electronics

MDPI

Review

Analysis of Cyber Security Aspects of Data Transmission in Large-Scale Networks Based on the LoRaWAN Protocol Intended for Monitoring Critical Infrastructure Sensors

Grzegorz Czeczot, Izabela Rojek * and Dariusz Mikołajewski

Faculty of Computer Science, Kazimierz Wielki University, 85-064 Bydgoszcz, Poland; dmikolaj@ukw.edu.pl (D.M.)
* Correspondence: izabela.rojek@ukw.edu.pl

Abstract: Cyber security is nowadays synonymous with the reliability of elements connected to the internet. Better control of factories, security systems or even individual sensors is possible through the use of Internet of Things technology. The security of the aforementioned structures and the data they transmit has been a major concern in the development of IoT solutions for wireless data transmission. If we add to this prospect of low-cost end devices, we can seriously consider implementing such solutions in critical infrastructure areas. This article aims to assess the state of the art and experience and identify the main risks and directions for further development in order to improve the cyber security situation of LoRaWAN-based networks. LoRaWAN meets the three key requirements of IoT applications (low cost, large-scale deployability, high energy efficiency) through an open standard and the construction of autonomous networks without third-party infrastructure. However, many research issues remain to be solved/improved such as resource allocation, link coordination, transmission reliability, performance and, above all, security. Thus, we have defined a research gap in the area of LoRaWAN security. The contribution of this work is to structure the knowledge in the field of LoRaWAN security, based on previous publications and our own experience, in order to identify challenges and their potential solutions. This will help move LoRaWAN security research to the next stage.

Keywords: wireless network; LPWAN; LoRa; IoT; security

Citation: Czeczot, G.; Rojek, I.; Mikołajewski, D. Analysis of Cyber Security Aspects of Data Transmission in Large-Scale Networks Based on the LoRaWAN Protocol Intended for Monitoring Critical Infrastructure Sensors. *Electronics* **2023**, *12*, 2503. https://doi.org/10.3390/electronics12112503

Academic Editor: Andrei Kelarev

Received: 2 May 2023
Revised: 29 May 2023
Accepted: 30 May 2023
Published: 1 June 2023

1. Introduction

The Internet of Things (IoT) is defined as a network of interconnected wired or wireless devices characterized by the ability to collect, process and share data and to interact with the environment based on this data. This combination makes it possible to create intelligent spaces in different areas of human activity, from the smart home to the smart factory. Such a broad definition includes automatic lawn sprinklers that are activated based on soil moisture, wireless electricity meters, car insurance that is tailored to driving style, or production management systems that use data on the condition of machines and the situation in the factory to predict the risk of failure (predictive maintenance) or optimal settings for the production cycle.

Among the many types of solutions offered by the IoT sector, such as Bluetooth, Wi-Fi, ZigBee, etc., that meet the objectives of communication, we distinguish those that are limited by the short range of data transmission. In order to overcome the constraints of the Low Power Wide Area Network (LPWAN), short-range protocols are introduced, which can be substituted by solutions that allow communication over long distances of several kilometres. The key features of LPWAN are as follows:

- Long range—connects rural devices from 2 km to as much as 1000 km, depending on the technology apart, and penetrates densely populated urban environments or complex interiors compared to traditional mobile communication;

- Low cost—reducing investments in expanding and upgrading infrastructure, costs of replacing power sources and ultimately operational expenditure;
- Low power—minimizes battery replacement costs with minimal power requirements and an extended battery life of up to 10 years;
- High scalability—operation of a larger number of cooperating devices in a larger area;
- High capacity—meets the needs of popular public network operators serving much larger markets by supporting millions of servicesfor each base station;
- Standardized—enables rapid deployment of IoT applications anywhere through device global availability and interoperability of LoRaWAN networks using a star topology where each network endpoint connects directly to a common central access point similar to Wi-Fi;
- Mobile—maintains communication with devices that are on the move without compromising on power consumption [1–10].

In the following analysis, the security aspect of LoRaWAN is presented in the context of using technology to monitor critical infrastructure. This article aims to assess the current state of knowledge and experience and identify the main risks and directions for further development to improve the situation in the area of cyber security for LoRaWAN-based networks. We will analyse the security aspects provided by the aforementioned technologies and carry out a comparison based on key criteria for IoT, such as network coverage and area coverage, latency, quality of service and battery life.

LoRaWAN meets the three key requirements of IoT applications (low cost, large-scale deployability, high energy efficiency) with an open standard and the construction of autonomous networks without third-party infrastructure. Many research problems remain to be solved/improved, such as resource allocation, link coordination, transmission reliability, performance and, above all, security. Even the fact that LoRaWAN has been used in several large-scale projects (solar power plant management in Carson City, NV, USA, or power monitoring in Lyon and Grenoble, France) has not solved all the research problems [11]. In this way, we have defined a research gap in the area of LoRaWAN security. The contribution of this work is to organize the knowledge in the field of LoRaWAN network security based on previous publications and own experiences and identify challenges and potential solutions. This will move LoRaWAN security research to the next stage.

Data security should be ensured along the entire information chain—from the data source (e.g., sensors) to their end user—regardless of the network topology/structure. This security should be provided at the cost of a small (1.3–7.0%) increase in power consumption in nodes per bit [12]. The optimal receiver implements a low-complexity demodulation process based on the Fast Fourier Transform (FFT). The superiority of LoRa modulation in the frequency-selective channel has been proven over frequency shift keying modulation [13]. The frequency-indexed LoRa scheme (FBI-LoRa) provides a solution to the problem of low data rates in conventional LoRa systems, which stands in the way of 5G and high-speed IoT networks. So far, at least two variants of the solution have been developed. In variant 1, the indices of the initial frequency bands (SFB) are used to carry the bits of information. To facilitate the actual implementation, the SFBs of each LoRa signal are divided into several groups before the modulation process in the proposed FBI-LoRa system. In variant 2, a combination of SFB indices and SFB group indices is used to carry the information bits. Research has shown that both variants increase transmission capacity in LoRa at the cost of a small loss in BER performance [14]. Favourable results in the area of high data rate transmission are also provided by the new system of differential chaos shift keying (DCSK) supported by index modulation (CTIM-DCSK) [15].

