sensors

Article

A Survey on the Security Challenges of Low-Power Wireless Communication Protocols for Communicating Concrete in Civil Engineerings

Gaël Loubet [1,*], Eric Alata [1], Alexandru Takacs [2] and Daniela Dragomirescu [1,*]

[1] LAAS-CNRS, Université de Toulouse, CNRS, INSA, 7, Avenue du Colonel Roche, 31400 Toulouse, France
[2] LAAS-CNRS, Université de Toulouse, CNRS, UPS, 7, Avenue du Colonel Roche, 31400 Toulouse, France
[*] Correspondence: gael.loubet@laas.fr (G.L.); daniela.dragomirescu@laas.fr (D.D.)

Abstract: With the increase in low-power wireless communication solutions, the deployment of Wireless Sensor Networks is becoming usual, especially to implement Cyber-Physical Systems. These latter can be used for Structural Health Monitoring applications in critical environments. To ensure a long-term deployment, battery-free and energy-autonomous wireless sensors are designed and can be powered by ambient energy harvesting or Wireless Power Transfer. Because of the criticality of the applications and the limited resources of the nodes, the security is generally relegated to the background, which leads to vulnerabilities in the entire system. In this paper, a security analysis based on an example: the implementation of a communicating reinforced concrete using a network of battery-free nodes; is presented. First, the employed wireless communication protocols are presented in regard of their native security features, main vulnerabilities, and most usual attacks. Then, the security analysis is carried out for the targeted implementation, especially by defining the main hypothesis of the attack and its consequences. Finally, solutions to secure the data and the network are compared. From a global point-of-view, this security analysis must be initiated from the project definition and must be continued throughout the deployment to allow the use of adapted, updatable and upgradable solutions.

Keywords: Wireless Sensor Network (WSN); Cyber-Physical System (CPS); cyber-security; Internet of Things (IoT); Structural Health Monitoring (SHM); data integrity; data confidentiality

check for updates

Citation: Loubet, G.; Alata, E.; Takacs, A.; Dragomirescu, D. A Survey on the Security Challenges of Low-Power Wireless Communication Protocols for Communicating Concrete in Civil Engineerings. *Sensors* **2023**, *23*, 1849. https://doi.org/10.3390/s23041849

Academic Editor: Amitabh Mishra

Received: 2 December 2022
Revised: 2 February 2023
Accepted: 3 February 2023
Published: 7 February 2023

1. Introduction

In the past years, climate change has led to a re-consideration of the fabrication and transportation processes, especially with the aims of minimizing carbon footprint and of using renewable energies. These global demands require the introduction of new paradigms, new materials, new energy sources, and new fabrication techniques. This is particularly true in the construction and civil engineering industries, where sustainability, maintainability, and reliability are required for structures and infrastructures [1]. To deal with these new demands, the use of Structural Health Monitoring (SHM) solutions is favored [2]. These consist of an autonomous and "permanent" inspection of the health of the structure to achieve intelligent data-driven diagnostics, and thus to prevent its irreversible failures, avoid its collapse, and allow preventive maintenance to be applied.

Cyber-Physical Systems (CPS), in the framework of the Internet of Things (IoT), are good candidates to implement the Structural Health Monitoring of civil engineering structures [3]. Indeed, these can monitor and/or control the physical world, as well as connect the physical and digital worlds (for instance by updating the digital/virtual models/twins/representations with the data collected by the nodes, but also by commanding the nodes based on the needs of the digital/virtual models/twins/representations). The physical part of the Cyber-Physical Systems can be based on the use of Wireless Sensor Networks (WSN) [4], which are able to wirelessly exchange (with the humans and/or machines) data commonly generated with Non-Destructive Testing (NDT) methods that do not alter the element under test [1,5,6]. With the digitalization and the miniaturization of electronics, this kind of embedded systems is always more effective and pervasive. Nevertheless, the long-term deployment of Wireless Sensor Networks is today mainly restricted by energy autonomy. To lengthen their limited lifespan, ambient energy harvesting and Wireless Power Transmission (WPT) solutions are investigated to power these [7,8]. By considering both Wireless Power Transmission and wireless communication, Wireless Sensor Networks can answer to the Simultaneous Wireless Information and Power Transfer (SWIPT) paradigm [9].

In addition, the cyber-security considerations (especially in terms of data integrity, availability, and confidentiality, but also of alteration or interruption of service) are usually not addressed during the design and implementation phases of the Cyber-Physical Systems and of its Wireless Sensor Network, but only *a posteriori,* or when necessary (e.g., after an attack, or an attempt of attack). However, the hardware and software solutions to protect a Cyber-Physical System have a significant cost, in terms of energy consumption and money, which must be considered at the earliest stages of a project [10].

In this paper, the low-level security analysis of a Wireless Sensor Network conducted during the McBIM project [11–14] will be presented. This project aims to propose an implementation of the concept of “communicating materials” [15] in the case of reinforced concrete, in part to ensure the Structural Health Monitoring of reinforced concrete structures thanks to Non-Destructive Testing methods based on the use of dedicated Wireless Sensor Networks.

Section 2 will address the designs of the proposed Cyber-Physical System, and of its Wireless Sensor Network based on Communicating Nodes (CN) and Sensing Nodes (SN). The Section 3 will deal with the presentation of the used wireless communication technologies namely LoRa/LoRaWAN and Bluetooth Low Energy (BLE), especially in regard of their native security features, their main vulnerabilities, and their common attacks. Section 4 will present the security analysis carried out during the McBIM project [11], by explicating the potential malicious objectives, the threat model, and the risks. Before concluding, Section 5 will propose the analysis of technical solutions used to prevent the attacks or limit their effects, and thus, to mitigate the risks.

2. Architecture of a Cyber-Physical System to Implement a Communicating Concrete

The proposed Cyber-Physical System, presented in Figure 1 and in detail in [11–14], is composed of a Wireless Sensors Network based on Communicating Nodes (CN) and Sensing Nodes (SN), organized in a two-levels network. Each element made of communicating concrete embeds at least one Communicating Node and several Sensing Nodes, this association forming a subnetwork. Their number is a function of the size of the element and the needs in terms of measurement (e.g., spatial accuracy, etc.).

The Communicating Nodes form an *ad-hoc* mesh network within a structure or a set of adjacent structures. These are intended to aggregate, and then process, store, and share the data transmitted by the Sensing Nodes. The data can be processed, stored, and shared locally in one or more Communicating Nodes of the network, and/or remotely in one or more other networks or even in the digital world (and especially in digital/virtual models/twins/representations), thanks to access to the Internet. Thus, bi-directional medium to long-range wireless communication technologies are required for the communications between the Communicating Nodes. Moreover, at least one Communicating Node per mesh network must be a reliable access point (or a gateway) to the digital world by providing a bi-directional connection to the Internet. Other bi-directional wireless communications technologies can be implemented to interface with other local Wireless Sensor Networks and/or devices. Because these have sufficient energy and processing resources, the Communicating Nodes can employ the usual solutions (e.g., cryptography, etc.) to protect the bidirectional wireless communications, but also the stored data. Thus, the safety aspects concerning the data storage by the Communicating Nodes, but also the wireless communications between the Communicating Nodes and from the Communicating Nodes to the Internet or to extern devices, are not discussed here in order to focus on the wireless communications between the Sensing Nodes (whose the hardware and software architectures are fixed) and the Communicating Nodes.

