




System for Supporting Implementation and Monitoring of Smart Campus Applications based on IoT Protocols

Franklin A. M. Venceslau¹^a, Ruan D. Gomes²^b and Iguatemi E. Fonseca¹^c

¹Federal University of Paraíba, João Pessoa, 58055-000, Brazil

²Federal Institute of Paraíba, Campina Grande, 58432-300, Brazil

Keywords: Smart Campus, IoT, MQTT, WSNs.

Abstract: This paper describes a system for monitoring Smart Campus applications based on IoT protocols. The system have as main goals to support the deployment of new sensors, actuators, and gateways in the campus, based on a pre-deployed network infrastructure, and to monitor the performance of applications along the time. The network architecture considered in this paper provides reliability through the use of diversity techniques at physical and data link layers, based on the IEEE 802.15.4g SUN standard, and it performs the persistence of information based on time series database. In order to support the network infrastructure evolution and the incorporation of new devices and applications, information about the currently running applications and about the quality of the data links and the wireless network's overload level can be collected by the proposed system. In this position paper, the architecture of the system is described in details, and initial results are discussed.

1 INTRODUCTION


Currently, several applications for smart cities and smart campuses have been proposed, for example: intelligent transport and lighting and environmental and energy resource monitoring (Ejaz et al., 2017). Most of these applications require the use of wireless transmission for communication between the sensing systems distributed across the city/campus to a centralized server. Given this perspective, some solutions for data transmission that already exist, such as Wi-Fi, Bluetooth and ZigBee, are often not adequate due to spatial range limitations.


An alternative may be the use of long-range and low-power networks, such as LoRa or SigFox (Vejlgaard et al., 2017). Both standards operate in the Sub-GHz spectrum, acting with efficient modulation techniques that allow the creation of sparse networks or networks with star topology, which are easier to deploy and maintain. However, these solutions have some disadvantages, since they are proprietary technologies, and have limited flexibility with regard to critical communication requirements on different devices. Among these limitations we can mention: in the case of SigFox, the dependence on an external


service provider in addition to its low transmission rate, about 600 bps under ideal conditions (Vejlgaard et al., 2017). In turn, LoRa, is a parameterizable option according to the spreading factor, however the maximum bit rate is 21.9 kbps, in the frequency range licensed in Brazil (Vejlgaard et al., 2017).

Another alternative to implement LPWAN networks is the IEEE 802.15.4-2015 standard, which defines three different modulation schemes aimed for applications of smart utility networks (SUN): SUN-FSK (Frequency-Shift Keying), SUN-OQPSK (Offset Quadrature Phase-Shift Keying), and SUN-OFDM (Orthogonal Frequency-Division Multiplexing) (Tuset-Peiró et al., 2020). Different from LoRa, this standard is open and offers a greater level of flexibility, since 31 different physical layer configurations are supported with bit rates ranging from 6.25 kbps to 800 kbps (Muñoz et al., 2018). In addition, it considers both the Sub-GHz and the 2.4 GHz band.

In order to build a scenario for the deployment of several smart campus applications, a network architecture was designed with the focus on providing reliable communication through the possibility of applying diversity techniques at the level of modulation and receiver, which is possible by using the IEEE 802.15.4-2015 standard, due to the possibility of using different modulation schemes and configurations in a single transceiver. At the same time, it is ex-

^a <https://orcid.org/0000-0003-2203-1708>

^b <https://orcid.org/0000-0003-4700-7843>

^c <https://orcid.org/0000-0002-5457-7601>

tremely important to have a way of managing the deployment and evolution of this network infrastructure, as well as providing the means to monitor the applications that are running at a given time, to provide information about reliability, and to verify the feasibility of inserting new devices on the network. In this context, this work proposes a management system, which connects to Gateways to configure and monitor the network, as well as to offer important information to support the implementation of new applications for network evolution.

2 RELATED WORK

Based on a previous bibliographic survey and on the studies listed as follow, it is observed that there is a relatively large number of studies that focus, in general, on describing monitoring applications (e.g. for smart energy) using sensor networks. Each study proposes its own analysis focusing on the techniques used, carrying out experiments with different IoT protocols and evaluating the efficiency in the data communication.

