for an input power of −20 dBm over LTE bands presented a range of 5–16% efficiency; while the six-band dual rectenna presented in [32] showed a range of efficiency between 37.7% and 41.4% with −15 dBm input power. In [33], A. Eid et al. presented an ultra-compact and flexible rectenna that can operate at the 2.4 GHz ISM band reaching up to 40% efficiency.

For a 2.4 GHz Wi-Fi Multi-SSID router and power of 0 dBm, the energy harvester presented in [30] has an efficiency of 50.18%, due to the power management unit which minimise losses. Using the same circuit design, it is possible to operate on several ISM band or cellular RF as well [34].

Huaguang He et al. depicted in [35] a 2 × 4 rectenna array for the range of 895–925 MHz and 1.6–2.65 GHz. They obtained an output pulse voltage of 3.3 V and 33 mA for 100 ms, with an efficiency of 33% for 1800 MHz, 41.5% for 900 MHz and 55% for 2.4 GHz. However, it is important to note that the use of rectenna arrays at indoor environments might be inappropriate if the multipath effect is not eliminated since RF energy harvesting is sensitive to the angle of incidence, so adding more rectennas to the harvester is not a straightforward solution.

The current challenge is to improve the conversion capacity and energy harvesting of the rectennas. There are several possibilities, such as broadband antennas or antenna arrays. Nevertheless, the first requires a matching network for each frequency band and the second ones add complexity.

4.3. Magnetic Induction

The third most relevant energy harvesting technique for indoor IoT smart meters or similar applications is magnetic induction. The basic requirement is to have a coil, either near or surrounding the wires carrying alternating current so that the change of inducted magnetic fields excite the coil, thus generating an electromotive force. This means that the electrical panel or distribution box must be opened, but no electrical disruption is needed as electrical circuits are not modified. This EH technique was studied and characterised in detail in our previous work “Smart Metering for Challenging Scenarios: A Low-Cost, Self-Powered and Non-Intrusive IoT Device”. In this paper [5], a metering IoT device was power supplied by the electromotive force generated inside the coil, providing around 1 mW of power for an average household mains line.

When sensors or devices require current measurement, as in this case, MIEH is the optimal choice since it uses the same physical principle as current probes. In this way, the whole system is more compact, simpler, and cost-efficient. This appreciation of the use of magnetic induction as EH has hardly been developed and even less applying wireless IoT communications. The effective mains current energy harvesting range of this device is similar to that at home, corresponding to a current between 2.2 and 6.4 A. Using IEEE 802.15.4 as wireless technology, Danilo Porcarelli et al. achieved in [36] a device is self-powered with a load of 300 W for at least 60 s of measurement.

5. Discussion

In this section, we assess the main challenge for autonomous indoor smart meters: power balance. We address the trade-off between working conditions, energy harvesting generation and wireless technology energy consumption.

The five wireless technologies in the scope are compared with different working conditions for the smart meter—metering period and buffer size—, at the same time they are evaluated to check if they comply with the available power generated by the EH techniques.

5.1. Wireless Technology Selection

After having characterised the five wireless technologies, we can now analyse the energy consumption each of them would have, and therefore discuss which one would be better depending on the power available.

This work was planned so that every wireless technology runs in the same development board. This allows us to not be dependent on the consumption of the metering process per se, being the same for all technologies. This was characterised in Section 2 hereof, and it is not worth considering for the wireless technologies comparison.

Figure 6 depicts a quantitative representation of the consumption needed for each technology—it is plotted out on a non-linear scale to enhance visualisation, since for the technologies requiring establishment, the vast majority of their consumption comes from that very process.

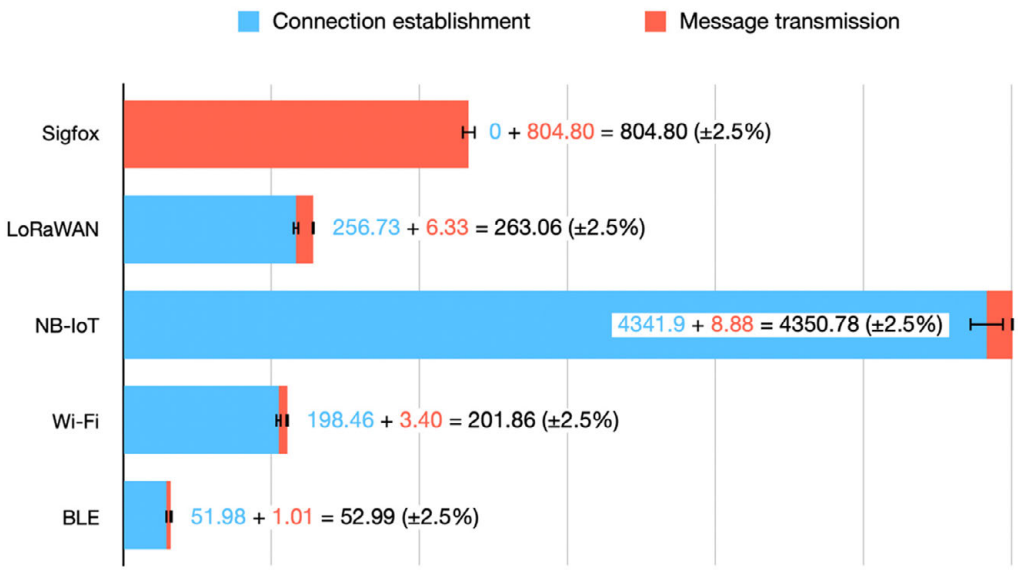


Figure 6. Quantitative representation of the wireless technologies' consumption. A confidence interval of 5% is depicted as the set of measurements for every technology were within this range.

These consumptions are those from Table 3, where they were characterised for 12-byte messages as it is the Sigfox limitation. However, for some technologies, increasing the message payload does not proportionally increase the message transmission consumption—as one could see in Section 3, Tables 4–8.

This way, we could reduce the number of messages—thus lowering the number of connection establishments—, and therefore decrease the whole energy consumption. For instance, with LoRaWAN in our configuration (SF7, 125 kHz), we can send messages of up to 222 bytes. For the case of BLE, our board lets us send messages of up to 25 bytes. For the case of both Wi-Fi and NB-IoT, this limit is much higher and above 1024 bytes—768 bytes is the limit considered for comparison.

Table 9 shows the full consumption for each wireless technology and every message size. Moreover, in Figure 7 (logarithmic scale) we can see the evolution on the consumption required by each technology as the payload increases from 12 to 768 bytes.

Table 9. Summary of energy consumptions (mAs) for all message sizes for all technologies.

Technology	12-Byte	24-Byte	48-Byte	96-Byte	192-Byte	384-Byte	768-Byte
Sigfox	804.80	1609.6	3219.2	6438.4	12,876.8	25,753.6	51,507.2
LoRaWAN	263.06	266.07	269.48	277.52	293.54	330.35	403.97
NB-IoT	4350.8	4350.8	4350.8	4351.0	4351.3	4351.8	4353.1
Wi-Fi	201.86	201.86	201.86	201.86	201.86	201.86	201.86
BLE	52.99	52.99	54.00	56.02	60.06	68.14	83.29

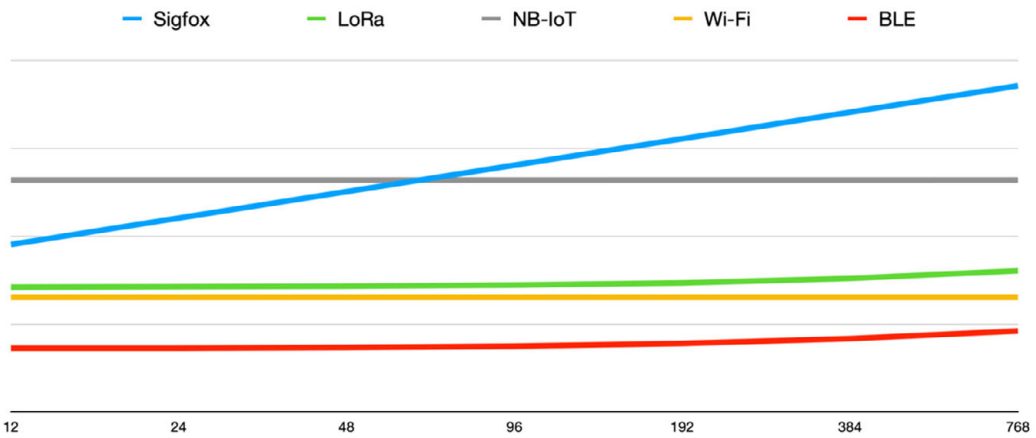


Figure 7. Plot of the wireless technologies' consumption in logarithmic scale for different message sizes.

Apart from the features of the communications—payload, communication establishment, number of transmissions—the characteristics of every use case will also determine the best suitable wireless technology for the application: what range should the device support, is there a strict real-time requirement for the data, can a public infrastructure be used, etc.

5.2. Energy Harvesting Technique Selection

For feasibility characterisation, not only the raw power available from the energy harvesting sources is important, but also their availability. For some EH sources, their availability may vary importantly whilst for others may be steadier, more predictable. For instance, indoor PV might be very different along time for the same space, as it will depend on the external weather, several people switching lights, and even the state of blinds. On the other hand, RF will be steadier along time as ambient radiation tends to be constant in the long term—it really only changes provided that new wireless technologies are deployed. MIEH may be also fairly predictable and constant, as the energy consumption of a building tends to be the same by periods—working days/weekends, working hours/nights, and holidays.

In order to avoid the lack of power supply, it could be possible to combine two types of EH techniques, such as PV and MIEH. However, this combination makes the device more complicated as two harvesting circuits would be required. Furthermore, the solar panel should be located outside the electrical panel to receive light, which adds complexity to the whole system. The same manner, if RF were used, the rectenna would also need to be outside the electrical panel to receive stronger signals.

The use of one EH source over another will depend on the specific use case: where will the device be located, will there be enough mains consumption to exploit MIEH, will there be ambient light to install a PV harvester, will there be much data to be transmitted, etc.

Nonetheless, for smart meters the best approach gets to be MIEH: no elements need to be placed outside the electrical panel, and the same physical device acts as current probe—crucial for metering—and harvester, which simplifies the device, hence providing an easy, fast way of deploying ubiquitous smart meters.

Although adding more harvesters or using better ones could solve the power balance problem, this would also make the device more expensive—and complex if several harvesters are combined. Since this work is focused on smart meters, MIEH is the most appropriate solution in terms of scalability, simplicity and ease of installation; even if some trade-offs are faced using this technique, such as reducing metering period.

5.3. Constraints for Energy Consumption of Smart Meters

We can reckon the average power demand for every case with Equation (2). The result (Ψ) would be in mAs, which is directly converted to mW multiplying by the voltage supply of the characterisation (5 V).

This calculus let us write Table 10, where all possible combinations are shown, properly depicting the average consumption of the device. This is the consumption that must be counter-balanced by the EH source in order to make the device autonomous.

Table 10. Smart meter average consumption (mW) depending on buffer size—i.e., message payload—, metering period and wireless technology.

Buffer Size (Bytes)	Metering Period (min.)	Sigfox	LoRaWAN	NB-IoT	Wi-Fi	BLE
12	**1**	15.07	11.31	39.69	10.89	9.85
	5	3.08	2.33	8.00	2.24	2.03
	10	*1.58*	*1.20*	4.04	*1.16*	*1.06*
	15	*1.08*	*0.83*	2.72	*0.80*	*0.73*
24	**1**	15.07	10.40	24.59	10.18	9.66
	5	3.08	2.15	4.98	2.10	2.00
	10	*1.58*	*1.11*	2.53	*1.09*	*1.04*
	15	*1.08*	*0.77*	*1.72*	*0.75*	*0.72*
48	**1**	15.07	9.95	17.03	9.83	9.57
	5	3.08	2.05	3.47	2.03	*1.98*
	10	*1.58*	*1.07*	*1.78*	*1.06*	*1.03*
	15	*1.08*	*0.74*	*1.21*	*0.73*	*0.71*
96	**1**	15.07	9.72	13.26	9.65	9.53
	5	3.08	2.01	2.72	*1.99*	*1.97*
	10	*1.58*	*1.05*	*1.40*	*1.04*	*1.03*
	15	*1.08*	*0.72*	*0.96*	*0.72*	*0.71*
192	**1**	15.07	9.60	11.37	9.57	9.50
	5	3.08	*1.99*	2.34	*1.98*	*1.97*
	10	*1.58*	*1.03*	*1.21*	*1.03*	*1.02*
	15	*1.08*	*0.71*	*0.83*	*0.71*	*0.71*

Table 10. *Cont.*

Buffer Size (Bytes)	Metering Period (min.)	Sigfox	LoRaWAN	NB-IoT	Wi-Fi	BLE
384	**1**	15.07	9.55	11.42	9.50	9.49
	5	3.08	*1.98*	2.15	*1.97*	*1.96*
	10	*1.58*	*1.03*	*1.12*	*1.03*	*1.02*
	15	*1.08*	*0.71*	*0.77*	*0.71*	*0.70*
768	**1**	15.07	9.52	9.95	9.50	9.49
	5	3.08	*1.97*	2.06	*1.97*	*1.96*
	10	*1.58*	*1.03*	*1.07*	*1.02*	*1.02*
	15	*1.08*	*0.71*	*0.74*	*0.71*	*0.71*

Considering EH generations as in Section 4 hereof, each table cell text is marked indicating the EH techniques that would comply to make the device autonomous—we consider a qualitative magnitude order, as claimed in Section 4:

- Circled: RF complies, so do MIEH and PV (never happens)
- Italics: MIEH complies, so does PV
- Underline: only PV complies
- Grey text: no EH technique would comply

$$\Psi = \frac{\Sigma \times \Gamma + \Phi + \Sigma \times T \times \Theta}{\Sigma \times T} \quad (2)$$

where:

- Σ is the buffer size (bytes)
- Γ is the consumption of a standard metering process (mAs)
- Φ is the consumption of a transmission for the designated technology (mAs)
- T is the metering period (s)
- Θ is the stand-by consumption (mA)

The optimal combination of energy harvesting technique and IoT wireless technology will depend on functional requisites (metering period), communication requirements (buffer size) and location constraints (EH source availability).

Enlarging the stand-by periods of event-driven IoT nodes enhances power requirements, making them lower. However, this means losing time-precision in measurements because fewer samples are taken. This phenomenon could even lead to missing information about short events, such as the consumption peak that happened when heating something in a microwave oven, which may last for 3–5 min, but might be missed if the metering period is set to a higher value.

Nevertheless, enlarging the measurements buffer does not always enhance energy consumption. In the case of Sigfox, there is no difference at all since Sigfox's consumption increases linearly as the buffer size increases, due to both its 12-byte payload limitation and the fact that it does not need any establishment consumption (see Table 4). The technology with the largest reduction in consumption by buffer enlargement is NB-IoT, mainly because it allows big payloads but requires a big establishment consumption; however, the transmission consumption per se is nearly the same with no regard to the message size (see Table 6). The others (LoRaWAN, Wi-Fi, BLE) present a restraint enhancement that, in most cases, will not be worth it as the data will update less frequently.

Moreover, as fewer measurements are taken—stand-by period extended, buffer size is increased, fewer wireless transmissions—the predominant consumption tends to be that coming from the smart meter per se, thus making wireless technologies consumption differences less noticeable in the overall average consumption of the IoT device. Notice

that the consumption coming from the stand-by period and the metering process is the same regardless of the wireless IoT technology.

It is important to note that, with the development board and wireless technologies used for this work, radiofrequency energy harvesting cannot be used since the amount of energy that can be harvested is lower than the necessary to meet the autonomous working conditions.

6. Conclusions

Feasibility of autonomous indoor IoT smart meters is mainly restricted by the limitations on the ambient energy available to harvest. Although IoT devices have achieved very low power consumptions in the recent years, wireless technologies still require a considerably large amount of power to perform. With the aim of facilitating the design and development of autonomous wireless smart meters, we have performed a comparative analysis of the energy consumption of the trendiest IoT wireless communication technologies (Sigfox, LoRaWAN, NB-IoT, Wi-Fi, BLE), and the most appropriate EH techniques for smart meter applications (PV, RF, MIEH). This analysis will help smart meter developers, metering solutions providers and smart metering adopters in the selection of the most suitable combination of wireless communication technology and energy harvesting technique—based on their use case characteristics and location constraints.

Regarding IoT wireless technologies, it has been shown that the most energy efficient happens to be BLE, followed by LoRaWAN and Wi-Fi, finally tailing NB-IoT and Sigfox. However, their specific consumption will be determined by the metering period and buffer size. Customarily, BLE will be the best choice if communication range is not a limiting factor; otherwise, it will be LoRaWAN. However, if a commercial managed receiving network is wished, NB-IoT or Sigfox will be the suitable ones depending on data constrains.

Concerning EH techniques, the most powerful is PV, followed by MIEH, and finally RF. Yet, considering the smart meter field, MIEH gets to be the most appropriate since it takes advantage of the metering component (current sensor) as energy harvester, reducing device complexity and costs. Besides, smart meters are usually located inside electrical panels or distribution boxes—where no light is present.

Results prove that selection of wireless technology and energy harvesting technique will depend on the desirable application requisites—metering period, communication period—and the location constraints—EH source availability.

Author Contributions: Conceptualization, methodology, validation, E.S. and G.d.C.; software, hardware, laboratory work, E.S. and L.M.; formal analysis, resources, visualization, data curation, E.S.; investigation, E.S., L.M. and G.C.; writing—original draft preparation, E.S. and L.M.; writing—review and editing, supervision, G.d.C.; project administration, funding acquisition, A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work is part of the CHIST-ERA research project "ABIDI: Context-aware and Veracious Big Data Analytics for Industrial IoT" and is funded by the State Research Agency (AEI) from Ministerio de Ciencia e Innovación (MICINN) of Spain, grant number PCI2019-103762.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Appendix A

This appendix contains current consumption graphs for every wireless technology characterised and the smart metering process.

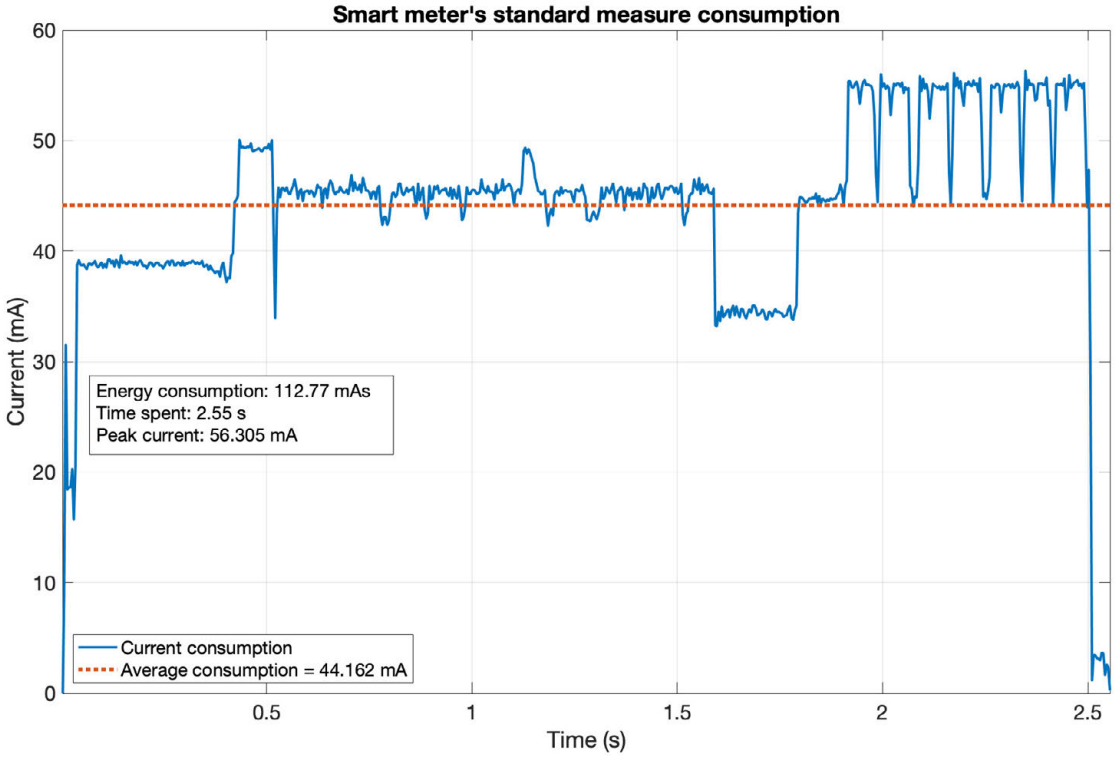


Figure A1. Current consumption detail of the smart meter's metering process.

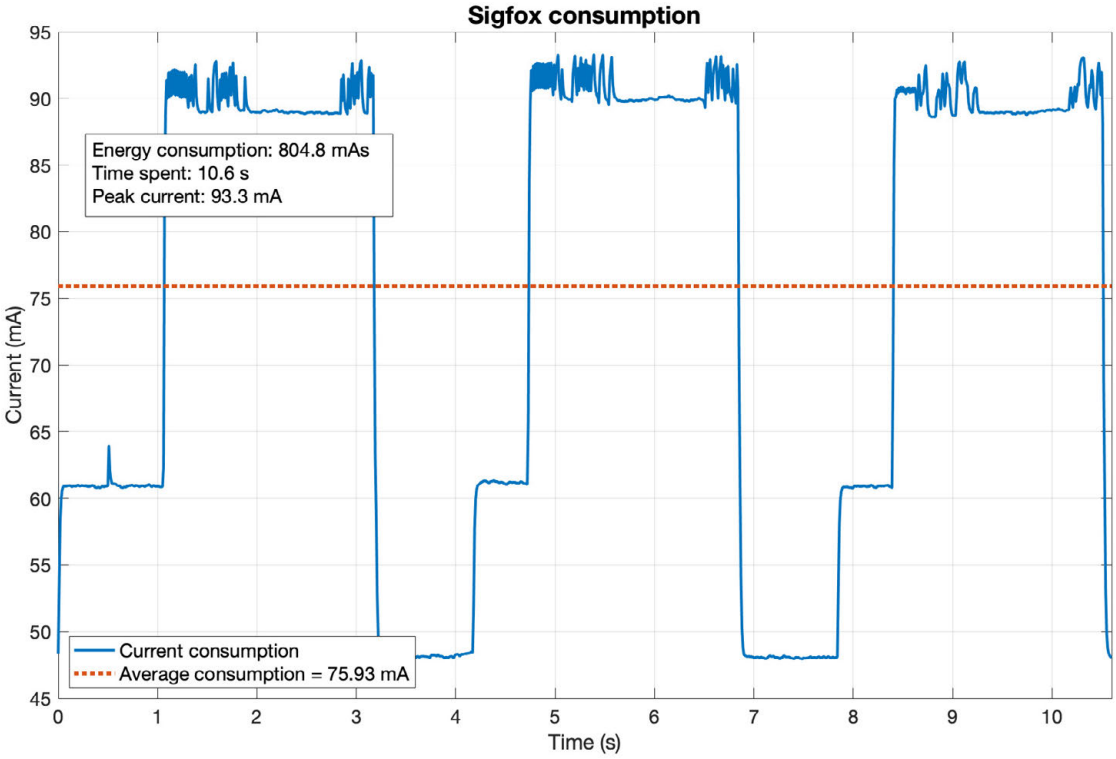


Figure A2. Current consumption detail for the Sigfox transmission. Data acquired at 100 s/s (samples per second).

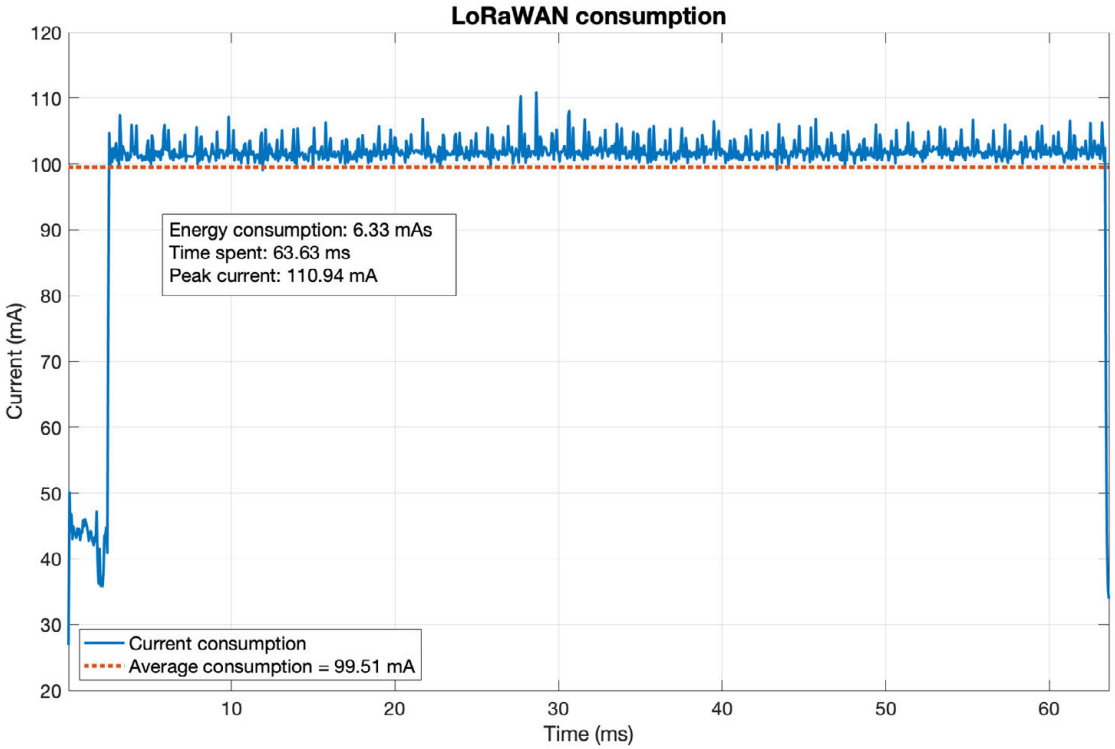


Figure A3. Current consumption detail for the LoRaWAN transmission. Data acquired at 100 kS/s, resampled at 1/6 for plotting.

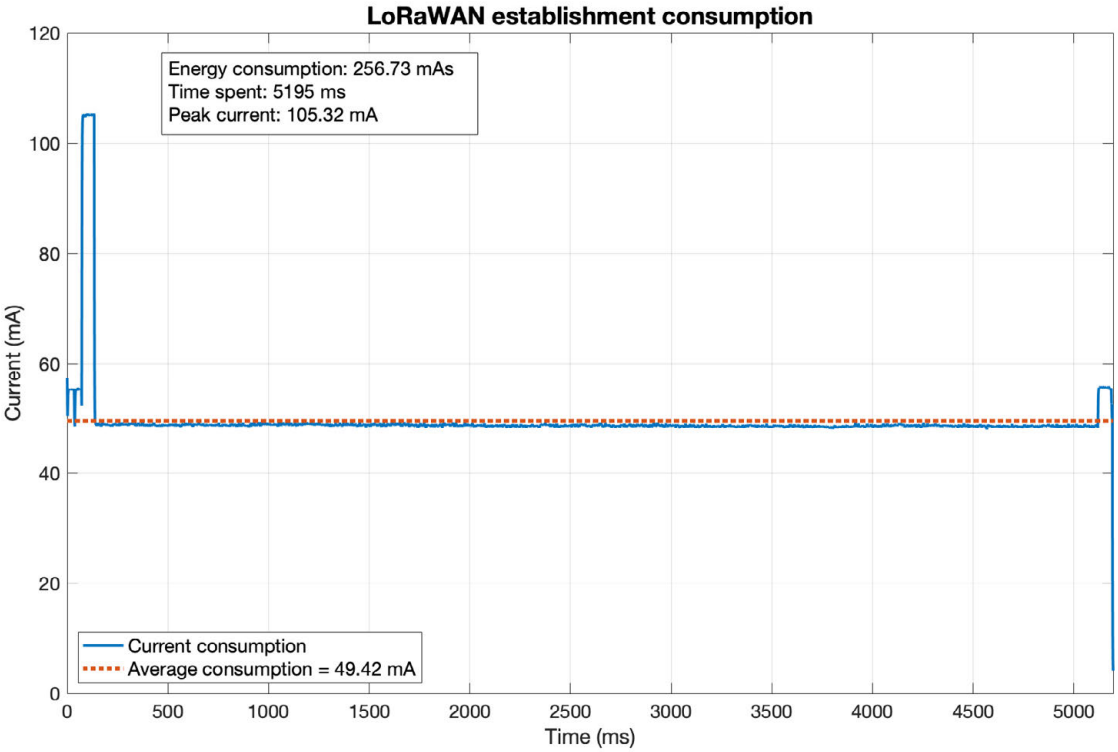


Figure A4. Current consumption detail for the LoRaWAN connection. Data acquired at 1 kS/s.

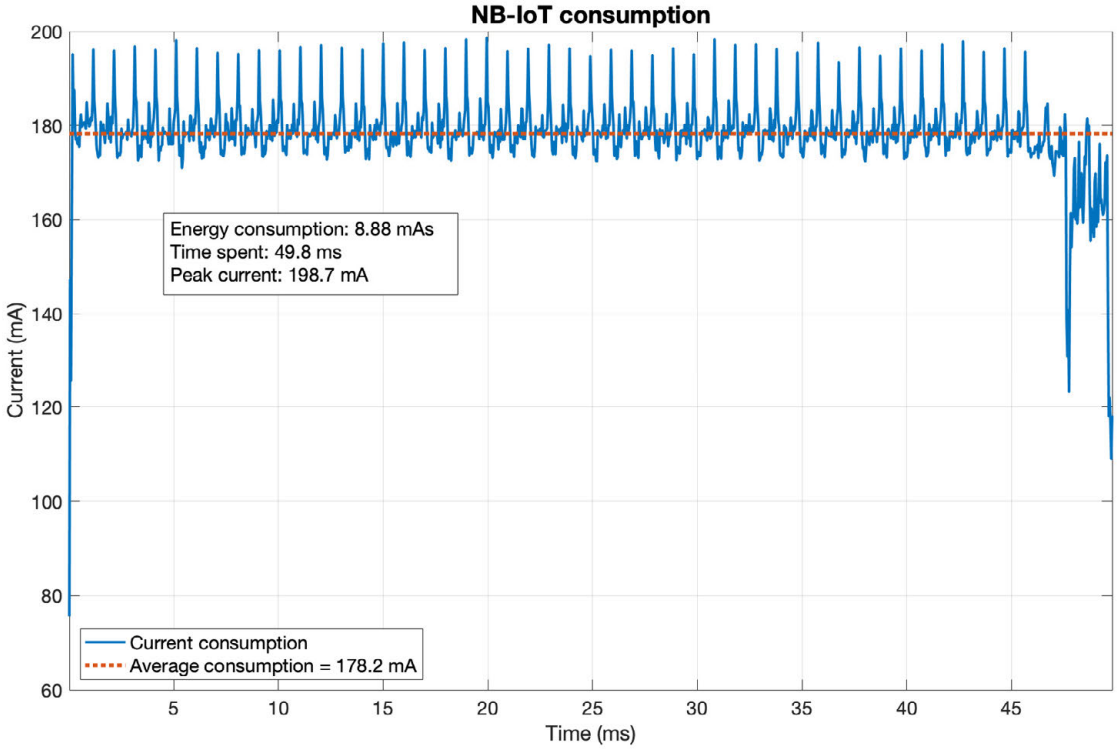


Figure A5. Current consumption detail for the NB-IoT transmission. Data acquired at 100 kS/s, resampled at 1/4 for plotting.

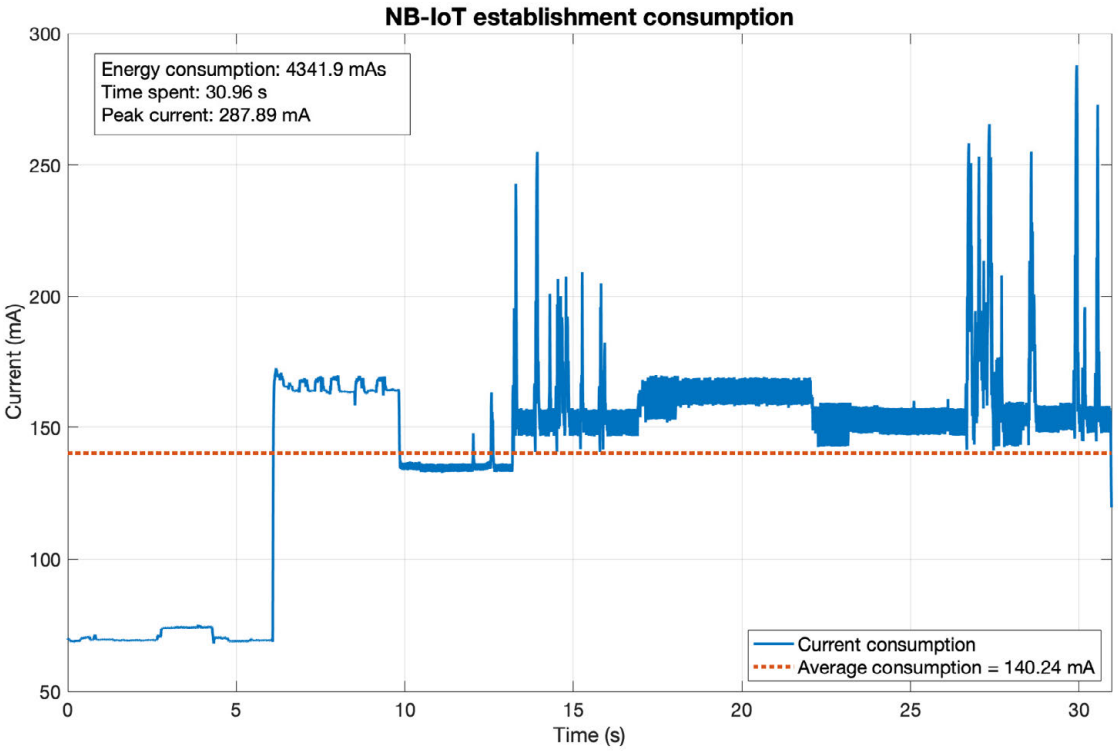


Figure A6. Current consumption for the NB-IoT connection establishment. Data acquired at 100 S/s.

