

Article

Wireless Communication and Management System for E-Bike Dynamic Inductive Power Transfer Lanes

Jose A. Afonso ^{1,*}, Helder G. Duarte ¹, Luiz A. Lisboa Cardoso ², Vitor Monteiro ²
and Joao L. Afonso ²

¹ CMEMS-UMinho, University of Minho, 4800-058 Guimarães, Portugal; a75121@alunos.uminho.pt

² Centro ALGORITMI, University of Minho, 4800-058 Guimarães, Portugal; lisboa.cardoso@ieee.org (L.A.L.C.); vmonteiro@dei.uminho.pt (V.M.); jla@dei.uminho.pt (J.L.A.)

* Correspondence: jose.afonso@dei.uminho.pt

Received: 25 July 2020; Accepted: 7 September 2020; Published: 10 September 2020



Abstract: This paper presents the design, implementation, and testing of a wireless communication system for automatic identification of e-bikes and management of their battery charging in the context of dynamic inductive wireless power transfer (DIWPT) lanes. The proposed system checks if an e-bike, uniquely identified by its RFID tag, is authorized to receive energy from the lane coils and acts accordingly. An authentication mechanism was developed based on the use of embedded Wi-Fi boards attached to the coils and communicating with a central HTTP server with a MySQL database. The developed management system also provides other features, such as the recording of the number of lane coils used by each e-bike for billing purposes. The results from experimental tests on a laboratory prototype were used to validate the developed functionalities and assess the quality of service provided by the proposed system.

Keywords: dynamic inductive wireless power transfer; network-based management system; automatic vehicle identification; wireless communication

1. Introduction

Bicycles, as an alternative to diminish the use of vehicles with combustion engines, can play an important role in combating climate change caused, in part, by the use of fossil fuels. They also constitute a means of transport that brings several other benefits compared to cars, such as physical exercise and health improvement, less space required for parking, and lower acquisition and maintenance costs. In particular, electric bicycles, or e-bikes, are increasingly becoming a sustainable alternative to satisfy the mobility needs of the population in urban contexts. Differently from the purely human-powered bicycles, e-bikes make it possible for less-fit individuals to ride on steep terrains and for longer distances. However, similarly to the case of standard road electric vehicles (EV), in e-bikes, the battery also accounts for an expressive part of both the initial and life-cycle costs of the vehicle. Based on the natural characteristics of e-bikes, they can be categorized as an EV, but with the possibility to be powered both by human traction and by batteries, they also contribute to mitigating the economic and environmental issues of batteries. Moreover, their use in conjunction with a dynamic inductive wireless power transfer (DIWPT) lane system [1] makes them a viable option as a battery-less EV for commuting and general lightweight urban transport.

One of the crucial design aspects of DIWPT lanes [2–5] is the synchronization of power switching of the primary coils, along the vehicle's path, with the presence of the vehicle itself. In the current best DIWPT research efforts, such as the FABRIC European project [6], this synchronization and the lane management itself are achieved at an implementation complexity that is not likely to be currently affordable for lightweight EV applications, such as e-bikes. The DIWPT management platform

developed in the context of the aforementioned project provides an extensive set of features [7]: authentication of EVs through local and remote services, local identification of EVs for sequential activation of the lane coils, charging process monitoring and delivering of charging session information to the cloud, as well as assisting the driver in keeping the EV aligned on the lane for maximum energy exchange, through the use of a vehicle camera. In this platform, each lane coil is equipped with a charging station control unit (CSCU), which is an embedded computer running a Debian-based operating system equipped with a CAN (Controller Area Network) interface for communication with the local power electronics controller, a IEEE 802.11p-based COHDA device [8] for communication with the EV, as well as a network interface (e.g., Ethernet, WLAN, or 3G) for communication with a system operator in a control room through the Internet. For authentication, the EV sends its credentials through 802.11p when approaching the charging lane. Additionally, the CSCU uses an Ethernet-connected Automatic Number Plate Recognition (ANPR) camera placed near the coils to verify if the EV entering the charging lane has been authenticated.

In reference [9], a new simple method for activating the power of primary coils, based on the detection of near-field RFID (Radio Frequency Identification) tags, was described and applied to e-bikes. In this method, attached to each primary coil, there is an RFID reader that independently detects the approach and recognizes e-bikes (actually, their tags), and, based on the tag identifier, promotes coil activation or not. For the RFID technology used in that design, both the reader modules and the tags are inexpensive, favoring its use in DIWPT lanes for e-bikes. In that work, however, two limiting factors were left for future handling: (1) scalability, specifically, the need for a network-based management system to handle centralized authorization for a large number of vehicles, in real-time; (2) performance regarding a maximum speed for e-bikes of about 30 km/h.

Regarding maximum speed, it is important to note that new e-bikes being introduced in the market can easily achieve more than 40 km/h, with EU regulation No. 168/2013 already categorizing e-bikes with a maximum speed of electrical assistance up to 45 km/h [10]. However, the PEDELEC (Pedal Electrically Assisted Cycles) class e-bikes [11], the most common in EU countries, have a maximum speed of electrical assistance restricted to 25 km/h, which is still less than the maximum speed that can be handled in [9]. On the other hand, the absence of a more flexible and complete management system to provide authorization for energy requests coming from vehicles is a far more urgent issue to solve, being essential for the adoption of a large scale DIWPT lane urban network for e-bikes.

Aligned with the abovementioned limiting factors, this work describes the design, implementation, and testing of a low-complexity network-based management system that enhances the DWIPT lanes system presented in [9] through the introduction of a series of new features. As the main contribution, the proposed system includes the development of a wireless communication network that connects the primary coils attached to the DIWPT lane to a central server, through which information about the e-bikes and the primary coils (from which they received energy) is transferred. The relevant data are stored in a database installed on the server in order to provide features such as authentication of the users/e-bikes and the accounting/billing of the energy consumption for each e-bike. The developed system also provides a set of functionalities for user account management, in the context of customer service desks.

In this paper, Section 2 provides a brief overview of the DIWPT lanes system for e-bikes, the requirements for the proposed network-based management system, and the architecture designed to satisfy these requirements. Section 3 describes the software development accomplished using the hardware selected for the implementation of the system architecture, as well as the structure of the main data packets defined in the context of the proposed network-based management protocol. Section 4 describes the experimental tests performed to validate the developed system prototype. Finally, Section 5 presents the conclusions and suggestions of future work.