Based on this perspective, this work gives a new contribution and aims at the implementation of the concept of “reuse” of the monitoring infrastructure. The proposed infrastructure is seen in a more generic concept, aimed at adding additional layers to provide a better reliability and availability, through data diversity and persistence techniques.

(Marfievici et al., 2017) proposes the implementation of a WSN (Wireless Sensor Network) to monitor an internal environment, composed of a small data-center room taking into account the existence of difficult factors for an accurate monitoring, for example account of the location within an industrial environment such as: temperature, fluctuations, noise and large amount of metallic surfaces that cause a high level of electromagnetic interference. A report based on 17 months of observations from 30 wireless sensor nodes was assembled. In this system, temperature, humidity, air flow level, among other aspects, were measured. After an initial period, a connectivity assessment carried out on the network revealed a high level of noise in some of the nodes, caused by the presence of different sources of interference. By increasing the CCA configuration and reallocating the positioning of some sink nodes, the network was able to achieve 99.2% reliability in the last 8 months of monitoring. In this way, it was possible to highlight the need for the adequate use of reliable tools and protocols, in addition to the definition of project methodologies for managing and deploying WSN in

real-world environments.

(Munoz et al., 2018) makes a very comprehensive analysis about the IEEE 802.15.4g standard, demonstrating through experiments some applications and simulations in indoor and outdoor environments. Several tests were carried out in order to obtain range measurements using the entire scope of the standard, carrying out experiments with different modulation schemes and covering all parameterization in the range comprising the range: 863-870 MHz, in four scenarios many different. The results obtained with the experiments demonstrated that communications with a high level of confidence and that use data rates of up to 800 kbps can be fully achieved in urban environments at 540 m between nodes, regardless of the minor interferences.

(Tuset-Peiró et al., 2020) presents a set of data obtained from the deployment of a single-hop IEEE 802.15.4g SUN (Smart Utility Network) network (11 nodes) in a large industrial environment (110,044 m²) for a long period of time (99 days). The data set contains 11 M entries with RSSI (Received Signal Strength Indicator), CCA (Clear Channel Assessment) and PDR (Packet Delivery Ratio) values. The analyzed results showed a high variability in the mean values of RSSI (that is, between -82.1 dBm and -101.7 dbm and CCA (that is between -111.2 dBm and -119.9 dBm, wich is caused by the effects of multipath propagation and external interference. According to observations made and being above the sensitivity limit for each modulation, these values resulted in poor average PDR values (ie, from 65.9 % to 87.4 %), indicating that additional schemes are of great importance for meet link reliability requirements for industrial applications. In this way, the set of data presented enables students, researchers and professionals to propose new mechanisms and evaluate their performance using realistic conditions, enabling the view of reliability of the RAW (Reliable and Available Wireless) WG (Working Group) at the IETF (Internet Engineering Task Force) (P. Thubert et al., 2020).

(Hossain et al., 2019) This article proposes an intelligent campus model using IoT technology to achieve intelligent management and service on campus. After reviewing several research studies, the authors suggest an intelligent IoT-based campus model that incorporates campus-oriented application services. The designed smart campus model was modeled based on the idea of the hierarchy of three networks as the perception layer, network layer and application layer. Services are provided to end users through mobile applications and screen monitoring infrastructure according to the proposed model. Before implementing this architecture, the challenges

of the intelligent campus design model were defined. The authors implemented some of the application services using a hardware and software platform. In the end, several experiments tested the feasibility of the proposed model of smart campus validated in the experiment. In this scenario, it was revealed that application services based on smart campus models based on IoT proved to be efficient for students, teachers and campus communities.