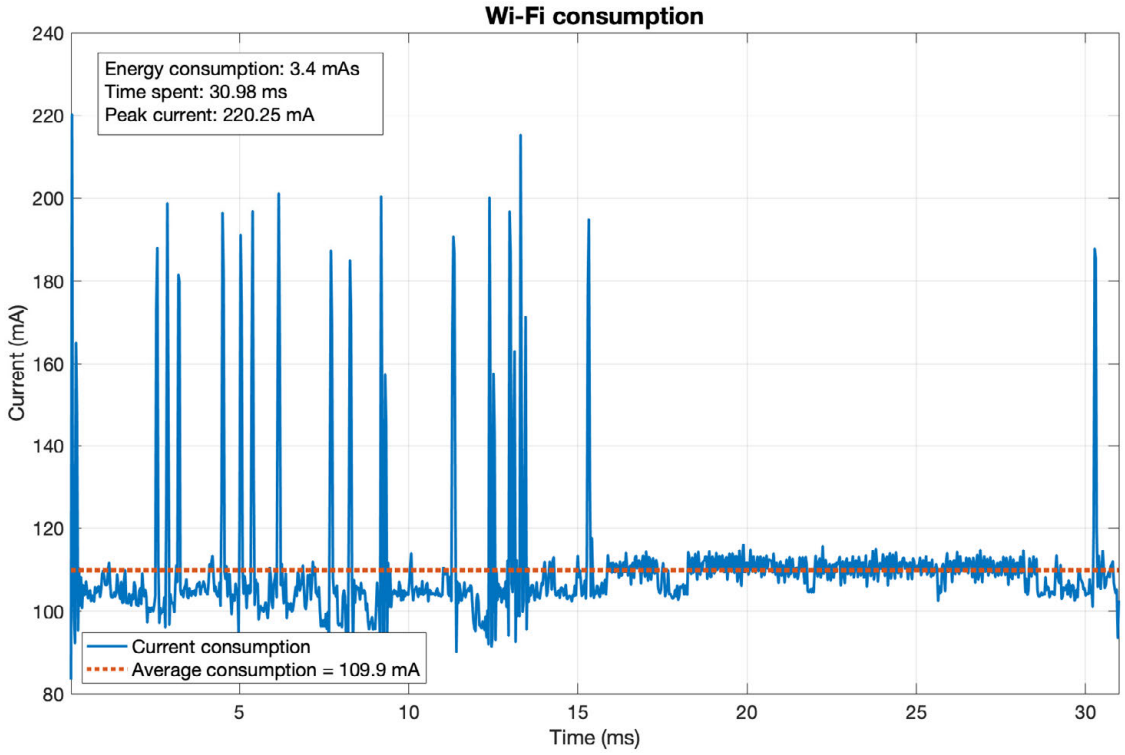


Figure A7. Current consumption detail for the Wi-Fi transmission. Data acquired at 100 kS/s, resampled at 1/3 for plotting.

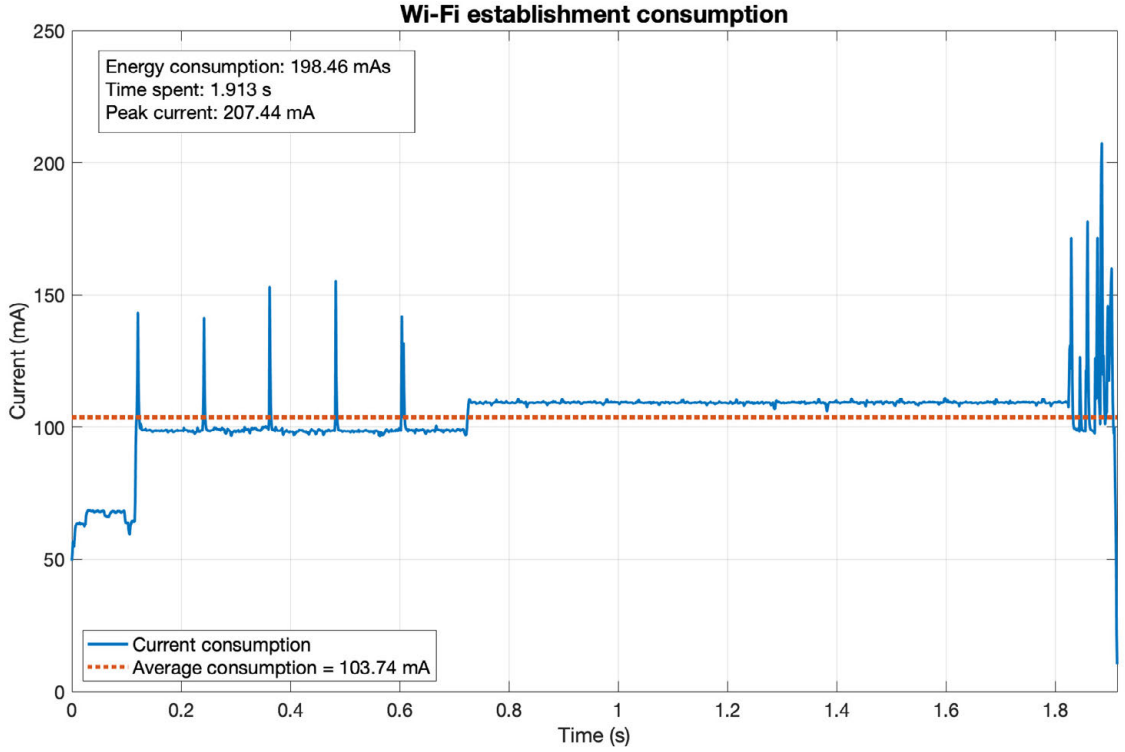


Figure A8. Current consumption detail for the Wi-Fi connection establishment. Data acquired at 1 kS/s.

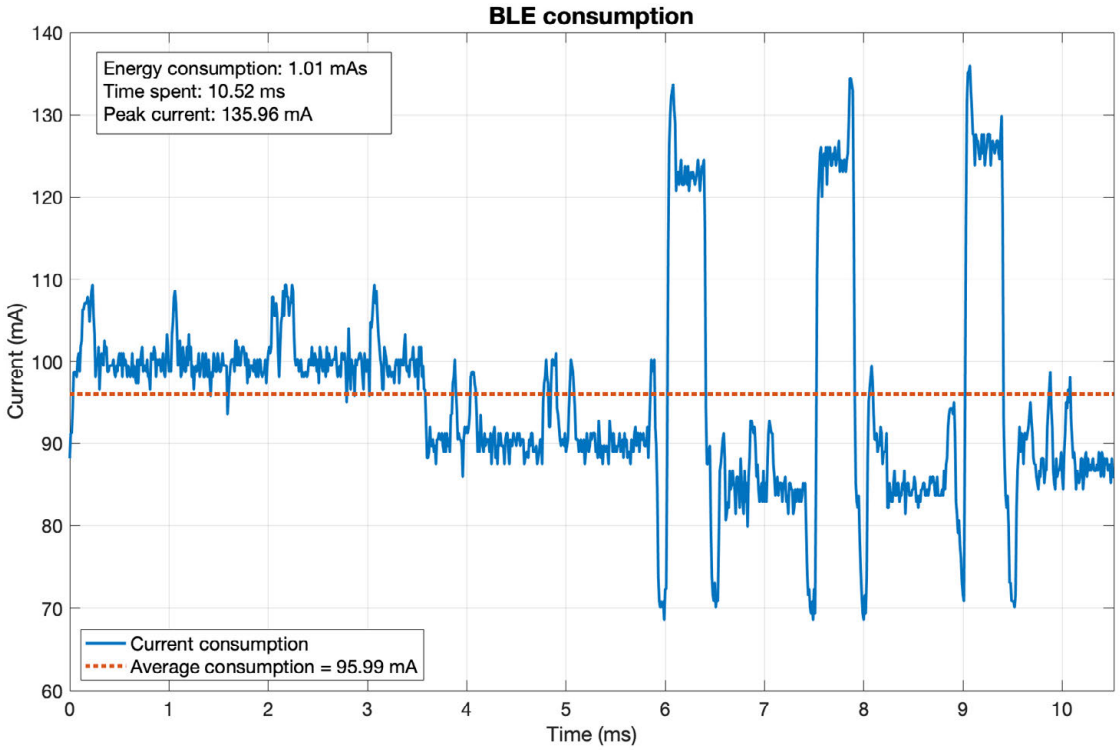


Figure A9. Current consumption detail for the BLE transmission. Data acquired at 100 kS/s.

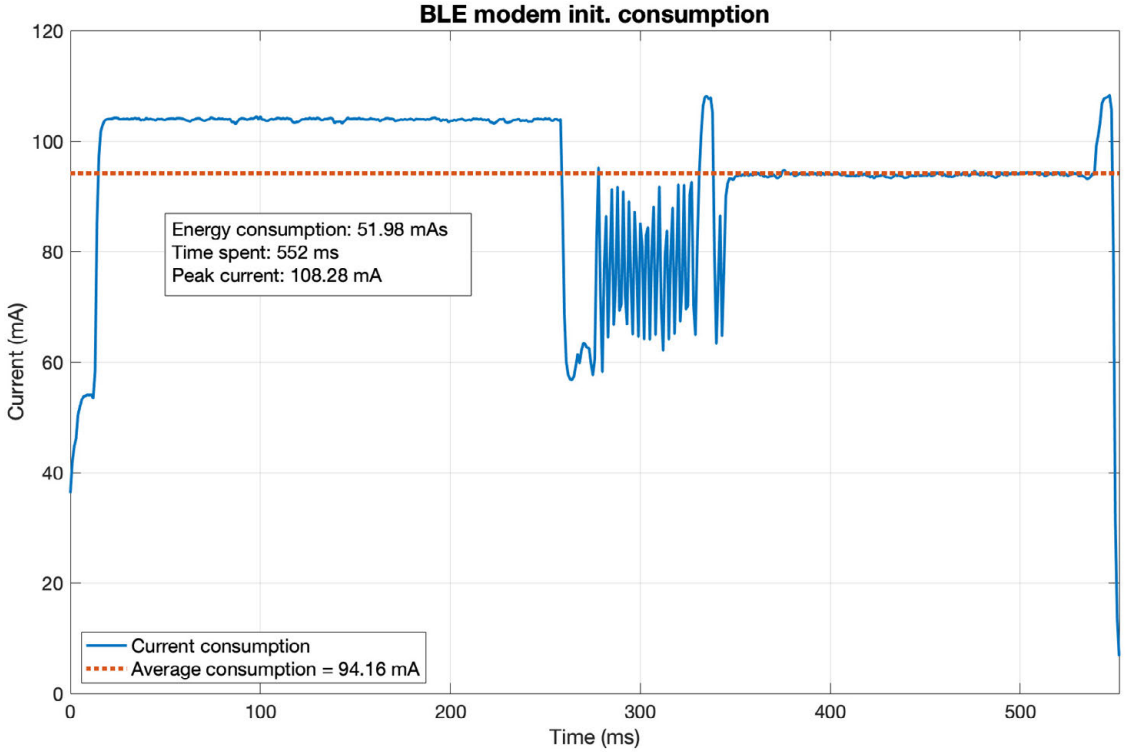


Figure A10. Current consumption for the BLE modem initialisation. Data acquired at 1 kS/s.

Appendix B

This appendix contains information about the process used to determine the Power Profiler's metering accuracy.

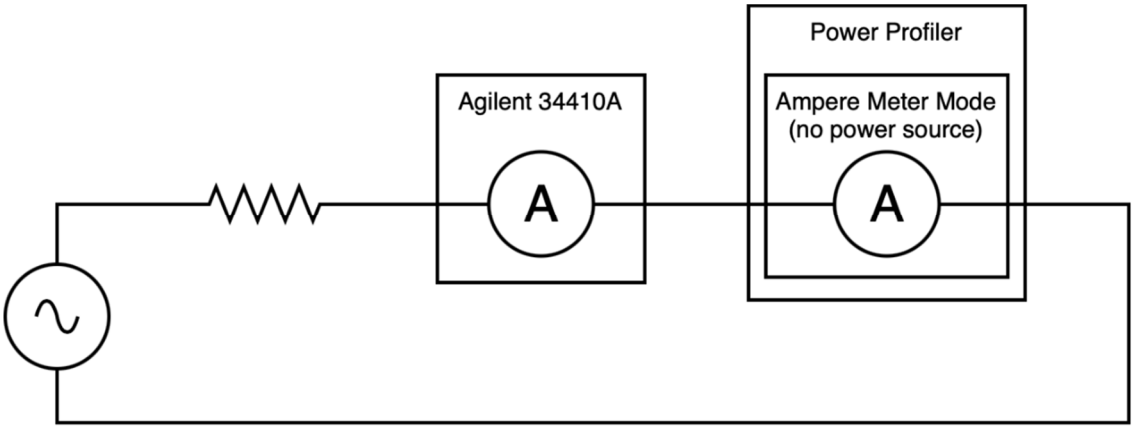


Figure A11. Setup used to determine the Power Profiler's accuracy.

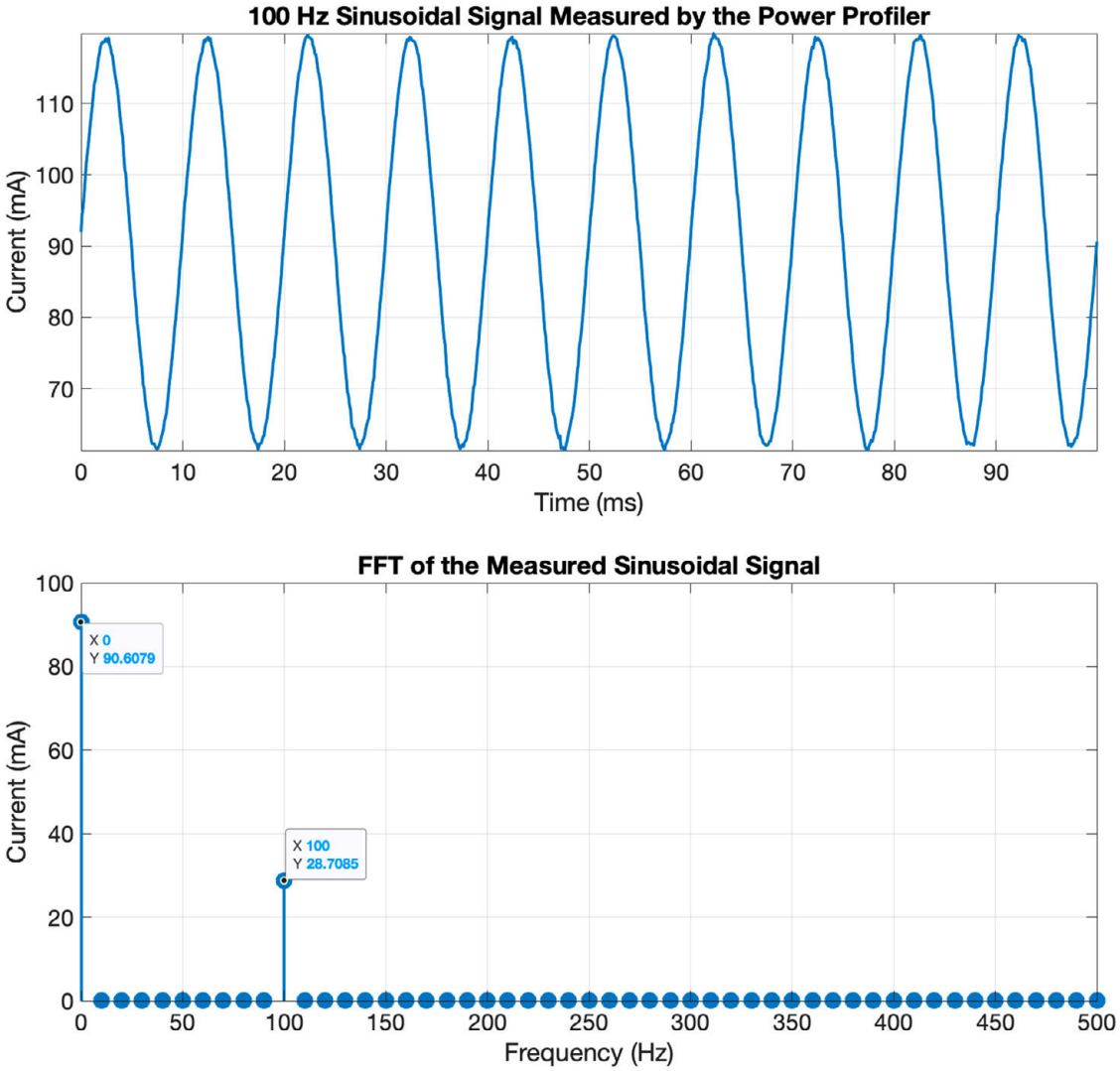


Figure A12. 100 Hz sinusoidal signal used to determine the Power Profiler's accuracy and its FFT.

References

1. Wegner, P. Global IoT Spending to Grow 24% in 2021, Led by Investments in IoT Software and IoT Security. 2021. Available online: https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/ (accessed on 8 November 2021).

2. Fotrune Business Insights Global IoT Market to Be Worth USD 1463.19 Billion by 2027 at 24.9% CAGR; Demand for Real-Time Insights to Spur Growth. 2021. Available online: https://www.globenewswire.com/en/news-release/2021/04/08/2206579/0/en/Global-IoT-Market-to-be-Worth-USD-1-463-19-Billion-by-2027-at-24-9-CAGR-Demand-for-Real-time-Insights-to-Spur-Growth-says-Fortune-Business-Insights.html (accessed on 8 November 2021).
3. Evans, D. The Internet of Things. How the Next Evolution of the Internet Is Changing Everything. 2021. Available online: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed on 8 November 2021).
4. Maayan, G.D. The IoT Rundown for 2020: Stats, Risks, and Solutions. 2020. Available online: https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx (accessed on 8 November 2021).
5. Saavedra, E.; Del Campo, G.; Santamaria, A. Smart Metering for Challenging Scenarios: A Low-Cost, Self-Powered and Non-Intrusive IoT Device. *Sensors* **2020**, *20*, 7133. [CrossRef] [PubMed]
6. Sendin, A.; Simon, J.; Urrutia, I.; Berganza, I. PLC deployment and architecture for Smart Grid applications in Iberdrola. In Proceedings of the 18th IEEE International Symposium on Power Line Communications and Its Applications, Glasgow, UK, 30 March–2 April 2014; pp. 173–178.
7. Sendin, A.; Berganza, I.; Arzuaga, A.; Pulkkinen, A.; Kim, I.H. Performance results from 100,000+ PRIME smart meters deployment in Spain. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 145–150.
8. Reinhardt, A.; Burkhardt, D.; Mogre, P.S.; Zaheer, M.; Steinmetz, R. SmartMeter.KOM: A Low-Cost Wireless Sensor for Distributed Power Metering. In Proceedings of the 2011 IEEE 36th Conference on Local Computer Networks, Bonn, Germany, 4–7 October 2011; pp. 1032–1039.
9. Woo, C.-K.; Ho, T.; Shiu, A.; Cheng, Y.-S.; Horowitz, I.; Wang, J. Residential outage cost estimation: Hong Kong. *Energy Policy* **2014**, *72*, 204–210. [CrossRef]
10. Praktiknjo, A.; Hähnel, A.; Erdmann, G. Assessing energy supply security: Outage costs in private households. *Energy Policy* **2011**, *39*, 7825–7833. [CrossRef]
11. Pycom FiPy Specsheets. Available online: https://docs.pycom.io/gitbook/assets/specsheets/Pycom_002_Specsheets_FiPy_v2.pdf (accessed on 8 November 2021).
12. Keysight Keysight 34410A Multimeter Datasheet. Available online: https://www.keysight.com/Us/En/Assets/7018-01326/Data-Sheets/5989-3738.Pdf (accessed on 8 November 2021).
13. Deutsche Telekom IoT NB-IoT, LoRaWAN, Sigfox: An up-to-Date Comparison. 2021. Available online: https://iot.telekom.com/resource/blob/data/492968/e396f72b831b0602724ef71056af5045/mobile-iot-network-comparison-nb-iot-lorawan-sigfox.pdf (accessed on 8 November 2021).
14. del Campo, G.; Gomez, I.; Cañada, G.; Piovano, L.; Santamaria, A. Guidelines and criteria for selecting the optimal low-power wide-area network technology. In *LPWAN Technologies for IoT and M2M Applications*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 281–305. ISBN 978-0-12-818880-4.
15. Technology | Sigfox. Available online: https://www.sigfox.com/en/what-sigfox/technology (accessed on 8 November 2021).
16. Nordic Semiconductor Power Profiler Kit II Specifications. Available online: https://infocenter.nordicsemi.com/index.jsp?topic=%2Fug_ppk2%2FUG%2Fppk%2FPPK_user_guide_Intro.html (accessed on 8 November 2021).
17. Espressif ESP32 Series Datasheet. Available online: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf (accessed on 8 November 2021).
18. Semtech Semtech SX1272 Datasheet. Available online: https://semtech.my.salesforce.com/sfc/p/#E0000000JelG/a/440000001NCE/v_VBhk1IolDgxwwnOpcS_vTFxPfSEPQbuneK3mWsXlU (accessed on 8 November 2021).
19. Yue, X.; Kauer, M.; Bellanger, M.; Beard, O.; Brownlow, M.; Gibson, D.; Clark, C.; MacGregor, C.; Song, S. Development of an Indoor Photovoltaic Energy Harvesting Module for Autonomous Sensors in Building Air Quality Applications. *IEEE Internet Things J.* **2017**, *4*, 2092–2103. [CrossRef]
20. Hande, A.; Polk, T.; Walker, W.; Bhatia, D. Indoor solar energy harvesting for sensor network router nodes. *Microprocess. Microsystems* **2007**, *31*, 420–432. [CrossRef]
21. Batista, D.; Oliveira, J.; Paulino, N.; Carvalho, C.; Farinhas, J.; Charas, A.; Dos Santos, P.M. Combined Organic Photovoltaic Cells and Ultra Low Power CMOS Circuit for Indoor Light Energy Harvesting. *Sensors* **2019**, *19*, 1803. [CrossRef] [PubMed]
22. Teran, A.S.; Moon, E.; Lim, W.; Kim, G.; Lee, I.; Blaauw, D.; Phillips, J. Energy Harvesting for GaAs Photovoltaics Under Low-Flux Indoor Lighting Conditions. *IEEE Trans. Electron Devices* **2016**, *63*, 2820–2825. [CrossRef] [PubMed]
23. Foti, M.; Tringali, C.; Battaglia, A.; Sparta, N.; Lombardo, S.; Gerardi, C. Efficient flexible thin film silicon module on plastics for indoor energy harvesting. *Sol. Energy Mater. Sol. Cells* **2014**, *130*, 490–494. [CrossRef]
24. Teran, A.S.; Wong, J.; Lim, W.; Kim, G.; Lee, Y.; Blaauw, D.; Phillips, J. AlGaAs Photovoltaics for Indoor Energy Harvesting in mm-Scale Wireless Sensor Nodes. *IEEE Trans. Electron Devices* **2015**, *62*, 2170–2175. [CrossRef]
25. Xie, L.; Song, W.; Ge, J.; Tang, B.; Zhang, X.; Wu, T.; Ge, Z. Recent progress of organic photovoltaics for indoor energy harvesting. *Nano Energy* **2021**, *82*, 105770. [CrossRef]
26. Politi, B.; Parola, S.; Gademer, A.; Pegart, D.; Piquemil, M.; Foucaran, A.; Camara, N. Practical PV energy harvesting under real indoor lighting conditions. *Sol. Energy* **2021**, *224*, 3–9. [CrossRef]
27. Tan, Y.K.; Panda, S. Energy Harvesting From Hybrid Indoor Ambient Light and Thermal Energy Sources for Enhanced Performance of Wireless Sensor Nodes. *IEEE Trans. Ind. Electron.* **2011**, *58*, 4424–4435. [CrossRef]

28. Rokonuzzaman, M.; Mishu, M.; Amin, N.; Nadarajah, M.; Roy, R.; Rahman, K.; Buhari, A.; Binzaid, S.; Shakeri, M.; Pasupuleti, J. Self-Sustained Autonomous Wireless Sensor Network with Integrated Solar Photovoltaic System for Internet of Smart Home-Building (IoSHB) Applications. *Micromachines* **2021**, *12*, 653. [CrossRef]
29. Visser, H.J.; Vullers, R.J.M. RF Energy Harvesting and Transport for Wireless Sensor Network Applications: Principles and Requirements. *Proc. IEEE* **2013**, *101*, 1410–1423. [CrossRef]
30. Angulo, F.; Navarro, L.; Quintero M, C.Q.; Pardo, M. A Simple WiFi Harvester with a Switching-Based Power Management Scheme to Collect Energy from Ordinary Routers. *Electronics* **2021**, *10*, 1191. [CrossRef]
31. Palazzi, V.; Hester, J.; Bito, J.; Alimenti, F.; Kalialakis, C.; Collado, A.; Mezzanotte, P.; Georgiadis, A.; Roselli, L.; Tentzeris, M.M. A Novel Ultra-Lightweight Multiband Rectenna on Paper for RF Energy Harvesting in the Next Generation LTE Bands. *IEEE Trans. Microw. Theory Tech.* **2017**, *66*, 366–379. [CrossRef]
32. Haboubi, W.; Takhedmit, H.; Luk, J.-D.L.S.; Adami, S.-E.; Allard, B.; Costa, F.; Vollaire, C.; Picon, O.; Cirio, L. An efficient dual-circularly polarized rectenna for RF energy harvesting in the 2.45 GHZ ISM Band. *Prog. Electromagn. Res.* **2014**, *148*, 31–39. [CrossRef]
33. Eid, A.; Hester, J.; Nauroze, A.; Lin, T.-H.; Costantine, J.; Tawk, Y.; Ramadan, A.H.; Tentzeris, M. A Flexible Compact Rectenna for 2.40 Hz ISM Energy Harvesting Applications. In Proceedings of the 2018 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting, Boston, MA, USA, 8–13 July 2018; pp. 1887–1888.
34. Muncuk, U.; Alemdar, K.; Sarode, J.D.; Chowdhury, K.R. Multiband Ambient RF Energy Harvesting Circuit Design for Enabling Batteryless Sensors and IoT. *IEEE Internet Things J.* **2018**, *5*, 2700–2714. [CrossRef]
35. He, H.; Li, T. Design of an indoor RF Energy Harvesting Module using Dual-Band Rectenna Array for IoT Applications. In Proceedings of the 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chengdu, China, 20–22 December 2019; Volume 1, pp. 1407–1410.
36. Porcarelli, D.; Brunelli, D.; Benini, L. Clamp-and-measure forever: A MOSFET-based circuit for energy harvesting and measurement targeted for power meters. In Proceedings of the 5th IEEE International Workshop on Advances in Sensors and Interfaces IWASI, Bari, Italy, 13–14 June 2013; pp. 205–210.

III. DOI: 10.3390/s22114159

A Universal Testbed for IoT Wireless Technologies: Abstracting Latency, Error Rate and Stability from the IoT Protocol and Hardware Platform

Sensors 2022, 22, 4159

https://doi.org/10.3390/s22114159

Pages 91–113 present the original manuscript as published

sensors

MDPI

Article

A Universal Testbed for IoT Wireless Technologies: Abstracting Latency, Error Rate and Stability from the IoT Protocol and Hardware Platform

Edgar Saavedra *, Laura Mascaraque, Gonzalo Calderon, Guillermo del Campo and Asuncion Santamaria

CeDInt-UPM, Universidad Politécnica de Madrid, Campus de Montegancedo, Pozuelo de Alarcón, 28223 Madrid, Spain; lmascaraque@cedint.upm.es (L.M.); gcalderon@cedint.upm.es (G.C.); gcampo@cedint.upm.es (G.d.C.); asun.santamaria@upm.es (A.S.)

* Correspondence: e.saavedra@upm.es

Abstract: IoT applications rely strongly on the performance of wireless communication networks. There is a wide variety of wireless IoT technologies and choosing one over another depends on the specific use case requirements—be they technical, implementation-related or functional factors. Among the technical factors, latency, error rate and stability are the main parameters that affect communication reliability. In this work, we present the design, development and validation of a Universal Testbed to experimentally measure these parameters, abstracting them from the wireless IoT technology protocols and hardware platforms. The Testbed setup, which is based on a Raspberry Pi 4, only requires the IoT device under test to have digital inputs. We evaluate the Testbed's accuracy with a temporal characterisation—accumulated response delay—showing an error less than 290 µs, leading to a relative error around 3% for the latencies of most IoT wireless technologies, the latencies of which are usually on the order of tens of milliseconds. Finally, we validate the Testbed's performance by comparing the latency, error and stability measurements with those expected for the most common IoT wireless technologies: 6LoWPAN, LoRaWAN, Sigfox, Zigbee, Wi-Fi, BLE and NB-IoT.

Keywords: testbed; latency; error rate; stability; performance; IoT; IIoT; LPWAN; wireless communications

Citation: Saavedra, E.; Mascaraque, L.; Calderon, G.; del Campo, G.; Santamaria, A. A Universal Testbed for IoT Wireless Technologies: Abstracting Latency, Error Rate and Stability from the IoT Protocol and Hardware Platform. *Sensors* **2022**, *22*, 4159. https://doi.org/10.3390/s22114159

Academic Editors: Gianni Pasolini, Margot Deruyck and Konstantin Mikhaylov

Received: 14 April 2022
Accepted: 26 May 2022
Published: 30 May 2022

1. Introduction

In the last few years, the IoT has been established as one of the most acknowledged paradigms, increasing the amount of related research and emerging technologies and services [1,2], both regarding IoT devices —35 billion ($\times 10^9$) devices connected in 2021 [3] and 75 billion devices expected by 2025 [4]—and monetary spending—more than EUR 1200 billion by 2027 [5].

The wireless paradigm for IoT allows medium and large coverage areas with relatively low energy consumption by providing small processing power requirements for devices as well as low transmission data rates [6,7], factors inherent in the IoT field itself. Despite the wide variety in wireless IoT technologies, some actors widely dominate the current picture of IoT communications, although this has always depended on the specific use case. Medium-range communications such as Bluetooth and Zigbee may have accounted for up to 28% of the wireless IoT chips in 2021 [8]. For long-range communications technologies, only four accounted for over 96% of global, installed active devices in 2021: NB-IoT, LoRa, LTE-M and Sigfox. NB-IoT leads this ranking with 47% of the global share, followed by LoRa with 36% [9]. In fact, low-power wide-area network (LPWAN) protocols that rely on licensed bands (NB-IoT, LTE-M) have surpassed those relying on non-licensed ones (LoRa, Sigfox) in 2021 [10].

However, different technologies provide different levels of performance and need different infrastructure requirements. Choosing one over another widely depends on the

specific use case [11], and it is not always clear how to compare their performance. The very specific use case will set the requirements for wireless technology. Requirements may be divided into technical factors (data rate, latency, range), implementation factors (cost, documentation, available coverage) and functional factors (energy consumption, location services, over-the-air upgrade) [12–15]. Into the bargain, exceptional attention must be paid to security, especially considering the rapid growth of IoT and its more-than-ever quasi-omnipresent presence in our lives. The research presented by Anand et al. in [16] and that presented by Malhotra et al. in [17] are great references regarding the security challenges in the IoT field.

Testbeds allow us to determine the realistic behaviour of IoT systems and even foresee future possible upgrades and enhancements to the systems. As IoT systems are intrinsically wide in nature, so are their possible characterisation targets, which make it arduously hard to develop and validate universal performance tests for IoT in different matters.

In the literature, one can find testbed systems evaluating some specific IoT characteristics, usually focused only on a few IoT technologies, for instance, the work of Pereira et al. [18], in which an experimental characterisation of mobile IoT latency is carried out, or that by Mroue et al. [19], evaluating LoRa, Sigfox and NB-IoT in a MAC layer-based approach.

There are also deep characterisations of specific IoT technologies for a relatively wide range of matters, such as the survey by Rashmi Sharan et al. of LoRa and NB-IoT [20]; or the work carried out by Alsukayti et al. [21], in which they analyse quality, transmission range, power consumption and data rates for different scenarios and technologies. On top of that, there are works evaluating different features, and challenges to face with eventual low-latency or high-reliability IoT communication networks, such as those in [22–24].

Yet, there is not sufficient research in the literature about actual, universal, ubiquitous, accountable testbeds. This may be due, indeed, to the massively wide nature of the IoT field. Hossain et al. propose a manner to overcome this issue with the work presented in [25], in which a large-scale IoT testbed-as-a-service is defined. Developing testbeds that can integrate various types of systems, interfaces and technologies is tough but still needed for a field with more variety and presence every day. This fact is clearly highlighted in [26], where the authors emphasise the lack of interoperability among IoT platforms and devices.

Specifically, no universal testbed regarding temporal end-to-end characterisation for IoT wireless technologies can be found in the literature. With this work, we want to abstract the IoT wireless technology characteristics as much as possible, providing a straightforward way of comparing wireless IoT technologies in different communication features: latency, error rate and stability. We developed a universal Testbed based on a Raspberry Pi 4 (RPi), which only requires the IoT device under test to have digital inputs (GPIO)—fact that can be taken for granted for virtually every IoT node. In the scope of this work, we analysed the performance of the following IoT wireless technologies: 6LoWPAN, LoRaWAN, Sigfox, Zigbee, Wi-Fi, BLE and NB-IoT.

The rest of the paper is organised as follows: Section 2 describes the Testbed and the workaround for this paper. In Section 3, we characterise the performance of the Testbed to determine its temporal accuracy and precision, i.e., error range. Section 4 presents real measurements and results from our Testbed for the wireless technologies under consideration. Finally, in Section 5, we briefly conclude the results of this work and discuss future milestones.

2. Universal Testbed

In this Section, the Testbed environment is described, both regarding the Testbed device itself and the laboratory set. First, we explain the IoT devices and configurations deployed for the different wireless technologies, and how *latency* must be considered on a user-level approach (Section 2.1). Then, we tackle some caveats regarding the wide variety of wireless technologies to consider (Section 2.2). Finally, in Section 2.3, the Testbed's user interface and measurement data presentation are explained.

2.1. Latency and Laboratory Workaround

Since distinct wireless IoT technologies have different topologies and key network components, we first need to define *latency*. Pure upload messages are considered as they are the main purpose of the majority of IoT applications: sending information from the node to the user-end. So, for this scope, let us define *latency*—see Figure 1.

