PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
HASSIBA BENBOUALI UNIVERSITY OF CHLEF (UHBC) Algeria
Faculty of Exact and Computer Sciences
Department of Computer Science

THESIS

Submitted for the diploma of
DOCTORAT
Field: Computer Science
Speciality: Telecommunications and Network Engineering
By:

Chaib mostefa

Title:

Biometric Security in IoT Application of Smart City

Board of Examiners

1	ARIDJ Mohamed	M.C.A	UHBC-Chlef	Chairman
2	TAHAR ABBES Mounir	Professor	UHBC-Chlef	Supervisor
3	ALLALI Mohamed Abdelmadjid	M.C.B	UHBC-Chlef	Supervisor assistant
4	BECHAR Rachid	M.C.A	UHBC-Chlef	Examiner
5	LOUAZANI Ahmed	M.C.A	University Saad Dahlab Blida1	Examiner
6	GUERROUMI Mohamed	Professor	USTHB Algiers	Examiner

UHBC Algeria 2023-2024

SUMMARY

The Internet of Things (IoT) refers to the interconnection of various objects in our daily life, including cars, refrigerators, cell phones, smart doors, patient monitoring devices, and any other monitoring equipment. These devices are equipped with a smart sensor, an actuator, and internet connectivity, allowing them to exchange, gather, and send data to a remote server. IoT is a hybrid of various core forms of technology with varying levels of communication. Many existing IoT systems rely on a number of protocols and technologies. This causes complications with IoT connectivity and networking. Our thesis focuses on LoRaWAN networks because of their flexibility, as well as the fact that wireless communication takes advantage of the LoRa physical layer's long-range properties.

The different levels' requirements necessitate varying levels of security. Researchers strongly recommend deploying biometric security devices at levels where direct human access is essential. Biometric security offer a scalable solution for IoT that combats unauthorized access and credential swapping. Indeed, the biometric traits of human organs serve as a unique identity for each individual since they are universal, permanent, distinct, and work perfectly. This identification will be regarded as critical data to be transmitted in the IoT network; as a result, packet loss should be minimal and packet delivery ratio high. This data will be shared over the same medium, posing a significant collision risk that must be addressed and avoided.

Collisions occur in wireless communication due to the large number of nodes sharing the same channel. As a result, substantial amounts of data are lost. To avoid this issue, Networks Communications employs the CSMA method for detecting channel occupancy by measuring the carrier's Received Signal Strength Indication (RSSI). However, the known CSMA is inefficient in LoRa-based networks, such as LoRaWAN, which employs the ALOHA protocol. Because the receiver can demodulate signals even below the noise floors, LoRa wireless communication uses the Channel Activity Detection (CAD) approach to avoid collisions.

This study makes a contribution by integrating a new LoRaWAN module into the NS3 simulator and introducing a novel CSMA method called FT-CSMA, which is based on the well-known CSMA used in WIFI IEEE 802.11 and WSN IEEE 802.15.4.

In this work, we describe some interesting areas of IoT use while highlighting their faults and limits. We then provide our proposal to alleviate one of these restrictions. Finally, we present the IoT applications with biometric security methods that have been developed the most by scientists.

Keywords: IoT System; Smart city; Biometric Security; IoT Applications; LoRaWAN; WPAN; LPWAN

ACKNOWLEDGEMENTS

First, I praise Allah, the Almighty, whose grace and wisdom made this work possible.

I would particularly like to thank my supervisor, Professor Tahar Abbes Mounir, for the competent help he gave me, and especially for his patience, humility, concern and encouragement. His critical eye was invaluable in helping me make my contributions. I also express my gratitude to my co-supervisor Doctor Allali Mohamed Abdelmadjid for his help. As well as Professor Tahar Abbes Miloud, the laboratory director, and his successor, for all their help and encouragement.

I would like to express my sincere thanks to the members of the jury for the honor they have bestowed on me by taking the time to read and evaluate this work and the invaluable advice they have given both to me and to all those present on this Scientific Advisory Board. I would therefore like to take this opportunity to thank the doctoral students: Chenaoui Ali, Bettach djalloul, Maabed Mohamed, Lotfi Bendiaf and Nouar abdelouahab for their encouragement, support and assistance.

I would also like to thank the teaching and administrative staff of the UHBC University of Chlef for their efforts in providing us with an excellent training program.

Finally, I would like to thank all those who have contributed in any way to the realization of this work.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF PUBLICATIONS

1. **C. Mostefa**, T. A. Mounir, A. M. Abdelmadjid, and A. Nouar, "Ft-csma: A fine-tuned csma protocol for lora-based networks," Journal of Communications, no. 2, pp. 65–77, 2024. doi: 10.12720/jcm.19.2.65-77.

2. N. Abdelouahab, T. A. Mounir, B. Selma, and **C. Mostefa**, "Impact of mobility model on lorawan performance," JCM Journal of Communications, vol. 19, no. 1, pp. 7–18, 2024. doi: 10.12720/jcm.19.1.7-18.

3. **C. Mostefa**, N. Abdelouahab, T. A. Mounir, S. Boumerdassi, S. Femmam, and Z. A. Amel, "Formal validation of adr protocol in lorawan network using eventb," in 2023 7th International Conference on Computer, Software and Modeling (ICCSM), 2023, pp. 11–15. doi: 10.1109/ICCSM60247.2023.00011.

4. **C. Mostefa**, T. a. Mounir, and A. Mohamed abdlmadjid, "Simulate a lora-based iot network by adding a module in ns-3," in 2023 First national Conference on: Artificial Intelligence, Smart Technologies and Communications, UHBC Chlef, Algeria, 2023.

INTRODUCTION

The Internet of Things (IoT) refers to a network of interconnected computing devices, mechanical and digital equipment, items, or people (the physical environment) with unique identifiers that may transfer data and interact with business processes. This technology has become an important component in the field of smart cities, and it is mostly dependent on sensors, which are swiftly and massively evolving. This study will look at the key issues of the smart city concept, contemporary IoT technologies, and, specifically, the limits and requirements that IoT end devices (ED) must achieve. These end devices typically include a radio transceiver and antenna, as well as a micro-controller that handles sensor sampling, processing, and transmission. They are often powered by batteries, which presents new issues in terms of energy efficiency, availability, and service quality. The IoT must also meet size, manufacturing costs, and environmental deployment standards.

The primary goal of this thesis is to present a viable approach to designing and deploying secure IoT networks using biometric systems and LoRa technology. In particular, suggest a channel access method to avoid interference caused by the vast deployment of LoRa components. To achieve this purpose, the theoretical background and simulation issues are thoroughly discussed. This document contains five chapters that address this goal.

First, we discuss IoT's position in smart cities, as well as its benefits and impact. The issues related with IoT in the context of smart cities are also highlighted by exploring the concept and definition of smart cities, followed by an overview of important enabling and emergent security and privacy challenges in this context, as well as the solutions that exist. Finally, a quick overview of some emerging IoT applications in a smart city.

Chapter two examine existing IoT networking topologies, such as WPAN and LP-WAN, as well as their architecture and associated layers. We then discuss the limitations and key challenges that each IoT system must meet and overcome. Many existing IoT systems use a variety of protocols and technologies. This creates issues for IoT communication and networking.

The security of IoT devices is one of the main challenges of this technology. and security functions, including access control, are in urgent need of updating. In this context, while biometric authentication is recognized as an effective technique for secure authentication, it is difficult to use with limited objects. Biometrics deals with the recognition of individuals based on their behavioral or biological characteristics. Human organs, which could be considered as biometric means, should have the following main desirable properties: universality, permanence, uniqueness, performance, collectability, acceptability and circumvention. However, the extraction and processing of these biometric data is the subject of immensely complex calculations. in the third chapter, we discuss the challenges

faced by biometric security systems in the IoT domain, the biometrics in question and some examples of applications.

Furthermore, chapter four present IoT collision detection and avoidance solutions rely on several access protocols, including CSMA/CA. However, this is inefficient for IoT devices with limited energy that are widely deployed by many operators, particularly those that use heterogeneous technology. As a result, we explain in depth the interference problem, available remedies, and research directions such as spectrum control.

The fifth chapter is dedicated to our contribution, which consists in proposing a new media access mechanism to improve the quality of service of networks based on LoRa technology, in particular LoRaWAN. Based on the LoRaWAN network specification and the identification of standard protocols for collision avoidance in such LPWAN environments, we propose a new protocol called: A Fine-tuned CSMA (FT-CSMA). This protocol exploits the so-called: Channel Activity Detection (CAD) technique, which is a type of listen-before-talk (LBT) specific to LoRa. Using an NS-3 simulation tool, we analyze the performance of this new protocol in several types of networks, and demonstrate that FT-CSMA is a timely choice that outperforms other protocols in terms of performance and quality of service.

1. THE ROLE OF IOT IN SMART CITIES

1.1. Introduction

IoT items include a wide range of devices such as wearables, smartphones, computers, PDAs, and tablets. They have become part of our daily lives due to their low cost, mobility, and increasing computational capacity. This diverse range of intelligent gadgets, comprised of integrated sensors and processors, may manage their internal states or the external environment around them, and by collapsing, they add convenience and accessibility to our life. The Internet of Things offers enormous benefits, and its applications are transforming the way we work and live. It also opens up new possibilities for innovation, expansion, and knowledge sharing across various entities. These interconnected smart gadgets can be used in a wide range of industries, including smart homes, smart cities, the environment, agriculture, smart grids, industry, healthcare, and transportation.

The primary goals of the smart city are to provide a high quality of life for the inhabitants, to improve business and competition by addressing numerous difficulties, and to ensure the overall system's sustainability. A city is called smart if it integrates mobile communications, the internet, and cloud computing to create convergent, omnipresent, and fully aware applications. One of the distinguishing features of a smart city is the integration of multiple heterogeneous systems and infrastructures linked by networks. These systems and applications, created by individuals and businesses alike, collaborate and coordinate to collect municipal data and achieve their objectives.

The IoT solution supports and adds to the smart city's objectives in terms of data management, communication, security, and interoperability. In fact, huge data gathering, processing, and transformation are key to the IoT architecture. Data analysis can help businesses enhance their performance. Furthermore, this data can be shared through platforms or the cloud.

1.2. Why IoT?

IoT solutions comprise a variety of technologies and methods that are constantly growing alongside wireless networks. It has grown rapidly, particularly with the wireless sensor network (WSN) revolution and machine-to-machine (M2M) communication systems. However, the requirement for end-to-end Internet Protocol version 6 (IPv6) capability and multi-asset interaction has rendered IoT solutions unavoidable.

However, (IoT) is not the only name for this new notion. There are several confusing designations, such as machine-to-machine (M2M), a subset of the Internet of Things, which relates to an automated communications machine-to-machine and machine-to-human

interactions that occur without human involvement.

Cisco [1] invented the Internet of Everything (IoE), which connects objects, devices, people, and data to a worldwide network. The Internet of Anything (IoA) connects all envisioned objects, as well as real, well-known objects, as implied by the definition of IoE. Web of Things (WoT), in which things connect to a web framework via the Internet and push their collected data to it. The industrial Internet of Things (IIoT). The Social Internet of Things (SIoT), which allows things to have their own social networks, can be used in the IoT context by projecting things into the social realm, necessitating new thing definitions (social objects).

Figure 1.1 depicts an inclusive link between these several ideas. M2M, as opposed to IoT, focuses on connectivity rather than actual object representation. As a result, the shift from M2M to IoT necessitates additional considerations.

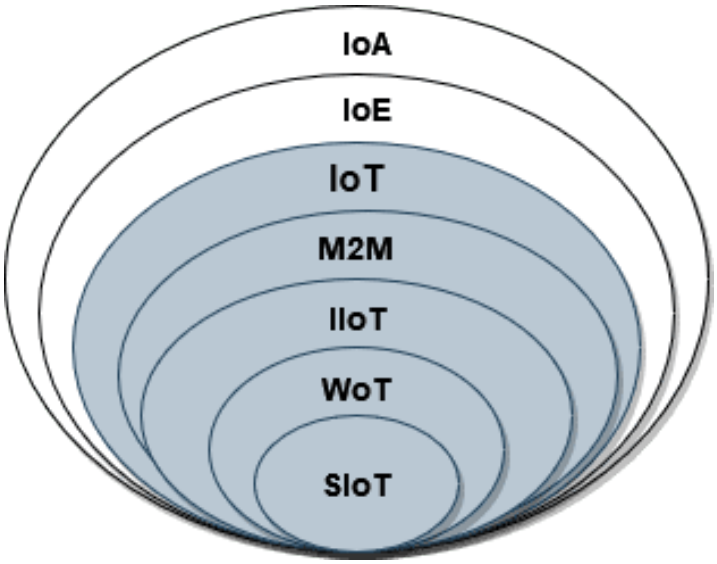

Fig. 1.1. Related IoT concepts [2]

1.2.1. IoT versus WSN

The creation of IoT is essentially inspired by WSN architecture, which addresses the issues associated with high energy consumption and short life cycles of WSN networks. WSNs are frequently used for monitoring purposes and to meet specific requirements. The Internet of Things, on the other hand, is a technology that connects hardware or many objects to the Internet, allowing them to talk with other devices, share data, and be used in more common scenarios. The protocols used in IoT are standardized, but WSNs may employ proprietary technology and protocols. IoT is more dynamic, as devices and things are moved around and connected to multiple networks. WSNs are usually static, with sensors placed in a precise spot and remained there. Typically, a single organization installations and uses the data collected by WSNs. IoT, on the other hand, is open, more decentralized, and can be static or mobile, comprising a variety of businesses and

individuals that exchange and exploit collected data.

1.2.2. IoT versus M2M

In [3], Rolando Herrero discusses the problems of M2M that led to the usage of IoT. This is because M2M is only useful for applications that require a simple decision, nonetheless interacting with other applications necessitates extensive standardization of transport and network layer protocols in order to improve communications. Scenarios in which many sensors with different parameters interact to make judgments on heterogeneous devices necessitate a consistent protocol, which most M2M solutions do not provide. The Internet of Things is essentially a super-set of M2M solutions made possible by standardization utilizing the Internet Protocol.

Traditional M2M systems are designed for applications that require monitoring, remote control, or optimisation of a single process. They provide point solutions for point problems. However, it is quite simple to justify this architecture for more sophisticated applications involving several systems. However, scaling is not easy, and interoperability with other systems as well as adaption to new scenarios can be difficult and expensive.

IoT and M2M are two technologies that enable remote access to items or sensors. M2M works by linking sensors from one location to another using integrated WiFi or a cellular module that runs from a server to software. They work by eliciting action-oriented responses. It is primarily one-way communication. In contrast, IoT refers to the transmission of data to a platform, the Internet, or a large-scale application. They communicate with one another, work in parallel, and constitute a unified network of services. These two technologies are defined by their capacity to establish connections with a wide range of items, devices, and systems. M2M requires a specific purpose; data received and transferred is precise, making it more closed than IoT. In short, the Internet of Things connects items such as physical equipment, buildings, cars, and people. In general, anything that can connect to the internet via network connectivity technology allows for data collection and exchange.

To create an IoT system, we simply add new sensors to M2M systems to collect more data, with the option of integrating the concept of Internet connectivity. This entails utilizing existing standard protocols. As a result, processing power is enhanced, allowing for vast data extraction and analysis with the goal of converting it into information. IoT is not the same as M2M; it is merely an evolution of the latter. To be more comprehensive, we may say that M2M is a subset of IoT or that IoT includes M2M. It's obvious that these two technological solutions are complementary.

1.3. Smart city

The literature defines smart cities differently depending on the study's setting and point of view. According to the participants' perceptions of a smart city, the authors envision a smart city as a system that enhances human and social capital through the interaction and judicious use of natural and economic resources, as well as the exploitation of technological and innovative solutions, with the goal of effectively achieving sustainable development and a high quality of life through a municipality-based multi-stakeholder partnership [4].

From a data management perspective, the authors of [5] define a smart city as a set of data management activities that operate within computer networks and are protected by data security and privacy mechanisms, with the goal of improving citizens' quality of life in five dimensions: public services, health, transportation, leisure, and administration.

A smart city, according to an ITU technical paper [6], is the activity of using information and communication technology (ICT) and other means to improve quality of life and rationalise resources while meeting the economic, social, environmental, and cultural needs of present and future generations.

From the aforementioned definitions, we can determine the major goals of smart cities:

- Improving quality of life (services)
- Efficiency (lower cost of living)
- Environmental sustainability (more effective use of public resources)

Nonetheless, it is always based on the expectations of smart city stakeholders or end users. This is because each group, whether inhabitants, academics, institutions, enterprises, or other individuals, has varying expectations of a smart city's capabilities and quality of service (QoS).

1.3.1. Key Technologies for Smart Cities

Digital technology is the third significant organizational revolution in modern urban systems, following the switch to electricity and the widespread adoption of automobiles. Smart cities are propelled by the digital wave, specifically the discovery of data resources, advancements in network technologies, and the acceleration of mobile usage around the smartphone.

When you look at the applications of a smart city, you will notice that they are not limited to IoT. It is a collection of technologies that work together to make certain applications possible. These technologies include cyberphysical systems (CPSs), data management and analytics, blockchain, real-time control, and AI/ML.

1.3.1.1 CPSs, IoT and Smart Cities

The Internet of Things does not encompass physical things or sophisticated equipment. This indicates that the Internet of Things (IoT) is a network of devices with limited capabilities, whereas CPSs are physical components and complex devices developed on the IoT platform. As a result, CPSs are projected to cover a greater range than IoT [3].

From a mechanistic standpoint, CPS are intelligent, integrated systems. They use sensor networks and on-board computing to monitor the physical environment. These systems can evaluate their surroundings and make human-assisted decisions. However, the Internet of Things is totally automated and does not require human participation.

In terms of technology, CPS is an intelligent system that integrates physical, networking, and computing capabilities. In contrast, the Internet of Things (IoT) refers to an increasing number of physical devices that are connected to the Internet.

In terms of reliability, faults in a CPS might have catastrophic implications, hence cyber-physical systems must be exceedingly dependable and secure. IoT devices, on the other hand, despite their importance, do not follow the same security protocols.

Given the distinctions between CPS and IoT, the scope of applicability varies. CPS combines actuators or sensors with networking technology. In this way, sensors and actuators incorporate human interaction into the feedback loop. IoT is a technology that allows diverse items to connect, interact, and exchange data. The data can then be processed and evaluated to yield valuable results.

1.3.1.2 Data Management in Smart Cities

Data management is the process of collecting, processing, and distributing data. Data acquisition is essentially the collecting of information from resources. Data capture employs a variety of technologies, including sensor networks, mobile ad hoc networks (MANET), drones, vehicular ad hoc networks (VANET), IoT, social networks, 5G, and others. Data processing is the finding of patterns within data. The most essential techniques include machine learning, deep learning, and real-time analytics.

Data distribution is the final phase in the smart city data management process. Methods of data dissemination include direct access, push, publish/subscribe services, and opportunistic routing.

Other writers [5] categorise data management activities into four phases:

1. data discovery and collecting,
2. data fusion, processing, and aggregation
3. data utilization

4. service delivery

Data traffic analysis can be added as a technology in the category of data management. Improving quality of experience and quality of service is the goal of data traffic analysis. In order to evaluate the performance of a communication system and avoid wasting energy, accurate modeling of traffic in smart cities and the IoT environment is necessary.

1.3.1.3 Blockchain Technology

The blockchain [7] is a distributed public ledger composed of peer-to-peer nodes. It is well-known due to the popularity of the Bitcoin cryptocurrency exchange platform. The immutable public ledger allows any transaction to be recorded securely and anonymously. To undermine the blockchain's security, a malevolent attacker would need to obtain more than 51% of the blockchain network's total processing power [8].

Blockchain has been utilised for a variety of purposes, including the execution of financial transactions, cryptocurrency, and smart contracts. Smart contracts are self-executing programmes, similar to Ethereum, that may be used to encapsulate specified rules in the same manner that regular contracts do. Blockchain technology shows significant potential for smart city applications. It can also be utilised to address specific security and privacy concerns in smart cities [9].

It is quite challenging to share data with all parties engaged in an IoT network while maintaining their security. Blockchain technology, given its features, can be used to protect apps in an IoT environment. The fundamental elements of security in blockchain include distributed characteristics, traceability, durability, certainty, tamper resistance, reliability, and data origin integration.

The data structure of blockchain, which takes the form of a distributed ledger employing public-key cryptography, allows for secure peer-to-peer transactions. Each link in the chain includes a reference to the hash of the previous link. However, the adoption of blockchain technology is hampered by its inability to scale as the number of IoT devices grows. As a result, transaction conflicts are expected to occur as latency increases.

A common example is a blockchain-based marketplace that creates a decentralized market for specific products or resources. Blockchain technology makes the market completely traceable and transparent for all players; every task execution and accompanying transaction is permanently recorded on blockchain nodes. Market mechanisms consider the reputation of resource providers and their resources. The reputation of resource suppliers is based on previous transactions and the quality of services provided. The blockchain-based marketplace promotes open and fair competition among various resource providers. One of the primary goals of this blockchain-based marketplace example is to increase confidence among all participants.

1.3.1.4 Cloud Computing

Control centres for smart city applications require powerful computing resources to interpret data and make sound decisions. However, adopting cloud-based storage and computation puts sensitive data at risk. This is because cloud servers are unreliable and outside the users' or organisations' control. Encrypted data should be transferred or stored on cloud servers rather than being stored in plain text and exposed to untrustworthy servers. On the other side, this raises the question of how smart city applications handle and analyse encrypted data. To address this issue, new encryption algorithms are being developed, including homomorphic and functional encryption schemes [10] [11].

Homomorphic encryption is an example of an asymmetric cryptosystem. These are basically algebraic algorithms that enable arbitrary treatments to be done to previously encrypted material without revealing it or gaining access to the private key. In this scenario, an encryption method is said to be homomorphic if the decrypted result of a treatment performed to encrypted data is equal to the result of the same treatment applied to unencrypted data.

1.3.1.5 Machine Learning

Several detailed research have been conducted on machine learning, AI, and data analytics for smart cities and IoT [12] [13] [14] [15] [16]. Here, we attempt to explain the fundamental concepts of this technology. Machine learning is a collection of ML algorithms that can learn without being explicitly programmed. ML attempts to create self-learning computer algorithms that can adapt to new data. These programmes alter their activities based on the data patterns discovered by ML algorithms. ML is typically divided into three categories: supervised learning, unsupervised learning, and reinforcement learning.

- A supervised learning algorithm uses labeled data, i.e. input data and corresponding output as labels, and infers models on a portion of the data known as the training set. Subsequently, it estimates the output for the newly added data by applying the models learned from the training data,
- Unsupervised learning algorithms, on the other hand, do not rely on labeled data and discover hidden patterns in the data. Decision trees, k-nearest neighbors, support vector machines and self-organizing maps are examples of supervised learning algorithms, while k-means, as a type of clustering algorithm, is an unsupervised method,
- • The use of basic classification and clustering algorithms is generally appropriate when analyzing simple models. For the analysis of more complex models, the use of neural networks is appropriate, as their performance is superior to other ML methods. Here the concept of deep learning enters the picture.

Deep learning is a type of ML that has been gaining popularity in both the academic and industrial communities in recent years. Deep learning is a set of ML algorithms designed to model high-level abstractions of data through linear and nonlinear transformations. At its core are neural networks, which consist of a set of neurons and edges that connect them. Each neuron is biased and each edge is weighted. A neural network is structured in such a way that it consists of an input layer, an output layer, and hidden layers in between. One of the drawbacks of neural networks is their scalability problem as the number of neurons increases.

ML techniques can be used for a variety of purposes in a smart city [13], [14]. They can be used either to optimize the performance of the network and the system as a whole, or to extract meaningful information from detected data. In the category of system optimization, they have been used to improve energy consumption, data routing and to predict sensor failures. As an example of the use of MLs to derive meaningful information from sensed data, they have been used in smart grids to transform historical electrical data into models and predict the risk of component failure so that maintenance work can be prioritized. Deep learning algorithms have been used with geospatial urban data to address different needs in smart cities. For example, to divide metropolitan areas according to residents' travel patterns, for traffic flow prediction and crowd density prediction in metropolitan areas, for electricity load forecasting, for smart water management networks.

1.4. Security and Privacy Challenges

Because the information gathered, stored, and shared in smart cities is sensitive, it is critical to take precautions against unauthorized access, disclosure, modification, and disruption of information. As a result, security and privacy needs must be addressed at the component layer, or application level for each smart city. Authentication and authorization systems are critical for achieving these security and privacy needs. Authentication and secure communication protocols enable to meet specific security needs in IoT environments by confirming user identification. In the next sections, we look into the security and privacy issues that are unique to smart cities [17].

However, smart city applications have distinct characteristics that create obstacles and render typical solutions inefficient. They necessitate the development of security solutions specifically tailored to the requirements of smart city applications. These distinctive traits include the merging of cyber and physical environments, the utilisation of resource-constrained IoT devices, this is due to restrictions in capacity, storage, and processing that prevent the use of cutting-edge security and privacy protection techniques, such as the implementation of cryptographic algorithms, as well as the heterogeneity of hardware and software components. This can cause compatibility issues when merging various technologies and devices. [18]

1.4.1. Privacy

The sensitivity of information in smart cities is due to its personal nature and because it is collected from people's environment and reflects their lifestyle. No patient in a smart hospital wants his or her state of health to be divulged, there are cases where the identity and location of a user in an intelligent transport application should not be divulged, the lifestyle of residents in a smart home is considered as privacy. This includes their consumption of energy, gas, water, web browsing and even their periods of existence in the homes that are collected by the aggregation meters. Intelligent transport applications include a navigation service that provides information on the current state of traffic (location), delays, destination, etc., which poses a threat to user privacy [19].

Some solutions are already available and can be used, such as encryption and anonymization mechanisms. These mechanisms can protect the confidentiality of data processed during detection. For the confidentiality of the network part of the IoT architecture, we find VPN (virtual private networks), TLS (transport layer security), DNSSEC (DNS security extensions) to ensure the authenticity and integrity of data origin; onion routing to mask the source of an IP (Internet protocol) packet, and PIR (private information retrieval).

1.4.2. Safe Interoperability

In smart cities, multiple stakeholders come together and form collaborations to deliver services to citizens. Each party would be represented as an individual domain with its own set of information resources and services, as well as its own security and privacy requirements. However, taking an example of an air pollution monitoring scenario where several stakeholders are involved, collaboration is paramount. These heterogeneous domains need to interact to achieve their service delivery objectives through the sharing of sensitive information. What's more, it's not just operators, the IoT is also involved, as objects can belong to different domains, such as smart sensors from the WSN domain, smart traffic signals from the smart traffic management domain and smart home alarms from the smart home domain [20].

The problem preventing organizations and stakeholders from sharing information and IT resources lies in guaranteeing security and confidentiality during inter-operation. Security is an absolute requirement in such inter-operation environments, due to the high possibility of malicious parties and the lack of trust between participating entities. A first solution is to enable privacy-friendly inter-domain access through integrated access control policies and appropriate mechanisms.

1.4.3. Insider Attacks

Smart city applications are also exposed to attacks that can be executed by potential adversary insiders such as employers and contractors, or by a component of the supply chain

or multi-domain environment. The challenge is that insiders perform actions within the organization's trusted network, and their actions are not subject to the same thorough security checks as external access. In addition, it may be easier for insiders to bypass security controls as they have more in-depth knowledge and training of the organization's network configurations, policies and security mechanisms deployed and implemented. In addition, data leaks outside the organization by insiders cannot be detected by anomaly detection systems or firewalls, as data is generally disclosed through legitimate channels.

The main challenge for an organization faced with insider threats is to authorize users with the right set of privileges, as insufficient privileges prevent employees from performing their tasks, while excessive privileges can be abused by malicious or inadvertent users [17].

1.4.4. Trust Management

In smart cities, trust is usually approached from an IoT perspective, where data collected by sensors is transmitted over the network, analyzed in real time and used for actuation. If the reliability of the data at any of these phases is not met, this signals a possible compromise and can prevent the proper functioning of the IoT devices that are part of a smart city. An adversary can usually carry out attacks against the communication protocol in order to disrupt the overall operation of the network. However, these attacks are usually dealt with by intrusion detection technology.

The authors in [18] give the unique characteristics of the IoT that pose problems with regard to trust assurance.

- The vulnerable, error-prone transmission medium: The radio frequency (RF) signal is typically used as the transmission medium in many IoT applications. The open nature of the RF signal makes it highly vulnerable to signal propagation errors and intentional eavesdropping or manipulation,
- IoT sensor data cannot be trusted: IoT applications typically offer sensor redundancy to improve data availability. However, reliable sensors, faulty sensors or even compromised sensors can generate different readings for the same observed object. Therefore, trust must be inferred from this inconsistent data, and we need to detect and manage these faulty and compromised IoT nodes,
- Constantly changing network topology: In IoT, given that nodes can be constantly on the move, network formation and topology change considerably over time, complicating the issue of data reliability

Three main trust-relatted attacks [18], Bad-mouth attack (BMA), Ballot-stuffing attack (BSA) and On-and-off attack (OA). These attacks can be handled by a solution based on historical data and network transactions. Several trust solutions based on the layered

architecture of the IoT are being developed [21], [22]. Other approaches adopt reputation, fuzzy techniques, a social network-based approach and historical behavior-based approaches to trust management [23].

1.5. IoT vs Samrt City Applications

IoT applications are a subset of the applications found in a smart city. Smart cities are made up of several technologies, so their applications are rather combinations of certain technologies to serve a specific purpose. However, an IoT application cannot be dissociated from a smart city.