2. System Design

In the DIWPT lanes system proposed in [1,9], the primary coils installed on the lane are activated by a positive reading from an RFID tag placed on the e-bike. Several primary coils installed sequentially in the lane provide energy to the secondary coil placed on the e-bike as it moves over the lane. This system avoids the need to create conventional stationary battery charging spaces, as well as congestion in these spaces and the time needed to wait for the battery to be charged.

Figure 1 illustrates the basic arrangement of an e-bike over a primary coil of the DIWPT lane system, to which RFID readers, with their collocated reading coils, were added in this work.

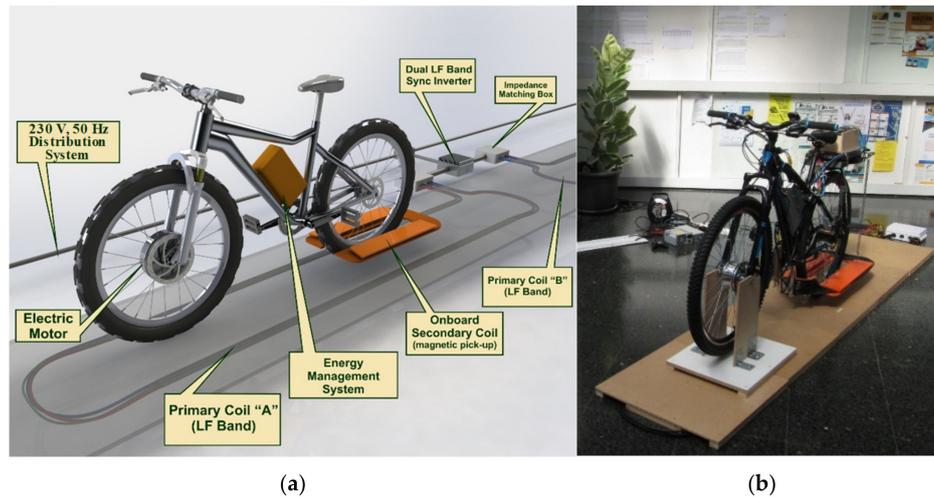


Figure 1. (a) E-bike adapted with an onboard energy harvest system positioned over a primary coil of the DIWPT lane. (b) The real prototype in a public demonstration at the University of Vigo in 2017.

The e-bike receives energy from the lane repeatedly, each time it enters the induction field of a primary coil (Figure 2). During this time, the powertrain is electrified by the energy harvested from the lane and, if a battery is optionally installed, the excess energy not used by the powertrain can be used to charge that battery. If no battery is installed on the e-bike, a small supercapacitor bank will supply the energy during the inter-coil transits, so that the e-bike can still be 100% electrically powered all the time, while moving on the lane. For safety and efficiency reasons, the activation of a primary coil should only occur when the power transfer is needed—that is, when an e-bike is within possible reach of its induction field. This condition is set when an RFID tag attached to the e-bike is detected and positively recognized, and is automatically reset when the e-bike leaves the field of induction, causing the power demand from the primary coil to fall below a pre-established minimum level; or by time-out, considering a minimum bicycle speed.

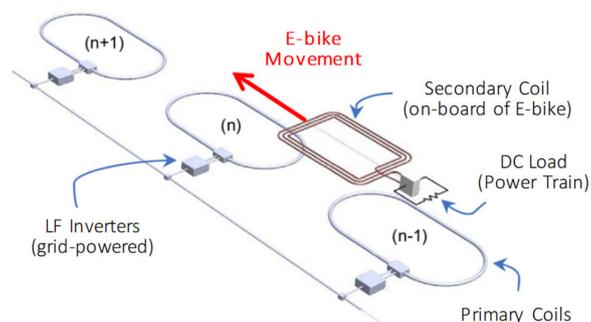


Figure 2. Configuration of the DIWPT lane system with consecutive primary coils.

2.1. Functional Requirements

The wireless communication and management system proposed in this paper enhances the DWIPT lane system referred to above with a set of new features. The main functionalities defined for the proposed system are related to the use of the e-bikes on the lane. Among these functionalities, it is essential to provide an e-bike authentication mechanism that operates at each primary coil, in order to determine if the e-bike is authorized to receive energy from that coil or not. Another required feature is the determination of energy consumption by each e-bike, in order to provide the respective billing.

The design of the developed system also provides a set of functionalities to be offered in the context of customer service desks, instead of the lanes. These functionalities are related to user account management and comprise registration of a new user in the system, billing of the user, and deletion of the account. Besides the satisfaction of the functional requirements referred to above, the system must provide an adequate level of quality of service to the users, which is expressed in terms of communication delay/response time and reliability. In order to satisfy the requirements stated in this section, the system architecture described in the next section was designed.

2.2. System Architecture

Figure 3 presents the architecture proposed in this paper for the conceived system, in order to satisfy the requirements defined in the previous section, as well as the technologies chosen for its implementation. One MFRC522 RFID reader board [12] is attached to each primary coil module, for the purpose of reading the RFID tag containing the unique UID (User Identifier) that is attached to each e-bike, in order to provide automatic vehicle identification. The RFID reader transfers the UID to the associated embedded Wi-Fi board via an SPI (Serial Peripheral Interface). Each Wi-Fi board connects directly to a Wi-Fi access point (AP), forming a wireless local area network (WLAN) and allowing the communication with the central server connected to a database. The server may be directly connected to the WLAN or may be accessed remotely through the Internet. In addition to the RFID reader and Wi-Fi board attached to each primary coil on the lane, these embedded boards may also be installed at customer service desks in order to perform functions associated with user account management, as explained below.

In Figure 3, the direction of movement of the e-bikes is from the right to the left. For illustration purposes, we may consider that the two e-bikes shown in the figure started their travel at the rightmost primary coil of the lane (although the developed system allows any e-bike to start the use of the lane at any primary coil). The RFID tag of the rightmost bicycle is detected by the RFID reader of that same coil. The Wi-Fi board then sends an authentication request to the server to query if this bicycle is allowed to use the energy supplied by this coil. The server then sends back an authentication response, which is broadcast to all Wi-Fi boards embedded on the lane, which store this information in local lists in order to decrease network traffic and improve response times.

As for the e-bike in the middle of the lane, it already has travelled through two primary coils, which means that the Wi-Fi board attached to the third primary coil already has the information of whether the bicycle is authorized to use its coil, which was received in a broadcast packet triggered by a previous primary coil. This means that the Wi-Fi board performs a local list authentication instead of sending an authentication request to the server. Nevertheless, this Wi-Fi board sends an energy consumption data packet to the server. In the current prototype, this packet only reports the use of the primary coil by the e-bike instead of the accurate energy consumption.