Latency: *The time a message takes from the moment when the transmitting device is called to send the message until the message is ready for utilisation at the other end (user-side).*

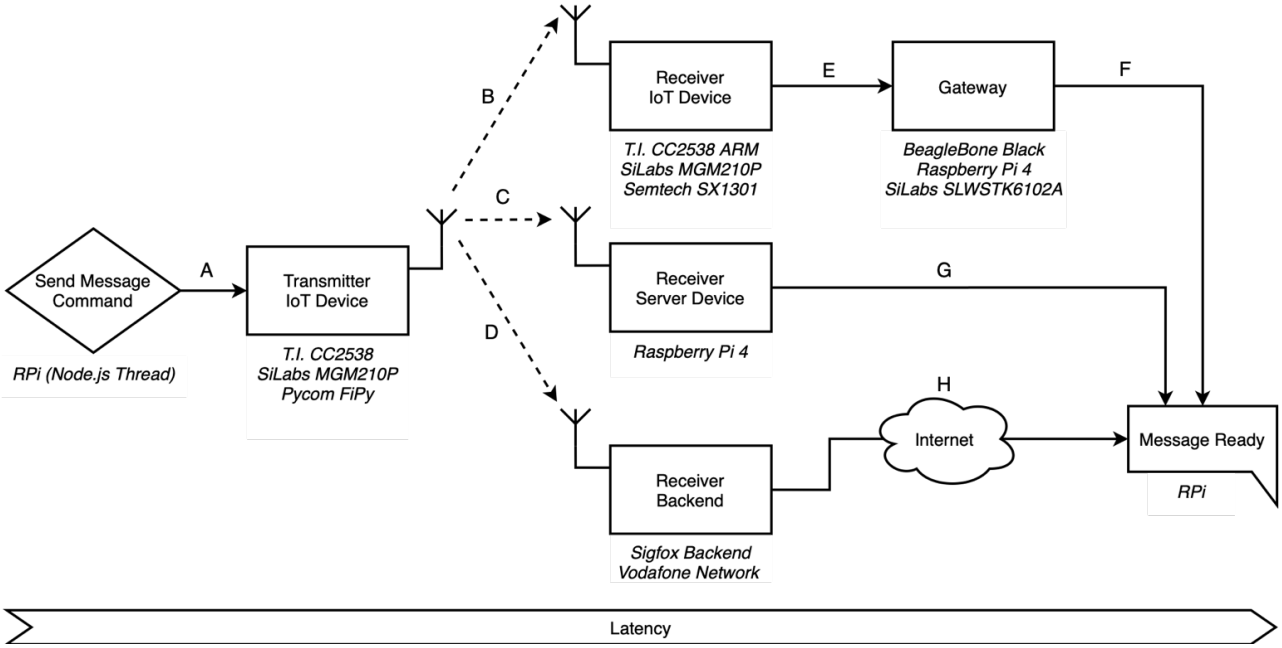


Figure 1. *Latency*: abstract definition and message paths for different wireless IoT topologies. These paths, along with the designated physical IoT devices—which are all compliant with the IoT technology of interest—actually portray the very use case deployed in the lab to do this work. Other configurations could be also used for certain technologies and other devices as well.

Hence, time considers neither the acknowledgement (ACK) of the message nor possible retransmissions. Provided the message were lost, the transmission would count as an error. In this manner, considering the different topologies regarding different wireless technology' specifications, three main groups can be defined: (1) technologies requiring a specific gateway; (2) technologies requiring public Internet usage; and (3) technologies requiring neither. Therefore, these groups (see Figure A1 for a detailed version on each technology) correspond to one of the following paths:

1. **A-B-E-F**: 6LoWPAN, ZigBee, LoRaWAN
2. **A-D-H**: Sigfox, NB-IoT
3. **A-C-G**: Wi-Fi, BLE

Notice that we did not use any routing protocol or routing device so as to make all wireless technologies point-to-point from the transmitter device to the receiver one. In Table 1, we can see the physical devices used for every wireless technology. The message commander is always the main RPi on which our Testbed software runs.

The first step from the RPi to the transmitter device is a wired link using two GPIOs. We described a naïve protocol for this communication based on 2 one-way digital signals: *R* (for reset) and *S* (for sequence). The *S* signal fires a rising-edge interrupt on the IoT transmitter device, which increases the message sequence number and sends it if *R* is high or otherwise resets it for a new test.

Table 1. Physical equipment, depending on the wireless technology.

Wireless Technology	RF Link Band	Transmitter	Receiver	Gateway/Internet
6LoWPAN	ISM 2.4 GHz	T.I. CC2538 ARM Based Mote	T.I. CC2538 ARM Based Mote	*gateway:* BeagleBone Black
LoRaWAN	ISM 868 MHz	Pycom FiPy	Semtech SX1301 Based Mote	*gateway:* Raspberry Pi 4
Sigfox	ISM 868 MHz	Pycom FiPy	Sigfox Backend	*public Internet needed*
Zigbee	ISM 2.4 GHz	SiLabs MGM210P	SiLabs MGM210P	*gateway:* SiLabs SLWSTK6102A
Wi-Fi	ISM 2.4 GHz	Pycom FiPy	Raspberry Pi 4	*none*
BLE	ISM 2.4 GHz	Pycom FiPy	Raspberry Pi 4	*none*
NB-IoT	LTE band 20	Pycom FiPy	Vodafone Network	*public Internet needed*

The next steps (B, C, D) are the RF link and correspond to the communication between the IoT end-device and its receiver—what we can consider the *pure* IoT communication phase. This path can be between two *similar* devices (path B: 6LoWPAN, Zigbee, LoRaWAN; or path C: Wi-Fi, BLE) or between the end-device and a public *base-station-type* receiver device (path D: Sigfox, NB-IoT).

In the last steps, the message travels (F, G, H) back to the main RPi, which parses the data received for latency, error and stability calculations. All communications are local, except for the last piece in the case of Sigfox and NB-IoT (H), as their own nature and working principles imply the usage of the carrier's infrastructure and the public Internet to finally return back to the RPi.

It is worth noting that there might be other possible topologies and configurations for the wireless technologies, especially for pieces E, F, G, H, as long as they comply with their specifications and requirements. This whole work is focused on the very setup we used for each wireless technology, bearing in mind our aim to make the message path as *local* and simple as possible in order to have the most control over it.

The Transmitter IoT Device's Firmware

The firmware of the transmitter IoT device is straightforward: it only needs to listen to a rising-edge interrupt and send a message accordingly, taking into account the *S-R* signals protocol. As a reference, the following piece of code depicts an implementation of the required firmware in MicroPython used with FiPy devices (LoRaWAN, Sigfox, Wi-Fi, BLE, NB-IoT):

```
import ...
S = Pin('P21', mode = Pin.IN, pull=Pin.PULL_DOWN)
R = Pin('P22', mode = Pin.IN, pull=Pin.PULL_UP)n = 0x0
def pin_handler(arg):
          global n
          n = 0x0 if R.value() == 0 else n+1
          send_message(n)
          return
try:
          S.callback(Pin.IRQ_RISING, pin_handler)
except KeyboardInterrupt:
          sys.exit(0)
```

Depending on the technology under characterisation, *send_message(n)* would call the required methods. As we are using point-to-point communications between the transmitter device and the receiver device, the message they exchange only contains a text string with the message sequence number as payload—the other parameters shown in Section 2.3.4

herein are set by the receiver device/gateway/backend to be delivered to the main RPi. In fact, the only task the *receiver* is in charge of is completing that information and steering it back to the RPi.

2.2. Considerations Regarding Different Wireless Technologies

Since different technologies behave differently, have different requirements and provide different support on the development board's software, some aspects of implementation must be known by the reader:

- Sigfox: The message payload was always set to be 12 bytes—the maximum allowed;
- LoRaWAN: is the most common configuration of Spreading Factor (SF7), and bandwidth (125 kHz) was used;
- BLE: We used advertisements to spread the message (two transmissions for each message). We did this because several problems were encountered in timing, and too many losses appeared when advertising only once—too many even to consider BLE an IoT technology. However, we attribute this to the fact of not being able to use point-to-point messages and only advertisements, and advertisements were the only BL- supported feature by Pycom at the time of doing this work;
- NB-IoT: We used Vodafone SIM card, i.e., Vodafone LTE network, with the layer of Pycom Pybytes as a backend for receiving messages;
- Wi-Fi: Hypertext transfer protocol (HTTP) was used as the application layer to send messages as it is an utterly common layer in Wi-Fi utilisation;
- 6LoWPAN: User datagram protocol (UPD) was used as the top layer to send messages;
- Zigbee: The clean Zigbee stack was used.

2.3. The Testbed's Interface

The Testbed's user interface is based on representational state transfer (REST) requests. Therefore, our Testbed provides an HTTP endpoint on port 8080 to listen to REST requests—get, put, post. A Node.js instance—the Testbed's interface backend—is listening to those requests so as to summon distinct actions accordingly.

So far, the basic, essential functions have been implemented, aiming to develop a more user-friendly interface with deeper functionality in the near future. It is noteworthy that two main types of resources can be categorised: (1) those used by the users themselves, i.e., the pure user interface described in Sections 2.3.1–2.3.3 and (2) the resource needed by IoT devices to send messages and thereby measure latency, error and stability, as described in Section 2.3.4

2.3.1. Start Test (Route: POST /start/{*idtech*}/period/{*period*}/limit/{*limit*})

This functionality must be invoked to start a new test for any wireless technology. The following parameters must be specified in the uniform resource identifier (URI) contents: wireless technology, period of transmissions and message limit, where:

- *idtech* is an integer designating the wireless IoT technology under test (required);
- *period* is the period between transmissions in milliseconds (defaults to 10,000);
- *limit* is the message limit (defaults to 100).

For instance, to start a 6LoWPAN test with half a second between messages and one thousand thereof, the request would be: /start/1/period/500/limit/1000.

2.3.2. Print Current Results (Route: GET /print)

This functionality prints the test results thus far on a remote secure shell (SSH) terminal, with the test still running. The user must have established an SSH connection with the RPi to see the results. Although it might be counterintuitive, results are not part of the request's response but a log in the SSH terminal. This functionality might be modified, as it seems more useful to send results alongside the REST response. They are presented in the

same format as described in Section 2.3.3 herein. This resource is useful to check the proper performance of an ongoing test.

2.3.3. Stop Test (Route: PUT/stop)

This invocation halts the current test, calculating the results and storing them in JavaScript Object Notation (JSON) format. The user may invoke this at any time to stop the ongoing test. The same functionality is auto-invoked if the test achieves the message limit, or any kind of exception occurs.

The JSON results file contains time (all timestamps in milliseconds) and loss information for every message as well as a summary with the most important information about the test. For instance, for the test in Section 2.3.1:

```
{
    ‘‘0’’:  {
        ‘‘start’’:                  1601290079097.324,
        ‘‘successful’’:             true,
        ‘‘end’’:                        1601290079127.223,
        ‘‘timestamp’’:              1601290079114,
        ‘‘latency’’:                29.899
    },
   ...
    ‘‘999’’:  {
        ‘‘start’’:                  1601290579130.133,
        ‘‘successful’’:             true,
        ‘‘end’’:                        1601290579152.390,
        ‘‘timestamp’’:              1601290579147,
        ‘‘latency’’:                22.257
    },
    ‘‘testInfo’’:  {
        ‘‘testStart’’:              1601290079071,
        ‘‘testEnd’’:                1601290579154,
        ‘‘limit’’:                  1000,
        ‘‘top’’:                        999,
        ‘‘period’’:                 500,
        ‘‘idtech’’:                 1,
        ‘‘avgLatency’’:             22.053,
        ‘‘minLatency’’:             19.573,
        ‘‘maxLatency’’:             283.493,
        ‘‘stdDev’’:                 11.220,
        ‘‘outliers’’:               32,
        ‘‘outliersRel’’:            3.20,
        ‘‘erorrCount’’:             0
        ‘‘errorRate’’:              0.00,
        ‘‘finishReason’’:                ‘‘limit’’
    }
}
```

For this kind of file, there are two main data groups:

- Individual message data (fields identified by a numeral, from “0” to “999” in this example):
    a. *start* is the timestamp when the IoT transmitter device was called to send the message;
    b. *successful* is a Boolean indicating if the message properly arrived at its destination;
    c. *end* is the timestamp when the RPi received the call-back from the IoT receiver device—the moment when the latency trip is completed;

d. *timestamp* is a timestamp recorded by some gateways when processing the messages (only for 6LoWPAN and LoRaWAN);
e. *latency* is the difference between *end* and *start*, i.e., the *latency* of the message.

- Whole test data (field "testInfo"):

a. *testStart* is the timestamp of the moment when the test began;
b. *testEnd* is the timestamp of the moment when the test finished;
c. *limit* is an integer indicating the number of messages defined in the test;
d. *top* is the maximum sequence number achieved when performing the test—it should be *limit*–1 if the test goes well;
e. *period* is the period between messages defined in the test configuration;
f. *idtech* is an integer designating the wireless technology;
g. *avgLatency* is the average *latency* for the whole test;
h. *minLatency* is the minimum registered *latency;*
i. *maxLatency* is the maximum registered *latency;*
j. *stdDev* is the standard deviation for the cluster of *latencies* recorded in the test;
k. *outliers* is the count of *latencies* out of *avgLatency* ±10%;
l. *outliersRel* is the relative number of outliers with respect to *top*+1;
m. *errorCount* is the messages lost count during the test;
n. *errorRate* is the relative error rate—*errorCount* with respect to *top*+1;
o. *finishReason* is the reason the test finished; usually, the test finishes because the message count (*top*) reaches its *limit.*

2.3.4. Callback (Route: POST /callback)

This is the endpoint to which the device under characterisation (user-end) must steer its responses, also in JSON format. As stated before, this endpoint is located on the main Testbed device (RPi) to reduce temporal incongruences.

These messages are used to calculate latency and losses—therefore error and stability as well. Response messages were designed to be very small—so as to not be affected by some wireless technologies' highly restricted bitrates—and have the following format:

```
{
        "id":  idtech,
        "sq":  seq,
        "ts":  epoch_ms
}
```

where:

- *idtech* is an integer designating the wireless technology;
- *seq* is the message sequence number, useful to sort messages upon arrival, measure latency and determine losses;
- *epoch_ms* is the timestamp of the device under characterisation in milliseconds—however, this time is not used to calculate this kind of *latency* as the Testbed device uses its own time reference for that.

3. The Testbed's Temporal Characterisation

In this Section we analyse the temporal performance of our Testbed device, as time-keeping and congruence is crucial when characterising latencies in the order of a few milliseconds. In the upcoming Sections 3.1–3.3, the device is characterised precisely to demonstrate its ability to work with IoT typical latencies, determining its error range in Section 3.4.

According to the IoT wireless technology spec sheets and the previous literature [11,12,27], the fastest latencies to consider would be on the order of tens of milliseconds (~10 ms). Hence, with a conservative approach of *one order of magnitude* precision, the error of our Testbed device should be on the order of milliseconds (~1 ms) to properly be used in this scenario.

The main software of our Testbed is a Node.js application running on a Debian-based operating system (OS), which manages the requests and accordingly calculates the results for a given test. Neither Node.js nor Debian are real-time intended. That being so, they introduce a delay when reacting to events and performing actions. Furthermore, since Node.js is JavaScript-based, it is synchronous—special care with time-related matters must be taken [28].

To characterise the response time and stability of our Testbed, we evaluated three matters which are considered fundamental to properly portray the Testbed's temporal response [29–31]:

1. Stability responding to external interrupts (Section 3.1);
2. Temporal stability of the internal clock (Section 3.2);
3. Auto-delay when responding to self-events (Section 3.3).

Our system introduces a certain delay every time it needs to react to some event or perform some action. This delay must be characterised accordingly to evaluate its influence on *latency* measurements. From these three parameters, we can evaluate the Testbed's precision and accuracy.

3.1. The Testbed's Reaction to External Interrupts

We used a waveform generator (Keysight 33220A) to make a 50 Hz square wave, with edges to trigger a GPIO interrupt (both rising and falling edge) on the RPi, meaning that the interrupt triggers 100 times a second—a 10 ms interrupt period. This frequency of events is far beyond what is needed for wireless IoT characterisation—one per second as much.

With this procedure, the RPi stores a timestamp in microseconds: this allows us to determine the temporal stability of the Testbed as we are using fixed-frequency square wave edges to trigger the interrupts.

We let the application run, reacting to 1.15 million interrupts and storing their microseconds timestamps; it ran for 192 min. Let us claim one million values are enough for characterising the stability of the system. From this array of interruption timestamps, we extracted the periods of trigger—the difference between every pair of timestamps.

Then, we analysed the data using Matlab. The array of periods was converted to a cluster of errors between the observed period by the RPi vs. the deterministic period of the waveform generator. The latter was double-checked using an oscilloscope (Keysight Infiniium MSO8064A), sampling at 1 MS/s with 256 averages. The oscilloscope read out a low-value width of 9.9555 ms and a high-value width of 10.0448 ms.

These values must correspond to the periods measured by the RPi. In fact, there are two main groups of observed periods when plotting the recorded data (see Figure 2), for which the cumulative distribution probability is half for each set, as expected with a 50%-duty-cycle square wave.

Converting these values to differences of time with respect to the deterministic values of both the low part and high part of the square signal let us plot an error image of the observed periods. In Figure 3, we depict this fact assuming the average central value for splitting the set of values as the deterministic period. The absolute values of the time drift for both sides of the wave are plotted out as a whole (blue bars) as well as the cumulative probability (red line).

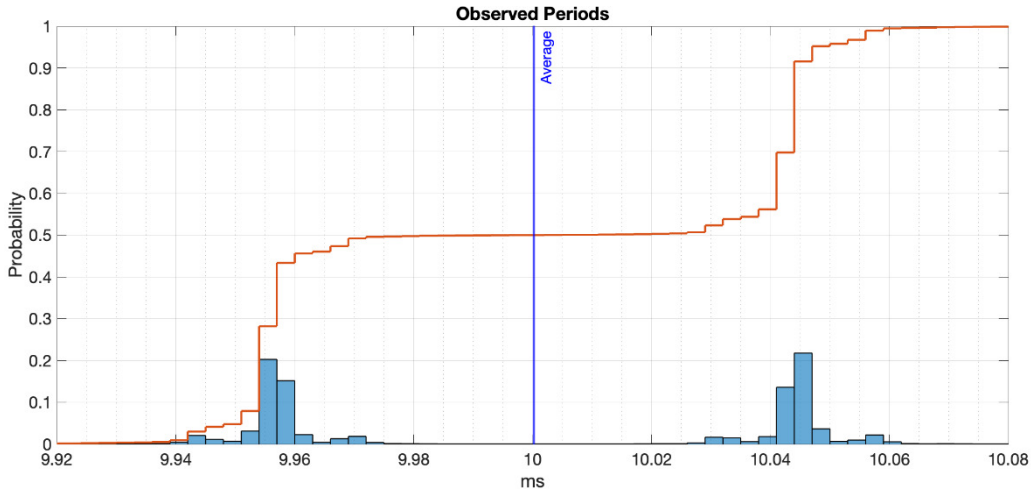


Figure 2. Histogram of the observed periods by the RPi reacting to an external 50 Hz square wave.

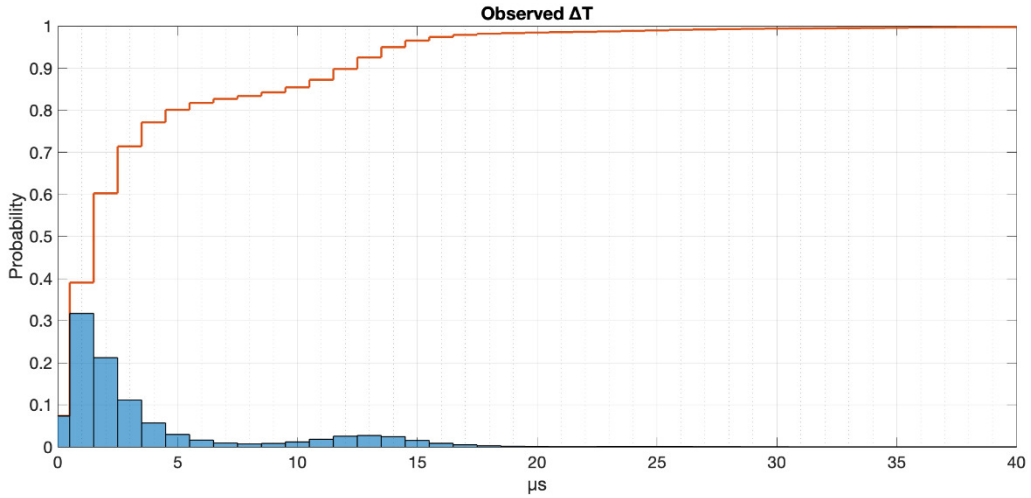


Figure 3. Histogram of the time drifting for both sides of the square wave.

As one can see, the time drifting realised when reacting to external interrupts is only a few microseconds, being <5 µs for 80% of the times, <12 µs for 90 % of the times and <15 µs for 95 % of the times. Table 2 depicts the most important data for this characterisation.

Table 2. Observed periods to external interrupts: important values.

Deterministic Low Width	Observed Avg. Low Period	Deterministic High Width	Observed Avg. High Period	90% Confidence ΔT
9.9555 ms	9.9556 ms	10.0448 µs	10.045 ms	12 µs

3.2. Temporal Stability of the Internal Clock

With this characterisation, we want to evaluate the long-term temporal stability of the Testbed's internal clock. We commanded the RPi to generate a 100 Hz square wave, toggling the logical value of a GPIO every 10 ms.

This GPIO was connected to a Nordic Semiconductor Power Profiler Kit II (PPK) with a 3.3 kΩ series resistor to measure current—the device we already checked as valid laboratory equipment in [11]. We set the PPK to sample the signal at a rate of 10 kS/s, complying with the Nyquist–Shannon sampling theorem for signals up to 5 kHz.

The data gathered with the PPK was processed in Matlab to determine its fast Fourier transform (FFT). Since the recorded signal it is a square wave, it will have *infinite* harmonics,

but the first one represents the fundamental frequency of the signal generated by the RPi, which is ideally 50 Hz—10 ms high, 10 ms low: 20 ms period.

In Figure 4, the FFT of the square wave generated by the RPi is depicted for a range of frequencies around the point of interest.

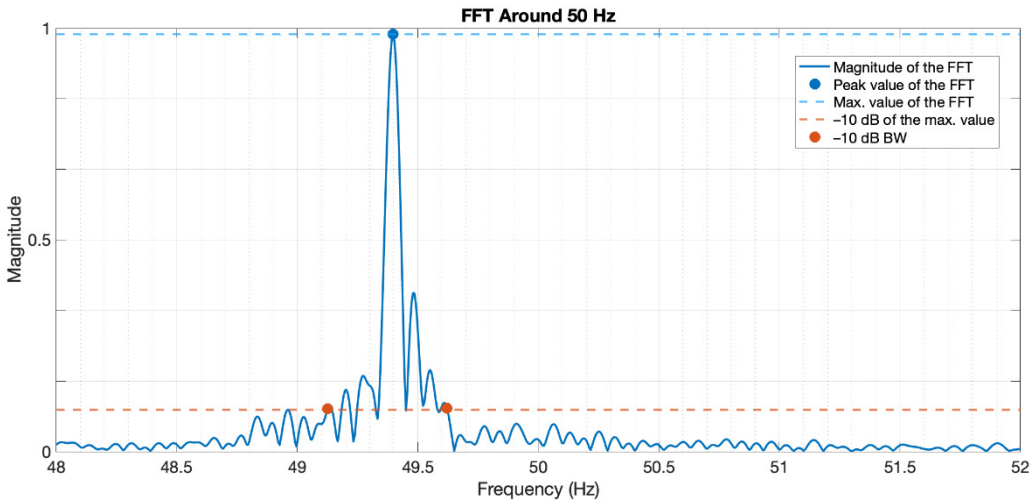


Figure 4. 50 Hz centred FFT of the RPi-generated square wave.

We can see that there is not only one peak at the desired frequency (50 Hz) but a predominant peak around 49.4 Hz with some small lobes around it—certain bandwidth (BW). This is due to the fact of the RPi not being 100% time-consistent. Moreover, the code itself and the OS resources spend some time that cannot be directly controlled. The magnitude of the signal does not show any units as the important matter is the relation in magnitude between the central frequency and the side lobes, and those values are also dependant on the FFT size. We also performed tests for other square wave frequencies between 10 Hz and 100 Hz, and the temporal deviation (in units of time) was coherent, which is the matter of interest for this analysis—not so, the frequency deviation, as it is relative to the frequency of the wave. Important data from this plot are shown in Table 3.

Table 3. Temporal stability of the Testbed's internal clock.

Target	Measured	Error	Relative Error	−10 dB BW [1]
50.0 Hz	49.4 Hz	0.6 Hz	1.2%	0.5 Hz
20.0 ms	20.24 ms	0.24 ms		49.1–49.6 Hz

[1] Range of frequency around the central peak for which the magnitude of the FFT is above a 10% of the peak magnitude.

With this, the error related to the internal clock's deviation can be claimed to have an average value of 240 µs, with 90% confidence values between 160 µs and 370 µs.

3.3. Self-Delay

To characterise the delay of the proper master device itself, having no other external reference per se, we used something we called a *hardware loop*—see Figure 5.

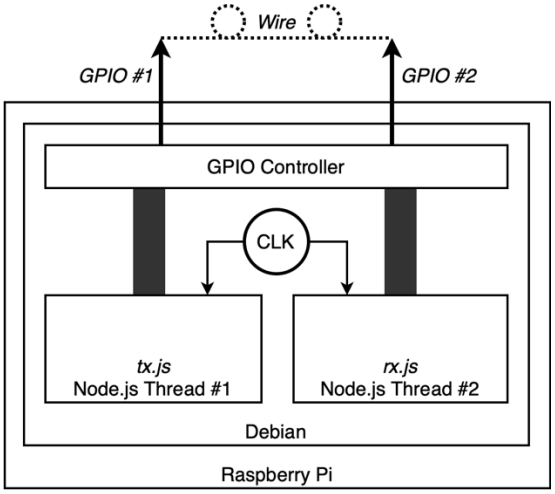


Figure 5. Hardware loop representation.

The *hardware loop* connects two GPIOs from the RPi in a manner that the proper Testbed device fires an interrupt on itself. Two Node.js threads are run, so that they do not interfere with one another:

1. *tx.js*: this process toggles a GPIO digital state, which is connected to another GPIO of the RPi, firing the interrupt; it stores the timestamp of the toggling process as well in microseconds;
2. *rx.js*: this process reacts to both rising and falling edge interrupts on the GPIO and stores the timestamp of the event in microseconds.

With this, we get two arrays of *equally referenced* timestamps: one corresponding to interruption command timestamps, the other corresponding to interruption reaction timestamps. The difference between them is the delay in charge of the Testbed device reacting to owned events. We set the *tx.js* script to fire an interrupt every 10 ms—100 per second. We let the test run for 24 h, thus firing more than eight million interruption events.

The average delay was 214.85 µs, with a standard deviation of 96.99 µs. The delays are depicted in Figure 6, along with the corresponding cumulative distribution function. As can be seen, 90% of the time, the introduced delay for self-reacting events is <240 µs.

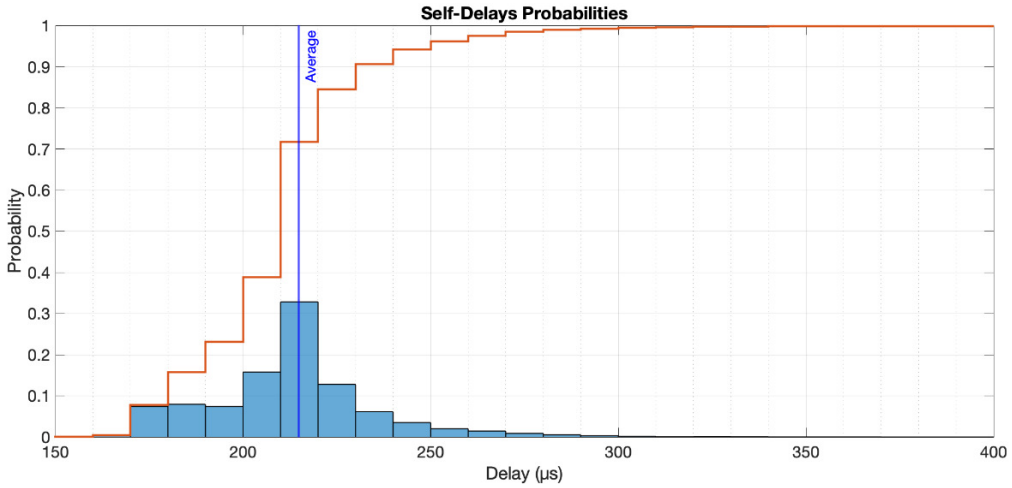


Figure 6. Self-delays probabilities.

3.4. Testbed's Error Range Validation

With the characterisation made in Sections 2.2 and 2.3, we have all the temporal variabilities of our device, with which we can estimate its error margin:

- External interrupts: the response to external interrupts seems to be very accurate and precise, with 90 % of drifting within 12 µs. Since we are working with latencies on the order of tens of milliseconds, we can consider this influence negligible (~0.1%).
- Internal clock: the internal clock presents an error in the order of hundreds of microseconds (240 µs), with 90% confidence values between 160 µs and 370 µs.
- Self-delay: the self-delay, which is probably the most important factor in our system since we are using the same Testbed to command external devices and measure time, has an average value around 215 µs, with a 90% confidence delay <240 µs and no values less than 160 µs.

With these matters, one can realise that the influences are always cumulative, meaning that the latencies measured by our Testbed will always be longer than actual latencies. Considering this, we can claim that the real latency of a message will be as in Equation (1):

$$\gamma = \varphi - \delta, \ \ \delta \in [320, \ 610] \ \mu s \tag{1}$$

where:

- γ is the actual latency;
- φ is the measured latency;
- δ is the introduced metering error, which is, according to our characterisation, a value in the range of 320 µs and 610 µs.

Thus, we can focus the result a little more, as in Equation (2):

$$\gamma \ (\text{ms}) = \varphi \ (\text{ms}) - \delta' - 0.32, \ \ \delta' \in [0, \ 0.29] \tag{2}$$

Hence, the error of our system can be said to be less than 290 µs, which means a relative error around 3% for latencies on the order of tens of milliseconds, i.e., that of most IoT wireless technologies. This error gets reduced as the wireless IoT latency increases, being around 1.5% for 20 ms, 0.6% for 50 ms, 0.3% for 100 ms, and negligible from 1 s and on—see Figure 7.

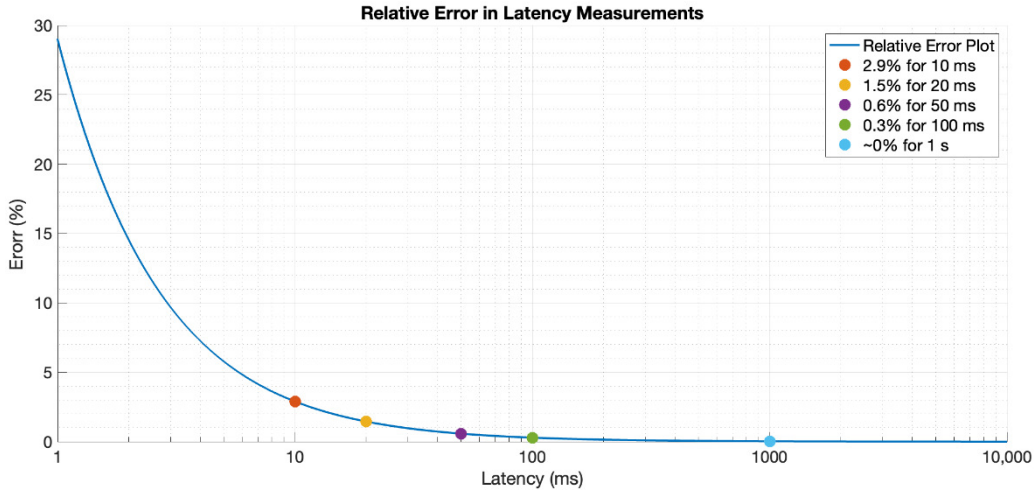


Figure 7. Testbed's relative error with respect to the latency value.

4. Measurements and Results

In this Section, we show example results for the measurements our Testbed can perform, proving its ability to perform communication reliability measurements with no regard to the wireless technology under test or the hardware platform used as IoT device. In Section 4.1, the Testbed's measuring parameters are presented; in Section 4.2 we analyse the performance of the following technologies, with expected latency in brackets [12]: 6LoWPAN (~20 ms), LoRaWAN (~300 ms), Sigfox (~4 s), Zigbee (~40 ms), Wi-Fi (~30 ms),

BLE (~30 ms) and NB-IoT (~2 s); following is a discussion about the results obtained in Section 4.3.

4.1. Parameters: Latency, Error, Stability

The three parameters that we evaluate in this work are: latency, error rate and stability. The following data is presented for each matter:

- Latency: minimum, average, maximum;
- Error rate: message loss count (Γ), relative error rate (E);
- Stability: standard deviation of latency (Λ), messages out of average latency $\pm$ 10%—outliers, both in absolute count (Π) and relative (K)—and a factor indicating a quality of stability (Ω) defined as in Equation (3) and Figure 8.

$$\Omega \ = \ [(1-\mathrm{E}) \times (1-\mathrm{K})]^2, \ \ \Omega, \mathrm{E}, \mathrm{K} \in [0, \ 1] \tag{3}$$

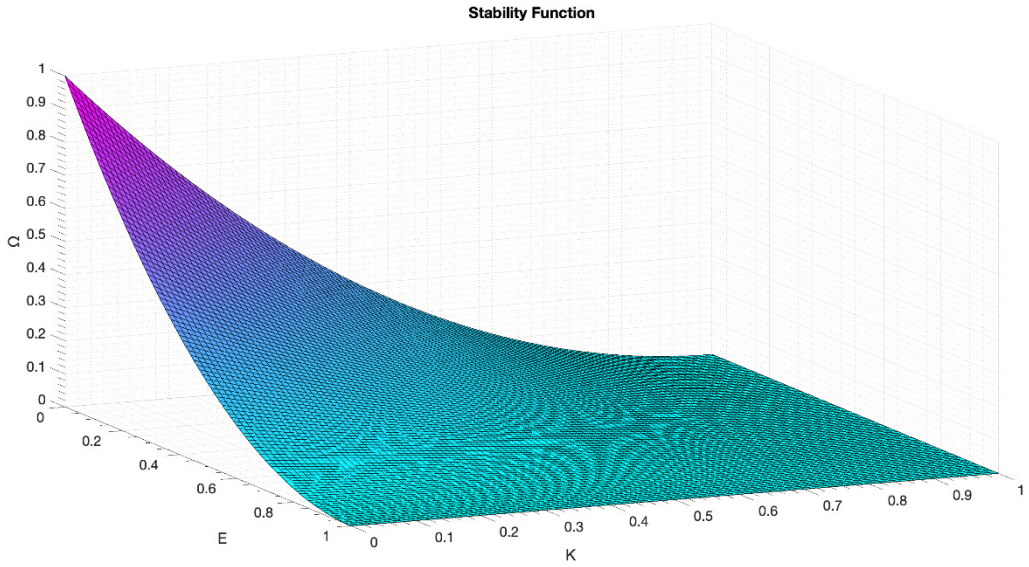


Figure 8. 3D plot of the stability function.

The stability function (Ω) serves as a rapid measurement of how accountable, reliable and congruent a designated technology in its performance is. It accounts for the variability of the latency and the number of losses. As can be seen, it rapidly decreases with any of the factors involved, as any small variation in the expected behaviour of the wireless protocol could eventually lead to fatal phenomena in critical applications—provided that strong temporal stability or message integrity is needed [32–35].

4.2. Real Tests

We performed tests for every wireless technology under characterisation to confirm the versatility of the Testbed device. In Table 4, we show the summary of results for tests with a period of transmissions (PT, seconds) and a message limit (ML, number) as follows:

- 6LoWPAN: ML 10,000; PT 1
- LoRaWAN: ML 10,000; PT 1
- Sigfox: ML 100; PT 15
- Zigbee: ML 10,000; PT 1
- Wi-Fi: ML 10,000; PT 1
- BLE: ML 500; PT 10
- NB-IoT: ML 5000; PT 5

Table 4. Results summary.