(Berouine et al., 2017) analyzes the implementation of a platform for monitoring and processing data in real time. In addition to these aspects, the authors also propose a model for real-time detection, modeling and visualization. A prototype was developed, based on the creation of a cluster composed of five devices, one main configured as a master and the other four as slaves. With a focus on testing the interfacing between different buildings, the assembled architecture for monitoring the quantities is detailed, from sensor nodes, Wi-Fi modules, microcontroller boards and cluster to measure data. The study proposes an architecture for monitoring based on a physical LAN topology. Several graphs were presented, showing the real power consumed as a function of the time variation for each application. As photovoltaic panels were used to supply part of the system, the graphics also illustrate the low energy consumption provided by the energy utilization in the supply of sensor nodes. In the experiment, data were collected in real time over a 24-hour period, with an interval of five seconds for each measurement cycle. Four evaluation metrics were generated: i) The instantaneous daily consumption of electricity for each monitored device, ii) The aggregate daily consumption of electricity used by all devices present in a security guardhouse, iii) The total energy consumption disaggregated from each device, iv) The total consumption of energy aggregated by the entire safety barrier. In the end, the system proved to be efficient when reaching the listed challenges and with satisfactory results in the implemented cluster, showing a report of the control applications with a high degree of energy autonomy.

(Ahmed et al., 2019) aims to design an Internet of Things (IoT) system architecture to manage the charging of electric vehicles on a university campus. The proposed electric vehicle management system consists of electric vehicles, charging stations, local parking controllers and a central university controller. The proposed architecture was designed in three layers: i) a power system layer, ii) a communication network layer and iii) an application layer. The components of the electric vehicle system, data traffic and communication requirements that must be taken into account are defined to implement campus smart park-

ing. The performance analysis and practical feasibility of implementing the IoT-based architecture were investigated for smart parking on the National Chonbuk University Campus in South Korea. The results showed a satisfactory result within the smart campus environment, with great possibility of expansion to other university environments in South Korea.

3 PROPOSED ARCHITECTURE

3.1 System Overview

This work proposes the development of a system for managing Smart Campus applications, aiming to provide support for the deployment and evolution of the wireless networks that offers connectivity to these applications, as well as monitoring the performance of applications and evaluate the feasibility of inserting new devices in the network, based on data collected from the current functioning of the network. In this context, a network architecture that uses different redundancy strategies, based on the IEEE 802.15.4-2015 Standard, is considered, to provide high reliability and availability.

The system proposed in this work is called RAW-Manager (Reliable and Available Wireless, inspired by the RAW Techs Internet Draft (P. Thubert et al., 2020)). In this network architecture the end nodes communicate with the applications that run in the cloud through Gateways and they can transmit the packets using different modulation schemes, using a single transceiver. Gateways are configured with multiple transceivers and are capable of receiving several packets simultaneously, using different modulation configurations. This architecture was initially proposed in (Tuset-Peiró et al., 2020), but in this work, only three physical layer configurations were considered and a single Gateway was used. The system proposed in this work will consider a more generic scenario, in which other physical layer configurations may be used, as well as multiple Gateways. The idea behind this perspective would be to use the best possible configuration obtained by each physical layer modulation variant. For example: in a data transmission using a type of modulation most suitable for when spatial reach is a critical factor. At the same time, we would have the possibility of using redundancy through another modulation configuration more conducive to situations in which the data rate is, in turn, the critical factor. In addition to these aspects, techniques for handling packet duplication and data persistence are considered.

In order to provide communication from the end

nodes to the IoT applications that will consume from the data obtained from the sensors, the CoAP and MQTT protocols will be explored. Each one is responsible for a part of the communication architecture. The first is used for the communication segment that does not have a direct Internet connection. In this section, wireless communication is provided using the IEEE 802.15.4-2015 standard. The second section, from the Gateway to the final IoT applications, is provided through the publisher / subscriber model of the MQTT protocol.

3.2 Architecture Description

One of the specific objectives of this study is to provide the ability to use transmission diversity mechanisms, through the simultaneous use of different modulation schemes, aiming to achieve a high level of availability and reliability. A centralized system is needed to configure the network devices and manage the information collected by different Gateways, which in turn can receive packets through different communication modules.