The range of communication network technologies that could be used to implement this system is vast. The choice of IEEE 802.11/Wi-Fi [13] was due to a series of advantages relative to the existing alternatives. Compared to other local area network (LAN) technologies, such as Ethernet [14], the advantage is that Wi-Fi is a wireless LAN, which eliminates the costs of installing and maintaining cables. The use of power wires for communication (using a power line communication technology) tends to increase the complexity in the design of the system (e.g., to guarantee that the wires are both suitable for power and communications). On the other hand, the Wi-Fi solution decouples the design

of the power and communication systems and is widely available in embedded boards. Moreover, the proposed wireless communication system allows the e-bike to send/receive information (through a device attached to the e-bike or the user’s smartphone), enabling the provision of new related features, which are not possible with a wired solution. In comparison with wireless personal area network (WPAN) technologies [15], such as classic Bluetooth and Bluetooth Low Energy (BLE) [16] or ZigBee [17], a fundamental advantage is that Wi-Fi is compatible with the Internet protocol stack, required for communication through the Internet, which does not happen with these WPAN standards. Other advantages over these WPANs are the greater range and higher data transmission rate. Although the energy consumption of the communication devices is higher, this is not a problem in the context of the proposed system, since the energy required by the embedded Wi-Fi boards is much lower than the average energy that the primary coils to which they are attached may supply. The main advantage of using Wi-Fi compared to mobile cellular networks is that Wi-Fi operates in ISM (Industrial, Scientific, and Medical) frequency bands, which do not require a license, whereas mobile cellular networks operate in frequency bands licensed to mobile service providers and therefore, have costs associated with data transmission.

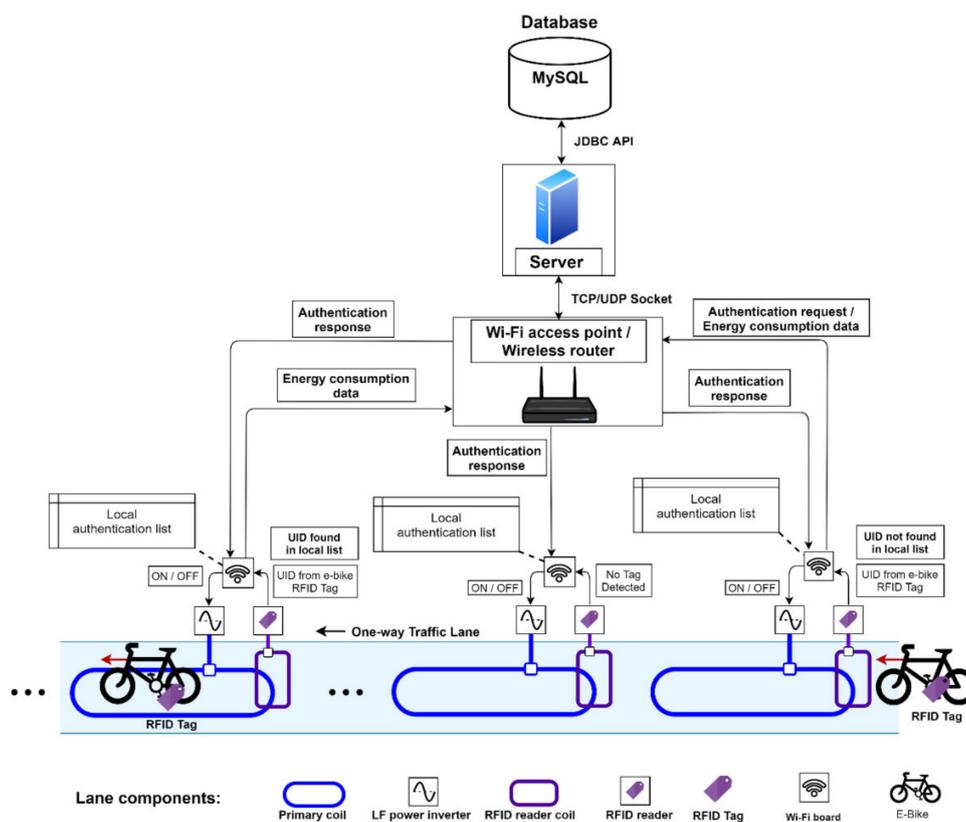


Figure 3. Architecture of the developed system.

The embedded Wi-Fi board used in this work is a low-cost ESP32-DevKitC-32D board, from Espressif Systems, which integrates the ESP32-WROOM-32D module [18]. This is a versatile embedded communication platform with support to Wi-Fi (IEEE 802.11b/g/n/e/i) and Bluetooth 4.2 (classic Bluetooth and Bluetooth Low Energy) wireless protocols, and is suitable to a wide range of applications. At the heart of the board is the ESP32-D0WDQ6 system on a chip, which includes a dual core microcontroller unit (MCU) and RF transceivers. It also supports several peripheral interfaces, such as SPI, I2S (Inter-IC Sound), I2C (Inter-Integrated Circuit), and UART (Universal Asynchronous Receiver–Transmitter).

The server is a computer responsible for coordinating the authorization of the use of the energy supplied by the lane, storing the energy consumption data for each e-bike, and managing the accounts and billing of the users. For this purpose, it receives requests (or information) and provides responses to the Wi-Fi boards placed on the lane and the service desk. In parallel, the server also makes requests to the database that is located on the same computer as the server, through the JDBC (Java Database Connectivity) API (Application Programming Interface), in order to guarantee the long-term storage of the information and its use when necessary. The database is equipped with a data model which includes the registration of each e-bike and respective energy consumption, as well as the current status of authorization of the user of the lane, allowing the system to reject the authorization of e-bikes based on lack of registration, improper use of the system, or debts from the users.

3. System Development

This section describes the system development performed using the components of the architecture conceived in Figure 3. Concerning the proposed wireless communication and management system, the main components are the server, the database, and the embedded modules. This section also presents the packet formats conceived for each data packet implemented in order to satisfy the functional requirements defined in Section 2.1.

3.1. Server and Database

The server plays a central role in the developed system, its main task being to control the authorization of access of the e-bikes to the energy supplied by the primary coils and to store the information of their energy consumption. The server is also responsible for tasks associated with user account management through service desks. It was implemented in Java.

