

Article

# Smart Campus: An Experimental Performance Comparison of Collaborative and Cooperative Schemes for Wireless Sensor Network

Carolina Del-Valle-Soto <sup>1,†</sup> , Leonardo J. Valdivia <sup>1,\*,†</sup> , Ramiro Velázquez <sup>2</sup> ,  
Luis Rizo-Dominguez <sup>3,†</sup>  and and Juan-Carlos López-Pimentel <sup>1</sup> 

<sup>1</sup> Facultad de Ingeniería, Universidad Panamericana, Álvaro del Portillo 49, Zapopan, Jalisco 45010, Mexico

<sup>2</sup> Facultad de Ingeniería, Universidad Panamericana, Josemaría Escrivá de Balaguer 101, Aguascalientes 20290, Mexico

<sup>3</sup> ITESO, Universidad Jesuita en Guadalajara, San Pedro Tlaquepaque 45604, Mexico

\* Correspondence: lvaldivia@up.edu.mx; Tel.: +52-33-13682200

† These authors contributed equally to this work.

Received: 20 July 2019; Accepted: 11 August 2019; Published: 15 August 2019



**Abstract:** Presently, the Internet of Things (IoT) concept involves a scattered collection of different multipurpose sensor networks that capture information, which is further processed and used in applications such as smart cities. These networks can send large amounts of information in a fairly efficient but insecure wireless environment. Energy consumption is a key aspect of sensor networks since most of the time, they are battery powered and placed in not easily accessible locations. Therefore, and regardless of the final application, wireless sensor networks require a careful energy consumption analysis that allows selection of the best operating protocol and energy optimization scheme. In this paper, a set of performance metrics is defined to objectively compare different kinds of protocols. Four of the most popular IoT protocols are selected: Zigbee, LoRa, Bluetooth, and WiFi. To test and compare their performance, multiple sensors are placed at different points of a university campus to create a network that can accurately simulate a smart city. Finally, the network is analyzed in detail using two different schemes: collaborative and cooperative.

**Keywords:** energy consumption; wireless sensor network; cooperation; collaboration

## 1. Introduction

The Internet of Things (IoT) is based on the connection of multiple devices to the Internet and data sharing between them. Data is first sent to the cloud where it is processed using analytics, and then sent back to other devices. This process depends completely on a centralized architecture. A Wireless Sensor Network (WSN) is considered the most critical element of the IoT model. In the context of IoT, these wireless networks play an essential role in increasing the ubiquity of networks [1] since wireless technology is the fundamental way in which “intelligent objects” communicate with each other and the Internet. In this sense, WSNs allow IoT scalability and provide enough functionality to support its integration with the current Internet architecture. Moreover, it is essential to study the scalability and the adaptation methods of the network in the face of packet transmission failures and topology changes [2].

IoT provides smarter services by the interconnection of various objects. Providing intelligent services requires data to be collected from different places, areas, and devices. Hence, in these kinds of applications, energy consumption is a key factor; sensors can be in remote zones and they can be challenging to access, so it is not possible to replace their batteries continuously. Due to the limitations of battery life, the nodes are designed to save as much energy as possible and most of the time they are

in sleep mode (low power consumption mode). It is thus essential to know the factors that have an impact on battery life [3]. Regarding the wireless medium, aspects that contribute to the deterioration of the information transmission must be taken into account as the channel parameters depend directly on the characteristics of the transmission medium. These characteristics affect the medium and the duration of the useful life of the batteries because there might be connections and disconnections of some nodes in the network. The conditions of the medium also influence the packet retransmission and listen attempts to the channel. This causes the routing protocol to increase its control messages and deteriorate its overhead [4].

WSNs are multi-functional, low-cost, and low-power networks that rely on communications among nodes or from sensor nodes to one or more sink nodes. Sink nodes, sometimes called coordinator nodes or root nodes, may be more robust and have larger processing capacity than other kinds of nodes. Sensor networks can be widely used in various environments even the hostile ones. Some of the many applications of WSNs are in the medical field, agriculture, monitoring, and detection, automation, and data mining. The key element of the IoT is that different devices are connected within the same environment being able to transmit and receive information about their immediate environment and interaction with users. The accuracy of the location allows interactions and data sharing between devices that automate and simplify tasks that generate comfort and facilitate daily work practices. Continuing developing technologies that combine IoT and location will lead to the development of better services for automation and support of daily life tasks.

Adaptive methods for wireless networks have been studied because of the introduction of many technologies for using different technical standards [5]. The concepts of coexistence and cooperation are currently booming in the literature. Both have to do with how the nodes relate to each other and to the network itself. A balanced network seeks to match the load of information traffic and routes, adapting the rules of routing protocol by means of control packages. Coexistence and cooperation offer an idea on how the device puts its functions at the service of the network regardless of the technologies or protocols in use. One of the challenges when analyzing these concepts is interference. There are different metrics that indicate the quality of links in wireless networks.

To analyze the terms that describe the relationship of the devices among them and with the network, it is important to define the degree of intelligence that these nodes possess, a term that is included in technological convergence. When talking about heterogeneous environments, we can mention different network topologies so that the devices exist in an environment that has different characteristics.

- Cooperative networks use self-configuration capabilities to dynamically adapt on demand, since they can respond to the needs of a specific user, within the policies defined by the operator, while optimizing the general resources of network.
- Cognitive networks work on the physical level of the protocol stack, handling emission frequencies and modulation parameters. Cognitive networks exhibit relevant characteristics such as: (1) identification of spectrum access opportunities, (2) selection of frequency bands to be used, (3) coordination among users for access to spectrum, and (4) spectral mobility.

The main disadvantage of cooperative networks lies in the shared management and interdependence of networks that are in an environment with common conditions. Cognitive networks have an agile cognitive process with which they can determine the current conditions of the network, in order to plan, decide, and act. The network can learn from these adaptations to make future decisions taking into account the final objectives: to develop communication protocols.

### *Motivation*

The motivation of this work is to evaluate the performance of different wireless technologies, such as: Zigbee, LoRa, Bluetooth Low Energy, and WiFi. These technologies have been widely spread in industrial applications due to their low cost and low power consumption. The comparative relations

of performance parameters intrinsic to different routing protocols are established to achieve the interconnection of networks of sensing devices with communication Long Range Wide-area network (LoRaWAN, sub-1 GHz) and BLE, in order to emulate an intelligent campus. Each network will have its own sniffer for the acquisition and analysis of the packets sent between the nodes, connectivity between BLE and LoRa devices through a gateway with the possibility of sending data to the cloud.

## 2. Related Work

The current revolution towards a universal connection between things, named IoT, is considered part of the Internet of the future. The long-term plan is to have approximately 28 billion connected devices by 2021 [6].

IoT is currently considered to be one of the most outstanding areas of future technology. In the following subsections we explain about the global applications in this area from smart houses, smart campuses, and smart cities; then we explain some research work focused on identifying the main challenges dealing with IoT. We conclude the section detailing previous works that have performed comparative studies between wireless protocols.

### 2.1. IoT Applications

A typical IoT application is a smart house where the refrigerator can report the current status of the food; the temperature of each room sets according to the preferences of the people occupying such space; and all devices working on identifying possible catastrophes such as a gas leak.

Another application is a smart campus which can use the new generation of information technology such as IoT, cloud computing, and big data to perceive, store, manage, and analyze all the key information of campus system; all of these can serve, for example, to save energy and assisting the staff such as faculty, students and administrative in decision making [7].

The evolution of IoT, starting from smart house, through smart campus and joining with other technologies such as big data, data analysis, among others, have paved the way to smart cities. This concept brings a bigger picture from the houses into a whole city where public transportation, energy, water supply, and environmental factors are at stake.

For example, there is a large number of different devices designed for IoT, but also modern smartphones can work since they include multiple sensors, communication standards, and can store data. The authors in [8], have looked at a different perspective by using smartphones to create the next generation of civil infrastructure monitoring systems. However, Esposte et al. [9], have identified that there are not enough tools to design the cities of the future. Therefore, they created InterSCity, which is a smart city platform that focuses on collaborative development of services, applications, and systems. Unfortunately, it is complex and requires a lot of time and a large budget to do enough testing to actually identify opportunities.

Consequently, researchers are now focusing on working on smart campuses, which is a bridgework between smart homes and cities.

A campus is large enough to provide challenges related to device positioning and at the same time it allows a safe environment to collect data from the parking lot, the usage of rooms, the amount of water and electrical energy during the day and monitor other aspects as well.

Thus, the authors in [10] used an agent-based computing paradigm to gather data from their smart university campus where they could test communication issues and solve them as a decentralized system.

Another example is [7] where key data is stored and analyzed to provide useful information to teachers, students, and staff. Monitoring a classroom to identify how much time is used and by how many people, can help take better decisions on how to assign classrooms to different groups in such a way that it is optimized.

Lghoul et al. [11] have mainly focused on profiling energy usage in campus buildings, setting power distribution system architecture, and pinpointing key micro-grid components. They propose

a general Microgrid (MG) testbed and simulate the operation of proposed MG model/architecture. They delineate relevant pros and cons towards a futuristic real-world/physical MG deployment in a university campus.

IoT is gaining a special moment and the application in smart campuses (respectively smart cities) requires essential technologies for the deployment of successful products and services as described by Lee and Kyoochun [12]. Such essential technologies are:

- (a) Radio frequency identification (RFID);
- (b) Middleware;
- (c) IoT software application;
- (d) Cloud computing; and
- (e) Wireless sensor networks (WSN).

In the following subsections we put our attention in WSN.