Fig. 1 illustrates the representation of the communication between the end nodes and the Gateways using the IEEE 802.15.4-2015 standard with different modulation configurations. This architecture was initially proposed in (Tuset-Peiró et al., 2020), in which an WSN with 11 end nodes and a Gateway was implemented, using three different modulation configurations (SUN-FSK, SUN-OQPSK and SUN OFDM), all at 50 kbps. The management system proposed in this paper will consider a more general scenario, with the possibility of having several Gateways and considering the combination of the use of modulation and receiver diversity.

With regard to application layer protocols, it is proposed to segment the network into two distinct groups. One group aims at a lower level approach, which deals with the transmission of data that are not directly visible to the final users. The other group addresses the application layer from the point of view of applications that run in the cloud and offer services to end users, their processes and agents involved.

As a communication protocol between the end nodes and the Gateway (the lowest level part), this proposal takes into account the use of CoAP (Naik, 2017). The focus at this segment is to provide a reliable communication channel between the end nodes, equipped with sensors or actuators, and the centralizing intermediate agent (Gateway). It is intended to implement CoAP within the Gateway, so that the packets would be received from the sensor nodes by the network. (Naik, 2017) At the Gateway, the

packets received from the sensor nodes must be converted to generate new packets in MQTT format, which is the protocol considered for communication between applications that run in the cloud with the sensor/actuator network.

It is worth mentioning that a factor that prevents the use of a single IoT protocol to provide the communication channel in this proposed infrastructure, is due to the fact that the MQTT requires an Internet connection to exchange data. However, the microcontrollers coupled to the sensor nodes considered in the proposed network do not have a network card for direct connection to the Internet. For this reason, the radio modules will communicate through a low-power wireless network and, only from the Gateway onwards, the data will be transmitted through the Internet.

At the end node, the information to be transmitted is organized in the payload of the packet. When the packet is received, in addition to the sensor data, other information must also be collected by the Gateway. It is intended to create a customizable data package from the information collected. This payload will consist of an Array containing several fields of relevant information, such as: RSSI, package identifier and other metrics related to the quality of transmission in the communication links. Regarding the value generated from RSSI, it is intended to use the radio module's own integrated converter, which already makes an automatic conversion transforming an integer value, normally between 0 to 255, to a value in dBm. Once this information reaches the Gateway, such data would be encapsulated in a format understood by the applications, in this scenario, using MQTT.

Fig. 2 illustrates the details of the communication methods used between the end node and the Gateway. Two main CoAP methods are used to exchange information between the sensing network composed of the end nodes and the Gateways.

At a higher level, the applications will communicate with the Gateway through the MQTT protocol, based on the Publisher-Subscriber model. In this communication model, there is a Broker, which once allocated in the cloud allows the creation of entities called "Topics", which allow a particular application interested in that group of data related to a given topic to subscribe to receive any information that is registered in the topic.

3.3 RAW-Manager

Fig. 3 shows the details of the RAW Manager and the communication between the Gateways until the final