LoRa is a continuous phase modulation without memory, which is considered to be an orthogonal modulation only for large M. LoRa has both a continuous and a discrete spectrum. The discrete spectrum contains 1/M of the total signal power [16]. LoRa modulation with chirp spread spectrum provides energy-efficient and reliable long-range communication of system performance degradation in fading channel environments [16–18]. To remedy this, a multiple-input-multiple-output (MIMO) configuration based on space-time

block coding (STBC) schemes were introduced, which became the basis of the LoRa STBC-MIMO system [18].

2. Technological Advantage of LoRaWAN in the Context of Choosing the Most Appropriate Way of Transmitting Signals

When starting to think about choosing the most secure IoT solution, it is necessary to take into account aspects such as the longest possible unattended operation, minimal power supply to the end elements and the ability to send data in critical situations in terms of power supply. First, we will briefly compare the network architecture of the selected technologies, then analyse them from a cybersecurity perspective in a second step, and finally summarize the considerations.

LoRaWAN constitutes the official ITU-T Y.4480 standard of the International Telecommunications Union (ITU). Further research and development of the LoRaWAN protocol are conducted and managed by the open non-profit organization LoRa Alliance.LoRaWAN is a media access control (MAC) layer protocol built on LoRa technology—a wireless telecommunications network providing communication over long distances (measured in kilometres) at very low bit rates. It is a radiofrequency modulation technique that manipulates the chirp spread spectrum (CSS) to equip non-digital, battery-driven devices with wireless communication capabilities. LoRa is the signal from physical end devices that transmits data to gateways (go-between computers that route data to or from networks). LoRaWAN operates in the unlicensed radio spectrum [1–10]. LoRa operates on the following radio transmission bands (available without a license) as given in Table 1.

Table 1. LoRa bands.

Region	Band [MHz]	Duty Cycle [%]	Output Power
EU	868	<1	+13
EU	433	<1	+10
US	915	No	+27
CN	779	<0.1	+10
AS	923	No	+13
IN	865	No	+27
KR	920	No	+11
RU	864	<1	+13
AU	915	No	+28
CN	470	No	+17

A LoRaWAN network has a star topology. Within this structure, end devices are connected to a single common gateway via individual LoRaWAN links. The architecture of the aforementioned system includes the following elements (Figure 1):

- End devices—wirelessly connected via radio gateways to LoRaWAN networks;
- Gateways—forwarding received LoRaWAN radio packets to the network server;
- Network server—the center of the star topology, based on a server that manages the entire system;
- Application servers—supporting application-level services for end-users [1–10].

LoRaWAN networks in the area of communication between end devices and network servers (NS) are based on the ALOHA method (the first known system for transmitting digital data by radio). In this system, end devices send data (asynchronously transmitted packets) to a network server via one or more gateways. Both gateways and end devices are registered with one of several network server providers (private and public) [1–10].

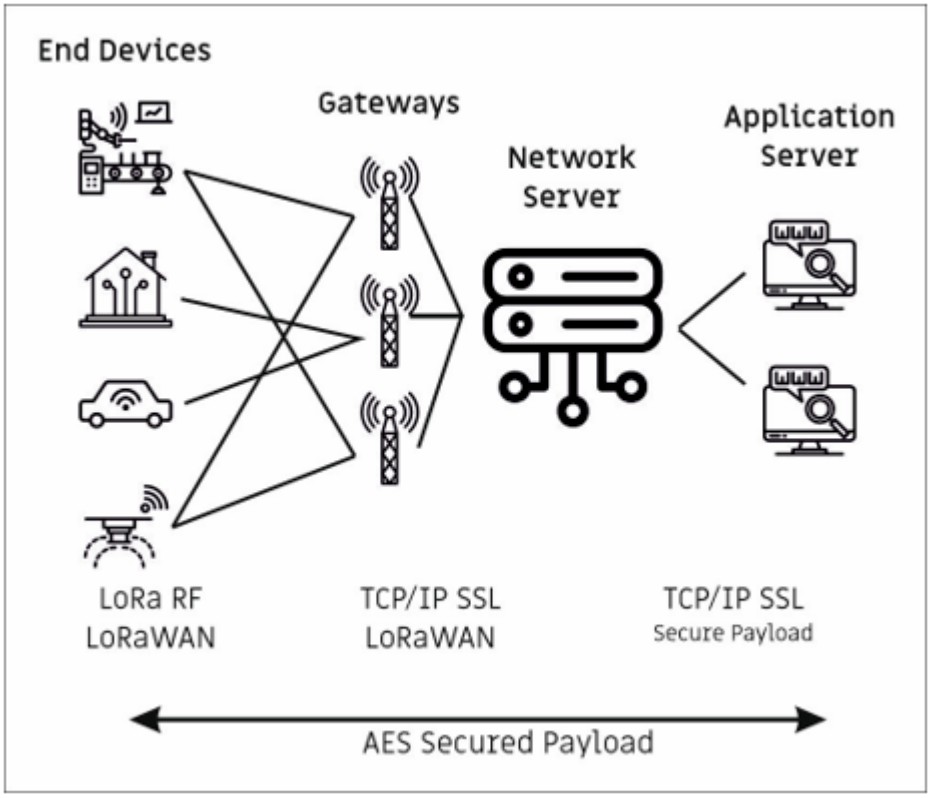

Figure 1. LoRaWAN network architecture.

3. Security in LPWAN

If IoT networks are to be widely used, for example, in critical infrastructure, they must be resilient to cybersecurity threats. Each of the last elements, by definition, provides data on which the whole strategy of action in crisis situations can be built. In this section, we will analyse the standards I have chosen in terms of the mechanisms that ensure security.

The Industrial Internet Consortium (IIC) has defined five characteristics that a device must meet to be considered safe [19]:

- Harmlessness—the device must operate without posing a direct or indirect threat to human life and health;
- Protection—the device must be protected against unauthorized use, both intentional and accidental;
- Privacy—information collected shall only be made available to authorized entities, and the user shall be informed of and consent to the data gathered by the device;
- Reliability—the device must perform the tasks required of it correctly, in the conditions for which it is intended, and within the time specified by the manufacturer;
- Flexibility—the equipment must retain the functions necessary to maintain the system in the event of failure [1–10,19].