### 2.2. Energy and Power Consumption

There are challenges to solve in IoT, for instance, the amount of energy that each accessory requires and the coexistence of thousands of wireless devices that may use different technologies for communicating [13]. In particular, coexistence is a severe threat to IoT, since the devices that are trying to communicate may collide with each other resulting in data lost, rendering the sensors useless. While there is substantial work on coexistence for Bluetooth, WiFi, and IEEE 802.15.14 standards [14], the forecast includes thousands of devices in a narrow range. This also considers the application of IoT to manufacturing and much more, which is called Industrial Internet of Things (IIoT), and it is based on the possibility of creating large-scale deployments. Consequently, some approaches include using a modified Medium Access Control (MAC) protocol. Nevertheless, there are multiple limitations as described by [15].

Another challenge of IoT is power consumption, in this sense, Mahmoud and Mohamad [16], have presented a study of wireless technologies for IoT applications. Their study was focused on the importance of using low-power wireless techniques by introducing a comparative between different low-power wireless communication techniques such as ZigBee, Low-Power WiFi, 6LowPAN, and LPWA.

### 2.3. Signal Interference and Collision

Interference and collisions are also important challenges in IoT. An approach sensing the spectrum to identify interference in IIoT devices is [17], but in practical use it takes a large amount of time to identify the issue and provide a solution. A more recent method [18] uses support vector machines that can sense under 300 ms and classifies external interference. In other words, a management system is required to minimize the amount of collisions and increase the effectiveness, such as [19] that uses a self-learning system based on reinforcement learning. Adeyemi et al. presented in [20] a robust data exploration study performed on daily Internet data traffic generated in a smart university campus for 12 consecutive months.

### 2.4. Comparison between Wireless Protocols

The comparison of different wireless technologies to decide which one is the best, has been very attractive for a sector of researchers. For example, the authors in [21], provide a comparative study of Bluetooth, Ultra-wideband (UWB), ZigBee, and WiFi wireless communication standards. They presented an overview evaluating the main features and behaviors of the standards in terms of various metrics: transmission time, data coding efficiency, complexity, and power consumption. The work did not draw any conclusion regarding which one is better because the authors concluded that more factors must be considered such as network reliability, roaming capability, recovery mechanism, chipset price, and installation cost.

Other work focused on finding a solution to the problem related to the selection criteria of a better wireless communication technology face up to the constraints imposed by the intended application and the evaluation of its key features is that of Chakkor Saad et al. [22]. They presented a comparative performance analysis of the following wireless protocols: WiFi, WiMax, UWB, Bluetooth, ZigBee, ZigBeeIP, and GSM/GPRS. They developed a quantitative evaluation with respect to transmission time, the data coding efficiency, the bite error rate, and the power and energy consumption. Their conclusion is that in order to determine which one is the most suitable, other factors must be taken into account such as network reliability, the link capacity between several networks with different protocols, security, the chipset price, the conformity with the application and the cost of installation.

More recently, Naidu and Kumar [23] have carried out a description on the wireless technologies importance, features, and a comparison about Bluetooth, ZigBee, WiFi, and Z-Wave; mainly focused on Self-organizing/Optimization Networks (SONs). The work of these authors was focused on home automation devices, integrating them with a smart hub. The authors describe WiFi SON, they concluded that it is a guaranteed network, offering quality of service and eliminating human interventions.

One of the characteristics of this type of WSN/IoT networks is the sleeping techniques that can be applied to optimize the energy consumption of the sensors. These types of techniques help to reduce the power of each part of the node, a task that consists essentially of turning off or bringing the device to a low-power mode when it is not used, while when in use, it is activated or awake. By reducing the consumption of each part of the node, the overall consumption is reduced and, therefore, the battery life is extended. In this work, sleep techniques are not properly applied; however, these mechanisms can resemble the connections and disconnections of the nodes that we analyze as a performance metric. Similarly, it must be taken into account that when a node falls asleep it is not necessarily disconnected from the network, but in some cases, depending on the applications, the nodes can temporarily turn off their microcontroller unit and thus, optimize their energy to the maximum and the power of the network. A recent approach to reduce the energy consumption in WSNs is through the setting of sleep scheduling. In addition, a relevant proposal is minimizing the number of nodes to cover a constrained area. Good results in terms of complexity, working-node ratio, scalability, and the time of network duration were obtained in [24].

Unlike the previously mentioned works, our research is concentrated in offering a comparison under a collaborative and cooperative scheme between the following wireless technologies: Zigbee, LoRa, Bluetooth Low Energy, and WiFi. These technologies have gained wide acceptance in industrial applications due to their low cost and low power consumption. Our experimental scenery is a campus, since we are looking for emulating a smart campus.

### 3. Wireless Communication Networks

We define a wireless communication network (WCN) as the association of wireless elements (WE) to share information with a specific task. The nature of WE defines the association schemes and the network features. A WE can be defined as an electronic artifact that possess sensing, acting, signal processing, and/or communication abilities to perform a specific work [25].

Technology integration in WE allows exploitation of different platforms for establishing WCNs. The network features are defined by the nature, status (Active/No Active), capacities, and relationship of WE considering their physical and technological limitations such as size, power transmission, energy consumption, computing capacity, frequency of operation, sensibility of interference, etc.

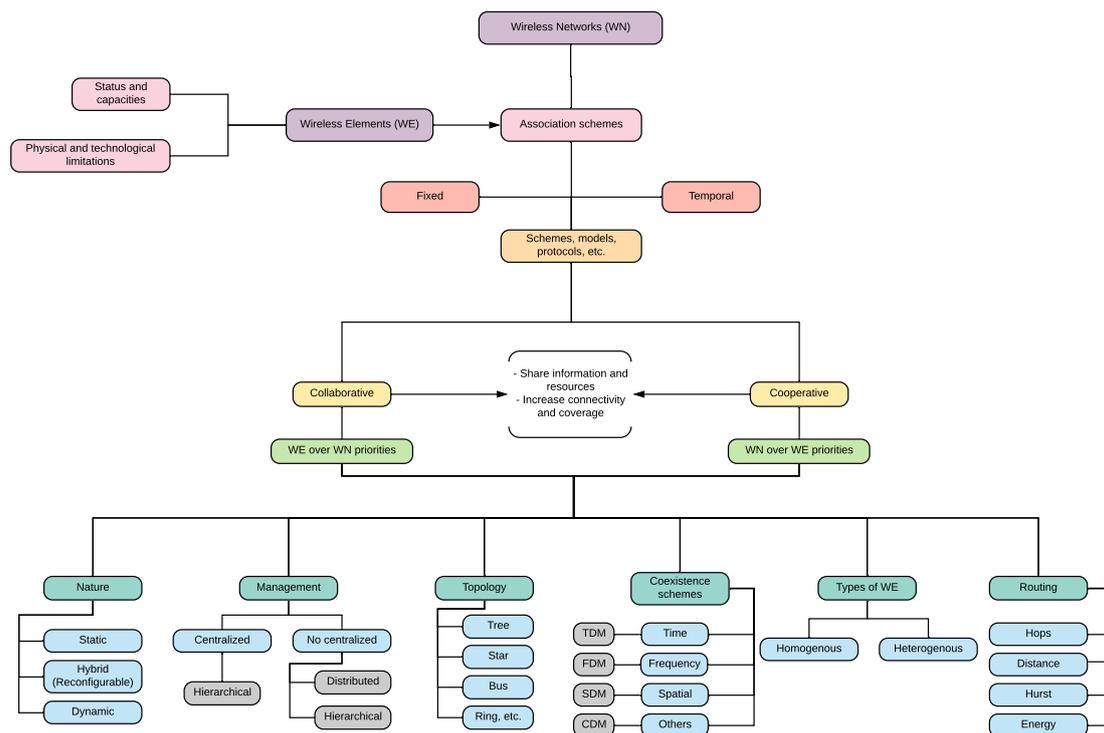
The networks are based on schemes, models, and protocols that establish the technology, transmission agreements, architecture, and management. This way, we can describe the association schemes according their functions. Two classes of schemes can be distinguished.

- *Collaborative scheme.* It consists of sharing resources and functions only if the WE has availability and does not jeopardize its operation, i.e., WE priorities are over Wireless Network (WN) priorities.

There are no strong commitments among their elements [26].

- *Cooperative scheme.* Its scheme is defined to share assigned resources and perform specific functions for all the elements in the networks. All the tasks must be performed through strict rules or protocols, i.e., WN priorities are over WE priorities. In this case there are strong commitments among their members [27].

WN can be classified as a WCN considering different aspects such as nature, management strategy, topology, coexistence scheme, and type of WE. Figure 1 shows a chart with basic concepts and aspects about WCN.



**Figure 1.** Concepts and aspects of Wireless Communication Networks.

The design of a WCN is motivated or influenced by some of the following requirements: Redundancy of information: the high density of devices makes the data obtained in one of them redundant with respect to other nodes of its environment. Limitation of resources: design and implementation of wireless networks must take into account resource limitations: energy, power, memory, and bandwidth. In addition to being generally limited in size, the devices will depend on their batteries and the power they can extract from the environment for their operation. Topology and dynamic environments. The conditions in which a sensor network is deployed is not fixed, but there may be node movement and even Disappearance or addition of others. Wireless networks must be able to reconfigure themselves autonomously. Unreliable transmission medium: The use of wireless communications has a considerably higher error rate than the wired communications. Security and privacy: these factors are especially important in military and surveillance applications. Therefore, denial of service, intrusion, or data manipulation attacks on these applications must be foreseen.

Networking is the mechanism to construct networks, where each node obtains information about their neighbors and the rules of communication that define the schemes, strategies, and protocols used to establish communication model among their members. Thus, we can describe, in wide sense, the networking process in following phases:

- *Observation.* Nodes must explore the channel conditions with the purpose of perceiving the existence of other nodes and noise. For this reason, each node must continuously sense the channel.
- *Recognition and identification.* Nodes can recognize information signals from the channel noise, as well as being a process that allows identification of the neighbors and the rest of members of networks.
- *Association scheme.* At this phase, the agreements about the guidelines and rules define the relationship of each node with the rest of nodes.
- *Transmission agreements.* Transmission power, modulation format, and frequency of operation are some examples of parameters agreed in this phase.
- *Topology and routing.* The interconnection network defines the topology, i.e., the available communication links among nodes establishing the architecture, while routing defines the paths that follow the information to reach its destination.
- *Management scheme.* There are schemes that ensure the operation, access to channel, and control of transmission parameters.