Measurement		6LoWPAN	LoRaWAN	Sigfox	Zigbee	Wi-Fi	BLE	NB-IoT
Latency (ms)	Min.	19.522	282.40	3467.1	34.174	25.294	13.382	329.29
	Avg.	22.116	296.96	3695.2	48.298	32.300	26.974	1797.3
	Max.	356.14	334.81	5651.0	95.295	178.10	125.40	10,275
Error	Γ	2	66	0	0	0	0	0
	E	0.02%	0.66%	0%	0%	0%	0%	0%
Stability	Λ (ms)	9.883	5.419	290.4	5.242	9.502	13.68	1352
	Π	386	2	4	2307	3197	480	4052
	K	3.86%	0.02%	4%	23.1%	31.9%	96.0%	81.0%
	Ω	0.924	0.993	0.922	0.592	0.463	0.002	0.036

These results function as a reference for every wireless technology in the scope, and the number of messages is representative so as to determine losses and stability—not for Sigfox due to its own limitations, but the results were consistent every time we repeated the test. It also confirms the universal aim of the Testbed developed.

In Appendix B, the reader can see cropped plots for the results depicted in Table 4 as a visual reference of the latency behaviour. In these plots, one thousand messages are usually depicted—except for Sigfox (100) and BLE (500)—with a light blue area indicating the non-outlying zone for stability calculation and an orange horizontal line representing the average *latency*.

4.3. Results Discussion

The results obtained within this work comply with those related in the literature and the protocol spec sheets: tens of milliseconds for 6LoWPAN, Zigbee, Wi-Fi and BLE; hundreds of milliseconds for LoRaWAN; some seconds for Sigfox and NB-IoT.

NB-IoT is the rarest scenario, since it is supposed to be a managed network with a strong infrastructure, and even quality of service (QoS). However, it presents a hard oscillatory behaviour with strong latency peaks, some of which even reach more than ten seconds—although this fact complies with the 3GPP Release-13 target of $\leq$10 s latency for 99% of messages [36].

Furthermore, we must consider that specifically in the case of NB-IoT, data travels through a backend of which we do not have any influence or knowledge. This backend (Pycom Pybytes) could be disturbing measurements and therefore be responsible for the incongruent, appealing peaks. The IoT device used as a transmitter device could also be misbehaving and altering the results. Nonetheless, this does not seem much of an option as this behaviour did not happen with Sigfox, which also relies on a public network and proprietary backend to work and for which we used the same development board as transmitter device (Pycom FiPy).

The selected devices always play some role in the final observed latencies as well as the specific topology actually deployed and even the software implemented. However, we can claim that the Testbed achieved its universal purpose, as we can measure latencies for a wide variety of wireless technologies and hardware platforms with truthful, consistent results. Furthermore, we demonstrated a proper accuracy for the Testbed with an error in the range of just 0–290 µs.

The selection of one technology over another would depend on the application requirements. On the one hand, thanks to the stability definition, we can have an overview of the uniformity in latency and error rate. On the other hand, with the latency measurement we get to know the immediacy in response to an event.

Generally, if the data are too sensitive (error and stability) and immediacy (latency) is not a strong requirement, one may choose Sigfox or LoRaWAN. If more immediacy is required, Zigbee and 6LoWPAN happen to be the perfect choice. Provided we need a high immediacy but stability is not a crucial factor, Wi-Fi tends to be an option.

In spite of that, if the use case had other specific key requirements, superseding latency, error rate and stability, those must be the decisive ones. For instance, if cost and low energy consumption play a key role, BLE would be the choice, but NB-IoT would be the preferred option for applications deployed in a wide area with hundreds or thousands of sensors.

It is noticeable that Zigbee, Wi-Fi and BLE present no losses. We point this to the following facts:

- Zigbee: we used the whole Zigbee stack, which handles losses itself.
- Wi-Fi: we used HTTP, which works over Transmission Control Protocol (TCP) and therefore handles losses as well.
- BLE: as stated in Section 2.2 hereof, we advertised every message twice, so the chance for the message getting lost is negligible.

Yet, it was no surprise that Sigfox and NB-IoT provided no losses. In the case of Sigfox it is due to the robustness of Sigfox's ultra-narrow band (UNB) modulation and the fact that every message is sent three times in three different carriers [37,38]—with the counterpart of slowness. In the case of NB-IoT, it uses a proprietary band with restricted access and QoS, and NB-IoT has its target in handling more than 50,000 devices per sector [36], which is very far from actuality at the moment of doing this work.

5. Conclusions

In this work, we presented a universal Testbed to characterise IoT wireless technologies in three crucial factors: latency, error rate and stability. The Testbed was characterised in Section 3, where we demonstrated its ability to measure time-sensitive matters—such as latency—with an error of 3%: <290 µs for typical IoT latencies around tens of milliseconds. For the wireless IoT technologies characterised in this work as exemplification, the results obtained fell in the expected range, which also helps validate the Testbed's performance.

The main advantages of this Testbed device are:

- Technology-agnostic: it has been designed to characterise any IoT wireless technology, with independence of the communication architecture and the protocols used;
- Cost, time, and resource efficient: it is based on the affordable Raspberry Pi board, and it can work on any Linux machine with a Node.js runtime;
- Portable and easy to deploy: the Testbed design allows its transportation and set up in any location;
- Replicable and scalable: based on standard HW and SW tools, it is easy to replicate, adapt and improve to measure other timing parameters.

Future Sights

To enhance the work in this matter, more technologies should be evaluated to keep the universal track of the Testbed device, such as Thread—based on 6LoWPAN and part of the future Matter [39] or GPRS—which are still widely used nowadays in machine-to-machine (M2M) communications.

Furthermore, the different IoT protocols should be more equated in terms of open systems interconnection (OSI) layers—although the OSI model (see Figure 9) may not be truly accurate for all of these IoT wireless technologies and some terminology might change, it serves as a reference [40–46]. In the tests performed within this work, we evaluated the following technologies at different layers:

- Applications: Zigbee, NB-IoT, Wi-Fi (HTTP);
- Transport: Sigfox, 6LoWPAN (UDP);
- Network: LoRaWAN;
- Data Link: BLE (advertisements, two repetitions per message).

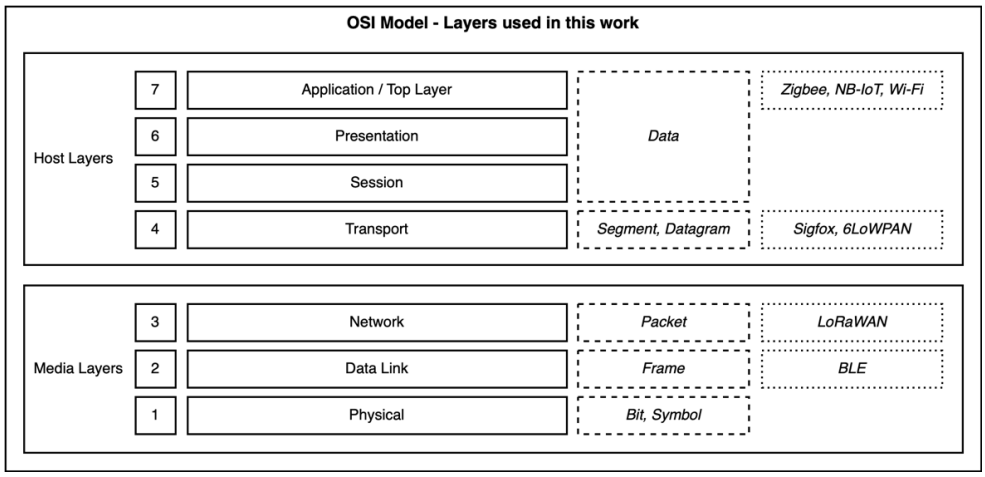


Figure 9. OSI model layer reference related to the specific layers we used with each wireless technology, showing its primary function, and data meaning and contents.

As one can see, different layers were used in different technologies, and some of them already implement recovery mechanisms or error mitigations. Moreover, there are limitations regarding some technologies in the use of certain layers:

- Zigbee, Sigfox, LoRaWAN: due to their own nature and definition, those layers are the ones to use between the end device and the receiver on the RF link;
- BLE: the equipment used in this work (Pycom FiPy), only supported BLE advertisements when doing these tests—other manufacturers may provide support for upper layers;
- NB-IoT: at the moment of this work, we could only use Pybytes' abstraction layer to send and receive NB-IoT messages; so, we are considering this the top layer.

Nonetheless, using the aforementioned layers is significative for IoT wireless technologies characterisation, as they are those of the most used layers in each technology. Yet, for 6LoWPAN, we could implement constrained application protocol (CoAP) or MQTT on the application layer to perform these tests as well because they are the most used top-layer-protocols for this technology. Into the bargain, even high-level, novel, IoT-targeted enhancements for future-proving existing wireless technologies could be tested, such as that in [47], in which Chen et al. present a Wi-Fi modification specifically designed to accommodate the large amount of data and nodes the IoT brings, or that in [48], in which Magsi et al. propose an adaptive data transmission framework for healthcare applications.

Additionally, it could be useful to implement a graphical web interface to display results and command tests apart from the command-line interface we have so far, and implementing some sort of logarithmic function—or other function of interest—to the period between messages could be helpful to perform stress tests, as the period would shrink continuously until an error threshold was reached.

Author Contributions: Conceptualization, methodology, validation, E.S. and G.d.C.; software, E.S. and L.M.; hardware, laboratory work, formal analysis, resources, visualization, data curation, E.S.; investigation, E.S., L.M. and G.C.; writing—original draft preparation, E.S.; writing—review and editing, supervision, G.d.C.; project administration, funding acquisition, A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work is part of the CHIST-ERA research project "ABIDI: Context-aware and Veracious Big Data Analytics for Industrial IoT", funded by the State Research Agency (AEI) of Ministerio de Ciencia e Innovación (MICINN) of Spain, grant number PCI2019-103762; and the research project "TECH-IoT: Tecnologías IoT para Interoperabilidad en Industria con Servicios de Uso Intensivo de Datos y Funciones de Control", funded by the AEI-MICINN of Spain, grant number EIN2019-103263.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Appendix A

This appendix contains an additional diagram for Section 2—Figure 1.

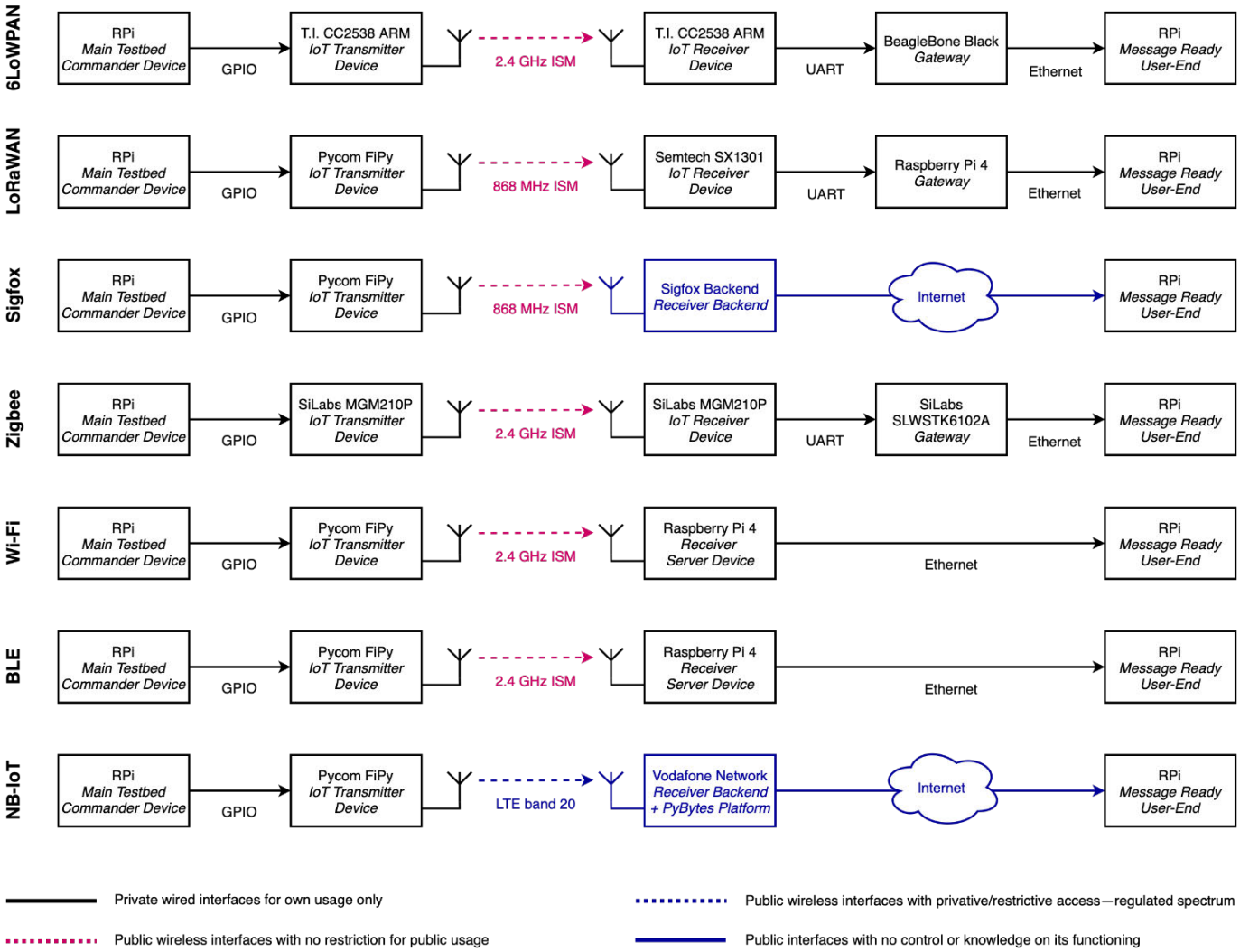


Figure A1. Detailed message paths for the wireless technologies characterised in this work, depicting the devices and interfaces used in each step. Note that other configurations—provided they comply with the standard—could be used, but these are the ones actually deployed in the laboratory for characterisation and Testbed validation. We also wanted to implement the most local approach possible in order to have more control over the message path.

Appendix B

This appendix contains plots for the latency measurements presented in Table 4.

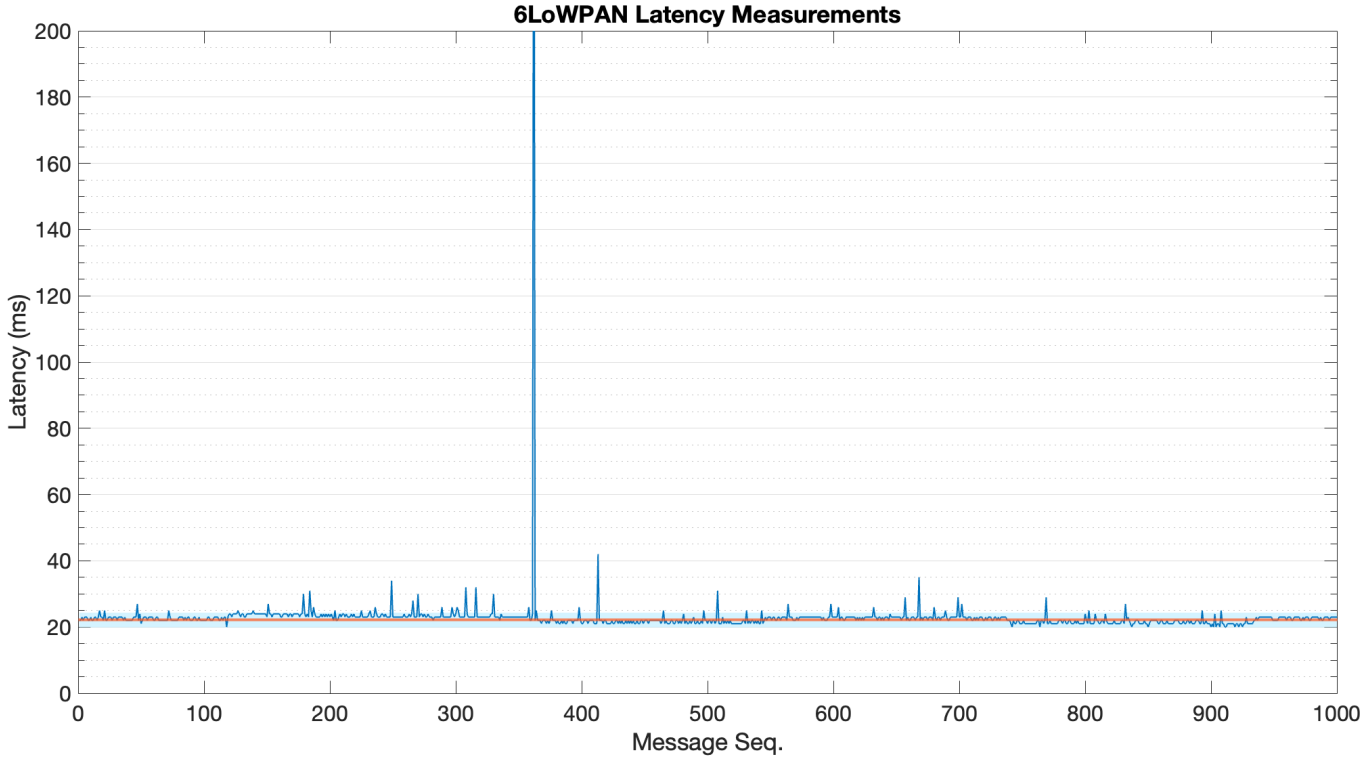


Figure A2. Latency plot for 6LoWPAN.

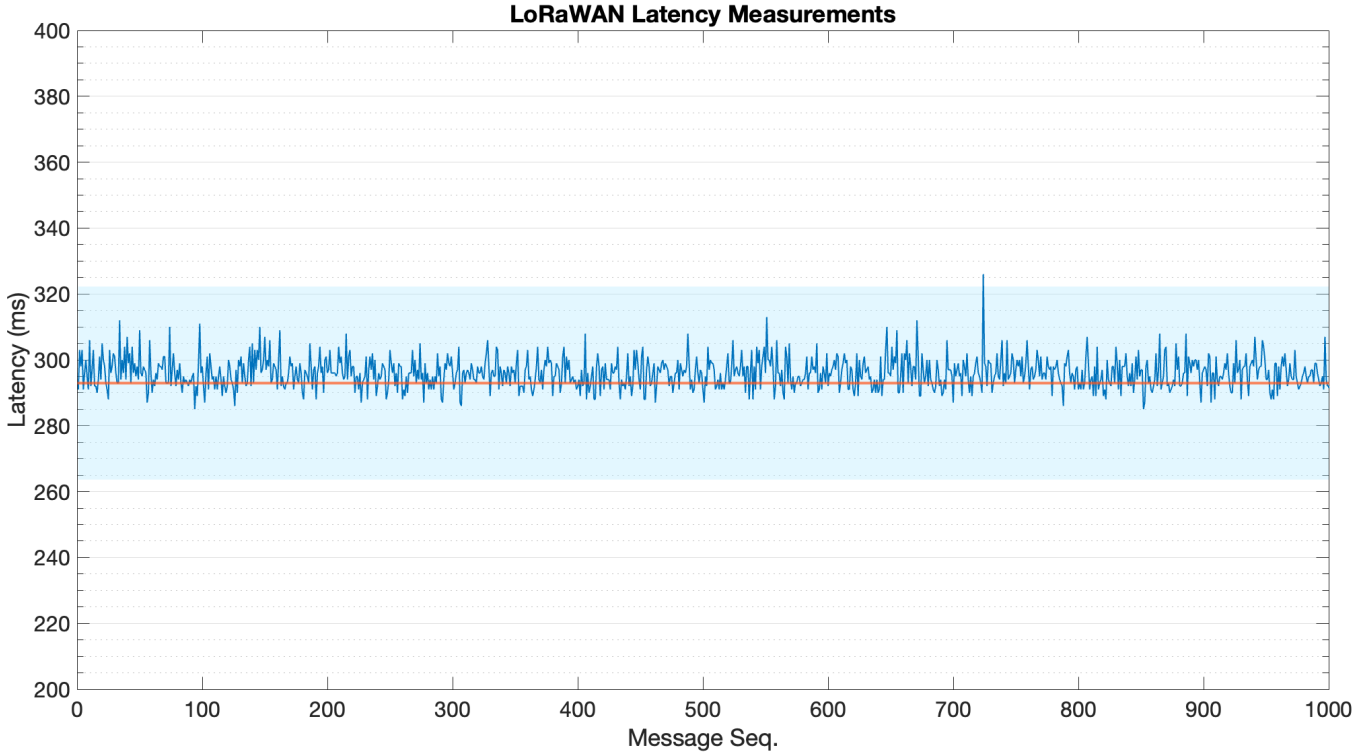


Figure A3. Latency plot for LoRaWAN.

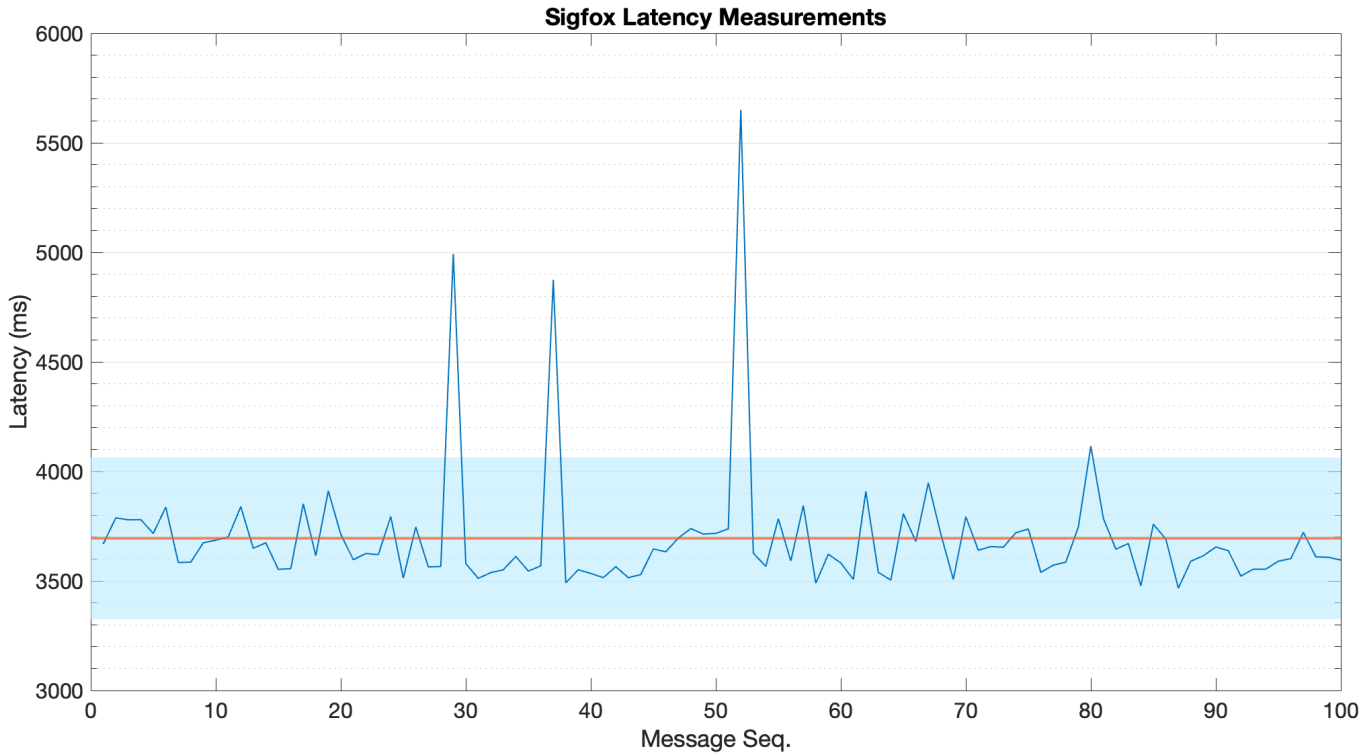


Figure A4. Latency plot for Sigfox.

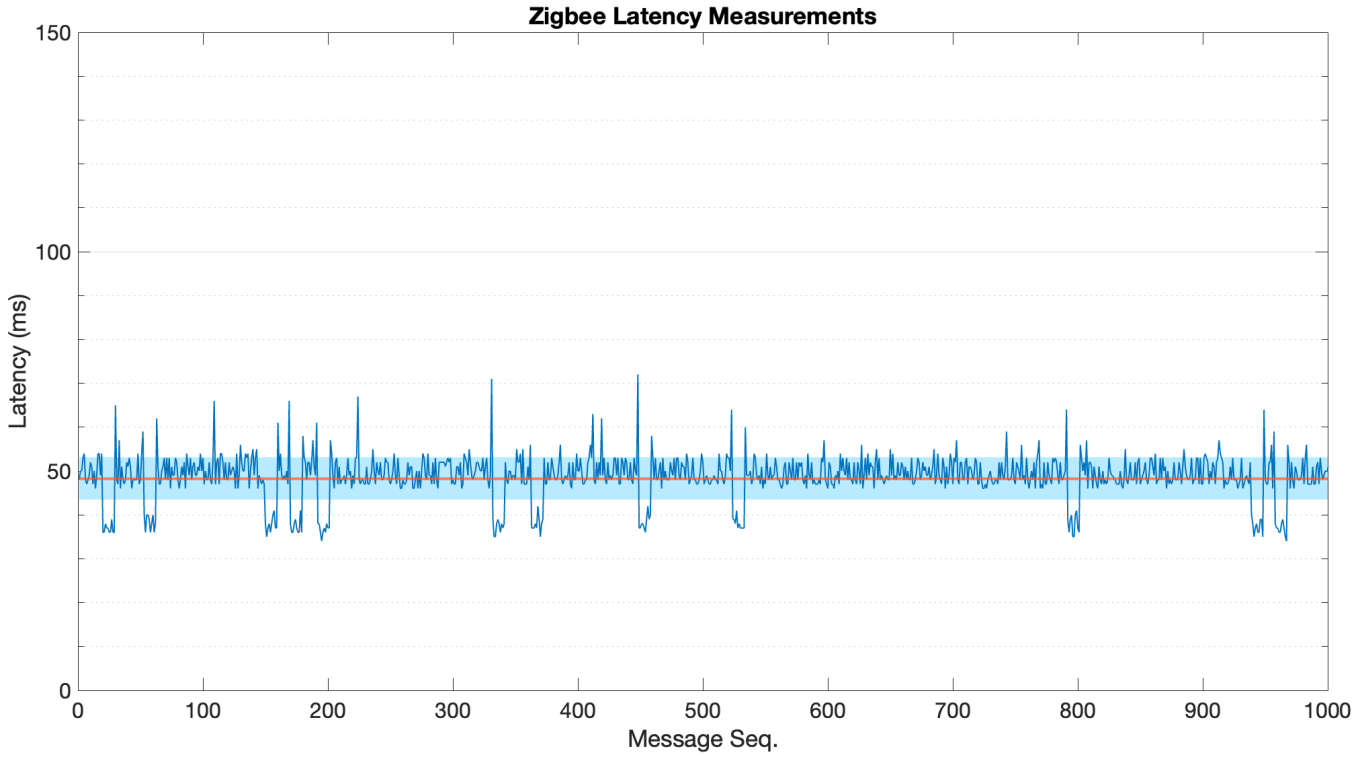


Figure A5. Latency plot for Zibgee.

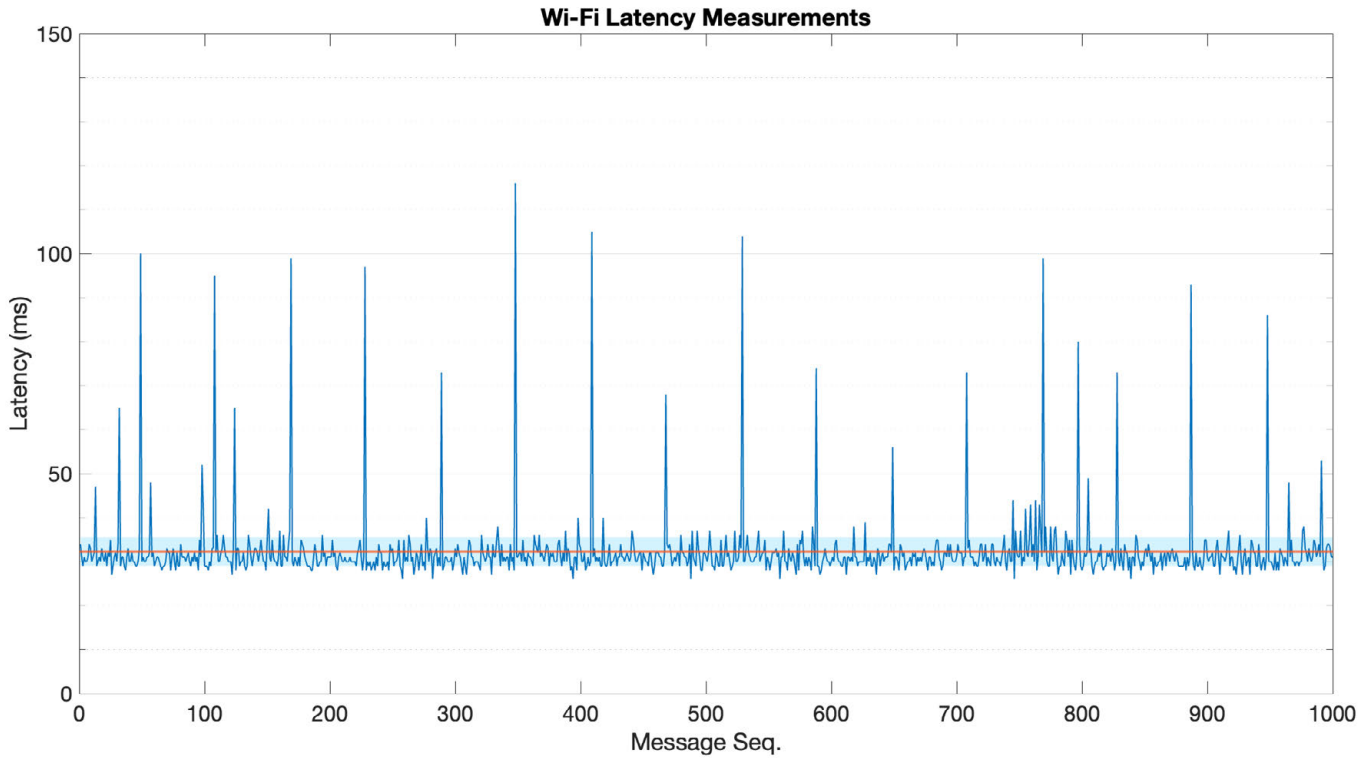


Figure A6. Latency plot for Wi-Fi.

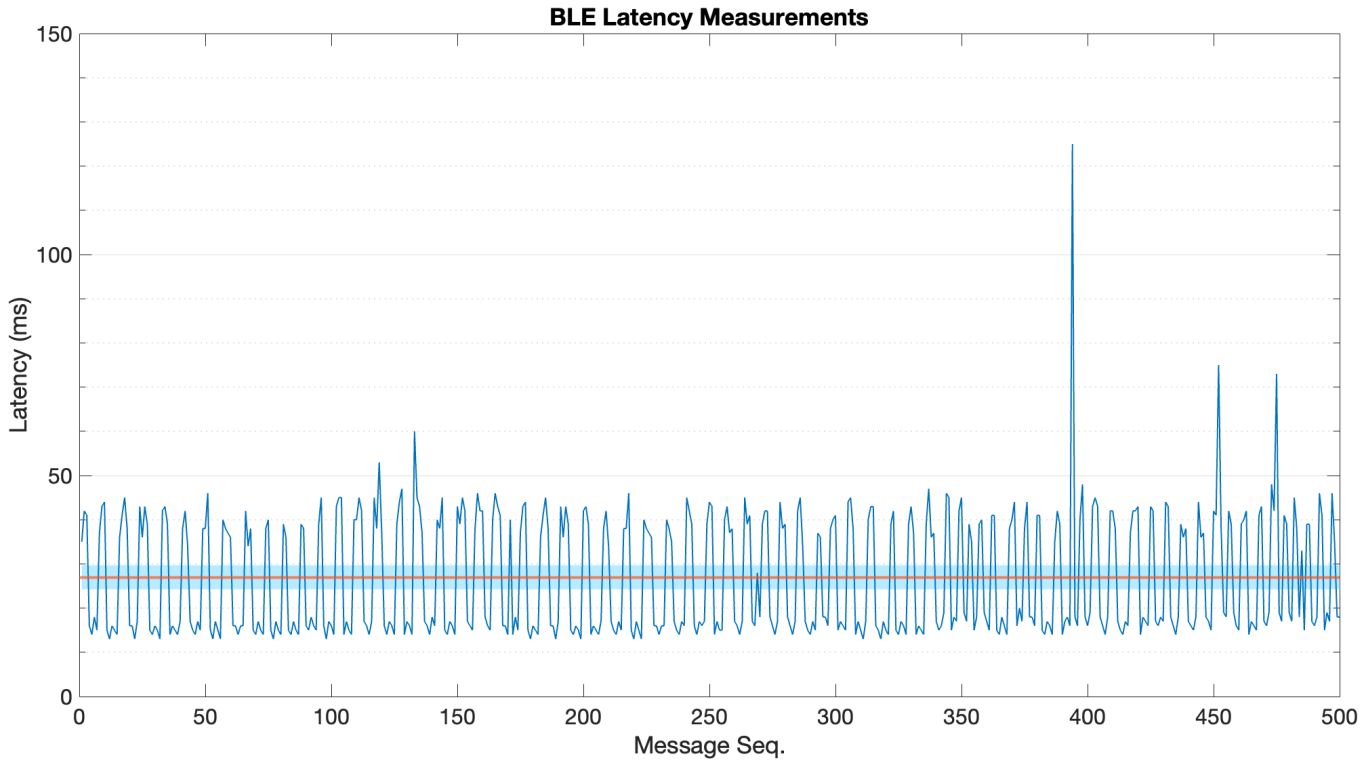


Figure A7. Latency plot for BLE.