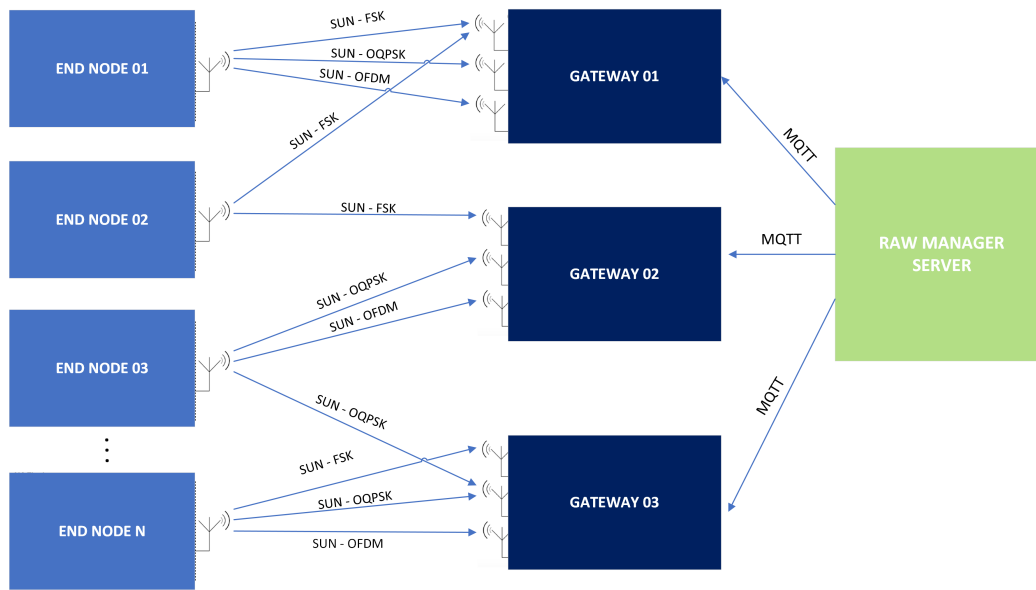


Figure 1: Communication Between End Nodes and Gateway.

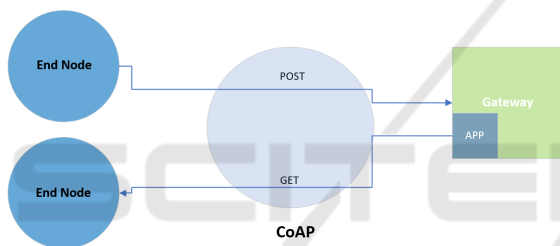


Figure 2: Details of Communication methods between end node and Gateway.

IoT applications. We can describe RAW Manager as a control application that will run inside an application server in the cloud, communicating with Gateways to collect information and also send configuration commands. Still in Figure 3 it is possible to see the representation of the details of functions involved and associated with the RAW Manager. FN1 represents the handling of duplicate packets within the control application, which manages the received packet. FN2 describes the communication between the database and the control application, through the exchange of messages through a structured query language (SQL). In turn, FN3 describes the ability of the final IoT applications to also send control commands or request data through their actuators. FN4 is the representation of the communication channel responsible for accessing the information of the packets that arrive through the network.

Still at the application level, it is intended to implement a functionality responsible for data persistence. Such a tool would read the data via MQTT and store the information obtained in a Time Series

Database (InfluxDB), a tool widely indicated for scenarios in which data storage is required that undergo constant variations as a function of time. It is also worth noting that the same packet can be received by more than one Gateway, if they have compatible modulations and are within reach of a given end node. Thus, before registering a package with the Broker, the RAW Manager is also responsible for handling these duplications. In what concerns the MQTT Broker, three topics are defined in this example: voltage, current and temperature.

Based on the network architecture proposed in (Tuset-Peiró et al., 2020), the Gateways represented in Fig. 4 will consist of a Single Board Computer (SBC) connected to multiple IEEE 802.15.4-2015 radio modules (three in the example), to receive the packets sent using different modulation schemes. Inside the Gateway a Python Script is responsible for the individual reading of each packet received by the radio module and converting it from the raw packet to a MQTT message.

Once the RAW Manager infrastructure is properly functional, several information obtained will be useful to evaluate the performance of the proposed network architecture. Metrics such as: i) packet delivery ratio, may determine the degree of reliability in transmission between different points inherent to the network, ii) the level of signal attenuation may reveal which phenomena or agents will be responsible for the degradation of the signal quality between sources and destination, iii) RSSI, it is possible to quantify the capacity of agents to hear, detect and receive signals between any devices on the network. In addition to