The database data model was implemented in MySQL and uses the JDBC API which, in general, serves to connect a Java application to a database and execute the SQL (Structured Query Language) instructions defined in the application.

Most of the packets referred to in Section 3.3, as well as user account management packets, may use TCP (Transmission Control Protocol) at the transport layer. On the other hand, since the authentication response packets from the server to the Wi-Fi boards at the lane are transmitted using broadcast, these packets use UDP (User Datagram Protocol), which only supports unicast communication. The programming of the sending of UDP packets by the server was done using the sockets of the class `DatagramSocket` in Java code.

For each e-bike traveling on the lane, the implemented system counts the number of primary coils from which it receives energy. Each time a primary coil is activated by passing an e-bike, its Wi-Fi board sends a packet signaling the use of the coil to the server, containing the UID of the RFID tag attached to the e-bike. For each path travelled by an e-bike, the server calculates the number of primary coils multiplied by the unit cost of using each primary coil (which, for testing, was set to 1 cent per coil). This result is added to the amount already stored in the database for the respective e-bike.

Figure 4 shows the flowchart that represents the processing of packets received by the server from the Wi-Fi boards attached to the primary coils installed on the DIWPT lane. The structure of the types of packets referred to in this section is described in Section 3.3. If the packet type is an authorization request, the server verifies if the UID of the e-bike is valid (green) or invalid (black), and sends an authentication response packet containing the respective packet type (green or black) by broadcast to all Wi-Fi boards connected to the local network. If the UID is valid, the server also increments by one the number of primary coils used by that e-bike. On the other hand, if the packet type is signaling the use of another primary coil—that is, if the e-bike has already obtained authorization from a previous coil on its path—the same procedure of incrementing by one the number of primary coils used by the e-bike identified by the UID contained in the packet is performed. If the packet received by the server does not match one of the types referred to above, the server assumes that it is a user account

management packet and transfers the processing to another part of the code, which is represented in Figure 5.

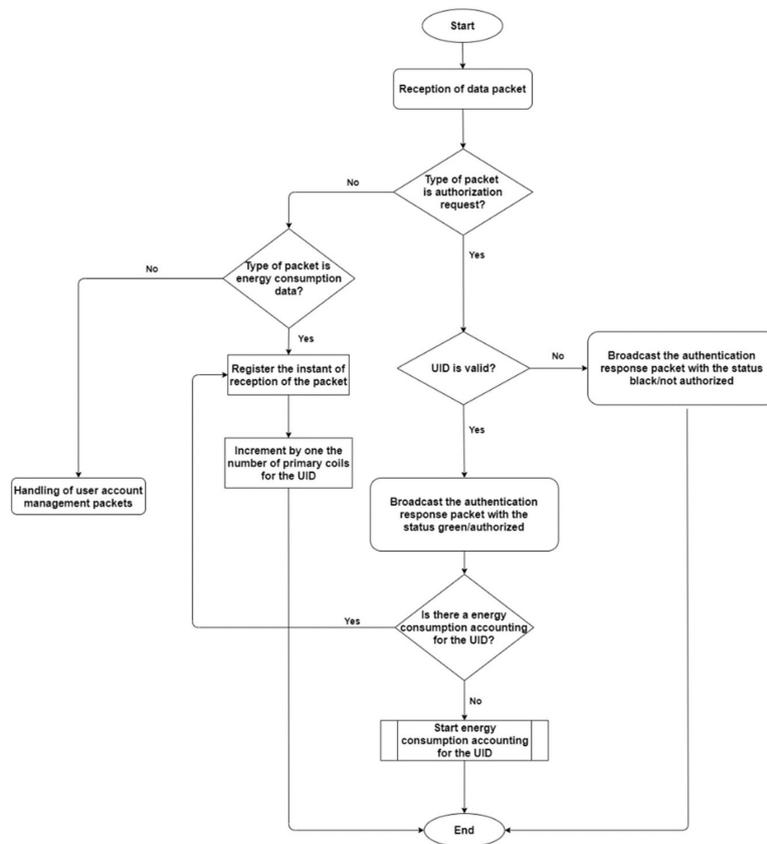


Figure 4. Flowchart of the processing of packets received from the DIWPT lane on the server.

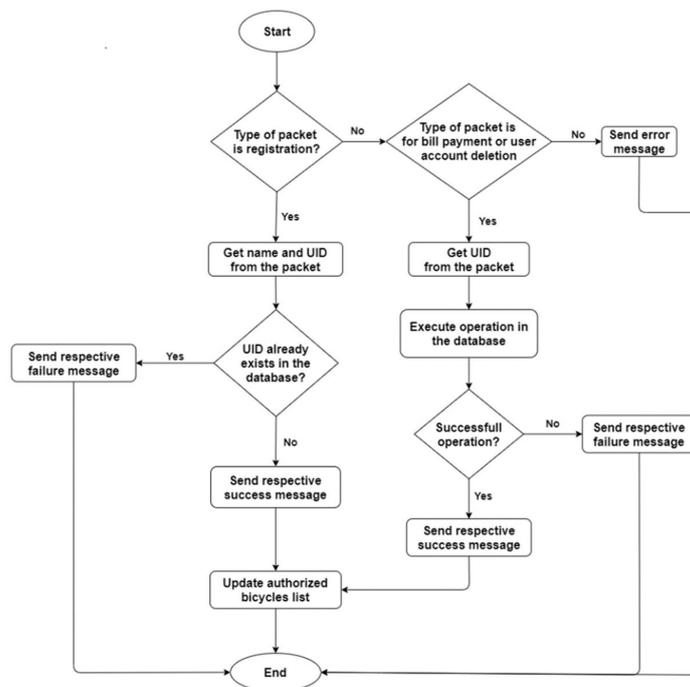


Figure 5. Flowchart of the processing of user account management packets received from the service desk.

Figure 5 presents the flowchart of the processing performed on the server for the main user account management packets received from the customer service desk. If it is a registration packet, the UID is checked in the database. If it is already registered, a failure message is sent back to the service desk; otherwise, the user data are registered, the UID is placed in the authorized list, and a success message is sent back. Otherwise, if it is a bill payment or user account deletion packet, the respective operation is performed in the database.

3.2. Embedded Boards

The embedded boards used in this system are an RFID reader and a Wi-Fi board, which communicate using the SPI interface.