Bhawana Rudra in [24] classifies smart city applications, including IoT, into seven categories Figure 1.2 Although, several classifications of smart city applications exist in the literature. However, this one [24] is more general, encompassing almost all activities and needs of all stakeholders:

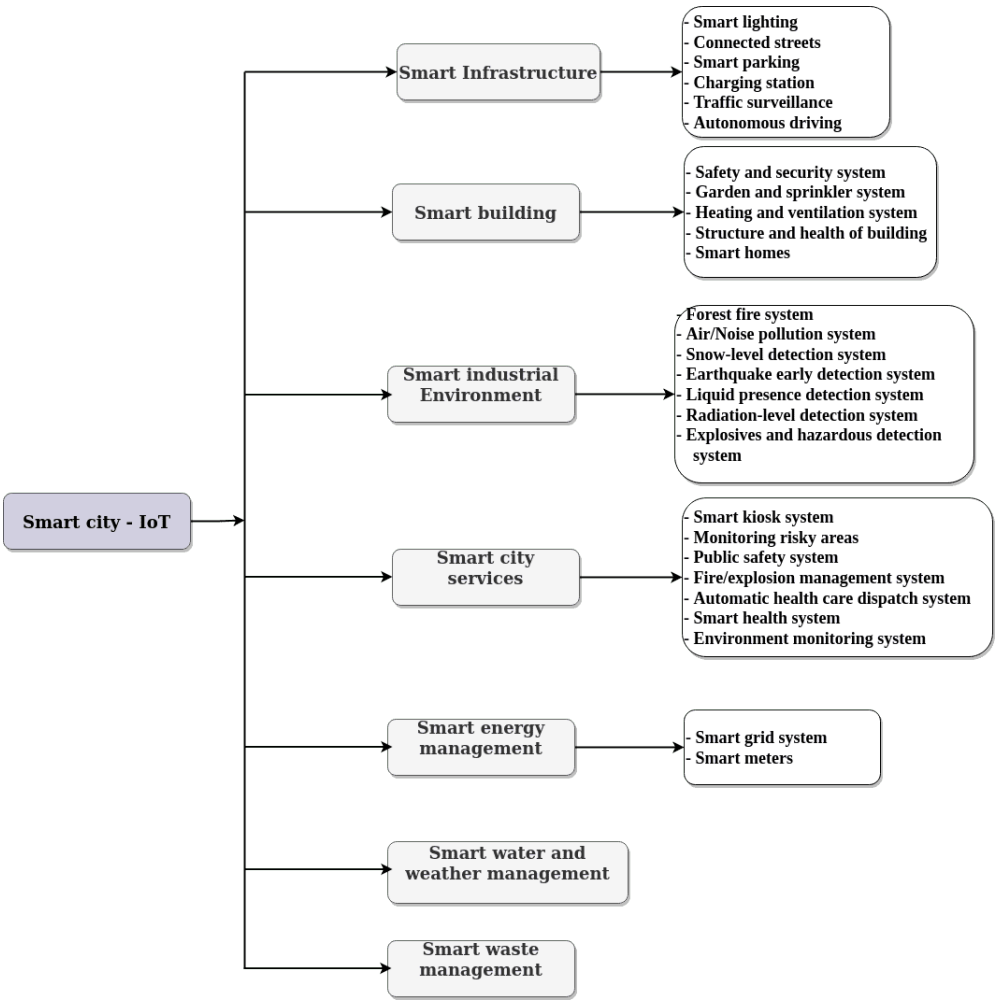

Fig. 1.2. Samrt City: IoT applications

1.5.1. Smart infrastructure

Applications in this category include [25]:

- Smart lighting: This saves energy both indoors and out. The idea is for the light to come on less when there's no one around, and to come on more intensely when it detects someone on its path. To control the light intensity of lighting units, sensors such as light sensors and motion sensors should be used. This will help reduce the energy consumption of lighting systems and exploit daylight by reducing light intensity in unoccupied areas. Motion sensors will detect the traffic situation, weather conditions and time of day, and depending on the presence of movement, the operation of the lights will be controlled,
- Connected streets: The ability to acquire data and transmit information in a smart city, particularly on traffic, roadworks, etc., enables resources to be used efficiently and public transport to be improved. Display panels and traffic lights will make it possible to control traffic and energy consumption using acquired and processed information,
- Smart parking: IoT technology is used to find vacant parking spaces in the parking lot. Parking information is collected by the sensor deployed in the parking space and transmitted to the server. The information is then transmitted to drivers to make a decision using different platforms such as cell phones or billboards.

1.5.2. Smart building and properties

The main uses for IoT in buildings are [25]:

- Safety and security systems: IoT will help implement security and assure the public by using biometrics, surveillance camera alarms and not allowing unauthorized people into the locality or homes. It can even detect and block access to the perimeter of restricted properties,
- Smart garden: Sprinklers connected to IoT and cloud technologies can be used to water the plant as needed. Sensors for soil moisture, fertilizer levels, atmospheric pressure and, depending on weather conditions, sprinklers (actuators) can program plant watering. Even robotic mowers can be used to stop excessive grass growth,
- Smart heating: A network of sensors can be used to monitor building temperature, pressure, humidity, etc., to ensure proper heating and ventilation, collect information and optimize systems to improve efficiency and performance. This system can be used to ensure proper heating and ventilation. Collecting information and therefore optimizing systems will improve efficiency and performance,

- Smart homes: IoT offers many applications for smart homes, such as smart TVs, security systems, fire detection, light control and ambient temperature monitoring using a variety of sensors. Collecting data from sensors and storing them in a database, provides demand-response methods for warning users and predicting possible risks. These sensors can be motion, physical, chemical, leakage/moisture, remote, biosensors, etc. The sensors detect and send data to the central controller in the home to make the best decision. Smart homes can be connected to the neighborhood to create an intelligent community.

1.5.3. Smart industrial environment

Industry has benefited from the vast majority of IoT applications. Also known, in the context of this study, as industrial internet of things (IIoT) that derives from industry 4.0, the aim is to use smart sensors and actuators to improve manufacturing and industrial processes. IIoT harnesses the data that machines produced in industrial environments, analyzing it in real time to make faster, more accurate decisions [25].

The combination of information technology (IT) and operational technology (OT) makes IIoT a more ideal approach to achieving production performance, while reducing operating costs. Through IIoT, new generations of smart factories are emerging, connecting all sensor-equipped devices to the Internet. This enables advanced visibility of activities thanks to real-time access to data. Cyber-physical system (CPS) technology, which uses intelligent embedded systems in production machines, is the fundamental essence of Industry 4.0. It combines with IoT to connect the real world of manufacturing with the virtual world. CPSs create smart factories by enabling an interactive industrial environment through the integration of networking, computing, and storage. In this way, smart products become increasingly identifiable and traceable. As a result, working environments become healthier and safer, while increasing productivity at lower cost [26].

This category includes fire detection by monitoring gas combustion, for example. Another example is monitoring air/noise pollution in areas where people are most numerous, in different places and at different times, and helping the municipality to put measures in place. This will also help residents to become more aware of the place and situation in which they live. Noise is perceived as noise pollution. Another type of application is the monitoring of snow levels and the prevention of landslides and avalanches, such as the condition of ski slopes in real time. Sensors monitor soil moisture, soil density and possible vibrations, as well as dangerous patterns in ground conditions.

1.5.4. Smart city services

This class includes 24/7 surveillance and analysis cameras, Wi-Fi services, digital signage for announcements. It even provides information on nearby events, stores, hotels, restaurants and more. It will provide visitors with a map for the additional data required

in cell phones. The risk zone monitoring application will be easy with the help of sensors in risk zones. It can send alerts in the event of accidents in neighboring areas, and send a message to avoid traffic temporarily in that particular area [25].

Another important application is the automatic dispatch of healthcare With the help of IoT technologies, medicines and drugs can be sent to patients, providing 24/7 healthcare. These technologies can also be used to call the ambulance or retrieve the patient in an emergency. A wireless body area network (WBAN) can be used to monitor patients in any location. The device inserted in the body will communicate with available communication technologies such as ZigBee, 6LowPAN and CoAP. Sensors placed around the city keep a watchful eye on the environment, monitoring the electromagnetic field, temperature, toxic gases in the air, any type of combustion gas in the air that could detect a fire, etc

1.5.5. Smart energy management

It includes the smart grid, which is a digital monitoring system that routes gas or electricity to the right destinations from the source. This technology can be applied to both residential and industrial areas. It uses intelligent, autonomous controllers for data management and maintains two-way communication. This application enables cost-effective energy distribution and transmission. This class also includes the smart meter application, which measures real-time information in the industrial or residential sectors. Energy consumption can be monitored, reports generated and even dashboards consulted via the Internet.

1.5.6. Smart water and weather management

IoT applications for water distribution vastly improve on the usual inadequate methods and serve to save this precious resource , especially when there are leaking pipes and other related problems. Deploying sensors at appropriate locations enables damage to be monitored and information sent to management. Water quality and quantity can be known from lakes, reservoirs, above ground pipes and a storage tank using IoT sensors. Wearable sensors can be deployed to monitor tap water, chemical leaks in water sources can be identified. Weather applications are enhanced with sensors, rainfall can be recorded and analyzed for irrigation management, reducing excessive water use and wastewater management. Localities can prepare to control raw sewage during storms. The weather system uses a variety of sensors to detect temperature, rain, solar radiation and wind speed to improve smart city efficiency.

1.5.7. Smart waste management

The intelligent waste management system is widely used and has been a great help to municipalities. Sensors attached to waste containers will detect the level of waste and

send an alert to the municipality for waste collection. This can improve recycling of collected waste and design intelligent itineraries for collection vehicles, saving time and unnecessary energy consumption [27].

1.6. Worldwide use-cases

1.6.1. Introduction

It is clear that the use of IoT makes society, be it municipalities or private or public investors, more profitable and economical day after day. Because IoT will be the main source of big data following the massive deployments of these devices and all kinds of connected objects. Several cities have become models through the involvement of their communities in the deployment of IoT applications and their efforts to improve the ecosystem.

As an example of the innovation of smart IoT applications implemented. The city of Barcelona, which implemented sensor technologies to assess traffic flow, and subsequently new bus networks and intelligent traffic management. Stockholm, where a fiber optic network covers the entire city. Santa Cruz, where information on criminal acts is analyzed using networks to help police officers. Songdo, Korea, where fully automated buildings submerge, intelligent street lighting, etc. Fujisawa, Japan, where carbon reduction has reached 70% through the implementation of an air monitoring system. Norfolk, England, where intelligent delivery services, data collection and systems analysis for the municipality. The smart cities that follow are just some examples among others that we cannot all mention [25].

1.6.2. London, England

London is one of Europe's smartest cities. After securing citywide 5G connectivity in 2017, faster, highspeed internet connections are being established, from an all-fiber network in 2021. Following this solid infrastructure, smart applications have emerged the city. Charging stations for electric vehicles, following the example of other cities in Europe and the United States. A driverless rapid transit system linking the city to the airport. Smart meters deployed throughout the city and surrounding area on demand.

1.6.3. Zurich, Switzerland

Since 2017, the city has reduced the electrical energy consumption of public lighting by 70%. This is the result of deploying intelligent street lamps that light up according to traffic density. By equipping these street lighting poles with other smart devices, they can charge electric cars, collect environmental data, measure traffic flow and even provide public Wi-Fi. With more smart objects, they can also help visitors locate free parking

spaces and send an alert when a garbage container is full. In addition to street lamps, the city has equipped several buildings exclusively with renewable energies under the "Green City" project. The city has set up an IoT network that monitors air quality and water levels. Interoperability with city agencies to improve police services by responding faster to threats, using mobility management devices. With the "Zürimobil" application, the city can provide real-time information on traffic and routes.

1.6.4. Taipei City, Taiwan

The city has established a robust digital and physical infrastructure, with the creation in 2016 of the "Taipei Smart City Project Management Office" to facilitate collaboration between private and public sector investors on smart city projects. In 2021, Taipei became the second smart city in Asia and fourth worldwide in the IMD Smart City Index. The major problem of the city of Taipei is the polluted air quality. This has prompted the city to draft a program to monitor air quality in the city, deploying sensors sending automated messages and alerts on traffic routes to warn citizens and redirect traffic into relatively clean areas. However, the fluidity of road traffic is ensured by an AI-based traffic lights monitoring system while reducing areas of concentration of air pollution. The city also uses a real-time smart waste management system using a digital map that informs waste collectors when the containers are full.

1.6.5. New York City, USA

Due to the city's densely populated area, IoT applications are focused on improving the services offered to citizens. By 2020, the wireless infrastructure network is significantly improved. This has led to the innovation of a pilot program of connected vehicles, for more smooth and safer traffic. Another smart system in the city is the automatic reading of meters that helps reduce water consumption by warning customers in case of an abnormality in the consummation. This mechanism has already saved hundreds of millions of dollars for the city and its citizens. Other applications are emerging in the city, have become standard in the field, such as LED indoor farming management, air quality monitoring and traffic flow, reuse of telephone cabins such as Wi-Fi and online charging stations.

1.6.6. Barcelona, Spain

Barcelona has been using smart city technology since 2015 following the transformation of its network and the development of its 5G infrastructure. This city with a futuristic vision, as a tourist area, autonomous 5G buses run through the city; live video streams enhanced by AI to reduce crime; network capacity management in the most popular tourist areas. Waste management, Smart Street lights, public transport and parking spaces are

standard applications like any other smart city. This city thrives by deploying AI-powered drones that ensure security while ensuring confidentiality. Let's not forget that free internet access is available throughout the city with thousands of Wi-Fi access points.

1.6.7. Busan, South Korea

The government developed the cloud infrastructure because of its good communication with objects. The aim is to connect the government, mobile application center to provide project and meeting rooms, consultancy centers for startups, access municipal data from any location. It enables developers to access the smart city, as a service-providing platform, to develop intelligent applications.

1.6.8. Jiujiang City, China

Among the projects carried out by this city, the installation of tens of thousands of video capture points for the video surveillance system, intelligent transport, the emergency command system and the intelligent urban management system, and many more have been developed and deployed. The construction of a broadband fiber optic network enables full coverage of urbanization areas, with support for new buildings and residential neighborhoods right from the design stage. Wireless coverage of the entire city, providing multiple access points on a large.

1.7. Conclusion

It's clear that IoT has permeated our daily lives, and promises more and smarter cities in the future. Not only does it enable resources to be rationalized and optimized more efficiently, it also improves citizens' quality of life. All this has become true thanks to the interactivity of the services provided by the city and other key technologies such as Blockchain, CPS, ML, cloud computing and the exploitation of Big Data. Despite the time and effort required to implement IoT in all urban areas, the related applications are highly profitable. Indeed, this technology has opened up a favorable market for startups active in the field of IoT for smart cities. These small companies, investors and governments have exploded IoT applications and given rise to model smart cities around the world.

The potential of the IoT can still be exploited to develop new applications for the benefit of society. It can enhance the role of information and communication technologies (ICT) in improving our quality of life. It can be harnessed for healthcare, transportation systems, environmental monitoring, personal and social aspects, smart cities, industrial control, and many more.

2. IOT TECHNOLOGIES

2.1. Introduction

IoT isn't just a technology, it's a term that covers a wide range of new techniques used in applications and services based on objects with computing and communication capabilities. It cannot be defined in terms of a communication protocol alone, nor can it be defined in terms of a single application or service [28].

Several definitions have been proposed, but organizations in the field such as the ITU define IoT as an infrastructure that will connect physical and virtual devices [29]. The IETF defines IoT as the Internet that supports both TCP/IP and non-TCP/IP suites, with objects identified by unique addresses [30]. The IEEE defines it as a network that connects uniquely identifiable virtual and physical devices using existing or emerging communication protocols [31]. These objects are dynamically configurable and have interfaces that must be remotely accessible over the Internet.

Although there are many definitions of IoT, there are certain requirements that are common to all IoT solutions. So it's important to know and understand the components of a typical IoT solution. In its simplest form, an IoT system consists of three basic elements, devices, a communication channel and an application.

2.1.1. IoT Devices

Also called dispositifs, or objects, are sensors and actuators embedded in small, limited computers based on Advanced RIS Machines (ARM): A Reduced Instruction Set Computer (RISC) system-on-chip (SoC) and system-on-module (SoM) architectures. An SoC includes a central processing unit (CPU), memory, storage, interface ports and analog, digital and radio frequency (RF) signal processing. It can also include a graphics processing unit (GPU) and support multiple peripherals. An SoM is a board that typically includes an SoC and other discrete chips to provide additional functionality. Devices interact with elements of the physical environment, called assets, through sensing and actuation. Sensing deals with temperature, humidity, lighting and stock levels, while actuation modifies the physical state of an entity, such as turning lights on and off.

1. **Sensors**: Sensors are logic devices that detect elements in the physical environment by sampling them and generating data. Sensors can be classified according to their size, from 1 nm up to a millimeter. They can be classified according to whether they interact with the environment passively or actively. Depending on the complexity of the embedded processor, a sensor can perform local processing that suppresses redundancy in a controlled way. Source coding can also be performed

at sensor level, where data is converted into information that can be transmitted at lower rates, reducing channel bandwidth requirements and improving power consumption. Battery life can be extended by means of duty cycles where devices go into "sleep", dramatically reducing power consumption at predefined intervals by supporting only wake-up interruptions and notifications. To minimize network throughput and preserve the energy consumption of all devices, it is preferable that duty cycles are coordinated across the entire network.

2. **Actuators and controllers** : Actuators are also logic devices that effect an external change of an asset in the physical environment. Actuation is generally linked to detection by feedback mechanisms associated with the information-knowledge transformation. This transformation, which takes place at the level of an application that analyzes the readings taken by input sensors, generates output commands that are transmitted to the device for actuation. Since actuation and detection are linked, a physical device can have both a logic actuator and a logic sensor. The presence of an actuator alone is much less common. Controllers, on the other hand, are logic devices that effect an internal change in the physical device to facilitate sensing or actuation. In most cases, controllers are deployed with sensors and actuators as logic devices on the same physical device.

3. **Gateways** : Gateways are logic devices that act as an interface between access IoT devices (sensors, actuators and controllers) and central applications. Core applications rely on analytics to make real-time decisions. Gateways are a little more advanced, requiring greater computational complexity to support multiple sensors, actuators and controllers simultaneously, which in turn requires more powerful and resourceful embedded processors that are powered by power lines. Gateways sit at the boundary between access and core, and are therefore edge devices. Nevertheless, networks can sometimes rely on sensors and actuators which, in turn, become temporary gateways that aggregate and transmit packets to core applications.

2.1.2. IoT Communication Channel

this is the medium that ensures connectivity between objects and applications. Communication between objects and an application is called multipoint-to-point (M2P), because it is from several devices to a single application. The channel is a very important component in the IoT system because of the constraints linked to the objects. Indeed, power constraints that limit transmission rates and spatial spans require several protocol stacks. Conversion between these different protocols is performed by small integrated devices called gateways.

Limiting factors such as transmit power, channel bandwidth and deployment cost favor one solution over another depending on the needs and requirements of a given scenario. An important consideration is that a transmitted signal is affected by chan-

nel noise, interference, and fading due to multipath signal propagation. By the time the signal reaches the receiver, it has been attenuated to a certain level of signal-to-noise ratio (SNR). Since the channel capacity theorem states that the maximum achievable data rate is a direct function of the SNR, higher SNR generally means higher data rates. It should be noted that the transmission rate is error free if the channel coding mechanism used is adequate. In IoT networks, this can be difficult. In order to conserve battery life, low signal power and low SNR are generally present, resulting in low transmission rates.

2.1.3. IoT Application

The final component, the application, processes information from devices and other inputs to generate knowledge that can be used to make decisions, either in an automated way using analytics performed by machine learning, signal processing and other techniques, or in a manual way with human interaction that usually involves data visualization. In general, for most IoT solutions, there is a transformation of data into knowledge.

Its aim is to convert the information generated by the sensor into knowledge by means of a simple threshold comparison mechanism that triggers an alarm or action. This transformation, which takes place within the application, is known as information-to-knowledge conversion. In general, the transformation of data into information takes place at the device level, while the transformation of information into knowledge is carried out by the application.

2.2. IoT Networking

There are several standard and non-standard protocols for WPANs and LPWANs that more or less meet the needs for IoT services. However, there are IoT requirements and limitations these technologies must overcome, such as power consumption, throughput, range, robustness, etc. Potential solutions include proprietary and unlicensed ISM band technologies, IEEE 802.15.4, Sigfox, LoRa, versus cellular network solutions such as LTE-A and NB-IoT. The choice of one of these technologies is not obvious. Therefor, a fairly detailed comparative study of the performance of certain WPAN and LPWAN technologies, particularly in terms of the physical layer and data link, is required.

While IoT depends on several categories of networking, the two primary types are WPAN and LPWAN. Note that WPANs are often referred to as low-power WPANs (LoWPANs), especially in the context of IoT. WPAN signal range is expressed in meters, while LPWAN range is expressed in kilometers. Similarly, WPAN data rate is expressed in megabits per second (Mbps), while LPWAN data rate is expressed in kilobits per second (Kbps). Although IoT networks are expected to provide end-to-end IP connectivity, partial IP connectivity is also possible, in both cases. This is particularly true in LPWAN scenarios, because of the very low throughput, a gateway provides the interface between

the proprietary physical, data link and network layers and the IP backbone. On the other hand, WPAN scenarios natively support end-to-end IP connectivity, and gateways only handle transformations of the physical and data link layers.

2.2.1. Architecture

The smart city connects physical, social and information communication infrastructures and helps to collect city-related data. To process and store informations, companies have adopted cloud-based platforms and started to develop low-cost smart sensors, driving the growth of the IoT. IoT deployment requires common standards to make devices work. The International Telecommunications Union (ITU), the Institute of Electrical and Electronics Engineering (IEEE) and the IETF specify certain requirements for machine interface-oriented devices for standardization, such as IEEE 802.15.4 for the link layer, IPv6 on Low-Power Wireless Personal Area Networks (6LowPAN) for the network layer and IPv6 Routing Protocol (RPL) for low-power networks, Constrained Application Protocol (CoAP) to provide (HTTP) GET for application-level state querying and modification [32].

From a functional point of view, IoT networks are packet-switched networks, made up of two types of components

1. endpoints or hosts (things), which are the source and/or destination of messages,
2. Geteway, which help propagate messages throughout the network.

Both components form communication systems with transmitters and receivers connected to channels via links. In the context of IoT, hosts (things) are typically sensors, actuators, controllers and devices in general, but also applications such as those making complex decisions.

A generalized IoT architecture that groups almost all the technologies Figure 2.1 given in [7]. In order to limit energy consumption and extend network lifetime, objects do not have a direct connection to the Internet, except for a few technologies such as NB-IoT. These exeptions can be powered by renewable energy or connected to external energy sources. Gateways are more powerful devices, generally without energy constraints, whose function is to receive wireless communications from objects and transmit messages to the platform via the Internet. The trade-off between energy consumption, expected network lifetime and connection quality (in terms of bandwidth, latency and coverage) is specific to each application.

2.2.2. Constraints

Links can be wireless when associated with free propagation, or wired when associated with guided propagation. Guided propagation generally involves (1) twisted copper con-

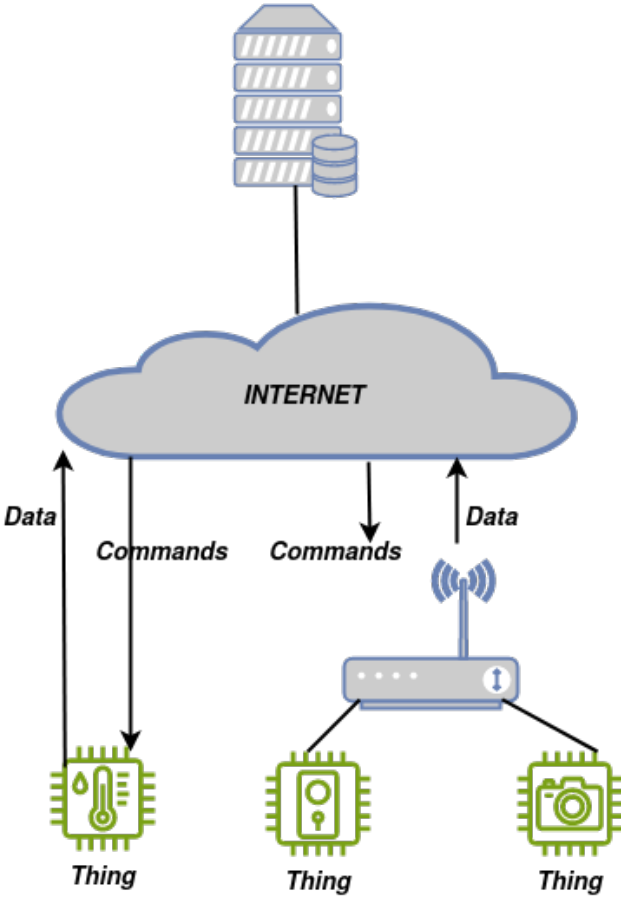

Fig. 2.1. General IoT architecture

ductors to attenuate electromagnetic interference (EMI), (2) coaxial cables made up of inner and outer conductors, separated by a dielectric insulating material offering better EMI immunity and higher transmission rates, and (3) optical fibers which are EMI-free and support much higher transmission rates.

On the other hand, free propagation occurs between corresponding antennas in the earth's atmosphere, underwater and in free space. In the IoT context, the choice between a wireless and a wired solution is linked to the cost and time required to deploy the devices. More specifically, to support a massive number of devices, wired solutions generally require huge infrastructure changes that are too costly and take too long to deploy. Wireless architectures with battery-powered devices are the most common type of IoT deployment. On the other hand, wired scenarios that take advantage of pre-existing cabling and repurpose it for communications are also widespread.

Depending on the needs and requirements of a given scenario, limiting factors such as transmission power, channel bandwidth and deployment costs favor one solution over another. An important consideration is that a transmitted signal is affected by channel noise, interference and fading due to multipath signal propagation. By the time the signal reaches the receiver, it has been attenuated so that it is affected by a specific level of signal-to-noise ratio (SNR). Since the channel capacity theorem states that the maximum

achievable transmission rate is a direct function of the SNR, a higher SNR generally means a higher transmission rate. Generally speaking, the key challenges that need to be addressed and resolved by any IoT technology are:

- **Scalability**: In a scenario where device density will be very high. IoT networks must support modulation and media access schemes that enable this wireless environment, and dynamically adapt network parameters to be most efficient when faced with frequent network overloads and packet collisions.
- **Cost**: Radio chips should be as inexpensive as possible, to help vendors gain market advantage and encourage investors and stakeholders to massively deploy IoT applications. Moreover, subscription costs to access the network must also be as low as possible.
- **Battery life**: IoT devices will generally run on battery power, and long battery life is necessary to reduce network maintenance costs. Any manufacturer's target for battery life is 5 to 10 years. This figure varies according to the number of detections, reports and transmission frequency.
- **Computing power**: IoT devices are expected to have very basic processors that consume less energy. This restriction also limits the complexity of the network protocols and modulation that must be used by these devices.
- **Deep indoor coverage**: A large number of devices are deployed inside buildings and structures. IoT devices are challenged to communicate even in the face of heavy shading, especially for critical applications where message transmission success rates are very strict.
- **Delay sensitivity**: Many applications where data traffic is latency-critical and cannot tolerate delays, such as alarm applications, suggest that a delay of 4 seconds is appropriate for the UL measured between the triggering event and the moment when the packet is ready to be transmitted to the network [28].
- **Network architecture**: The Iot technology should outline a core network architecture, a security framework and a radio access network interface, as well as the associated protocol stacks [28].

Note that throughput and persistent connection are not considered crucial to IoT device performance, as IoT devices are not expected to support high throughput. Instead, data should be shared infrequently and in small quantities. As well, IoT devices are not always and constantly active. The majority will be in standby or sleep mode to reduce battery consumption.

2.2.3. Topology

There are two main families of IoT networks: wireless personal area networks (WPANs) and low-power wide-area networks (LPWANs). Although both types of family try to preserve battery life, each prioritizes a few factors over the others, such as signal coverage and transmission rate.

2.2.3.1 WPAN

WPANs represent a large family of technologies that enable coverage of no more than a few hundred meters. The transmission rates supported by these technologies are in the Kbps range, and are therefore fast enough to support IPv6 natively or with an additional adaptation layer. In the following, we will discuss a list of these technologies.

- IEEE 802.15.3 features very high transmission rates, up to 55 Mbps, with 64-QAM modulated signals on the 2.4 GHz ISM band. They are deployed in the form of piconets, with each piconet managed by a piconet coordinator (PNC) that supports a network of devices synchronized by means of beacons.
- ITU-T G.9959 is another technology, derived from Z-Wave technology, which supports very low transmission rates. This standard is deployed in mesh topologies that enable transmission from one endpoint to another, relying on intermediate nodes that act as repeaters. This reduces transmission power requirements by extending network coverage, but increases overall latency.
- DECTULE stands for Digital Enhanced Cordless Telecommunications Ultra Low Energy. This technology is managed by the ULE Alliance. It aims to provide a long coverage range of 60 and 500 meters for indoor and outdoor scenarios respectively, medium transmission rates, very low power consumption combined with reduced duty cycles resulting in battery life in excess of five years and low latency. The topology is a star with hop links between devices to a base station that acts as the IoT gateway. The network can support up to 400 devices.
- Near Field Communication (NFC) systems. Devices communicate with each other via contactless transactions. NFC also enables efficient, convenient and easy access to digital content. NFC is based on several contactless card mechanisms, and is therefore backwards compatible with existing infrastructure. NFC devices support three modes of operation: (1) NFC emulation, (2) NFC read/write, and (3) NFC peer-to-peer, which enables devices to communicate with each other. It is this NFC peer-to-peer mode that enables IPv6 connectivity in the IoT context.

2.2.3.2 LPWAN

WPAN technologies are relatively powerful enough to provide transmission rates that natively support IPv6. However, the range of direct transmission is generally quite short, rarely exceeding a few hundred meters. LPWAN technologies attempt to increase device coverage, but with a lower SNR that further reduces transmission rates and MTU sizes. These limitations prevent these devices from fully supporting IPv6, so most LPWAN mechanisms are hybrid technologies with proprietary access network stacks that rely on IoT gateways to enable IP support.