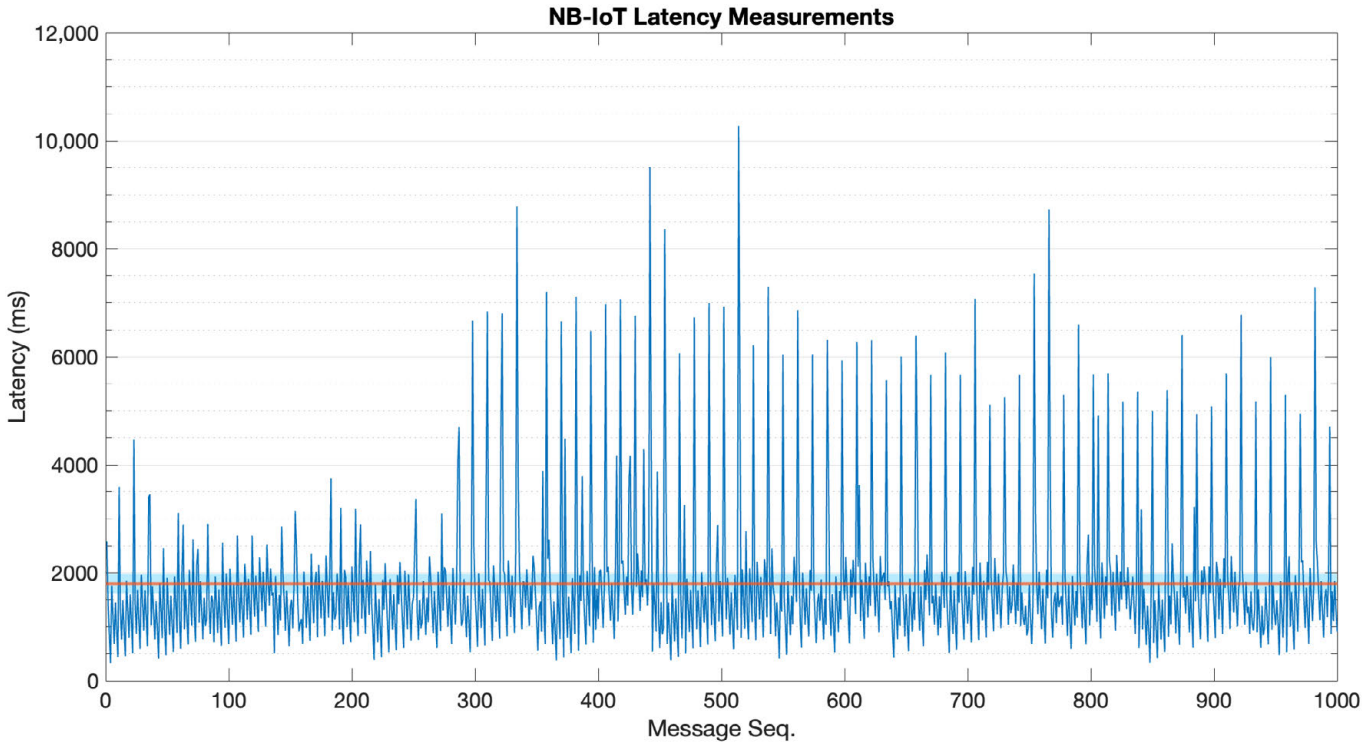


Figure A8. Latency plot for NB-IoT.

References

1. Wegner, P. Global IoT Spending to Grow 24% in 2021, Led by Investments in IoT Software and IoT Security. Available online: https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/ (accessed on 14 April 2022).
2. Evans, D. The Internet of Things. How the Next Evolution of the Internet Is Changing Everything. Available online: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed on 14 April 2022).
3. Maayan, G.D. The IoT Rundown For 2020: Stats, Risks, and Solutions. Available online: https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx (accessed on 14 April 2022).
4. Newman, D. Return on IoT: Dealing with the IoT Skills Gap. Available online: https://www.forbes.com/sites/danielnewman/2019/07/30/return-on-iot-dealing-with-the-iot-skills-gap/?sh=5f453ccb7091 (accessed on 20 May 2022).
5. Fotrune Business Insights Global IoT Market to be Worth USD 1463.19 Billion by 2027 at 24.9% CAGR; Demand for Real-Time Insights to Spur Growth. Available online: https://www.globenewswire.com/en/news-release/2021/04/08/2206579/0/en/Global-IoT-Market-to-be-Worth-USD-1-463-19-Billion-by-2027-at-24-9-CAGR-Demand-for-Real-time-Insights-to-Spur-Growth-says-Fortune-Business-Insights.html (accessed on 14 April 2022).
6. Farrell, S. (Ed.) Low-Power Wide Area Network (LPWAN) Overview. Available online: https://tools.ietf.org/pdf/rfc8376.pdf (accessed on 20 May 2022).
7. Chaudhari, B.S.; Zennaro, M.; Borkar, S. LPWAN Technologies: Emerging Application Characteristics, Requirements, and Design Considerations. *Future Internet* **2020**, *12*, 46. [CrossRef]
8. Internet of Business Bluetooth and ZigBee to Dominate Wireless IoT Connectivity. Available online: https://internetofbusiness.com/iot-driving-wireless-connectivity/ (accessed on 20 May 2022).
9. Pasqua, E. 5 Things to Know About the LPWAN Market in 2021. Available online: https://iot-analytics.com/5-things-to-know-lpwan-market/ (accessed on 20 May 2022).
10. IoT Analytics State of IoT 2021: Number of Connected IoT Devices Growing 9% to 12.3 Billion Globally, Cellular IoT Now Surpassing 2 Billion. Available online: https://iot-analytics.com/number-connected-iot-devices/ (accessed on 20 May 2022).
11. Saavedra, E.; Mascaraque, L.; Calderon, G.; del Campo, G.; Santamaria, A. The Smart Meter Challenge: Feasibility of Autonomous Indoor IoT Devices Depending on Its Energy Harvesting Source and IoT Wireless Technology. *Sensors* **2021**, *21*, 7433. [CrossRef] [PubMed]
12. del Campo, G.; Gomez, I.; Cañada, G.; Piovano, L.; Santamaria, A. Guidelines and criteria for selecting the optimal low-power wide-area network technology. In *LPWAN Technologies for IoT and M2M Applications*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 281–305, ISBN 978-0-12-818880-4.
13. Hedi, I.; Speh, I.; Sarabok, A. IoT network protocols comparison for the purpose of IoT constrained networks. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017; pp. 501–505. [CrossRef]

14. Moraes, T.; Nogueira, B.; Lira, V.; Tavares, E. Performance Comparison of IoT Communication Protocols. In Proceedings of the 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy, 6–9 October 2019; pp. 3249–3254. [CrossRef]
15. Al-Kashoash, H.A.A.; Kemp, A.H. Comparison of 6LoWPAN and LPWAN for the Internet of Things. *Aust. J. Electr. Electron. Eng.* **2016**, *13*, 268–274. [CrossRef]
16. Anand, P.; Singh, Y.; Selwal, A.; Singh, P.K.; Felseghi, R.A.; Raboaca, M.S. IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications towards Smart Grids. *Energies* **2020**, *13*, 4813. [CrossRef]
17. Malhotra, P.; Singh, Y.; Anand, P.; Bangotra, D.K.; Singh, P.K.; Hong, W.-C. Internet of Things: Evolution, Concerns and Security Challenges. *Sensors* **2021**, *21*, 1809. [CrossRef]
18. Pereira, C.; Pinto, A.; Ferreira, D.; Aguiar, A. Experimental Characterization of Mobile IoT Application Latency. *IEEE Internet Things J.* **2017**, *4*, 1082–1094. [CrossRef]
19. Mroue, H.; Nasser, A.; Hamrioui, S.; Parrein, B.; Motta-Cruz, E.; Rouyer, G. MAC layer-based evaluation of IoT technologies: LoRa, SigFox and NB-IoT. In Proceedings of the 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), Jounieh, Lebanon, 18–20 April 2018; pp. 1–5. [CrossRef]
20. Sinha, R.S.; Wei, Y.; Hwang, S.-H. A survey on LPWA technology: LoRa and NB-IoT. *ICT Express* **2017**, *3*, 14–21. [CrossRef]
21. Alsukayti, I.S. A Multidimensional Internet of Things Testbed System: Development and Evaluation. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 1–17. [CrossRef]
22. Schulz, P.; Matthe, M.; Klessig, H.; Simsek, M.; Fettweis, G.; Ansari, J.; Ashraf, S.A.; Almeroth, B.; Voigt, J.; Riedel, I.; et al. Latency Critical IoT Applications in 5G: Perspective on the Design of Radio Interface and Network Architecture. *IEEE Commun. Mag.* **2017**, *55*, 70–78. [CrossRef]
23. Ma, Z.; Xiao, M.; Xiao, Y.; Pang, Z.; Poor, H.V.; Vucetic, B. High-Reliability and Low-Latency Wireless Communication for Internet of Things: Challenges, Fundamentals, and Enabling Technologies. *IEEE Internet Things J.* **2019**, *6*, 7946–7970. [CrossRef]
24. Atutxa, A.; Franco, D.; Sasiain, J.; Astorga, J.; Jacob, E. Achieving Low Latency Communications in Smart Industrial Networks with Programmable Data Planes. *Sensors* **2021**, *21*, 5199. [CrossRef] [PubMed]
25. Hossain, M.; Noor, S.; Karim, Y.; Hasan, R. IoTbed: A Generic Architecture for Testbed as a Service for Internet of Things-Based Systems. In Proceedings of the 2017 IEEE International Congress on Internet of Things (ICIOT), Honolulu, HI, USA, 25–30 June 2017; pp. 42–49. [CrossRef]
26. Rana, B.; Singh, Y.; Singh, P.K. A systematic survey on internet of things: Energy efficiency and interoperability perspective. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4166. [CrossRef]
27. Deutsche Telekom IoT NB-IoT, LoRaWAN, Sigfox: An Up-to-Date Comparison. Available online: https://iot.telekom.com/resource/blob/data/492968/e396f72b831b0602724ef71056af5045/mobile-iot-network-comparison-nb-iot-lorawan-sigfox.pdf (accessed on 20 October 2021).
28. Madsen, M.; Tip, F.; Lhoták, O. Static analysis of event-driven Node.js JavaScript applications. *ACM SIGPLAN Not.* **2015**, *50*, 505–519. [CrossRef]
29. Reisizadeh, A.; Pedarsani, R. Latency analysis of coded computation schemes over wireless networks. In Proceedings of the 2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 3–6 October 2017; pp. 1256–1263. [CrossRef]
30. Chen, P.W.-C.; Sastry, S.S. Latency and Connectivity Analysis Tools for Wireless Mesh Networks. Available online: http://www2.eecs.berkeley.edu/Pubs/TechRpts/2007/EECS-2007-87.html (accessed on 20 May 2022).
31. Ageev, A.; Macii, D.; Petri, D. Experimental Characterization of Communication Latencies in Wireless Sensor Networks. Available online: https://www.imeko.org/publications/tc4-2008/IMEKO-TC4-2008-170.pdf (accessed on 20 May 2022).
32. Soltani, S.; Misra, K.; Radha, H. On link-layer reliability and stability for wireless communication. In Proceedings of the 14th ACM International Conference on Mobile Computing and Networking-MobiCom'08, San Francisco, CA, USA, 14–19 September 2008; ACM Press: San Francisco, CA, USA, 2008; p. 327. [CrossRef]
33. Hong, S.; Chun, Y. Efficiency and stability in a model of wireless communication networks. *Soc. Choice Welf.* **2010**, *34*, 441–454. [CrossRef]
34. Thomas, S.R.; Tucker, R.L.; Kelly, W.R. Critical Communications Variables. *J. Constr. Eng. Manag.* **1998**, *124*, 58–66. [CrossRef]
35. Liberal, F.; Ramos, M.; Fajardo, J.O.; Goia, N.; Bizkarguenaga, A.; Mesogiti, I.; Theodoropoulou, E.; Lyberopoulos, G.; Koumaras, H.; Sun, L.; et al. *User Requirements for Future Wideband Critical Communications*; Glyndwr University: Wrexham, UK, 2013; pp. 341–348.
36. Ratasuk, R.; Vejlgaard, B.; Mangalvedhe, N.; Ghosh, A. NB-IoT system for M2M communication. In Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, Doha, Qatar, 3–6 April 2016; pp. 1–5. [CrossRef]
37. Saavedra, E.; del Campo, G.; Santamaria, A. Smart Metering for Challenging Scenarios: A Low-Cost, Self-Powered and Non-Intrusive IoT Device. *Sensors* **2020**, *20*, 7133. [CrossRef]
38. Lavric, A.; Petrariu, A.I.; Popa, V. SigFox Communication Protocol: The New Era of IoT? In Proceedings of the 2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI), Lisbon, Portugal, 29–30 August 2019; pp. 1–4. [CrossRef]
39. Unwala, I.; Taqvi, Z.; Lu, J. Thread: An IoT Protocol. In Proceedings of the 2018 IEEE Green Technologies Conference (GreenTech), Austin, TX, USA, 4–6 April 2018; pp. 161–167. [CrossRef]

40. Alani, M.M. OSI Model. In *Guide to OSI and TCP/IP Models*; SpringerBriefs in Computer Science; Springer International Publishing: Cham, Switzerland, 2014; pp. 5–17, ISBN 978-3-319-05151-2.
41. Ramya, C.M.; Shanmugaraj, M.; Prabakaran, R. Study on ZigBee technology. In Proceedings of the 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, India, 8–10 April 2011; pp. 297–301. [CrossRef]
42. Oliveira, L.; Rodrigues, J.; Kozlov, S.; Rabêlo, R.; Albuquerque, V. MAC Layer Protocols for Internet of Things: A Survey. *Future Internet* **2019**, *11*, 16. [CrossRef]
43. Ertürk, M.A.; Aydın, M.A.; Büyükakkaşlar, M.T.; Evirgen, H. A Survey on LoRaWAN Architecture, Protocol and Technologies. *Future Internet* **2019**, *11*, 216. [CrossRef]
44. Ayoub, W.; Samhat, A.E.; Nouvel, F.; Mroue, M.; Prevotet, J.-C. Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1561–1581. [CrossRef]
45. Jha, R.K.; Puja; Kour, H.; Kumar, M.; Jain, S. Layer based security in Narrow Band Internet of Things (NB-IoT). *Comput. Netw.* **2021**, *185*, 107592. [CrossRef]
46. Salva-Garcia, P.; Alcaraz-Calero, J.M.; Wang, Q.; Bernabe, J.B.; Skarmeta, A. 5G NB-IoT: Efficient Network Traffic Filtering for Multitenant IoT Cellular Networks. *Secur. Commun. Netw.* **2018**, *2018*, 1–21. [CrossRef]
47. Chen, C.; Li, J.; Balasubramaniam, V.; Wu, Y.; Zhang, Y.; Wan, S. Contention Resolution in Wi-Fi 6-Enabled Internet of Things Based on Deep Learning. *IEEE Internet Things J.* **2021**, *8*, 5309–5320. [CrossRef]
48. Magsi, H.; Sodhro, A.H.; Al-Rakhami, M.S.; Zahid, N.; Pirbhulal, S.; Wang, L. A Novel Adaptive Battery-Aware Algorithm for Data Transmission in IoT-Based Healthcare Applications. *Electronics* **2021**, *10*, 367. [CrossRef]

IV. DOI: 10.3390/app14083411

Leveraging IoT Harmonization: An Efficacious NB-IoT Relay for Integrating 6LoWPAN Devices into Legacy IPv4 Networks

Applied Sciences 2024, 14, 3411

https://doi.org/10.3390/app14083411

Pages 115–133 present the original manuscript as published

applied sciences

MDPI

Article

Leveraging IoT Harmonization: An Efficacious NB-IoT Relay for Integrating 6LoWPAN Devices into Legacy IPv4 Networks

Edgar Saavedra *, Asuncion Santamaria, Guillermo del Campo and Igor Gomez

CeDInt-UPM, Universidad Politécnica de Madrid, Campus de Montegancedo, 28223 Pozuelo de Alarcón, Spain; asun.santamaria@upm.es (A.S.); guillermo.delcampo@upm.es (G.d.C.); igor.gomez@upm.es (I.G.)
* Correspondence: e.saavedra@upm.es

Featured Application: This novel approach provides a seamless, straightforward means to make 6LoWPAN devices—pragmatically any kind of incumbent from IPv6-based IoT networks—more accessible under the scope of the omnipresent, classic IPv4 Internet.

Abstract: The burgeoning complexity and heterogeneity of IoT networks, coupled with their rapid growth, constant evolution, and new players, present significant challenges in terms of connectivity, interoperability, management, and usability. These networks, composed of a diverse array of devices, technologies and the like, demand innovative solutions to bridge the gaps between different IoT technologies and communication protocols. This article presents a simple, yet efficacious communication Relay to address one of these critical gaps. This Relay uses NB-IoT to ease the integration of 6LoWPAN-based IoT devices (IPv6) into the public legacy Internet (IPv4). This device translates 6LoWPAN, IPv6 CoAP messages into Internet-standard REST requests, so that appropriate handling of devices' data be achieved in several stages. Thus, the Relay establishes two branches of communications: (i) the local network where the 6LoWPAN gateway is placed, and (ii) the public NB-IoT network. User interaction and data analysis are achieved by virtue of Home Assistant, where former 6LoWPAN devices are now discovered and shown as proper Home Assistant entities thanks to the Relay's ease of integration into the open-source platform. This novel approach not only ensures efficient data and network management, but it also meets the urgent necessity for advanced solutions in enhancing actual IoT interconnectivity and monitoring. The unprecedented pace at which IoT devices, players and different networks have been proliferating in recent times is not compatible with countless manufacturer-dependent platforms, applications, and proprietary protocols that the IoT field has been leading with so far, almost from its beginnings.

Keywords: IoT; LPWAN; NB-IoT; 6LoWPAN; LTE; home assistant; IPv6; wireless communications; wireless sensor networks

Citation: Saavedra, E.; Santamaria, A.; del Campo, G.; Gomez, I. Leveraging IoT Harmonization: An Efficacious NB-IoT Relay for Integrating 6LoWPAN Devices into Legacy IPv4 Networks. *Appl. Sci.* **2024**, *14*, 3411. https://doi.org/10.3390/app14083411

Academic Editors: Christos Markides, Achilleas Achilleos and Georgia Kapitsaki

Received: 9 March 2024
Revised: 31 March 2024
Accepted: 6 April 2024
Published: 18 April 2024

1. Introduction

In the era of the Internet of Things (IoT), the unprecedented proliferation of devices connected to the Internet has made them omnipresent. These devices, ranging from simple sensors to complex systems, are increasingly becoming the backbone of many critical applications across various sectors, including healthcare, agriculture, driving, smart cities, or industrial automation [1].

Nonetheless, the diversity of IoT technologies, including different communication protocols and network standards, poses significant challenges in achieving seamless interoperability. Specifically, the integration of 6LoWPAN (IPv6-based) devices within legacy IPv4 networks—classical internet networks—remains a critical hurdle, hindering the realization of the full potential of IoT applications [2,3].

The transition from IPv4- to IPv6-based computer machinery and networking has not been accomplished yet, with no real coexistence between the two [4–6]. In fact, there

are still several foundational issues to address for this movement to be completed, such as the following: (i) providing support and compatibility for certain operating systems, hardware and platforms; (ii) resolving unstable routing or name services; and (iii) managing discordant security policies.

The situation is not very different in the IoT scope, and is even worse. IoT devices used to count on fewer resources; they have less ease of expansion, and lack up-to-date, long-term service usage. Moreover, the heterogeneity and vast number of IoT devices exacerbate the challenges associated with achieving a seamless transition and interoperability between IPv4 and IPv6 in this very field [7–9]. This is compounded by the diversity of communication protocols that are unique to IoT ecosystems, which further complicate the will to integrate.

Thus, it is of paramount importance to deploy devices/systems that not only facilitate communications between IPv4 and IPv6 networks, but also address the unique constraints and very protocols of IoT devices. Such solutions require innovative, yet simple approaches to ensure compatibility among players, whilst providing efficacious, reliable connectivity in a greatly heterogeneous, resource-constrained environment.

1.1. Addressing the Unforeseen, Long-Term Byproducts

The significance of interoperability in the IoT cannot be overstated. This not only ensures that devices from different manufacturers can communicate with each other, but also facilitates the development of scalable, flexible, and more efficient IoT ecosystems. Despite the advances in networking technologies, the coexistence of IPv6-enabled devices—such as those based on 6LoWPAN—with the prevailing IPv4 infrastructure, presents a complex challenge. For decades, this challenge has been compounded by the fast evolution of IoT devices and the continuous invention of new technologies, techniques, solutions, protocols, and systems [9,10].

This study promotes a simple, novel, efficacious approach to address the interoperability challenge between 6LoWPAN and IPv4 networks through the design of a simple narrowband IoT (NB-IoT) Relay. This Relay performs as a bridge, enabling 6LoWPAN devices to communicate within legacy IPv4 networks seamlessly; at the same time, the former become visible within the all-IPv4 world. However, the approach of this research is not a tunnel. Tunneling solutions tend to be patches meant to overcome the lack of supporting hardware or compatible software, thereby providing IPv6 talkability to prevent isolation [11,12]. The Relay we propose, on the other hand, does not masquerade packets to make them compatible, but performs protocol translation for the sake of actual interoperability.

Our solution is not only simple, hassle-free, and cost-effective, but also offers an accountable method for data communication by translating 6LoWPAN, IPv6 CoAP messages into standard IPv4 RESTful requests. By facilitating this translation, the relay ensures that 6LoWPAN devices can be integrated into existing network infrastructures without significant changes or upgrades. This fact is crucial, considering the large number of infrastructures that may be dependent on IoT networks functioning properly, which would otherwise require significant analysis and costs to overhaul.

Using the NB-IoT offers several advantages such as wide coverage, high power efficiency, and agnostic infrastructures. These matters make the NB-IoT an ideal choice for IoT applications that require little human interaction, as well as those that are expected to be deployed in very heterogeneous and diverse use cases and locations [13,14]. Furthermore, the integration of the Relay with a Home Assistant (HA) [15,16], a state-of-the-art, open-source, *home-and-beyond* automation platform, exemplifies the practical application of the proposed solution, demonstrating its effectiveness in real-world scenarios, as well as our commitment to open sourcing.

1.2. Previous Literature

Given the unique nature of this project and the recent actual emergence of the NB-IoT, identifying case studies with similar objectives and complexities proved to be challenging. This project's distinctive problem statement and the incorporation of a broad range of apparently distant technologies span multiple areas of specialization. Nevertheless, there are a few projects worth mentioning—projects that embarked on facilitating this transition we are targeting.

One such initiative, as presented by Da Silva et al. in [17], aimed at the "Design and Construction of Wireless Sensor Network Gateway with IPv4/IPv6 Support". This project's primary objective was to develop a communication gateway facilitating bidirectional exchanges between IPv4/IPv6 clients and a 6LoWPAN sensor network. This endeavor involved setting up a 6LoWPAN sensor network using TinyOS-operated communication motes. The implementation leveraged TinyOS's BLIP protocol for IPv6 communication over IEEE 802.15.4 wireless links, complemented by client applications for both IPv6 and IpPv4 to request sensor readings from specific network nodes. The outcomes affirmed the gateway's capability to ensure interoperability between IPv6/IPv4 clients and the sensor network, enabling direct interactions with the sensor nodes.

Another interesting and novel approach, conceptually similar to ours, is that proposed by Arzo et al. in [18], who introduced a network format translator into a virtualized environment. This approach aims at bridging the gap between different IoT networks, enabling seamless communication across various technology platforms. By implementing a testbed utilizing the NS3 simulator, the study demonstrated the feasibility of communicating across different IoT technologies, such as transmitting packets between LoRaWAN, Wi-Fi, and 6LoWPAN networks. Nonetheless, it is worth noting that this approach does not focus on the actual, hassle-free IoT interoperability, but feasible technical realization—they did not carry out an actual test with in-the-flesh networks, but a simulation thereof using NS3.

Furthering the exploration into IPv6/IPv4 gateway implementations, another noteworthy project is "Network Processors Applied to IPv4/IPv6 Transition", as discussed by Grosse et al. in [19]. This research introduced a high-speed IPv6/IPv4 gateway utilizing network processors, which focuses on handling substantial traffic volumes and facilitating network address, port, and protocol translation (NAPT-PT) between IPv6 and IPv4 networks. The study detailed significant performance enhancements over conventional computer/server-based implementations, and addressed the limitations concerning network address and protocol translation and firewall processing compared to general-purpose processors.

Additionally, "A SOCKS-Based IPv6/IPv4 Gateway Mechanism", documented by Kitamura in [20], describes a SOCKS protocol-based IPv6/IPv4 gateway mechanism enabling seamless communication between IPv6 and IPv4 nodes. This mechanism supports heterogeneous communication and the forwarding of IPv4 and IPv6 connections at the application layer, without introducing new protocols or compromising existing communication functionalities. The resulting SOCKS-based IPv6/IPv4 gateway mechanism facilitates heterogeneous communication and connection forwarding, maintaining the SOCKS mechanism's communication environment without necessitating DNS system modifications or alterations to existing applications, thanks to sockification through a SOCKS library installation on the nodes.

On top of that, surveys like Ghumman's [21] delve into IPv4/IPv6 transition, exploring the most important methodologies such as dual stack, tunneling, and network address translation protocol translation, with their respective impacts on IoT infrastructure. Ghumman's research highlights the intricacies of IPv6 transition methods and their potential to address the burgeoning demands for IP addresses in the IoT realm. The research also emphasizes the difficulty of implementing real translators, mainly due to the great diversity of devices and few resources available. This survey underscores the importance of IPv6 for enhancing IoT security, scalability, and connectivity, marking a critical step towards the future of Internet protocols and their application within the IoT ecosystem.

These examples represent the most current, closest approaches in the endeavor to implement a gateway or Relay. While each project bears unique features, they collectively underscore the research domain's focus on creating and implementing communication gateways between these two pivotal technologies, highlighting the field's ongoing relevance and the imperative for advanced solutions in promoting IoT interconnectivity. It is worth noting that all of the projects share a common goal: to facilitate and optimize communication between different network protocols, evidencing the evolution of research in this area, although the NB-IoT seems to be the least-represented research in this field so far.

Hence, the device presented in this study contributes to the growing body of literature on IoT interoperability by providing a simpler, easier, yet reliable solution to a pressing problem. Previous research in this area focused on various aspects of IoT communications, but the use of future-proof NB-IoT as the main communications layer to cross the bridge adds another dimension to the discourse—as a new, unique approach to aid the integration of 6LoWPAN devices into IPv4 networks. As the IoT landscape continues to evolve, the significance of developing interoperable solutions that can adapt to the changing technological environment cannot be underestimated.

In conclusion, we not only present a novel solution to a critical challenge in IoT interoperability, but also highlight the importance of simplicity and efficacy in the design of communication relays—or gateways. The findings of this study are expected to have significant implications on the development of future IoT networks, paving the way for more integrated, versatile, user-friendly IoT ecosystems.

1.3. Article's Structure

The rest of the paper is organized as follows:

Section 2 explains the significant, basic issue with the IoT field, which is the enormous variety of devices, protocols, technologies, manufacturers, etc., as well as this field's slow, step-by-step evolution for more than a decade. It has leveraged a wide range of heterogeneous use cases and devices, thereby dragging interoperability and universal deployment barriers. The two big players in the game are explained, 6LoWPAN and NB-IoT, alongside their matching upper-layer protocols, namely CoAP and REST; we also describe our approach to overcome to this issue, so that the reader can appreciate the Relay's scope; finally, Section 2 explains our vision on HA as an essential enabler in IoT harmonization.

Section 3 presents the Relay itself and its abstraction working schemas, focusing on its main components, keys, and distinct primary resources—both hardware and software—as well as specific things that were tailored for its development and actual implementation in a real-world scenario, highlighting the main issues encountered during this stage, as well as the primary outcomes of interest.

In Section 4, we conclude the satisfactory results of our Relay, highlighting this type of research's importance in the pursuit of a real, profound IoT blending in society. To finalize, we discuss security concerns and future sights on the long-term IoT paradigm.

2. The Elephant in the Room: Great Diversity

In addressing the multifaceted domain of the Internet of Things, a critical, often overlooked issue emerges as *the elephant in the room*: the pervasive challenge of interoperability across a rapidly expanding and evolving network of devices. This challenge is not merely a technical inconvenience, but a fundamental barrier to realizing the IoT's transformative potential. Interoperability—or lack thereof—affects everything from user experience and system efficacy to the scalability and adoption of IoT solutions on a global scale.

Despite the increasing acknowledgment of its importance, the nuanced complexities and underlying technological disparities that contribute to interoperability challenges remain underexplored. In the ensuing subsections, we delve into the core aspects of these challenges, ranging from protocol diversity and network compatibility to the integration hurdles posed by legacy systems and emerging standards. By dissecting these issues, we

aim to lay a comprehensive foundation for understanding the critical need for innovative solutions that can bridge these gaps, thus setting the stage for the novel contributions of our research.

2.1. One Simple Approach to Help Harmonization

The primary objective of this paper is to develop and implement a solution to connect and expose data from IoT sensors to the Internet, based on the 6LoWPAN protocol. This solution involves creating a communications Relay that allows leaf nodes in the network to communicate with the cloud. This Relay device would host a two-way communications system: (i) a local area network, to speak with the 6LoWPAN coordinator, and (ii) NB-IoT, which provides the transparent, logical-direct path to the cloud platform where data are integrated.

6LoWPAN sensors usually exchange information using the CoAP protocol. Network coordinators usually use their own methods, platforms, or *secret recipes* to subsequently make these data appear somewhere else where access is granted (IPv4 networks). However, this layer is usually opaque and tailored specifically for the very brand/use case itself, with little to no chance of modification.

To overcome this issue, we propose a new type of *Thing* based on a low-cost FiPy module [22]. This development board comes handy, as it runs on the well-known ESP32 family of chips, and it incorporates Wi-Fi for the local access path, NB-IoT for the global path, as well as some other wireless technologies such as BLE, Sigfox, and LoRa. The main architecture of the system can be seen in Figure 1.

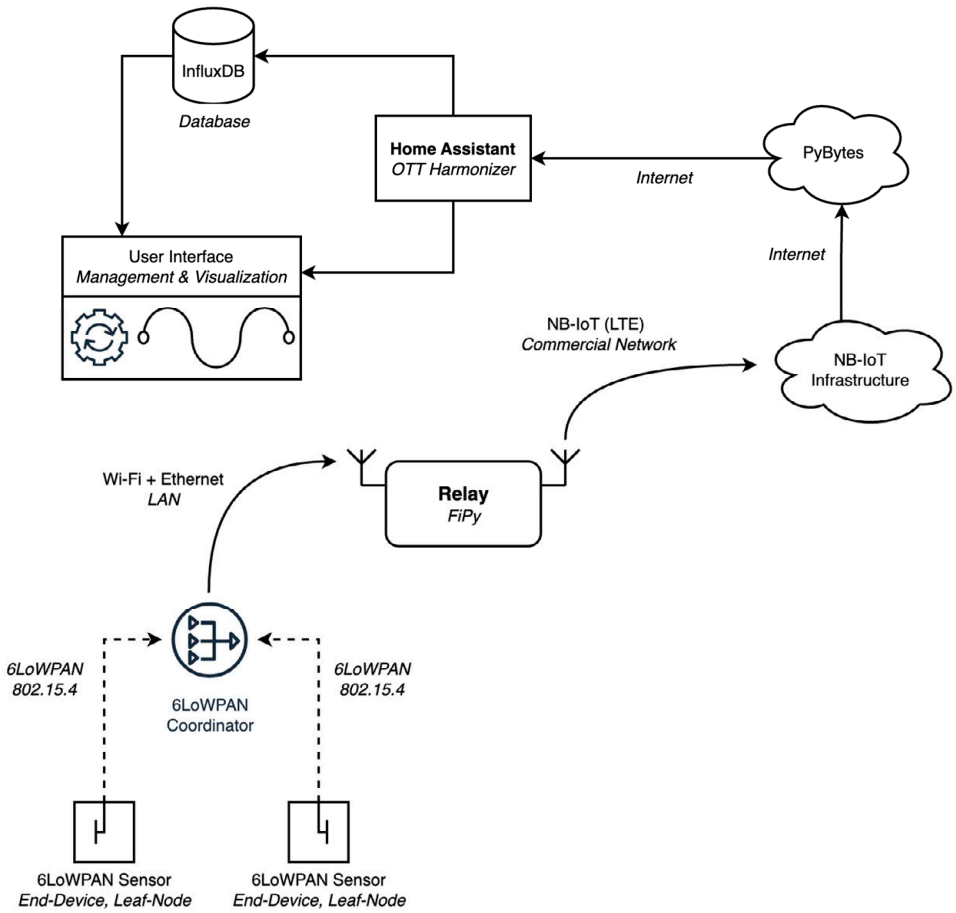


Figure 1. General block diagram for this project's architecture.

Thus, data would be requested to the 6LoWPAN coordinator by the Relay, which afterwards properly parses the data as a JSON document, then uploads it to the cloud.

Notice that there is a middleware platform in between called PyBytes [23]. Although this could be avoided, it is the most straightforward manner to use NB-IoT with Pycom development boards.

Furthermore, this approach is almost carrier agnostic, leveraging ubiquity and ease of implementation. Only two parameters are to be set in the Relay's program code, the APN and LTE band. However, in Europe, the band is often FDD #20 (~800 MHz), regardless of the mobile carrier and country, and the APN is a static parameter per carrier. With this, the developer only needs to invoke Pybytes' library functions to send messages to the back end.

The LTE modem scans the designated band, and then attaches to the very narrow-band carrier commanded by the network, which may change its central frequency between geographical locations, even inside the same country and mobile operator. For this research, 1NCE [24] was chosen as the mobile carrier, which was actually using Vodafone's NB-IoT towers/network; they are just a reseller providing quasi-global NB-IoT service.

Once attached and connected to the cellular network, the Relay can successfully send data to Pybytes, which then sends these data directly to the Home Assistant API to accordingly store and cure the incoming data on the InfluxDB database, eventually triggering automations or whatsoever, should they be set up.

In summary, this study presents a comprehensive solution for the collection, processing, transmission, and exposure of IoT sensor data to the Internet, utilizing leading-edge, open-source technologies, and ensuring a new roadmap for work in the coming years, offering high interoperability thanks to the use of standard protocols in the IoT industry.

To prove the Relay's proper functioning, we set up a simple indoor testbench in a medium-sized room with a typical setup composed of the following: (i) a 6LoWPAN network with one coordinator node and two ambient sensor nodes; (ii) the Relay itself, centered on the FiPy board, which embeds the NB-IoT modem; and (iii) a Wi-Fi router, providing LAN/WLAN connectivity between the coordinator node and the Relay device. Apart from this reachable set up, there were also an AWS-Lightsail server where the Home Assistant instance was deployed, exposing the endpoint to which Pybytes would forward NB-IoT messages, and providing the web interface for the user to visualize data and interact with the system.

2.2. 6LoWPAN

In the realm of the Internet of Things (IoT), enhancing energy efficiency and connectivity in various environments necessitates innovative networking solutions. Devices in these networks are often interconnected in a mesh topology, leveraging an adaptation of the 802.15.4 standard through 6LoWPAN. 6LoWPAN, standing for IPv6 over Low-Power Wireless Personal Area Networks, is pivotal for enabling devices with constrained processing and power resources to communicate over the IPv6 protocol, thus offering notable advantages such as interoperability and flexibility. The protocol's extensive addressing structure, provided by IPv6, significantly aids in scaling IoT networks by facilitating the addressing of a virtually unlimited number of devices.

Moreover, 6LoWPAN's efficiency in bandwidth utilization is achieved through header compression mechanisms. This efficiency is crucial in reducing the size of transmitted data packets, an essential feature in wireless sensor networks where transmission capacity and battery longevity are of paramount importance. Consequently, the application of 6LoWPAN in IoT device communication propels the interoperability, scalability, and efficiency of deployments, facilitating the establishment of comprehensive networks.