Presently, dynamic and intermittent behavior of WE represent relevant challenges for networking, so the new requirements of WCN such as flexibility in architecture, mobility, and high traffic play a very important role for modern networks. Reconfigurable ability is considered a prominent network paradigm for future WCN [28]. Besides, high density of WE also represents additional challenges due to closeness of WE and the phenomena that it involves, e.g., multiuser channel access problem, multiuser, and multiple access interferences.

Reconfigurable wireless networks (RWN) are dynamic networks suitable for the frequent changes in topology, connectivity, routing, WE status, and wireless channel conditions. These networks have the ability of modifying their configuration, with or without infrastructure, that establish the allocation decisions; self-organization networks imply an *intelligence* process, which can have centralized or no centralized management, that make them attractive to networks as sensors and ad-hoc.

The access to resources and multiple transmissions in WCN face important challenges such as:

- *Coexistence.* It consists of the study of the presence of WE in a given area, the communication among WE, and their influence in the wireless communication channel. Coexistence schemes ensure the communication of multiple WE through the management and distribution of resources.
- *Energy efficiency.* It refers to the efficient use of energy by WE. Strategies seeking to extend the lifespan of battery due to the limited source of energy. Thus, there are strategies based on efficient routing, schedule, low processing systems, and topology and traffic control which reduce the energy consumption from different aspects.
- *Interference.* The received signals from wireless channel can be distorted due to the presence of interference which can be caused by natural or transmission factors. Hence, techniques for mitigation, avoidance, cancelation, and management interference play an important role.
- *Reception algorithms.* It refers to strategies used to extract the information from the channel. The study of algorithms based on reception and detection strategies are proposed which can be classified according to the techniques and methodologies used [29].
- *Security.* Protocols and strategies that provide privacy and authentication of information to avoid vulnerabilities due to malicious eavesdropping.
- *Complexity.* It refers to the difficulty of resolving computational problems through efficient algorithms.

Communication systems used for RWN use orthogonal or semi-orthogonal multiple access channel techniques to avoid multiple users channel problems. They consider temporal, spectral, and spatial dimensions to separate users. However, their implementation requires to control the access to resources using elaborated schemes and protocols to ensure the communication.

These devices have limited resources such as low power, computing capacity, narrow bandwidth transmission, so on, high sensibility to interference, and autonomous behavior. New trends incorporate a communication system that allows the formation of temporal wireless reconfigurable networks (WRN), i.e., sensors and ad hoc networks, that share information by establishing communication links through technologies and schemes that ensure their operation in free bands or unlicensed, e.g., BLE, ZigBee, and WiFi in the bands 2.4 and 5 GHz.

The high density of WDs leads the multiuser channel problem, which occurs when multiple users share spectrum resources. The multiuser channel is divided in two types, the first is the broadcast channel where a single WD transmits signals to many WD receivers e.g., the relationship between the base station (BS) and user equipment (UEs) in cellular networks. Secondary, the multiple access channel uses schemes that distribute the resources and permit the transmission among many transmitters with one receiver [30,31].

The access to the multiuser channel employs schemes to allocate users with conditions to communicate. The schemes based on random allocation is known as random multiple access (RMA) scheme that is widely used e.g., in satellite networks and large wireless networks without signaling overheads [32]. On the other hand, the schemes based on multiple access allocation assign dedicate channels to users using orthogonal or semi-orthogonal division of resources [31,33]. This way, some techniques based on multiple access schemes have been proposed to provide uniformly the resources considering the temporal, frequency and spatial parameters or combinations to separate users [34,35].

The presence of multiple WDs in a given area is widely studied because it can change the transmission considerations in the wireless channel. Multiple access schemes are useful techniques that require previous agreements. This way, the schemes can be described in temporal, spectral, spatial or combinations.

- *Temporal*. This scheme establishes transmission periods which can be used orderly or opportunistically. For example, time division multiplexing (TDM) techniques are orderly schemes due to the fact that time is divided in intervals with the same length that are assigned to each active user. Cognitive Radio technologies is an opportunistically scheme due to the fact that the channel is used by secondary users only when it is possible without disturbing the primary user transmission.
- *Spectral*. This scheme consists of assigning sub-bands to each communication link. They can be assigned one-per-user or flock-per-user during a communication session, i.e., single-carrier (SC) or multi-carrier (MC) basis systems. Frequency division multiplexing (FDM) and multi-carrier technologies are some examples of this kind of scheme.
- *Spacial*. This scheme consists of spatially separating the resources considering their coverage area forming clusters, cells, or sectors coverage to allow their reuse. These schemes are widely used in satellite communications and wireless mobile telephony systems.

### 3.1. Energy Efficiency

The efficient use of energy is a very important challenge in WCNs due to the limited source (battery). For this reason, energy considerations have been focused on maximizing the lifetime of the batteries of the WDs that form the WCN. According to [36], the energy efficiency protocols proposed can be classified into four strategies considering the battery outage, the time to unavailability of applications functionality and the time of the first network partitioning. This way, the strategies to energy efficiency are classified as:

1. Energy efficiency routing that reduces energy consumption for each end-to-end transmission.
2. Scheduling the WDs status to save energy and ensure the network and application functionalities.
3. Topology control by turning node transmission power to find the optimum transmission power with the minimum energy consumption that ensures the connectivity.
4. Strategies that reduce the volume of information transferred.

### 3.2. Interference

The received signals from wireless channel can be distorted due to the presence of interference, which are caused by natural or transmission factors. Hence, techniques for mitigation, avoidance, cancelation, and management of interference play an important role. The interference caused by multiple transmissions are of interest as example.

- Multiple access interference (MAI) occurs when multiple communications links access to channel.
- Multipath interference (MPI) is produced by different propagation paths to reach a specific receiver.
- Multiuser interference (MUI) occurs when simultaneous communication links exist in the same channel from different WDs. Two particular cases can be identified: *Exposed* and *Hidden* terminals.

### 3.3. Synchronization

It is the process where the WDs define the alignment of transmission parameters, which allows the establishment of communication links, i.e., to define the information necessary to ensure the hookup and linkup among WDs. This process plays an important role given that it has impact in both physical and higher levels.

### 3.4. Security

The dynamic and flexibility of RWN represent a challenge for implementation of security schemes due to frequent changes in the network status, e.g., sporadic connectivity, variable number of active WDs, temporal topology, etc. In addition, it is desirable to provide authentication and privacy requirements to avoid vulnerabilities due to malicious eavesdropping devices. Commonly, the schemes require associative mechanisms, security protocols which can be proactive or reactive and involve cross layer functions or coding signals [37,38].

### 3.5. Complexity

It refers to the difficulty to resolve computational problems analyzing the algorithms implemented in the WDs and the use of resources as memory, storage, energy, time, etc., [39]. The challenge in complexity is to implement efficient algorithms for wireless systems that permit to reduce the power consumption and the size of devices while decreasing its manufacturing cost. However, the simplicity must ensure the *quality of service* (QoS) and privacy.

## 4. Performance Metrics Study

Metrics of the network layer are fundamental because they show the performance and usefulness of a routing protocol. Each routing protocol is designed for specific applications and certain scenarios. These metrics indicate how the bandwidth use is affected by the overhead of the routing protocol in use. In addition, the availability of effective routes and the ability of the network for self-configuration show the capacity of the protocol to recover from topology changes [40]. Recovery times have an impact on the latency in the network, and even though the networks conform with different technologies, it is highly essential to understand and evaluate the performance metrics as shown in [41]. This analysis allows network customization to improve its different aspects and provide better communication.

Therefore, using these metrics the proactive and reactive protocols can be compared. To perform such comparison a simulated and a real scenario were implemented. The next section describes the simulation.

Figure 2 describes performance metrics in a general way. The measurement and control of these performance parameters provide the network optimization because some parameters influence others, allowing the information in a wireless network to be delivered reliably.

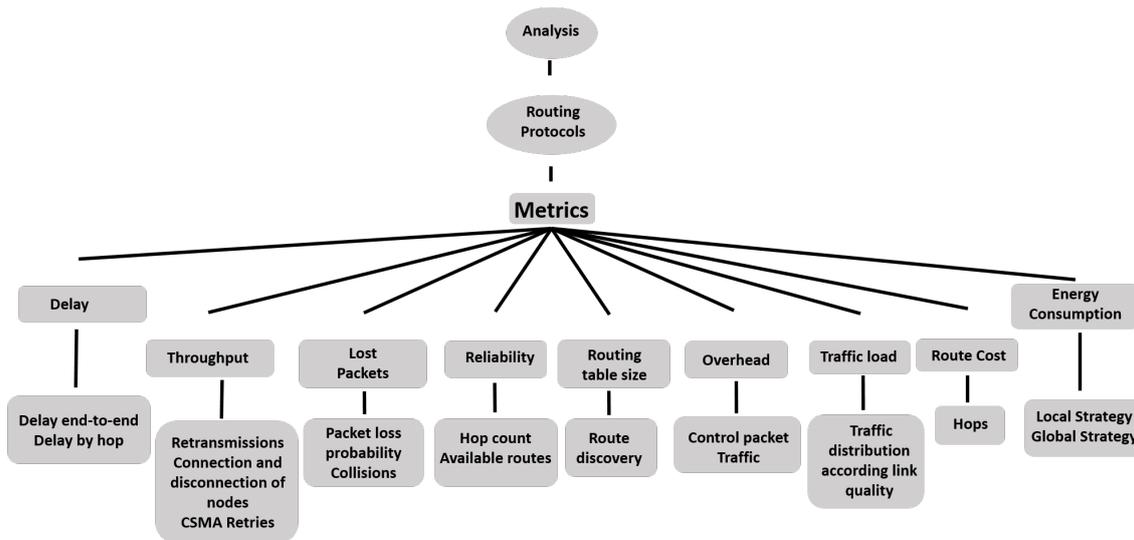


Figure 2. General performance metrics.