Figure 2.2 [3] shows the relationship between throughput and coverage of different IoT technologies. Conventional cellular technologies like 5G offer high throughput and coverage, but their energy consumption is not efficient for IoT. Likewise, IEEE 802.11-derived technologies, most of which consume too much power to be effective in IoT environments. IoT WPAN systems such as IEEE 802.15.4 and BLE are energy efficient, but have both low throughput and very limited coverage. LPWAN technologies complement WPAN by improving range while minimizing power consumption to provide years of battery life. LPWAN devices typically transmit very small packets only a few times per hour over long distances.

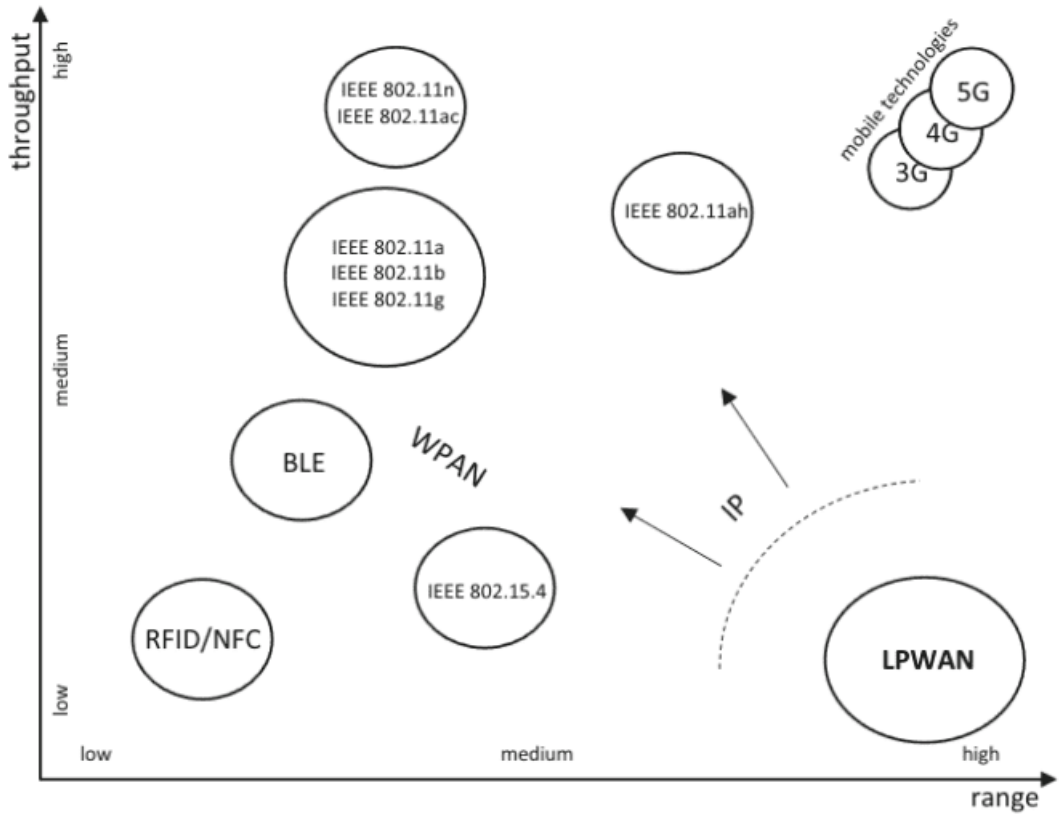

Fig. 2.2. IoT coverage vs throughput

Several performance factors characterize an LPWAN technology to be suitable for IoT, namely

1. network topology,
2. device coverage,
3. battery life,
4. interference resistance,
5. node density,
6. security,
7. one-way versus two-way communication,
8. the nature of the applications.

The following list presents several leading LPWAN technologies that are relevant to IoT.

- SigFox is a low-energy technology for wireless communication. The data carried is small, with coverage of up to 50 km, in a star-shaped network topology. SigFox uses Ultra Narrow Band (UNB) technology designed to handle low data transfer speeds, from 10 to 1,000 bps, and can operate on a small battery [33].
- D7AP is an open source protocol stack for LPWAN communications. Its physical and link layers are derived from active RFID (as opposed to passive RFID). The D7AP standard was originally designed for military purposes, with multi-year battery life and support for low-latency, long-range wireless mobility. Initially designed for asset tracking, it has been reoriented towards location-based services associated with smart cards and device tracking. As an RFID mechanism, it complements traditional short-range NFC technologies, enabling devices to communicate with each other.
- NB-Fi is an open, full-stack protocol that forms the basis of a commercial turnkey LPWAN solution. Its aim is to provide robust, reliable interaction between devices and base stations acting as traditional IoT gateways. NB-Fi offers long battery life combined with low hardware cost. In addition, NB-FI attempts to reduce deployment costs and times by simplifying the network topology. Typical transmission ranges are around 10 km and 30 km for urban and rural environments respectively.
- IQRF is an open LPWAN framework including devices, gateways and applications used in scenarios ranging from telemetry and industrial control to home and building automation. It's a protocol based on transmission in the 433 MHz and 915/868 MHz ISM bands, with GFSK modulation it achieves transmission rates of up to 20 Kbps with 64-byte frames and 500-meter coverage.

- RPMA is a media access scheme that forms the basis for robust LPWAN technology. RPMA operates only on the 2.4 GHz ISM band, as this ISM band is less restrictive and does not impose duty cycle limits which, in turn, limit transmission rates. The available 2.4 GHz spectrum is divided into 1 MHz channels that can be grouped together to support different deployments [33].

- Telensa is a proprietary LPWAN technology that concentrates primarily on smart city applications, but does not support indoor communications. Millions of Telensa devices have been deployed in over several smart city networks worldwide. Although Telensa supports bidirectional traffic associated with both sensors and actuators. Telensa is not just a technology, but a framework for creating smart city applications via an API. It provides integration mechanisms with supporting services such as billing and metering systems [33].

- Sensor Network Over White Spaces (SNOW) is an experimental LPWAN technology based on transmission in the white space spectrum with modulation on unoccupied bands typically between 547 and 553 MHz. Typically, a base station determines the white space frequencies for devices by means of a database on the Internet. The available bandwidth is divided into subcarriers, and with a technique known as distributed OFDM, several transmitters can send traffic simultaneously. The frame size is 40 bytes, including a 28-byte header, enabling a nominal transmission rate of 50 Kbps. SNOW supports a star topology with a single base station acting as an IoT gateway with a transmission range of up to 1.5 km.

- Nwave is a commercial LPWAN solution for mobile devices. The physical layer provides UNB transmission on the 915/868 MHz ISM band. With a single-hop star topology, Nwave can cover up to 10 km in urban environments. Long range and low power consumption result in transmission rates of around 100 bps and a maximum device battery life of nine years. Nwave provides its own applications for collecting and analyzing sensor data in real time, enabling city planners to allocate resources.

- The IEEE 802.15.4k (TG4k) is a new standard for Low Energy Critical Infrastructure Monitoring (LECIM) applications. Its transmission is based on the 2.4 GHz, 915/868 MHz and 433 MHz ISM bands. This technique enhances the reach of IEEE 802.15.4 by dividing the spectrum into discrete channels with bandwidths ranging from 100 KHz to 1 MHz, and by using three different modulations that combine DSSS with BPSK, OQPSK or FSK. The appropriate scheme is chosen according to the device and communication constraints, and also by adjusting the spreading factor. IEEE 802.15.4k also introduces a FEC scheme based on convolutional codes. Its link layer provides MAC via CSMA/CA and ALOHA. This standard operates in a star topology with a nominal coverage of 3 km. Transmission rates of up to 50 Kbps are possible.

- The IEEE 802.15.4g (TG4g) has introduced a new Wireless Smart Utility Networks (Wi-SUN) standard aimed at smart metering applications. IEEE 802.15.4g aims to

correct the shortcomings of traditional IEEE 802.15.4 WPAN, which is heavily affected by interference and multipath fading, which reduce communication reliability. But also complex and costly multi-hop transmissions for long-distance communications. IEEE 802.15.4g modulation takes place in the 2.4 GHz and 915/868 MHz ISM bands and is supported by three different physical layers that offer a compromise between transmission rates and power consumption: (1) FSK combined with FEC, (2) DSSS with OQPSK and (3) OFDMA in scenarios affected by multipath fading. Although nominal transmission rates can range from 6.25 Kbps to 800 Kbps, the standard defines OFDMA as the default mandatory transmission mode with a transmission rate of 50 Kbps. The corresponding MTU size is also larger, without affecting the transmission delay. The maximum frame size is 1,500 bytes, enabling transmission of a complete IPv6 datagram on a single frame without fragmentation. The link layer can be configured to provide a MAC based on IEEE 802.15.4 or IEEE 802.15.4e. Typical signal coverage is around 10 km.

- EC-GSM-IoT was standardized in 3GPP Release 13. In parallel with LTE-M and NB-IoT, both based on LTE. This one is based on enhanced GPRS, known as 2.75G. This version increases coverage and reduces power consumption, operating on the GSM 850-900 MHz and 1800-1900 MHz bands. The channel bandwidth is 200 MHz, the same as for GSM networks, and the MAC is implemented using a combination of FDMA with TDMA and FDD. Its modulation provides transmission rates of between 70 Kbps and 240 Kbps, respectively. Latency is typically less than two seconds, lower than that of LTE-M and NB-IoT. What's more, EC-GSM-IoT is designed to provide coverage in locations with difficult radio conditions, such as indoor basements where many sensors are typically installed. Battery life is around ten years, security and confidentiality are guaranteed by mutual authentication, and existing mechanisms ensure confidentiality and encryption.

2.3. Popular IoT Technologies

In the previous sections, we introduced some examples of technologies classified as WPAN and LPWAN topologies.

The comparison made by S. Al-Sarawi et al. in [34] in 2017 between the communication protocols of the following technologies: 6LoWPAN, IEEE802.15.4, ZigBee, BLE, RFID, NFC, Z-Wave, SigFox and Cellular; does not include LoRa technology despite its popularity after three years of release. After studying the security, energy consumption, throughput and coverage of these technologies, he concludes that 6LoWPAN will be the protocol of the future, because it supports IPv6, adapts to all network topologies, has low energy consumption, low cost and its networks are scalable.

In the following, we will present detailed descriptions of the physical and link layers of some WPAN technologies such as IEEE 802.15.4, and of several LPWAN technologies

such as LoRa, NB-IoT and LTE-M. The advantages and limitations of each technology will enable us to argue, and then choose, the best technology Satisfying the requirements of the vast range of IoT applications.

2.3.1. 802.15.4

The IEEE 802.15.4 specification introduces a set of physical layer and link technologies for use in WPANs [35]. It is one of the preferred mechanisms for supporting ultra-low power consumption, and therefore long battery life. IEEE 802.15.4 also serves as the physical layer and link mechanism for standalone standards such as ZigBee, ISA 100.11a and WirelessHART, protocols that integrate M2M and CPS solutions. While ZigBee is based on profiles that target home automation and smart energy scenarios, WirelessHART and ISA 100.11a target industrial automation and control. These standards use IEEE 802.15.4 in combination with higher proprietary layers that do not generally enable native IP connectivity.

In most modern IoT scenarios, IEEE 802.15.4 is used in combination with IETF protocols to provide efficient end-to-end IPv6 connectivity.

As a general rule, limiting signal coverage and the amount of data transmitted reduces energy consumption, which in turn reduces transmission rates. This is further enhanced by the management of duty cycles when shutdown and standby modes are controlled.

2.3.1.1 Physical Layer

Two types of device are defined by the IEEE 802.15.4: (i) Full Function Device (FFD) with all possible functions, a PAN coordinator, a router or finally a device connected to a sensor (smallest possible function, called an end device). (ii) Reduced Function Device (RFD) a device with limited functions, designed for simple applications (signaling the status of a sensor, controlling the activation of an actuator). It is considered an end device.

To communicate on the same network, an FFD (at least) and RFDs must use the same physical channel among those defined according to the chosen frequency band. The FFD can talk to both RFDs and FFDs, while the RFD talks to an FFD only. The 2003 standard specifies 3 possible frequency bands, but others are also considered. The following Table 2.1 from [36] shows the main frequency bands allocated to certain regions in the IEEE 802.15.4 standard.

After defining 4 possible physical levels in 2006 (different modulation types), two new physical levels were added in 2007 (802.15.4a):

1. UWB: Direct-sequence ultra-wideband, in 3 regions: $<$ 1 GHz, between 3 and 5 GHz and between 6 and 10 GHz

2. CSS Chirp Spread Spectrum, allocated in the 2.4 GHz band

Countries	Frequencies	Channels	Throughput	Comment
worldwide	2.4 à 2.4835 GHz	16 channels of 5 MHz	250 kbit/s	- most common frequency. - OQPSK symbol=2 bits
Americas Australia	902 à 928 MHz	10 channels in 2003 then 30 in 2006	40 kbit/s 250 kbit/s in 2006	4 phy levels,In 2006, special coding and a dynamic exchange to 868 MHz band.
Europe	968 à 968.6 MHz	1 channel in 2003 then 3 in 2006	20 kbit/s 100 kbit/s in 2006	- same as 915 MHz.

TABLE 2.1. FREQUENCIES AND MODULATION TYPES IN IEEE802.15.4

In 2009, 802.15.4c and 802.15.4d added further physical levels: one in the 780 MHz band using O-QPSK or MPSK, another in the 950 MHz band using GFSK or BPSK. Note that the multitude of possibilities on different frequencies and different types of modulation offer more opurtunities for manufacturers to build their products according to an adequate standard.

2.3.1.2 Link layer

All participating devices form a network, which can have various topologies, and exchange frames (the basic unit of information exchange). The standard defines 4 types of frame:

1. data frame: for sending regular data
2. acknowledgment frame
3. beacon frame: used by the PAN coordinator to signal physical layer parameters and trigger communication with associated devices
4. MAC command frame: generally used in beacon mode to activate MAC services.

In this standard, the MAC layer is responsible for beacon management, channel access, GTS (Guaranteed Time Slot) management, frame validation and more. However, there are two modes of operation for the MAC layer. For more details, please refer to the standard [35].

- non-beacon mode, using CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). In this mode, the coordinator remains in the data waiting state by default. This mode is generally used for sensors (such as switches) that are asleep most of the time. When an event occurs, the sensors wake up instantly and send an alert frame. The coordinator in this type of network must be mains-powered, as

it never sleeps: by default, it is in the listening state. In this type of network, the coordinator does not emit a beacon and prevents any synchronization of devices. The advantage of this solution is that it optimizes sensor battery autonomy and uses the channel only when it is necessary to transmit useful data. On the other hand, with CSMA/CA, access to the channel is not guaranteed within a given period (depending on network density and the number of devices wishing to transmit at the same time).

- beacon mode, with a beacon sent at regular intervals to synchronize the devices, guaranteeing throughput to the sensor with a GTS. The aim of this mode is to synchronize devices with the coordinator by periodically sending a beacon. All devices (including the coordinator) operate independently. However, to communicate on the network, they need to synchronize with the coordinator's (or a router's) wake-up time, as it is responsible for routing data across the network. When a beacon is received, all devices are informed when the coordinator is active and when they can transmit. Devices then know when they can hibernate or transmit.

2.3.1.3 Limitations

IEEE 802.15.4 has certain limitations, but so do many other IoT technologies, which affect its reliability. One of these is interference from other transmissions in the ISM bands. Example technologies, as we have already seen, almost all operate in ISM bands, notably the 2.4 GHz band. As a result, this band is overloaded if different operators use it at the same time. In contrast, radio waves propagate mainly by scattering on surfaces and by diffraction on and around them, where multipath fading results from the fact that signals take different paths and arrive at the receiver with different phases. This implies either constructive interference if all the signals have the same phase, or destructive interference if the signals interact negatively (opposite), always accompanied by simple fading.

The standard also suffers from the communication range, which is on the order of 200 meters in outdoor environments. Coverage can be improved by using multi-hop transmissions in a mesh topology. However, devices that relay messages present three problems:

1. additional deployment costs
2. increased latency
3. security issues and reduced communication reliability

The latter is due to the problem of multi-point failures caused by multi-hop compared to single-hop communication systems. One way to improve reliability is to increase transmission power, but the inherent nature of IoT solutions generally precludes this.

2.3.2. NB-IoT

Narrowband IoT (NB-IoT) is a cellular-based LPWAN technology first introduced in Release 13 (3GPP), then enhanced by the addition of several IoT features to existing Global System for Mobile Communications (GSM) network architectures and the long-term evolution (LTE) of 4G. NB-IoT is also known as LTE Cat M2. The main objective is to provide extensive coverage at a very low cost per device. Added to this, reduced device complexity and backward compatibility are also at the heart of NB-IoT.

Compared to other LPWAN technologies, NB-IoT attempts to improve in-building coverage while operating with a significant number of its devices at low data rates and low latency. NB-IoT's main requirements are very low-cost devices with a unit price of less than 5$, a battery life of more than ten years with little human intervention, and support for around 50,000 devices per cell.

2.3.2.1 Physical Layer

NB-IoT is based on frequency-division half-duplex (FDD) communication, where traffic flows on two different, non-overlapping channels to minimize interference. NB-IoT typically achieves a transmission rate of around 200 bps. In addition, NB-IoT, as a narrowband IoT technology, requires channels of 180 kHz for both directions. This bandwidth allocation is associated with three scenarios depending on the licensed bands; (1) standalone allocation where a GSM network operator can replace a GSM 850-900 MHz carrier with NB-IoT, (2) in-band allocation where an LTE network operator can allocate a physical resource block (PRB) to deploy in-band within NB-IoT, and (3) guardband allocation where an LTE network operator can also deploy an NB-IoT carrier in a guardband between two LTE channels.

NB-IoT is seen as an improvement on the mechanisms introduced by LTE. Among the many mechanisms that NB-IoT is adopting from LTE, modulation schemes in particular, NB-IoT downlink traffic is based on OFDMA, while uplink traffic is based on single-carrier FDMA (SC-FDMA), employing QPSK and BPSK modulations. The reason for this difference is that, although SC-FDMA is more complex than OFDMA, it is also much more energy-efficient and therefore more suitable for the transmission of constrained devices. The main difference between OFDMA and SC-FDMA lies in the way they organize user data streams in frequency and time.

In OFDMA, traffic is transmitted simultaneously on different sub-channels. Similarly, in the SC-FDMA scheme, the same traffic is transmitted sequentially over individual time slots. The overall throughput is the same for both scenarios. The maximum transmission power for uplink and downlink transmissions is 23 and 46 dBm, respectively. For battery and energy conservation, NB-IoT relies on two different mechanisms: power saving mode (PSM) and extended discontinuous reception (eDRX). In power-saving mode, the node sleeps for up to 413 days and cannot be reached by the base station. Similarly, for the

eDRX system, a device is usually inactive for only a few hours.

2.3.2.2 Link Layer

As already mentioned, the NB-IoT network topology is based on the LTE infrastructure. It comprises (1) a network core called the Evolved Packet Core (EPC), (2) an Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) and (3) the UE, which consists of IoT devices. The EPC includes a Mobility Management Entity (MME) that manages device mobility but also performs several actions such as device tracking, session management and the selection of the Serving Gateway (S-GW) for initial device attachment and authentication. The S-GW routes data packets across the network, and acts as an anchor point for device handover during transition between different eNode base stations (eNBs). The P-GW is the interface between the 3GPP network and an external network, such as the IP network. Finally, the Home Subscriber Server (HSS) is a database used for mobility, session and user, as well as access authorization.

The MAC sublayer of the link layer is responsible for processing retransmissions, time advance, multiplexing, random access and priority management, time advance, multiplexing, random access, priority management and scheduling. Resource allocation must ensure that the maximum number of devices is served in a given cell, while achieving a specific level of throughput, spectral efficiency and coverage.

2.3.2.3 Limitations

Although NB-IoT offers excellent coverage and obstacle penetration, making it suitable for remote and urban areas, this technology uses licensed cellular spectrum. NB-IoT deployments require additional hardware components, which can be time-consuming and require coordination with multiple stakeholders, including network operators and infrastructure providers. NB-IoT is less powerful than LTE-M, as it does not have the speed or bandwidth required for high data transfer. This is a disadvantage for IoT applications that require large amounts of data. NB-IoT is not a good choice for applications requiring constant, real-time data transfer. NB-IoT has a higher latency than technologies such as 4G-LTE or 5G, which can lead to delays in data transmission. What's more, its operation is limited to 4G.

2.3.3. LoRa

LoRa itself represents the physical layer of this technology, a modulation technique based on the radar technique known as Chirp Spread Spectrum (CSS). Being copyrighted, no clear description of the modulation is available. All the information found in articles and books comes from the patent [37] and from semi-official documents from Semtech and the LoRa Alliance, such as [38] [39] [40]. However, a few researchers have analyzed

and successfully reverse engineered modulation. They have even succeeded in mathematically reformulating the LoRa signal like [41]. When LoRa is purely a physical layer implementation, LoRaWAN is a LoRa-based complementary network protocol. It is designed to satisfy IoT requirements. It provides bi-directional communication, end-to-end security with AES-128 encryption, mobility, and location-based services. Figure 2.3 shows the relationship between the LoRa Physical Layer and the LoRaWAN MAC Layer in the OSI Stack.

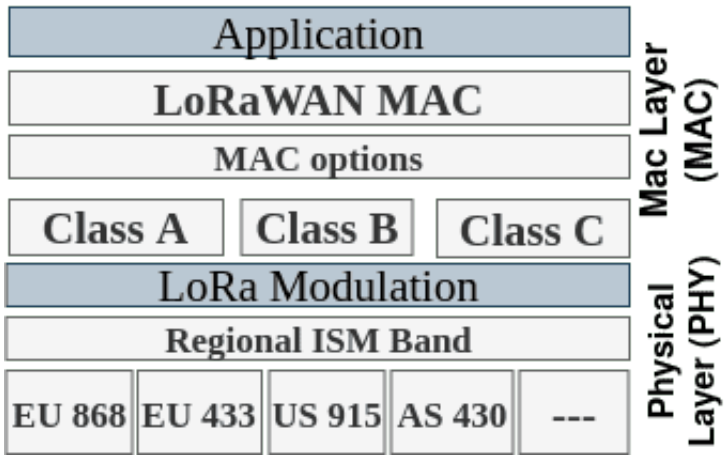

Fig. 2.3. LoRaWAN stack

2.3.3.1 Physical Layer

The principle of CSS is to linearly vary the frequency of the sinusoidal signal for a fixed period of time, known as chirp.This modulation can be used to "broadcast" information over a wider spectrum than it would normally occupy. This uniform distribution of a symbol over a wider bandwidth offers resistance to frequency-selective noise and interference, at the cost of lower spectral efficiency. It is also more resistant to multipath interference and the Doppler effect than more conventional modulations. Let's assume that the frequency band available for transmission is $B = [f_0, f_1]$. A chirp can be constructed to increase linearly in frequency from a starting frequency $f_s \in B$ to that same frequency, winding back from f_1 to f_0 when it reaches the end of the available band Figure 2.4. Since the frequency varies for a symbol, the starting frequency of a chirp represents the symbol [42].

The number of bits LoRa encodes in a symbol is an adjustable parameter, called the SF spreading factor. The spread factor of a transmission is also used to determine the duration of a symbol T_s, according to the following expression:

$$T_s = \frac{2^{SF}}{B} \tag{2.1}$$

This means that, if the bandwidth is fixed, an increase in the spreading factor of 1 will double the symbol duration Figure 2.5. Similarly, if the bandwidth increases, the chirp

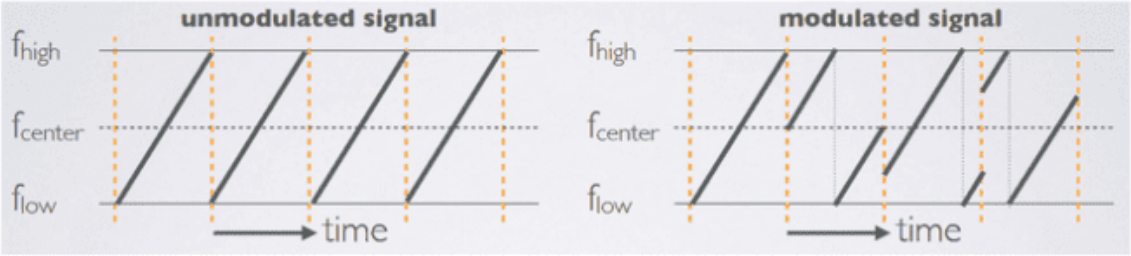

Fig. 2.4. LoRa CSS modulation

transmission rate increases and, consequently, the modulation bit rate. Increasing the transmission time of a chirp (symbol) makes the message more resistant to interference or noise. On the other hand, this effect can be partially offset by the fact that, for higher spreading factors, the number of possible symbols increases according to the formula: 2^{SF}, making the occurrence of symbol errors more likely: the reason for this is that signal synchronization on the receiver side is particularly critical when low data rates are used. Furthermore, the transmission of longer messages is more prone to collisions.

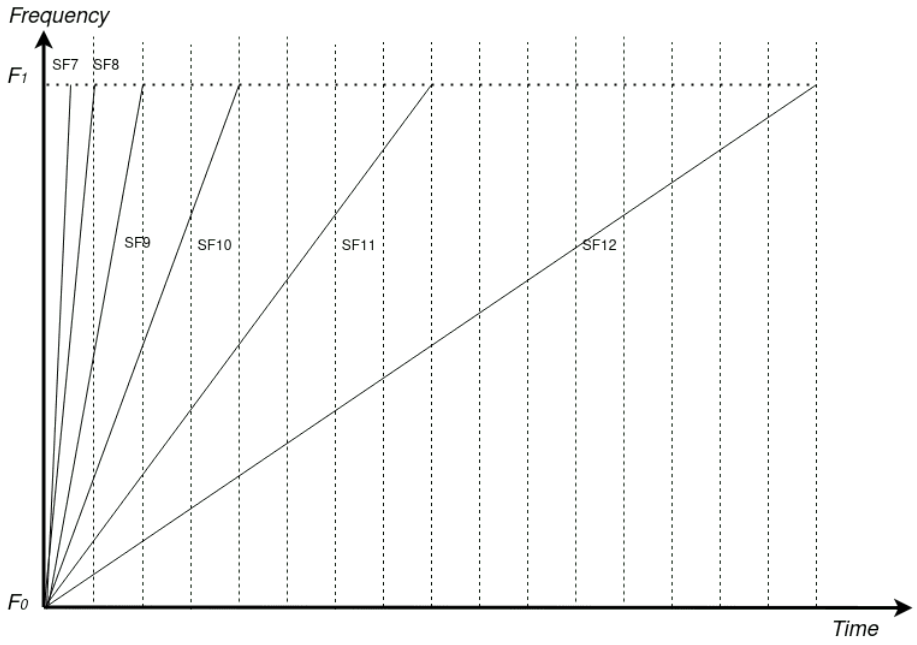

Fig. 2.5. Symbol transmission time

For the signal to be received correctly, a receiver needs a signal intensity Received Signal Strength Indicator (RSSI) above the noise floor, and a signal-to-noise ratio (SNR) above a given threshold to separate the original signal from the modulated carrier. RSSI is a relative measure of whether the signal received is strong enough to provide a good wireless connection. SNR is used to determine the quality of the received signal.

The data sheet [38] states that LoRa can demodulate certain signals that are below the noise floor. The Table 2.2 shows the minimum SNR required for demodulation at

different spreading factors.

SpreadingFactor (RegModulationCfg)	Spreading Factor (Chips / symbol)	LoRa Demodulator SNR
6	64	−5 dB
7	128	−7.5 dB
8	256	−10 dB
9	512	−12.5 dB
10	1024	−15 dB
11	2048	−17.5 dB
12	4096	−20 dB

TABLE 2.2. RANGE OF SPREADING FACTORS

For error detection/correction, LoRa uses a ratio called the Coding Rate (CR), which increases the number of bits to be transmitted. It tackes values from $\frac{4}{5}$ to $\frac{4}{8}$, In the case of $CR = \frac{4}{8}$, there will be 8 bits actually transmitted each time each time we wish to transmit 4 bits. In this example, this results in doubling the number of bits sent. These redundant bits help restore data if corrupted by interference. It's easier to correct corrupted data if there are more redundant bits, but bandwidth will be reduced and power consumption will increase.

Orthogonality is a characteristic explored by all technologies in order to increase transmission capacity and avoid interference, and thus achieve higher throughput. LoRa modulation exploits this property by making the various spreading factors pseudo-orthogonal. This is true even when the same center frequency and bandwidth parameters are used. This allows correct reception of transmissions as long as their SFs are different and the signal-to-interference-plus-noise ratio (SINR) of the received packet is above a certain threshold.

The regional parameters document [43] also includes physical layer parameters such as frequency plans (channel plans), mandatory channel frequencies and data rates for trunk request messages. It also includes MAC layer parameters such as maximum payload size. In the following Table 2.3 you'll find some frequency plans.

Plan ID	Frequency Plan	Common Name
1	EU863-870	EU868
2	US902-928	US915
3	CN779-787	CN779
4	EU433	EU433
5	AU915-928	AU915
6	CN470-510	CN470
7	AS923-1	AS923
8	AS923-2	AS923-2
9	AS923-3	AS923-3
10	KR920-923	KR920
11	IN865-867	IN865
12	RU864-870	RU864
13	AS923-4	AS923-4

TABLE 2.3. FREQUENCY PLANS

But there are recommended default settings that can be applied to all regions. Here are just a few:

- RX1 delay: 1s
- RX2 delay: 2s (RX1 delay + 1s)
- Joint 1 acceptance time: 5
- Joint 2 acceptance time: 6s

2.3.3.2 Link Layer

Long Range Wide-Area Network (LoRaWAN), is a media access control (MAC) protocol sublayer. It's a protocol optimized for battery-powered devices, which can be mobile or fixed. In these networks, the topology is a star of stars, with gateways relaying messages between end devices and a central network server. The latter routes packets from each network device to the associated application server Figure 2.6.