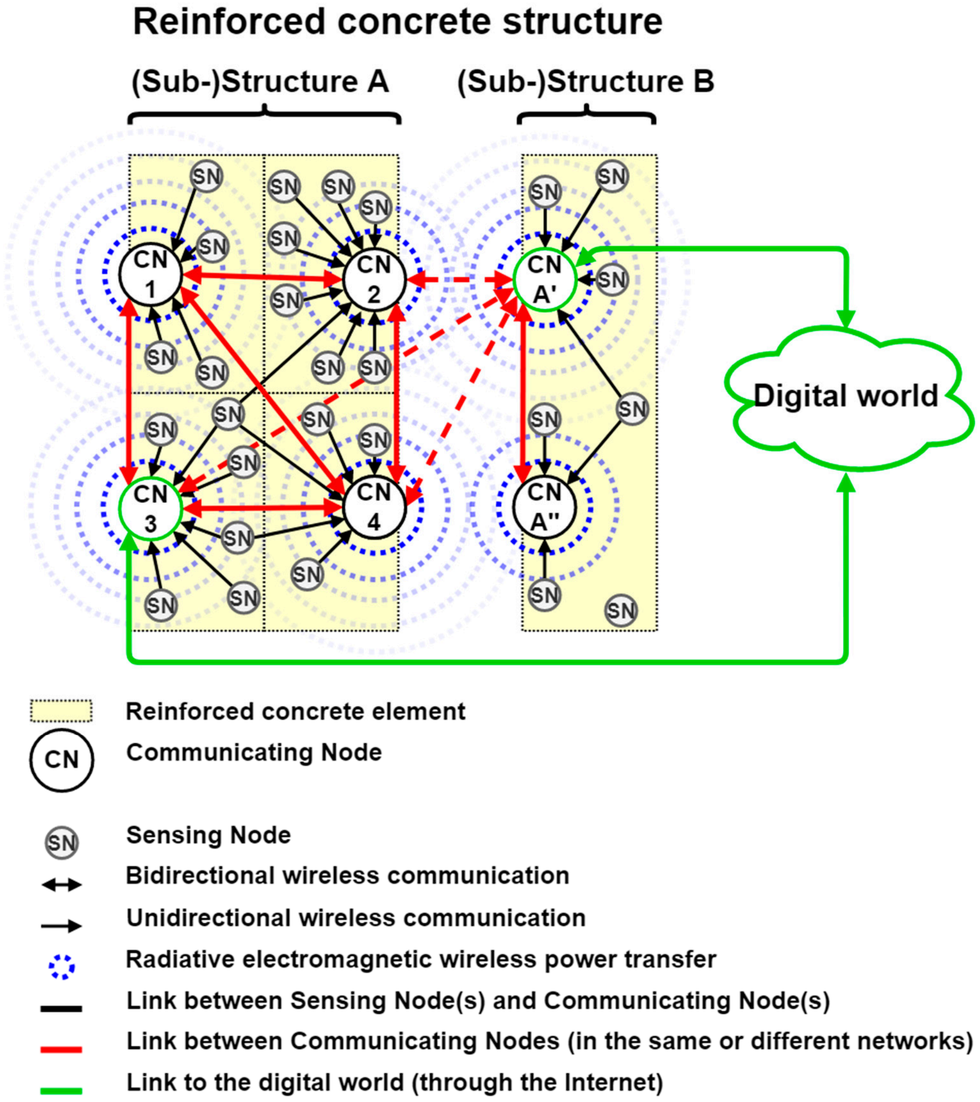
Reinforced concrete structure
(Sub-)Structure A
(Sub-)Structure B
CN 1
CN 2
CN 3
CN 4
CN A'
CN A''
SN
Digital world
Reinforced concrete element
CN
Communicating Node
SN
Sensing Node
Bidirectional wireless communication
Unidirectional wireless communication
Radiative electromagnetic wireless power transfer
Link between Sensing Node(s) and Communicating Node(s)
Link between Communicating Nodes (in the same or different networks)
Link to the digital world (through the Internet)

Figure 1. Block diagram of the architecture of the Cyber-Physical System dedicated to the implementation of communicating concrete.

A star network of Sensing Nodes is available around each Communicating Node, which, thus, becomes a central hub in a subnetwork. The Sensing Nodes are intended to measure relevant parameters of the monitored element and/or its environment (e.g., temperature, relative humidity, mechanical deformation, etc.). The collected and pre-processed data must then be transmitted to the associated Communicating Node(s) with directional medium-range wireless communication technologies (e.g., LoRaWAN or Bluetooth Low Energy) reliable even through the reinforced concretes. In addition to the recovery of the data sent by the Sensing Nodes, the Communicating Nodes have to wirelessly power the Sensing Nodes located in their neighborhood. By tuning their wireless power source (in terms of the waveform, output power, and/or periodicity of activation), the Communicating Nodes can set up the periodicity of functioning of the Sensing Nodes. A radiative electromagnetic Wireless Power Transfer system is used to achieve this Wireless Power Transfer.

The Sensing Nodes are the core elements of this Cyber-Physical System, because gathering the main constraints: inaccessible, energy-autonomous, fully wireless, and long-term usable, resilient, and reliable, during their entire lifetime expressed in decades. Thus, these are designed as simply as possible in order to minimize the risk of failure, and are also battery-free and able to cold-start. In their current implementation, which is fully presented in [12–14], the Sensing Node is completely inaccessible and cannot be changed, repaired, or updated. Indeed, there is no physical access (these are encapsulated in the core of the reinforced concrete), nor wireless access (no data downlink is implemented), with an exception for the Wireless Power Transfer that can control the periodicity of activation. It could be noted that in the implementation based on the LoRa technology, a unique antenna is used both for harvesting the electromagnetic power transmitted by the Communicating Node(s) and for sending the collected data to the Communicating Node(s). Due to their limited resources (in terms of processing and energy), their inaccessibility, and their targeted lifespan, the Sensing Nodes are the focus of this low-level security analysis, and in particular their wireless communications with the Communicating Node(s).

Because of the specific implementation and design constraints, this case study of communicating concrete differs from more usual deployments of Wireless Sensors Network, especially because the Sensing Nodes have a very limited (physical and/or wirelessly) and resources (mainly in terms of available energy but also in terms of processing and data storage resources).

Firstly, as there is no physical access to the Sensing Nodes once deployed (as these are encapsulated in reinforced concrete), it is assumed that the attacker cannot physically access it either. Thus, it seems useless to consider the physical attacks for this case study. Nevertheless, this makes impossible to change, repair, update, or upgrade the hardware part of the Sensing Nodes, once deployed and/or after an attack or a compromise.