This system uses high frequency (HF) near-field RFID technology. The low-cost RFID tags and RFID reader boards (model MFRC522) used in this system are part of the MIFARE Classic family of products from NXP Semiconductors. In the standard MIFARE readers, the detection volume is only a few centimeters wide. Subsequently, the antennas and matching circuitry of both the RFID reader and the tag have undergone changes in order to increase the reading range and meet the system requirements of maximum distance-to-lane and lateral vehicle misalignment tolerance up to 40 cm [9].

The MFRC522 RFID reader board [19] integrates a chip with read/write capabilities for contactless communication, through electromagnetic induction, at the frequency of 13.56 MHz. The MFRC522 is compatible with the ISO/EC 14443A standard and is also equipped with SPI, UART, and I2C interfaces.

The programming of the Wi-Fi boards used in the scope of the work described in this paper (model ESP32-DevKitC-32D) was done using the Arduino IDE (Integrated Development Environment). The ESP32 board controls the RFID reader through the SPI and communicates with the server through Wi-Fi. When the ESP32 board is turned on, it initializes the RFID reader board and establishes the connection with the Wi-Fi AP/router. In each ESP32 board, it was only necessary to configure the name of the Wi-Fi local network and the respective password. After establishing the Wi-Fi connection, a UDP socket is created between the ESP32 board and the server, using the existing API in the board's Wi-Fi library for Arduino.

These embedded boards can be installed at a customer service desk or on a lane, next to the respective primary coil it will control. In the first case, the ESP32 board processes the different packets associated with user account management, while in the second case, the board processes packets associated with the authorization of use of the lane and the number of primary coils used by the e-bikes.

Figure 6 presents a flowchart of the charging authorization processing performed by the ESP32 boards attached to the primary coils at the lane when its RFID reader detects a new RFID tag. Each ESP32 board maintains two lists that store UIDs of the RFID tags attached to the e-bikes. One of the lists, the BlackList, stores only UIDs for e-bikes not authorized to use the system, while the GreenList stores only UIDs for authorized e-bikes. Each list consists of an array of N_L positions that store the 8-byte UIDs contained in the packets received from the server by order of insertion, according to its authorization status (green or black). These packets are received via broadcast, in response to the authentication request made by the ESP32 board itself or by a nearby board, or when the authorization status in the database changes. When a list is full, the oldest UID is removed to make way for the most recent one.

The implementation of these lists provides a local cache in each ESP32 board, which means that it does not have to send the authorization request to the server when it already has the e-bike UID stored in one of the two local lists, thus reducing response time and data traffic, and consequently, increasing system efficiency. This is particularly true for ESP32 boards attached to the next primary coils in the path of the e-bike, which receive this information via broadcast. In the event that the UID is not present in any of the two lists, the system grants to the e-bike a short-term provisional authorization to use the DIWPT lane, while an authentication query to the server is made. If the server's response indicates that the UID is not authorized, the provisional authorization is cancelled and the power transfer is interrupted immediately.

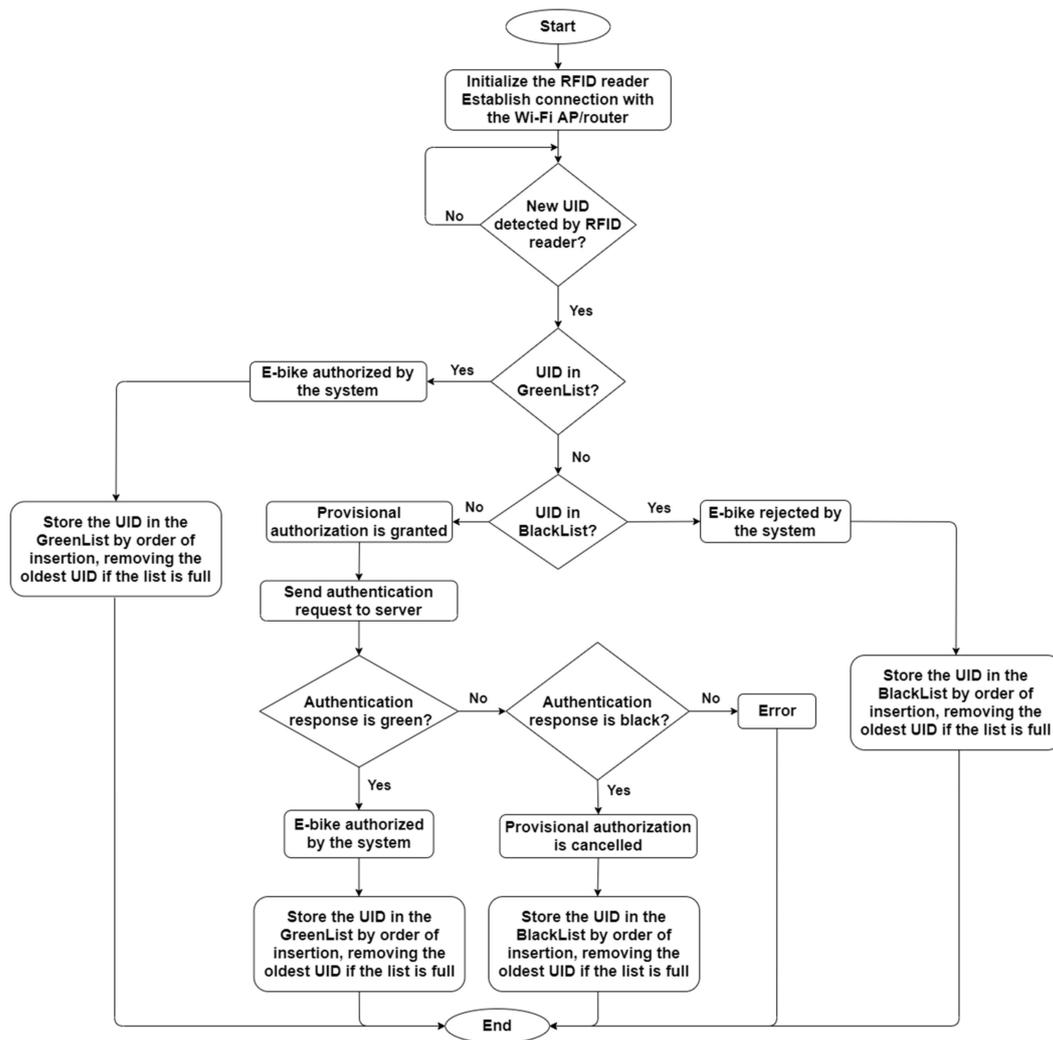


Figure 6. Flowchart of the authorization processing performed by the ESP32 boards at the lane.