Transmission security is based on symmetrical cryptography using session keys derived from device root keys stored in a join server, with associated key derivation operations. Gateways are connected to the network server via secure standard IP connections (LTE, 4G, 5G, Ethernet, etc.), while end devices use single-hop LoRa or FSK communication to one or more gateways, all communications are generally bidirectional.

The communication is distributed over different channels with selected frequencies and data rates, with a compromise between communication range and message duration. LoRa data rates range from 0.3 kbps to 50 kbps. However, optimization of battery life

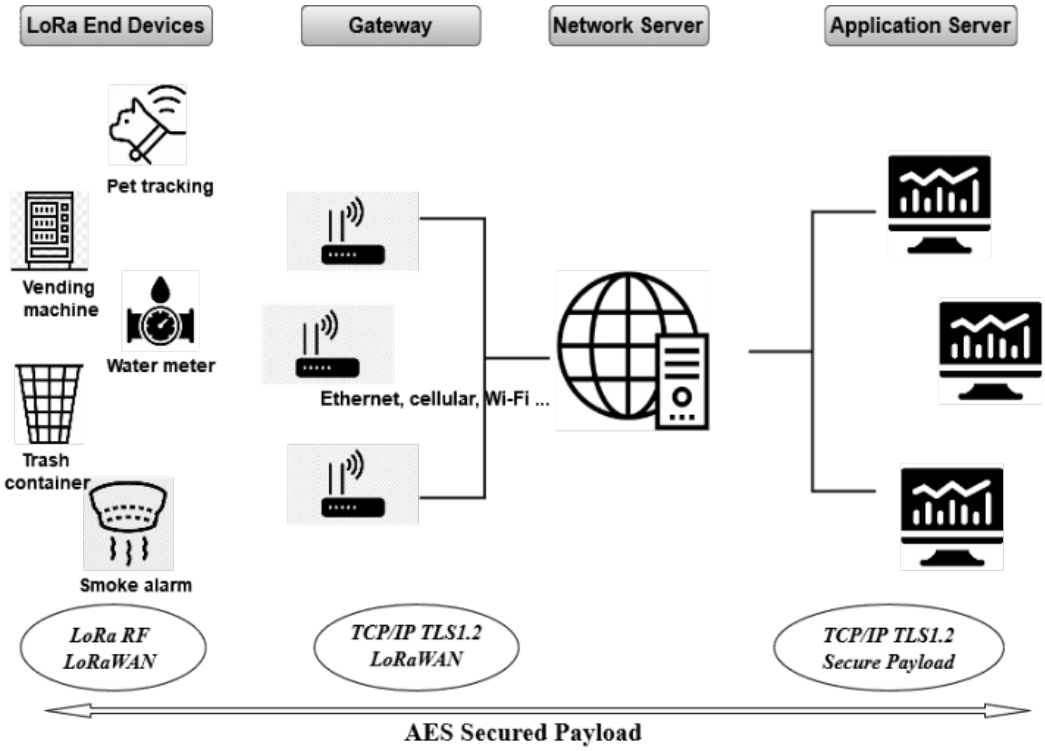

Fig. 2.6. LoRaWAN architecture

and overall network capacity can be managed individually by means of an adaptive data rate (ADR) system.

End devices can transmit on any available channel at any time, using any available data rate, provided the following rules are met:

- The end device changes channel pseudo-randomly with each transmission. The resulting frequency diversity makes the system more resistant to interference.
- The end device respects the maximum transmission duty cycle according to the sub-band used and local regulations.
- The final device respects the maximum transmission duration (or waiting time) in relation to the sub-band used and local regulations.

Note that the regional parameters specify the maximum transmit duty cycle and latency per sub-band for each region in the LoRa physical layer.

In a LoRa network, three classes are specified, a base class (called class A) which must be implemented in all terminal devices, and two optional classes (class B, class C). In all cases, communications are bidirectional.

1. Class A: Uplink transmission from each terminal device is followed by two short downlink reception windows, RX1 and RX2. The uplink transmissions of the end

device are based on its own communication needs on a random time principle according to the ALOHA protocol. Downlink communications from the server will have to wait for the next scheduled uplink Figure 2.7.

2. Class B: Terminal devices operating in this class have programmed reception slots. In addition to the random reception windows of Class A, additional reception windows are opened at programmed times. These windows are synchronized by synchronization beacons from the gateway.

3. Class C: Terminal devices have, almost, continuously open reception windows, which are only closed during transmission. This affects battery life, but they offer the lowest latency.

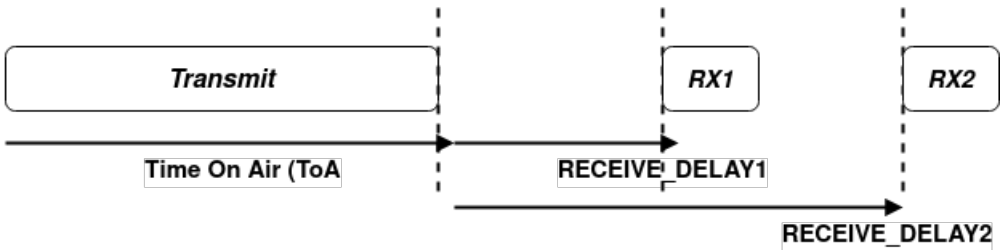

Fig. 2.7. Receive slot timing

2.3.4. LoRa vs NB-IoT

LoRa works in the ISM bands, while NB-IoT operates in licensed spectrum, like LTE. Although both technologies deliver a higher quality of service (QoS), IoT applications requiring frequent messages will be better served by NB-IoT, as it has no duty cycle limits, but at the cost of a higher total deployment cost than LoRaWAN.

LoRaWAN and NB-IoT end devices consume less energy in standby mode. Message synchronization means that NB-IoT consumes much more energy than LoRaWAN, which is an asynchronous protocol, and for the same data rate conditions, NB-IoT consumes a higher peak current due to OFDM/FDMA modulation.

NB-IoT can be deployed directly in areas that already have cellular coverage, but deployment costs are higher as private network deployments will require the acquisition or leasing of RF spectrum from network operators. LoRaWAN has demonstrated better in-building penetration capabilities than NB-IoT, which is a factor influencing cost and performance. NB-IoT's lower link budget also reduces battery life.

Table 2.4 from the whitepaper [44] summarizes the main features of both LoRaWAN and NB-IoT technologies.

Technology Parameters	LoRaWAN	NB-IoT
Bandwidth	125kHz	180kHz
Coverage	165 dB	164 dB
Battery Life	15+ years	10+ years
Peak Current	32 mA	120 mA
Sleep Current	1μA	5μA
Throughput	50Kbps	60Kbps
Latency	Device Class Dependent	< 10 s
Security	AES 128 bit	3GPP(128 to 256 bit)
Geolocation	Yes (TDOA)	Yes (in 3GPP Rel 14)
Cost Efficiency (Device and Network)	High	Medium

TABLE 2.4. COMPARING LORAWAN AND NB-IOT

2.3.5. LoRa vs 5G

Another document from the LoRa alliance [45] gives a comparison with NB-IoT/LTE and a complementary approach between LoRaWAN and 5G technology in terms of QoS. LoRaWAN and 5G meet different needs. But together, they meet all the massive, critical requirements of the IoT. Besides the difference in transmission bands, LoRaWAN serves the massive IoT with its low data rates, thousands of end devices connected to a single gateway, lower deployment costs, long range and high penetration, support for mobility and roaming, and finally with long battery life of up to 15 years. While 5G serves the critical IoT with its high data rates, less coverage, lower latency and better QoS, which is required by video, voice and emergency services.

2.4. Conclusion

The two main families of IoT networks are Wireless Personal Area Networks (WPAN) and Low Power Wide Area Networks (LPWAN). The differences between these two wireless families are signal coverage and data rates. As wireless technologies, both families attempt to conserve battery life, each focusing on one or the other. Specifically, WPANs sacrifice signal coverage to support higher data rates, while LPWANs sacrifice data rates to support greater signal coverage.

Among the LPWAN technologies on the market (LoRa, Sigfox and NB-IoT), our interest is in LoRa technology, and in particular its open LoRaWAN protocol. The presentation of LPWAN and WPAN networks, and details of LoRa's physical and MAC layers, enabled us to compare this technology with others in terms of performance and QoS.

3. BIOMETRIC SECURITY IN IOT

3.1. Introduction

Security is a major concern for IoT applications. In particular, the integrity of data and IoT devices, e.g. sensor readings and actuator commands, is the basic guarantee for securing IoT operations. Effective mechanisms must be designed to protect IoT communications in terms of confidentiality, integrity, authentication and non-repudiation of information flows. IoT devices must be identified to ensure data integrity from its origin, which typically relies on trusted third parties, for example an identity provider. Authentication and encryption algorithms are used to protect the confidentiality and integrity of IoT data. Once sensory data is sent to data storage, data security relies on the data storage service.

The usual solution for certifying the security of things is identification technology, which maps a unique identifier (UID) to an entity to make it unambiguous. UIDs can be created as a single measure, so that the combination of their values is exclusive. In the IoT, "things" or objects have an identity identified by a numerical name. There are two categories of techniques for assigning a UID to an entity or objects: traditional techniques and biometric techniques. Traditional IoT security is either knowledge-based (such as a password, PIN or any type of personal information to authenticate a user), or object-based (such as smart cards. IoT biometric security indicates the measure associated with human characteristics. IoT biometric validation or real-time verification is used to recognize entities in groups under observation.

Biometric authentication is recognized as an effective technique for secure authentication. however, its use in the IoT context is difficult. Its feasibility in such systems has to deal with physical and administrative constraints, including a limited Internet connection, a limited budget, the need for easy development and the high level of security required.

3.2. IoT security challenges

The lack of a common standard and architecture for IoT security will not facilitate its implementation. It is difficult to guarantee security and user confidentiality in a heterogeneous network like the IoT. The enormous exchange and collection of information in the IoT by connected objects represents one of the security issues, based on the distribution of keys between devices. On the other hand, issues of confidentiality and access operations are extremely critical. The growing number of intelligent objects around us, containing sensitive data, requires transparent and easy management of access control, by varying privileges for example. In this context, one solution is to group objects into virtual networks controlled by a single device. Another approach is to support access control in the application layer on a per-provider basis [46].

Despite the fact that various IoT applications have improved the quality, flexibility and scalability of the infrastructure of different ecosystems, by reducing errors, saving costs and improving the performance and security of processes and transactions, most existing IoT architectures maintain a centralized data center for the storage and processing of sensor data, which can present a risk of security breaches, single-point failure and malicious attacks such as DDoS. In addition, data interception can occur when IoT devices transfer data between each other, calling into question the reliability of the data collected.

The majority of IoT devices are deployed in unmanaged locations, and it may be impossible to monitor the huge number of devices all the time. This makes devices vulnerable to multidimensional damage. Traditional security mechanisms, such as asymmetric encryption, are demanding in terms of computing power for IoT devices with limited capabilities. The data collected by the sensors can be stored, transmitted and processed by many different intermediate systems, increasing the risk of manipulation and falsification. Unreliable and open wireless channels pose additional data security risks. The complexity of the IoT system adds to the above-mentioned vulnerabilities.

3.2.1. IoT security flaws

Here are some typical attacks on IoT networks from the lower to the upper layer [8].

- Attacks to End Devices: Attackers physically capture and control nodes through node capture attacks or through physical access. Stored secret information, such as keys and certificates, becomes visible. Then, they can use this information to impersonate legitimate nodes and carry out other attacks, such as fake data injection attacks.

- Attacks to Communication Channels: Attackers can eavesdrop and interfere with transmission channels, thus exploiting the nature of radio. They can easily obtain the transmitted information if the signal is not encrypted. Even though the signals are encrypted, they are still capable of analyzing signal streams and inferring private information, such as the location of sources or destinations. They can also interfere and even jam wireless channels by sending noisy signals.

- Attacks to Network Protocols: Several network protocols are vulnerable and can be exploited by attackers. These can launch sybil attacks, response attacks, man-in-middle attacks, blackhole, wormhole, etc. For example, a Sybil device impersonates multiple legitimate identities in IoT systems. Such attacks would compromise the efficiency and accuracy of the voting mechanism and multi-path routing protocols.

- Attacks to Sensory Data: Many IoT networks use ad hoc, hop protocols. This offers forwarding attackers the opportunity to falsify data or inject false data. However, authentication algorithms deployed cannot completely prevent data falsification. This attack is legitimate because the false data injected into the targeted network is

tagged with legitimate identities. Therefore, erroneous instructions will be returned by IoT applications in response to these injections and thus provide erroneous services. This will compromise the reliability of IoT applications and networks in the case of a road traffic management application for example. Fake data injection attacks can hardly be prevented by authentication algorithms.

- Denial of Service (DoS) Attack: DoS attack represents a category of attacks that exhaust resources and congest services of IoT systems. A typical example is the sleep deprivation attack which involves keeping devices or nodes awake all the time until they run out of battery power. These attacks exploit the resource, network and communication limitations of IoT devices. Such attacks can therefore be catastrophic as they deplete the limited energy of sensory nodes, reduce network connectivity, cripple the entire network, and reduce the network lifetime.

- Software Attacks: These are attacks that use software backdoors to modify software and control operations. Typical software attacks include viruses/worms/malicious scripts. Generally, Intrusion Detection System (IDS) is used to combat this type of attacks.

3.3. Biometrics overview

Biometrics is a technology of identifying or verifying people based on their physiological and behavioral characteristics or traits. The selection of biometric traits should follow requirements such as universality, distinctiveness, permanence, and collectability. In addition, requirements for recognition accuracy and matching speed are to be met in the design of a practical biometric system. The choice of biometrics characteristics generally depends on the needs of the authentication application. For example, Voice biometrics is suitable for mobile security because the device that detects voice sounds is already built into the cell phone.

Biometric recognition uses two aspects of the human body's characteristics, namely distinctiveness and permanence. Fingerprints, face, iris, hand geometry, gait, DNA (deoxyribonucleic acid), etc. are some of the most common physiological traits used in IoT biometric security. The most interesting aspect of IoT biometric authentication is that it can identify the person who is not registered in the system, but is still trying to access it. There are two types of biometric modalities: physiological and behavioral.

3.3.1. Physiological features

Any directly measurable part of the human body belongs to the physiological characteristics. Systems for recognizing faces, fingerprints, irises, Palm Print, DNA (Deoxyribonucleic Acid), Hand Veins and hand geometry fall into this category.

3.3.2. Behavioral features

Behavioral features are a type of indirect measurement of human characteristics, through feature extraction and machine learning. The most common features are signature, keystroke dynamics, gait and voice.

3.4. Biometric Security System

There are two types of identity matching: authentication and recognition or identification. A person's assertions are proved or disproved by verification, while the identification process identifies him or her. Figure 3.1 describes a biometric security system .

A typical biometric authentication system consists of two phases [47]:

1. Enrolment phase where a set of features are extracted from the user's biometric image and stored in a database as template data
2. Verification phase where the biometric features of the query are extracted in the same way as in the enrolment phase, then compared with the template data. If the similarity score between the model data and the query data is above a predefined threshold, the verification is successful; otherwise, it's a failure.

Biometric authentication systems are monomodal if they use a single trait, otherwise they are multimodal.

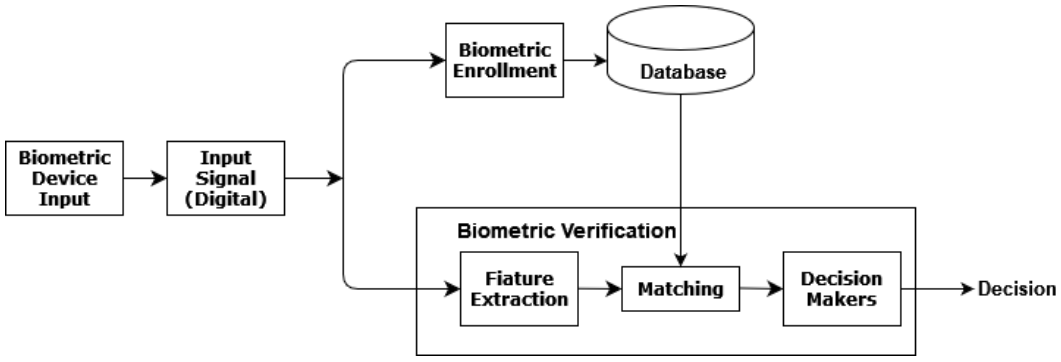

Fig. 3.1. Biometric security system

Uncertainties due to the biometric acquisition process, and noise in biometric authentication systems are inevitable. Samples of the same biometric trait captured at different times or under different conditions are likely to be different. Such anomalies and variabilities can lead to erroneous authentication procedures in a real attempt, or to false success in an impostor attempt. It is therefore necessary to evaluate the performance of a biometric authentication system using a number of measures. Conventional evaluation measures are false acceptance rate (FAR), false rejection rate (FRR), equal error rate (EER) and recognition accuracy (RA) [48].

1. False acceptance rate (FAR): The FAR is the probability of mistaking biometric samples from different subjects to be from the same subject.

2. False rejection rate (FRR): The FRR is the probability of mistaking biometric samples from the same subject to be from different subjects.

3. Equal error rate (EER): The EER is the error rate when FAR and FRR have the same value. The FAR and FRR are inversely related, which means that when one increases, the other should decrease.

4. Recognition accuracy (RA): RA is computed as the percentage of correct predictions out of the total number of observations. This metric is a common performance measure in machine and deep learning-based schemes.

3.4.1. Biometric vs standard security systems

Biometric-based security has many advantages over conventional security system [49]:

- Precise information: it provides more precise and secure information than PIN or password-based security systems. The user doesn't need to remember the password/PIN, and no malicious person can breach security by duplicating, guessing or hacking biometric information on the system's server

- Easy and secure to use: Biometrics are very easy and secure to use. Hackers cannot possess the biometric information of legitimate users.

- Accountability: Repudiation and denial of activities is not possible in a system using biometrics. However, the responsibility of the system user will also increase for any kind of malfunction and misuse of the system.

- Security of biometric information: This can be a long-term security solution, as biometric data cannot be guessed or stolen. In password systems, on the other hand, a sequence of numbers, symbols and letters is used to construct a password, which is very difficult to remember. Also, in token-based systems, the token can be easily stolen or lost. Consequently, both a password and token-based system present a high risk of use when secret information is shared or disclosed. But this is not the case with biometric features, which are free from the problems of fraud, sharing and duplication.

- Scalability: Biometric systems are flexible and scalable from the user's point of view. Users can use their characteristics, which are not very discriminating, according to their needs. However, to achieve a higher level of security in a large-scale database, and with greater identification precision, it is recommended to use more discriminating features. Indeed, the risk of collision in the hash value of biometric data is lower than in conventional security systems.

- Time savings: The speed of biometric identification is another advantage over traditional security techniques. Verification takes just a fraction of a second. What's more, using this technology can only benefit an organization's income by increasing productivity and reducing costs by eliminating fraud and wasted time in the verification process.

- User-friendly systems: Biometric systems are user-friendly and easy to install on electronic devices. The operational functionality of the biometric system will require minimal training, and it does not need to rely on administrators for passwords.

- Versatility: The availability of biometric scanners on the market makes them suitable for almost any application. Today, many organizations and businesses use biometric devices at security checkpoints, to verify an employee's entry or exit time and presence. In remote patient monitoring systems, biometric identity can be used to send an emergency message to a rescue team. A soldier can ask for help to get out of a dangerous situation by identifying himself with a biometric scanner and transmitter. In short, biometric security systems have versatile applications in different IoT environments.

3.4.2. Limitations of biometrics in IoT

3.4.2.1 Limitations of Applying Biometric-Cryptographic

Sensitive data collected by IoT devices is encrypted to be protected and unchanged during transmission between IoT devices and the server. A technique called biometric cryptography, or bio-cryptosystem for short, a combination of biometrics and cryptography and taking advantage of both. Specifically, in a symmetric biometric-cryptographic system, a secret key can be transparently linked to biometric data using fuzzy engagement or fuzzy vault, in the enrollment and validation processes. verification.

This technique is not a common option in biometric authentication systems for the IoT. The first reason is that binding or generating cryptographic keys is computationally intensive, imposing high computational costs on resource-constrained IoT devices. The second reason is that fuzzy logic techniques often cannot be directly applied to feature sets formed in the cryptographic domain. Indeed, these techniques require fixed-length feature representations in order to measure feature disparity using metrics such as Hamming distance or definite difference, but the raw biometric data collected by IoT devices in the required formats creates an additional computational burden, and also decreases authentication accuracy.

However, Privacy-preserving techniques, such as cancelable biometrics [50] and homomorphic encryption, are effective methods in the latest search results. For voidable biometrics, biometric data is transformed by a non-invertible function to achieve template data protection during the enrolment phase. In the verification phase, the same non-

invertible transformation is applied to the query data. Verification is then performed in the transformed domain to reduce the risk of biometric data leakage. Homomorphic encryption enables mathematical operations on data without the intervention of the decryption key. The confidentiality of biometric data remains intact, and the correspondence between encrypted model data and encrypted query data is performed without degrading accuracy.

3.4.2.2 Selection of Biometric Traits

There are no guidelines on selecting appropriate biometric features for an IoT biometric security system. Each biometric trait has its own characteristics, which leads to very different authentication performances. IoT applications are diverse and there is no single biometric trait capable of meeting all the requirements of IoT-oriented authentication scenarios. For example, despite the strong authentication performance offered by using iris, voice is clearly a better choice than iris in the smart speaker authentication scenario. Similarly, the use of multimodal biometrics improves authentication accuracy and security, but multimodal biometric systems make the entire system more complex and less cost-effective, thereby increasing the storage, processing, and computational burden of IoT devices.

3.4.2.3 Uncertainty of Biometric Data

A typical example of biometric data uncertainty is fingerprint recognition, when a contact sensor is used to capture finger images, non-linear distortion and rotation of the fingerprints are inevitable due to skin elasticity, skin moisture content, finger movement, contact pressure, sensor. Because of this uncertainty, the match between the fingerprints in the request and those in the stored template could fail. Consequently, biometric authentication is by nature a probabilistic task, and there is an inevitable uncertainty and risk of error. Despite these difficulties, research is underway to improve the quality and discriminating power of biometric data, as well as the performance of biometric authentication systems, so that their role in protecting IoT security is more effective.

One solution to reduce the effects of biometric uncertainty may be to adopt a stable, discriminating feature representation. Another solution is to use powerful deep learning techniques to try and achieve good matching performance.

3.4.2.4 Limited Resources of IoT Devices

IoT devices have limited computing resources, if we exclude CPS. Biometric recognition includes complex calculations such as data processing, matching and decision making, and can lead to higher costs and increased load in an IoT environment. Therefore, any new biometric authentication system should optimize the use of limited storage and battery power in IoT devices, while responding quickly to authentication requests. Fur-

thermore, the implementation of a biometric system relies directly on the hardware of an IoT device. For example, IoT devices without camera sensors cannot feature face-based authentication.

Therefore, lightweight and green mechanisms have been proposed for IoT devices to make biometric systems more energy efficient [51].

3.5. Biometrics IoT applications

Biometric security can be used in all areas of IoT applications where human-machine interaction is required. They can be used in smart home systems. A biometric locking system. Signalling the health status of elderly people, by connecting to the IoT health system using the biometric identification / verification system. In transport systems, the system can verify an end-user's identity when parking a car or paying a traffic fine, etc. Using biometric verification, traffic police can check whether a car belongs to a driver or not. Biometric security can be useful for IoT healthcare systems. All healthcare professionals must pass a biometric check before prescribing or accessing a patient's data. If a person is involved in an accident, biometric information can help identify them and obtain their medical history. Researchers are currently trying to introduce IoT into agricultural systems. The following are just a few examples of applications where biometric security systems have been implemented with the IoT.

3.5.1. Biometric-Based eHealth System

A biometric authentication system for secure communication in medical systems is proposed in [52]. In such systems, a patient can receive treatment from home by accessing his or her biometric smartcard using a mobile device via the Internet. To this end, patients first register with an authentication server to obtain their biometric smartcard, and then they can obtain various medical services from medical servers by punching their smartcard. Figure 3.2 shows the network structure of this scheme.

There are four phases of this scheme :

- setup phase: The authentication server generates two keys, one private and the other publishes it as a public key,
- registration phase: In this phase, all medical servers (MS) and patients register under the authentication server (AS), using their unique identifiers. Only, the patient uses the sensor of a mobile device to scan their biometric data and extracts the biometric characteristic. Apart from his unique identity, he also chooses a password via the mobile application. The AS finally burns the data into the memory of the biometric smart card and issues the card to the patient.

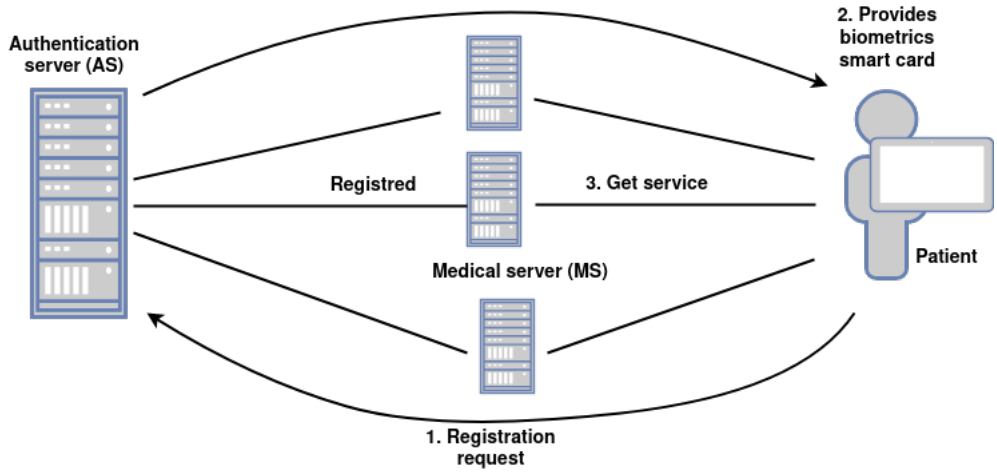

Fig. 3.2. Network structure of Maitra and Giri scheme

- log-in phase: To access the medical servers (MS), the patient inserts the biometric smart card into their mobile device, which also scans their biometrics and extracts the characteristic. The patient then provides their password to the mobile device. It remains for the mobile application to choose the appropriate MS in collaboration with all the medical servers.
- authentication and session key agreement phase: After authentication and using a timeout system the AS, the MS and the patient use a session key for secure data communication in the same session.

3.5.2. Biometric-based smart home security system

The system [53] uses the web camera connected to the Raspberry Pi equipped with sensors such as passive infrared and an ultrasonic sensor. During movement, the camera captures an image of the person in front of the door, then real-time facial recognition is performed. If the person's image matches that of one of the members of the house, the door will unlock, otherwise the doorbell will ring. If an intruder attempts to break the door, an alarm will be triggered at the same time as a text message and an email containing the intruder's image will be sent to the owner. This system is battery powered in the event of a power outage. Additionally, the home owner can track the activity happening in the house using an app connected to the Raspberry Pi via the Internet. Via this application the owner can also add new people to the databases, such as guests for example. The system hardware structure is shown in Figure 3.3.

This biometric system uses the Local Binary Pattern (LPB) technique to extract facial biometric data. Other newer smart home management apps to make it secure, safer and automated like in [54]. Home automation also concerns remote control and monitoring of all home management. However, in this application we note the use of a multimodal biometric system by combining the image of the face and the fingerprint enchanced by a passcode.

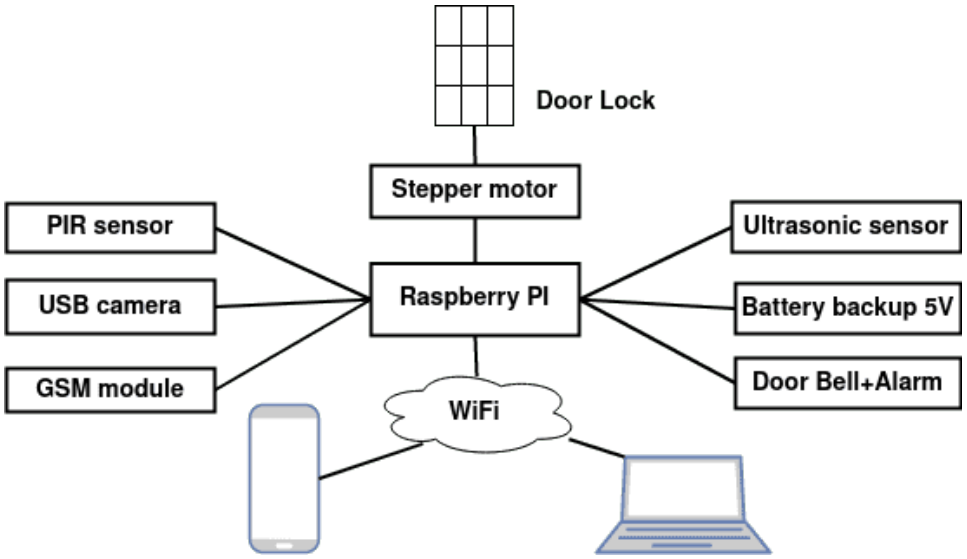

Fig. 3.3. System Hardware structure

3.5.3. Biometric-based IoT application with Machine Learning

Various machine-learning techniques for extracting and analyzing dominant features are used to improve the performance of a biometric system. In particular, classification algorithms have been proposed and successfully used to classify genuine and impostor subjects. k-Nearest Neighbors (KNN), Support Vector Machine (SVM), Naive Bayes (NB), Decision Trees (DT), Random Forest (RF), Gaussian Mixture Model (GMM) and Convolutional Neural Network (CNN) are existing machine-learning and classification methods in the literature, generally used to develop a biometric system. In [49], There is a description of the use cases of various types of Machine learning and Deep learing in IoT applications, with a performance study and comparison of diferent ML techniques. There is also an application for Person Authentication Based on Biometric Traits Using Machine Learning Techniques. A CNN model is trained using an architecture similar to ResNet50, but can accept a low-resolution image as input. Performance parameters were calculated, and the performance of the studied model was compared with traditional ML techniques. The experimental result shows the excellency of deep learning in terms of precision, recall, F1-score, and accuracy for both the face and iris databases.