Then, because of the specific design of the Sensing Nodes: with limited energy resources, limited processing resources, and limited data storage resources, but also without a data downlink; it is assumed that the attacker cannot wirelessly access it to reconfigure or compromise its firmware or exploit its processing resources (e.g., hijacking the network for others activities). Nevertheless, this makes it impossible to employ classic cryptographic solutions (because of the lack of energy and processing resources) but also to update or upgrade the software part of the Sensing Nodes, whose version of the communication protocol or the security algorithms. Thus, the main challenge lies in ensuring the authentication of legitimate frames received by the Communicating Node(s).

Also, as a single and standardized wireless communication protocol is employed, both the attacker and the designer are aware of the attacks detailed in the scientific literature, and the designer must use this knowledge to deploy specific and tailored countermeasures to protect the Sensing Nodes and/or to mitigate the risks.

As the propagation medium of the electromagnetic waves between the Sensing Nodes and the Communicating Nodes (namely the reinforced concrete) is very harsh and greatly attenuates the radiofrequency signals, the attacker can easily overwrite the legitimate wireless communications to craft malicious messages. Nevertheless, the Communicating Nodes can be allowed to use this knowledge to identify malicious frames based on signals with abnormally high-power levels.

Finally, as the Sensing Nodes are remotely and wireless powered by a radiative electromagnetic Wireless Power Transfer solution, a frame reception must be preceded by a power transfer managed by the meshed network of Communicating Nodes. Thus, any frame reception that does not complain about this behavior can be considered suspicious by the Communicating Node(s).

3. Low-Level Security Aspects of the LoRaWAN and Bluetooth Low Energy Wireless Communications Protocols

For the next, and because already implemented in the proposed solutions [12–14], both the LoRaWAN [16,17] and Bluetooth Low Energy [18,19] wireless communication protocols will be analyzed regarding their low-level security aspects. The implemented security features, their most usual vulnerabilities, and their common attacks will be introduced for each one, even if these are not applicable to the current implementations. Whatever the targeted application and the environment of deployment, all these elements concerning the studied wireless communication protocols must be known and considered. Given the use of standard protocols, it is necessary to continuously conduct the monitoring of technological development on the security aspects of the employed protocols, as these directly impact the object and its use. This is the case here, where all these aspects concerning the LoRaWAN and Bluetooth Low Energy technologies must be considered for Sensing Nodes (whose hardware and software architectures are fixed) communicating from the core of reinforced concretes.

3.1. LoRaWAN

Regarding the LoRaWAN wireless communication protocol, the 1.0.3 version of the specification, the use of Class A devices, and the absence of acknowledgment (and more generally of data downlink) will be considered, as currently implemented in the Sensing Nodes [16,17]. Its low-level security aspects are recent research topics [16,17,20–26].

3.1.1. Native Security Features

A LoRaWAN device has a unique 64 bits identifier (*DevEUI*) and a unique 32 bits address (*DevAddr*), and must be authenticated in order to transmit data to a network. This authentication can be achieved by over-the-air activation (OTAA) (not implemented in the McBIM project) or by activation by personalization (ABP) (implemented in the McBIM project). In both cases, the device obtains two unique AES-128 symmetric session keys named *AppSKey* and *NwkSKey* assigned before data communication for a unique communication session. *NwkSKey* is shared with the network server and is used to calculate and verify the MIC (Message Integrity Code) of all data frames to ensure data integrity; and to encrypt and decrypt the payload field of a MAC (Medium Access Control) data frames. Whilst, *AppSKey* is shared with the application server and is used to encrypt, by an XOR operation, and decrypt the payload field of application-specific data frames. The over-the-air activation procedure ensures unicity for keys by generating these from a unique key named *AppKey*, this at each reset or re-join request; whilst this is the responsibility of the developer in the activation by personalization procedure to ensure the unicity for the static keys assigned and stored directly in the device. This unicity allows to reduce the probability of compromising the whole network while a node is compromising. In order to prevent replay attacks and packet losses, two frame counters can be used to keep uplink and downlink messages synchronized. If the difference between these is greater than a limitation value, the frames are dropped. In the current implementation, the frame counter is disabled for development purposes, because the application deployed on the application server must be updated each time a Sensing Node is programmed with a new firmware. An acknowledgement frame can be sent in response to an accepted uplink frame. If not received, the uplink frame can be retransmitted. After several attempts, the frame can be considered lost or rejected. In the proposed implementation, the acknowledgement is disabled in order to limit energy consumption by not considering the data downlink, whatever its form. Thus, the LoRaWAN specification provides an authentication procedure to join a network; the encryption of the payload based on an Advanced Encryption Standard (AES) algorithm and the use of keys: the *NwkSKey* or the *AppSKey*; and an integrity check of each data frame sent. More, some additional procedures are available to ensure some security functions.

3.1.2. Usual Vulnerabilities

1. Physical access to devices

By having physical access to devices, it becomes possible to extract the device and network security keys (e.g., through reverse engineering by deriving the key from public information, etc.), especially *AppSKey* and *NwkSKey* which are necessary to decrypt the communications; and thus, to compromise both the device and the network. The consequences are that: the communications could be decrypted; an attacker could create a mock device with the same credentials to impersonate a legitimate device; the data payload can be manipulated; etc. It is also possible to use hardware, especially a radio module, near the targeted device to intercept its communications. To prevent compromises, the critical data should not be shared.

2. Lack of association between frames

One of the most important vulnerability is the lack of association between data frames and their acknowledgements, especially during the over-the-air activation procedure, which promotes replay attacks and acknowledgement spoofing. Two solutions have been implemented: the frame counter is included in the calculation of the message integrity code; and an acknowledgement flag is added.

3. Re-use of nonce values

Nonce values are values pseudo-randomly generated and used only once to derive the security keys during the over-the-air activation procedure. Because not tracked in some versions, there is a risk of generating a value already used, making the network vulnerable to replay attack or eavesdropping. A solution has been implemented: the nonce values are turned into counters; and the last used values are stored and tracked.

4. Frame counter management

When a device is rebooted or when its frame counters overflow, these latter are set to 0. By being able to reset a device, the frames obtained before by sniffing the communications could be replayed back during a replay attack. For the activation by personalization procedure, a solution could be to store the counter values in the server during the reboot of a device, and rejecting all the messages while the new counter does not reach the stored value. This would decrease the availability of the device. For the over-the-air activation procedure, a solution has been implemented: new security keys are generated at each reconnection.

5. Lack of end-to-end integrity protection

The integrity of the application data is not protected during its transmission between the network and application servers. The specifications acknowledge this vulnerability but are left to the developer of the application to implement its own security features.

6. Packet and payload vulnerabilities

The frames are not time-stamped to validate the time of the transmission, which makes it vulnerable to replay attacks. More, its payload length is the same before and after the encryption. Therefore, an attacker could overflow counters to restore the key stream from the encrypted messages.

7. Credentials Misconfiguration

Security of exchanges relies on cryptographic keys embedded in the devices. These cryptographic keys are used to provide authentication of the device and confidentiality of exchanged data. On the other hand, some devices need bi-directional communications which imply the possibility for a remote system to connect to the device using a password. A common mistake, during the deployment of devices, is to reuse the same keys and passwords for all devices. As well, we can consider that these default values are well known to the intruder. For instance, this weakness leads to the mirai worm [27].