LoRaWAN defines 128-byte security keys as network session key (NwkSKey), application session key (AppSKey) and application key (AppKey) using AES-128, similar to the algorithm in the 802.15.4 standard. This is implemented in several stages: when a device joins the network/activation, an AppSKey (private) and a NwkSKey (shared with the network) network session key are generated, used for the duration of the session and unique for each device/for each session. In addition, with static activation, these keys remain unchanged, and with dynamic activation, these keys are regenerated with each activation.

NwkSKey is used for interaction between the node and the web server, validating the integrity of each message through its Message Integrity Code (MIC) control-based AES-CMAC. In this way, the MIC prevents intentional manipulation of the message (similar

to a checksum but with greater cryptographic power). The aforementioned mechanism is also used to map the non-universal device address (DevAddr) to the unique DevEUI and AppEUI.

AppSKey is used to encrypt and decrypt the message container between the node and the Handler/Application Server component of the IoT network.

The AppKey is only shared between the device and the application. Dynamically activated devices (OTAA) use an AppKey to derive two AppSKeys during the activation procedure. In IoT, there are two options: a default AppKey to activate all devices or an AppKey customized for each device.

The three classes of end devices in LoRAWAN are shown in Table 2.

Table 2. Classes in LoRaWAN.

Name	Application
A (All)	• Must be supported by all devices; • Most energy-efficient communication class; • Includes battery-powered sensors or actuators with no delay limitation.
B (Beacon)	• Energy-efficient communication class for downlink with latency control; • Use of slot communication synchronized with network Bacon; • Battery-based power supply.
C (Continuous)	• Devices that can afford continuous listening, without downlink communication delays; • Main driver.

3.1. Class-A End Devices (Bi-Directional)

After sending the uplink, the terminal listens for messages on the 1 s and 2 s uplink before returning to sleep mode:

- Purpose: the lowest power end-device system;
- Each uplink transmission of the end device is followed by two short downlink reception time windows;
- The downlink communication from the server occurs shortly after the end device sends the uplink transmission;
- The choice of transmission time is based on the communication needs of the end device i.e., as in the ALOHA protocol.

3.2. Class-B End Devices with Scheduled Receive Slots (Bi-Directional)

Because Class A has priority, the device periodically replaces ping slots with an uplink sequence, followed by receive windows when the device has a need:

- Mid-power consumption;
- At the scheduled time, additional reception windows are opened;
- To realize this, the end device receives the time synchronized by the beacon from the gateway.

3.3. Class-C End Devices with Maximal Receive Slots (Bi-Directional)

Class-C end devices keep the reception windows open almost continuously, only closed when transmitting large power consumption.The terminal must follow the following activation procedure to connect to the LoRaWAN network:

1. Over-the-air activation (OTAA):

The LoRaWAN end device and the application server share a secret key (AppKey)—during the attachment procedure, they exchange input data with each other to generate two session keys:

- NwkSKey for MAC commands encryption;

- AppSKey for application data encryption.

2. Activation by personalization (ABP)

NwkSkey and AppSkey are previously stored on the LoRaWAN end device—it sends the data directly to the LoRaWAN network.

NS is used to manage gateways, terminals, applications and users across the LoRaWAN network. A typical LoRaWAN NS has the following functionalities:

- Establishment of secure AES-128 protected connections for message transport between end devices and application server (end-to-end security);
- Verification of device addresses;
- Authentication of end devices and integrity of messages from them;
- Deduplication of uplink messages;
- Selection of the gateway that is most suitable for sending downlink messages;
- Sending ADR messages to optimize device data rates;
- Acknowledging uplink data messages;
- Directing uplink messages to the appropriate application servers;
- Forwarding join requests and join accept messages between devices and the join server;
- Responding to MAC layer commands.

4. Discussion

The Discussion section is divided into the following subsections: challenges, solutions, comparison, taxonomy, limitations of own research and directions for further research.

4.1. Challenges

Improvement in cyber security in LoRaWAN can be achieved threefold: by AI, by adaptive data rates and energy consumption, and thanks to lightweight cryptography. The consensus is that big data can be gathered by various IoT solutions and analysed using AI methods and techniques dedicated to specific applications, services, products and audience groups (logistics, manufacturing, customer service, cars, boats, etc.), including novel human-to-human (H2H), human-to-machine (H2M), machine-to-human (M2H), and machine-to-machine (M2M)communication. Basic solutions in the area of artificial intelligence include traditional neural networks, convolutional neural networks (CNNs belonging to deep learning), recurrent neural networks and long short-term memory (LSTM), especially for image and time series recognition.

Improving the performance and safety of the aforementioned real-time solutions (e.g., for driver assistance and autonomous vehicles) is one of the biggest challenges to their rapid deployment. Several optimization solutions (adaptive moment estimation algorithm (Adam), Nesterov-accelerated adaptive moment estimation (Nadam), and stochastic gradient descent algorithm (SGD)) have been developed to increase the speed of solution finding, often based on hybrid (mathematical-engineering-computing) approaches. However, further development is still required: deep learning for massive data sets and critical data; enhancing IoT security and privacy; advanced IoT data preprocessing and AI-based modelling, including those dedicated to specific IoT applications (from agriculture, forestry and fisheries through industry, health, science and education to culture and the arts) [1–10].

4.2. Solutions

Most commonly, concepts based on LoRaWAN with low power consumption and low cost are proposed, supported by machine learning techniques (data-driven approach) and high accuracy in localization/movement analysis thanks to signal strength measurements of the transmitting device (received signal strength indicator (RSSI) and signal-to-noise ratio (SNR), up to 98.8%) [20].

The RSSI and SNR are two of the most commonly used indicators of signal strength. In wireless communications, good signal strength and S/N ratio are required to distinguish the original signal from the modulation.

The Received Signal Strength Indicator (RSSI) is a term used to measure the relative quality of a received signal to a client device, but it has no absolute value. In other words, it represents the total signal power in the channel bandwidth.The RSSI includes useful signal, background noise and interference. It is only supplied by the gateway for each received communication and is therefore only available for upstream (device-to-gateway) communications. It is an important parameter for both gateways and terminals.