3.6. Conclusion

Biometric authentication systems have proven their worth in standard systems. Applying this approach in an IoT environment will certainly address vulnerabilities in the various layers of the IoT architecture. However, despite the significant advantages of applying biometrics to guarantee IoT security, there are still a number of potential challenges.

Biometric security can be used in all IoT application areas. Biometrics is used at the application level where human-machine interaction is required. Safety systems can

be used in intelligent home systems. A person can use an intelligent biometric door locking system. An elderly person can report their health status by connecting to the IoT health system using a biometric identification / verification system. In the IoT, a transport system can verify the identity of an end-user when parking a car or paying a fine, and so on. Traffic police can check whether or not a car belongs to a driver, using biometric verification.

4. INTERFERENCE IN IOT NETWORKS

4.1. Introduction

LPWAN is the most common topology used in IoT networks, however, it have a number of problems to solve: Penetration, Security, Bidirectional communications, Inter-technology communication,Support for mobility, Nodes density,Scheduling mechanisms,Adaptive power control,Technology co-existence and interference, etc [55]. Some of them have solutions that are not effective enough, while others are still under development and other problems have yet to be tackled.

That said, standard protocols developed essentially for multiple channel access offer basic solutions. However, with the emergence of mobile telephony and the massive use of the ISM band, new requirements and problems have arisen. As a result, new approaches are required, and standard solutions need to be improved or rethought to meet these needs. Current research focus on the analysis of RF frequencies [56] to solve the problem of interference need improvement and enhancement.

So, before tackling the problem of interference, it's important to recall a few facts about waves and their propagation, which are the origins of signal degradation and this phenomenon and to explain the concept of multiple channel access and the network layer responsible for controlling it.

4.2. Propagation

Images, voices, music and all kinds of information transmitted by radio, television and cell phones are electromagnetic waves. This information is coded by the length and frequency of the waves, which are carried in air and in a vacuum without any physical support. Antennas, environmental electrical parameters in which radio waves must travel and distance influence wave propagation, while the physical characteristics of the waves affect their interference.

Propagation is also relatively dependent on usable frequencies, the minimum signal level required at reception to ensure the required quality of service, and other parameters such as the type of environment, atmospheric conditions or physical constraints. Signal power losses must also be taken into account, depending on the propagation mode and the type of space.

Electromagnetic energy radiates outwards from the source, usually an antenna, at close to the speed of light, and is attenuated and influenced by the medium it passes through. At another distant point, this energy is detected to recover the information it contains, while eliminating noise and other unfavorable factors introduced along the trans-

mission path. Understanding radio wave propagation is therefore essential when planning and operating radio communication systems [57], to guarantee link availability and optimize investment and operating costs.

Radio waves can travel through different modes depending on the medium they pass through.

1. Propagation in free space (direct wave): In this mode, radio waves are not affected by the earth or its atmosphere.
2. Ground-wave propagation (surface wave): Here, radio waves follow the curvature of the earth's surface.
3. Ionospheric propagation (reflected wave): Radio waves are refracted by the ionized layers of the atmosphere in this mode.
4. Tropospheric propagation (refraction): Transmission occurs in a "line-of-sight" manner, with some atmospheric refraction involved.
5. Scattering propagation: This mode utilizes natural phenomena like tropospheric turbulence or ionized meteor trails to disperse radio waves.

These different propagation modes allow radio waves to travel in various ways and are used in different communication systems for specific purposes Figure 4.1.

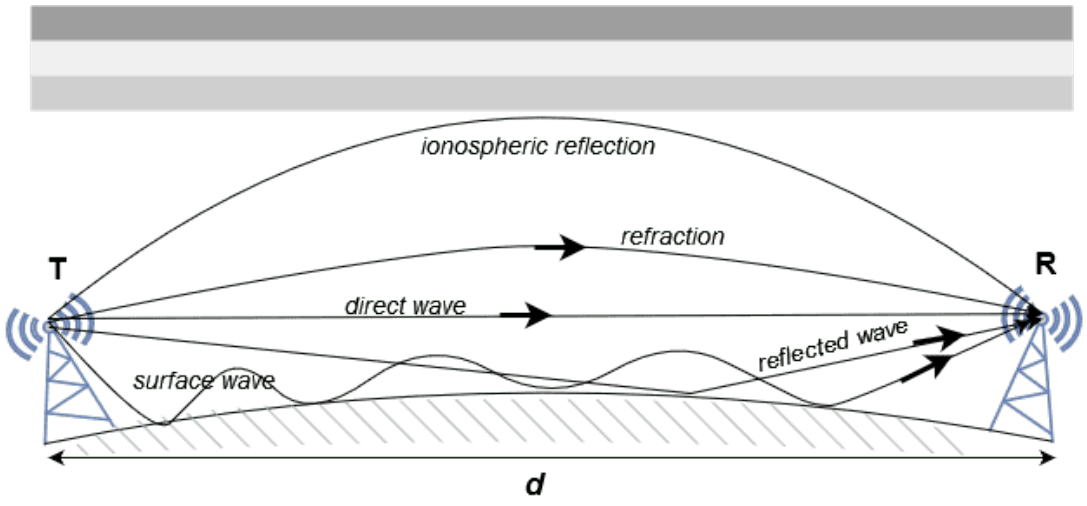

Fig. 4.1. Electromagnetic propagation modes

The direct wave and the reflected wave constitute the space wave, in the presence of two materials, air and ground, with boundary conditions. The air represented by the troposphere will produce a bending of the space wave in the form of refraction. Obstacles in the path of the space wave will cause diffraction.

4.3. Signal degradation

Like light waves, radio waves are affected by reflection and refraction. Atmospheric and natural phenomena such as rain, snow and fog also attenuate these waves. Therefore, multipath interference, fading and attenuation losses are the three main types of signal degradation [58].

4.3.1. Multipath

Multipath between transmitting and receiving antennas is mainly due to reflections from the earth's surface, the ionosphere, natural or artificial objects and atmospheric refraction. This phenomenon results in a phase shift between the reflected wave and the original wave, as a function of the path distance. This can lead to interference at the receiver, known as multipath interference. The dependence of the phase shift of the received combined signal on frequency can lead to serious problems in broadband transmissions.

4.3.2. Fading

Fading is caused by abnormal changes in the refractive index of the atmosphere. Normally, the atmosphere refracts or bends radio waves towards the earth's surface. However, discontinuities in temperature or humidity levels along the path can cause radio waves to deviate more than normal. This leads to changes in the received signal strength, or even a total loss, with the waves never reaching the receiving antenna.

4.3.3. Attenuation

Atmospheric attenuation losses are more serious, relative to the increase in radio frequency. Fading and increased error rates are generally taken into account during the design process, using meteorological data for the region in which the radio link is located.

4.4. Electromagnetic Sources

Our ecosystem is crowded with radio frequencies of all kinds, and RF signals are likely to become increasingly numerous. In particular, the frequencies of the ISM spectrum bands were originally reserved for industrial, scientific and medical purposes. This part of the spectrum is used by WiFi, Bluetooth and many other emerging communication systems, including IoT devices.

To design a reliable wireless communication system, it's vital to be aware of all possible electromagnetic sources, whether caused naturally or by devices around us. In fact, the new system must take into account not only the degradation caused by propagation, but

also the interference caused by these sources. This spectrum and possibly other spectra such as natural and man-made sources of Electromagnetic can be classified into several main categories. Some of these source categories are [59]:

1. Ambient EMI, made up of numerous sources such as television, AM, FM and satellite radio. They can affect sensitive electronic equipment located close to EMI sources. The probability of EMI causing an interference problem is high because the radiated power of the source is high in the vicinity. In other words, its frequency in the band is high

2. Threats linked to high-power electromagnetic pulses, aimed at disabling electrical and electronic equipment used by military organizations, such as high-altitude nuclear electromagnetic pulses. They can totally destroy the operation of electrical and electronic equipment

3. Power quality degradation factors can affect the operation of equipment supplied by a main power source. These power system degradation factors include, for example, overvoltages, and high and low voltages. They can affect the normal operation of the equipment they supply. Transients such as power surges are capable of destroying electronic interface circuits and can cause disturbances in electronic circuits.

4. Medical equipment used in medical establishments has many sources of electromagnetic interference, such as magnetic resonance imaging (MRI) systems, resuscitation equipment such as ventilators, cardiac defibrillators, infusion pumps, and so on. The signals from the human body that these devices monitor are very weak. They are measured in units of microvolts and micro-amperes. Hearing aids, wireless patient monitoring systems, magnetic resonance imaging systems, implantable cardiovascular devices, drug pumps and portable diagnostic equipment are other devices likely to be affected by electromagnetic interference.

4.5. Interference

Interference is caused mainly by heterogeneous and homogeneous devices, and by the coexistence and proximity of other networks. Such interference can considerably reduce quality of service (QoS). This problem still persists, especially in the ISM band, where LoRa operates, as many of the technologies mentioned in the previous sections share this band.

4.5.1. Categorizing signals

The degree to which signals affect a wireless communication system, in terms of interference, varies relatively according to the type of spectrum transiting and the bandwidth in which the system operates. Understanding the properties of the spectrum and the different

types of interference helps to solve the interference problem. Interference is grouped into six general areas [60]:

- in-band interference: These are unwanted signals from a transmitter that fall within the operating bandwidth of the system in question. Here, the interference passes through the receiver's front end, but causes problems when it is so close to the signal of interest. the desired signal will be corrupted if the amplitude of the interference is greater than it is. If they have roughly the same amplitude in the band, it may be difficult to distinguish the interference from the signal.

- co-channel interference: This is one of the most common types of radio interference, caused by another radio transmitting simultaneously in the same wireless system (on the same frequency channel). Wireless networks try to minimize this possibility by ensuring that transmitters listen for an open channel before transmitting, but there is nevertheless a risk of simultaneous transmissions. This type of interference increases in IoT networks, where a large number of devices and objects exist.

- out-of-band interference: This interference is caused by a wireless system transmitting energy in a frequency band that is not its intended use. This is due to inadequate filtering, non-linearity and/or signal leakage. For example, a poorly designed or filtered transmitter emits harmonics that fall into a higher frequency band.

- adjacent-channel interference: This interference occurs because the energy produced by the signal itself scatters into other nearby channels. The surrounding upper and lower channels are affected by these parasitic emissions, usually resulting from a sudden change in the transmitted signal, starting or stopping. They can also be generated by modulation and intermodulation distortion.

- downlink interference: They can alter downlink connections, usually between a base transceiver station (BTS) or gateway and a mobile device. This is known as co-channel interference. As mobile devices are usually widely dispersed, this type of interference usually affects only a few nodes, leaving the communication of the system as a whole relatively intact.

- uplink interference: Uplink or reverse link interference affects communications sent from a node to a BTS receiver or gateway, or from a base station to a satellite. Uplink interference determines the capacity of each cell site in cellular networks. It is one of the main causes of degraded cell site performance.

4.5.2. Future solutions

New research is focusing on the idea of RF data analysis and The cloudification of radio frequency (RF) data. This is a major trend that represents the next frontier after the

cloudification of big data. It can open up new fields of research, services and applications in the field of big data analysis, as RF data is associated with metadata. This data can even be represented using XML or an ontology [61].

This new RF data analysis services helps to determine the spectrum utilization capacity of a wireless system. In this way, control can identify spectrum-sharing opportunities. Under spectrum sharing [62], a radio is allowed to use temporarily unoccupied spectrum (white space) if it knows its position and maximum power that could be used at that location without interfering with other systems in place.

V. Stoynov et al. conclude in [55] that the implementation of the latter (RF data analysis) is an excellent way to develop new intelligent algorithms for spectrum analysis for more efficient use of the available spectrum, and for better interference management that gives better transmission quality management. It also envisages more research into the actual use of spectrum in the ISM band through different scenarios, with the aim of accessing these resources more efficiently.

4.6. Multiple Access Protocols

Framing, error control and flow control are provided by data link control, which is responsible for the reliable transmission of the message on the transmission channel. This layer is sufficient for a dedicated link between sender and receiver. Where several stations can access the channel simultaneously, multiple access protocols are needed to reduce collisions and avoid cross-talk between channels, and can also detect or avoid data loss.

In wireless networks, there is no dedicated channel for communicating or transferring data between two devices. Several stations access the medium and transmit data simultaneously, which can lead to collisions. A multiple access protocol is therefore used in these networks. Multiple access protocols can be subdivided, according to the literature, into three categories: Random Access Protocols, Controlled access protocols and Channelization protocols. The taxonomy of existing MAC Half Duplex protocols is shown in Figure 4.2 [63].

4.6.1. Random Access Protocols

No station has priority over another. Each station can send data depending on the state of the medium (idle or busy). In these protocols, there is no fixed time for sending data, and no fixed sequence. They are subdivided into several categories:

- Pure Aloha: When a station sends data, it waits for an acknowledgment. If the acknowledgment does not arrive within the specified time, the station waits a random amount of time, called the backoff time T_b, and resends the data. This reduces the probability of another collision since not all stations wait the same amount of time.

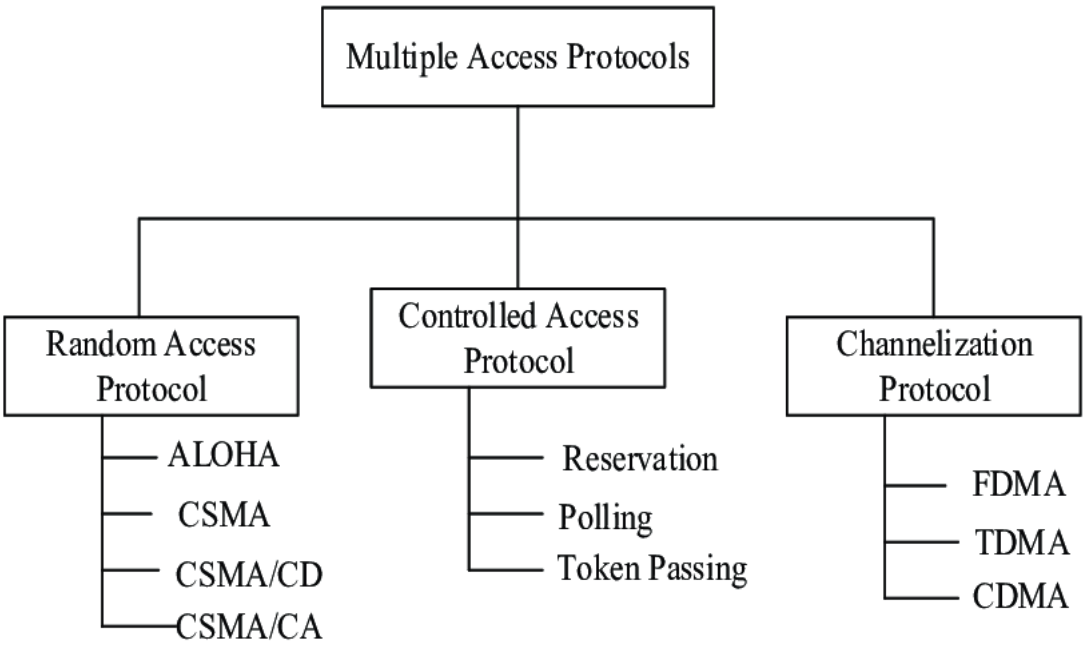

Fig. 4.2. Taxonomy of existing medium access control (MAC) protocols

- Slotted Aloha: In order to improve Aloha, time is divided into slots, so that data can only be sent at the beginning of these slots. If the frame is ready to be sent, the station has to wait for the next slot. This reduces the probability of collision.

- CSMA/CA: This mechanism reduces the number of collisions, by first detecting the medium (whether it's idle or busy) before transmitting data. If the channel is idle, it sends data, otherwise it waits for the channel to become idle. However, the risk of collision is always present in CSMA due to the propagation delay. In fact, if a station starts sending data, the other stations always see the medium free because of the propagation delay, and can also send in their turn. Several modes have been developed to improve this protocol. These include 1-Persistent, Non-persistent, P-Persistent and O-Persistent.

  Figure 4.3 [64] shows the well-known Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol used by 802.11 WLANs. CSMA/CA is used to minimize the probability of collisions on the network by determining the state of the wireless medium. Two carrier detection mechanisms are defined by the 802.11 standard. They determine whether the medium is idle or busy.

  1. Physical carrier detection uses the physical radio interface to sample the wireless medium to detect transmissions.
  2. Virtual carrier detection refers to the use of duration values in a frame's MAC header and NAV timers to virtually determine whether another station is transmitting.

  This protocol is based on three main techniques [64]:

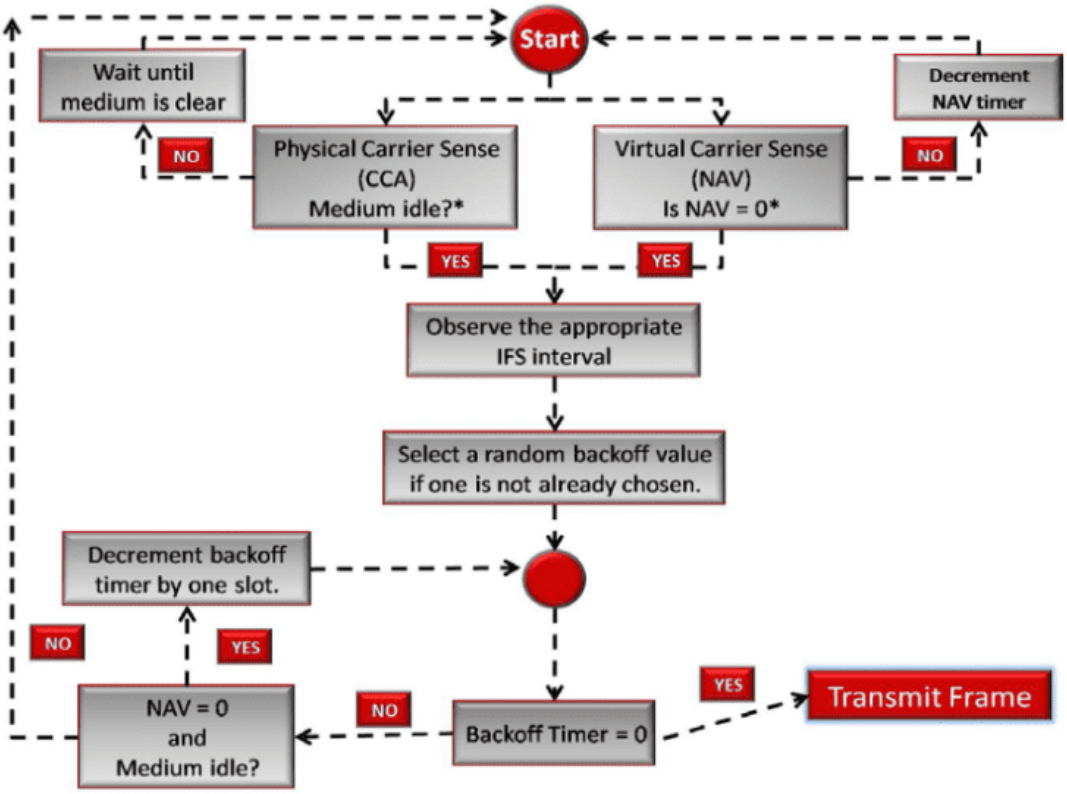

Fig. 4.3. 802.11 arbitration

1. **Interframe space**: The main purpose of this technique is to avoid collisions due to propagation delay. When the medium becomes inactive, sending is delayed for a certain amount of time called inter-frame space or IFS. After this time, a new verification of the medium's inactivity is required. The duration of the IFS depends on the station's priority.
2. **Contention window**: this is a period of time divided into slots. If the sender wants to send data, he waits for a time equvalent to a random number of slots, which doubles each time the medium is busy. and each time he restarts the timer when the channel is unoccupied again.
3. **Acknowledgement**: Data retransmission is necessary if acknowledgement is not received within the time limit.

4.6.2. Controlled access protocols

End devices communicate with each other to find out which one has the right to send a message. In the end, only one node transmits at a time, to avoid collision. The three methods of this category are:

- reservation: A station must reserve before sending data, according to two chronological time periods.

1. A fixed reservation interval divided into slots equivalent to the number of stations. Each slot is in fact a request to send that all stations will read and thus know who will transmit.
2. A frame transmission period that varies according to network strategy.

The reservation method can reduce competition for network resources, thus reducing packet loss. It is adapted to Quality of Service (QoS) requirements by offering different types of reservation for different types of traffic. This ensures that priority traffic receives the network resources it needs, such as bandwidth and latency, to guarantee high-quality performance. This method makes more efficient use of available bandwidth, thanks to the time and frequency multiplexing of reservation requests on the same channel. However, light network loads will cause a reduction in channel capacity and data rate. As a consequence, execution time will increase.

- Polling: In this protocol, a primary station acts as a controller, and the others are secondary stations. All messages must pass through the controller, which sends a broadcast message containing the address of the node selected to grant access. The addressed node responds and sends data where appropriate. If there is no data, a "reject poll" (NAK) message is sent back. However, polling messages cause overhead, in addition to the heavy reliance on controller reliability.

- Token passing: In this multiple access protocol, devices pass a special token to each other to gain access to the communication channel. Data transmission is only possible when the stations hold the token, which ensures that only one device can transmit at a time.

4.6.3. Channelization Protocols

In this protocol, the bandwidth is shared in time, frequency and code to enable several stations to access the channel simultaneously.

- Frequency division multiple access (FDMA): The available bandwidth is divided into equal bands, separated by guard bands so that no two bands overlap to avoid crosstalk and noise. As a result, each station can be allocated its own band.

- Time Division Multiple Access (TDMA): the bandwidth is time-shared between several stations. Stations are allocated their own slots to transmit data. However, the problem of slot synchronization is solved by adding synchronization bits to each slot. Another propagation delay problem is solved by adding guard bands.

- Code division multiple access (CDMA): all transmissions are routed simultaneously. There is no bandwidth or time division. Perfect data reception is only possible if data from different stations can be transmitted simultaneously in different code languages.

- Orthogonal Frequency Division Multiple Access (OFDMA): The bandwidth is partitioned into smaller subcarriers to increase global performance, and data is transmitted via these subcarriers.

- Spatial Division Multiple Access (SDMA): the use of multiple antennas at the transmitter and receiver separates the signals of several users located in different spatial directions. This technique is commonly found in MIMO (multiple-input, multiple-output) wireless communication systems.

4.7. Technology co-existence and interference

We discussed the concept of spectrum sharing in the introduction of this section, under the name of cognitive radio networks. Spectrum sharing or dynamic spectrum access techniques aim to solve the problem of spectrum inefficiency inherent in current static channel allocation policies. However, this technology lacks the intelligence to learn and predict spectrum use and the potential for alternative spectrum use.

Several studies of spectrum analysis or monitoring have been carried out using analytical models or or a real time models. However, they are limited to a certain number of locations or have a short time duration, and have used a single spectrum analyzer, instead of multiple frequency bands.

An approach described in [65] for interference recognition based on the analysis of a large amount of data obtained from long-term spectrum monitoring. The detection of a specific type of interference in the uplink of a 3G network caused by the "ducting" effect. The authors demonstrated that Hjorth's parameters allow large amounts of data to be processed to create a set of Robust Feature Descriptor (RFD), applicable to Cluster Analysis (CA) and to the detection and identification of interference and frequency channels. This approach reduces the dimensionality of the primary parameter space, which can be used to solve problems related to spectrum analysis and detection in cognitive radio systems and networks.

The cloud-based radios is an another technological trend that has emerged recenly. P. Baltiiski et al. in [66] propose cloud-based cognitive radio architectures with long-term spectrum monitoring system. However, this method generates gigantic amounts of data, hence the need for big data technologies and machine learning. This system can be used for spectrum allocation and management In order to avoid collisions, for example. By introducing a frequency-time resource indicator as a measure of spectrum usage, a detailed analysis of spectrum occupancy and usage activity in a predefined frequency band is routed.

Authors in [55] has carried out a study of LPWAN networks operating in the ISM band. Existing studies on LoRa, SigFox and IQRF show that coexistence leads to significant performance degradation. The authors argue that current solutions for the coex-

istence of WiFi networks, WSNs and Bluetooth do not apply well to LPWAN networks, because the vast coverage area of LPWANs can produce an unparalleled number of hidden terminals. The coexistence of different technologies on the same spectrum is a great challenge.

In practice, a device operating in unlicensed spectrum, such as the ISM bands, offers no guarantee of quality of service, and communication is more likely to suffer interference than its limitation by the link budget. Licensed spectrum, on the other hand, is paid for by operators in order to gain operating exclusivity.

There are a number of collision mitigation mechanisms that can be implemented to solve the interference problem generated between sensors belonging to the same LPWAN. Either through regulation (such as LBT or transmitter duty cycle limits), or through voluntary mechanisms such as CSMA / CSMA-CA (discussed in the previous section). However, the latter mechanisms suffer from the problem of spectrum evaluation. This is because channel evaluation at the transmitter does not necessarily coincide with channel conditions at the target device.

4.8. Conclusion

The radio frequency spectrum is becoming increasingly crowded, and RF signals are likely to become more numerous. This is particularly true for frequencies in the ISM spectrum bands, originally reserved for industrial, scientific and medical purposes. In many emerging communication systems, including IoT networks such as WPAN and LPWAN, this part of the spectrum is used. Understanding electromagnetic interference is essential, not only for electronics and telecommunications professionals, but also for anyone who uses technology on a daily basis. In this chapter we've explained what electromagnetic interference is, how it can affect devices and why it's important to manage it [67].

5. FT-CSMA: A FINE-TUNED CSMA PROTOCOL FOR LORA-BASED NETWORKS

5.1. Introduction

Wireless networks have become ubiquft-csmaitous in diverse applications, yet their limited frequency range necessitates using a single transmission medium or channel. Consequently, multiple nodes share this same channel, which can result in collisions and potential data loss. As a result, data loss remains a significant concern within wireless networks. To avoid this problem, network communications use the CSMA method to detect channel occupancy by measuring the carrier's Received Signal Strength Indication (RSSI). In LoRa-based networks, the CSMA protocol is a commonly used medium access control mechanism. However, it has been noted that this protocol may not be very efficient, this is because the receiver can detect signals even when they are below its noise level. Therefore, it is evident that the limitations of the CSMA protocol in these situations are quite significant. Furthermore, due to the orthogonality of LoRa signals with distinct Spreading Factors (SF), i.e., transmissions employing several SFs in the same channel, LoRa technology uses the Chirp Spread Spectrum (CSS) modulation approach. Wireless communication employs the Channel Activity Detection (CAD) strategy to avoid collisions.

Our contribution is to propose an optimized technique for minimizing collision occurrences in Lora networks. This technique has been optimized and integrated as a new module and component in the NS3 simulator. This technique, called FT-CSMA, is based on the CSMA mechanism used in WiFi IEEE 802.11 and WSN IEEE 802.15.4.

Recent studies have delved into various strategies to reduce collisions in LoRa networks, which have emerged as a promising technology for Internet of Things (IoT) applications. In this context, this study proposes a technique called FT-CSMA that aims to enhance the reliability of LoRa networks. The proposed method optimizes carrier detection time, which is a critical factor that determines the network's ability to transmit data successfully. By reducing collisions and improving the network's reliability, FT-CSMA can help address the challenges associated with IoT applications that require low-power, long-range communication.

Moreover, the proposed technique is compatible with the existing LoRaWAN protocol, which can facilitate its adoption by network operators and device manufacturers. Based on the data given in Table 5.2, our protocol offers faster sensing time compared to other algorithms, synthesized in Table 5.1, such , LoHEC , and the three LMACs. Our technique requires no synchronization messages to stabilize LoRa networks. This sets it apart from the strategy and FCA-LoRa, which generate more control messages, leading

to network overload. Additionally, our methodology has a minimal impact on latency. It is important to note that improving one network performance factor may affect others, such as energy consumption, packet delivery ratio, and delay. However, the delay was significantly affected by all other proposals made as part of this study, which is different in this research. FT-CSMA tests achieved a 5% increase in packet delivery ratio through incremental enhancements and adjustments and a 2% reduction in energy consumption compared to the original LoRa methodology. FT-CSMA has the potential to significantly improve the performance of LoRa wireless communication systems while maintaining optimal energy efficiency.

These findings leave no doubt about the game-changing potential of FT-CSMA, which is set to disrupt the industry and establish itself as the go-to solution for reliable and sustainable wireless communication.

5.2. Collision managment

It's worth noting that collisions can arise from various signals, not just LoRa. However, this research delves explicitly into collisions caused by LoRa signals, a topic that has yet to receive much attention. In this section, we'll introduce the main LoRa mechanisms and features that ensure stable and dependable transmission.

To avoid collisions, the LoRa modulation technique utilizes CSS by splitting the channel in different ways called "Spreading Factors" (SF). These SFs are orthogonal, which means multiple signals using different SFs can be sent simultaneously without any interference. However, if two packets with the same SF arrive on the same channel simultaneously, they may collide. This collision can be prevented if one packet is at least six decibels (dB) stronger than the other.

ADR also indirectly helps to avoid collisions. To ensure reliable node access to the network with low energy consumption. It controls the nodes to operate with a better distribution of SF. This reduces collisions considerably [68].

The Industrial Scientific Medical (ISM) bands are limited, and many communities use them. Therefore, so as not to abuse their use, the European Telecommunications Standards Institute (ETSI) recommends the duty cycle to alleviate the capacity of networks. For example, the regulations of the 868 MHz ISM band recommend and limit the duty cycle to 0.1% or 1%, depending on the selected sub-band. It consists of not using the same sub-band for a limited time [69].

$$T_{off} = \frac{ToA}{Dutycycle} - ToA \tag{5.1}$$

If a LoRa frame takes a Time on Air (ToA), then the device must not communicate during a Time of Toff. These constraints offer adequate sharing of resources and minimize intra- and inter-network collisions. The above features, mechanisms, and requirements do not

entirely prevent collisions. In addition, the use of the Channel Activity Detection (CAD) mechanism, recently integrated into the LoRa modules, can help avoid collisions. This mechanism will be detailed afterward.