3.1.3. Common Attacks

1. Radio jamming

The radio jamming consists of a malicious entity in transmitting a powerful radio signal near devices and/or gateways, to disrupt the radio transmissions. Because of Chirp

Spread Spectrum (CSS) modulation coexistence issues, malicious LoRa transmissions on the same frequency and with the same spreading factor used by the legal LoRa transmissions are sufficient to interfere with these. Almost all the transmissions can be affected and wiped out at the frequency used. This attack can be detected by observing a sudden drop out from the network. Once detected, it is recommended to change the frequency band.

2. Replay attack

During a replay attack, the attacker captures a valid data transmission to repeat or delay it to fool the network (both device and gateway can be targeted). The attack requires knowledge of the frequencies and channels used during the communications. These can be prevented with the use of the tracking frame counters, join procedure via over-the-air activation, or physical protection; and could lead to Denial of Service (DoS) which intends to disrupt services.

3. Acknowledgement spoofing

This attack results from the lack of association between a frame and its acknowledgment. The attacker prevents the reception (e.g., via jamming) and captures the downlink acknowledgement in order to acknowledge another uplink frame from the same device. The purpose of this attack is mainly: to take control of the gateways; to damage the network; or to provoke Denial of Service. This is also possible on uplink frames if the attacker can prevent their reception by gateways.

4. Bit flipping

The lack of end-to-end integrity protection of application data enables bit flipping. If the transport layer security between the network and application servers does not exist or is compromised, and if the attacker is able to act on this channel, then the application data can be altered and the confidentiality of the application compromised.

5. Eavesdropping

Eavesdropping can be passive (e.g., sniffing) or active (e.g., relay attack, man-in-the middle). During the sniffing attack, the most common passive eavesdropping method, the attacker captures the frames transmitted over a network between the devices and the gateways. From the gathered information, the attacker can launch further to compromise the operation of the network at several levels.

6. Relay attack

Relay attack occurs when a malicious entity creates a relay between the devices and the network server, and initiates a communication to relay the frames to another malicious entity.

3.2. Bluetooth Low Energy

Regarding the Bluetooth Low Energy wireless communication protocol, the 5th version of the specification and the use of the topology based on broadcasters and observers will be considered, as currently implemented in the Sensing Nodes [18,19]. Its low-level security aspects are recent research topics [18,28–38].

3.2.1. Native Security Features

Several security mechanisms are already implemented by default in Bluetooth Low Energy technology, such as the frequency hopping which avoids interferences with other devices using the same frequency band. More, the implementation of some security processes is recommended in [18,28]. First, two security modes with several levels of security are defined to encrypt and sign data. The mode 1 is dedicated to data encryption. Its level 1 provides no security; its level 2 the unauthenticated pairing with encryption; its level 3 the authenticated pairing with encryption; and its level 4 the authenticated secure connection pairing with encryption. Mode 2 is dedicated to connection-based data signing. Its level 1 and level 2 provide, respectively, the unauthenticated and the authenticated pairing with data signing. Second, a security manager is used for the pairing process during which devices exchange information to establish secure connection (Mode 1, level 4) which avoids temporary key brute-force attacks. The pairing process has three main phases: the exchange (with no encryption) of pairing features (based on the abilities) between the devices in order to select the most suitable method to generate short-term (or temporary) key (four methods are available, namely "just works", "passkey", "out-of-bands" and "numeric comparison"); the generation and the exchange of the short-term key used to encrypt the frames dedicated to the pairing and the authentication, and which protect against man-in-the-middle attacks; finally, the generation and the exchange of the long term key used to encrypt all the next communications. An optional phase consists of the exchange of transport key parameters which can be used to store the security keys and the information exchanged during the pairing process, which will allow later re-connections without needing to repeat the entire process. Then, the Bluetooth Low Energy communications are encrypted using an AES-128 cipher block chaining-message authentication code algorithm based on 128 bits key length generated with the elliptic curve Diffie-Hellman method. The communications using encryption and authentication use a Message Integrity Code appended to the payload, and a Cyclic Redundancy Check (CRC) mechanism to protect it all. The communications using authentication but not encryption use a 12-byte signature computed with a 128-bit AES algorithm placed after the data payload, as well as an input counter to prevent replay attacks. Moreover, a privacy feature is provided to limit the tracking of the identity of a device: its address is private and changes frequently, via the encryption of its public address. Finally, trust modes are defined to characterize the communications. Communication with a device "trusted" allows a fixed connection and unrestricted access to all its services, while communication with an "untrusted" device restricts its access to a set of services.

3.2.2. Usual Vulnerabilities

1. Pairing process

Although the short-term key is not transmitted through the packet, its 16 bytes input value is predictable. For the "just works" method, its value is predefined to '0 × 00' and this method is vulnerable to man-in-the-middle attacks because the authenticity of the connection cannot be verified. For the "passkey" method the generation parameters are transmitted through packets. Thus, an attacker could calculate its value and decrypt data.

2. Discoverability

Bluetooth Low Energy has a discoverability mode used before the pairing process. A discoverable device is vulnerable because it allows all the devices located in its neighborhood to access information, such as its name, its class, and its services. Turning off the discoverability mode prevents devices from scanning attacks.

3.2.3. Common Attacks

Bluetooth Low Energy technology, and more generally Bluetooth technology, is vulnerable to many attacks, whose: the PIN (Personal Identification Number) theft (by cracking or off-line recovery, etc.); eavesdropping (sniffing, man-in-the-middle, relay, etc.); cloning (Medium Access Control address spoofing, forced re-pairing, brute-force, chopping, etc.); the treacherous (backdoor, bumping, etc.); the Denial of Service (radio jamming, Medium Access Control address duplication, synchronous connection-oriented, enhanced synchronous connection-oriented, battery exhaustion, big negative-acknowledgement, guaranteed service, smacking, etc.); the surveillance (printing, stumbling, tracking, etc.); and the miscellaneous others (snarfing, bugging, jacking, free calling, whisperer, etc.); etc. Nevertheless, eavesdropping and Denial of Service attacks are more usual.

1. Eavesdropping: sniffing

Sniffing is the most common passive approach for eavesdropping. This attack can take place during different stages of Bluetooth Low Energy communication, such as a new connection, an active connection, or a negotiation phase. However, in the case of Bluetooth Low Energy, sniffing is complex and expensive as 40 channels are used with a fast Frequency Hopping Spread Spectrum (FHSS) technique. During the establishment of a new connection, the connection request packet can be captured. This one contains several parameters to set the frequency hopping algorithm and the Cyclic Redundancy Check calculation. Knowing these parameters, the attacker can use these to set up its algorithm to listen from at least one of the three advertising channels, if it is too expensive to sniff all of these at once. During an active connection, the attacker can deduce the connection parameters through an exhaustive approach that assumes that all channels are systematically used, and which is not effective on short communications because a lot of time is required. During the negotiation phase, the attacker can obtain the encryption keys to decrypt the next communications.