Sensor networks usually have similarities, so it is necessary to know some comparison criteria that allow us to decide which of them is the most suitable to implement and thus, solve our problems. The most important and useful metrics for comparing sensor networks are the following:

- *Response time*: The speed at which the data packets are sent among the different nodes.
- *Network lifetime*: The durability and resistance of the devices and, in general, of the network, must be considered if a budget is allocated or limited or both.
- *Security*: Security is vital in any field, but, in wireless networks, it is complicated to secure information. However, it is relevant to assess the risks or vulnerabilities that the network may experience.
- *Types of data that can be transmitted*: Wireless technologies such as WiFi or ZigBee, do not transmit the same types of data. It is important to select and analyze the data that it is desired to send to choose the most appropriate one. Packets that carry the information in the network are traffic packets, while the control packets are those used by the routing protocol to establish the network rules. These control packages constitute the overhead of the network, so if a network has a high overhead, there will be a higher probability of collisions.
- *Battery life*: One of the main issues in sensor networks is the energy required by the components of the masses. The life of the batteries is expected to be extended by using the application of a sleep technique to the nodes of the system.
- *Packet retransmission*: In WSNs a sensor node may need to transmit a packet multiple times to ensure delivery. This may be due to packets which have been either damaged or lost and needs to be resending or just for forwarding packets to other nodes. The indiscriminate use of packet retransmission has a negative impact on battery life.
- *Resilience*: It is the network ability to face faults or changes in its normal operation maintaining an acceptable level of service.
- *Complexity and cost*: The complexity represented by the installation of the sensor network is considered one of the most important criteria. From this, the cost can be derived, this being an agent of great relief in any project.
- *Listening to the channel retries*: According to each data link layer algorithm, the nodes listen to the channel before transmitting to know if there are collisions. After a specific number of attempts, the packet is dropped. If the number of listening tries is high, it means that the channel has high interference.

- *Packet loss*: It occurs when information packets do not arrive in the expected way. Some of the causes can be damaged hardware. Hardware capacity (bottlenecks): when some component of the network cannot assume a certain amount of traffic, thus encouraging data flow. Congestion in the network: when a device is at 100% capacity, generating a queue waiting to be discarded after a particular time if it is a long time, the difference with bottlenecks is that it can be a general problem and not just a device. Bugs in the software of network devices: When the software of the devices has errors. Other: interference or “noise” in the wireless network, proximity to other wireless devices, distance, physical elements (walls), etc. Then, the packet loss leads to the following problems: Information out of date (delay in the information received), slow loading, interruption of loads, closure of connections, incomplete information.

## 5. Energy

A wireless sensor network is a set of devices distributed in such a way that the sensors implemented in such network are capable of transmitting the parameters to which they are exposed, for example, temperature, pressure, humidity, etc.; in this way, a network of sensors is composed of the following elements:

- Sensors
- Radio transmitter/receiver
- CPU/memory
- Power source, usually a battery.

Regarding the energy problem, there are some aspects that directly affect node battery consumption. The term unbalanced energy depletion, shown in [42], describes a situation where the nodes that are closer to the coordinator node carry more traffic, and so they consume more energy than those nodes further away from the root node. This imbalance causes the overall energy to be distributed non-uniformly in the network, making some nodes to run out of power faster than others [43].

## 6. Model

There is a gateway with LoRa technology and WiFi which is the general hub of all the nodes. This gateway receives data from all devices and sends the information to a platform called the things network. The devices that are held as nodes are divided into three technologies: BLE, LoRa, and ZigBee. The LoRa modules make the direct transmission to the gateway, each LoRa node contains its own ID allowing the things network to distinguish which device is making the transmission. The BLE modules work as beacons, this allows any BLE module that is running like a beacon scanner to receive data, but in order to read the information it is necessary to decrypt the packets, this scanner contains a LoRa transmitter, this way it is possible to communicate with the main gateway and send all the information of the BLE modules. Zigbee nodes work in the same way, there is a mesh topology in which everyone communicates with each other, but there is a coordinator who creates the network, this coordinator has a LoRa module that allows communication with the gateway.

The developed network consists of four parts:

- *Zigbee Nodes*: A set of high-level wireless communication protocols, based on the IEEE 802.15.4 standard, i.e., communicating using the 2.4 Ghz frequency. It consists of five devices, a device is configured as coordinator, the main function of this device is to create the network in mesh topology, in this way the other four devices can be connected to the network and have communication between them, allowing an additional device withdrawn from the coordinator because the information packet passes through the other devices to the coordinator. Each of the devices contains a temperature sensor, allowing measurement of the ambient temperature in different locations within the university. The coordinator sends a signal to know which devices

are connected to the network and these send their temperatures every 5 min. After obtaining all data, the coordinator sends the information through another protocol called LoRa to the gateway.

- LoRa nodes: It is a specification for low power and wide-area networks, LPWAN, designed specifically for low power consumption devices, operating in local, regional, national, or global networks. In Mexico, LoRa uses the 915 MHz frequency. The topology of LoRa is point-to-point, there is a gateway or hub and one or more nodes, the gateway oversees reading all the packets that are on that frequency. The nodes are devices that transmit small information frames to avoid a high consumption of energy. The created network consists of five different devices:
  1. Garbage sensor: This device contains a sensor called Time of Flight, which measures distance by means of infrared. The main function of this device is to measure the amount of garbage that is in a boat, in this way you can anticipate that the boat will be full, and the garbage will fall. The device makes a constant monitoring every 3 min and goes back to sleep to lower its consumption. Those monitors take a measurement of the sensor and send the value of that measurement to the gateway, after sending it back to sleep.
  2. Light Sensor: This device also using the Time of Flight sensor knows the amount of environmental light, so it is possible to know if it is day or night, if a door is open among other applications. The functionality of this device is very similar to that of garbage with the variation of the data sent to the gateway.
  3. Accelerometer sensor: The node contains an accelerometer sensor, which function is to mediate accelerations in  $x$ ,  $y$ ,  $z$ . This way, it is possible to know if there was displacement or some change of state of an object. This node takes a measurement every 5 min to know if there was any change in its location, if so, it sends a message to the gateway notifying with the values in  $x$ ,  $y$ ,  $z$  to know what its displacement was.
  4. Gyroscope Sensor: It is a mechanical device used to measure, maintain, or change the orientation in the space of an appliance or vehicle. It is essentially composed of a body with rotational symmetry that rotates around the axis of such symmetry. It informs if there was any movement on the device's own axis. The node takes a measurement every 5 min if there is no change in the sensor and sends a value. If a change occurs before the measurement is taken, the device wakes up to carry out a transmission.
  5. Environmental sensor: This node presents humidity and temperature sensors allowing knowledge of the temperature and humidity in a certain space. This node takes a sensor measurement every hour due to the little change that occurs in that period of time.
  6. Gateway: it is the device that acts as a connection interface between devices and allows sharing resources between two or more computers. The gateway used contains the LoRa and WiFi protocols. This gateway obtains all the transmitted data through the LoRa protocol, these data are then transmitted through WiFi allowing them to be found on the ThethingsNetwork platform. In this platform it is possible to display the data separately from each node. Knowing when it made its last transmission, the frequency of transmission of each device and its measurements. This device obtains all the data transmitted by the ZigBee coordinator, all the data transmitted by the LoRa nodes and the data transmitted by the BLE concentrator.
- BLE Nodes: It is an industrial specification for Wireless Personal Area Networks (WPAN), which operates on the frequency of 2.4 Ghz as well as ZigBee. There are four BLE nodes that work as beacons, it is a low-consumption device that emits a broadcast signal, i.e., they are devices that are constantly sending data. In this case they have a light sensor and they are constantly sending the value of light. In addition, there is a fifth device which works as beacon scanner, the function of this device is to receive all the data of the other nodes, decode them and send them through LoRa using another module that contains that protocol.

In Figure 3, a representative scheme of the sensors according to the wireless technology and their respective application is presented. Coordinating nodes are observed that will serve as a bridge between three of the studied technologies: WiFi, ZigBee, and Bluetooth Low Energy (BLE).

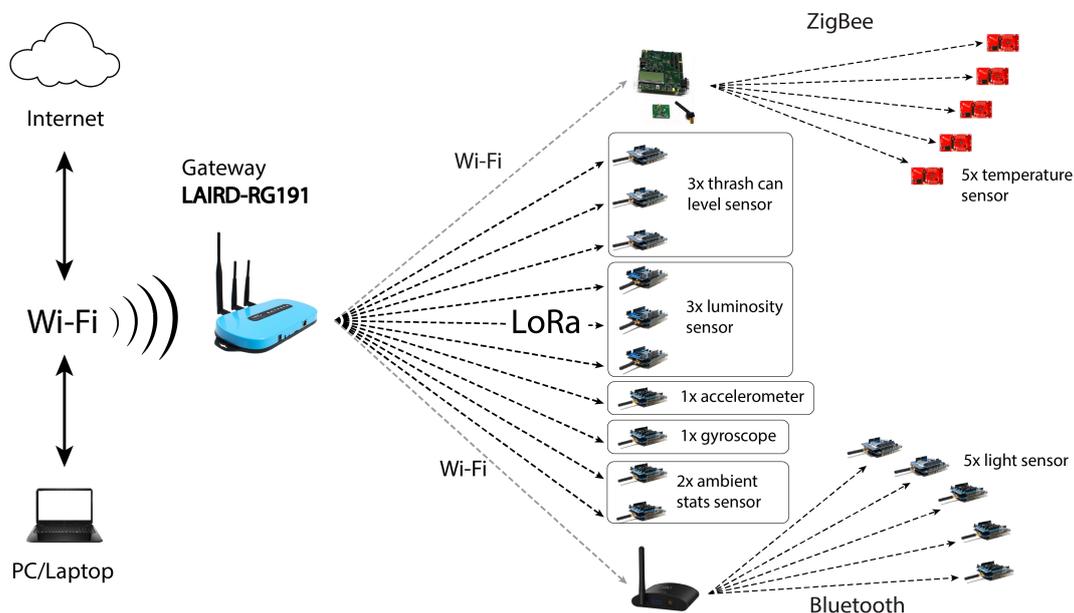


Figure 3. Network sensors under each technology.