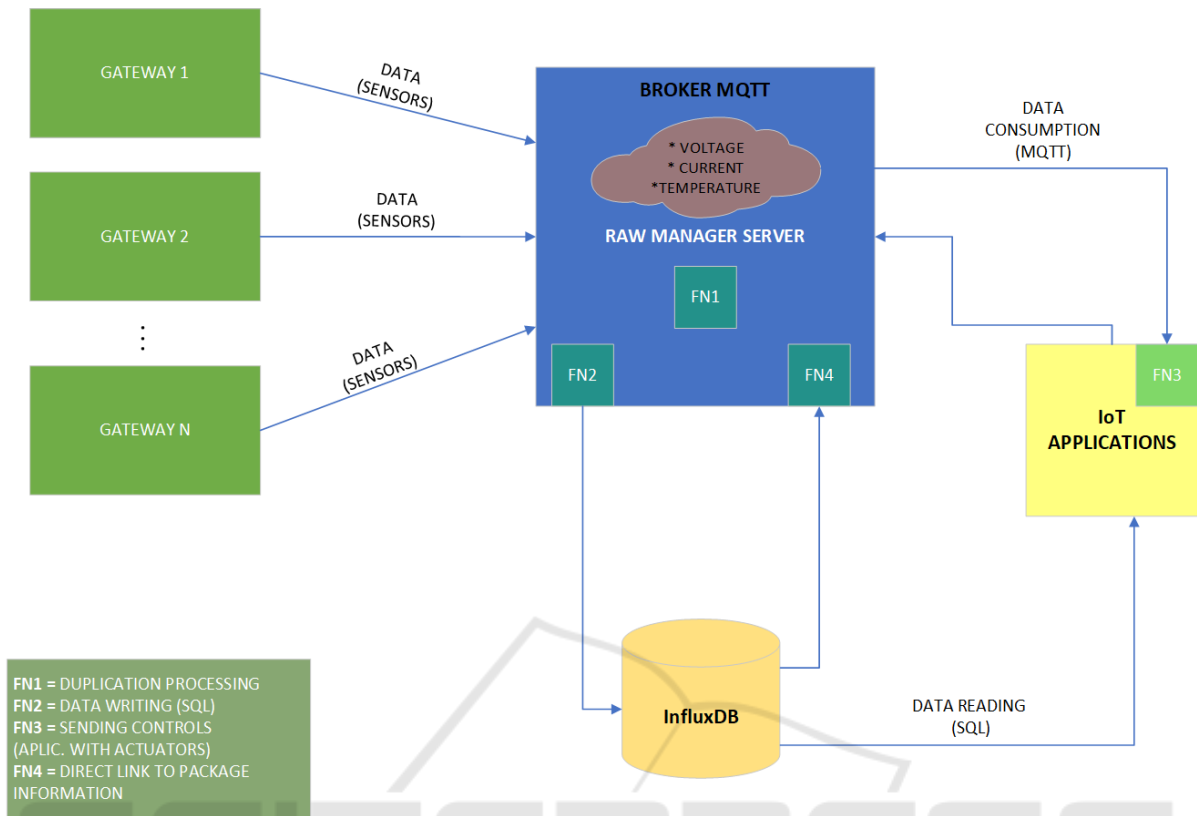


Figure 3: Detailing of RAW Manager with message exchange via MQTT.

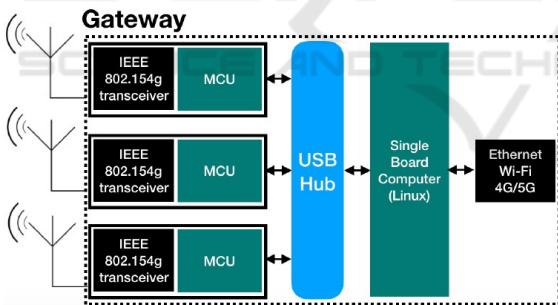


Figure 4: Detail of the Internal Architecture of the Gateways. Based on (Tuset-Peiró et al., 2020).

these listed aspects, the RAW Manager will support the deployment of new devices or the evolution of the network infrastructure, with the possibility of reusing the infrastructure for different applications.

The validation of this architecture will be done through the deployment of a network, aiming at the application of energy consumption monitoring. As the support system is at the heart of this study's proposal, the sensor network's validation strategy consists of a case study, aimed at measuring and monitoring electrical quantities, which aims to mitigate the waste of electrical energy, through sectorial monitoring . Through the implementation of an architecture

based on hardware and software.

After measuring the values, the system also proposes the collection of data from the monitored environment, registration in a database system based on time series and the possibility of remote management on a web platform. In the end, it is expected that the system will allow the monitored environment to identify the points of greatest consumption in the network, enabling the identification of the main points of energy waste, in addition to the construction of a wireless sensor network capable of receiving other sensor devices that can monitor different phenomena relevant to an Intelligent Campus environment. Until then, several communication and remote management experiments have been carried out. To date, the tests have proved to be efficient, exchanging data between devices of totally different computational capacity and between different communication platforms, both in real and simulated environments. It is worth mentioning that the entire system is being programmed locally aiming at the minimum dependence on services provided by others, enabling the system to operate with the maximum autonomy and freedom possible.