The integration of 6LoWPAN with NB-IoT represents a strategic advancement that capitalizes on the strengths of both technologies. The NB-IoT is celebrated for its exceptional coverage, power efficiency, and reliability, providing a reliable communication layer for IoT devices in scenarios where traditional connectivity options are impractical or overly power consuming. This symbiosis between 6LoWPAN and NB-IoT enhances the seamless and efficient transmission of data from localized, star-of-stars IoT networks to the broader

Internet, effectively narrowing the divide between localized IoT networks and the expansive global Internet infrastructure. Such integration is essential for the development of IoT systems that are scalable, interoperable, and capable of efficient operation across diverse environments and protocols, marking a significant step towards the realization of fully connected and efficient IoT ecosystems [3,25,26].

There are at least two main types of devices expected in 6LoWPAN networks: (i) coordinators and (ii) leaves. Our testing scenario is composed of one coordinator node and two leaves, as follows:

The coordinator node (see Figure 2, left), centered on a BeagleBone Black, offers a robust platform for managing network communications and data processing tasks. This single-board computer's significant processing power and connectivity options make it ideal for overseeing the operations of an IoT network. The coordinator node is enabled by a 6LoWPAN standard communication module, establishing it as the network's central hub. Notably, the BeagleBone Black implements a CoAP (Constrained Application Protocol) server, designed to handle request-based communications from the network's sensor nodes. This setup is pivotal for managing the energy-efficient protocol operations, ensuring that data are relayed efficiently from the sensor nodes to the coordinator, and then onwards as required. The 6LoWPAN device connects to the BeagleBone via UART. This connection method is instrumental in maintaining the system's overall low power consumption and simplicity, whilst ensuring a low-data-rate, seamless stream from the capillary network.

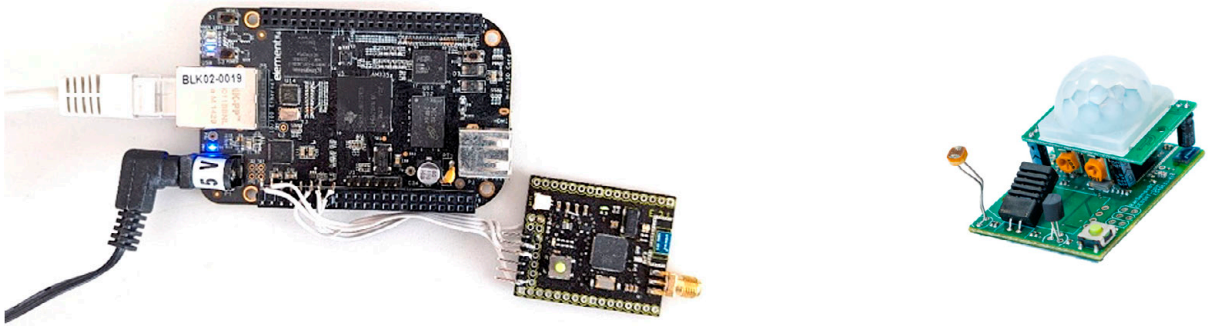


Figure 2. Left: coordinator node: BeagleBone Black + 6LoWPAN border–router node; **right**: ambient sensor nodes used in this project.

Standard/leaf nodes (see Figure 2, right) were deployed, which in the scope of this study happen to be ambient sensors, although any kind of device would be set the same way. Parameters gathered by ambient sensors are typical IoT parameters—temperature, humidity, luminosity, and motion—so they seemed to be a good choice to implement for testing. In alignment with the principles of low power consumption and efficient communication, these ambient sensors utilize a request-based CoAP. This protocol is specifically tailored for constrained devices like ours, allowing them to operate on minimal power by only activating when sending or receiving data as needed. These sensors' design reflects a meticulous balance between power efficiency and operational capability, ensuring that even with their limited energy resources, they provide reliable data transmission.

2.3. NB-IoT

Cellular networks have been a cornerstone in the evolution of communications over the past few decades, offering uninterrupted connectivity almost anywhere in the world. From their early versions, which primarily supported calls and text messages, to modern high-speed networks facilitating data, video, and other multimedia applications, they have transformed how we communicate and access information.

However, with the increasing need to connect with people as well as devices within the Internet of Things, there emerged a requirement for specific technologies that could

adapt to these new demands. In this study, the narrowband IoT (NB-IoT) comes into play as a solution based on cellular networks [27–34].

As a modern and meticulously designed technology, the NB-IoT stands out as the optimal solution tailored to meet the specific needs of IoT communication networks. Its recent development allows it to surpass other technologies by optimizing every facet, thus ensuring superior efficiency and performance in the IoT realm. The NB-IoT's youth and thoughtful development make it perform well in its scope. This advantage is further bolstered by the backing of telecommunications operators, who ensure long-term support by investing heavily in this technology. Such investments have made the NB-IoT remarkably affordable and accessible for a wide range of applications. We consider the NB-IoT to be an optimal technology for a wide range of IoT use cases, as explained in the next subsections.

2.3.1. Global, Carrier-Grade Network

The advent of the NB-IoT marks a significant milestone in the evolution of global, carrier-grade networks, offering a robust solution for extending IoT connectivity across a myriad of devices worldwide. Engineered to operate within the licensed spectrum, the NB-IoT benefits from the ease-of-use, reliability, and security that are inherent to carrier-managed networks, ensuring stable and secure communications for IoT devices, even in the most challenging environments. In addition, licensed bands augment its resilience to external attacks, QoS, and general control over the network's lowest layers.

Its unique capacity to penetrate deep into buildings and underground areas, mainly due to its usual functioning on sub-gigahertz bands, makes it an ideal choice for a wide range of applications, from smart metering in utilities to asset tracking in logistics. Moreover, the NB-IoT's highly efficient power usage can extend devices' battery lives for years, reducing the maintenance costs associated with IoT deployments.

As part of the global LTE standard, the NB-IoT enjoys widespread international support from telecom operators, facilitating seamless, cross-border IoT solutions and driving forward the vision of a fully interconnected world. The global reach and carrier-grade reliability of the NB-IoT stand as pillars for the next wave of IoT innovation, enabling a new realm of applications that were previously untenable due to connectivity and power constraints. In the specific case of Spain, where this research was carried out, the three largest carriers (Telefónica, Vodafone, Orange) provide virtually full NB-IoT coverage over the whole population. This fact is vital for enabling solutions for a wide variety of scenarios, especially considering that a single NB-IoT sector, usually three sectors per cell, can operate more than 100,000 devices [35].

2.3.2. Low-Power Communication Technology

The NB-IoT stands out in the realm of low-power wireless communication technologies due to its exceptional capabilities that are specifically tailored for the modern IoT. Standardized by the 3GPP in Release 13 back in 2016, the NB-IoT was meticulously crafted to support the burgeoning demand for a network that can efficiently connect a vast number of devices across extensive areas without the burden of high energy consumption. By leveraging a narrow bandwidth of around 200 kHz for its transmissions, The NB-IoT is not only able to ensure low-speed data exchange, but also significantly extends the battery life of IoT devices, making it an indispensable technology for scenarios where devices are expected to operate for years without battery replacement.

The NB-IoT's design focuses on minimal energy usage, while still providing robust and reliable connectivity. This is particularly advantageous for a wide array of IoT applications that necessitate prolonged device longevity. Its enhanced coverage and deep penetration capabilities make it perfectly suited for monitoring environmental factors in remote or difficult-to-access locations [36].

The advent of the NB-IoT as a low-power communication technology marks a pivotal advancement in the IoT ecosystem. Its ability to offer extensive coverage, superior indoor penetration, and ultra-low energy consumption while leveraging existing cellular network

infrastructures makes it an ideal candidate for a plethora of IoT applications. This positions the NB-IoT as a cornerstone technology in the ongoing evolution of smart cities, agriculture, environmental monitoring, and beyond, heralding a new era of connectivity that is both efficient and sustainable.

2.3.3. Streamlined for IoT—An LTE Evolution

The evolution of the NB-IoT on an established technology like LTE, and its implementation over a licensed frequency spectrum, optimizes network capabilities, relieving devices of hardware and software complexity demands. Adoption of the NB-IoT is further propelled by its integration into existing cellular network infrastructure, allowing for its cost-effective rollout and seamless scalability. It can be deployed on a GSM (2 G) channel, on 4 G guard-band space, or on the standard 4 G/5 G spectrum and equipment [31]. This integration ensures that the NB-IoT benefits from the established security and reliability features of cellular networks, as well as their carriers' know-how, providing a secure, efficacious communication channel for transmitting sensitive information.

Despite being derived from LTE specifications, the NB-IoT standard was designed to maintain as simple a communication interface as possible, aiming to lower device manufacturing costs and minimize battery consumption. Many LTE features that are unnecessary for IoT services have been omitted in the NB-IoT, such as handover for voice quality, carrier aggregation for signal quality enhancement, and dual connectivity for multi-carrier communication.

2.3.4. Frequency Band Utilization and Messaging

The NB-IoT's strategic approach to frequency band utilization significantly enhances its applicability across a broad spectrum of IoT deployments. It operates in three distinct modes: (i) in-band, utilizing the LTE carrier blocks; (ii) guard-band, leveraging the unused spectrum in LTE guard bands; and (iii) stand-alone, repurposing existing GSM frequency bans; in so doing, the NB-IoT exhibits unparalleled flexibility in network implementation. This flexibility is critical in densely populated urban environments as well as in rural areas, where spectrum efficiency and coverage requirements vary greatly.

The architecture of the NB-IoT was meticulously engineered to support the transmission of small data packets, corresponding to periodic updates from IoT devices. The NB-IoT's design specifically addresses IoT requirements, enabling its efficient management of compact data packets. This efficiency is critical for applications that require frequent updates from a vast array of devices, such as utility meters, environmental sensors, and health monitors, ensuring that the network remains uncluttered and responsive.

The NB-IoT provides a solid foundation for wide-area IoT applications, which, combined with 1600-byte messages, makes the NB-IoT a highly versatile technology. It not only caters to dense, complex urban environments, but also extends its benefits to remote, underserved rural locations, where connectivity has traditionally been a challenge.

2.4. Protocols Involved within the Application Layer: CoAP and REST

In the IoT ecosystem, ensuring efficient communication between devices is pivotal. Among the protocols tailored for the IoT, CoAP and REST stand out for their utility in constrained environments and web-based applications, respectively.

2.4.1. CoAP: Constrained Application Protocol

CoAP is a lightweight protocol designed for machines. It is akin to a compact version of HTTP for devices with limited resources, using a straightforward model for sending and receiving messages. Unlike HTTP, it operates over UDP, making it better suited for the minimal power and processing capabilities of IoT devices. CoAP supports interactions in IoT applications that require minimal bandwidth and energy consumption [37].

2.4.2. REST: Representational State Transfer

REST leverages the existing HTTP infrastructure to create or access resources using standard HTTP methods. It is widely adopted for web APIs, enabling straightforward and flexible interactions with services. RESTful interfaces are favored for their scalability and ease of integration across diverse platforms, making them suitable for complex IoT ecosystems where different devices and services need seamless communication [38].

Both CoAP and REST are integral to the IoT application layer, offering distinct advantages for device-to-device and device-to-service communication. CoAP excels in constrained environments, while REST is preferred for broader web integration, highlighting the importance of selecting the right protocol based on the specific requirements of an IoT deployment.

2.5. Home Assistant: Agnostifying Data in Pursuit of a Diverse Coherence

Home Assistant (HA) technology stands as a paradigm of open-source home automation; it is designed with a strong emphasis on privacy and local control. Emerging as an antidote to the fragmentation and privacy concerns associated with proprietary or cloud-based solutions, HAs champion interoperability among diverse smart devices without sacrificing user privacy. The platform's open-source nature not only underscores its commitment to transparency and security, but also paves the way for unparalleled flexibility and customization. Users can tailor the platform to their specific needs, benefiting from the collective intelligence of a global developer community committed to advancing HA's capabilities [15,39].

Developed initially in 2013 by Schoutsen, HA's foundation in Python and open-source principles has fostered a rich ecosystem of contributions. The platform integrates a wide array of devices and services through modular components, ensuring a cohesive and customizable user experience across various devices and technologies. This inclusive architecture has facilitated the rapid adoption and continuous growth of HAs, supported by an active community and frequent updates that introduce new functionalities and integrations.

The significance of the HA community cannot be overstated. It thrives on continuous contributions of new integrations, enhancements, and fixes, serving as an invaluable resource for newcomers and experienced users alike. The platform's extensive documentation further aids users in navigating installation, configuration, and customization processes, making HA technology accessible to a broad audience.

As HA technology evolves, it consistently adapts to the burgeoning landscape of IoT devices and user expectations, ensuring its relevance in the ever-changing domain of home automation. Its dedication to privacy, localization, and flexibility, coupled with robust community support and comprehensive documentation, positions HA technology as a pivotal player in the home automation ecosystem. While originally tailored for home lab use, HA technology's adaptability hints at broader applications, including industrial settings. This exploration underscores HA technology's potential as a versatile and robust IoT management platform, extending beyond traditional home automation to encompass a wider array of environments and applications, such as emerging smart cities' platforms [40].

In fact, HAs stand at the forefront of driving the IoT's scalability and interoperability, offering a compelling model for open-source development by facilitating an expansive, community-driven approach to smart devices integration. This platform highlights the value of an open-source ethos to foster innovation, as it enables rapid integration of devices across sundry manufacturers and protocols, breaking barriers often encountered in proprietary ecosystems.

3. Relaying

In this section, we unveil the intricacies of the Relay, focusing on the essential components and resources foundational to its design. This includes an examination of both its hardware and software elements, alongside bespoke developments tailored for its construction and actual deployment. By presenting the Relay's architecture and operational

capabilities, this section aims to elucidate its role and efficiency within the broader context of IoT applications, demonstrating the Relay's simple yet efficacious functioning.

3.1. Starring Hardware

The Relay's main hardware component is the FiPy board by Pycom, an innovative choice reflecting our commitment to versatility and integration. This powerful development board supports a multitude of communication standards, including Sigfox, LoRaWAN, NB-IoT, Wi-Fi, and BLE, all within a single device. The choice of FiPy is pivotal, owing to its unique ability to navigate across various network technologies, thus facilitating seamless communication in diversified IoT ecosystems. Its dual-core 32-bit LX6 microcontroller, programmed in MicroPython, offers a flexible and efficient platform for developing IoT applications that require multi-network connectivity.

3.2. Collecting with CoAP

To address the complexities of IoT communications within a sophisticated network environment, a comprehensive solution was developed to bridge the gap between CoAP and HTTP protocols through the implementation of a RESTful micro-server. This approach was realized using Python, a language chosen for its flexibility and extensive support, and because of its presence in the core of HA technology; thus, leaner integration between them can be achieved if needed. We took advantage of Flask [41], a microframework celebrated for its minimalistic yet powerful features at the same time that it helps us accelerate web-related coding.

The backbone of this communication server is the CoAPython library [42], which plays a pivotal role in integrating CoAP protocol functionalities, facilitating seamless interactions between IoT devices. CoAP messages are accordingly parsed, as stated by the simple data model of the 6LoWPAN devices deployed in this project.

In this fashion, significant data values and sensor states can be extracted from CoAP messages, then incorporated into a more common, current, and suitable format. This process mostly involves data *JSONification* and basic modeling. This conversion process, although not intricate, is critical for ensuring that data from foreign IoT devices are discoverable, easily accessible, and manageable through common Internet web technologies. In Figure 3, the reader can see a simple diagram of the network abstracted to the upper layers that depicts the changes in protocols we are dealing with.

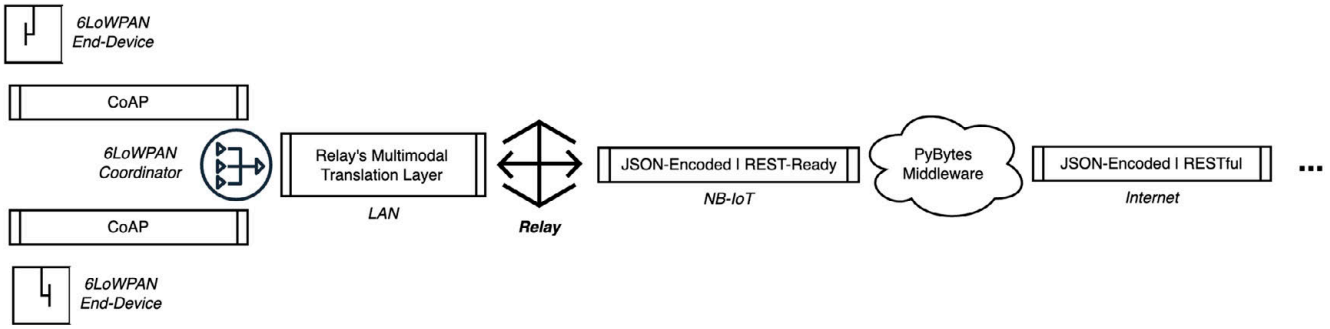


Figure 3. A coarse, protocol-oriented representation of the IoT chain.

The server architecture is designed with resource efficiency in mind, as always-first, major IoT mantra, allowing for lightweight operations that maintain system performance while handling data exchanges. Flask's ability to create a minimal yet functional web server environment has been instrumental in this regard, providing only essential components to support RESTful interactions and CoAP compliance, whilst not overwhelming the system with unnecessary matters. Moreover, the server's configuration includes a set of predefined routes, each catering to specific data retrieval or device interaction needs, as one of the main

intricacies with iPv6 networks is their routing's lack of ease and iPv4 direct compatibility, a fact that is usually worsened by the *(ab)* use of NAT and tunneling.

This structured, kind of isolated approach not only simplifies usability for developers and system integrators, but also enhances the system's reliability and scalability by clearly defining communication pathways and data processing methodologies, helping future-proofing. In our actual testing deployment, the server was connected via Wi-Fi to the same LAN as the 6LoWPAN coordinator was connected to.

The server periodically queries every IoT device comprising the designated 6LoWPAN network, as claimed by the coordinator. Note that there are also methods implemented to retrieve network characteristics from the coordinator, such as lists of devices, individual device information and sensing capabilities thereof, network telemetries and quality indexes, sensor data and states per se, etc. As stated, the server collects and organizes data into JSON documents following the appropriate models. These data are now available to be pushed to the middleware: PyBytes.

3.3. Pushing with NB-IoT

Integration of the NB-IoT into our Relay system underscores a strategic embrace of cellular technology for the IoT. Pycom provides PyBytes as the easiest, most direct connection of their own branded development boards with the cloud using, among other technologies, the NB-IoT. Nonetheless, hassle-free NB-IoT bridging is especially remarkable, as current utilization of the NB-IoT within the end-user scope is still cumbersome. Integration tends to be carrier-dependent, and documentation is scarce. In fact, carriers or vendors from whom rights to use NB-IoT communications must be acquired—usually (e)SIM cards—are hard to find.

Thus, having a carrier-agnostic middleware which masks carrier-related issues and avoids specific settings tuning is something worth highlighting. With this, once PyBytes is properly configured and the modem effectively connects to the NB-IoT's network (Figure 4), sending data to the middleware using the NB-IoT just implies using a library function in the fashion of the following:

```
...
pybytes.send(chunk)
...
```

```
SYSTEM FSM          STATE                SYSTEM FSM          STATE

RRC TOP FSM         SCANNING             ESM BEARER FSM      BEARER_NULL
RRC SEARCH FSM      WAIT_RSSI            SMS MT FSM          IDLE
RRC ACTIVE FSM      NULL                 SMS MO FSM          IDLE
PMM PLMN FSM        NORM_WAITCELL        LPP FSM             IDLE
EMM MAIN FSM        NULL                 HP MAIN FSM         IDLE
EMM AUTH FSM        KASME_DEFINED        HP USIM FSM         READY
EMM CONN FSM        NULL                 HP SMS MO FSM       IDLE
EMM TAU FSM         NULL                 HP SWI MT FSM       IDLE
EMM TEST FSM        NULL                 HP CAT FSM          IDLE
```

Figure 4. AT commands (finite state machines' states) printed by the LTE modem in console when the FiPy module is authenticating in the NB-IoT network.

For the cycle to be completed and NB-IoT messages properly forwarded from PyBytes to the HA instance, rules must be defined in the middleware. These rules are evaluated every time a new message is received—messages are called Signals within the PyBytes middleware, as depicted in Figure 5.

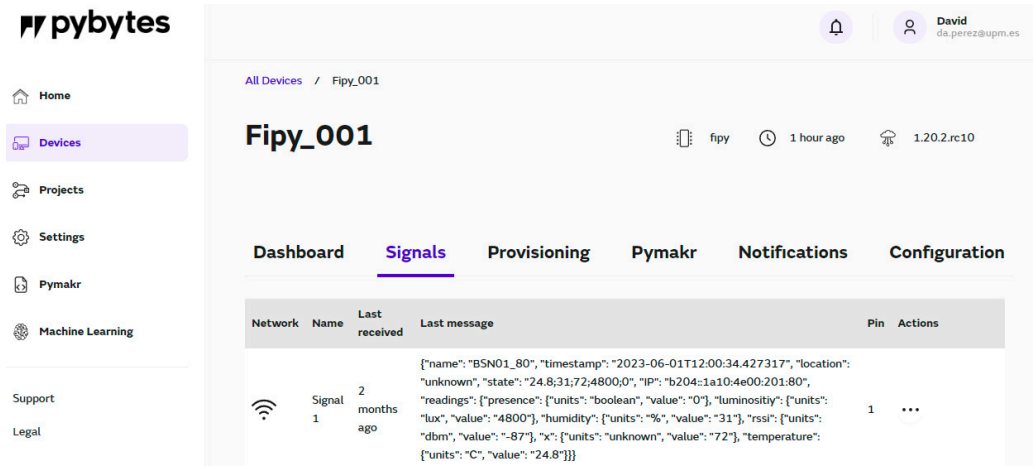


Figure 5. PyBytes' back-end displaying the so-called Signals Table The reader may see an example of one such message received from the Relay. In its structure, crucial pieces of information like the 6LoWPAN device's identification, sensing values states, and measurement timestamps can be observed.

For this project's specific case, we just checked if new messages had an identifier embedded in one specific field of the Relay's forwarded messages. If so, a POST REST request was sent to the HA API—with the proper authorization token—which would handle it accordingly and hopefully store the information received in the designated sensor states.

3.4. Pulling with Home Assistant

Connecting the Relay to the HA showcases our dedication to creating user-centric, future-proof, expandable IoT solutions. This being a specifically tailored ad hoc use case, manual sensor definition must be conducted in the HA configuration files for them to be properly integrated.

As an example, Figure 6 depicts the definition of two custom templated sensors used within this project's scope. Note that the sensors' value templating vastly varies according to the JSON data model we use in the HA API requests. In the following example, we were barely able to input the whole JSON text string into the API as an input text field, which afterward split into meaningful sensors, as shown in Figure 6.

```
sensor:
  - platform: template
    sensors:
      bs79_net:
        friendly_name: "NetID_79"
        unique_id: "sensor.bs_79_net_20230721_0"
        value_template: "{{ states('input_text.batsense_1').split(',')[0]}}"
      bs79_nameshort:
        unique_id: "sensor.bs_79_name_20072023_0"
        friendly_name: "Name_79"
        value_template: "{{ states('input_text.batsense_1').split(',')[1]}}"
```

Figure 6. Exemplification of two custom templated sensors defined in the HA's realm.

The HA's core was complemented with other modules such as Grafana for rapid, seamless data visualization and simple integration thereof. Home Assistant dashboards and other UI resources could be used to control appliances or actuator devices, as well as set certain configuration parameters.

By pulling data into the HA, users can leverage its extensive ecosystem of plugins and integrations to automate tasks, visualize data, and control smart devices, effectively

making the Relay an integral part of a sophisticated home-and-beyond automation system. A simple card displaying the data from the pair of sensors defined in Figure 6, but in a more meaningful manner, is shown in Figure 7 (left); a more complex dashboard for the same pair of sensors Is depicted in Figure 7 (right).

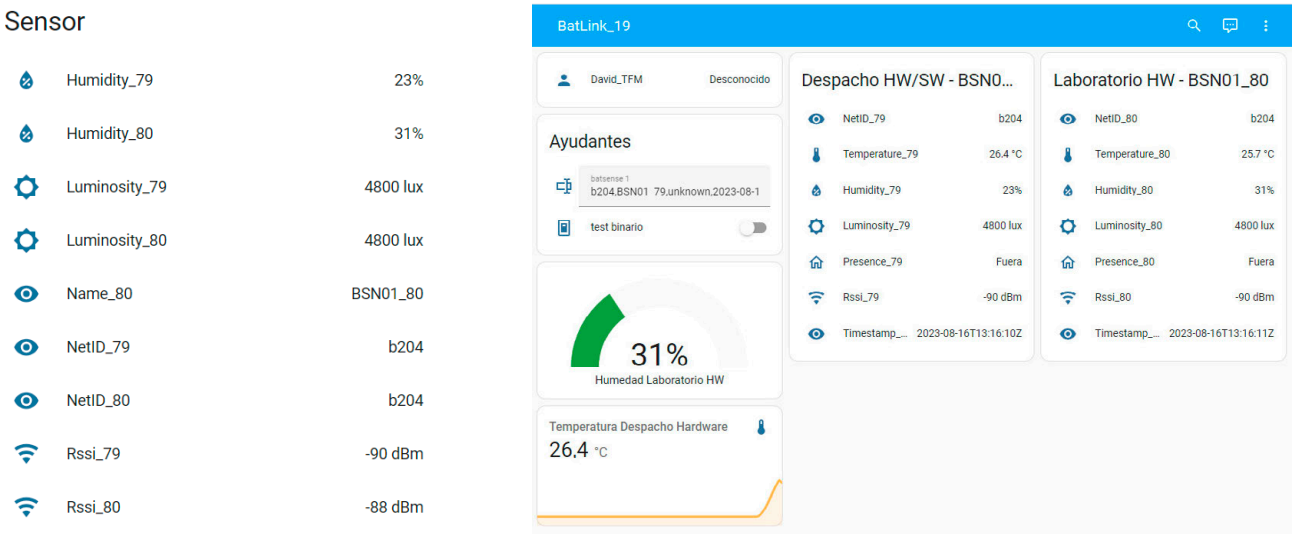


Figure 7. Two custom templated sensors natively displayed in the HA.

3.5. Storing with InfluxDB

The integration of InfluxDB within HA offers a powerful combination for home automation performance and beyond. InfluxDB, a time series database, is designed to handle high write and query loads, making it ideal for storing and analyzing vast amounts of IoT data, like those generated by an HA. These streams of data can grow easily several hundreds of megabytes per day when a handful of devices are frequently polled.

This integration allows users to efficiently log data from various sensors and devices managed by the HA, enabling detailed analysis and visualization of trends over time. Such capabilities significantly enhance the potential for optimizing home environments, energy usage, and understanding patterns in daily routines, including outliers.

InfluxDB also comes with Kronograf for data visualization and Telegraf for monitoring the database's performance, metrics, and the like.

4. Conclusions and Loose Ends

The Relay system developed through this research may serve as a pivotal stride towards achieving tangible IoT interoperability, a feat that remains largely elusive in contemporary settings. The Relay, designed with an emphasis on simplicity, ease of deployment, usability, and efficacy, empowers a broad spectrum of users to implement it with minimal complexities, thereby accelerating the realization of genuine IoT harmonization.

Through a proper selection and integration of hardware, software, and infrastructure components, including the FiPy module, the NB-IoT infrastructure and the HA ecosystem, our research met its technical objectives. At the same time, we are facilitating the real, deep integration IoT needs to become a usable part of society's daily life.

The Relay's design, highlighted by its straightforward yet thoughtfully intended implementation, underscores its innovative approach to dismantling the barriers that currently hinder seamless IoT communication. Immediate next steps involve a deeper characterization of the Relay, including time responses and latency variations due to its presence, eventual packet loss and error rate, and performance stability. So far, we carried out qualitative, naked eye evaluation procedures where it seemed to perform as expected; however, further, more precise tests must be realized, such as those carried out in [14].

Deployment of communication relays like this, as well as the adoption of standardized IoT protocols, will gain market interest in the long term. Although big players and industry leaders may initially be reticent to forego their control on proprietary systems, open ecosystems end up driving larger market and investment figures, with new, often unexpected relations among different players. This may eventually lead to enormous expenditures in the research and innovation of such fields, which big players and investors may also take advantage of.

However, the IoT is evolving rapidly, which may be an issue from a standardization perspective, as the diverse and evolving nature presents a challenge in establishing timely harmonious, global standards. To help overcome these barriers, stakeholders like standardization bodies and industry leaders must keep collaborating to foster IoT harmonization, thereby unlocking the full potential of IoT interoperability and connectivity.

By providing a clear pathway for the ad hoc development and deployment of such relays in real-world scenarios, these findings may lay a foundation for future advancements in IoT interoperability, highlighting the synergy between diverse technologies, tools, and software systems in overcoming the complexities of IoT ecosystems.

4.1. Security-Proofing—Concerns on IoT Network Reliance

Integrating communication relays into IoT networks brings to light several security challenges that are paramount to maintaining the integrity, confidentiality, and safety of data traversing these networks, as well as services dependent on them. A multi-faceted approach is necessary, including encryption, authentication, regular updates, proactive monitoring, and compliance with established security standards.

Such a strategy ensures the integrity and reliability of data transmission across the interconnected expanse of IoT devices and platforms, especially when unanticipated protocol translation systems and new devices are integrated within the networks. As these relays facilitate data transmission across different network layers and protocols, they inherently increase the system's attack surface, presenting potential vulnerabilities for exploitation that must be addressed from the beginning [43,44].

Implementing security measures can help in maintaining secure communications involving IoT relays. They help ensure safe and reliable transmission of data across diverse IoT ecosystems. This not only protects the network from potential threats, but also builds trust among users and stakeholders, fostering the growth and development of secure, interconnected IoT applications. Security measures like the following must urgently be taken into consideration when implementing systems like this project's Relay [45,46]:

4.1.1. Vulnerabilities and Long-Term Patching

Communication relays, by their function, could be targeted by attackers seeking to intercept or manipulate data. These nodes become critical points of security, especially considering they are exposed two-fold, as they need to interact with two different networks. Therefore, deep attention with robust protection measures are necessary. Encryption protocols, such as TLS/SSL, are vital in securing data in transit, ensuring that data passing through the relay remains confidential and tamper proof. Nevertheless, one must not ignore up-and-coming quantum computing, which may be used to break classic cryptographic algorithms in a matter of seconds.

Fortunately, so-called Post-Quantum Cryptography (PQC) is being actively developed, and has already proven to be reliable. PQC algorithms provide protection against both classical and quantum attacks, and they can be implemented on classical, binary computers [47–50].

This is a vital requisite to guarantee long-term security and integrity within IoT networks, as these devices are expected to continue relying on classic computing CPUs for years to come, even when quantum computing starts to settle in other fields. However, it is mandatory for vendors, developers, and the like to ensure current IoT devices receive

future firmware updates, as failing to do so may result in significant vulnerable points within larger networks.

Keeping the Relay and its connected devices updated with the latest security patches is fundamental in protecting against known vulnerabilities. Automated update mechanisms can facilitate this process, ensuring that the system is resilient against emerging threats.

4.1.2. Compliance with Standards and Risk Mitigation

Complying with established security standards and frameworks, such as those outlined by the International Organization for Standardization (ISO), provides a structured approach to securing IoT ecosystems. These standards offer guidelines on best practices for IoT security and risk mitigation, from device manufacturing to data transmission and storage. Security strategies should be adaptive, capable of evolving with the changing threat landscape and technological advancements in the IoT and in any other field.

4.1.3. Authentication and IDPS

Rigorous authentication mechanisms are essential for verifying the identity of devices, and especially users interacting with the Relay. Implementing strong, multi-factor authentication can significantly reduce the risk of unauthorized access. Access control policies further ensure that devices and users have only the necessary permissions, following the principle of least privilege.

Deploying intrusion detection and prevention systems (IDPS) at strategic points within the network can help in identifying and mitigating potential security breaches in real time. These systems monitor network traffic for suspicious activities, providing an additional layer of security by alerting administrators to possible attacks. IDPS become important in devices like this Relay, as they expose various network interfaces connecting matching distinct networks.

4.2. Future-Proofing—Scalability

The pivotal role of open-source technologies is monumental in the advancement of truly interconnected systems, platforms, and ultimately societies. The primary barriers to the current amalgamation and seamless interoperability of IoT systems mainly arise from proprietary strategies adopted by certain manufacturers. These entities aim to dominate the ecosystem with their unique technologies and protocols. A shift towards a more transparent approach, with shared developments and requirements, could not only accelerate economic growth and exceed market expectations, but also bolster security measures through early detection and vulnerabilities resolution.

The open-source paradigm, exemplified by Home Assistant technology, invites an extensive community of developers and end users to contribute towards swift and coherent evolution. This collaborative approach promises to expedite innovation, facilitating the introduction of novel devices and software solutions, thus catalyzing essential real-time interoperability for the IoT's future.

The NB-IoT, with its low power demand, wide area coverage, thoughtful design, and strong carriers' backing, stands out as an enormously capable backbone for supporting the scalability of IoT solutions like the one presented in this article. The NB-IoT's deep coverage and support, along with its minimal energy consumption model, is particularly advantageous for scalable IoT ecosystems, requiring fewer resources for connectivity while maintaining robust performance.

The narrowband-IoT's capabilities extend to ensuring longer battery life for connected devices, which is a critical consideration for IoT scalability. By enabling devices to operate for years on a single battery charge, the NB-IoT reduces the need for frequent maintenance, further lowering the resources required for a scalable IoT solution. This efficiency is particularly beneficial for applications in smart metering, asset tracking, and environmental monitoring, where devices are often deployed in tough, hard-to-reach scenarios.

HA's lightweight, flexible architecture allows for easy, virtually-endless integrations with a wide array of devices and services, including those leveraging NB-IoT technology. This ease of scalability makes it an ideal platform for deploying and managing large-scale IoT applications. The synergy between HAs' versatility and the NB-IoT's efficacious connectivity paves the way for creating extensive, reliable IoT networks that can grow and evolve with little effort.

The combined approach of utilizing Home Assistants for device management and the NB-IoT as a universal means of connectivity exemplifies a solution that demands as few resources and particularities as possible. This leads to a robust, ubiquitous framework for IoT harmonization as we claimed in this article. This framework helps accelerate the deployment of scalable solutions without the burden of resource allocation, infrastructure development, or maintenance.

The coordination of a few well-founded technologies presents a forward-thinking approach to IoT development. We believe that these such approaches will become more common. These combinations not only champion scalability and interoperability for IoT systems, but they also significantly reduce the expertise and concreteness often required for creating and expanding use case-tailored IoT solutions.

The (near) future of IoT lies in the adoption of open, efficacious, and scalable solutions, promising a more interconnected, truly harmonious and seamless IoT realm.