In Figure 4, a satellite map of the university campus of the Universidad Panamericana in Guadalajara, Mexico is shown. We have an outline of the approximate positions of the main sensors, so that it serves as a basis for taking measurements. This map is useful to get an idea of the green areas, buildings, or constructions, pedestrian and vehicular routes and the approximate total area where the sensors are located.

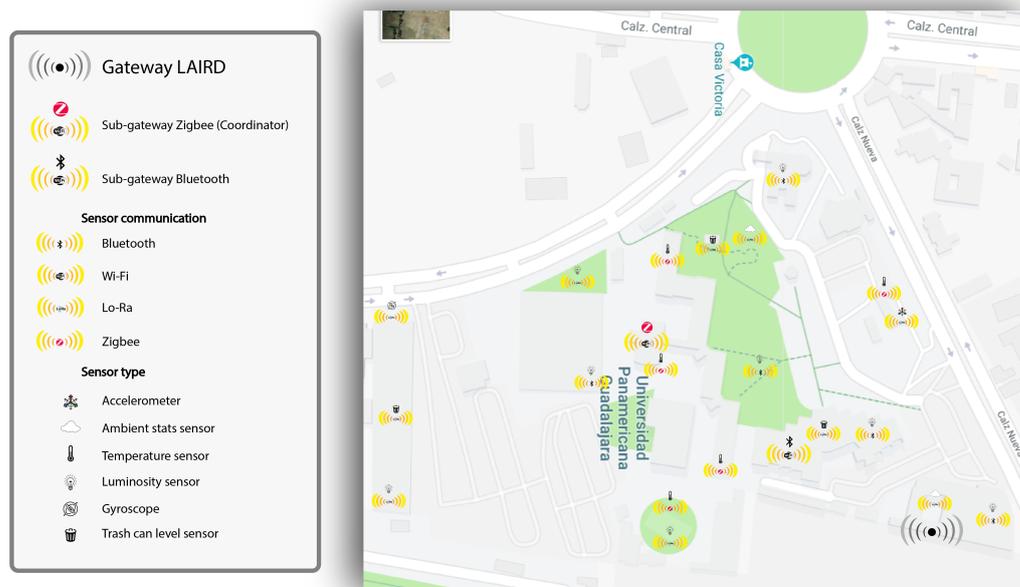


Figure 4. Network sensors position along the university campus.

The coexistence between Bluetooth and BLE in the same device is ensured by the common MAC layer. This layer also performs channel quality measurements (such as Received Signal Strength Indication (RSSI), Quality of service, and packet loss rate for Bluetooth) to update the channel map with “good” channels and eliminate those channels marked as “bad”.

### Scenario

Analyzing altogether the four technologies studied, we can say that BLE is used for short-range wireless connectivity with a transmission rate lower than that achieved by WiFi. BLE is characterized by transmitting small amounts of information at low frequency and allows creation of mesh networks with low energy consumption. This advantage of mesh networks takes advantage of some devices as repeaters. With respect to WiFi, there is currently an extensive infrastructure already installed that transfers data and can handle large amounts of data to provide broadband connectivity. In this technology, there is a greater loss of information, although there is greater sensitivity. In the network of the common networks of a business or academic environment, the network is saturated because there are usually many connected devices. It is an adequate standard for file transfer, but it consumes too much energy to develop IoT applications. WiFi is optimized to have many nodes connected to the same access point without causing too much packet saturation. ZigBee is a wireless technology focused on domestic and industrial applications and has significant advantages such as low consumption in complex systems, superior security, robustness, high scalability, and capacity to support many nodes. Zigbee works in the same frequency band as BLE with low data rate. One of the great advantages of ZigBee is that it presents a mechanism for a node to know when to transmit depending on the communication channel. This reduces collisions when there are multiple devices simultaneously. LoRaWAN is designed to implement wide-area networks (WANs) with specific characteristics to support mobile, bidirectional, economic, and secure communications for IoT, Machine to Machine (M2M), smart cities, and industrial applications.

The considered network is composed of a sink node and a set of homogeneous sensor nodes, which are randomly scattered in the interested area. Figure 5 is an example of one of the sensor installations on the front of a tree in a building near the entrance to the university campus. The nodes have a plastic protection box and are of easy installation.



**Figure 5.** Sensor in a tree in the center of a building near to the entrance of the university campus.

Figure 6 shows an example of the frames captured in the *thethingsnetwork* web application ([www.thethingsnetwork.org](http://www.thethingsnetwork.org)). In this interface, through the console tab, we can see the applications that we have activated and properly configured. In each of them, an Application ID is configured to differentiate the device and a description of it. In the Data tab the configuration of the packets

transmitted and received by the sensor can be found. Within the characteristics of the packets, there are the reception and transmission times, the packet count ID to know which packet is lost and the sensor data to observe the changes depending on the application. If we detail the Uplink or Downlink tabs, we find the data presented in Figure 7. Here the components of the Fields and the Metadata are described. In the Fields, we have important information about the variables that we are analyzing, such as the sensor’s battery. In the Metadata, we find parameters of physical layer performance, MAC layer, and network layer, such as frequencies, modulations, interference and other parameters also related to the gateway for each technology.

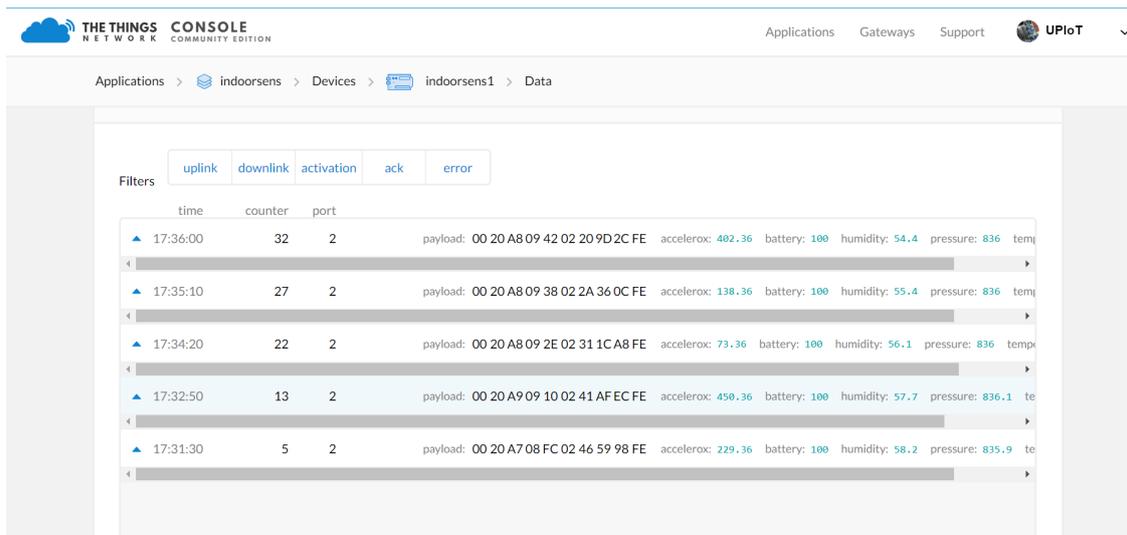


Figure 6. Data for network packets.

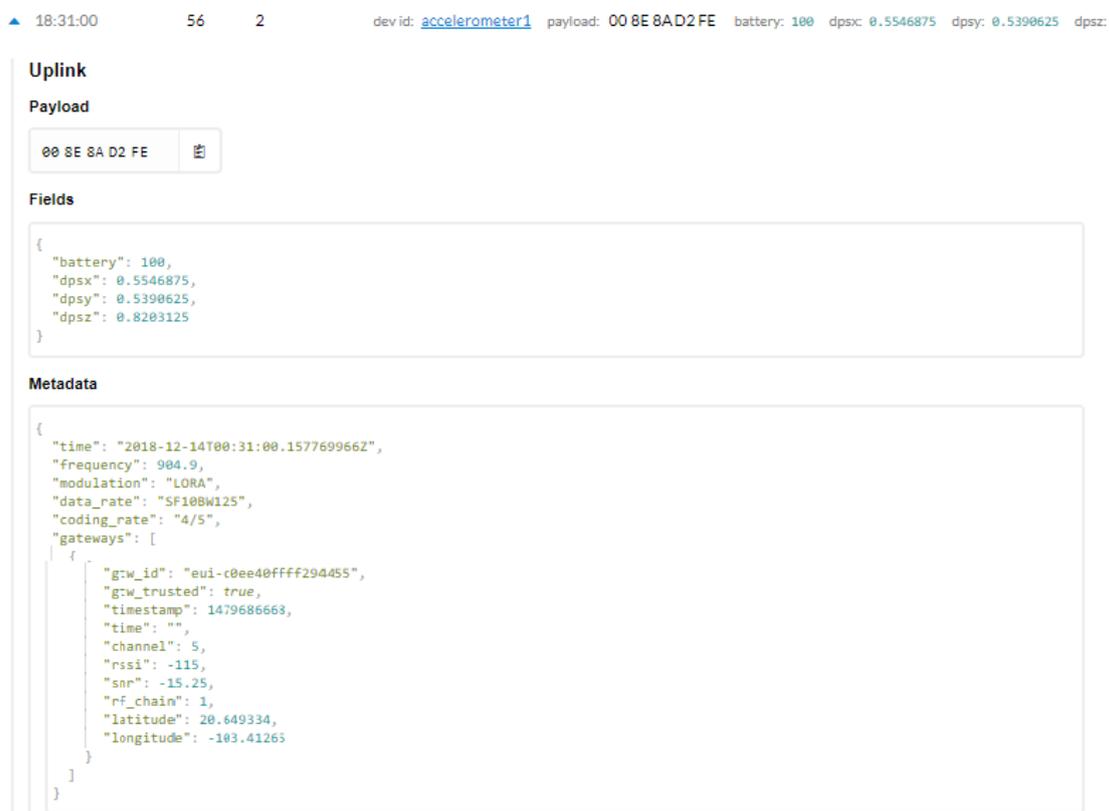


Figure 7. Frame of metadata for network packets.