3.3. Data Packets Structure

At the application layer level of the OSI model, with the exception of some user account management packets, which may contain more fields (such as the name of the user), the data packets transferred between the server and the Wi-Fi boards installed in the DIWPT lane consist of only two fields: the packet type (1 byte) and the e-bike UID (8 bytes). The packet type in each case is represented by a character, as indicated below between parentheses.

As shown in Figure 3, there are two types of packets that can be sent from a Wi-Fi board on the DIWPT lane to the server: an authentication request (#) and energy consumption data (%), where the Wi-Fi board signals the use of its primary coil. On the other hand, the server packets for the Wi-Fi boards, which are sent via broadcast to all boards in the same WLAN, are divided into two categories: authentication response, which can be green/authorized (?) or black/not authorized (/); and updating of a UID status in the local lists (as a result of a change in the respective status in the database, associated, for example, with the non-payment of an invoice or with debt settlement), from green to black (&) or vice versa (\$).

4. Experimental Results

The experimental tests presented in this section were designed to validate the functioning of the network-based management system and the satisfaction of its functional and non-functional

requirements. They have so far been performed in a laboratory setup with the original RFID reader antennas and no actual vehicles running on the inductive lanes.

For these tests, a prototype system was implemented using the architecture represented in Figure 3, with two ESP32 boards, two MFRC522 RFID reader boards, and four RFID tags. The Wi-Fi AP/router used in these tests was a Huawei HS8247W, supplied by Vodafone Portugal ISP (Internet Service Provider, Lisbon, Portugal). The server software and respective database were installed on a Lenovo Ideapad Y700-15ISK-80NV personal computer (PC) running the Ubuntu 18.04 operating system (London, UK). This PC has an Intel Core i7-6700HQ processor, 256 GB SSD (Solid State Drive), and 16 GB of RAM (Random Access Memory).

The server was placed in the same WLAN of the embedded boards. The local IP (Internet Protocol) address of the Wi-Fi AP/router was 192.168.1.1. The IP address assigned to the server was 192.168.1.10, whereas the IP addresses assigned to the ESP32 boards were 192.168.1.4 and 192.168.1.6.

4.1. Quality of Service

In terms of non-functional requirements, two relevant quality of service (QoS) parameters in the context of this system are the authentication query delay (minimum, mean, maximum, and standard deviation) and the corresponding delivery ratio.

In order to have an adequate number of sample points to measure these parameters, 1000 authorization queries were performed from one of the ESP32 boards to the server. The query delay is the time elapsed since the authorization request packet is sent to the server by the ESP32 board (start time) until the broadcast authorization response is received by the same ESP32 board (end time). The fact that both the start and end times were measured on the same device in this test setup ensures that there were no clock synchronization issues. The delivery rate was measured simultaneously using the 1000 queries and was calculated as the ratio between the authorization response packets received and the authorization request packets sent by the ESP32 board. This test was carried out without any other device being connected to the WLAN, in order to exclude other traffic sources that could have an effect on the results. The results obtained in this test are presented in Table 1.

Table 1. Results of measurement of the authentication query delay and delivery ratio.

Parameter	Value
Minimum delay	4.5 ms
Mean delay	104.2 ms
Maximum delay	211.6 ms
Standard deviation	68.1 ms
Delivery ratio	99.8%

With primary coils of minimum length of 325 cm and a maximum vehicle speed of 25 km/h, the minimum time taken for an e-bike to traverse a primary coil is approximately 468 ms, which is greater than the maximum query delay registered in Table 1, even after adding the RFID reading delay of approximately 30 ms [9]. Therefore, the next primary coil in the path of the e-bike will already have the authentication response stored in cache, so it will not need to make a new authentication request, unless the response is lost (which happened in 0.2% of the cases in this test). In this case, the next primary coil would also give provisional authorization and send a new authentication request, but the following coil would probably not have to do so.

The use of TCP instead of UDP has the advantage of increasing the delivery rate to 100% for unicast packets. However, as referred to before, the broadcast of the authentication responses might not be made using TCP. The query delay would also tend to be higher with TCP, due to its higher protocol overhead and the retransmissions of lost packets.

It should be noted that the query delay results may vary depending on the equipment used in the system (e.g., Wi-Fi router and server computer). Moreover, if the server were placed remotely,

outside of the local network, the query delays would also tend to increase. Therefore, the provisional authorization mechanism implemented in the system is useful to eliminate lags in the authorization grant, which could possibly be perceived negatively by the users.

4.2. Functional Requirements

An extensive set of tests covering all functional requirements defined in Section 2.1 was carried out. This section presents the results of the tests used to validate the implementation of the functionalities related to the use of the DIWPT lane, more specifically, the e-bike authentication mechanism and the energy consumption accounting process, which, in the context of this prototype, records the number of primary coils used by each e-bike.

The authentication requests sent from ESP32 boards on the lane and the associated broadcast authentication responses from the server are among the most critical features of the system, given that the primary coils activate the power transfer to an e-bike on a provisional basis when the RFID tag is read and the UID is not found in any of the two local ESP32 board lists. However, after the authentication response arrives to the primary coils, if the UID is not authorized, the power supply is cut off.

Figure 7 shows the MySQL shell including four previously registered UIDs, where it is visible that the e-bike with the UID “6292E71F” (green underline) is classified as “green” (authorized), whereas the e-bike with the UID “D2C35043” (red underline) is classified as “black” (not authorized).

```
mysql> SELECT * FROM bicycle;
+-----+-----+-----+-----+
| id      | owner      | debt | listType |
+-----+-----+-----+-----+
| 03DAD283 | Luisa Gomes | 0    | green    |
| 6292E71F | Helder Gomes | 9    | green    |
| 821AD583 | Patricia Gomes | 0    | green    |
| D2C35043 | Paulo Gomes | 2    | black    |
+-----+-----+-----+-----+
4 rows in set (0.00 sec)

mysql> 
```

Figure 7. MySQL shell with four registered UIDs.

Figure 8 shows the results for the tests associated with the authentication mechanism, from the point of view of the ESP32 boards. Besides the two RFID tags with UIDs underlined in Figure 7, these tests involve two RFID readers and the corresponding ESP32 boards, with IP addresses 192.168.1.4 and 192.168.1.6, represented by the terminal windows on the left and right of the Figure 8, respectively. Likewise, the terminal window of Figure 9 represents the authentication packets sent and received by the server, as well as the associated tasks.