5.2.1. Carrier-Sense (CS) Principle

The reason why LoRa does not use the existing carrier sense (CS) mechanism is not apparent. This section highlights the difference between previous CS mechanisms, namely ALOHA and CSMA, and the LoRa CAD mechanism. Especially the properties of LoRa signals that influence the choice of this mechanism. Besides these reasons, a brief explanation is required of these CS mechanisms because almost all the works cited in the state of the art derive from them.

5.2.1.1 Aloha

It was the first Protocol to communicate over wireless media. Its principle is simple: as soon as a packet arrives, the node transmits it. It is pure Aloha (P-ALOHA). This protocol leads to huge collisions if the network is important, mainly because of overlapping packets. Another derived Aloha, called Slotted Aloha S-ALOHA, improves the first one:

- It uses frames of the same size;
- The time is divided into equal synchronized slots;
- Each frame is transmitted at the beginning of each slot as soon as it arrives;
- If a collision occurs, the Device attempts to transmit the frame at the next slot until success.

The synchronization of time slots necessarily requires a control system. In LoRaWAN, the Network server, through a gateway, plays the controller role. All this is possible if the nodes are of class B or C, which can receive commands from the gateway periodically. However, for class A, it is not possible. Because the LoRa node opens only two short periods after transmitting a message. i.e., the node is not visible to the gateway until it sends.

Despite their simplicity, synchronization and retransmissions generate more traffic and, therefore, more collisions. In addition, it is necessary to acknowledge them. As a result, gateways create more traffic and, therefore, more collisions.

5.2.1.2 CSMA in IEEE 802.11

IEEE describes two CSMA processes: the Distributed Coordination Function (DCF) and the Point Coordination Function (PCF). This study discusses only the basic DCF, where

acknowledgment is not mandatory. Two concepts are the basis of the DCF operation: The back-off Exponent and the DCF Inter-Frame Space (DIFS) time.

1. DIFS: It is a fixed part starting the waiting time before each transmission attempt, which is equal to $50\mu s$;
2. Back-off scheme: Consists in choosing a random number between $[0, CW - 1]$ where $CW = 2 * k$, and k is the number of attempts. A calculus of the back-off time from this number is as follows: $Back{-}off_{Time} = rand(0, CW{-}1) * SlotTime$. where $SlotTime = 20\mu s$. After each transmission failure, the CW window doubles until it reaches its maximum. A reset of the CW follows each successful transmission. Alternatively, when the number of attempts reaches its maximum. This method uses the Back-off two times when a medium is busy or when a device does not receive an acknowledgment;
3. Distributed Coordination Function (DCF) operation: There are two modes in DCF. The basic one and the one using RTS/CTS. In the primary mode:
   - The node that wants to transmit checks if another node is transmitting on the channel;
   - If the channel is idle for a DCF Inter-Frame Space (DIFS) Time, it transmits;
   - Otherwise, it waits for the end of transmission, followed by a DIFS, and then generates a Back-off time. This time is decremented as long as the channel is idle during each DIFS; if, in the meantime, the channel becomes busy, then the counter freezes and continues to decrement when the channel becomes idle again during a DIFS. The transmission will be done only if the counter reaches 0;
   - If a collision occurs, then the CW window doubles.

5.2.1.3 CSMA in IEEE 802.15.4

If the device is ready to transmit, it immediately starts Back-off, randomly selecting several back-off periods in the interval. The duration of each back-off period is 0.32 ms. Once the Back-off time has expired, it detects the carrier. If the channel is idle, the device transmits its frame. If the channel is busy, the back-off exponent BE increases by 1, and a new number is selected in the new range .The device restarts the Back-off, followed by carrier detection until the maximum number of attempts is reached.

5.2.1.4 RSSI and SNR

To show that the CSMA mechanism, based on the signal power, is infeasible. Table 2.2 [70] contains the Signal over Noise (SNR) of each SF that a LoRa module can tolerate to receive the signals correctly.

These values show the possibility of demodulating the LoRa signal up to 100 times below the noise floor for SF12 ($-20dBm$). In other words, detecting a high-powered signal does not necessarily mean the channel is busy. The negative SNR means that the signal strength is less than the noise strength, and the demodulator can still decode it. However, if the negative value is less than the minimum SNR of $-20dBm$ at SF12, it does not guarantee that the receiver will be able to demodulate the signal.

Another particularity of LoRa is the ability to decode partially superposed frames. The study done in [71] shows that the LoRa receiver can decode a frame, partially overlapped with another one, as long as at least six symbols remain non-overlapped;

5.2.1.5 LoRa CAD mechanism

The entire range of LoRa SX126X and SX127X radio components implements CAD. It is a simple Listen Before Talk (LBT). The principle is to detect the occupancy of the channel by the presence of a preamble of a transiting signal on the same channel having the same SF (in the case where the likelihood of a collision is maximum). This takes minimal time and reduces energy consumption [72]. In the range SX128X of LoRa and above, these modules can also detect the data payload by extending the time. The flow chart below, Figure 5.1 explains the CAD operation [38].

If enabling CAD, packet transmission is only possible after a CAD operation. If a device detects a preamble, it skips until the next time by waiting a random time (Back-Off) and tries again using the same procedure.

5.3. Related Work

Several authors have tried to improve the CAD concept by the CSMA mechanism or channel/SF hopping approach.

T. H. To and A. Duda [69] created a module in NS3 with a custom CSMA. Even if the CAD and how its Clear Channel Assessment (CCA) works are not referred to, it offers two CSMA techniques, CSMA and CSMA-X, close to the CSMA in IEEE 802.15.4 that is used in WSN. Only the CCA time is fixed, and the back-off time is randomly chosen.

C. Pham gives a brief comparison, in [73], between the basic CSMA in IEEE 802.11 designed for wifi and the one in IEEE 802.15.4 intended for WSN. Due to the nature of WSN, where there is no coordinator, it adapts the first one for LoRaWAN networks, $CSMA^{LoRa}_{802.11}$. Its principle is to define the times used in CSMA regarding the time of a LoRa symbol. As the latter is a function of the SF and the BW then DIFS, SIFS, and the back-off will depend on it. $DIFS = 9CAD$, $SIFS = 3CAD$, CW from $18CAD$, and double up to $144CAD$. It claims that this adaptation of CSMA for LoRa is not reliable. The author proposes another one called, $CSMA^{LoRa}_{new}$, where the DIFS is based on the maximum ToA. This means a 255-byte packet sent with SF12 is equivalent to $9150ms$. During

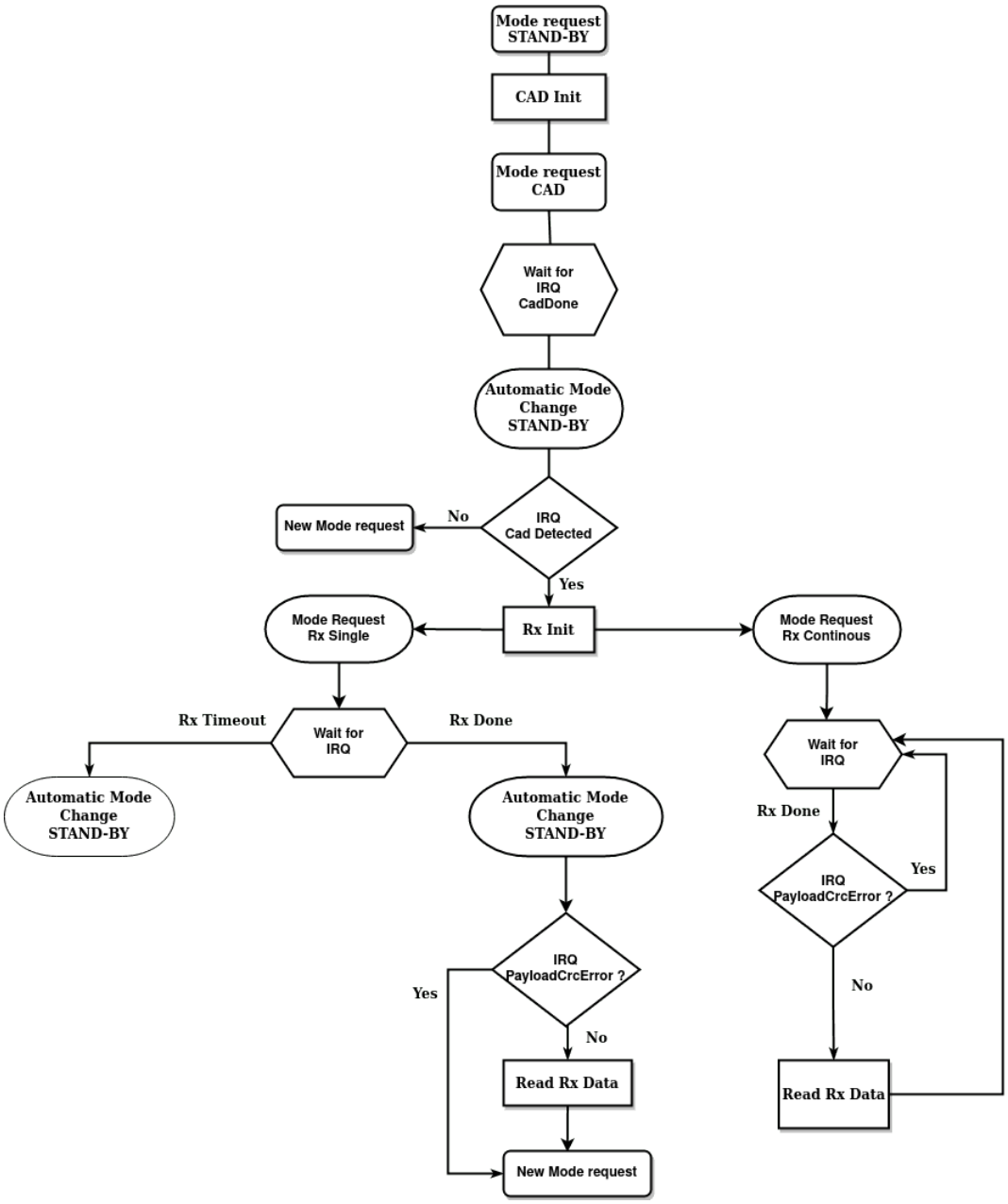

Fig. 5.1. LoRa CAD Flow [38]

this time, DIFS(ToAmax), 9CAD operations are performed with a duration of 1000ms. With this configuration, One CAD will be performed every 1143ms in the case of SF12. The Back-Off of this version is constant and takes ToAmax. Despite the effort put into his work, the author only compares the energy consumption between his two proposals, except for the explanation that the reliability and energy efficiency of $CSMA^{LoRa}_{new}$ against $CSMA^{LoRa}_{802.11}$. In addition, the results in terms of quality of service are not reported.

J. Liando et al. [74] proposed CSMA-CAD. The authors claim that two symbols are sufficient for the duration of a CAD. His state diagram shows that if, after one CAD, the channel is busy, then it takes another SF randomly. It achieves a 20% improvement in PDR at the expense of an energy loss of around 1.70mJ. It also testifies that an ideal

CSMA can increase throughput by up to 56X compared with its CSMA-CAD.

L. Beltramelli et al. [75] studied the performance of three-channel access methods. Pure Aloha, Slotted Aloha, and Non-Persistent CSMA by proposing a probabilistic analytical model for the distribution of nodes around a gateway and their possible interferences. With the support of simulations done in MatLab, they confirm that:

1. These methods, respectively, improve the throughput in the case of a large enough number of nodes;
2. S-ALOHA is more reliable than P-ALOHA at the expense of energy in the case of a small number of nodes;
3. CSMA is the most reliable and energy-efficient only if the nodes are close to the gateway and have a small SF.

N. Kouvelas et al. [76] model their p-CARMA with Markov chains. Every event is launched by probability, even the CAD operation. The operation's duration depends on several symbols, as Table III shows. While the back-off time, also executed with a probability, is randomly chosen between 0 and the ToA of its packet load. During back-off, the device does not detect the channel but goes into sleep mode. In this model, three probability values must be defined. The probability of generating and transmitting a frame, finding the channel busy or idle, and a probability that depends on the number of nodes. Depending on the values of these probabilities, three versions of p-CARMA are compared with the ALOHA standard. It shows a performance of 20% in PDR and a gain of around $0.48J$ in energy.

Pham and M. Ehsan. proposes, in [77] an approach that is totally different from the others. It introduces additional messages called RTS, carrying only the size of the future packet to be sent. The node wishing to transmit makes a back-off, sends an RTS, and finally listens to the other RTSs. If the channel is idle, it transmits; otherwise, it repeats the previous steps. He claims this approach reduces collisions from the outset and provides no guarantee for PDR, despite results showing a reduced battery life from 1265 to $1031 days$.

A. Triantafyllou et al. [78] have presented their new and improved methods of accessing the FCA-LoRa medium. Its principle is to schedule and synchronize the nodes' transmissions through the gateway by broadcasting beacon frames. With simulations made in OMNeT++, he claims that his method can improve the throughput by up to 50% in the case of a gateway and many nodes up to 600 and that with several gateways and $500 nodes$, it reaches 49% more throughput. In the paper, the nodes can only transmit after receiving a beacon frame. However, this mechanism is only feasible with LoRa classes B or C. In these classes, the node periodically opens a short reception window (class B) or continuously (class C). In this way, the nodes can be located and possibly receive frames. In all cases, its graphs show improvements in energy efficiency and QoS.

C. Shao and O. Muta, claim in [79] that the network is heterogeneous Due to the multiplicity of SFs. The paper proposes a CSMA-like protocol called LoHEC based on CAD. It aims to improve energy fairness between nodes. In LoHEC, the end devices perform several CAD operations NSF spaced by CAD intervals to access the channel. This protocol mainly aims to determine CAD intervals based on energy consumption under different SF. The results show that LoHEC can improve energy fairness by 0.6 to 0.8 times compared to other solutions. However, the multiplicity of SFs in LoRa is never considered heterogeneous. On the contrary, their orthogonality and diversity are the key elements of this technology that improve communication capacity. Moreover, in the literature, the times used by the CAD operation are calculated in terms of the time of a symbol, which depends on the SF and the BW.

S. H. Alonso et al. [80] introduced the Longest First Slotted CSMA (LFS-CSMA). By combining S-ALOHA and CSMA, they define the time of the longest frame as the time slot. The main feature is the delay in transmitting the frames, so they finish just at the end of the time slot. In this configuration, the longest frames will be sent first. The other competing frames, which are less long, will listen to the channel with the CAD mechanism before transmitting. They give probabilistic analytical models for P-ALOHA, S-ALOHA, and their LFS-CSMA to prove their proposals. The comparison between the latter in terms of performance shows an improvement in their proposal. Nevertheless, the studies done by operating with a single SF are restrictive and demonstrate the performance of only one part of a network. It remains to be seen what the results and overall performance of a network operating with all possible LoRa SFs would be.

A. Gamage et al. [81] adopted the basic CSMA DFS for his LMAC-1. He sets the DIFS to $12CAD$ operations and a random back-off (BO) between 4 and 64 times the duration of a successful CAD. With the same parameters, he proposes a second LMAC-2. It only switches to another channel/SF in the latter when DIFS or BO fails. This switchover is based on information gathered by the nodes during previous CAD operations. Both proposals are ideally suited for LoRa Class A. For class B, he proposes LMAC-3, an improved version of LMAC-2. The information collected by the nodes is replaced by beacon messages from the gateways. These contain statistics on the channel/SF. Real-life tests show a good improvement in QoS and energy for class A. For class B, delivery stabilizes at 90%, with the lowest energy consumption of all methods.

F. Yu et al. [82] propose a study of the CAD operation itself, which is worth mentioning here. They found that a CAD can detect the channel occupancy of another signal with different SF and BW in the narrow bands, leading to false positives. False positives occur when these signals have the same slope in the time-frequency domain, coinciding with a doubling of the BW and an increase in the SF by two values. They argue that the CAD is based on cross-correlation for carrier detection. They propose LoRadar, a cross-channel scanning method that distinguishes the effective channel based on the distribution of results collected during many successive $7*CAD$. The duration of the CAD itself is reduced to one symbol and preceded by RSSI measurements to lend credibility to the distribution.

This LoRadar (Scan) mechanism achieves accuracy with a detection time reduction of 90% compared to the CAD mechanism.

5.4. Materials and methods

Table 5.1 distinguishes the parameters used in the previous CSMA proposals cited in the related work section. Despite all these results, collisions persist, and the need for a new approach continues.

Based on the documentation provided in the previous section and according to the parameter Table 5.1, the list above summarizes the main constraints that a new CSMA protocol has to overcome:

- The time required for a CAD operation does not guarantee the absence of a signal in transit;
- CAD operations can lead to false positives;
- Increasing the number of CAD operations also increases energy consumption;
- A random mechanism is needed to separate the times between concurrent nodes;
- Channel detection periodically during the back-off time only increases energy consumption.

5.4.1. Design and Implementation in NS3

Based on discrete events, we chose the NS3 network simulator to design and test our project open-source software, licensed under the GNU GPLv2, designed for teaching and research . Several implementations of LoRaWAN modules exist in NS3 [83]. The LoRaWAN module from David Magrin signetlabdei/LoRaWAN chosen for testing does not implement CAD. ALOHA is the basic protocol used. Our contribution is to add the CAD operation to this module to test the performance of the LoRaWAN network with CAD carrier sense in terms of quality of service and scalability. These tests led us to propose the so-called FT-CSMA.1, a simple CSMA collision avoidance mechanism. Finally, the implementation of the CSMA proposed in [81] allowed us to propose the final FT-CSMA, an amalgamation between the CSMA of WIFI in 802.11 and WSN in 802.15.4. In addition, with these modifications, all the suggestions proposed and cited in recent works can be tested and improved. In particular, the addition of other high-performance CSMA mechanisms. The following details the FT-CSMA proposal's temporal sequence.

Ref	Year	CSMA	CS Duration	Back-off/CW	Environment	Results
[69]	2018	CSMA CSMA-X	CCA $CCG = 10ms$	$T_{sf} = rand(0, 2^k - 1)$ $T_{offset} = 1s$	Framework +NS3	Lower collision and energy consumption
[73]	2018	$CSMA^{LoRa}_{802.11}$ $CSMA^{LoRa}_{new}$	$9 * CAD$ Sequence $9 * CAD$ at ToA_{max}	$18 - 144 * CAD$ Expo ToA_{max} Fixe	Framework	Energy efficiency, collision avoidance
[74]	2019	CSMA-CAD	1 CAD = 2 symbols	$SF = rand(7, 12)$	Simulation	+ 20% PDR 56 x throughput
[75]	2020	NP-CSMA	1 CAD = 2 symbols		MonteCarlo	Improve throughput with small SF
[76]	2020	P-CARMA	P * CAD $P\epsilon[0..1]$	$T_{sf} = rand(0, ToA)$	Framework +NS3	+ 20% PDR - 0.48J energy
[77]	2021	RTS msgs	$7 * T_{preamb} + ToA_{RTS}$	$7 * T_{preamb}$	Framework	Reduce collision, Battery life 234days
[78]	2021	FCA-LoRa	GW Synchron Beacons broadcast		OMNeT++	+(49-50)% throughput
[79]	2022	LOHEC	$N_{sf} = \frac{N * E_{min}}{E_{sf}}$ CAD	$T_{sf} = \frac{T_{min} * E_{sf}}{E_{min}}$ $T_{offset} = rand(0..T_{sf})$	Framework	Improve energy by 0.6 – 0.8 times
[80]	2022	LFS-CSMA	$Slot = ToA_{max} + T_g$ Fr Algin at End Slot	Next Slot	Analytic	Improve QoS, energy
[81]	2022	LMAC-1 LMAC-2 LMAC-3	$12 * CAD$	$4..64 * CAD$ Auto select channel Select Channel by Ack	Framework	+90% PDR in Class B with the lowest energy consumption
*	2023	FT-CSMA	$1CAD$	$rand(1, 3) * CAD$	NS3	+ 5% PDR +2% energy

TABLE 5.1. RECENT CSMA PROPOSAL PARAMETERS

5.4.1.1 CAD/FT-CSMA operation time

According to the Semtech documentation quoted in "CAD Mechanism" section, the CAD time should be:

$$T_{CAD} = T_{symb} + \frac{32}{BW} \tag{5.2}$$

where: $T_{symb} = \frac{2^{SF}}{BW}$ Another technical document [39] describes the ideal detection

time as 1, 2, 4, 8, or 16 symbols. Almost half of this time defines the RX reception mode. However, in the Datasheet [38], the time of the CAD operation depends on the SF. Table 5.2 clearly demonstrates that in order to ensure accurate preamble detection and prevent false results, it is imperative to subtract several symbols. This study adopts this configuration in both implementation and testing. This is an adequate time for this type of operation. The abuse of using several CADs to ensure carrier detection is energy-consuming.

Spreading Factor	number of symbols
7	1.92
8	1.78
9	1.75
10	1.77
11	1.80
12	1.85

TABLE 5.2. CAD DURATION IN TERM ON SF

In [77], non-detection of the carrier, even if it exists, does not mean a false detection. Only sometimes, this solution misses avoiding a collision. What is important is that if the detection is positive, then it is sure there is a signal in the air. This choice meets criterion number 1. False-positive results for the second criterion are avoided using one of the three basic frequencies of the exclusive 125kHz bandwidth specified by regulation [43] 868.10 MHz, 868.30 MHz, 868.50 MHZ.

5.4.1.2 CAD/FT-CSMA waiting time (Back-off)

After the CAD operation, the channel can be busy or idle. When busy, the device waits to restart the CAD until the channel becomes idle to transmit. As all messages sent, this time must follow the duty cycle regulation, which is 1% in our case. However, nothing in the documentation specifies the value of this waiting time.

To avoid overlapping frames. We choose T_{bk} as the back-off time, with the highest ToA value corresponding to the highest SF value SF12. To satisfy the fourth and fifth criteria, it is best to add an additional Time $B * T_{CAD}$ to the Back-off. Where B is a random number from 1 to 3 $B = rand(1, 3)$. And T_{CAD} is the time of the CAD operation itself. Finally, back-off time is

$$T_{Backoff} = T_{bk} + B * T_{CAD} \tag{5.3}$$

All of these times ensure the end of transmissions of frames operating with large SF and therefore long ToA. Above all, to avoid any possible synchronization between nodes that are competing on the channel. The back-off time T_{bk} is calculated according to the payload used in the simulations and not LoRa's maximum payload of 255 bytes.

The LoRa modem has two types of packet format: explicit and implicit. The explicit packet includes a short header, a code rate and an optional CRC. Figure 5.2 shows the packet format [39].

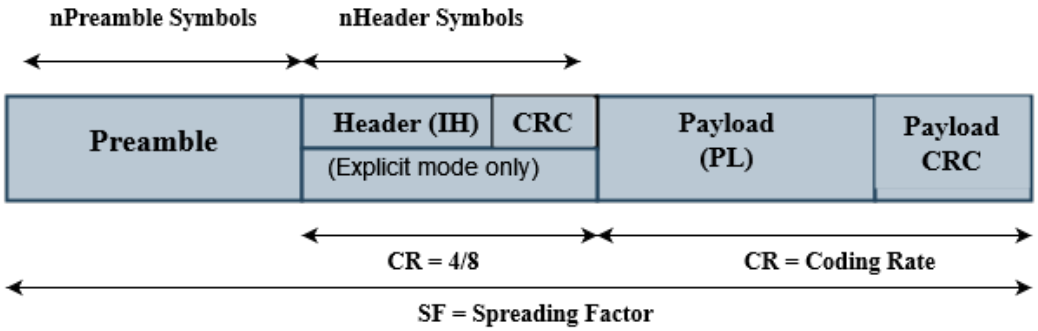

Fig. 5.2. LoRa packet

Equations (5.4 - 5.7) from the data sheet [39] are used to calculate T_{bk}, which is defined as the highest ToA.

$$ToA = T_{preamble+T_{payload}} \tag{5.4}$$

$$T_{preamble} = (n_{preamble} + 4.25) * T_{symb} \tag{5.5}$$

$$T_{payload} = n_{payload} + T_{symb} \tag{5.6}$$

$$n_{payload} = 8 + max(\left\lceil \frac{8PL - 4SF + 28 + 16CRC - 20IH}{4(SF - 2DE)} \right\rceil (CR + 4), 0) \tag{5.7}$$

where:

- $8 \leq n_{preamble} \leq 255$;
- PL the simulation payload size 12/24 bytes;
- SF the spreading factor, $7 \leq SF \leq 12$;
- $IH = 0$ Header enabled, 1 otherwise;
- CRC the Cyclic redundancy check in bits;
- CR the coding rate.
- $DE = 1$ LowDataRateOptimize=1, 0 otherwise

Note that the device does not periodically detect the channel during the back-off time but only at the end. This is the principle used in WSN networks. Testing will be done first on T_{bk}, a fixed Time; second, on a specified waiting time defined in terms of the number

of symbols; and third, on a random time. In all cases, the device transmits directly after detecting a free channel with CAD or waits for another Back-off time, whether random or fixed.

5.4.1.3 CAD/FT-CSMA energy consumption

During the whole CAD operation, the node must take on two modes. The CAD mode detects the preamble, followed by the reception mode (Rx) to detect the data symbols. The latter takes a very short time to reduce the power consumption. The device is considered to be in standby or sleep mode during the back-off time. The table on [38] page 45 gives a power consumption of $6mA$ in CAD mode and $11.5mA$ in Rx mode. These measures are correct when a LoRa device operates in $125kHz$ bandwidth. Nevertheless, in the SX1261/2 series, in the CAD mode, the devices detect the LoRa preamble or data, while the previous series could only detect LoRa preambles. To generalize the implementation and cover all ranges of LoRa devices, nodes are set to CAD mode for half of the CAD operation time and the other half in RX mode. The Table 5.3 below summurize the power consumption.

Module	Rx (mA)	CAD (mA)	STB(mA)
SX1272	10.8	5.6	1.5
SX1276/7/8/9	11.5	6	1.5

TABLE 5.3. LORA CAD CONSUMPTION

Therefore, the power consumption when operating at 125 kHz, is:

$$E = E_{CAD} + E_{Rx} \tag{5.8}$$

$$E = T_{CAD} * P_{CAD} + T_{Rx} * P_{Rx} \tag{5.9}$$

With the assumption that the times of both modes are equal $T_{CAD} = T_{Rx} = T$, then:

$$E = T * (P_{CAD} + P_{Rx}) \tag{5.10}$$

Finally: $E = T * (6 + 11.5)$, then: $P_{total} = 17.5mA$.

For FT-CSMA, the additional Back-off time is in standby or sleep mode. The device is set to standby mode despite consuming more power than sleep mode. This is because, firstly, the duration is low; secondly, the device can perform CAD-back-off operations several times; and thirdly, for generalization reasons.

When the device tries to transmit, there are two possible situations: the device may never run the Back-off, and then consumption is:

$$START_P = P_{total} = 17.5mA$$

. Or it runs one or three back-offs, so consumption is

$$Min_P = P_{total} + 1 * P_{standby} = 17.5 + 1 * 1.5 = 19mA$$

$$Max_P = P_{total} + 3 * P_{standby} = 17.5 + 3 * 1.5 = 22mA$$

The average consumption is, therefore, $20.5mA$. The device repeats this step without exceeding the Duty Cycle, so it aborts the transmission, or the channel will be idle with a successful transmission.

5.4.2. Implemented Algorithm

The CAD algorithm in the flowchart cited in the previous section Firuge 5.1 needs to mention the duration of each step. It is very technical, and its implementation concerns the LoRa module framework. The FT-CSMA algorithm below contains a simplified CAD version tagged with the necessary time for each stage. Note that the Semtech data sheets do not indicate the duration of the Back-off. It is better to wait for a random time without specifying exact values.

After explaining the choice of parameters for our new FT-CSMA method: the CAD waiting time, the back-off time after a busy channel, and the energy consumed in each stage, it's convenient to conclude the work with the following algorithm:

Algorithm 1 FT-CSMA algorithm with Simplified CAD

Require: Packet to send
Require: In STANDBY or In Sleep
1: $T_{tr} \Leftarrow 0$
2: run CAD ▷ $T_{CAD} = n \times T\,symbol$
3: $T_{tr} \Leftarrow T_{tr} + T_{CAD}$
4: **while** Channel busy and $T_{tr} \leq DC$ **do**
5: BackOff ▷ $T_{BackOff} = rand(1,3) \times T_{CAD}$
6: run CAD ▷ $T_{CAD} = n \times T\,symbol$
7: $T_{tr} \Leftarrow T_{tr} + T_{CAD} + T_{BackOff}$
8: **end while**
9: **if** Channel idle **then**
10: Transmit
11: turn to STANDBY
12: End
13: **end if**

It starts with an initial CAD operation before entering the while loop to avoid unnecessary back-off. The (n) here, in the comment, is the number of symbols the CAD operation should take according to Table 5.2 configuration. Note that another component ensures the algorithm termination, which calculates the transmission time T_{tr} and compares it with the duty-cycle DC, also implemented at the MAC level of this module.

5.5. Results and discussion

We used simulator NS3 version 3.37. It offers a wide range of propagation models. All simulated scenarios use Log Distance Path Loss with a Path-Loss Exponent (PLE) of 3.7, corresponding to urban areas. It also uses several mobility models. However, with the activation of ADR, the standard suggests static devices [84]. Therefore, constant mobility is our choice.

5.5.1. Device Locations and SF Distribution

The node's distributions are uniformly within a disc of radius 6400m. Since the goal of CAD is to improve packet delivery by avoiding collisions, the simulation should run on many nodes. Furthermore, taking the simulation results after sending at least 20 periods is preferable. This precaution ensures that the CAD mechanism is operational even after the nodes have converged to the SF, Data Rate (DR), and stability frequency. The nodes automatically achieve this convergence either with the Adaptive Data Rate ADR mechanism or the LoRa LowDataRateOptimize mechanism.