## 7. Results

In the network we have implemented, the most severe aspects to be analyzed under coexistence are presented among the BLE, WiFi, Lora, and ZigBee devices, because LoRa can be configured for other frequencies. ZigBee allows the dynamic selection of channels, a scanning function goes through a list of compatible channels in search of beacon, receiver energy detection, indication of link quality. A feature called frequency agility is specified in the ZigBee standard to improve the robustness of ZigBee networks. According to this function, if an interference is detected in the current channel, a ZigBee network can move to a clear channel depending on some mechanisms. The ZigBee operation in the 2.4 GHz band is favored by the choice of the 16 available channels. The frequency agility feature facilitates the use of these additional channels. When a network is integrated for the first time, the node looks for a channel with the least noise or traffic. If additional overtime traffic appears or if there is noise, the host application looks for a better channel and moves the entire network to the new channel, allowing the network to adapt to changes in Radio Frequency RF environments. Table 1 shows the specifications of the studied wireless technologies.

**Table 1.** Specifications of the studied wireless technologies.

Technology	Standard	Frequency	Range	Typical Transfer Ratio
ZigBee	IEEE 802.15.4	2.4 GHz	10–100 m	250 kbps
LoRaWAN	LoRaWAN	433 MHz, 868 MHz and 915 MHz	2–15 km	0.3–50 kbps
WiFi	802.11n	2.4 GHz and 5 GHz	50 m	150–200 Mbps
BLE	IEEE 802.15.1	2.4 GHz (ISM)	50–150 m (Smart/LE)	1 Mbps (Smart/LE)

Tables 2 and 3 show the results of the different protocols under the cooperative and collaborative schemes. The metrics used together with the results should be analyzed together as they affect each other. When a node connects to the network the route discovery stage starts, in the case of ZigBee the gateway must assign an ID to the connected node. On the other hand, some protocols send control messages so that other nodes respond them, and in this way, the new node creates its neighbor tables and depending of the configuration also creates its routing tables. Hence, the more percentage of disconnected nodes the discovery process will occur more times.

**Table 2.** Nodes under the cooperative scheme.

Metric SD (%)	Zigbee	SD (%)	LoRaWAN	SD (%)	WiFi	SD (%)	BLE	SD (%)
Transmission rate (Kbps)	250	NA	27	NA	165,000	NA	25,000	NA
Delay end-to-end (s)	2.52	1.12	3.44	1.13	2.87	1.08	3.09	1.23
Retransmissions	1.67	1.02	2.33	1.13	2.40	1.2	1.93	1.15
Channel retries	1.93	1.12	2.60	1.21	3.11	1.04	2.44	1.22
Disconnection nodes (%)	1.00	1.03	2.30	1.18	3.00	1.21	1.20	1.09
Packet loss (%)	6.00	1.01	4.00	1.06	6.0	1.10	5.00	1.02
Available routes (%)	70	1.12	80	1.13	75	1.18	90	1.02
Overhead (%)	30	1.14	35	1.08	40	1.13	30	1.21
Resilience (s)	3.00	1.24	2.50	1.12	3.00	1.26	2.20	1.22
Energy consumption (J)	2.96	1.29	3.50	1.21	5.00	1.02	4.50	1.20

**Table 3.** Nodes under the collaborative scheme.

Metric	Zigbee	SD (%)	LoRaWAN	SD (%)	WiFi	SD (%)	BLE	SD (%)
Transmission rate (Kbps)	250	NA	27	NA	165,000	NA	25,000	NA
Delay end-to-end (s)	2.81	1.14	3.92	1.13	3.04	1.14	3.50	1.15
Retransmissions	1.82	1.14	2.63	1.24	2.55	1.14	2.21	1.14
Channel retries	2.04	1.10	2.84	1.20	3.33	1.11	2.61	1.06
Disconnection nodes (%)	0.89	1.09	2.15	1.22	2.83	1.22	1.06	1.23
Packet loss (%)	9.00	1.13	12.0	1.08	10.0	1.19	11.00	1.20
Available routes (%)	65	1.11	74	1.21	65	1.22	83	1.14
Overhead (%)	33	1.04	40	1.08	45	1.10	38	1.20
Resilience (s)	3.20	1.20	2.80	1.11	3.50	1.21	2.90	1.22
Energy consumption (J)	3.05	1.17	3.80	1.14	5.10	1.18	4.70	1.19

Moreover, when a node tries to connect to the network, control messages are sent, therefore, the higher the percentage of disconnection of nodes, the greater the overhead. In the same way, having a greater number of packets in the network will result in more collisions and as a consequence in a greater number of retransmissions, the channel will be busier and will increase the channel retries. It is important to note that the channel retries occur when a node access the channel to verify if it is free, and if so transmit the packet. Finally, by increasing the disconnected nodes, retransmissions and channel retries the energy consumption will increase.

Otherwise, when a node is disconnected from the network some routes are canceled and new routes are created, when the node reconnects, the network enters a non-stable state, the time it takes to pass from non-stable state to a stable state is known as resilience. Therefore, the lower the resilience, the higher the energy consumption, since the network will take longer to configure and achieve new stable routes. This is directly related to the available routes, when this metric is low, there is a greater possibility of packet loss, which causes a greater number of retransmissions and finally energy consumption increases.

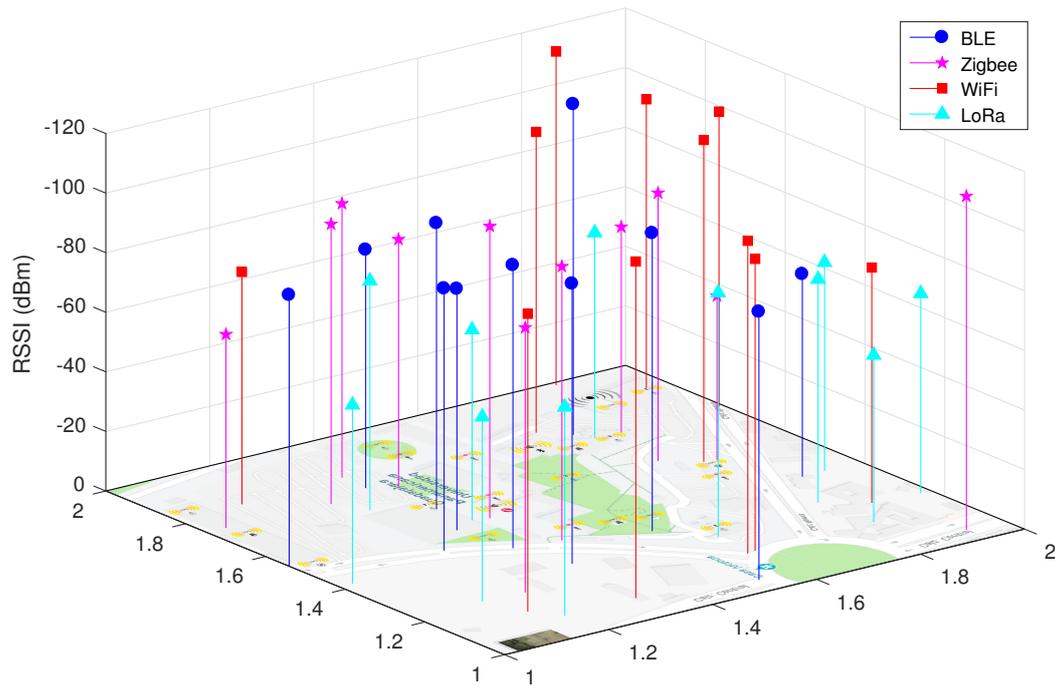
Tables 2 and 3 show results of performance metrics to observe the behavior of the network under the cooperative and collaborative schemes. Samples were taken from the network running for 24 h. The tests are carried out during a weekday so that the number of users and the vehicular flow is that of a normal day with activity on campus. Metrics are an average obtained every hour by all the sensors that work under each technology. The tests are carried out in an area of 300 square meters with indoor and outdoor sensors. No battery change was made for any of the sensors. The maximum number of packet retransmissions is 3, before the packet is discarded. The maximum number of retries to listen to the channel is 5, before the packet is discarded. It is well known that cross traffic affects adversely the network parameters. Thus, the scenarios experimented in this work, in practical terms, the traffic is only related to sensor network and it is expected that variation tends to be small value. A slightly variation is observed during experimentation and it can be observed that is independent of protocol. The data of the metrics studied present a standard deviation between 1 and 1.3% for the four technologies presented in each performance metrics for the cooperative and collaborative schemes. This shows that the measurements taken over 24 h can reflect a similar behavior with a small variation in the morning hours, where the traffic of people and vehicles decreases remarkably.