For this test, the GreenList and the BlackList of both ESP32 boards were configured with three $N_L = 3$ positions. At the beginning of the test, the lists of both ESP32 boards were empty. First, the RFID tag with UID “D2C35043” was read by the board associated with the IP address 192.168.1.4. As Figure 8 shows, the UID was not found in its local lists, so the ESP32 board sent an authentication request to the server, receiving as the response a packet with the content “/D2C35043”, where the character “/”, which represents the packet type, indicates that the UID is not authorized. Since the authentication responses are sent by broadcast, the same packet arrived also to the ESP32 board with IP address 192.168.1.6, thus both boards inserted this UID in their respective BlackLists. Next, the RFID tag with UID “6292E71F” was read by the ESP32 board with IP address 192.168.1.6. Once again, the UID was not found in the board’s local lists, so it sent an authentication request packet to the server and received an authentication response packet with the content “?6292E71F”, where the “?” indicates

that this UID is authorized. The same authentication response arrived at the left window, so both boards inserted the UID in their GreenLists.

```

ESP32 board IP address: 192.168.1.4
Received UID from RFID reader: D2C35043
Not found. Send authorization request

Received authentication resp.: /D2C35043
Insert UID on the BlackList
BlackList:0:D2C35043
BlackList:1:
BlackList:2:

Received authentication resp.: ?6292E71F
Insert UID on the GreenList
GreenList:0:6292E71F
GreenList:1:
GreenList:2:

Received UID from RFID reader: D2C35043
UID already exists in the BlackList

Received UID from RFID reader: 6292E71F
UID already exists in the GreenList

ESP32 board IP address: 192.168.1.6
Received authentication resp.: /D2C35043
Insert UID on the BlackList
BlackList:0:D2C35043
BlackList:1:
BlackList:2:

Received UID from RFID reader: 6292E71F
Not found. Send authorization request

Received authentication resp.: ?6292E71F
Insert UID on the GreenList
GreenList:0:6292E71F
GreenList:1:
GreenList:2:

Received UID from RFID reader: D2C35043
UID already exists in the BlackList

Received UID from RFID reader: 6292E71F
UID already exists in the GreenList

```

Figure 8. Results for the tests of the authentication mechanism from the point of view of the ESP32 boards.

```

Received auth. req.: #D2C35043 Source address: 192.168.1.4
UID is not authorized
Broadcast authorization response for UID D2C35043

Received packet: /6292E71F Source address: 192.168.1.10

Received auth. req.: #6292E71F Source address: 192.168.1.6
UID is authorized
Broadcast authorization response for UID 6292E71F
Start energy consumption accounting for UID
[UID: 6292E71F Number of Coils: 1]

Received packet: ?6292E71F Source address: 192.168.1.10

Received consumption: %6292E71F Source address: 192.168.1.4
Energy consumption accounting exists
Adds primary coil
[UID: 6292E71F Number of Coils: 2]

Received consumption: %6292E71F Source address: 192.168.1.6
Energy consumption accounting exists
Adds primary coil
[UID: 6292E71F Number of Coils: 3]

```

Figure 9. Results for the functional requirement tests from the point of view of the server.

The same operations described in the previous paragraph can be viewed from the point of view of the server in Figure 9. As shown in this server window, whenever the server sent an authentication response to the ESP32 boards, via broadcast, the same packet was received (and ignored) by the server, which has IP address 192.168.1.10.

The results concerning the validation of the energy consumption accounting process are also shown in the same terminal windows. In Figure 9, when the authentication request packet for UID “6292E71F” arrived to the server from the ESP32 board with IP address 192.168.1.6, the server automatically started the energy consumption accounting for this UID (according to the flowchart represented in Figure 4) and set to 1 the number or coils traveled by the e-bike with this UID, since this UID was authorized (green). Later, as shown in Figure 8, the RFID tag with UID “D2C35043” was read again by both boards, as identified with red braces. In this case, the ESP32 boards no longer made an authentication request to the server, because the UID was found in their BlackLists. Next, the RFID tag with UID “6292E71F” was read again by both boards, as identified with green braces. Since this UID was found

in the GreenLists of both boards, they did not have to send another authentication request to the server. However, each board sent an energy consumption data packet to the server (not represented in Figure 8). The results of reception of these packets by the server were visible in Figure 9, where two primary coils were added, which meant that the number of coils associated with this UID was incremented to 2 and then to 3.

The proposed system was validated in the laboratory, emulating real operating conditions, but its operation is also viable in outdoor environments. For instance, regarding issues related to external noise, the IEEE 802.11/Wi-Fi standards [20] provide several mechanisms to minimize the effect of noise and interference: (1) there are multiple channels available, providing flexibility to choose the most suitable one in the installation area; (2) the IEEE 802.11 CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) MAC (Medium Access Control) protocol works through detecting an ongoing transmission and waiting until the channel is free in order to avoid collisions; (3) in the eventuality that a packet is corrupted, it is retransmitted at the MAC level. Moreover, unlike indoor environments, where a Wi-Fi network may face interference from several other neighbor networks, and even from other devices operating in the same frequency band (such as microwave ovens), outdoor environments tend to be less crowded.

5. Conclusions and Future Work

The wireless communication and management system presented in this paper introduces a series of functionalities to support dynamic inductive wireless power transfer (DIWPT) lane systems which are adequate for e-bikes, in terms of vehicle authentication, energy consumption accounting, and user account management.

Authentication responses are broadcast by the server to all Wi-Fi boards controlling DIWPT lane modules in the same local area network, which store the authorization status in corresponding local lists. This means that the next Wi-Fi boards in the path of an e-bike, most of the time, will not need to send a new authentication request to the server. Together with the provisional authorization mechanism, this design approach decreases network traffic and improves response times, contributing to a better user experience.

The results from the experimental laboratory tests were used to validate all functional requirements defined for the proposed system. The results were also presented for non-functional requirements associated with the quality of service, accompanied by the respective discussion.

The tests were carried out with a single Wi-Fi local network. In a more practical setup covering the entire extent of a DIWPT lane, it would be necessary to expand the system architecture through the implementation of an extended Wi-Fi network, with multiple access points, each one covering part of the lane. This architecture is specified in the IEEE 802.11/Wi-Fi standard and is commonly used in larger areas, such as a university campus. Within the terminology used by this architecture, the network segment covered by a single access point is known as a BSS (Basic Service Set) and the extended network is known as an ESS (Extended Service Set). It would also be appropriate to host the central server and respective database in a cloud.