2. Eavesdropping: man-in-the-middle

Man-in-the-middle attacks occur when an attacker intercepts the communications between two devices and modifies them. Some attacks consist in cloning the GATT (Generic ATTribute) server to simulate an identical device to which the master device will be connected. It allows the fake device to connect to the legitimate device to capture the traffic, impersonate a device, inject data, modify or redirect packets, provoke Denial of Service, etc. These attacks are easy to implement as only requiring a communication between two devices and as the attacker can negotiate the encryption parameters.

3. Radio jamming

Using a strong radio signal near a Bluetooth Low Energy device can cause interferences and jam communications. The attacker can jam the connected communications and the advertising transmissions by saturating the radio spectrum, until interrupting connected communications or hijacking connected communications by forcing the master to disconnect. Preventing radio jamming is difficult as it requires physical protection from interference.

4. Other attacks

Bluetooth Low Energy is also vulnerable to replay attacks, relay attacks, and spoofing attacks.

5. Audit tools

Several audit tools, such as [39], exist to test the resistance to attacks of the devices under test.

4. Security Analysis and Threat Models for Reinforced Concrete Structural Health Monitoring Applications

Both the LoRaWAN and Bluetooth Low Energy wireless communication protocols will be studied regarding their current implementation in the framework of the McBIM project [12–14]. The wireless communications between inaccessible Sensing Nodes encapsulated in the reinforced concrete and accessible Communicating Nodes located on the surface of the reinforced concrete will be mainly considered. These are currently only unidirectional from the Sensing Nodes to the Communicating Nodes and carry non-critical measurement data. More, the Sensing Nodes are not able to receive downlink frames but can be controlled by the Communicating Nodes through the Wireless Power Transfer system. Then, the bidirectional communications within the mesh network of Communicating Nodes and with the Internet will be only skimmed through. In any case, all wireless communications: from the Sensing Nodes to the Communicating Nodes; between the Communicating Nodes; and between a Communicating Node and the Internet; raise low-level security issues, whose importance depends on the data transmitted: their type, their criticality, their reliability, etc. Thus, a security analysis could be achieved for each of these wireless interfaces, but also on the hardware side of the Sensing Nodes and the Communicating Nodes, for instance by applying a Failure Mode, Effects, and Criticality Analysis (FMECA) [40].

4.1. Malicious Objectives

Three main types of malicious objectives have been identified for the targeted application: the invasion of privacy; the alteration of service; and the interruption of service. Because of low computing resources, the hijacking of the network for others activities (e.g., mining cryptocurrencies, launching a Denial of Service (DoS) attack, etc.) seems improbable.

4.1.1. Invasion of Privacy

Invasion of privacy consists in gathering information on the activities in the instrumented infrastructure, for instance through sniffing or other eavesdropping techniques. This could be realized by the infrastructure owner to acknowledge, for instance, the movements or activities of the users (such as employees, etc.) in the infrastructure. An outsider of the structure could also gather information on activities in order to identify the best moment to trespass in the infrastructure (such as for robbing or degrading, etc.) or to collect classified information (such as the use of the infrastructure, the available equipment, etc.).

4.1.2. Alteration of Service

The services delivered by the communicating reinforced concrete can be altered by the falsification of the measurement, for instance through man-in-the-middle attacks, relay attacks, or replay attacks; or by modifying the transmitted frames. As an example, an attacker could emulate a failure (such as a significant crack, a fire, etc.) to make people believe in the possible collapse of the infrastructure or at least its unsafety.

4.1.3. Interruption of Service

The services delivered by the communicating reinforced concrete can be interrupted by stopping the communications, for instance through Denial of Service attacks, radio jamming attacks, or battery exhaustion attacks (such as by avoiding the Wireless Power Transfer from the Communicating Nodes to the Sensing Nodes, etc.).

4.2. Threat Models

The proposed threat model is based on two-range attacks: the short-range and the long-range.

4.2.1. Short-Range Attack

The short-range attacks provide physical access to the attacker which can be either inside the infrastructure or outside it but near enough to place malicious objects (such as malicious Sensing Nodes, malicious Communicating Nodes, etc.). Nevertheless, the Sensing Nodes are considered physically and wirelessly inaccessible.

4.2.2. Long-Range Attack

The maximum range of the attacks depends on the wireless communication technology, the transmission power, and the type of communication. In this case, the attacker is able to communicate with legitimate nodes or to emit an enough powerful radio signal to jam the wireless communications, but also to control the periodicity of activation of the Sensing Nodes by employing its own radiative electromagnetic power source(s).

4.3. Risks

The risk scales, both for the probability and the impact of an attack, are based on personal estimations related to the state of the art available in the scientific literature and have been the subject of a consensus among a dozen of experts from the security and different technical fields, working on the McBIM project. The impact of an attack depends on the potential harm this can inflict both to the material and the humans, due to the failure of its detection.

4.3.1. Invasion of Privacy

The invasion of privacy implies several risks such as surveillance, the insertion of a malicious node into the network, the insertion of fake data, and the compromise of node(s). Their analysis is proposed in Table 1.

Table 1. Analysis of the risks implied by an invasion of privacy.

Risk	Probability	Impact
Surveillance	**Likely**	**Insignificant to critical,** depends on the activities
Insertion of a malicious node into the network	Sensing Node embedded in the reinforced concrete: **Unlikely**	Sensing Node embedded in the reinforced concrete: **Minor**
	Sensing Node non-embedded in the reinforced concrete: **Likely**	Sensing Node non-embedded in the reinforced concrete: **Minor**
	Communicating Node: **Even**	Communicating Node: **Major to critical** (especially if a gateway to the Internet is targeted)
Insertion of fake data	**Likely**	**Moderate to critical**
Compromise of node(s)	Sensing Node: **Unlikely**	Sensing Node: **Minor**
	Communicating Node: **Likely**	Communicating Node: **Major to critical** (especially if a gateway to the Internet is targeted)

4.3.2. Alteration of Service

The alteration of service implies several risks such as the deduction of the infrastructure activities or the alteration of data; and is time-consuming and expensive to detect and correct. Their analysis is proposed in Table 2.

Table 2. Analysis of the risks implied by an alteration of service.

Risk	Probability	Impact
Deduction of the infrastructure activities	**Likely** depends on the implemented security mechanisms	**Minor to critical** depends on the activities (e.g., critical in a nuclear plant, etc.)
	Even depends on the implemented security mechanisms	**Moderate to critical** (e.g., emulation of a failure, a collapse, a fire, etc.)

4.3.3. Interruption of Service

The interruption of service implies several risks such as radio jamming, the battery exhaustion, the creation of relays, the creation of cycles, the damage of the rectenna, data recovery from nodes, and the alteration of the full infrastructure; and is time-consuming and expensive during the time of unavailability. Their analysis is proposed in Table 3.

Table 3. Analysis of the risks implied by an interruption of service.