The IEEE 802.11 standard defines that RSSI can be on a scale from 0 to 255 and that each chipset manufacturer can define its own maximum RSSI value. This value is presented as a negative number; the closer the value is to 0, the stronger the signal received.

The main factors affecting RSSI are as follows:

- Loss of the cable/connector;
- Gain of the antenna;
- Directional losses.

The signal-to-noise ratio (S/N or SNR) is the ratio of the received signal power to the noise floor.

This relationship is expressed by the following equation:

$$SNR(dB) = P_{received_{signal}}(dBm) - P_{noise}(dBm) \quad (1)$$

Positive SNR means that the signal power is greater than the noise power and the receiver can demodulate the signal. However, LoRa can also demodulate signals below the noise floor.

The Table 3 below shows the minimum SNR required for demodulation at different spreading factors:

Table 3. Minimum SNR required for demodulation at different spreading factors.

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

The SNR indicates that the signalpower has a lower value than the noise power. For example, the value of −30 dB is below the minimum SNR of −20 dBm @ SF12, so it does not provide a guarantee that the receiver will be capable of demodulating the signal.

The modernized adaptive-data-rate ADR++ algorithm uses an energy efficiency regulator based on the analysis of the aggregated energy use of all nodes to adjust the average SNR of recent records. This provides an increase in network-wide power consumption reduction of up to 17.5% and increases the packet success rate by up to 31.55% compared to ADR+ [21]. It supports confidentiality, integrity and authentication, which are difficult in IoT devices considering reduced energy and computing resources. For the above reasons, the applications support lightweight encryption algorithms featuring dedicated communication protocols and lightweight security—notably reduced Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) [22].

An additional requirement is the IoT network architectures that are optimal in terms of environmental sustainability. In addition to the appropriate range, power and support for a wide range of devices, the virtualization of LoRaWAN network units and programmatic network definition has been introduced here. The new MQTT2MULTICAST protocol

improves network latency by up to 90% and reduces SDN traffic load by 55% with high scalability (up to tens of thousands of LoRaWAN gateways) using commercial solutions [23]. A new anti-server and endpoint spoofing authentication system for multiple endpoints (as part of the LoRa Alliance) can reduce connection delays caused by network server verification messages [24]. Long range, low data volumes, a very large number of devices, low cost and low energy consumption are the requirements for LPWAN technologies, which are increasingly a key part of IoT applications. A comparative review of the five LPWAN technologies (LoRa/LoRaWAN, NB-IoT, SigFox, Telensa and Ingenu/RPMA) yielded results that in terms of network throughput, adaptive data rate, device lifetime cost, LoRa/LoRaWAN and SigFox are the best, and in terms of high quality of service and low latency, NB-IoT is the best. The availability and efficiency of simulators are becoming increasingly important, and LoRa/LoRaWAN is king [25]. Network performance analysis shows that LoRaWAN is cheaper and more energy efficient than NB-IoT, but NB-IoT provides higher network connection bandwidth, especially in developing countries [26]. Battery-less devices, where energy collected from the environment is stored in small capacitors, are already an alternative to sustainable IoT today; however, they cause unpredictability and intermittent behaviour in the device. Problems are prevented by scheduling tasks, detecting transmissions on a battery-free LoRaWAN device, and building a balance between sleep, device shutdown and application task execution, which is an optimization problem. Class A LoRaWAN can measure temperature and transmit its value at least once every 5–100 s, depending on the capacity of the capacitor used and the optimization of the operating mode [27]. IoT security and privacy can be compromised in any work environment (even in agriculture), hence the need to use multi-layered architectures suitable for dynamically changing distributed cyber-physical environments [28]. Ensuring security and privacy in a network of fully distributed low-cost network services requires a multi-layer (e.g., five-layer) architecture of a distributed hotspot network. This complex approach provides scalability, rented access data gateway networking, optimal coverage, better network security and better data rates, where blockchain reinforces the architecture's decentralized behaviour [29]. Test stands are being built for the experimental validation and security of such networks [30]. Using static keys (as most encryption software does) to authenticate and encrypt the node is not as secure as session keys in LoRaWAN, work is underway on a centralized lightweight session key mechanism for Blom-Yang (BYka) key agreement standards [31]. The volume is also affected by compatibility between the LoRaWAN protocols in the two main versions, v1.0 and v1.1 [32]. According to research so far, only 66.67% of packets coming from an illegal gateway are dropped [33]. Fast and reliable detection of wireless attacks (i.e., at the physical layer) improves the integrity and reliability of the LoRaWAN network. The vulnerability review also highlights the need to improve key refresh and device authentication [34]. The new key management protocol supports LoRaWAN key updates and is based on i.a. hash chain generation (sharing a common hash chain) and using the salt hashing algorithm to encrypt the keys [35]. The key management part of LoRaWAN version 1.1 remains ambiguously defined, hence various attempts to develop a key management scheme: key generation, key backup, key update and backward compatibility of keys [36]. Wireless channels are also used in the urban tunnel environment, which is a complex and demanding environment for the propagation of radio waves (limited dimensions, built-in metal elements). Even in such conditions, proper planning can ensure optimal coverage and good quality of service in the LoRaWAN and ZigBee networks [37]. Key management architecture in LoRaWAN networks based on blockchain and smart contracts (open source) was also developed, achieving similar execution times and latency values in small and medium networks as in their traditional counterparts [38]. Nevertheless, breaches can still exploit specification shortcomings and limited device performance, e.g., during wireless activation (OTAA) of LoRa nodes, hence the Secure-Packet-Transmission (SPT) project under the LoRaWAN v1.1 standard and using One-Time Password (OTP) [39,40]. A compromise is needed because a highly secured protocol consumes more battery power due to the increased computational

cost [41]. Newly implemented communication protocols should be designed with security in mind—vulnerabilities in key management are still visible [42]. Flawed DRAM chips in common Android/ARM-based mobile platforms are not immune to deterministic Rowhammer attacks [43]. Resilience testing of Industrial IoT (IIoT) using LoRaWAN includes testing the resilience of LoRaWAN gateways to malicious attacks on the network and firmware of the IIoT node, by eavesdropping, replaying network traffic, modifying firmware or injecting malicious code (into the firmware, operating system and kernel driver). A simulation-based analysis of the methods allows the validation of security architecture concepts to ensure full IIoT security in a LoRaWAN environment [44]. Gateways in LoRaWAN used for IIoT can be vulnerable to malicious attacks that are difficult to mitigate, which can cause failures and loss of performance in network traffic. The use of public key infrastructure (PKI) with a two-tier certification authority (CA) configuration—a root CA and an intermediate CA—has been proposed as a solution. This ensures that even ca. 2/3 of incoming packets from the illegal gateway are rejected [33]. Hardware mechanisms were also developed to ensure secure storage of keys and electronic signatures (traceability, immutability) using secure RFID/NFC modules and IoT infrastructure using LoRaWAN in combination with Hyperledger Fabric. This runs smoothly for >70 transactions per second for 16 peers [45]. LoRaWAN vulnerabilities identified to date include the following:

- Plaintext recovery;
- Malicious modification of message;
- Forgery of the delivery report;
- Replay attack (i.e., selective denial of service on an IoT device);
- Battery depletion attack.

Research is ongoing to protect against or mitigate the effects of the above attacks [46]. It is also important to bear in mind that, for example, in an urban or industrial environment, LoRaWAN deployments will continue to operate for up to many decades, while continuously maintaining operational security and upgrading security standards. Even surveys have been developed in the area of evaluating LoRaWAN security changes over time [47].

4.3. Comparison

Bluetooth Low Energy (BLE) and Zigbee were selected for comparison with LoRaWAN in terms of security as its direct and biggest competitors. LoRa has greater coverage, lower power consumption, requires less infrastructure and is cheaper, but it has lower data speeds and higher latency than its competitors. LoRaWAN has become the go-to network (preferred technology) for IoT devices that can be easily integrated for better functionality, but it is unclear whether this will remain the case once the 5G network infrastructure is extended. Details of the network security of two competing technologies are outlined below, but a lot depends on specific settings, including topology and power consumption.

4.3.1. Bluetooth Low Energy

BLE is often referred to as a Bluetooth Smart Module. It is a lightweight variant of Bluetooth and is described in the Bluetooth 4.0 specification. Before being adopted by the SIG, it was developed internally as Nokia's Wibree product. It was added to the Bluetooth standard in 2010. The BLE communication protocol is optimized for the fast transmission of small blocks of data at cyclic intervals. This allows the host processor to run in low-energy mode for as long as possible while no data is being transmitted. Another important element is the short time it takes to establish a connection for data exchange—just a few milliseconds.

The Bluetooth SIG describes a number of profiles—principles of operation of the device in specific applications—for low-power devices based on the original Bluetooth specification. The expectation is that manufacturers will implement the aforementioned device-dedicated specifications in order to achieve compatibility. It is possible for a device to implement many such profiles. Most of the currently used low-power profiles are derived

from the generic attribute profile (GATT). The Bluetooth mesh profile is an exception to this rule and is based on a General Access Profile (GAP) [1].

Power consumption has been reduced at each layer of the communication architecture. In the physical layer, the modulation index has been increased in comparison with classic Bluetooth, which has made it possible to limit the current in the transmitter and receiver circuits. The link layer, which also helps to reduce power consumption, has been adapted to quickly establish and reestablish connections. The Bluetooth Low Energy controller is responsible for a number of important tasks, such as connection establishment and duplicate packet rejection, so that the device's main processor can stay in low power mode for longer periods. They are as follows:

- Supply current—the maximum current that Bluetooth LE modules draw from the 3.7 V source is about 15 mA. With classic Bluetooth, it is 40 mA or more. This makes it possible to work for months or even years on a single battery;
- Data transmission—very short data packets (from 8 to 27 octets) are supported, transmitted at speeds of up to 1 Mb/s;
- Frequency hopping—known from other Bluetooth implementations, the mechanism of hopping the operating frequency. Used to minimize interference with other technologies in the 2.4 GHz band;
- Host Control—Places most of the communication intelligence in the controller, allowing the host to sleep for extended periods and only be woken by the controller when action is required. This provides the greatest energy savings in portable devices, where power consumption is typically much higher than that of the communication controller;
- Delays—Bluetooth Smart allows you to establish a connection and transfer data in as little as 3 ms. This allows the application to establish a connection, transfer data and then quickly disconnect;
- Range—the increased modulation index allows connections over distances of more than 100 m;
- Stability—a 24-bit CRC checksum is used on all packets;
- Topology—One-to-one and one-to-many star topology connections are possible. 32-bit addressing isused for eachslave data packet [1–10].

4.3.2. Zigbee

ZigBee is a protocol for data transmission in wireless networks, such as mesh and cluster trees. Its operation is similar to Wi-Fi, but it is characterized by lower energy consumption, low bit rates (up to 200 and 50 kbps), and a range of up to 100 m. Communication in ZigBee is two-way, meaning that any device can receive or send a signal, and some can even forward it. One of its advantages is that it can be accessed instantly, which is why it is so popular in motion sensors, for example.

ZigBee at the lower layers of the model (PHY and MAC) uses the IEEE 802.15.4 standard, which provides wireless transmission in the 2.4 GHz band (globally) and 868 MHz and 915 MHz (in selected regions of the world) [1]. The media access scheme is CSMA/CA. The modulation is O-QPSK for 2.4 GHz and BPSK for 868/915 MHz. In the 2.4 GHz band, there are 16 channels with a width of 5 Mhz.

ZigBee technology was developed by the ZigBee Alliance in 2002. It brings together several hundred world-renowned companies, including Samsung, Philips, Siemens, Bosch, Motorola, Amazon and Xiaomi. Version 1.0 of the ZigBee specification was created in 2004, while the ZigBee 3.0 specification was introduced in 2016.

ZigBee devices can be divided into three types, each performing a different function:

- Coordinator—the central device. Each network can have only one of these devices. The coordinator acts as the starting node from which other devices can join. It usually acts as a data collection device. The coordinator is usually limited in the number of devices that can connect to it. The most popular coordinators include Samsung SmartThings, Apple HomeKit, Bosch Home Connect, Google Home Hub, Amazon Echo and Nest Audio;

- Router—this device is similar in function to a traditional network router. Its job is to amplify the signal and increase the range, creating hops. A repeater can be a device that plugs into the mains, such as a light bulb, switch, relay, smart socket or wall switch. However, it must have an N wire. Devices without N are not routers;
- End device—this is a battery-powered device such as a motion, smoke or flood sensor. Such a device is connected directly to the gate and provides it with information about its status and what it is currently measuring. To reduce power consumption, the device can temporarily go into sleep mode and wake up in milliseconds. To achieve ZigBee certification, the device must last at least 2 years on battery power [1–10].