Specifically, Table 2 describes the results of the main performance metrics for the nodes under the cooperative scheme, i.e., when the technologies studied are in operation in the same geographical area and the priorities of the network are above the priorities of the sensor. The result of the metrics described is an average of the sensors that are under the wireless communication protocol. With respect to the end-to-end delay, ZigBee is the fastest due to its topology and message concentration. Subsequently, WiFi follows the speed of information delivery due to the greater sensitivity of the WiFi antenna and this gives an advantage, in addition to the fact that bandwidth is greater. On the other hand, the protocol with most retransmissions is WiFi, it is important to mention that a high retransmission rate increases delay and energy consumption. Additionally, retransmission as well as control packets contribute to the network overhead, being WiFi the protocol with the highest overhead,

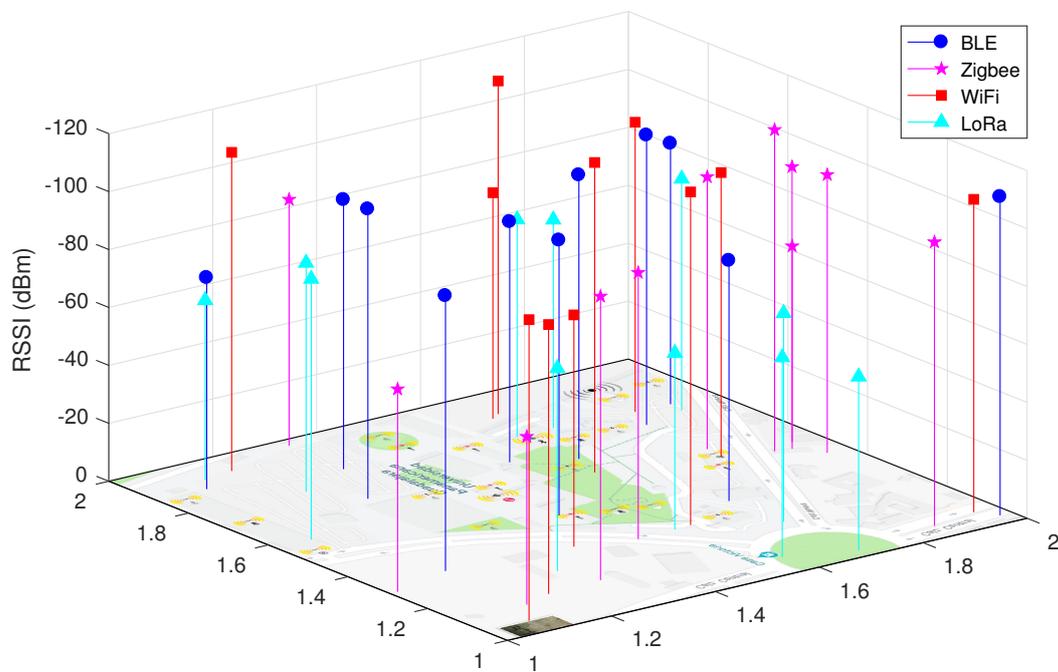
so it has a higher probability of collisions. Another important metric is resilience, in this case BLE and LoRa have the best response times, since after a failure they return to a normal operating state in a shorter time than WiFi and ZigBee.

In the collaborative scheme specified in Table 3, which consists of sharing resources and functions only if the sensor has availability, the sensor priorities are over the network priorities. In comparison with the results of Table 2, the end-to-end delay increases; however, the ZigBee remains the fastest. Following this trend, retransmissions as well as lost packets increase. Because the retransmissions increased in all the protocols, it is expected that the percentage of overhead will also increase, since more packets are sent. Finally, it is important to mention that in critical applications where safety becomes a priority, two characteristics of the network are of high importance: resilience and availability. However, Table 3 shows that the resilience time increased with respect to the configuration of Table 2, therefore in collaborative scheme, it will take more time to achieve a normal operating state after a failure, a key factor in critical systems. On the other hand, the energy consumption directly affects the availability, most of the sensors are battery powered, i.e., the more energy they consume the faster the battery will run out. In this aspect, the collaborative scheme is better, since it consumes less energy, being ZigBee the protocol with the lowest consumption.

These Figures 8 and 9 show random measurements (11 for each wireless technology). These figures are intended to show the intensity of the received signal. In this way, we can see under which scheme we can determine if a signal is sufficient to establish a wireless connection when other technologies and diverse environmental situations are present. Then, each of these measurements helps us to know the strength with which the devices listen or could hear the signal at that specific point. Likewise, we observe that for both schemes, WiFi is the technology with higher RSSI levels (in dBm), which shows that there are areas of very low signal coverage, while the technology that exhibits the best levels (very good coverage) presents is LoRa, possibly because its operating frequency is different and faces fewer collisions. The position of each measurement was performed in a uniformly distributed manner throughout the area of the university campus, where the sensors were located. For the cooperative scheme shown in Figure 8, the average RSSI value in dBm for BLE is  $-90.36$ , for ZigBee it is  $-85.36$ , for WiFi it is  $-99.09$  and for LoRa it is  $-68.36$ . For the collaborative scheme shown in Figure 9, the average RSSI value in dBm for BLE is  $-92.73$ , for ZigBee it is  $-87.91$ , for WiFi it is  $-100.73$  and for LoRa it is  $-71.82$ . We can then state that both schemes differ between 8 and 10% with the cooperative scheme being less interfering. It is important to bear in mind that the best transmission signals are observed in values close to  $-75$  dBm. This makes sense considering that the LoRa technology is the one with the best coverage and, therefore, will present the least number of collisions. The one that presents worse coverage is WiFi and is understandable due to the large number of devices connected to campus networks, it is logical that the characteristics of a campus present a smaller scale than the characteristics of a city. Of the three technologies that are in the same frequency band, ZigBee has better signal coverage (between good and medium coverage). These figures help to better understand Tables 2 and 3 due to the metrics related to the interference of the channel such as: collisions, packets retransmissions, resilience, among others.

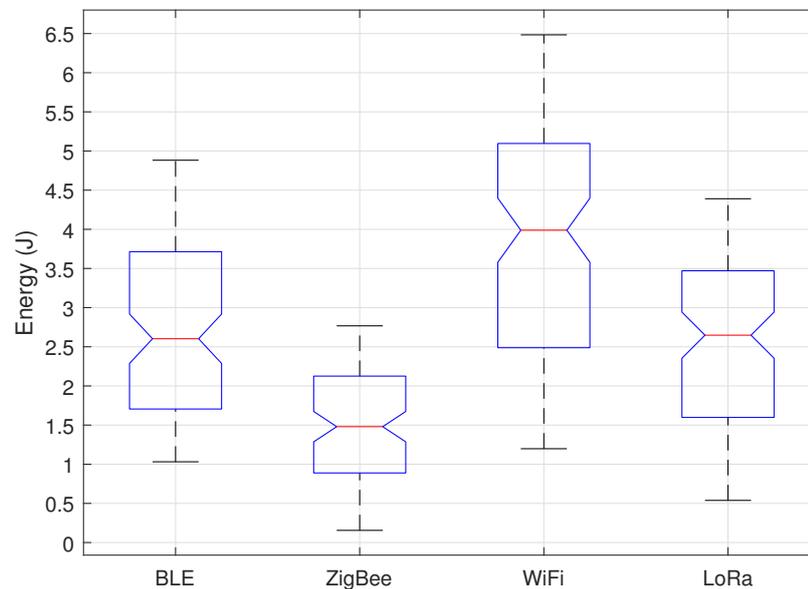


**Figure 8.** Received Signal Strength Indication (RSSI) values in dBm under cooperation scheme for each technology.

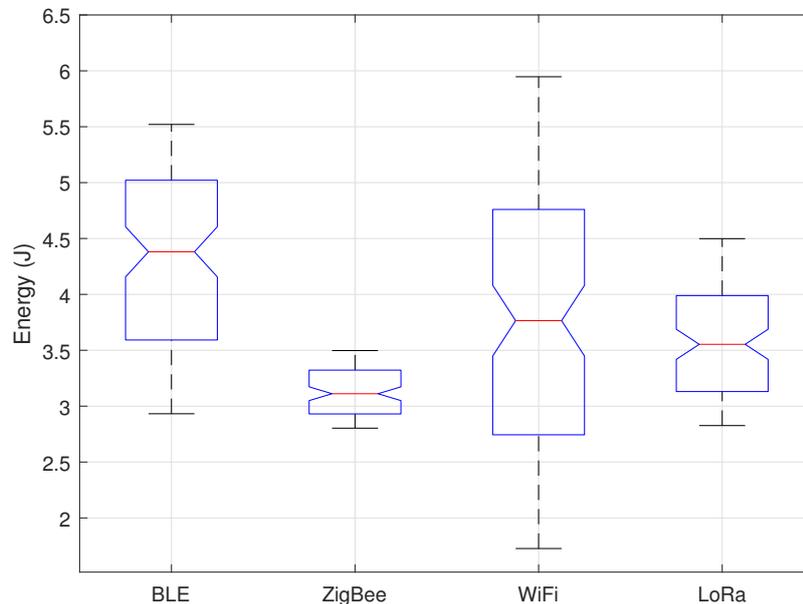


**Figure 9.** RSSI values in dBm under collaboration scheme for each technology.

As mentioned above, one of the key metrics in any sensor network is energy consumption. Figures 10 and 11 show a summary of the energy consumption for each protocol under the cooperative and collaborative schemes.