Risk	Probability	Impact
Radio jamming	Between the Sensing Nodes and the Communicating Nodes: **Likely**	Between the Sensing Nodes and the Communicating Nodes: **Insignificant to critical** depends on the number of affected nodes
	Between the Communicating Nodes: **Likely**	Between the Communicating Nodes: **Moderate to major**
	Between a Communicating Node and the Internet: **Likely**	Between a Communicating Node and the Internet: **Critical**
Battery exhaustion	Alteration of the Wireless Power Transfer: **Improbable**	Wireless Power Transfer: **Critical**
	Destruction of the Sensing Nodes components: **Unlikely** (e.g., mechanical break, etc.)	Sensing Nodes: **Insignificant to critical** depends on the number of affected nodes
	Destruction of the Communicating Nodes: **Even**	Communicating Nodes: **Major to critical** depends on the number of affected nodes
Creation of relays	Sensing Node embedded in the reinforced concrete: **Unlikely**	Sensing Node embedded in the reinforced concrete: **Minor**
	Sensing Node non-embedded in the reinforced concrete: **Likely**	Sensing Node non-embedded in the reinforced concrete: **Major**
	Communicating Node: **Likely**	Communicating Node: **Major to critical** (e.g., a malicious device takes the place of a failed node)
Creations of cycles	**Likely**	**Minor to critical** depends on the type of activities and of data
Damage to the rectenna	**Unlikely** (e.g., very energetic electromagnetic wave, etc.)	**Critical**
Data recovery from nodes	**Even**	**Minor to critical** depends on the type of data
Alteration of the full infrastructure	**Unlikely**	**Critical**

5. Additional Technical Solutions

In addition to native security features, four main technical solutions can be employed separately or conjointly to prevent the attacks: cryptography [41,42]; Secure Element (SE) [43]; Intrusion Detection System (IDS) [44,45]; and multilayer signature [46].

5.1. Cryptography

The wireless communications can be secured by employing the cryptography features offered both by the LoRaWAN and the Bluetooth Low Energy protocols, especially through the encryption of the data, respectively thanks to an AES-128 counter algorithm and an AES-128 cipher block chaining-message authentication code algorithm. Nevertheless, additional levels (s) of cryptography can be employed. The use of cryptography is a flexible solution easy to implement, but it is computationally expensive and which requires secrets to be stored in a safe and non-volatile manner. Moreover, it is power-consuming and generating of latency, thus poorly suited to battery-free low-energy devices.

For instance, and from preliminary experimentations, the power consumption of an NXP QN9080 all-in-one module (MicroController Unit (MCU) and Bluetooth Low Energy transceiver) [47] powered at 1.8 V and designed to achieve (in a suboptimal broadcaster configuration: a start-up, a temperature measurement with the internal sensor, and the transmission of three 21-bytes long advertising frames in 3 different channels (36, 37 and 38) at +0 dBm), can be drawn by almost 90% only by disabling the Security Libraries (SecLib) and mainly the Random Number Generation (RNG) module, even if these are only initialized and never used. Thus, the duration of the process can be reduced from 2.7 s to 355 ms, and the energy needed from 7.9 mJ to 731 µJ.

5.2. Secure Elements

The use of Secure Elements can be an alternative way to secure the Wireless Sensor Network [39]. This one is tamper-resistant hardware embedded chip used to secure the storage of confidential and cryptographic data, to host securely applications, and to implement end-to-end security. Resistive Random-Access Memory (RAM) Physical Unclonable Functions (PUF) can be implemented to manage the authentication, the key generation and the storage. The Secure Elements are relatively cheap and consume less energy than using software cryptography. However, its driver (used to manage the communication between the micro-controller unit and the secure element) must be deployed within the microcontroller. Finally, the wire connection to the microcontroller unit must be protected.

5.3. Intrusion Detection System

An Intrusion Detection System can be another alternative way to secure the Wireless Sensor Network. This one is based on two detection methods: the signature-based and the anomaly-based methods. The first is not yet adapted for the low-power Wireless Sensor Networks, as we do not yet have enough knowledge of malicious behavior to propose a database of signatures of malicious activities. The second method uses learning systems to model the legitimate behaviors and detect the suspicious behaviors, by comparing observation with the reference model. In the McBIM project, two learning phases can be imagined: one during the manufacture of an element made of communicating reinforced concrete, during which the Communicating Node(s) detect the legitimate Sensing Nodes in its neighborhood; and the other during the construction of a complete structure made of several elements, during which each Communicating Node detects the legitimate Communicating Nodes in its neighborhood. The intrusion detection systems provide visibility on the network and add a layer of defense, but require maintenance and can be sensitive to false positives and negatives.

5.4. Multilayer Signature

The multilayer signature (sometimes called *footprint* or *fingerprint*) tends to use a singularity of each communicating object to characterize it and certify the authenticity of its communications in the framework of an Attack Detection System (ADS). This signature can be defined from the hardware (e.g., by the use of a metasurfaces antenna [48]) or the embedded software.

5.5. Implementable Features

Tables 4 and 5 gather some optional security features respectively provided by the LoRaWAN and the Bluetooth Low Energy protocols, with the attacks this prevents and its drawbacks. Just because some attacks are avoided does not mean that there are no more risks.

Table 4. LoRaWAN security issues and protection mechanisms.

Security Mechanisms	Attacks Prevented	Consequences of a Successful Attack	Drawbacks
Over-the-air activation procedure	• Replay attack	• Connection of a malicious device to the network server • Injection of (fake) data • Etc.	• Risk of replay attacks reduced but still possible if the reset and overflow of the frame counter are not well considered • Increases latency • Increases power consumption • Requires data downlink
Frame counter	• Replay attack	• (Re)Use of a valid message to connect a malicious device to the network server • (Re)Injection of (fake) data • Etc.	• Could decrease the availability of a device • Reset and overflow must be well considered
Message acknowledgement	• Replay attack • Acknowledgement spoofing	• (Re)Use of a valid message to connect a malicious device to the network server • (Re)Injection of (fake) data • Etc.	• Increases latency • Increases power consumption • Requires data downlink

5.6. Security Recommendations and Perspectives in the Case of Communicating Concrete

As a result of the security analysis, it appears that the Sensing Nodes can be considered as always intact over time (unalterable because both their hardware and software are inaccessible and fixed). However, an attacker could still be able to disrupt wireless communications despite the implementations of all the countermeasures presented in this section. Nevertheless, it is possible to mitigate the risks and their consequences. Indeed, the Communicating Nodes have knowledge about the network topology, the context of deployment, the targeted application, but also the behaviors of each Sensing Node. These can also be enriched with a behavioral Intrusion Detection System allowing the detection and identify attacks. Thus, the implementation of a least a behavioral Intrusion Detection System seems essential and this solution can be easily updated and does not impact the architecture and implementation of the Sensing Nodes, but also the architecture and hardware implementation of the Wireless Sensor Network. Moreover, this behavioral Intrusion Detection System can also be deployed in the digital world (and in the digital/virtual models/twins/representations).

Table 5. Bluetooth Low Energy security issues and protection mechanisms.