The ZigBee network topologies are as follows:

- Star topology—mainly used in home networks. A single device acts as the coordinator, and all other end devices communicate directly with it. The disadvantage of this type of network is that if the coordinator fails, the whole network fails;
- Tree topology—a popular unit consisting of a root and its dependent nodes. In the case of ZigBee, the coordinator plays the role of the root, and end devices can only be placed on the last branches. This topology allows more nodes to be connected, thus covering a larger area. The disadvantage is that there are delays in transmission, and the failure of one node can affect the operation of other devices;
- Mesh topology—the most complex network structure. Each device can communicate with another, either directly or through other devices. This is the best ZigBee network topology because if one node fails, data can be taken over by another device [1–10].

4.4. Taxonomy

The LoRaWAN taxonomy is based on a comprehensive set of standards, regulations and best practices. The design of LoRaWAN security follows state-of-the-art principles, i.e., the use of standardised, proven algorithms and end-to-end security. The basic properties supported in LoRaWAN security include mutual authentication, integrity protection and confidentiality [48].

What is important in the context of the taxonomy is that it is intended to bring together national cyber security centres into a coherent and efficient network—hence the taxonomy of the Joint Research Centre (JRC) is intended to unify cyber security terminology, definitions and domains in order to, on the one hand, cover all aspects and competences of cyber security and, on the other, to prevent confusion and misunderstanding when planning and implementing national and international projects in the area of cyber security and privacy research and innovation. Hence, it was rightly proposed to base cyber security domains on four dimensions: research, sector, technology and use cases. This will identify and support developments at different levels, from a network of European cyber security research and competence centres (including universities and research centres as the basis of the European Cyber Security Atlas) to leading technologies serving the different paradigms supported by the EU (from Industry 4.0 and Industry 5.0 to the Green Deal). It is noteworthy that this taxonomy supports horizontal policies.

With a unified approach, cyber security has become an easier priority for organisations to achieve and can be used more easily to build awareness among the public, especially with the prevalence of mobile internet access in the market for services, not only industrial ones.

The existing regulatory framework provides a number of good new options for LoRaWAN, including more options for gateways.

In 2023, the European Commission proposed an EU Cyber Solidarity Act to improve the response to cyber threats across the EU. comprising a European Cyber Security Shield and a comprehensive cyber crisis response mechanism [49].

4.5. Limitations of Our Own Studies

Despite the increase in the number of publications and presented solutions, the key topics are still issues related to the physical and network layers and possible improvements

and extensions of current standards [22,50,51]. There is a lack of practical implementation of existing analyses of weaknesses and threats.

4.6. Directions for Future Research

The development of IoT systems, including the Internet of Vehicles (IoV), depends on achieving a breakthrough in application and data processing efficiency with limited resources and network heterogeneity in order to develop new services with low latency, high throughput, accuracy and reliability. This is necessary to enable the creation of smart factories and smart cities for our digital societies that are creative, safe and collaborative [51–53]. There are already new opportunities related to, among others, space, air, terrestrial and (sub)marine cellular networks, collaborative learning, collaborative intelligence, security and privacy [24,54,55].

5. Conclusions

Security remains one of the key issues with wireless IoT technologies. The large number of proposed concepts confirms that in recent years there have been a number of publications on security, including LoRa and LoRaWAN, which have grown tremendously.

LoRaWAN is, in our opinion, the most secure solution—it has authentication and encryption, but networks and devices can be compromised if the security keys used are not randomly distributed between devices or if cryptographic numbers (nonces) are reused. It is advisable to use only LoRaWAN-certified CM devices to ensure that the device has been tested to comply with the standard. LoRaWAN provides application providers with dedicated end-to-end encryption. This must be accompanied by secure device/network implementation and deployment to maintain the built-in security mechanisms.

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

Funding: The work presented in the paper has been financed under a grant to maintain the research potential of Kazimierz Wielki University.

Data Availability Statement: Data is unavailable due to privacy and cyber security.

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

References

1. Gomez, C.; Oller, J.; Paradells, J. Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology. *Sensors* **2012**, *12*, 11734–11753. [CrossRef]
2. Sornin, N.; Luis, M.; Eirich, T.; Kramp, T.; Hersent, O. LoRa Specification 1.0. Lora Alliance Standard Specification. 2015. Available online: www.lora-alliance.org (accessed on 30 April 2023).
3. Adelatando, F. The Things Network Global Team, LoRaWAN Distance World Record Broken, Twice. Available online: www.thethingsnetwork.org (accessed on 30 April 2023).
4. Vilajosana, X.; Tuset-Peiro, P.; Martinez, B.; Melià-Seguí, J.; Watteyne, T. Understanding the Limits of LoRaWAN. *IEEE Commun. Mag.* **2017**, *55*, 34–40.
5. Seller, O.B.A. Wireless Communication Method. U.S. Patent No. 9,647,718, 9 September 2015.
6. Lee, C.-J.; Ryu, K.-S.; Kim, B.-J. Periodic Ranging in a Wireless Access System for Mobile Station in Sleep Mode. U.S. Patent No. 7,194,288, 20 March 2007.
7. Alghamdi, A.M.; Khairullah, E.F.; Al Mojamed, M.M. LoRaWAN Performance Analysis for a Water Monitoring and Leakage Detection System in a Housing Complex. *Sensors* **2022**, *22*, 7188. [CrossRef] [PubMed]
8. Quigley, T.J.; Rabenko, T. Latency Reduction in a Communications System. U.S. Patent No. 7,930,000, 19 April 2011.
9. Bankov, D.; Khorov, E.; Lyakhov, A. On the Limits of LoRaWAN Channel Access. In Proceedings of the 2016 International Conference on Engineering and Telecommunication (EnT), Moscow, Russia, 29–30 November 2016; pp. 10–14.
10. Seneviratne, P. *Beginning LoRa Radio Networks with Arduino—Build Long Range, Low Power Wireless IoT Networks*; eBook; Apress: New York, NY, USA, 2019.