Figure 5.3 shows the position of the nodes and their SFs at the start of the simulation; two black spots mark the two gateways. Figure 5.4 shows the same nodes with new SFs after 20 simulation periods. The nodes closest to the gateway take the SF7 value, marked with red dots, while those furthest away take the SF12 value, marked with a blue(x) sign.

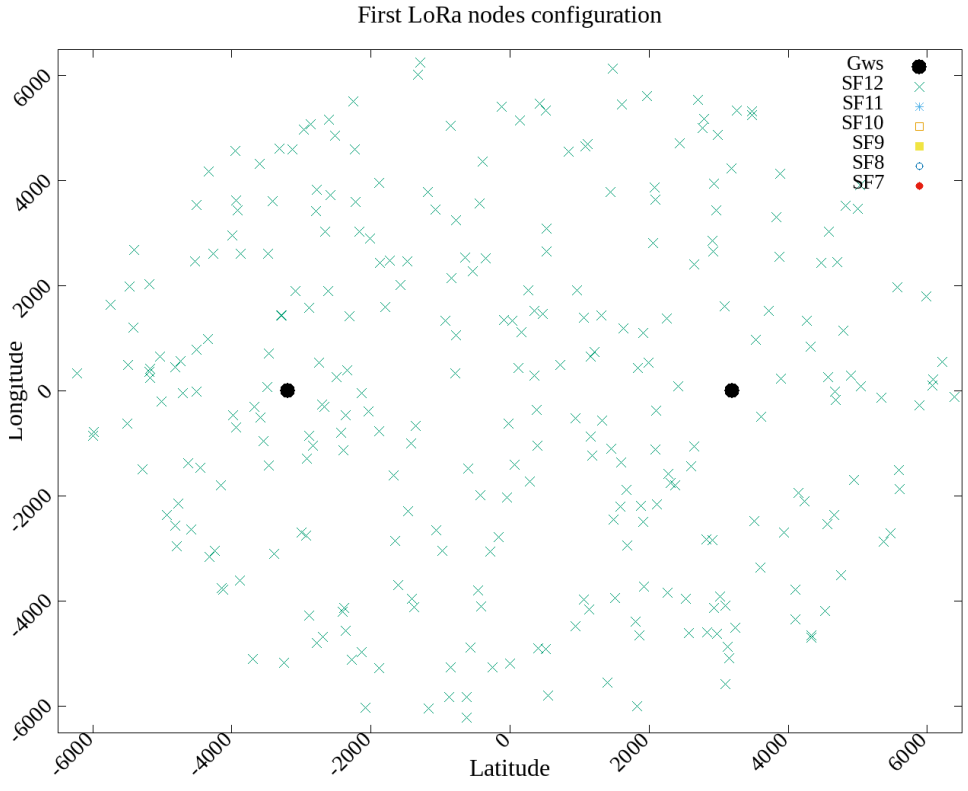

Fig. 5.3. Initial Nodes State

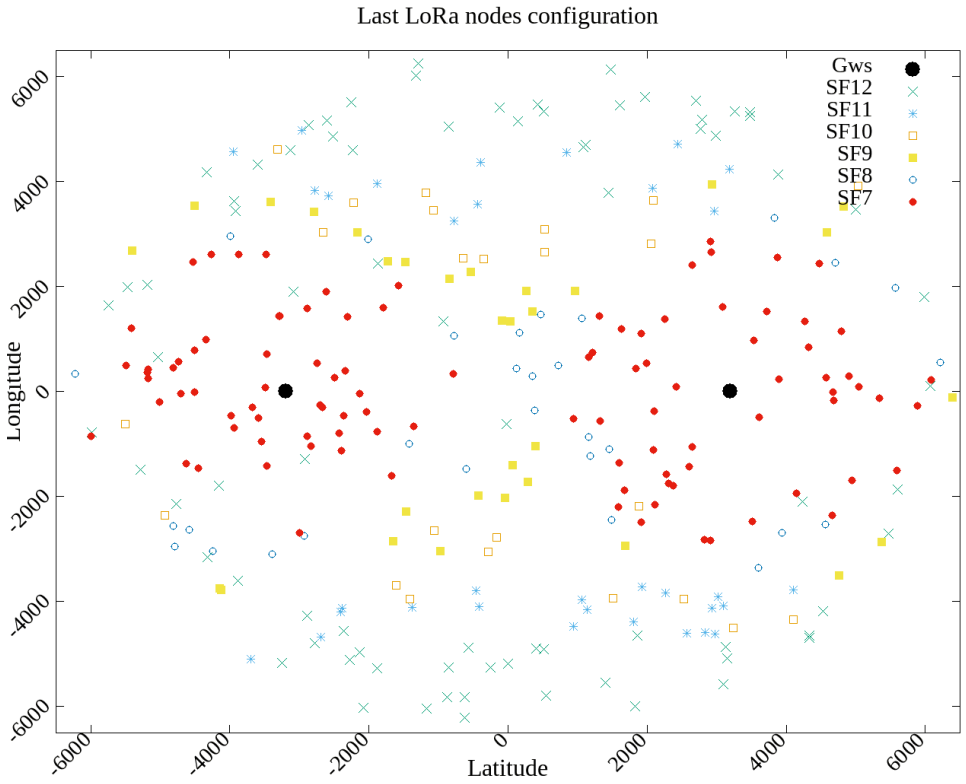

Fig. 5.4. Convergence Nodes State

In other words, to ensure reception, messages must arrive with an RSSI higher than the gateway's sensitivity and with an acceptable Signal over Noise Ratio (SNR) as shown in Table 2.2.

In energy terms, power consumption increases with distance since the ToA transmission time doubles as the SF increases, forcing distant nodes to operate with high transmission power Tx, therefore, more energy, to ensure link stability, as shown in Figure 5.5.

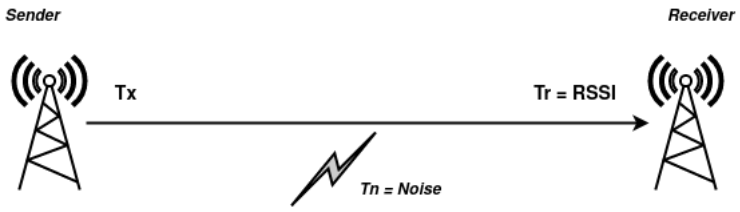

Fig. 5.5. LoRawan link budget

5.5.2. Simulation Scenarios

Another MAC protocol is implemented. S-ALOHA in NS3's LoRaWAN module for validation and comparison. For a given application, the LoRa nodes deployed are generally equipped with the same sensors, i.e., they send messages of the same size. In this context,

S-ALOHA is a suitable candidate and easy to implement. For simplicity's sake, the slot synchronization module is omitted. S-ALOHA time slots are also the maximum ToA as the previous CAD back-off time $T_{slot} = T_{bk}$.

To explore LoRa's scalability, from one hundred to a thousand nodes are uniformly distributed randomly (with constant density) within a disc of radius $6400m$. Table 5.4 below summarizes the main parameters used in the simulated scenarios. Nodes generally have a sensor that collects data in the order of a few bytes. Therefore, 24-byte or 12-byte packets are perfectly suitable for testing.

Parameter	Value
Propagation	Log distance (PLE=3.7)
Environment	Line of the site (Free space)
Mobility	Constant (Uniform in a disc)
Radius	6400 m (Disc surface)
Transmission range	3200m - 9600m
BW / SF	125 kHz / 7-12
Type of traffic	CBR
Packet Size	12 - 24 Bytes
Simulation Time	180s x 20 periods
Gateways / Nodes	1-5 / 100-1000
Back-off Time	$1.15507s, 1.48275s, T_{bk} + rand(1,3) * T_{CAD}$
T_{bk}	Max (ToA) with simulated packet payload
Rand	Uniform Random Variable with timestamp seed
ADR / CAD	Enabled / Enabled

TABLE 5.4. SIMULATION PARAMETERS.

Using this basic implementation, also one of the proposals cited above in state of the art is implemented, like LMAC in [81]. A discussion on this work is at the end of this section.

5.5.3. Impact on QoS

Packet Delivery Ratio (PDR) and Delay are the leading measures of Quality of Service (QoS). Gateway loads with a large number of nodes increase collisions. This is when PDR starts to fall, and CAD shows its effect. We cannot display all simulation results here, from 1 to 5 gateways. Only the 1-gateway and the 4-gateway scenario are chosen as samples. Numerical results are given as a comparison and improvement of FT-CSMA over Aloha.

5.5.3.1 PDR

In Figure 5.6, one gateway, when the number exceeds approximately 390 Nodes, CAD improves the PDR by more than 5%, followed by S-ALOHA by 4%. In Figure 5.7, four gateways, improvement begins at roughly 600 EDs.

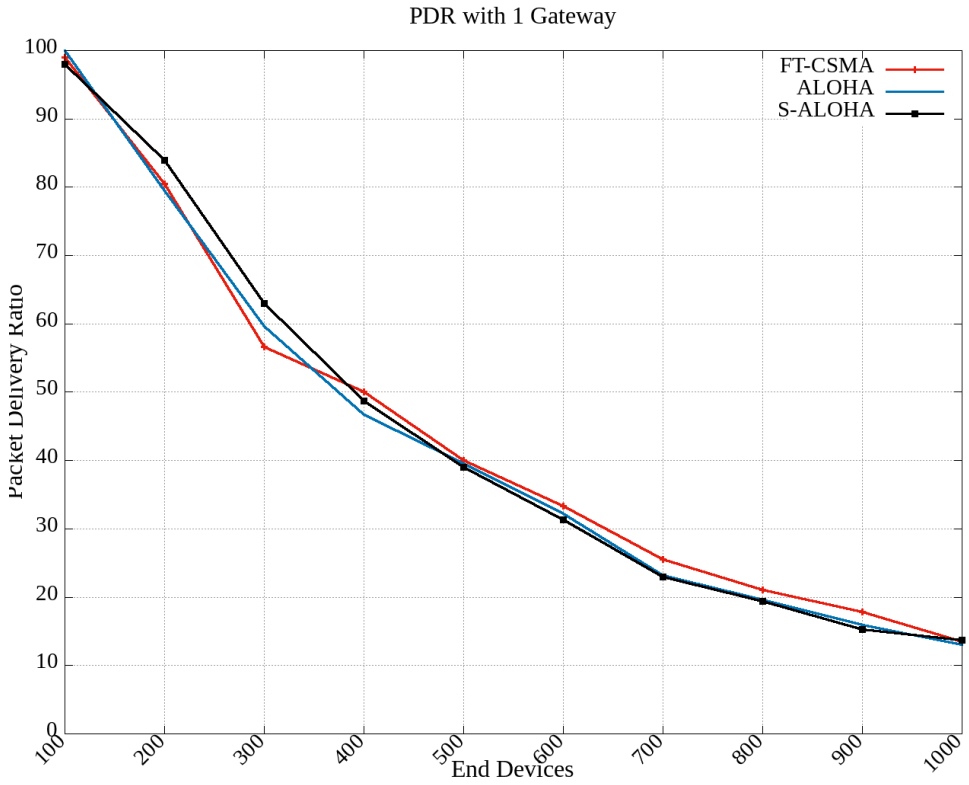

Fig. 5.6. PDR with one gateway

Note that the PDR for one gateway drops very fast as the number of nodes increases. This is due to the limited capacity of a gateway in terms of the number of nodes. Even if the Gateway is multi-channel, i.e., it can receive simultaneously on 8 or 10 channels and 6 SF, it cannot support many devices.

The end-device distribution also has an impact on the PDR. As the number of nodes increases, more nodes will have the same distance from the gateway and, therefore, influenced by ADR, operate in the same SF. As a result, the probability of collisions increases.

We can already conclude that a large IoT network requires a preliminary study on the minimum number of gateways to cover the massive number of deployed nodes.

5.5.3.2 Delay

Delays, however, start to deteriorate as the load increases because of waiting times and back-offs. The previous results show a relationship between this behavior and the PDR. In Figure 5.8, one gateway, the increase in delay starts at 320 nodes to reach (1.19 – 0.66 = 0.53%) at 1000 nodes.

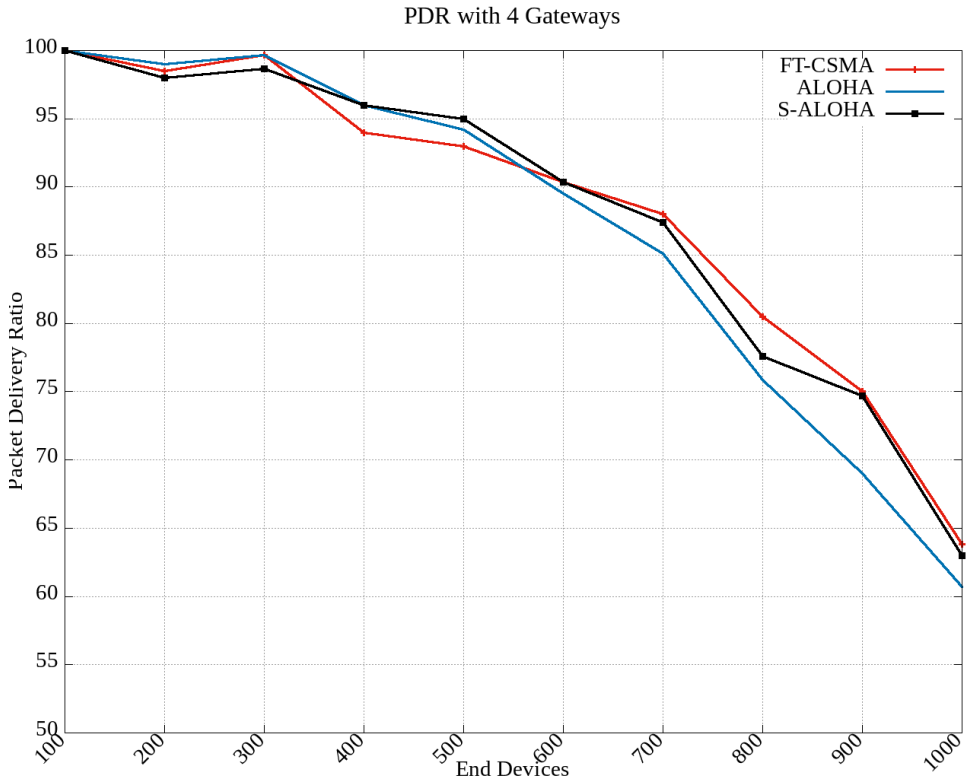

Fig. 5.7. PDR with four gateways

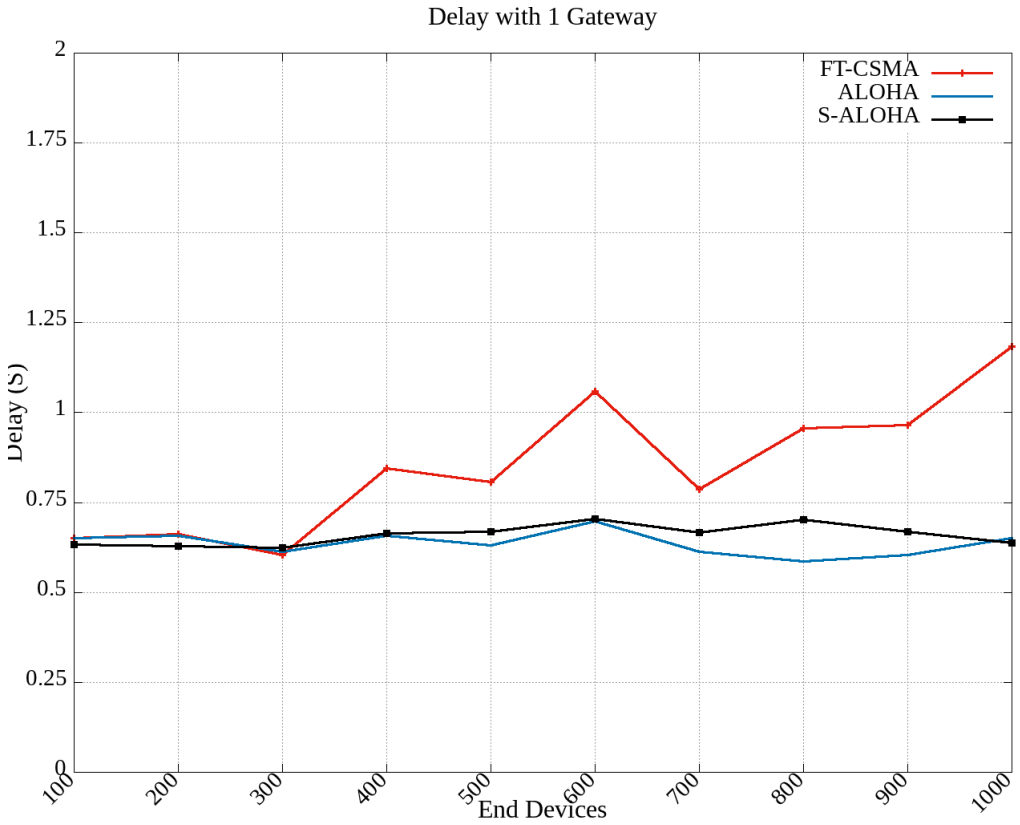

Fig. 5.8. Delay with one gateway

In Figure 5.9, four gateways, Like the PDR, the degradation begins at 580 nodes and reaches a loss of only (0.77 − 0.58 = 0.19%) at 1000 nodes.

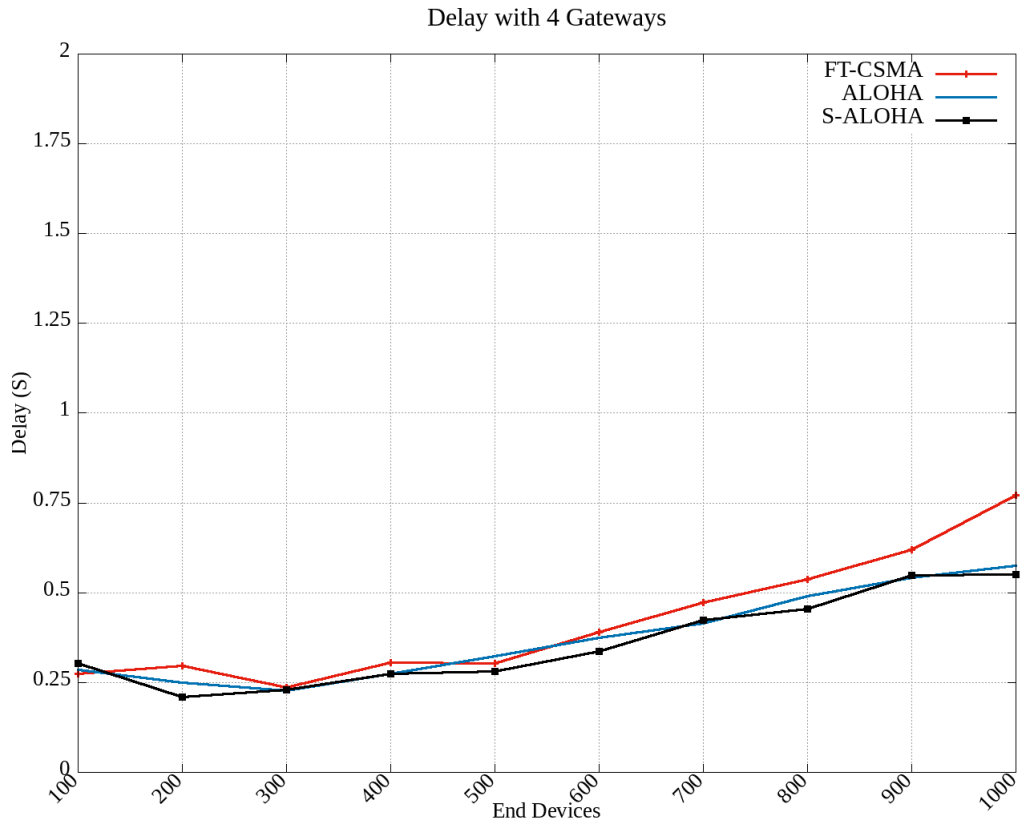

Fig. 5.9. Delay with four gateways

If a planned network requires a specific margin for the PDR, we can estimate the maximum number of nodes allocated for each gateway deployed to stay within this margin. Table 5.5 shows an example of a study on the estimated distribution of nodes per gateway to achieve an acceptable PDR of 90%, with reservations about the environment and node positions. These results apply to the FT-CSMA scenario, while the ALOHA scenario is below.

GW	EDs (12B)	Average	EDs (24B)	Average
1	150	150	140	140
2	300	150	260	130
3	480	160	400	133
4	630	157	560	140
5	740	148	700	140
1average		153		137

TABLE 5.5. NODE DISTRIBUTION PER GATEWAY

The capacity of gateways in terms of devices is not our current research, but we can already observe the impact of collisions and packet size.

5.5.3.3 Energy

Based on the results obtained, it can be concluded that the energy consumption is consistent with the expected values. In Figure 5.10, it is observed that with a single gateway, the energy consumption is improved by approximately $(1.85 - 0.35 = 1.5\%)$. However, for a sufficient number of nodes where collisions are maximal, near 1000 End devices, it is evident that the energy consumption increases to $(2.9 - 0.9 = 2\%)$.

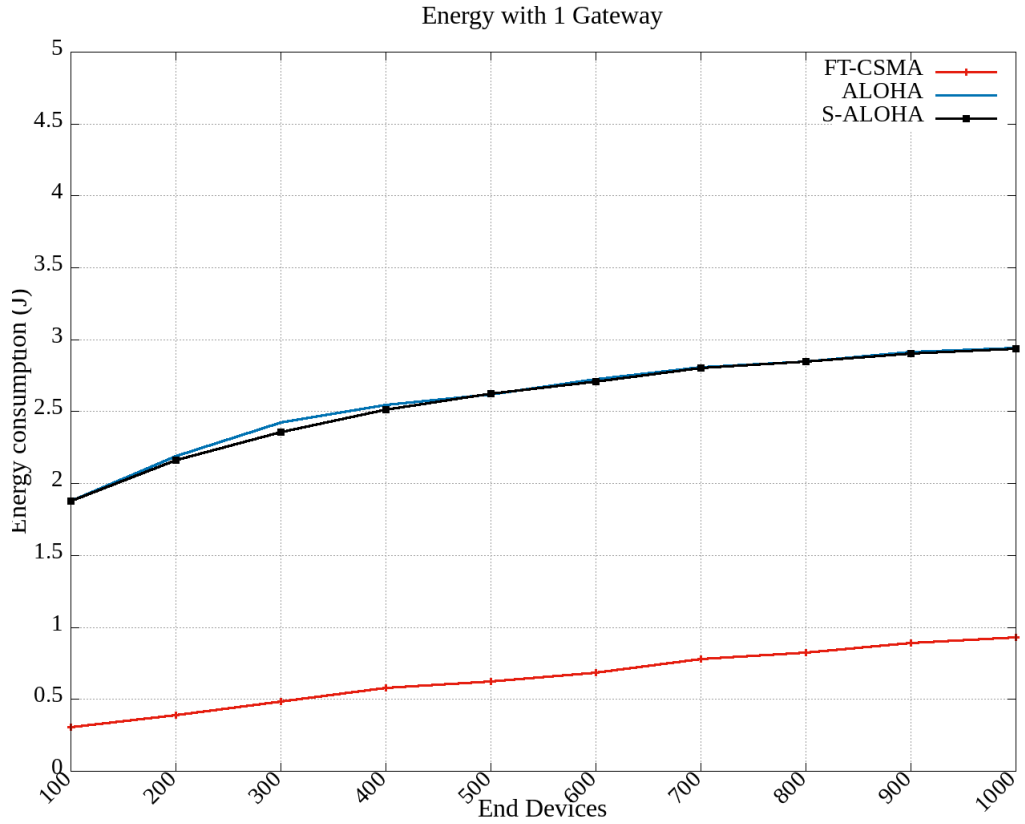

Fig. 5.10. Energy consumption with one gateway

In Figure 5.11, we observe similar results for four gateways where the improvement starts at $(1.3 - 0.3 = 1\%)$ and reaches $(2.5 - 0.8 = 1.7\%)$. The reduction in energy consumption is due to the decrease in retransmissions. The low-consumption CADs, followed by a single transmission, replace these energy-costing retransmissions if the device finds the channel idle. i.e., in energy consumption, the sum of all CAD operations and a single transmission following them is less than the sum of retransmissions without enabling CAD.

According to the results of the analytical and theoretical models performed on S-ALOHA, the improvements are not entirely apparent. This is because:

- The difference in packet processing time depending on the SF, even if the packets have the same size;
- The simultaneous sending of packets at the start of the experiment;

- The packets lost by attenuating signals for nodes further away from Gateways.

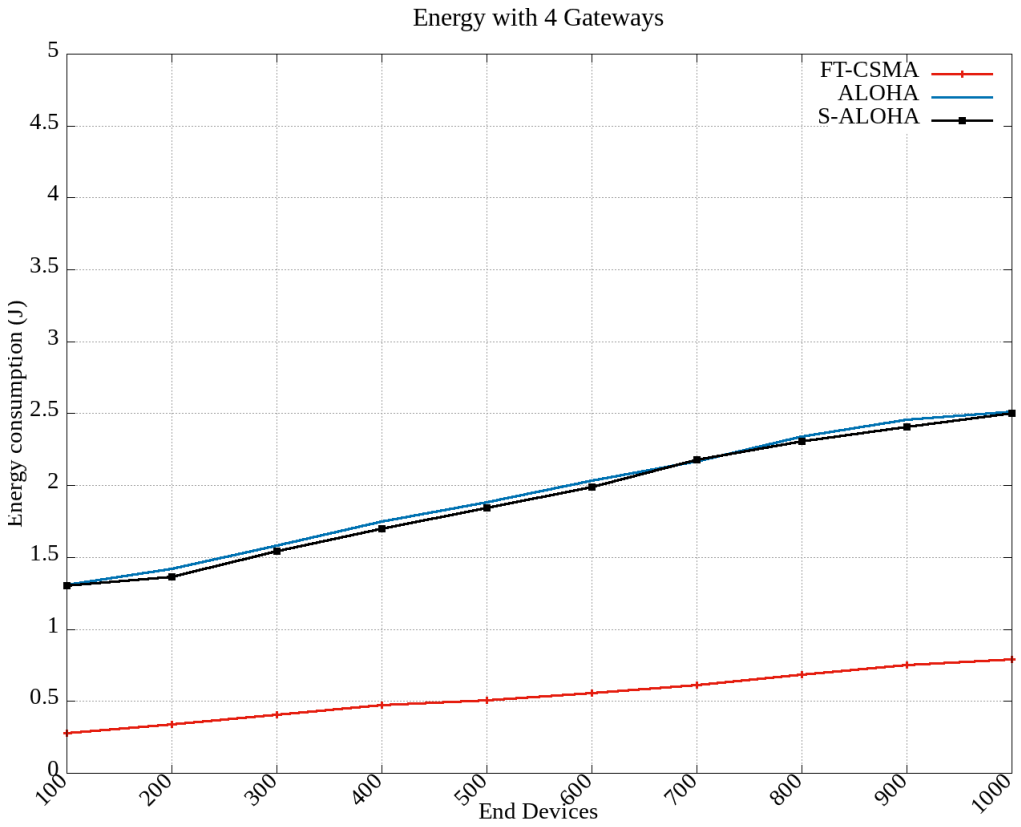

Fig. 5.11. Energy consumption with four gateways

5.5.3.4 Comparison with Other Proposals

We have also implemented the LMAC-1 version of the previously cited article in [81]. Table 5.6 illustrates the parameters used in the simulation.

Difs Time (CAD)	Back-off Time (CAD)
4	[4-32]
8	[4-32]
12	[8-64]

TABLE 5.6. LMAC-1'S PARAMETERS SIMULATION

Figure 5.12 and Figure 5.13 show the difference between the LMAC-1 scenarios and FT-CSMA regarding quality of service. The results with 4 Gateways, 24 bytes of payloads, and a radius of 6400m are given. The other simulations look the same as previous one.