Security Mechanisms		**Attacks Prevented**	**Consequences of a Successful Attack**	**Drawbacks**
Security Mode 1: Encryption	Level 1	• None	• Decryption of data • Traffic observation • Traffic injection • Denial of service	• N/A
	Level 2	• Limited eaves-dropping protection		• Requires encrypted link • Requires data downlink
	Level 3	• Eavesdropping • Replay attack		• Requires encrypted link • Requires data downlink
	Level 4	• Eavesdropping • Replay attack • Man-in-the-middle		• Requires encrypted link • Requires secure communication • Requires data downlink
Security Mode 2: Data signing	Level 1	• None	• Traffic observation • Traffic injection	• Cannot be combined with security Mode 1 • Connection-based data signing • Requires signing • Requires data downlink
	Level 2	• Eavesdropping • Replay attack		• Cannot be combined with security Mode 1 • Connection-based data signing • Requires signing • Requires data downlink
Pairing process: Temporary key generation	*Just work*	• Passive attacks	• Impersonate devices • Decryption of data • Traffic observation • Traffic injection • Denial of services	• Requires data downlink
	Passkey	• Passive attacks • Man-in-the-middle		• Input or output ability • Requires data downlink
	Out-of-band	• Passive attacks • Man-in-the-middle		• Requires another interface • Requires data downlink
	Numeric comparison	• Passive attacks • Man-in-the-middle		• Requires binary input • Requires data downlink

Table 5. *Cont.*

Security Mechanisms	Attacks Prevented	Consequences of a Successful Attack	Drawbacks
Discoverable mode disabled	• Prevents from accessing information such as names, class, services, etc.	• Theft of sensitive data	• No data transmission allowed
Trust mode	• Limits automatic access to all services	• Only a trusted device just compromised enables access to all the services of an attacker	• Removes pairing information
Privacy feature	• Identity tracking	• Theft of sensitive data	• Available only with connected mode • Only a trusted device can be connected

6. Conclusions

This paper presents the security analysis carried out in the framework of the McBIM project which aims at implementing a communicating reinforced concrete based on a Wireless Sensor Network using wirelessly powered battery-free nodes with low resources (energy, processing, storage). Firstly, the implemented Cyber-Physical System is presented, as well as the employed wireless communication protocols, namely LoRaWAN and Bluetooth Low Energy, in regards to their native security features, their main vulnerabilities, and their most usual attacks. Then, a focus on the issues specific to the proposed implementation is achieved, especially by defining the current implementation, the main hypothesis of attack, and their consequences (from the invasion of privacy to alteration or even interruption of service). The unidirectional wireless communications from the Sensing Nodes (wirelessly powered, battery-free, and low resources) to the Communicating Node(s) are mainly considered, even if other wireless communications are implemented in the proposed Cyber-Physical System (especially in a mesh network of Communicating Nodes, with the Internet, or with local wireless devices such as smartphones), and attacks based on direct access to the Sensing Nodes are not considered as these are assumed to be physically and wirelessly inaccessible (encapsulated in the reinforced concrete and without data downlink). The solutions to secure both the data and the network are studied, in particular, those provided by the considered standards but also those that are in the state-of-the-art, and considered in regards to the available resources (energy, processing, storage). Finally, even if several solutions are implementable *a posteriori*, these must be studied and used from the beginning of the implementation and thought with a global point-of-view. In the presented case study, the use of a behavioral Intrusion Detection System (deployed both in the Communicating Nodes and in the digital/virtual models/twins/representations) seems to be a relevant solution to mitigate the risks.

Author Contributions: Conceptualization, G.L., E.A., A.T. and D.D.; methodology, G.L. and E.A.; validation, G.L., E.A., A.T. and D.D.; investigation, G.L., E.A., A.T. and D.D.; writing—original draft preparation, G.L.; writing—review and editing, G.L., E.A., A.T. and D.D.; visualization, G.L.; supervision, E.A., A.T. and D.D.; project administration, D.D.; funding acquisition, A.T. and D.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the French National Research Agency (ANR) under the McBIM project (Communicating Material at the disposal of the Building Information Modeling), grant number ANR-17-CE10-0014.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank Clarisse ERPELDINGER for its valuable help during the security analysis and Philippe HERAIL for its power characterization of the Bluetooth Low Energy module, and also all their French partners in the McBIM project: CRAN (Nancy, France), LIB (Dijon, France), and FINAO SAS/360SmartConnect (Trans-en-Provence, France) for the relevant discussions about security, placed in the core of the project definition.

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

References

1. Bungey, J.H.; Millard, S.G.; Grantham, M.G. *Testing of Concrete in Structures*, 4th ed.; CRC Press: Boca Raton, FL, USA, 2006; p. 353.
2. Farrar, C.R.; Worden, K. An introduction to structural health monitoring. *Philos. Trans. R. Soc. A* **2007**, *365*, 303–315. [CrossRef] [PubMed]
3. Bhuiyan, M.Z.A.; Wu, J.; Wang, G.; Cao, J.; Jiang, W.; Atiquzzaman, M. Towards cyber-physical systems design for structural health monitoring: Hurdles and opportunities. *ACM Trans. Cyber-Phys. Syst.* **2017**, *1*, 1–26. [CrossRef]
4. Abdulkarem, M.; Samsudin, K.; Rokhani, F.Z.; Rasid, M.F.A. Wireless sensor network for structural health monitoring: A contemporary review of technologies, challenges, and future direction. *Struct. Health Monit.* **2020**, *19*, 693–735. [CrossRef]
5. Taheri, S. A review on five key sensors for monitoring of concrete structures. *Constr. Build. Mater.* **2019**, *204*, 492–509. [CrossRef]
6. Kot, P.; Muradov, M.; Gkantou, M.; Kamaris, G.S.; Hashim, K.; Yeboah, D. Recent advancements in non-destructive testing techniques for structural health monitoring. *Appl. Sci.* **2021**, *11*, 2750. [CrossRef]
7. Ma, D.; Lan, G.; Hassan, M.; Hu, W.; Das, S.K. Sensing, computing, and communications for energy harvesting iots: A survey. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 1222–1250. [CrossRef]
8. Peruzzi, G.; Pozzebon, A. A review of energy harvesting techniques for Low Power Wide Area Networks (LPWANs). *Energies* **2020**, *13*, 3433. [CrossRef]
9. Perera, T.D.P.; Jayakody, D.N.K.; Sharma, S.K.; Chatzinotas, S.; Li, J. Simultaneous wireless information and power transfer (SWIPT): Recent advances and future challenges. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 264–302. [CrossRef]
10. Ali, R.F.; Muneer, A.; Dominic, P.D.D.; Taib, S.M.; Ghaleb, E.A. Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review. In *Advances in Cyber Security*; Springer: Singapore, 2021.
11. McBIM. Available online: https://mcbim.cran.univ-lorraine.fr/ (accessed on 4 November 2022).
12. Loubet, G.; Takacs, A.; Gardner, E.; De Luca, A.; Udrea, F.; Dragomirescu, D. LoRaWAN battery-free wireless sensors network designed for structural health monitoring in the construction domain. *Sensors* **2019**, *19*, 1510. [CrossRef]
13. Loubet, G.; Takacs, A.; Dragomirescu, D. Implementation of a Wireless Sensor Network Designed to Be Embedded in Reinforced Concrete. In Proceedings of the IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society, Singapore, 18–21 October 2020.
14. Sidibe, A.; Loubet, G.; Takacs, A.; Dragomirescu, D. A Multifunctional Battery-Free Bluetooth Low Energy Wireless Sensor Node Remotely Powered by Electromagnetic Wireless Power Transfer in Far-Field. *Sensors* **2022**, *22*, 4054. [CrossRef]
15. Kubler, S.; Derigent, W.; Thomas, A.; Rondeau, E. Problem definition methodology for the "Communicating Material" paradigm. *IFAC Proc. Vol.* **2010**, *43*, 198–203. [CrossRef]
16. LoRa Alliance Technical Committee. LoRaWAN 1.0.3 Specification. 2018. Available online: https://lora-alliance.org/resource_hub/lorawan-specification-v1-0-3/ (accessed on 4 November 2022).
17. LoRa Alliance Technical Committee Regional Parameters Workgroup. RP2-1.0.3 LoRaWAN Regional Parameters. 2018. Available online: https://lora-alliance.org/resource_hub/rp2-1-0-3-lorawan-regional-parameters/ (accessed on 4 November 2022).
18. *IEEE 802.15.1-2005*; IEEE Standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.1: Wireless Medium Access Control (MAC) and Physical layer (PHY) specifications for Wireless Personal Area Networks (WPANs). IEEE Standards: Piscataway, NJ, USA, 2005.
19. 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]
20. Noura, H.; Hatoum, T.; Salman, O.; Yaacoub, J.P.; Chehab, A. LoRaWAN security survey: Issues, threats and possible mitigation techniques. *Internet Things* **2020**, *12*, 100303. [CrossRef]
21. Yang, X. LoRaWAN: Vulnerability Analysis and Practical Exploitation. Master's Thesis, Delft University of Technology, Delft, The Netherlands, 2017.
22. Aras, E.; Ramachandran, G.S.; Lawrence, P.; Hughes, D. Exploring the security vulnerabilities of LoRa. In Proceedings of the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, UK, 21–23 June 2017.