Concerning the DIWPT lane system, it would be useful to provide a more comprehensive billing method through an accurate measurement of the energy received from each primary coil of the lane, instead of just the indication of the use of each coil. The individual energy consumption from each coil could be included in the energy consumption data packet sent by the Wi-Fi boards, and then, the total consumption for each e-bike could be stored at the server.

The user account management functionalities performed at the service desk are currently carried out using a text-based user interface. For the commercial deployment of the system, it would be necessary to develop new user-friendly graphical user interface applications in order to allow their use by attendants and customers.

Taking into account that security is a relevant matter, concerning the wireless communication, IEEE 802.11/Wi-Fi already provides some security mechanisms. Other additional security techniques

may be incorporated in the proposed system in the future; however, this topic is not the focus of this paper.

Author Contributions: J.A.A. and H.G.D. performed the tasks associated with conceptualization, methodology, formal analysis, and main writing—original draft preparation. L.A.L.C., V.M. and J.L.A. collaborated in the writing—review and editing. J.A.A., H.G.D., L.A.L.C., V.M. and J.L.A. have read and agreed to the published version of the manuscript.

Funding: This work was supported by FCT national funds, under the national support to R&D units grant, through the reference project UIDB/04436/2020 and UIDP/04436/2020.

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

References

1. Cardoso, L.A.L.; Martinez, M.C.; Melendez, A.A.N.; Afonso, J.L. Dynamic inductive power transfer lane design for e-bikes. In Proceedings of the IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2307–2312.
2. Lukic, S.; Pantic, Z. Cutting the Cord: Static and Dynamic Inductive Wireless Charging of Electric Vehicles. *IEEE Electr. Mag.* **2013**, *1*, 57–64. [[CrossRef](#)]
3. Song, K.; Koh, K.E.; Zhu, C.; Jiang, J.; Wang, C.; Huang, X. A Review of Dynamic Wireless Power Transfer for In-Motion Electric Vehicles. In *Wireless Power Transfer*; Coca, E., Ed.; IntechOpen: Rijeka, Croatia, 2016.
4. Deng, B.; Jia, B.; Zhang, Z. Dynamic Wireless Charging for Roadway-Powered Electric Vehicles: A Comprehensive Analysis and Design. *Prog. Electromagn. Res. C* **2016**, *69*, 1–10. [[CrossRef](#)]
5. Patil, D.; McDonough, M.K.; Miller, J.M.; Fahimi, B.; Balsara, P.T. Wireless Power Transfer for Vehicular Applications: Overview and Challenges. *IEEE Trans. Transp. Electr.* **2018**, *4*, 3–37. [[CrossRef](#)]
6. Laporte, S.; Coquery, G.; Deniau, V.; De Bernardinis, A.; Hautière, N. Dynamic Wireless Power Transfer Charging Infrastructure for Future EVs: From Experimental Track to Real Circulated Roads Demonstrations. *World Electr. Veh. J.* **2019**, *10*, 84. [[CrossRef](#)]
7. Cirimele, V.; Diana, M.; Bellotti, F.; Berta, R.; El Sayed, N.; Kobeissi, A.; Colussi, J. The fabric ICT platform for managing wireless dynamic charging road lanes. *IEEE Trans. Veh. Technol.* **2020**, *69*, 2501–2512. [[CrossRef](#)]
8. COHDA Wireless. Available online: <http://www.cohdawireless.com/> (accessed on 1 June 2020).
9. Cardoso, L.A.L.; Afonso, J.L.; Martinez, M.C.; Meléndez, A.A.N. RFID-Triggered Power Activation for Smart Dynamic Inductive Wireless Power Transfer. In Proceedings of the IECON-The Annual Conference of the IEEE Industrial Electronics Society (IES), Beijing, China, 29 October–1 November 2017.
10. EU 168/2013, Regulation (EU) No. 168/2013 of the European Parliament and of the Council of 15 January 2013 on the Approval and Market Surveillance of Two- or Three-wheel Vehicles and Quadricycles. Available online: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013R0168> (accessed on 2 June 2020).
11. Association Française de Normalisation (AFNOR). *European Standard NF EN 15194*; European Committee for Standardization (CEN): Brussels, Belgium, 2017.
12. Jamaluddin, A.; Harjunowibowo, D.; Rochim, M.A.; Mahadmadi, F.; Kakanita, H.B.; Laksono, P.W. Implementation of RFID on Computer Based Test (RF-CBT) System. In Proceedings of the IEEE International Conference on Electric Vehicular Technology and Industrial, Mechanical, Electrical and Chemical Engineering (ICEVT & IMECE), Surakarta, Indonesia, 4–5 November 2015; pp. 153–156.
13. Hiertz, G.R.; Denteneer, D.; Stibor, L.; Zang, Y.; Costa, X.P.; Walke, B. The IEEE 802.11 universe. *IEEE Commun. Mag.* **2010**, *48*, 62–70. [[CrossRef](#)]
14. Law, D.; Dove, D.; D’Ambrosia, J.; Hajduczenia, M.; Laubach, M.; Carlson, S. Evolution of Ethernet standards in the IEEE 802.3 working group. *IEEE Commun. Mag.* **2013**, *51*, 88–96. [[CrossRef](#)]
15. Siep, T.M.; Gifford, I.C.; Braley, R.C.; Heile, R.F. Paving the way for personal area network standards: An overview of the IEEE P802.15 Working Group for Wireless Personal Area Networks. *IEEE Pers. Commun.* **2000**, *7*, 37–43. [[CrossRef](#)]
16. Bluetooth SIG, Version 5.0; Specification of the Bluetooth System. Available online: <https://www.mouser.it/pdfdocs/bluetooth-Core-v50.pdf> (accessed on 14 May 2020).
17. Baronti, P.; Pillai, P.; Chook, V.W.; Chessa, S.; Gotta, A.; Hu, Y.F. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. *Comput. Commun.* **2007**, *30*, 1655–1695. [[CrossRef](#)]

18. Expressif Systems, “ESP32-WROOM-32”, V2.8 Datasheet. 2019. Available online: https://www.espressif.com/sites/default/files/documentation/esp32-wroom-32d_esp32-wroom-32u_datasheet_en.pdf (accessed on 13 May 2020).
19. NXP Semiconductors N.V. “MFRC522 Standard Performance MIFARE and NTAGfrontend”, 112139 Datasheet. Available online: <https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf> (accessed on 27 April 2016).
20. IEEE. *802.11-2016—IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*; IEEE: Piscataway, NJ, USA, 2016.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).