Even though the QoS results seem very close for energy consumption, however, Figuez 5.14 shows the success of CAD on LMAC-1. Henceforth, the one with $DIFS = 4CAD$

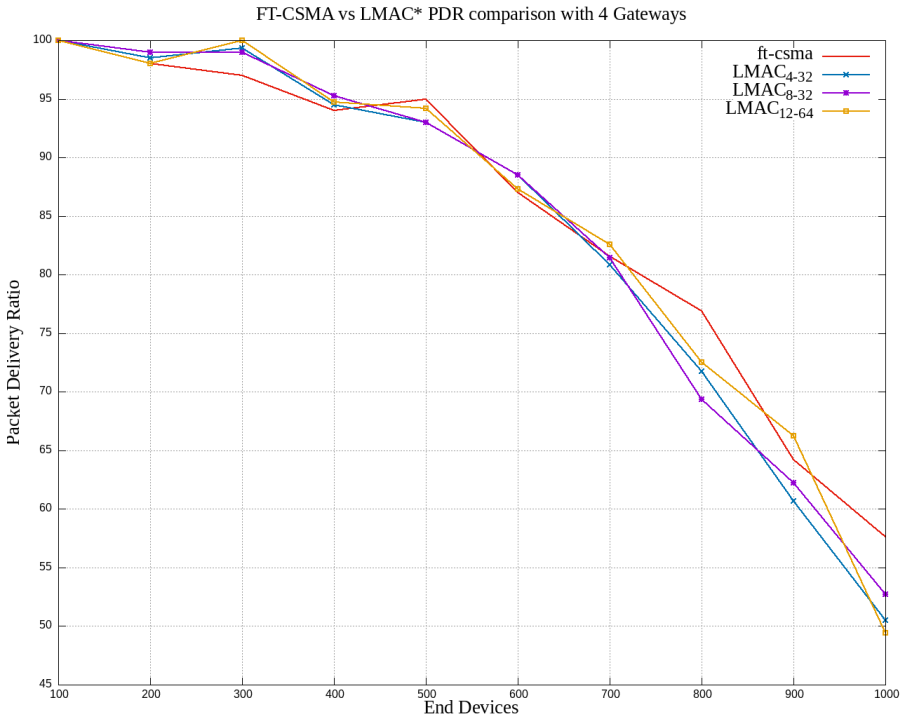

Fig. 5.12. FT-CSMA vs LMAC* PDR

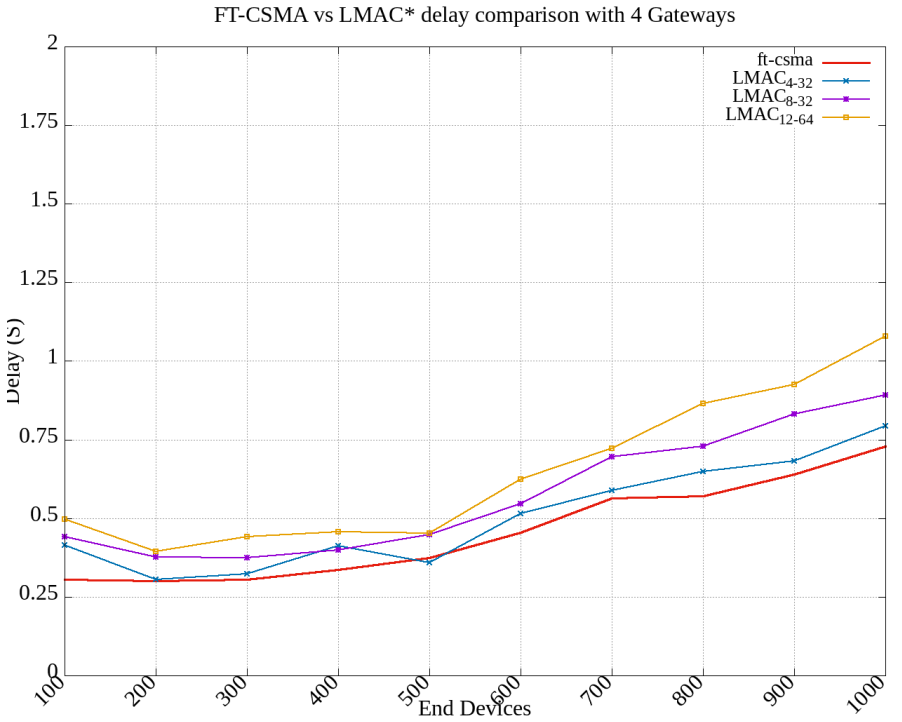

Fig. 5.13. FT-CSMA vs LMAC* Delay

and a Back-off between [4-32] gives the best results. This proves that using CAD in CSMA methods relatively avoids collisions. However, overuse of the technique does have an impact on energy consumption. Therefore, the choice of the number of CADs used in DIFS or Back-Off is made with extreme prudence.

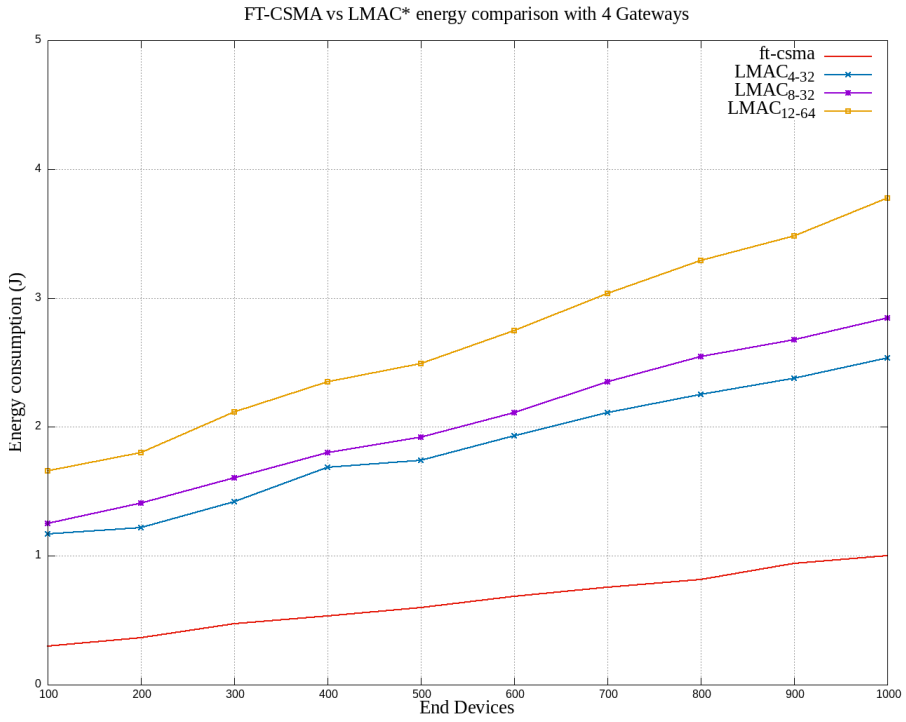

Fig. 5.14. FT-CSMA vs LMAC* Energy

Note that using CADs in the Back-off consumes additional energy. For this reason, we should adopt the Back-off used in CSMA 802.15.4 without channel detection here instead of CSMA 802.11 in [81].

5.6. Conclusion

Wireless networks are prone to collisions that can negatively impact their efficiency, dependability, and scalability. Carrier Sense Multiple Access (CSMA) protocols have been developed through extensive scientific research to mitigate this issue. While signal strength-based CSMA approaches are commonly used, CSMA protocols that rely on channel activity detection (CAD) are crucial for successfully deploying LoRa technology.

Here, we present a new, modernized CSMA protocol called FT-CSMA. To ensure dependable and efficient CAD operation, selecting an appropriate CAD number, determining proper CAD durations, and incorporating a back-off delay is necessary. FT-CSMA is a well-optimized method, following the trustworthy and established techniques, such as those standardized and implemented for IEEE CSMA specifications. The NS3 simulator has been instrumental in demonstrating our remarkable improvements in Packet Delivery Ratio (PDR) of about 5% and significant improvements in energy efficiency up to 2%, without significantly compromising the delay. The findings of this research indicate that CAD operations are successful. LoRa-based networks and low-power wide area network (LPWAN) technologies can be leveraged for numerous applications in the Internet of Things (IoT) ecosystem.

By integrating Channel Activity Detection (CAD) into NS3's LoRaWAN module, this study provides valuable insights to the scientific community. Firstly, our objective is to thoroughly test the proposed CSMA solutions by conducting multiple CAD processes and evaluating their effectiveness before introducing a new, more optimized option. Secondly, exploration in the field of RF spectrum analysis or intelligent spectrum sharing looks promising, and a new cognitive radio architecture, for ISM band specialy is needed.

CONCLUSION

The growth of the world population and rapid urbanization have dramatic environmental consequences. Problems are multiplying at an incredible rate, such as resource and energy consumption, greenhouse gases, and urban waste. Smart cities solve these environmental problems by improving the quality of life of citizens. To achieve this, smart city applications leverage various technologies. In this thesis, we began with an overview of the key enabling and emerging technologies for smart cities. Ensuring security in smart cities is a big challenge, so we focus on a few security elements, such as risk management, trust, insider threats, and secure interoperability.

One of the constraints associated with IoT is the massive use of ISM channels, which causes significant interference and consequently affects QoS. We discuss the protocols for accessing the medium and how various topologies can coexist.

The aim of this thesis is to introduce our contribution by developing a new mechanism for improving the quality of service of LoRa-based networks, in particular Lo-RaWAN. First, we presented LoRa technology and the LoRaWAN network specification. We then identified the standard protocols for collision avoidance in such LPWAN environments and provided a state-of-the-art review of the proposed protocols for LoRaWAN networks.

We proposed a new protocol called A Fine-tuned CSMA (FT-CSMA) based on channel detection (CAD), which is a type of listen before talk (LBT) specific to LoRa. FT-CSMA is a well-optimised method, following trustworthy and established techniques, such as those standardised and implemented for IEEE CSMA specifications.

The NS3 simulator has been instrumental in demonstrating our remarkable improvements in Packet Delivery Ratio (PDR) of about 5% and significant improvements in energy efficiency up to 2%, without significantly compromising the delay. The findings of this research indicate that CAD operations are successful. LoRa-based networks and low-power wide area network (LPWAN) technologies can be leveraged for numerous applications in the Internet of Things (IoT) ecosystem, including various distributed measurement systems (DMS) for pollution, structural health monitoring, environmental monitoring, and transportation control. By integrating Channel Activity Detection (CAD) into NS3's LoRaWAN module, this study provides valuable insights to the scientific community.

On the basis of the results obtained in this research, our objective is first to thoroughly test the proposed CSMA solutions by conducting multiple CAD processes and evaluating their effectiveness before introducing a new, more optimized option. Secondly, study optimal gateway placement and frequency planning. In parallel, exploit the network server communication links with the gateways to effectively identify bottlenecks and propose different strategies for managing collisions and the entire communication system. In ad-

dition, the current LoRa simulation model will be enhanced to support Class B and C devices. Thirdly, exploration in the field of RF spectrum analysis or intelligent spectrum sharing looks promising, and a new cognitive radio architecture for ISM band specialization is needed. We believe that proposing a global IoT architecture is a promising area of research. It unifies heterogeneous IoT technologies and supports interoperability, big data processing, and the guarantee of security and privacy.

We also presented associated future research directions. We looked at the role of IoT in smart cities, describing the basics of what IoT is and what constitutes a smart city, followed by smart city segments. The benefits of IoT and their impact on smart cities, as well as national and international case studies, are also discussed. The variety of IoT technologies created across all industries justifies this. Therefore, the immersion of new architectures, topologies, protocols, and networks. We have presented the architecture of IoT networks and the main topologies involved, including wireless personal area networks (WPAN) and low-power wide area networks (LPWAN), which differ in signal coverage and data rates. However, both seek to preserve battery life. Specifically, WPANs sacrifice signal coverage to support higher data rates, while LPWANs sacrifice data rates to support greater signal coverage.

This page intentionally left blank

BIBLIOGRAPHY

[1] cisco and its affiliates. "The internet of everything global private sector economic analysis." (2013), [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf.

[2] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi, "Iot survey: An sdn and fog computing perspective," *Comput. Netw.*, vol. 143, pp. 221–246, Oct. 2018. DOI: 10.1016/j.comnet.2018.07.020. [Online]. Available: https://doi.org/10.1016/j.comnet.2018.07.020.

[3] R. Herrero, "Introduction to iot networking," in *Practical Internet of Things Networking: Understanding IoT Layered Architecture*. Cham: Springer International Publishing, 2023, pp. 3–26. DOI: 10.1007/978-3-031-28443-4_1. [Online]. Available: https://doi.org/10.1007/978-3-031-28443-4_1.

[4] V. Fernandez-Anez, "Stakeholders approach to smart cities: A survey on smart city definitions," in *Smart Cities*, E. Alba, F. Chicano, and G. Luque, Eds., Cham: Springer International Publishing, 2016, pp. 157–167.

[5] A. Gharaibeh *et al.*, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2456–2501, 2017. DOI: 10.1109/COMST.2017.2736886.

[6] A. J. Sekhar N. Kondepudi Vinod Ramanarayanan, "Smart sustainable cities an analysis of definitions," ITU-T Focus Group on Smart Sustainable Cities, technical reports, 2014.

[7] D. Pennino, M. Pizzonia, A. Vitaletti, and M. Zecchini, "Blockchain as iot economy enabler: A review of architectural aspects," *Journal of Sensor and Actuator Networks*, vol. 11, no. 2, 2022. DOI: 10.3390/jsan11020020. [Online]. Available: https://www.mdpi.com/2224-2708/11/2/20.

[8] X. Wang *et al.*, "Survey on blockchain for internet of things," *Computer Communications*, vol. 136, pp. 10–29, 2019. DOI: https://doi.org/10.1016/j.comcom.2019.01.006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366418306881.

[9] F. Chentouf and S. Bouchkaren, "Security and privacy in smart city: A secure e-voting system based on blockchain," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, p. 1848, Apr. 2023. DOI: 10.11591/ijece.v13i2.pp1848-1857.

[10] K. Munjal and R. Bhatia, "A systematic review of homomorphic encryption and its contributions in healthcare industry," *Complex & Intelligent Systems*, vol. 9, pp. 1–28, May 2022. DOI: 10.1007/s40747-022-00756-z.

[11] A. Marandi, P. G. M. R. Alves, D. F. Aranha, and R. H. Jacobsen, "Lattice-Based Homomorphic Encryption For Privacy-Preserving Smart Meter Data Analytics," *The Computer Journal*, bxad093, Sep. 2023. DOI: 10.1093/comjnl/bxad093. eprint: https://academic.oup.com/comjnl/advance-article-pdf/doi/10.1093/comjnl/bxad093/51779097/bxad093.pdf. [Online]. Available: https://doi.org/10.1093/comjnl/bxad093.

[12] C. V. Mahamuni, Z. Sayyed, and A. Mishra, "Machine learning for smart cities: A survey," in *2022 IEEE International Power and Renewable Energy Conference (IPRECON)*, 2022, pp. 1–8. DOI: 10.1109/IPRECON55716.2022.10059521.

[13] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, "Applications of artificial intelligence and machine learning in smart cities," *Computer Communications*, vol. 154, pp. 313–323, 2020. DOI: https://doi.org/10.1016/j.comcom.2020.02.069. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366419320821.

[14] Z. Lv, D. Chen, R. Lou, and Q. Wang, "Intelligent edge computing based on machine learning for smart city," *Future Generation Computer Systems*, vol. 115, pp. 90–99, 2021. DOI: https://doi.org/10.1016/j.future.2020.08.037. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X20306889.

[15] J. Chin, V. Callaghan, and I. Lam, "Understanding and personalising smart city services using machine learning, the internet-of-things and big data," in *2017 IEEE 26th International Symposium on Industrial Electronics (ISIE)*, 2017, pp. 2050–2055. DOI: 10.1109/ISIE.2017.8001570.

[16] D. Luckey, H. Fritz, D. Legatiuk, K. Dragos, and K. Smarsly, "Artificial intelligence techniques for smart city applications," in *Proceedings of the 18th International Conference on Computing in Civil and Building Engineering*, E. Toledo Santos and S. Scheer, Eds., Cham: Springer International Publishing, 2021, pp. 3–15.

[17] A. Tasiran and B. Kizilkaya, "Statistical analysis of low-power sensor motes used in iot applications," in Mar. 2020, pp. 207–226. DOI: 10.1049/PBCE128E_ch10.

[18] W. Li, H. Song, and F. Zeng, "Policy-based secure and trustworthy sensing for internet of things in smart cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 716–723, 2018. DOI: 10.1109/JIOT.2017.2720635.

[19] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, "Landscape of iot security," *Computer Science Review*, vol. 44, May 2022. DOI: 10.1016/j.cosrev.2022.100467.

[20] A. Brutti, A. Frascella, N. Gessa, P. de sabbata, and C. Novelli, "Interoperability in the smart city: A semantic approach for merging flexibility with strictness," Jun. 2018, pp. 434–439. DOI: 10.1109/SMARTCOMP.2018.00042.

[21] J. Wang, B. Sun, Y. Yang, and X. Niu, "Distributed trust management mechanism for the internet of things," *Applied Mechanics and Materials*, vol. 347-350, Mar. 2013. DOI: 10.2991/iccsee.2013.552.

[22] L. Gu, J. Wang, and B. Sun, "Trust management mechanism for internet of things," *Communications, China*, vol. 11, pp. 148–156, Feb. 2014. DOI: 10.1109/CC.2014.6821746.

[23] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015. DOI: https://doi.org/10.1016/j.comnet.2014.11.008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128614003971.

[24] B. Rudra, "Impact of internet of things in smart cities," in *IoT Technologies in Smart Cities: From sensors to big data, security and trust* (Control, Robotics and Sensors), Control, Robotics and Sensors. Institution of Engineering and Technology, 2020, pp. 41–61. DOI: 10.1049/PBCE128E_ch2. [Online]. Available: https://digital-library.theiet.org/content/books/10.1049/pbce128e_ch2.

[25] M. Imran, Ed., *IoT Technologies in Smart Cities: From sensors to big data, security and trust* (Control, Robotics and Sensors). Institution of Engineering and Technology, 2020. [Online]. Available: https://digital-library.theiet.org/content/books/ce/pbce128e.

[26] S. F. Ahmed *et al.*, "Industrial internet of things enabled technologies, challenges, and future directions," *Computers and Electrical Engineering*, vol. 110, p. 108 847, 2023. DOI: https://doi.org/10.1016/j.compeleceng.2023.108847. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790623002719.

[27] T. Kumar, *Smart Environment for Smart Cities*. Jan. 2020. DOI: 10.1007/978-981-13-6822-6.

[28] W. Guibene, K. E. Nolan, and M. Y. Kelly, "Survey on clean slate cellular-iot standard proposals," in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 2015, pp. 1596–1599. DOI: 10.1109/CIT/IUCC/DASC/PICOM.2015.240.

[29] V. P. Kafle, Y. Fukushima, and H. Harai, "Internet of things standardization in itu and prospective networking technologies," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 43–49, 2016. DOI: 10.1109/MCOM.2016.7565271.

[30] I. Ishaq *et al.*, "Ietf standardization in the field of the internet of things (iot): A survey," *Journal of Sensor and Actuator Networks*, vol. 2, no. 2, pp. 235–287, 2013. DOI: 10.3390/jsan2020235. [Online]. Available: https://www.mdpi.com/2224-2708/2/2/235.

[31] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, and P. Urien, "Internet of things: A definition and taxonomy," in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 2015, pp. 72–77. DOI: 10.1109/NGMAST.2015.71.

[32] I. Ishaq *et al.*, "Ietf standardization in the field of the internet of things (iot): A survey," *Journal of Sensor and Actuator Networks*, vol. 2, pp. 235–287, Apr. 2013. DOI: 10.3390/jsan2020235.

[33] N. Naik, "Lpwan technologies for iot systems: Choice between ultra narrow band and spread spectrum," in *2018 IEEE International Systems Engineering Symposium (ISSE)*, 2018, pp. 1–8. DOI: 10.1109/SysEng.2018.8544414.

[34] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of things (iot) communication protocols: Review," in *2017 8th International Conference on Information Technology (ICIT)*, 2017, pp. 685–690. DOI: 10.1109/ICITECH.2017.8079928.

[35] "Ieee standard for low-rate wireless networks," *IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015)*, pp. 1–800, 2020. DOI: 10.1109/IEEESTD.2020.9144691.

[36] J.-F. Mainguet, *La norme ieee 802.15.4*. [Online]. Available: https://liaison.mainguet.org/802_15_4.htm.

[37] N. S. Olivier B.A. SELLER, "Low power longrange transmitter," US 14/170,170, 2014. [Online]. Available: https://patents.google.com/patent/US20140219329A1.

[38] S. Corporation, "Ds_sx1276-7-8-9_w_app_v7," Tech. Rep., 2020.

[39] S. Corporation, "Ds.sx1261-2.w.app rev. 2.1," Tech. Rep., Dec. 2021.

[40] S. Corporation, "Lora modulation basics," Tech. Rep., May 2015.

[41] L. Vangelista, "Frequency shift chirp modulation: The lora modulation," *IEEE Signal Processing Letters*, vol. 24, no. 12, pp. 1818–1821, 2017. DOI: 10.1109/LSP.2017.2762960.

[42] M. Knight and B. Seeber, "Decoding lora: Realizing a modern lpwan with sdr," *Proceedings of the GNU Radio Conference*, vol. 1, no. 1, 2016. [Online]. Available: https://pubs.gnuradio.org/index.php/grcon/article/view/8.

[43] L. Alliance, "Rp002-1.0.3 lorawan regional parameters," Tech. Rep., May 2021.

[44] L. alliance & ABI research, *Lorawan and nb-iot: Competitors or complementary?* 249 South Street Oyster Bay, New York 11771 USA, 2019. [Online]. Available: https://resources.lora-alliance.org/technology-comparisons/lorawan-and-nb-iot-competitors-or-complementary.

[45] L. alliance, *Lora alliance massive and critical iot requirements infographic*, 2022. [Online]. Available: https://resources.lora-alliance.org/infographic/lora-alliance-lorawan-and-5g-infographic.

[46] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015. DOI: 10.1109/COMST.2015.2444095.

[47] B. Mróz-Gorgoń, W. Wodo, A. Andrych, K. Caban-Piaskowska, and C. Kozyra, "Biometrics innovation and payment sector perception," *Sustainability*, vol. 14, Aug. 2022. DOI: 10.3390/su14159424.

[48] L. P. Taylor, "Chapter 20 - independent assessor audit guide," in *FISMA Compliance Handbook*, L. P. Taylor, Ed., Boston: Syngress, 2013, pp. 239–273. DOI: https://doi.org/10.1016/B978-0-12-405871-2.00020-8. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780124058712000208.

[49] G. Kumar, S. Bakshi, and P. Sa, *Person authentication based on biometric traits using machine learning techniques*, Oct. 2020. DOI: 10.1201/9781003054115.

[50] W. Yang *et al.*, "A cancelable iris- and steganography-based user authentication system for the internet of things," *Sensors*, vol. 19, no. 13, 2019. DOI: 10.3390/s19132985. [Online]. Available: https://www.mdpi.com/1424-8220/19/13/2985.

[51] W. Yang, S. Wang, G. Zheng, J. Yang, and C. Valli, "A privacy-preserving lightweight biometric system for internet of things security," *IEEE Communications Magazine*, vol. 57, no. 3, pp. 84–89, 2019. DOI: 10.1109/MCOM.2019.1800378.

[52] T. Maitra and D. Giri, "An efficient biometric and password-based remote user authentication using smart card for telecare medical information systems in multi-server environment," *Journal of medical systems*, vol. 38, p. 142, Dec. 2014. DOI: 10.1007/s10916-014-0142-x.

[53] S. Pawar, V. Kithani, S. Ahuja, and S. Sahu, "Smart home security using iot and face recognition," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 2018, pp. 1–6. DOI: 10.1109/ICCUBEA.2018.8697695.

[54] S. Ibrahim, V. K. Shukla, and R. Bathla, "Security enhancement in smart home management through multimodal biometric and passcode," in *2020 International Conference on Intelligent Engineering and Management (ICIEM)*, 2020, pp. 420–424. DOI: 10.1109/ICIEM48762.2020.9160331.

[55] V. Stoynov, V. Poulkov, and Z. Valkova-Jarvis, "Low power wide area networks operating in the ism band- overview and unresolved challenges," in *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*, V. Poulkov, Ed., Cham: Springer International Publishing, 2019, pp. 96–109.

[56] D. Murray, "Using rf recording techniques to resolve interference problems," in *2013 IEEE AUTOTESTCON*, 2013, pp. 1–6. DOI: 10.1109/AUTEST.2013.6645046.

[57] S. Venkatesh, "Radio wave propagation," vol. 923, pp. 164–164, Jul. 2007. DOI: 10.1063/1.2767029.

[58] J. Davis, "Signal quality degradation," in *High–Speed Digital System Design*. Cham: Springer International Publishing, 2006, pp. 79–86. DOI: 10.1007/978-3-031-79740-8_4. [Online]. Available: https://doi.org/10.1007/978-3-031-79740-8_4.

[59] M. Kaur, S. Kakar, and D. Mandal, "Electromagnetic interference," in *2011 3rd International Conference on Electronics Computer Technology*, vol. 4, 2011, pp. 1–5. DOI: 10.1109/ICECTECH.2011.5941844.

[60] J. J. Carr, "Chapter 3 - fundamentals of electromagnetic interference," in *The Technician's EMI Handbook*, J. J. Carr, Ed., Woburn: Newnes, 2000, pp. 23–27. DOI: https://doi.org/10.1016/B978-075067233-7/50003-X. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B978075067233750003X.

[61] *Rf data analytics: Another idea which time has come – cots journal*, COTS journal, Oct. 2017. [Online]. Available: https://www.cotsjournalonline.com/index.php/2017/10/24/rf-data-analytics-another-idea-time-come/ (visited on 01/11/2024).

[62] J. Kruys and L. Qian, "Rf spectrum, usage and sharing," Jun. 2011. DOI: 10.1007/978-94-007-1585-1_1.

[63] M. Amin, M. S. Hossain, and M. Atiquzzaman, "In-band full duplex wireless lans: Medium access control protocols, design issues and their challenges," *Information*, vol. 11, p. 216, Apr. 2020. DOI: 10.3390/info11040216.

[64] G. H. C. Marcus Burton CWNE, "802.11 arbitration," CWNP, marcus.burton@cwnp.com, gt@gthill.com, Tech. Rep. 21, 2009.

[65] I. Iliev, B. Bonev, K. Angelov, P. Petkov, and V. Poulkov, "Interference identification based on long term spectrum monitoring and cluster analysis," in *2016 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, 2016, pp. 1–5. DOI: 10.1109/BlackSeaCom.2016.7901562.

[66] P. Baltiiski, I. Iliev, B. Kehayov, V. Poulkov, and T. Cooklev, "Long-term spectrum monitoring with big data analysis and machine learning for cloud-based radio access networks," *Wireless Personal Communications*, vol. 87, May 2015. DOI: 10.1007/s11277-015-2631-8.

[67] C. Mostefa, T. A. Mounir, A. M. Abdelmadjid, and A. Nouar, "Ft-csma: A fine-tuned csma protocol for lora-based networks," *Journal of Communications*, no. 2, pp. 65–77, 2024. DOI: 10.12720/jcm.19.2.65-77.

[68] C. Mostefa, N. Abdelouahab, T. A. Mounir, S. Boumerdassi, S. Femmam, and Z. A. Amel, "Formal validation of adr protocol in lorawan network using event-b," in *2023 7th International Conference on Computer, Software and Modeling (ICCSM)*, 2023, pp. 11–15. DOI: 10.1109/ICCSM60247.2023.00011.

[69] T.-H. To and A. Duda, "Simulation of lora in ns-3: Improving lora performance with csma," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–7. DOI: 10.1109/ICC.2018.8422800.

[70] TTN. "Rssi and snr | the things network." (), [Online]. Available: https://www.thethingsnetwork.org/docs/lorawan/rssi-and-snr/.

[71] C. Goursaud and J. M. Gorce, "Dedicated networks for iot: Phy / mac state of the art and challenges," *EAI Endorsed Transactions on Internet of Things*, vol. 1, no. 1, Oct. 2015. DOI: 10.4108/eai.26-10-2015.150597.

[72] SEMTECH. "How-to-ensure-your-lora-packets-are-sent-properly/." (), [Online]. Available: https://lora-developers.semtech.com/documentation/tech-papers-and-guides/.

[73] C. Pham, "Investigating and experimenting csma channel access mechanisms for lora iot networks," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, 2018, pp. 1–6. DOI: 10.1109/WCNC.2018.8376997.

[74] J. Liando, A. Jg, A. Tengourtius, and M. Li, "Known and unknown facts of lora: Experiences from a large-scale measurement study," *ACM Transactions on Sensor Networks*, vol. 15, pp. 1–35, Feb. 2019. DOI: 10.1145/3293534.

[75] L. Beltramelli, A. Mahmood, P. Österberg, and M. Gidlund, "Lora beyond aloha: An investigation of alternative random access protocols," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3544–3554, 2021. DOI: 10.1109/TII.2020.2977046.

[76] N. Kouvelas, V. S. Rao, R. V. Prasad, G. Tawde, and K. Langendoen, "P-carma: Politely scaling lorawan," ser. EWSN '20, Lyon, France: Junction Publishing, 2020, pp. 25–36.

[77] C. Pham and M. Ehsan, "Dense deployment of lora networks: Expectations and limits of channel activity detection and capture effect for radio channel access," *Sensors*, vol. 21, no. 3, p. 825, Jan. 2021. DOI: 10.3390/s21030825. [Online]. Available: http://dx.doi.org/10.3390/s21030825.

[78] A. Triantafyllou, P. Sarigiannidis, T. Lagkas, I. D. Moscholios, and A. Sarigiannidis, "Leveraging fairness in lorawan: A novel scheduling scheme for collision avoidance," *Computer Networks*, vol. 186, p. 107 735, 2021. DOI: https://doi.org/10.1016/j.comnet.2020.107735. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128620313232.

[79] C. Shao and O. Muta, "Heterogeneous carrier-sense multiple access for improved energy fairness in lorawan," in *2022 Tenth International Symposium on Computing and Networking (CANDAR)*, 2022, pp. 172–178. DOI: 10.1109/CANDAR57322.2022.00031.

[80] S. Herrería-Alonso, A. Suárez-González, M. Rodríguez-Pérez, and C. López-García, "Enhancing lorawan scalability with longest first slotted csma," *Computer Networks*, vol. 216, p. 109 252, 2022. DOI: https://doi.org/10.1016/j.comnet.2022.109252. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S138912862200322X.

[81] A. Jg, J. Liando, C. Gu, R. Tan, and O. Seller, "Lmac: Efficient carrier-sense multiple access for lora," *ACM Transactions on Sensor Networks*, vol. 19, Sep. 2022. DOI: 10.1145/3564530.

[82] F. Yu, X. Zheng, L. Liu, and H. Ma, "Loradar: An efficient lora channel occupancy acquirer based on cross-channel scanning," in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, 2022, pp. 540–549. DOI: 10.1109/INFOCOM48880.2022.9796845.

[83] C. Mostefa, T. a. Mounir, and A. Mohamed abdlmadjid, "Simulate a lora-based iot network by adding a module in ns-3," in *2023 First national Conference on: Artificial Intelligence, Smart Technologies and Communications (UHBC)*, UHBC Chlef, Algeria, 2023.

[84] N. Abdelouahab, T. A. Mounir, B. Selma, and C. Mostefa, "Impact of mobility model on lorawan performance," *JCM Journal of Communications*, vol. 19, no. 1, pp. 7–18, 2024. DOI: 10.12720/jcm.19.1.7-18.