23. Dönmez, T.C.; Nigussie, E. Security of LoRaWAN v1. 1 in backward compatibility scenarios. *Procedia Comput. Sci.* **2018**, *134*, 51–58. [CrossRef]
24. Butun, I.; Pereira, N.; Gidlund, M. Analysis of LoRaWAN v1.1 security. In Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Object, Los Angeles, CA, USA, 25 June 2018.
25. Eldefrawy, M.; Butun, I.; Pereira, N.; Gidlund, M. Formal security analysis of LoRaWAN. *Comput. Netw.* **2019**, *148*, 328–339. [CrossRef]
26. Tsai, K.L.; Leu, F.Y.; Hung, L.L.; Ko, C.Y. Secure session key generation method for LoRaWAN servers. *IEEE Access* **2020**, *8*, 54631–54640. [CrossRef]
27. Griffioen, H.; Doerr, C. Examining mirai's battle over the internet of things. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual, 9–13 November 2020.
28. National Institute of Standards and Technology. NIST Special Publication 800-121—Revision 2—Guide to Bluetooth Security. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf (accessed on 4 November 2022).
29. Dunning, J. Taming the blue beast: A survey of bluetooth based threats. *IEEE Secur. Priv.* **2010**, *8*, 20–27. [CrossRef]
30. Sandhya, S.; Devi, K.S. Analysis of Bluetooth threats and v4.0 security features. In Proceedings of the 2012 International Conference on Computing, Communication and Applications, Dindigul, India, 22–24 February 2012.
31. Ryan, M. Bluetooth: With low energy comes low security. In Proceedings of the 7th USENIX Workshop on Offensive Technologies (WOOT 13), Washigton DC, USA, 13 August 2013.
32. Bräuer, S.; Zubow, A.; Zehl, S.; Roshandel, M.; Mashhadi-Sohi, S. On practical selective jamming of bluetooth low energy advertising. In Proceedings of the 2016 IEEE Conference on Standards for Communications and Networking (CSCN), Berlin, Germany, 31 October–2 November 2016.
33. Kwon, G.; Kim, J.; Noh, J.; Cho, S. Bluetooth low energy security vulnerability and improvement method. In Proceedings of the 2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), Seoul, Republic of Korea, 26–28 October 2016.
34. Cope, P.; Campbell, J.; Hayajneh, T. An investigation of Bluetooth security vulnerabilities. In Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 9–11 January 2017.
35. Lonzetta, A.M.; Cope, P.; Campbell, J.; Mohd, B.J.; Hayajneh, T. Security vulnerabilities in Bluetooth technology as used in IoT. *J. Sens. Actuator Netw.* **2018**, *7*, 28. [CrossRef]
36. Hassan, S.S.; Bibon, S.D.; Hossain, M.S.; Atiquzzaman, M. Security threats in Bluetooth technology. *Comput. Secur.* **2018**, *74*, 308–322. [CrossRef]
37. Zhang, Y.; Weng, J.; Dey, R.; Fu, X. Bluetooth Low Energy (BLE) Security and Privacy. In *Encyclopedia of Wireless Networks*; Springer: Cham, Switzerland, 2019; pp. 1–12.
38. Pallavi, S.; Narayanan, V.A. An overview of practical attacks on ble based iot devices and their security. In Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 15–16 March 2019.
39. Cayre, R.; Nicomette, V.; Auriol, G.; Alata, E.; Kaaniche, M.; Marconato, G. Mirage: Towards a Metasploit-like framework for IoT. In Proceedings of the 2019 IEEE 30th International Symposium on Software Reliability Engineering (ISSRE), Berlin, Germany, 28–31 October 2019.
40. *Mil-Std-1629A*; Military Standard Procedures for Performing a Failure Mode, Effects and Criticality Analysis. US Department of Defense: Washington, DC, USA, 1980.
41. Dhanda, S.S.; Singh, B.; Jindal, P. Lightweight cryptography: A solution to secure IoT. *Wirel. Pers. Commun.* **2020**, *112*, 1947–1980. [CrossRef]
42. Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access* **2021**, *9*, 28177–28193. [CrossRef]
43. Schläpfer, T.; Rüst, A. Security on iot devices with secure elements. In Proceedings of the Embedded World Conference 2019, Nuremberg, Germany, 26–28 February 2019.
44. Elrawy, M.F.; Awad, A.I.; Hamed, H.F. Intrusion detection systems for IoT-based smart environments: A survey. *J. Cloud Comput.* **2018**, *7*, 1–20. [CrossRef]
45. Khraisat, A.; Alazab, A. A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity* **2021**, *4*, 1–27. [CrossRef]
46. Safi, M.; Dadkhah, S.; Shoeleh, F.; Mahdikhani, H.; Molyneaux, H.; Ghorbani, A.A. A Survey on IoT Profiling, Fingerprinting, and Identification. *ACM Trans. Internet Things* **2022**, *3*, 1–39. [CrossRef]
47. NXP—QN908x Ultra Low Power Bluetooth 5 System-on-Chip Solution. Available online: https://www.nxp.com/docs/en/nxp/data-sheets/QN908x.pdf (accessed on 4 November 2020).
48. Ma, Q.; Xiao, Q.; Hong, Q.R.; Gao, X.; Galdi, V.; Cui, T.J. Digital Coding Metasurfaces: From Theory to Applications. *IEEE Antennas Propag. Mag.* **2022**, *64*, 96–109. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.