11. Sundaram, J.P.S.; Du, W.; Zhao, Z. A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 371–388. [CrossRef]
12. Prodanović, R.; Rančić, D.; Vulić, I.; Zorić, N.; Bogićević, D.; Ostojić, G.; Sarang, S.; Stankovski, S. Wireless Sensor Network in Agriculture: Model of Cyber Security. *Sensors* **2020**, *20*, 6747. [CrossRef]
13. Vangelista, L. Frequency Shift Chirp Modulation: The LoRa Modulation. *IEEE Signal Process. Lett.* **2017**, *24*, 1818–1821. [CrossRef]
14. Ma, H.; Fang, Y.; Cai, G.; Han, G.; Li, Y. A New Frequency-Bin-Index LoRa System for High-Data-Rate Transmission: Design and Performance Analysis. *IEEE Internet Things J.* **2022**, *9*, 12515–12528. [CrossRef]
15. Fang, Y.; Zhuo, J.; Ma, H.; Mumtaz, S.; Li, Y. Design and Analysis of a New Index-Modulation-aided DCSK System with Frequency-and-Time Resources. *IEEE Trans. Veh. Technol.* **2023**, *99*, 1–14. [CrossRef]
16. Chiani, M.; Elzanaty, A. On the LoRa Modulation for IoT: Waveform Properties and Spectral Analysis. *IEEE Internet Things J.* **2019**, *6*, 8463–8470. [CrossRef]
17. Ma, H.; Cai, G.; Fang, Y.; Chen, P.; Han, G. Design and Performance Analysis of a New STBC-MIMO LoRa System. *IEEE Trans. Commun.* **2021**, *69*, 5744–5757. [CrossRef]
18. Elshabrawy, T.; Joerg, R. Closed-Form Approximation of LoRa Modulation BER Performance. *IEEE Commun. Lett.* **2018**, *22*, 1778–1781. [CrossRef]
19. Buchheit, M.; Hirsch, F.; Martin, R.A.; Bemmel, V.; Espinosa, A.J.; Zarkout, B.; Hart, C.F.; Tseng, M. Industrial Internet Consortium (IIC) The Industrial Internet of Things Trustworthiness Framework Foundations An Industrial Internet Consortium Foundational Document. Version V1.00—2021-07-15. Available online: https://www.google.com.hk/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&ved=0CAIQw7AJahcKEwioh-ry6KD_AhUAAAAAHQAAAAAQAg&url=https%3A%2F%2Fwww.iiconsortium.org%2Fpdf%2FTrustworthiness_Framework_Foundations.pdf&psig=AOvVaw0EBJFtHbs8LhCv9N2km7Qq&ust=1685665852309027 (accessed on 21 May 2023).
20. Perković, T.; DujićRodić, L.; Šabić, J.; Šolić, P. Machine Learning Approach towards LoRaWAN Indoor Localization. *Electronics* **2023**, *12*, 457. [CrossRef]
21. Al-Gumaei, Y.A.; Aslam, N.; Aljaidi, M.; Al-Saman, A.; Alsarhan, A.; Ashyap, A.Y. A Novel Approach to Improve the Adaptive-Data-Rate Scheme for IoTLoRaWAN. *Electronics* **2022**, *11*, 3521. [CrossRef]
22. Goulart, A.; Chennamaneni, A.; Torre, D.; Hur, B.; Al-Aboosi, F.Y. On Wide-Area IoT Networks, Lightweight Security and Their Applications—A Practical Review. *Electronics* **2022**, *11*, 1762. [CrossRef]
23. Navarro-Ortiz, J.; Chinchilla-Romero, N.; Delgado-Ferro, F.; Ramos-Munoz, J.J. A LoRaWAN Network Architecture with MQTT2MULTICAST. *Electronics* **2022**, *11*, 872. [CrossRef]
24. Fan, C.-I.; Zhuang, E.-S.; Karati, A.; Su, C.-H. A Multiple End-Devices Authentication Scheme for LoRaWAN. *Electronics* **2022**, *11*, 797. [CrossRef]
25. Almuhaya, M.A.M.; Jabbar, W.A.; Sulaiman, N.; Abdulmalek, S. A Survey on LoRaWAN Technology: Recent Trends, Opportunities, Simulation Tools and Future Directions. *Electronics* **2022**, *11*, 164. [CrossRef]
26. Ugwuanyi, S.; Paul, G.; Irvine, J. Survey of IoT for Developing Countries: Performance Analysis of LoRaWAN and Cellular NB-IoT Networks. *Electronics* **2021**, *10*, 2224. [CrossRef]
27. Sabovic, A.; Delgado, C.; Subotic, D.; Jooris, B.; De Poorter, E.; Famaey, J. Energy-Aware Sensing on Battery-Less LoRaWAN Devices with Energy Harvesting. *Electronics* **2020**, *9*, 904. [CrossRef]
28. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access* **2020**, *8*, 34564–34584. [CrossRef]
29. Ray, P.P.; Skala, K. Internet of Things Aware Secure Dew Computing Architecture for Distributed Hotspot Network: A Conceptual Study. *Appl. Sci.* **2022**, *12*, 8963. [CrossRef]
30. Pospisil, O.; Fujdiak, R.; Mikhaylov, K.; Ruotsalainen, H.; Misurec, J. Testbed for LoRaWAN Security: Design and Validation through Man-in-the-Middle Attacks Study. *Appl. Sci.* **2021**, *11*, 7642. [CrossRef]
31. Pathak, G.; Gutierrez, J.; Ghobakhlou, A.; Rehman, S.U. LPWAN Key Exchange: A Centralised Lightweight Approach. *Sensors* **2022**, *22*, 5065. [CrossRef]
32. Loukil, S.; Fourati, L.C.; Nayyar, A.; Chee, K.-W.-A. Analysis of LoRaWAN 1.0 and 1.1 Protocols Security Mechanisms. *Sensors* **2022**, *22*, 3717. [CrossRef] [PubMed]
33. Mohamed, A.; Wang, F.; Butun, I.; Qadir, J.; Lagerström, R.; Gastaldo, P.; Caviglia, D.D. Enhancing Cyber Security of LoRaWAN Gateways under Adversarial Attacks. *Sensors* **2022**, *22*, 3498. [CrossRef]
34. Ruotsalainen, H.; Shen, G.; Zhang, J.; Fujdiak, R. LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. *Sensors* **2022**, *22*, 3127. [CrossRef]
35. Hakeem, S.A.A.; El-Kader, S.M.A.; Kim, H. A Key Management Protocol Based on the Hash Chain Key Generation for Securing LoRaWAN Networks. *Sensors* **2021**, *21*, 5838. [CrossRef]
36. Chen, X.; Lech, M.; Wang, L. A Complete Key Management Scheme for LoRaWAN v1.1. *Sensors* **2021**, *21*, 2962. [CrossRef]
37. Celaya-Echarri, M.; Azpilicueta, L.; Lopez-Iturri, P.; Picallo, I.; Aguirre, E.; Astrain, J.J.; Villadangos, J.; Falcone, F. Radio Wave Propagation and WSN Deployment in Complex Utility Tunnel Environments. *Sensors* **2020**, *20*, 6710. [CrossRef]
38. Ribeiro, V.; Holanda, R.; Ramos, A.; Rodrigues, J.J.P.C. Enhancing Key Management in LoRaWAN with Permissioned Blockchain. *Sensors* **2020**, *20*, 3068. [CrossRef]