Author Contributions: Conceptualization, A.S and E.S.; methodology and validation, E.S. and G.d.C.; hardware and software, E.S. and I.G.; laboratory work, formal analysis, resources, visualization, and data curation, E.S.; investigation, E.S. and I.G.; writing—original draft preparation, E.S.; writing—review and editing and supervision, A.S.; project administration and funding acquisition, A.S. and G.d.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by the CHIST-ERA EU project "ABIDI: Context-aware and Veracious Big Data Analytics for Industrial IoT" (PCI2019-103762), the Spanish National project "OPERA: Optics Designs to Improve the Performance of Radiative Cooling Systems" (TED2021-132660B-I00), both funded by the Spanish Ministry of Science, Innovation and Universities (MICIN); the HORIZON EU project "MOBILITIES for EU: New Mobility Solutions for Climate Neutrality in EU Cities" (101139666), funded by the European Commission; and the project"IoTMadLab: *Laboratorio IoT de Madrid*", an emerging Smart Cities Laboratory created by Madrid's City Council and UPM.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. IoT Analytics State of IoT 2021: Number of Connected IoT Devices Growing 9% to 12.3 Billion Globally, Cellular IoT Now Surpassing 2 Billion. Available online: https://iot-analytics.com/number-connected-iot-devices/ (accessed on 8 April 2024).
2. del Campo, G.; Gomez, I.; Cañada, G.; Piovano, L.; Santamaria, A. Guidelines and Criteria for Selecting the Optimal Low-Power Wide-Area Network Technology. In *LPWAN Technologies for IoT and M2M Applications*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 281–305, ISBN 978-0-12-818880-4.
3. Al-Kashoash, H.A.A.; Kemp, A.H. Comparison of 6LoWPAN and LPWAN for the Internet of Things. *Aust. J. Electr. Electron. Eng.* **2016**, *13*, 268–274. [CrossRef]
4. Wu, P.; Cui, Y.; Wu, J.; Liu, J.; Metz, C. Transition from IPv4 to IPv6: A State-of-the-Art Survey. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1407–1424. [CrossRef]
5. Hyun, J.; Li, J.; Kim, H.; Yoo, J.-H.; Hong, J.W.-K. IPv4 and IPv6 Performance Comparison in IPv6 LTE Network. In Proceedings of the 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), Busan, Republic of Korea, 19–21 August 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 145–150. [CrossRef]
6. Lencse, G.; Kadobayashi, Y. Comprehensive Survey of IPv6 Transition Technologies: A Subjective Classification for Security Analysis. *IEICE Trans. Commun.* **2019**, *E102.B*, 2021–2035. [CrossRef]

7. Jara, A.J.; Ladid, L.; Skarmeta, A. The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2013**, *4*, 97–118. [CrossRef]
8. Samad, F.; Abbasi, A.; Memon, Z.A.; Aziz, A.; Rahman, A. The Future of Internet: IPv6 Fulfilling the Routing Needs in Internet of Things. *Int. J. Future Gener. Commun. Netw.* **2018**, *11*, 13–22. [CrossRef]
9. Ziegler, S.; Crettaz, C.; Ladid, L.; Krco, S.; Pokric, B.; Skarmeta, A.F.; Jara, A.; Kastner, W.; Jung, M. IoT6—Moving to an IPv6-Based Future IoT. In *The Future Internet*; Galis, A., Gavras, A., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; Volume 7858, pp. 161–172, ISBN 978-3-642-38081-5.
10. Newman, D. Return On IoT: Dealing with the IoT Skills Gap. Available online: https://www.forbes.com/sites/danielnewman/2019/07/30/return-on-iot-dealing-with-the-iot-skills-gap/?sh=5f453ccb7091 (accessed on 8 April 2024).
11. Savolainen, T.; Soininen, J.; Silverajan, B. IPv6 Addressing Strategies for IoT. *IEEE Sens. J.* **2013**, *13*, 3511–3519. [CrossRef]
12. Triantafyllou, A.; Sarigiannidis, P.; Lagkas, T.D. Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 5349894. [CrossRef]
13. Saavedra, E.; Mascaraque, L.; Calderon, G.; del Campo, G.; Santamaria, A. The Smart Meter Challenge: Feasibility of Autonomous Indoor IoT Devices Depending on Its Energy Harvesting Source and IoT Wireless Technology. *Sensors* **2021**, *21*, 7433. [CrossRef] [PubMed]
14. Saavedra, E.; Mascaraque, L.; Calderon, G.; Del Campo, G.; Santamaria, A. A Universal Testbed for IoT Wireless Technologies: Abstracting Latency, Error Rate and Stability from the IoT Protocol and Hardware Platform. *Sensors* **2022**, *22*, 4159. [CrossRef] [PubMed]
15. Nabu Casa Home Assistant | Documentation. Available online: https://www.home-assistant.io/docs/ (accessed on 8 April 2024).
16. Cujilema Paguay, J.A.; Hidalgo Brito, G.A.; Hernandez Rojas, D.L.; Cartuche Calva, J.J. Secure Home Automation System Based on ESP-NOW Mesh Network, MQTT and Home Assistant Platform. *IEEE Lat. Am. Trans.* **2023**, *21*, 829–838. [CrossRef]
17. Da Silva Campos, B.; Rodrigues, J.J.P.C.; Mendes, L.D.P.; Nakamura, E.F.; Figueiredo, C.M.S. Design and Construction of Wireless Sensor Network Gateway with IPv4/IPv6 Support. In Proceedings of the 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 5–9 June 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 1–5. [CrossRef]
18. Arzo, S.T.; Zambotto, F.; Granelli, F.; Bassoli, R.; Devetsikiotis, M.; Fitzek, F.H.P. A Translator as Virtual Network Function for Network Level Interoperability of Different IoT Technologies. In Proceedings of the 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), Tokyo, Japan, 28 June–2 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 416–422. [CrossRef]
19. Grosse, E.; Lakshman, Y.N. Network Processors Applied to IPv4/IPv6 Transition. *IEEE Netw.* **2003**, *17*, 35–39. [CrossRef]
20. Kitamura, H. A SOCKS-Based IPv4/IPv6 Gateway Mechanism. Available online: https://www.rfc-editor.org/rfc/pdfrfc/rfc3089.txt.pdf (accessed on 8 April 2024).
21. Ghumman, F.A. Effects of IPV4/IPv6 Transition Methods in IoT (Internet of Things): A Survey. *SSRN* **2019**. [CrossRef]
22. Pycom FiPy Specsheets. Available online: https://docs.pycom.io/gitbook/assets/specsheets/Pycom_002_Specsheets_FiPy_v2.pdf (accessed on 8 April 2024).
23. Pycom Pybytes 3. Available online: https://docs.pycom.io/pybytes/ (accessed on 8 April 2024).
24. 1NCE 1NCE | About. Available online: https://1nce.com/en-eu/about (accessed on 8 April 2024).
25. Jiménez Ruíz, L. Diseño de Implementación de Etapa de Comunicación Basada En 6LoWPAN Para Plataforma Modular de Redes de Sensores Inalámbricas. Bachelor's Thesis, Universidad Politécnica de Madrid, Madrid, Spain, 2016. Available online: https://oa.upm.es/43013/1/TFG_LUIS_JIMENEZ_RUIZ.pdf (accessed on 8 April 2024).
26. del Campo, G.; Calatrava, S.; Canada, G.; Olloqui, J.; Martinez, R.; Santamaria, A. IoT Solution for Energy Optimization in Industry 4.0: Issues of a Real-Life Implementation. In Proceedings of the 2018 Global Internet of Things Summit (GIoTS), Bilbao, Spain, 4–7 June 2018; pp. 1–6. [CrossRef]
27. Ayoub, W.; Samhat, A.E.; Nouvel, F.; Mroue, M.; Prevotet, J.-C. Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1561–1581. [CrossRef]
28. Beyene, Y.D.; Jantti, R.; Tirkkonen, O.; Ruttik, K.; Iraji, S.; Larmo, A.; Tirronen, T.; Torsner, A.J. NB-IoT Technology Overview and Experience from Cloud-RAN Implementation. *IEEE Wirel. Commun.* **2017**, *24*, 26–32. [CrossRef]
29. Deutsche Telekom IoT NB-IoT, LoRaWAN, Sigfox: An Up-to-Date Comparison. Available online: https://testhardware.iot.telekom.com/LoadDocument/3522258863259434205/NB-IoT,%20LoRaWAN,%20Sigfox%20-%20An%20Up-to-date%20Comparison.pdf (accessed on 8 April 2024).
30. Gbadamosi, S.A.; Hancke, G.P.; Abu-Mahfouz, A.M. Building Upon NB-IoT Networks: A Roadmap Towards 5G New Radio Networks. *IEEE Access* **2020**, *8*, 188641–188672. [CrossRef]
31. Ratasuk, R.; Vejlgaard, B.; Mangalvedhe, N.; Ghosh, A. NB-IoT System for M2M Communication. In Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, Doha, Qatar, 3–6 April 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–5. [CrossRef]
32. Mroue, H.; Nasser, A.; Hamrioui, S.; Parrein, B.; Motta-Cruz, E.; Rouyer, G. MAC Layer-Based Evaluation of IoT Technologies: LoRa, SigFox and NB-IoT. In Proceedings of the 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), Jounieh, Lebanon, 18–20 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–5. [CrossRef]
33. Salva-Garcia, P.; Alcaraz-Calero, J.M.; Wang, Q.; Bernabe, J.B.; Skarmeta, A. 5G NB-IoT: Efficient Network Traffic Filtering for Multitenant IoT Cellular Networks. *Secur. Commun. Netw.* **2018**, *2018*, 9291506. [CrossRef]

34. Sánchez Rosado, D. NB-IoT Tecnologías Celulares Narrow-Band: Análisis Práctico de Las Soluciones de Telefónica y Vodafone. Master's Thesis, Universidad Complutense de Madrid, Madrid, Spain, 2019. Available online: https://docta.ucm.es/rest/api/core/bitstreams/28c3c5e5-4159-472b-bf0d-a9f21e546009/content (accessed on 8 April 2024).
35. Jia, G.; Zhu, Y.; Li, Y.; Zhu, Z.; Zhou, L. Analysis of the Effect of the Reliability of the NB-Iot Network on the Intelligent System. *IEEE Access* **2019**, *7*, 112809–112820. [CrossRef]
36. Mangalvedhe, N.; Ratasuk, R.; Ghosh, A. NB-IoT Deployment Study for Low Power Wide Area Cellular IoT. In Proceedings of the 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–8 September 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6. [CrossRef]
37. Wikipedia Constrained Application Protocol. Available online: https://en.wikipedia.org/wiki/Constrained_Application_Protocol (accessed on 8 April 2024).
38. Wikipedia Representational State Transfer. Available online: https://en.wikipedia.org/wiki/REST (accessed on 8 April 2024).
39. Nabu Casa, Home Assistant Community Home Assistant | Repositories. Available online: https://github.com/orgs/home-assistant/repositories (accessed on 8 April 2024).
40. Del Campo, G.; Saavedra, E.; Piovano, L.; Luque, F.; Santamaria, A. Virtual Reality and Internet of Things Based Digital Twin for Smart City Cross-Domain Interoperability. *Appl. Sci.* **2024**, *14*, 2747. [CrossRef]
41. Flask | Documentation. Available online: https://flask.palletsprojects.com/en/3.0.x/ (accessed on 8 April 2024).
42. CoAPython3. Available online: https://github.com/Tanganelli/CoAPthon3 (accessed on 8 April 2024).
43. Lencse, G.; Kadobayashi, Y. Methodology for the Identification of Potential Security Issues of Different IPv6 Transition Technologies: Threat Analysis of DNS64 and Stateful NAT64. *Comput. Secur.* **2018**, *77*, 397–411. [CrossRef]
44. Sabir, M.R.; Fahiem, M.A.; Mian, M.S. An Overview of IPv4 to IPv6 Transition and Security Issues. In Proceedings of the 2009 WRI International Conference on Communications and Mobile Computing, Kunming, China, 6–8 January 2009; IEEE: Piscataway, NJ, USA, 2009; pp. 636–639. [CrossRef]
45. Poole, O. *Network Security: A Practical Guide*; Computer Weekly Professional Series; Butterworth-Heinemann: Oxford, UK, 2003; ISBN 978-0-7506-5033-5.
46. Whitman, M.E.; Mattord, H.J.; Mackey, D.; Green, A. *Guide to Network Security*; Course Technology/Cengage Learning: Boston, MA, USA, 2013; ISBN 978-0-8400-2422-0.
47. Alagic, G.; Alperin-Sheriff, J.; Apon, D.; Cooper, D.; Dang, Q.; Liu, Y.-K.; Miller, C.; Moody, D.; Peralta, R.; Perlner, R.; et al. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019; p. NIST IR 8240.
48. Chen, L.; Jordan, S.; Liu, Y.-K.; Moody, D.; Peralta, R.; Perlner, R.; Smith-Tone, D. *Report on Post-Quantum Cryptography*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016; p. NIST IR 8105.
49. Kumar, M.; Pattnaik, P. Post Quantum Cryptography(PQC)—An Overview: (Invited Paper). In Proceedings of the 2020 IEEE High Performance Extreme Computing Conference (HPEC), Waltham, MA, USA, 22–24 September 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–9. [CrossRef]
50. Song, F. A Note on Quantum Security for Post-Quantum Cryptography. In *Post-Quantum Cryptography*; Mosca, M., Ed.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2014; Volume 8772, pp. 246–265, ISBN 978-3-319-11658-7.

5. Discussion

The findings presented in this thesis represent a comprehensive framework for addressing the critical challenges inherent in the design and deployment of self-sustaining Internet of Things systems. By advancing the integration of energy harvesting and wireless communication protocols, this research contributes to a new paradigm of IoT development, where autonomy, resilience, and sustainability are paramount. The implications of these findings are multifaceted, encompassing technical innovation, societal transformation, and environmental stewardship, while establishing a strong foundation for future advancements.

At the core of this research lies an exploration of diverse energy harvesting techniques, including solar, thermal, mechanical, and RF sources. By tailoring these energy sources to the requirements of specific communication protocols, such as NB-IoT, LoRa, Sigfox, and BLE, the thesis delivers a robust methodological framework for optimizing IoT device performance in varied contexts. This alignment ensures that devices can operate autonomously for extended periods without reliance on external power sources, significantly reducing maintenance demands and operational costs. Furthermore, this approach addresses the growing concern of electronic waste, positioning energy-harvesting IoT systems as a key enabler of environmentally sustainable technology.

The decentralized architecture of energy-harvesting IoT networks offers a scalable and resilient alternative to traditional systems. By distributing operational loads across energy-harvesting nodes, these networks reduce the risk of single points of failure and enhance their capacity to adapt to dynamic environments. The flexibility inherent in this design enables deployments in a wide range of applications, from industrial automation and rural energy monitoring to urban resource management. The thesis includes compelling real-world implementations that demonstrate the practical utility of these systems, underscoring their potential to revolutionize IoT deployments across diverse domains.

From a societal perspective, this research emphasizes the transformative potential of self-powered IoT systems to improve quality of life and bridge the digital divide. In urban environments, these systems enable efficient management of resources, including traffic flow, energy consumption, and public safety infrastructure. By leveraging autonomous operation, they reduce the costs and complexities associated with traditional IoT deployments, paving the way for smarter cities and communities. Meanwhile, in underserved or remote regions, self-powered IoT systems empower local populations by facilitating connectivity and enabling data-driven decision-making. Applications in precision agriculture, remote healthcare, and disaster response highlight the critical role of these technologies in promoting equity and resilience.

The environmental implications of energy-harvesting IoT systems are equally significant. These technologies offer a viable solution to the challenges posed by energy-intensive deployments, reducing the ecological footprint of IoT applications while enabling monitoring and conservation efforts in sensitive ecosystems. By harnessing ambient energy sources, these systems provide a sustainable alternative to conventional power solutions, supporting initiatives in biodiversity monitoring, forest fire prevention, and water resource management. The integration of energy-efficient protocols further enhances their capacity to operate in energy-scarce environments, making them an essential component of global sustainability strategies.

Despite the advancements achieved, several challenges remain that warrant continued exploration. The heterogeneity of IoT devices and protocols presents significant barriers to interoperability, complicating the integration of diverse systems. This thesis underscores the need for standardized frameworks and semantic interoperability mechanisms to enable seamless communication and coordination among heterogeneous networks. Additionally, the widespread adoption of IoT technologies raises critical cybersecurity concerns, necessitating the development of robust encryption, authentication, and data privacy measures. Blockchain-based identity management and decentralized authentication solutions are promising avenues for addressing these challenges, ensuring the integrity and security of IoT ecosystems.

The optimization of energy efficiency is another critical area of focus. While this research highlights the benefits of energy harvesting, further advancements are needed to maximize energy availability and adaptability. Hybrid energy systems that combine multiple harvesting techniques, such as solar and mechanical sources, offer considerable potential for enhancing reliability in diverse environmental conditions. Advanced power management algorithms capable of dynamically allocating resources based on real-time energy inputs and system demands represent another promising area for innovation. These strategies not only improve system reliability but also extend the operational lifespans of IoT devices, ensuring their viability in long-term deployments.

Emerging technologies, such as machine learning and edge computing, provide additional avenues for enhancing the functionality and scalability of IoT systems. Machine learning algorithms can optimize energy consumption, enable predictive analytics, and enhance decision-making capabilities, making IoT systems more intelligent and adaptive. Similarly, edge computing reduces latency and distributes computational resources, improving system responsiveness and efficiency. The integration of these technologies with energy-harvesting systems creates a powerful synergy that addresses the growing demands of IoT applications in real-time data processing and autonomous operation.

This research also highlights the importance of expanded testbed development for evaluating IoT systems under diverse operational scenarios. Modular testbeds capable of simulating a wide range of environmental conditions are essential for assessing the performance, scalability, and reliability of emerging technologies. By providing a controlled environment for experimentation, these platforms facilitate the development of next-generation IoT systems that are not only more efficient but also more resilient to the challenges posed by dynamic and unpredictable environments.

Another critical consideration is the integration of IoT systems into existing infrastructure and operational workflows. The research emphasizes the importance of designing IoT solutions that complement rather than disrupt existing systems, ensuring seamless adoption and minimal resistance from stakeholders. This requires careful consideration of factors such as cost, scalability, and user-friendliness, as well as the provision of comprehensive training and support for end-users. By addressing these practical concerns, IoT systems can achieve broader acceptance and generate greater impact across diverse applications.

In addition to technical considerations, this research also explores the broader societal, ethical and regulatory implications of IoT deployments. The widespread adoption of IoT technologies raises questions about data ownership, privacy, and accountability, particularly in applications involving sensitive or personal information. This thesis advocates for IoT systems that are deployed in a manner which respects individual rights and promotes public trust. Collaborative efforts among researchers, policymakers, and industry stakeholders are essential for achieving these goals and fostering the responsible development of IoT technologies.

‘On the Trade-Offs Between Energy Harvesting & Wireless Communications for Stand-Alone IoT Devices’ presents a transformative vision for the future of IoT systems, grounded in the integration of energy harvesting and low-power communication protocols. By addressing critical challenges related to autonomy, scalability, and sustainability, the research lays the groundwork for creating resilient IoT ecosystems capable of meeting the evolving demands of a connected world. The findings have far-reaching implications, offering a roadmap for achieving technological, societal, and environmental objectives. Through continued research and innovation, the full transformative potential of IoT can be realized, driving progress and sustainability in an increasingly interconnected global landscape. This thesis not only contributes to the advancement of IoT technologies but also underscores the critical role of interdisciplinary collaboration in shaping the future—and present—of a sustainable and equitable digital society.

5.1. Harvesting & Wireless — Tailoring

One of the most significant contributions of this thesis lies in the identification and optimization of energy-protocol pairings, which greatly enhance the sustainability and autonomy of IoT devices. Through careful alignment of specific energy harvesting methods—including solar, thermal, mechanical, and RF energy—with compatible low-power communication protocols such as NB-IoT, LoRa, BLE, and Sigfox, this research demonstrates the potential to achieve a highly reliable balance between energy availability and communication requirements. This tailored approach reduces dependency on external power sources, minimizes maintenance demands, and enhances the feasibility of deploying IoT devices in remote or hard-to-reach environments where conventional power sources are either unavailable or impractical.

Energy Source Suitability

A critical insight from this thesis is the adaptability of IoT systems through the integration of diverse energy harvesting methods, making design decisions contingent on specific use case conditions and requirements. The research identifies that magnetic induction is an optimal choice for smart meters due to its inherent compatibility with their operational nature. Magnetic fields generated by electrical systems can be leveraged to power monitoring devices, reducing the need for external energy sources. This finding is particularly relevant for urban and industrial energy monitoring applications where magnetic fields are abundant.

Solar energy harvesting emerges as the most effective solution for outdoor applications such as agricultural monitoring and environmental sensors. The abundance of sunlight in these settings ensures consistent energy availability, especially when paired with efficient photovoltaic cells and advanced energy storage systems. The thesis explores the use of flexible and high-efficiency PV cells, capable of maintaining functionality even under varying weather conditions or partial shading, enhancing the robustness of deployments in agricultural fields and ecological reserves.

Thermal energy harvesting proves particularly advantageous in industrial settings, where significant temperature gradients often exist. By converting waste heat into electrical energy, thermal energy harvesters provide a sustainable and untapped energy source for IoT devices. This thesis also highlights potential applications in environments where industrial machinery or pipelines create consistent thermal differentials, thereby eliminating the need for battery replacements in challenging conditions.

RF energy harvesting offers unique flexibility for dynamic urban environments. IoT devices in such settings can capitalize on the ubiquitous RF signals from Wi-Fi routers, mobile networks, and broadcast systems. The thesis presents an in-depth analysis of the trade-offs associated with RF energy harvesting, including challenges related to power density and signal interference, and demonstrates how advancements in RF rectenna design can overcome these limitations. By enabling small IoT devices to gather power from multiple RF bands, this approach supports the proliferation of autonomous IoT systems in dense urban settings.

The research underscores that selecting energy sources according to deployment environment conditions is pivotal for achieving sustained, autonomous IoT operations. Beyond selecting energy sources, this thesis emphasizes the importance of optimizing energy storage and management systems. The integration of supercapacitors and hybrid storage solutions ensures that energy harvested from ambient sources is efficiently stored and utilized, even under fluctuating environmental conditions. By combining these storage systems with dynamic power management algorithms, IoT devices can adaptively prioritize energy-intensive operations during surplus conditions while conserving energy for transmission-demanding periods. These mechanisms significantly extend device lifespans, reduce maintenance needs, and facilitate deployments in hazardous or inaccessible locations.

Wireless Protocol Customization

Equally significant is the tailored selection and configuration of wireless communication protocols to complement specific energy harvesting sources. Comparative analyses of BLE, LoRaWAN, and NB-IoT conducted in this thesis illustrate how these technologies perform under varying energy constraints and environmental conditions, guiding protocol selection for specific use cases. The research provides a detailed exploration of the trade-offs among data rate, range, and energy efficiency.

LoRaWAN, for instance, excels in long-range communication with minimal power consumption, making it ideal for rural and remote deployments. Its ability to self-manage networks and operate with intermittent energy availability aligns well with solar and thermal energy harvesting applications. In contrast, NB-IoT is better suited for urban environments and industrial settings where higher data throughput and availability are required. The protocol’s ability to operate in licensed spectrum bands ensures robust communication even in congested networks. Sigfox is identified as the preferred choice for scenarios demanding delivery success and stability over extended periods, particularly in low-bandwidth applications such as environmental monitoring or smart metering.

Additionally, this thesis demonstrates the significant energy savings achievable through configurable protocol settings. By optimizing packet sizes, adjusting transmission intervals, and selectively enabling security features, IoT systems can conserve energy without compromising functionality. The thesis also discusses the role of emerging wireless technologies such as Wi-Fi HaLow and Zigbee, which offer promising alternatives for niche applications requiring short-range, high-density connectivity. These findings underscore the delicate balance between maintaining robust communication and preserving energy, providing a blueprint for future IoT systems that are both efficient and adaptable.

Paring Thereof

One of the key outcomes of this research is the systematic pairing of specific energy harvesting sources with compatible communication protocols to maximize performance under designated operational conditions. Specifically, the smart meter use case was detailed extensively in [Saavedra 2021], where a comprehensive evaluation of combinations of energy harvesting techniques and IoT wireless technologies is provided, factoring in functional requisites such as metering periods, communication requirements such as buffer sizes, and environmental constraints such as energy source availability. In that work, **Table 3** was presented as a wrapping blueprint on the aforementioned matters, i.e., combination of energy harvesting technique and IoT wireless technology depending on the functional requisites (metering period), communication requirements (buffer size) and location constraints (EH source availability).

Table 3. Smart meter average consumption (mW) depending on buffer size—message payload—, metering period and wireless technology; where italics mean that magnetic induction EH complies, so does PV; underline means that only PV complies; grey text means that no EH technique would comply.

Buffer Size (Bytes)	Metering Period (min.)	Sigfox	LoRaWAN	NB-IoT	Wi-Fi	BLE
12	1	15.07	11.31	39.69	10.89	9.85
	5	3.08	2.33	8.00	2.24	2.03
	10	*1.58*	*1.20*	4.04	*1.16*	*1.06*
	15	*1.08*	*0.83*	2.72	*0.80*	*0.73*
24	1	15.07	10.40	24.59	10.18	9.66
	5	3.08	2.15	4.98	2.10	2.00
	10	*1.58*	*1.11*	2.53	*1.09*	*1.04*
	15	*1.08*	*0.77*	*1.72*	*0.75*	*0.72*
48	1	15.07	9.95	17.03	9.83	9.57
	5	3.08	2.05	3.47	2.03	*1.98*
	10	*1.58*	*1.07*	*1.78*	*1.06*	*1.03*
	15	*1.08*	*0.74*	*1.21*	*0.73*	*0.71*
96	1	15.07	9.72	13.26	9.65	9.53
	5	3.08	2.01	2.72	*1.99*	*1.97*
	10	*1.58*	*1.05*	*1.40*	*1.04*	*1.03*
	15	*1.08*	*0.72*	*0.96*	*0.72*	*0.71*
192	1	15.07	9.60	11.37	9.57	9.50
	5	3.08	*1.99*	2.34	*1.98*	*1.97*
	10	*1.58*	*1.03*	*1.21*	*1.03*	*1.02*
	15	*1.08*	*0.71*	*0.83*	*0.71*	*0.71*
384	1	15.07	9.55	11.42	9.50	9.49
	5	3.08	*1.98*	2.15	*1.97*	*1.96*
	10	*1.58*	*1.03*	*1.12*	*1.03*	*1.02*
	15	*1.08*	*0.71*	*0.77*	*0.71*	*0.70*
768	1	15.07	9.52	9.95	9.50	9.49
	5	3.08	*1.97*	2.06	*1.97*	*1.96*
	10	*1.58*	*1.03*	*1.07*	*1.02*	*1.02*
	15	*1.08*	*0.71*	*0.74*	*0.71*	*0.71*

This research highlights the nuanced trade-offs involved in these pairings, such as balancing energy harvesting efficiency against protocol-specific energy demands and ensuring that storage solutions can accommodate peak energy consumption during transmission bursts. By developing a

decision-making framework that integrates these considerations, the thesis equips future researchers and practitioners with the tools to design IoT systems optimized for diverse applications and environmental conditions. By addressing the intricate dependencies between energy availability, protocol efficiency, and deployment context, this research lays the groundwork for the development of resilient, autonomous IoT systems capable of operating in diverse and challenging environments. The insights presented here not only advance the state of the art in IoT design but also open new pathways for innovation in sustainable technology.

5.2. Scalability & Interoperability

Both scalability and interoperability are foundational to designing robust, future-proof IoT systems. By integrating energy-harvesting devices into decentralized network architectures and addressing the inherent challenges of heterogeneous IoT ecosystems, this research offers a comprehensive framework for enabling large-scale, sustainable, and inclusive IoT deployments. These advancements lay the groundwork for systems capable of meeting the demands of increasingly interconnected and complex environments.

Scalability Through Decentralized Network Design

The integration of energy-harvesting devices into IoT networks fosters decentralized architectures that enable scalability without requiring extensive infrastructure investments. This approach demonstrates how energy-harvesting nodes can act as autonomous, distributed components within peer-to-peer networks, effectively managing data flow and reducing bottlenecks in high-density IoT environments. Such networks not only enhance responsiveness and adaptability but also provide the flexibility to scale across larger geographical areas and dynamic operational conditions.

By leveraging decentralized designs, IoT systems can adapt to applications such as smart cities, remote environmental monitoring, and industrial automation. These settings often demand the ability to scale dynamically as additional sensors and devices are integrated into the system. Energy-harvesting nodes play a pivotal role by ensuring that scaling occurs with minimal increases in energy demand and infrastructure complexity. For example, this thesis highlights implementations in rural energy monitoring, where decentralized architectures allow widespread deployment of sensors over large areas, reducing dependency on centralized power grids and infrastructure. Similarly, in industrial automation, distributed energy-harvesting devices enhance the efficiency and flexibility of production processes, enabling adaptive resource allocation and minimizing downtime.

The scalability of these architectures is further reinforced by their inherent resilience. Decentralized networks distribute workloads and eliminate single points of failure, ensuring that IoT systems remain operational even under adverse conditions. This feature is particularly critical for mission-critical applications, such as disaster response or environmental conservation, where system reliability is paramount. The research also explores the integration of fault-tolerant mechanisms, including redundancy at the node level and intelligent routing algorithms, which further bolster the resilience and scalability of decentralized networks. These advancements align with the growing need for IoT solutions that can handle expanding data loads and increasing operational demands.

Interoperability in Complex IoT Ecosystems

As IoT ecosystems become increasingly heterogeneous, ensuring seamless integration and communication across diverse devices, platforms, and protocols is essential. This thesis advances

the state of the art in interoperability by addressing key challenges and proposing innovative solutions that enable cohesive and collaborative IoT networks.

One major contribution is the development of mechanisms for bridging legacy and modern systems. The coexistence of IPv6 and IPv4 networks often poses challenges for IoT deployments that need to integrate older devices with newer infrastructures. This research demonstrates practical methods, such as relay mechanisms and protocol translation layers, that harmonize communication across these networks. By maintaining continuity and inclusivity, these solutions support the gradual evolution of IoT ecosystems while preserving the functionality of legacy systems.

Another critical advancement is the introduction of semantic interoperability frameworks. These frameworks enable devices with disparate architectures to exchange meaningful data, facilitating intelligent decision-making and system-wide coordination. By leveraging standardized ontologies and data models, the thesis lays the groundwork for smarter, more collaborative networks capable of supporting complex, multi-vendor ecosystems. Such frameworks are particularly valuable in applications where interoperability is vital, such as healthcare IoT systems that require seamless integration of devices from multiple manufacturers to deliver cohesive patient care.

Open-source ecosystems also play a significant role in overcoming interoperability challenges. Platforms like Home Assistant exemplify the power of community-driven initiatives in fostering modular and interoperable solutions. This research highlights how open-source platforms encourage innovation, reduce vendor lock-in, and provide adaptable solutions for diverse IoT applications. By embracing open standards and collaborative development, these ecosystems empower developers and users to tailor IoT solutions to their specific needs, ensuring long-term adaptability and sustainability.

Scalability and Sustainability in Practice

The research aligns technical advancements with broader goals of sustainability and scalability, demonstrating how decentralized architectures and interoperability frameworks contribute to the long-term viability of IoT ecosystems. One notable contribution is the development of modular testbeds for evaluating IoT systems. These testbeds provide a standardized methodology for assessing critical parameters such as latency, error rate, and energy consumption. By enabling reproducibility and reliability in IoT research, they facilitate the iterative improvement of IoT technologies and ensure that deployments are optimized for real-world conditions.

Energy efficiency and resource optimization are central to the scalability of IoT systems. Decentralized architectures supported by energy-harvesting nodes reduce both energy and electronic waste by enabling autonomous operation and minimizing reliance on centralized systems. This thesis emphasizes the dual benefits of these advancements: they not only enhance the environmental sustainability of IoT deployments but also reduce operational costs, making large-scale deployments economically feasible. Practical examples include the use of energy-harvesting sensors in rural and industrial settings, where decentralized designs eliminate the need for extensive wiring and power infrastructure, reducing environmental impact and facilitating rapid deployment.

Real-world demonstrations further validate the feasibility and impact of these concepts. For instance, in agricultural monitoring, decentralized energy-harvesting sensors provide precise, real-time data on soil moisture and temperature, enabling farmers to optimize irrigation and reduce water waste. In industrial automation, energy-harvesting devices support predictive maintenance by continuously monitoring machinery conditions and alerting operators to potential failures before

they occur. These use cases exemplify how IoT systems can scale effectively while maintaining operational efficiency and minimizing environmental impact.

In conclusion, the integration of scalability and interoperability into IoT system design is essential for addressing the growing demands of a connected world. By leveraging decentralized architectures, fostering seamless integration across heterogeneous devices, and aligning technical innovations with sustainability goals, this research provides a blueprint for building robust and future-proof IoT ecosystems. The findings presented here not only advance the state of the art but also lay the foundation for continued innovation in scalable, sustainable, and interoperable IoT solutions capable of transforming industries and improving quality of life on a global scale.

5.3. Broader Implications

Broader implications of this research extend far beyond isolated use cases, emphasizing its transformative potential to shape the evolution of IoT ecosystems across a far-reaching, wide range of domains. By addressing critical challenges and proposing innovative solutions, this thesis provides a comprehensive framework for leveraging IoT technologies to address complex global challenges. Through continued research and innovation, the findings presented here have the potential to transform industries, protect the environment, and improve quality of life for communities around the world. The work serves as a catalyst for realizing the full promise of IoT technologies, driving progress towards a more connected, sustainable, and equitable future.

Industry

By addressing critical challenges in deploying IoT systems within resource-constrained environments, the findings contribute significantly to the advancement of Industry 4.0. This includes enabling predictive maintenance, optimizing energy use, and fostering smarter automation systems. Such capabilities are of paramount importance to industries striving to enhance operational efficiency, reduce downtime, and achieve sustainable production processes[*].

The industrial implications of this research are multifaceted. Predictive maintenance, supported by self-powered IoT devices, enables real-time monitoring of machinery and infrastructure, reducing unexpected breakdowns and associated costs. The integration of autonomous IoT systems into supply chains enhances visibility and control, allowing for dynamic resource allocation and just-in-time operations. Furthermore, by minimizing energy consumption through tailored energy harvesting and storage solutions, industries can significantly lower their carbon footprint while maintaining operational efficiency. These advancements align with global efforts to transition towards more sustainable and resilient industrial ecosystems, making the findings of this thesis particularly relevant in the context of ongoing digital transformation initiatives.

Environment

The research also holds profound promise for environmental conservation. Self-powered IoT devices, by virtue of their ability to operate autonomously and sustainably, offer a compelling solution for reducing the ecological footprint of large-scale deployments. This is particularly critical in

[*] It is worth noting that the outcomes of this thesis remain at the stage of proofs of concept and have not yet been industrially or commercially exploited.

sensitive ecosystems where conventional technologies may disrupt natural processes or impose significant maintenance burdens. Applications in biodiversity monitoring, for instance, demonstrate how IoT sensors can provide detailed insights into wildlife behavior and habitat health without human intervention. Similarly, the deployment of IoT systems for forest fire prevention enables the early detection of environmental changes, facilitating timely interventions that can mitigate disaster risks. In aquatic ecosystems, self-sustaining IoT devices are used to monitor water quality, ensuring the health and sustainability of critical resources. These examples illustrate how IoT technologies can support global sustainability efforts while promoting environmental stewardship on a large scale.