4 CONCLUSIONS AND FUTURE WORKS

This paper describes a system for monitoring smart campus applications based on IoT protocols. Throughout this article, the details of the proposed architecture were made, the main objective of which is to support the deployment of new sensors, enabling remote management of control applications by network administrators, in addition to allowing the monitoring of the analyzed applications as a function of time, providing reliability through the use of diversity techniques in the physical and data link layers, based on the IEEE 802.15.4g SUN standard. Communication tests were performed with different protocols using websockets, public test instances of the MQTT protocol and local implementations in order to verify the degree of reliability in communication with different levels of QoS (Quality of Service). Where, so far, the results have been promising.

The next steps to consolidate this work will focus on providing a reliable exchange of messages between devices that operate in different modulation schemes, respecting the predefined critical levels of QoS. As future work it is expected that the proposed architecture can be reused for use with the most diverse types of sensors in order to monitor other areas of interest on the smart campus, such as: vehicle traffic control, parking, intelligent lighting and security.

ACKNOWLEDGEMENTS

The authors would like to thank the partnership between the Federal University of Paraíba and the Federal Institute of Paraíba, the Coordination for the Improvement of Higher Education Personnel (CAPES), and the Brazilian National Council for Scientific and Technological Development (CNPq 421461/2018-7).

REFERENCES

- Ahmed, M. A., Alsayyari, A. S., and Kim, Y.-C. (2019). System architecture based on iot for smart campus parking lots. In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pages 1–5. IEEE.
- Berouine, A., Lachhab, F., Malek, Y. N., Bakhouya, M., and Ouladsine, R. (2017). A smart metering platform using big data and iot technologies. In *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, pages 1–6. IEEE.
- Ejaz, W., Naeem, M., Shahid, A., Anpalagan, A., and Jo, M. (2017). Efficient energy management for the internet of things in smart cities. *IEEE Communications Magazine*, 55(1):84–91.
- Hossain, I., Das, D., and Rashed, M. G. (2019). Internet of things based model for smart campus: Challenges and limitations. In *2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2)*, pages 1–4. IEEE.
- Marfievici, R., Corbalán, P., Rojas, D., McGibney, A., Rea, S., and Pesch, D. (2017). Tales from the c130 horror room: A wireless sensor network story in a data center. In *Proceedings of the first ACM international workshop on the engineering of reliable, robust, and secure embedded wireless sensing systems*, pages 24–31.
- Munoz, J., Chang, T., Vilajosana, X., and Watteyne, T. (2018). Evaluation of ieee802.15.4g for environmental observations. *Sensors*, 18:3468.
- Muñoz, J., Chang, T., Vilajosana, X., and Watteyne, T. (2018). Evaluation of ieee802.15.4g for environmental observations. *Sensors*, 18(10).
- Naik, N. (2017). Choice of effective messaging protocols for iot systems: Mqtt, coap, amqp and http. In *2017 IEEE international systems engineering symposium (ISSE)*, pages 1–7. IEEE.
- P. Thubert, E., Cavalcanti, D., Vilajosana, X., Schmitt, C., and Farkas, J. (2020). Reliable and Available Wireless Technologies. Internet-Draft.
- Tuset-Peiró, P., Gomes, R. D., Thubert, P., Cuerva, E., Egusquiza, E., and Vilajosana, X. (2020). A dataset to evaluate IEEE 802.15.4g SUN for Dependable Low-Power Wireless Communications in Industrial Scenarios. *MDPI Data*, XX(XX).
- Vejlgaard, B., Lauridsen, M., Nguyen, H., Kovács, I. Z., Mogensen, P., and Sorensen, M. (2017). Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot. In *2017 IEEE 85th vehicular technology conference (VTC Spring)*, pages 1–5. IEEE.