39. Gao, S.-Y.; Li, X.-H.; Ma, M.-D. A Malicious Behavior Awareness and Defense Countermeasure Based on LoRaWAN Protocol. *Sensors* **2019**, *19*, 5122. [CrossRef] [PubMed]
40. Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebeke, J. A Survey of LoRaWAN for IoT: From Technology to Application. *Sensors* **2018**, *18*, 3995. [CrossRef] [PubMed]
41. You, I.; Kwon, S.; Choudhary, G.; Sharma, V.; Seo, J.T. An Enhanced LoRaWAN Security Protocol for Privacy Preservation in IoT with a Case Study on a Smart Factory-Enabled Parking System. *Sensors* **2018**, *18*, 1888. [CrossRef] [PubMed]
42. Sanchez-Iborra, R.; Sánchez-Gómez, J.; Pérez, S.; Fernández, P.J.; Santa, J.; Hernández-Ramos, J.L.; Skarmeta, A.F. Enhancing LoRaWAN Security through a Lightweight and Authenticated Key Management Approach. *Sensors* **2018**, *18*, 1833. [CrossRef]
43. Van der Veen, V.; Fratantonio, Y.; Lindorfer, M.; Gruss, D.; Maurice, C.; Vigna, G.; Bos, H.; Razavi, K.; Giuffrida, C. Drammer: Deterministic Rowhammer Attacks on Mobile Platforms. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1675–1689.
44. Coppola, M.; Kornaros, G. Automation for Industry 4.0 by using Secure LoRaWAN Edge Gateways. In *Multi-Processor System-on-Chip*; Andrade, L., Rousseau, F., Eds.; ISTE Ltd.: London, UK; Wiley: New York, NY, USA, 2021; Volume 2.
45. Bakoyiannis, D.; Tomoutzoglou, O.; Kornaros, G.; Coppola, M. From Hardware-Software Contracts to Industrial IoT-Cloud Block-chains for Security, Privacy and Authenticity. In Proceedings of the 2021 Smart Systems Integration (SSI), Grenoble, France, 27–29 April 2021; pp. 1–4. [CrossRef]
46. Yang, X.; Karampatzakis, E.; Doerr, C.; Kuipers, F. Security Vulnerabilities in LoRaWAN. In Proceedings of the 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, FL, USA, 17–20 April 2018; pp. 129–140. [CrossRef]
47. Hessel, F.; Almon, L.; Hollick, M. LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and their Systematic Mitigation. *ACM Trans. Sen. Netw.* **2023**, *18*, 70. [CrossRef]
48. European Commission, Joint Research Centre (JRC). JRC Cybersecurity Taxonomy. 2021. [Dataset] PID. Available online: http://data.europa.eu/89h/d2f56334-a0df-485b-8dc8-2c0039d31122 (accessed on 25 May 2023).
49. EU Cyber Solidarity Act. Available online: https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-cyber-solidarity-act (accessed on 29 May 2023).
50. Delgado-Ferro, F.; Navarro-Ortiz, J.; Chinchilla-Romero, N.; Ramos-Munoz, J.J. A LoRaWAN Architecture for Communications in Areas without Coverage: Design and Pilot Trials. *Electronics* **2022**, *11*, 804. [CrossRef]
51. Rojek, I.; Macko, M.; Mikołajewski, D.; Saga, M.; Burczynski, T. Modern methods in the field of machine modeling and simulation as a research and practical issue related to Industry 4.0. *Bull. Pol. Acad. Sci. Tech. Sci.* **2021**, *69*, e136719. [CrossRef]
52. Rojek, I.; Mikołajewski, D.; Macko, M.; Szczepański, Z.; Dostatni, E. Optimization of Extrusion-Based 3D Printing Process Using Neural Networks for Sustainable Development. *Materials* **2021**, *14*, 2737. [CrossRef]
53. Rojek, I.; Mikołajewski, D.; Kotlarz, P.; Macko, M.; Kopowski, J. Intelligent system supporting technological process planning for machining and 3D printing. *Bull. Pol. Acad. Sci. Tech. Sci.* **2021**, *69*, e136722.
54. Sales Mendes, A.; Jiménez-Bravo, D.M.; Navarro-Cáceres, M.; Reis QuietinhoLeithardt, V.; Villarrubia González, G. Multi-Agent Approach Using LoRaWAN Devices: An Airport Case Study. *Electronics* **2020**, *9*, 1430. [CrossRef]
55. Gava, M.A.; Rocha, H.R.O.; Faber, M.J.; Segatto, M.E.V.; Wörtche, H.; Silva, J.A.L. Optimizing Resources and Increasing the Coverage of Internet-of-Things (IoT) Networks: An Approach Based on LoRaWAN. *Sensors* **2023**, *23*, 1239. [CrossRef] [PubMed]