Society

Beyond environmental and industrial applications, the societal implications of this research are equally profound. In urban environments, self-sustaining IoT systems have the potential to revolutionize smart city initiatives, improving quality of life by enabling efficient resource management, real-time traffic monitoring, and enhanced public safety. These systems can optimize energy distribution, reduce waste, and support dynamic urban planning, ensuring that cities are equipped to handle the challenges of rapid urbanization and climate change. Additionally, self-powered IoT systems can bridge the digital divide by providing access to advanced technologies in underserved or remote regions. By enabling connectivity and facilitating data-driven decision-making, these innovations empower communities to address local challenges and seize opportunities for development.

Sustainability

The implications of this research also extend into the realm of global sustainability and policy. The deployment of IoT systems that integrate energy harvesting and low-power communication protocols aligns with international goals such as the United Nations Sustainable Development Goals (SDGs). By providing scalable and inclusive solutions to challenges in energy access, resource management, and environmental protection, this thesis contributes to the broader mission of fostering sustainable development worldwide. Moreover, the adoption of these technologies can drive the creation of new regulatory frameworks and standards that promote the responsible and ethical use of IoT systems, ensuring that their deployment benefits society.

This thesis not only advances the state of the art in IoT research but also lays a comprehensive roadmap for the sustainable, scalable, and inclusive deployment of IoT systems. The findings serve as a foundation for future research in several key areas. Hybrid energy systems that combine multiple harvesting techniques, such as solar and thermal energy, offer opportunities to further enhance energy availability and reliability in diverse environments. Adaptive machine learning models can optimize energy consumption dynamically, enabling IoT systems to respond intelligently to changing conditions and demands. The expansion of interoperability frameworks will also be crucial for ensuring seamless integration across heterogeneous networks and diverse application contexts, paving the way for more cohesive and collaborative IoT ecosystems.

Yet, deeper research on the ethical and societal dimensions of IoT deployments is necessary. As IoT systems become increasingly pervasive, questions about data privacy, ownership, and security will become more pressing. This thesis provides a—starting—steppingstone for addressing these challenges by advocating for the development of robust encryption methods, decentralized authentication protocols, and transparent data governance models. By aligning technological advancements with ethical considerations, the full transformative potential of IoT technologies can be realized in a manner that respects individual rights and promotes social equity.

6. Conclusion

This thesis presents an in-depth investigation into the integration of energy harvesting with wireless communication protocols for autonomous IoT devices, focusing on enhancing sustainability, scalability, and adaptability in various real-world applications. Through comprehensive research, including experimental validation, theoretical analysis, and field deployments, this study has developed innovative frameworks and methodologies that contribute significantly to the IoT field. Below is a summary of the primary findings and answers to the key research questions addressed throughout this work.

The insights and methodologies developed in this thesis offer a versatile blueprint for IoT systems across various sectors, including healthcare, environmental monitoring, smart cities, and industrial automation. By providing a systematic approach to pairing energy sources with communication protocols and implementing adaptive management and security frameworks, this research paves the way for cross-disciplinary IoT applications.

The findings are broadly applicable, enabling IoT developers and researchers to adapt these strategies to meet specific industry needs, promoting innovation and sustainability within and beyond traditional IoT environments.

The insights and recommendations presented in this thesis illustrate the transformative potential of integrating energy harvesting with IoT technology. This vision extends beyond the current applications of IoT, positioning energy-harvesting devices as foundational elements in the next generation of sustainable, resilient, and adaptable technology systems. The findings offer a pathway for IoT to not only address immediate operational needs but also to become a driver of environmental and social progress on a global scale.

By enabling IoT systems to operate autonomously and efficiently across diverse sectors, this thesis contributes to the foundation of a technology landscape that is both connected and sustainable, ensuring that IoT continues to serve the needs of a rapidly changing world. The continued exploration and application of these concepts in future research and development will further solidify IoT's role in fostering a more efficient, connected, and ecologically conscious future.

6.1. Future Research

This thesis provides valuable insights into integrating energy harvesting with wireless communication protocols for autonomous IoT devices, offering a robust framework for creating sustainable and resilient IoT systems. Nevertheless, the findings open up numerous avenues for further research and highlight potential applications that could extend and amplify the impact of this work. In this section, we outline key recommendations for future research and discuss the broader applicability of the findings across various domains.

By advancing the integration of energy harvesting and wireless communication, this research provides a framework for developing sustainable, autonomous IoT systems. The findings of this thesis hold significant implications for IoT applications across numerous sectors, including environmental monitoring, smart agriculture, industrial automation, and smart cities. For instance, autonomous IoT sensors powered by solar or thermal energy can continuously monitor environmental conditions in remote areas, while RF-powered devices could support healthcare applications within

densely populated facilities. The flexibility and adaptability of these solutions highlight the potential of energy-harvesting IoT devices to reduce maintenance costs, minimize environmental impact, and support scalable, resilient IoT networks.

Therefore, this thesis presents a comprehensive study on the integration of energy harvesting methods with wireless communication protocols, establishing best practices for pairing specific energy sources with compatible protocols. These insights contribute to the development of self-sustaining IoT devices capable of operating autonomously in diverse environments. As IoT technology continues to evolve, the integration of energy harvesting will be essential in supporting sustainable, scalable, and efficient IoT ecosystems that can meet the demands of a connected world. This research provides a strong foundation for future innovation in energy-efficient IoT design, supporting the advancement of resilient and resource-conscious IoT solutions.

Advanced Energy Harvesting Technologies

Future research should delve into emerging energy harvesting methods, such as piezoelectric materials, hybrid photovoltaic-thermoelectric systems, and novel RF harvesting techniques. While this thesis primarily focuses on established sources like solar, thermal, and RF energy, innovative materials and hybrid systems are showing promise for generating higher and more stable energy outputs. Exploring these sources could provide a richer understanding of how hybrid energy harvesting configurations might address power variability challenges, especially for IoT devices deployed in environments with fluctuating energy availability. Additionally, the integration of flexible or wearable energy harvesters could open new applications in fields like healthcare, smart clothing, and mobile IoT.

Machine Learning for Predictive Power Management

Building on the adaptive power management strategies discussed in this research, future studies could investigate the application of machine learning models, particularly those trained on environmental and operational data, to optimize power usage more dynamically. Predictive models could forecast energy availability based on historical data, seasonal variations, and real-time environmental factors, enabling IoT devices to adapt their functionality preemptively. Reinforcement learning approaches could also be explored, allowing devices to learn optimal power usage strategies based on feedback from real-world operations. This advancement could be transformative for remote and autonomous IoT applications, especially where manual adjustments to device settings are impractical.

Edge Computing & Localized Data Processing

As the volume of data generated by IoT devices grows, future research could focus on integrating edge computing capabilities to process data locally, reducing transmission requirements and conserving energy. By deploying lightweight, energy-efficient processors at the device level, IoT systems could filter, aggregate, and analyze data in real time, sending only essential information to the cloud. This approach would not only reduce latency and bandwidth demands but also allow devices to operate autonomously in low-bandwidth environments. Future studies could explore energy-efficient processing algorithms that could operate on harvested energy, enabling real-time decision-making in applications like environmental monitoring and industrial automation.

Security Solutions for Post-Quantum IoT Networks

With the rise of quantum computing, the development of post-quantum cryptographic protocols is becoming essential. Research could focus on creating quantum-resistant encryption tailored for energy-constrained, energy-harvesting IoT devices. The challenge lies in optimizing cryptographic techniques that provide robust security without depleting limited energy resources. Studies could investigate hybrid encryption models that combine traditional and quantum-resistant methods, as well as lightweight cryptographic algorithms optimized for real-time data protection in critical applications, such as healthcare and industrial IoT.

Enhanced Interoperability Standards for Multi-Protocol IoT Networks

As IoT ecosystems become more heterogeneous, future research could aim to develop interoperability standards that facilitate seamless integration of devices operating on various communication protocols. While this thesis highlights the compatibility of specific energy sources with certain protocols, broader interoperability frameworks are essential for IoT networks that span diverse environments and application requirements. Efforts could be directed towards developing universal translation layers or protocol-agnostic communication standards, allowing energy-harvesting devices to interoperate regardless of the protocols used in neighboring networks. Such research would be instrumental for expanding IoT systems in smart cities and multi-tenant industrial environments.

References

[Al-Amiedy 2022] Al-Amiedy T.A., Anbar M., Belaton B., Kabla A.H.H., Hasbullah I.H., Alashhab Z.R. (2022) A systematic literature review on machine and deep learning approaches for detecting attacks in RPL-based 6LoWPAN of internet of things. Sensors 22:3400

[Alenezi 2020] Alenezi M., Chai K.K., Chen Y., Jimaa S. (2020) Ultra-dense LoRaWAN: Reviews and challenges. IET Communications 14:1361–1371. https://doi.org/10.1049/iet-com.2018.6128

[Al-Kashoash 2016] Al-Kashoash H.A.A., Kemp A.H. (2016) Comparison of 6LoWPAN and LPWAN for the Internet of Things. Australian Journal of Electrical and Electronics Engineering 13:268–274. https://doi.org/10.1080/1448837X.2017.1409920

[Alobaidy 2020] Alobaidy H.A.H., Mandeep J.S., Nordin R., Abdullah N.F. (2020) A Review on ZigBee Based WSNs: Concepts, Infrastructure, Applications, and Challenges. ijeetc 189–198. https://doi.org/10.18178/ijeetc.9.3.189-198

[Alsukayti 2020] Alsukayti I.S. (2020) A Multidimensional Internet of Things Testbed System: Development and Evaluation. Wireless Communications and Mobile Computing 2020:1–17. https://doi.org/10.1155/2020/8849433

[Anand 2020] Anand P., Singh Y., Selwal A., Singh P.K., Felseghi R.A., Raboaca M.S. (2020) IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications towards Smart Grids. Energies 13:4813. https://doi.org/10.3390/en13184813

[Arzo 2021] Arzo S.T., Zambotto F., Granelli F., Bassoli R., Devetsikiotis M., Fitzek F.H.P. (2021) A Translator as Virtual Network Function for Network Level Interoperability of Different IoT Technologies. In: 2021 IEEE 7th International Conference on Network Softwarization (NetSoft). IEEE, Tokyo, Japan, pp 416–422

[Atutxa 2021] Atutxa A., Franco D., Sasiain J., Astorga J., Jacob E. (2021) Achieving Low Latency Communications in Smart Industrial Networks with Programmable Data Planes. Sensors 21:5199. https://doi.org/10.3390/s21155199

[Ayoub 2019] Ayoub W., Samhat A.E., Nouvel F., Mroue M., Prevotet J.-C. (2019) Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility. IEEE Commun Surv Tutorials 21:1561–1581. https://doi.org/10.1109/COMST.2018.2877382

[Beyene 2017] Beyene Y.D., Jantti R., Tirkkonen O., Ruttik K., Iraji S., Larmo A., Tirronen T., Torsner A.J. (2017) NB-IoT Technology Overview and Experience from Cloud-RAN Implementation. IEEE Wireless Commun 24:26–32. https://doi.org/10.1109/MWC.2017.1600418

[Cai 2012] Cai F., Farantatos E., Huang R., Meliopoulos A.P.S., Papapolymerou J. (2012) Self-powered smart meter with synchronized data. In: 2012 IEEE Radio and Wireless Symposium. IEEE, Santa Clara, CA, USA, pp 395–398

[Camps-Mur 2013] Camps-Mur D., Garcia-Saavedra A., Serrano P. (2013) Device-to-device communications with Wi-Fi Direct: overview and experimentation. IEEE Wireless Commun 20:96–104. https://doi.org/10.1109/MWC.2013.6549288

[Chaudhari 2020] Chaudhari B.S., Zennaro M., Borkar S. (2020) LPWAN Technologies: Emerging Application Characteristics, Requirements, and Design Considerations. Future Internet 12:46. https://doi.org/10.3390/fi12030046

[Chen 2021] Chen C., Li J., Balasubramaniam V., Wu Y., Zhang Y., Wan S. (2021) Contention Resolution in Wi-Fi 6-Enabled Internet of Things Based on Deep Learning. IEEE Internet Things J 8:5309–5320. https://doi.org/10.1109/JIOT.2020.3037774

[Cho 2014] Cho K., Park W., Hong M., Park G., Cho W., Seo J., Han K. (2014) Analysis of Latency Performance of Bluetooth Low Energy (BLE) Networks. Sensors 15:59–78. https://doi.org/10.3390/s150100059

[Chren 2016] Chren S., Rossi B., Pitner T. (2016) Smart grids deployments within EU projects: The role of smart meters. In: 2016 Smart Cities Symposium Prague (SCSP). IEEE, Prague, Czech Republic, pp 1–5

[Cujilema 2023] Cujilema J.A., Hidalgo Brito G.A., Hernandez Rojas D.L., Cartuche Calva J.J. (2023) Secure home automation system based on ESP-NOW mesh network, MQTT and Home Assistant platform. IEEE Latin Am Trans 21:829–838. https://doi.org/10.1109/TLA.2023.10244182

[de Carvalho 2017] de Carvalho J., Rodrigues J.J.P.C., Alberti A.M., Solic P., Aquino A.L.L. (2017) 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). pp 1–6

[del Campo 2018] del Campo G., Calatrava S., Canada G., Olloqui J., Martinez R., Santamaria A. (2018) IoT Solution for Energy Optimization in Industry 4.0: Issues of a Real-life Implementation. In: 2018 Global Internet of Things Summit (GIoTS). IEEE, Bilbao, pp 1–6

[del Campo 2020] del Campo G., Gomez I., Cañada G., Piovano L., Santamaria A. (2020) Guidelines and criteria for selecting the optimal low-power wide-area network technology. In: LPWAN Technologies for IoT and M2M Applications. Elsevier, pp 281–305

[Del Campo 2024] Del Campo G., Saavedra E., Piovano L., Luque F., Santamaria A. (2024) Virtual Reality and Internet of Things Based Digital Twin for Smart City Cross-Domain Interoperability. Applied Sciences 14:2747.

https://doi.org/10.3390/app14072747
[DeutscheTelekom 2021] DeutscheTelekom I. (2021) NB-IoT, LoRaWAN, Sigfox: An up-to-date comparison. https://iot.telekom.com/resource/blob/data/492968/e396f72b831b0602724ef71056af5045/mobile-iot-network-comparison-nb-iot-lorawan-sigfox.pdf. Accessed 5 Mar 2024
[Drula 2007] Drula C., Amza C., Rousseau F., Duda A. (2007) Adaptive energy conserving algorithms for neighbor discovery in opportunistic Bluetooth networks. IEEE J Select Areas Commun 25:96–107. https://doi.org/10.1109/JSAC.2007.070110
[Duflot 2006] Duflot M., Kwiatkowska M., Norman G., Parker D. (2006) A formal analysis of bluetooth device discovery. Int J Softw Tools Technol Transfer 8:621–632. https://doi.org/10.1007/s10009-006-0014-x
[Ergen 2004] Ergen S.C. (2004) ZigBee/IEEE 802.15. 4 Summary. UC Berkeley, September 10:11
[Ertürk 2019] Ertürk M.A., Aydın M.A., Büyükakkaşlar M.T., Evirgen H. (2019) A Survey on LoRaWAN Architecture, Protocol and Technologies. Future Internet 11:216. https://doi.org/10.3390/fi11100216
[Evans 2021] Evans D. (2021) The Internet of Things. How the Next Evolution of the Internet Is Changing Everything. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Accessed 5 Mar 2024
[Farahani 2011] Farahani S. (2011) ZigBee wireless networks and transceivers. newnes
[Gbadamosi 2020] Gbadamosi S.A., Hancke G.P., Abu-Mahfouz A.M. (2020) Building Upon NB-IoT Networks: A Roadmap Towards 5G New Radio Networks. IEEE Access 8:188641–188672. https://doi.org/10.1109/ACCESS.2020.3030653
[Gee 2010] Gee K., Chee K., Noordin N.K., Ali B.M. (2010) A review of 6LoWPAN routing protocols. Proceedings of the Asia-Pacific Advanced Network 30
[Ghumman 2019] Ghumman F.A. (2019) Effects of IPV4/IPv6 Transition Methods in IoT (Internet of Things):A survey. SSRN Journal. https://doi.org/10.2139/ssrn.3402664
[Gomez 2019] Gomez C., Veras J.C., Vidal R., Casals L., Paradells J. (2019) A Sigfox Energy Consumption Model. Sensors 19:681. https://doi.org/10.3390/s19030681
[Gregori 2002] Gregori E., Conti M., Campbell A.T., Omidyar G., Zukerman M. (2002) NETWORKING 2002: Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications: Second International IFIP-TC6 Networking Conference Pisa, Italy, May 19–24, 2002 Proceedings. Springer Berlin Heidelberg, Berlin, Heidelberg
[Grosse 2003] Grosse E., Lakshman Y.N. (2003) Network processors applied to IPv4/IPv6 transition. IEEE Network 17:35–39. https://doi.org/10.1109/MNET.2003.1220694
[Gunathilaka 2012] Gunathilaka W.M.D.R., Dinesh H.G.C.P., Gunasekara G.G.C.M., Narampanawe K.M.M.W.N.B., Wijayakulasooriya J.V. (2012) Ambient Radio Frequency energy harvesting. In: 2012 IEEE 7th International Conference on Industrial and Information Systems (ICIIS). IEEE, Chennai, India, pp 1–5
[Han 2015] Han J., Hu J., Yang Y., Wang Z., Wang S.X., He J. (2015) A Nonintrusive Power Supply Design for Self-Powered Sensor Networks in the Smart Grid by Scavenging Energy From AC Power Line. IEEE Trans Ind Electron 62:4398–4407. https://doi.org/10.1109/TIE.2014.2383992
[Haxhibeqiri 2018] Haxhibeqiri J., De Poorter E., Moerman I., Hoebeke J. (2018) A Survey of LoRaWAN for IoT: From Technology to Application. Sensors 18:3995. https://doi.org/10.3390/s18113995
[Hedi 2017] Hedi I., Speh I., Sarabok A. (2017) IoT network protocols comparison for the purpose of IoT constrained networks. In: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, Opatija, Croatia, pp 501–505
[Hildebrandt 2017] Hildebrandt N., Spillmann C.M., Algar W.R., Pons T., Stewart M.H., Oh E., Susumu K., Díaz S.A., Delehanty J.B., Medintz I.L. (2017) Energy Transfer with Semiconductor Quantum Dot Bioconjugates: A Versatile Platform for Biosensing, Energy Harvesting, and Other Developing Applications. Chem Rev 117:536–711. https://doi.org/10.1021/acs.chemrev.6b00030
[Hossain 2017] Hossain M., Noor S., Karim Y., Hasan R. (2017) IoTbed: A Generic Architecture for Testbed as a Service for Internet of Things-Based Systems. In: 2017 IEEE International Congress on Internet of Things (ICIOT). IEEE, Honolulu, HI, USA, pp 42–49
[Hyun 2015] Hyun J., Li J., Kim H., Yoo J.-H., Hong J.W.-K. (2015) IPv4 and IPv6 performance comparison in IPv6 LTE network. In: 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, Busan, South Korea, pp 145–150
[Jara 2013] Jara A.J., Ladid L., Skarmeta A. (2013) The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 4:97–118. https://doi.org/10.22667/JOWUA.2013.09.31.097
[Jia 2019] Jia G., Zhu Y., Li Y., Zhu Z., Zhou L. (2019) Analysis of the Effect of the Reliability of the NB-Iot Network on the Intelligent System. IEEE Access 7:112809–112820. https://doi.org/10.1109/ACCESS.2019.2932870
[Jiménez 2016] Jiménez L. (2016) Diseño de implementación de etapa de comunicación basada en 6LoWPAN para plataforma modular de redes de sensores inalámbricas. TFT, Unicersidad Politécnica de Madrid

[Khairy 2019] Khairy S., Han M., Cai L.X., Cheng Y. (2019) Sustainable Wireless IoT Networks With RF Energy Charging Over Wi-Fi (CoWiFi). IEEE Internet Things J 6:10205–10218. https://doi.org/10.1109/JIOT.2019.2936837

[Kitamura, H.] Kitamura, H. A SOCKS-Based IPv4/IPv6 Gateway Mechanism. https://www.rfc-editor.org/rfc/pdfrfc/rfc3089.txt.pdf. Accessed 5 Mar 2024

[Kumar 2018] Kumar G., Tomar P. (2018) A Survey of IPv6 Addressing Schemes for Internet of Things: International Journal of Hyperconnectivity and the Internet of Things 2:43–57. https://doi.org/10.4018/IJHIoT.2018070104

[Lavric 2019] Lavric A., Petrariu A.I., Popa V. (2019) SigFox Communication Protocol: The New Era of IoT? In: 2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI). IEEE, Lisbon, Portugal, pp 1–4

[Lencse 2018] Lencse G., Kadobayashi Y. (2018) Methodology for the identification of potential security issues of different IPv6 transition technologies: Threat analysis of DNS64 and stateful NAT64. Computers & Security 77:397–411. https://doi.org/10.1016/j.cose.2018.04.012

[Lencse 2019] Lencse G., Kadobayashi Y. (2019) Comprehensive Survey of IPv6 Transition Technologies: A Subjective Classification for Security Analysis. IEICE Trans Commun E102.B:2021–2035. https://doi.org/10.1587/transcom.2018EBR0002

[Logan 2012] Logan B.E., Rabaey K. (2012) Conversion of Wastes into Bioelectricity and Chemicals by Using Microbial Electrochemical Technologies. Science 337:686–690. https://doi.org/10.1126/science.1217412

[Ma 2019] Ma Z., Xiao M., Xiao Y., Pang Z., Poor H.V., Vucetic B. (2019) High-Reliability and Low-Latency Wireless Communication for Internet of Things: Challenges, Fundamentals, and Enabling Technologies. IEEE Internet Things J 6:7946–7970. https://doi.org/10.1109/JIOT.2019.2907245

[Maayan 2020] Maayan G.D. (2020) The IoT Rundown For 2020: Stats, Risks, and Solutions. https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx. Accessed 5 Mar 2024

[Malhotra 2021] Malhotra P., Singh Y., Anand P., Bangotra D.K., Singh P.K., Hong W.-C. (2021) Internet of Things: Evolution, Concerns and Security Challenges. Sensors 21:1809. https://doi.org/10.3390/s21051809

[Mane 2021] Mane S.Y. (2021) LPWAN's – Overview, Market Scenario and Performance Analysis of Lora, Sigfox Using NB-Fi Range Calculator. In: 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON). IEEE, Pune, India, pp 1–4

[Mitchison 2019] Mitchison M.T. (2019) Quantum thermal absorption machines: refrigerators, engines and clocks. Contemporary Physics 60:164–187. https://doi.org/10.1080/00107514.2019.1631555

[Moghe 2010] Moghe R., Yang Y., Lambert F., Divan D. (2010) Design of a low cost self powered "Stick-on" current and temperature wireless sensor for utility assets. In: 2010 IEEE Energy Conversion Congress and Exposition. IEEE, Atlanta, GA, pp 4453–4460

[Moraes 2019] Moraes T., Nogueira B., Lira V., Tavares E. (2019) Performance Comparison of IoT Communication Protocols. In: 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC). IEEE, Bari, Italy, pp 3249–3254

[Mroue 2018] Mroue H., Nasser A., Hamrioui S., Parrein B., Motta-Cruz E., Rouyer G. (2018) MAC layer-based evaluation of IoT technologies: LoRa, SigFox and NB-IoT. In: 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM). IEEE, Jounieh, pp 1–5

[Newman 2019] Newman D. (2019) Return On IoT: Dealing With The IoT Skills Gap. https://www.forbes.com/sites/danielnewman/2019/07/30/return-on-iot-dealing-with-the-iot-skills-gap/?sh=5f453ccb7091. Accessed 5 Mar 2024

[Pan 2007] Pan M.-S., Tseng Y.-C. (2007) ZigBee and Their Applications. In: Mahalik NP (ed) Sensor Networks and Configuration. Springer Berlin Heidelberg, Berlin, Heidelberg, pp 349–368

[Paprotny 2010] Paprotny I., Leland E., Sherman C., White R.M., Wright P.K. (2010) Self-powered MEMS sensor module for measuring electrical quantities in residential, commercial, distribution and transmission power systems. In: 2010 IEEE Energy Conversion Congress and Exposition. IEEE, Atlanta, GA, pp 4159–4164

[Pasqua 2021] Pasqua E. (2021) 5 things to know about the LPWAN market in 2021. https://iot-analytics.com/5-things-to-know-lpwan-market/. Accessed 20 May 2022

[Pereira 2017] Pereira C., Pinto A., Ferreira D., Aguiar A. (2017) Experimental Characterization of Mobile IoT Application Latency. IEEE Internet Things J 4:1082–1094. https://doi.org/10.1109/JIOT.2017.2689682

[Porcarelli 2013] Porcarelli D., Brunelli D., Benini L. (2013) Clamp-and-measure forever: A MOSFET-based circuit for energy harvesting and measurement targeted for power meters. In: 5th IEEE International Workshop on Advances in Sensors and Interfaces IWASI. IEEE, Bari, Italy, pp 205–210

[Praktiknjo 2011] Praktiknjo A.J., Hähnel A., Erdmann G. (2011) Assessing energy supply security: Outage costs in private households. Energy Policy 39:7825–7833. https://doi.org/10.1016/j.enpol.2011.09.028

[Putra 2022] Putra B.D., Munadi R., Walidainy H., Syahrial, Arif T.Y., Putra A.T. (2022) Smart University Development Challenges using Lora or Sigfox technology: A Systematic Literature Review. In: 2022 FORTEI-International Conference on Electrical Engineering (FORTEI-ICEE). IEEE, Riau, Indonesia, pp 36–40

[Ramya 2011] Ramya C.M., Shanmugaraj M., Prabakaran R. (2011) Study on ZigBee technology. In: 2011 3rd International Conference on Electronics Computer Technology. IEEE, Kanyakumari, India, pp 297–301

[Rana 2021] Rana B., Singh Y., Singh P.K. (2021) A systematic survey on internet of things: Energy efficiency and interoperability perspective. Trans Emerging Tel Tech 32. https://doi.org/10.1002/ett.4166

[Ratasuk 2016] Ratasuk R., Vejlgaard B., Mangalvedhe N., Ghosh A. (2016) NB-IoT system for M2M communication. In: 2016 IEEE Wireless Communications and Networking Conference. IEEE, Doha, Qatar, pp 1–5

[Reinhardt 2011] Reinhardt A., Burkhardt D., Mogre P.S., Zaheer M., Steinmetz R. (2011) SmartMeter.KOM: A low-cost wireless sensor for distributed power metering. In: 2011 IEEE 36th Conference on Local Computer Networks. IEEE, Bonn, Germany, pp 1032–1039

[Ritchie 2020] Ritchie H., Roser M. (2020) CO_2 emissions. Our World in Data

[Rzepecki 2019] Rzepecki W., Ryba P. (2019) IoTSP: Thread Mesh vs Other Widely used Wireless Protocols – Comparison and use Cases Study. In: 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, Istanbul, Turkey, pp 291–295

[S. Farrell 2018] S. Farrell Ed. (2018) Low-Power Wide Area Network (LPWAN) Overview. https://tools.ietf.org/pdf/rfc8376.pdf. Accessed 5 Mar 2024

[Saavedra 2020] Saavedra E., del Campo G., Santamaria A. (2020) A Novel, Self-Powered, Non-Intrusive, Sigfox-Enabled Smart Meter for Challenging Scenarios. In: 2020 16th International Conference on Intelligent Environments (IE). IEEE, Madrid, Spain, pp 115–118

[Saavedra 2021] Saavedra E., Mascaraque L., Calderon G., del Campo G., Santamaria A. (2021) The Smart Meter Challenge: Feasibility of Autonomous Indoor IoT Devices Depending on Its Energy Harvesting Source and IoT Wireless Technology. Sensors 21:7433. https://doi.org/10.3390/s21227433

[Saavedra 2022] Saavedra E., Mascaraque L., Calderon G., Del Campo G., Santamaria A. (2022) A Universal Testbed for IoT Wireless Technologies: Abstracting Latency, Error Rate and Stability from the IoT Protocol and Hardware Platform. Sensors 22:4159. https://doi.org/10.3390/s22114159

[Saavedra 2024] Saavedra E., Santamaria A., Del Campo G., Gomez I. (2024) Leveraging IoT Harmonization: An Efficacious NB-IoT Relay for Integrating 6LoWPAN Devices into Legacy IPv4 Networks. Applied Sciences 14:3411. https://doi.org/10.3390/app14083411

[Sabir 2009] Sabir M.R., Fahiem M.A., Mian M.S. (2009) An Overview of IPv4 to IPv6 Transition and Security Issues. In: 2009 WRI International Conference on Communications and Mobile Computing. IEEE, Kunming, Yunnan, China, pp 636–639

[Salva-Garcia 2018] Salva-Garcia P., Alcaraz-Calero J.M., Wang Q., Bernabe J.B., Skarmeta A. (2018) 5G NB-IoT: Efficient Network Traffic Filtering for Multitenant IoT Cellular Networks. Security and Communication Networks 2018:1–21. https://doi.org/10.1155/2018/9291506

[Samad 2018] Samad F., Abbasi A., Memon Z.A., Aziz A., Rahman A. (2018) The Future of Internet: IPv6 Fulfilling the Routing Needs in Internet of Things. IJFGCN 11:13–22. https://doi.org/10.14257/ijfgcn.2018.11.1.02

[Sánchez 2019] Sánchez D. (2019) NB-IoT | Tecnologías celulares narrow-band: análisis práctico de las soluciones de Telefónica y Vodafone. TFM, Universidad Complutense de Madrid

[Savolainen 2013] Savolainen T., Soininen J., Silverajan B. (2013) IPv6 Addressing Strategies for IoT. IEEE Sensors J 13:3511–3519. https://doi.org/10.1109/JSEN.2013.2259691

[Schulz 2017] Schulz P., Matthe M., Klessig H., Simsek M., Fettweis G., Ansari J., Ashraf S.A., Almeroth B., Voigt J., Riedel I., Puschmann A., Mitschele-Thiel A., Muller M., Elste T., Windisch M. (2017) Latency Critical IoT Applications in 5G: Perspective on the Design of Radio Interface and Network Architecture. IEEE Commun Mag 55:70–78. https://doi.org/10.1109/MCOM.2017.1600435CM

[Sendin 2012] Sendin A., Berganza I., Arzuaga A., Pulkkinen A., Kim I.H. (2012) Performance results from 100,000+ PRIME smart meters deployment in Spain. In: 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm). IEEE, Tainan, Taiwan, pp 145–150

[Sendin 2014] Sendin A., Simon J., Urrutia I., Berganza I. (2014) PLC deployment and architecture for Smart Grid applications in Iberdrola. In: 18th IEEE International Symposium on Power Line Communications and Its Applications. IEEE, Glasgow, United Kingdom, pp 173–178

[Sinha 2017] Sinha R.S., Wei Y., Hwang S.-H. (2017) A survey on LPWA technology: LoRa and NB-IoT. ICT Express 3:14–21. https://doi.org/10.1016/j.icte.2017.03.004

[Sinha 2024] Sinha S. (2024) State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally. https://iot-analytics.com/number-connected-iot-devices/

[Sothmann 2015] Sothmann B., Sánchez R., Jordan A.N. (2015) Thermoelectric energy harvesting with quantum dots. Nanotechnology 26:032001. https://doi.org/10.1088/0957-4484/26/3/032001

[Tandon 2016] Tandon R., Simeone O. (2016) Cloud-aided wireless networks with edge caching: Fundamental latency trade-offs in fog Radio Access Networks. In: 2016 IEEE International Symposium on Information Theory (ISIT). IEEE, Barcelona, Spain, pp 2029–2033

[Thierschmann 2015] Thierschmann H., Sánchez R., Sothmann B., Arnold F., Heyn C., Hansen W., Buhmann H., Molenkamp L.W. (2015) Three-terminal energy harvester with coupled quantum dots. Nature Nanotech 10:854–858. https://doi.org/10.1038/nnano.2015.176

[Tozlu 2012] Tozlu S., Senel M., Mao W., Keshavarzian A. (2012) Wi-Fi enabled sensors for internet of things: A practical approach. IEEE Communications Magazine 50:134–143

[Ulukus 2015] Ulukus S., Yener A., Erkip E., Simeone O., Zorzi M., Grover P., Huang K. (2015) Energy Harvesting Wireless Communications: A Review of Recent Advances. IEEE J Select Areas Commun 33:360–381. https://doi.org/10.1109/JSAC.2015.2391531

[Unwala 2018a] Unwala I., Taqvi Z., Lu J. (2018) Thread: An IoT Protocol. In: 2018 IEEE Green Technologies Conference (GreenTech). IEEE, Austin, TX, pp 161–167

[Unwala 2018b] Unwala I., Taqvi Z., Lu J. (2018) IoT Security: ZWave and Thread. In: 2018 IEEE Green Technologies Conference (GreenTech). IEEE, Austin, TX, pp 176–182

[Wang 2014] Wang Z.L. (2014) Triboelectric nanogenerators as new energy technology and self-powered sensors – Principles, problems and perspectives. Faraday Discuss 176:447–458. https://doi.org/10.1039/C4FD00159A

[Wegner 2021] Wegner P. (2021) Global IoT spending to grow 24% in 2021, led by investments in IoT software and IoT security. In: IoT Analytics. https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/. Accessed 5 Mar 2024

[Woo 2014] Woo C.K., Ho T., Shiu A., Cheng Y.S., Horowitz I., Wang J. (2014) Residential outage cost estimation: Hong Kong. Energy Policy 72:204–210. https://doi.org/10.1016/j.enpol.2014.05.002

[Yang 2019] Yang Z., Chang C.H. (2019) 6LoWPAN Overview and Implementations. In: EWSN. pp 357–361

[Zhu 2012] Zhu G., Pan C., Guo W., Chen C.-Y., Zhou Y., Yu R., Wang Z.L. (2012) Triboelectric-Generator-Driven Pulse Electrodeposition for Micropatterning. Nano Lett 12:4960–4965. https://doi.org/10.1021/nl302560k

[Ziegler 2013] Ziegler S., Crettaz C., Ladid L., Krco S., Pokric B., Skarmeta A.F., Jara A., Kastner W., Jung M. (2013) IoT6 – Moving to an IPv6-Based Future IoT. In: Galis A, Gavras A (eds) The Future Internet. Springer Berlin Heidelberg, Berlin, Heidelberg, pp 161–172

[Zohourian 2023] Zohourian A., Dadkhah S., Neto E.C.P., Mahdikhani H., Danso P.K., Molyneaux H., Ghorbani A.A. (2023) IoT Zigbee device security: A comprehensive review. Internet of Things 22:100791. https://doi.org/10.1016/j.iot.2023.100791