**Figure 10.** Energy in Joules under cooperation scheme for each technology.



**Figure 11.** Energy in Joules under collaboration scheme for each technology.

Figure 10 shows that under the cooperative scheme the protocol with the lowest energy consumption is ZigBee, where the minimum consumption value is 0.2 Joules, but most of the sensors consume between 0.8 and 2.1 Joules, with the median being 1.5 Joules. ZigBee consumes about half of the LoRa protocol, since the latter has an average value of 2.4 Joules; however, 50% of the sensors consume between 2.4 and 4.3 Joules. On the other hand, BLE and WiFi have very scattered data, reaching to consume values as low as 1.1 Joules up to 6.8 Joules as in the case of WiFi, with the median

value of 3.2 Joules for BLE and 4.8 Joules for WiFi. In this way, it is clear that the protocol with the best consumption is ZigBee, additionally it has less dispersed data so that a more exact battery life calculation can be made, otherwise in WiFi the scattered data would cause different battery life time for each sensor.

By contrast, Figure 11 shows the protocols under the collaborative scheme; however, the results are very similar to those in Figure 10, with the ZigBee protocol having the lowest energy consumption. It is important to mention that in a comparison between schemes, the cooperative has a lower energy consumption in all protocols except for WiFi, in which values are very similar. The biggest difference is the dispersion of the data, for the ZigBee protocol the range in the cooperative scheme is 3.6 Joules and in the collaborative scheme is 0.7 Joules, something similar occurs for both LoRa and BLE. This low dispersion indicates that all the sensors consume practically the same energy (at least in ZigBee), so that the lifetime of their batteries will be very similar, being able to program a more efficient maintenance of the network.

## 8. Conclusions

The main motivation of this work is to contrast low-consumption wireless technologies applied to IoT that are characterized by transmitting small amounts of information in a reliable and flexible way, consume little battery in devices, and have great scalability in the communications system.

Concerning data, we can control the information management of applications in our computers such as photos, videos, mails, etc. But for IoT, it does not work in the same way. It captures information at every moment it considers necessary, instead of capturing it when requested. People usually become subjects for data collecting, instead of users of IoT services, and most cases they are not aware of it. Because it is not easy for people to know when sensors are activated. The privacy stack framework bridge of today's Internet of Things between IoT and user, starts with awareness. It concerns on how IoT services might open communication channels to users and subjects. The IoT protocol work has not gone into privacy data standardization, in other words, the bridge between privacy and public status is minimal. Second, the inference part proposes users to be conscious of the constantly grow of inferences, because data and IoT learning techniques rise their capabilities every day. Inferences helps users to understand what IoT devices learn about them and helps the system to improve privacy with a natural language to understand which are our privacy preferences.

**Author Contributions:** The methodology was proposed by C.D.-V.-S., the investigation and the formal analysis work were done by L.J.V. and C.D.-V.-S., the validation work was done by R.V., the data analysis work was finished by J.-C.L.-P. and L.R.-D., and the original draft was finished by L.J.V., C.D.-V.-S. and R.V.

**Funding:** This research received no external funding.

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

## References

1. Yigitel, M.A.; Incel, O.D.; Ersoy, C. QoS-aware MAC protocols for wireless sensor networks: A survey. *Comput. Netw.* **2011**, *55*, 1982–2004. [[CrossRef](#)]
2. Aswale, P.; Shukla, A.; Bharati, P.; Bharambe, S.; Palve, S. An Overview of Internet of Things: Architecture, Protocols and Challenges. In *Information and Communication Technology for Intelligent Systems*; Springer: Berlin, Germany, 2019; pp. 299–308.
3. Silva, J.D.C.; Rodrigues, J.J.; Al-Muhtadi, J.; Rabêlo, R.A.; Furtado, V. Management Platforms and Protocols for Internet of Things: A Survey. *Sensors* **2019**, *19*, 676. [[CrossRef](#)] [[PubMed](#)]
4. Sikandar, A.; Kumar, S.; Singh, P.; Tyagi, M.K.; Kumar, D. Energy Efficient Transmission in the Presence of Interference for Wireless Sensor Networks. In *International Conference on Application of Computing and Communication Technologies*; Springer: Berlin, Germany, 2018; pp. 55–64.
5. Liang, J. Collaborative Mechanism of Enhanced Coexistence of Collocated Wireless Networks. US Patent 7099671B2, 29 August 2006.

6. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [[CrossRef](#)]
7. Luo, L. Data Acquisition and Analysis of Smart Campus Based on Wireless Sensor. *Wirel. Pers. Commun.* **2018**, *102*, 2897–2911. [[CrossRef](#)]
8. Alavi, A.H.; Buttlar, W.G. An overview of smartphone technology for citizen-centered, real-time and scalable civil infrastructure monitoring. *Future Gener. Comput. Syst.* **2019**, *93*, 651–672. [[CrossRef](#)]
9. Del Esposte, A.D.M.; Santana, E.F.Z.; Kanashiro, L.; Costa, F.M.; Braghetto, K.R.; Lago, N.; Kon, F. Design and evaluation of a scalable smart city software platform with large-scale simulations. *Future Gener. Comput. Syst.* **2019**, *93*, 427–441. [[CrossRef](#)]
10. Fortino, G.; Russo, W.; Savaglio, C.; Shen, W.; Zhou, M. Agent-oriented cooperative smart objects: From IoT system design to implementation. *IEEE Trans. Syst. Man Cybern. Syst.* **2018**, *48*, 1949–1956. [[CrossRef](#)]
11. Lghoul, R.; Abid, M.R.; Khallaayoun, A.; Bourhane, S.; Zine-Dine, K.; Elkamoun, N.; Khaidar, M.; Bakhouya, M.; Benhaddou, D. Towards a real-world university campus micro-grid. In Proceedings of the 2018 International Conference on Smart Energy Systems and Technologies (SEST), Sevilla, Spain, 10–12 September 2018.
12. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Bus. Horiz.* **2015**, *58*, 431–440. [[CrossRef](#)]
13. Dhanda, S.S.; Singh, B.; Jindal, P. Wireless technologies in IoT: Research challenges. In *Engineering Vibration, Communication and Information Processing; Lecture Notes in Electrical Engineering*; Springer: Singapore, 2019; Volume 478, pp. 229–239.
14. Yang, D.; Xu, Y.; Gidlund, M. Wireless coexistence between IEEE 802.11- and IEEE 802.15.4-based networks: A survey. *Int. J. Distrib. Sens. Netw.* **2011**, *7*, 912152. [[CrossRef](#)]
15. Bauwens, J.; Jooris, B.; Giannoulis, S.; Jabandžić, I.; Moerman, I.; De Poorter, E. Portability, compatibility and reuse of MAC protocols across different IoT radio platforms. *Ad Hoc Netw.* **2019**, *86*, 144–153. [[CrossRef](#)]
16. Mahmoud, M.S.; Mohamad, A.A.H. A Study of Efficient Power Consumption Wireless Communication Techniques/Modules for Internet of Things (IoT) Applications. *Adv. Internet Things* **2016**, *6*, 19–29. [[CrossRef](#)]
17. Chiwewe, T.M.; Mbuya, C.F.; Hancke, G.P. Using Cognitive radio for interference-resistant Industrial wireless sensor networks: An overview. *IEEE Trans. Ind. Inform.* **2015**, *11*, 1466–1481. [[CrossRef](#)]
18. Grimaldi, S.; Mahmood, A.; Gidlund, M.; Alves, M. An SVM-based method for classification of external interference in industrial wireless sensor and actuator networks. *J. Sens. Actuator Netw.* **2017**, *6*, 9. [[CrossRef](#)]
19. Soffker, P.; Block, D.; Wiebusch, N.; Meier, U. Resource Allocation for a Wireless Coexistence Management System based on Reinforcement Learning. In Proceedings of the 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Turin, Italy, 4–7 September 2018; pp. 1101–1104.
20. Adeyemi, O.J.; Popoola, S.I.; Atayero, A.A.; Afolayan, D.G.; Ariyo, M.; Adetiba, E. Exploration of daily Internet data traffic generated in a smart university campus. *Data Brief* **2018**, *20*, 30–52. [[CrossRef](#)] [[PubMed](#)]
21. Lee, J.; Su, Y.; Shen, C. A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. In Proceedings of the 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON 2007), Taipei, Taiwan, 5–8 November 2007; pp. 46–51. [[CrossRef](#)]
22. Saad, C.; Mostafa, B.; Cheikh, E.A.; Abderrahmane, H. Comparative Performance Analysis of Wireless Communication Protocols for Intelligent Sensors and Their Applications. *Int. J. Adv. Comput. Sci. Appl.* **2014**, *5*. [[CrossRef](#)]
23. Naidu, G.A.; Kumar, J. Wireless Protocols: Wi-Fi SON, Bluetooth, ZigBee, Z-Wave, and Wi-Fi. In *Innovations in Electronics and Communication Engineering*; Saini, H.S., Singh, R.K., Kumar, G., Rather, G., Santhi, K., Eds.; Springer: Singapore, 2019; pp. 229–239.
24. Mostafaei, H.; Montieri, A.; Persico, V.; Pescapé, A. A sleep scheduling approach based on learning automata for WSN partial coverage. *J. Netw. Comput. Appl.* **2017**, *80*, 67–78. [[CrossRef](#)]
25. Drossos, N.; Mavrommati, I.; Kameas, A. Towards ubiquitous computing applications composed from functionally autonomous hybrid artifacts. In *The Disappearing Computer*; Springer: Berlin, Germany, 2007; pp. 161–181.
26. Ochiai, H.; Mitran, P.; Poor, H.V.; Tarokh, V. Collaborative beamforming for distributed wireless ad hoc sensor networks. *IEEE Trans. Signal Process.* **2005**, *53*, 4110–4124. [[CrossRef](#)]
27. Chen, H.; Zhai, C.; Li, Y.; Vucetic, B. Cooperative strategies for wireless-powered communications: An overview. *IEEE Wirel. Commun.* **2018**, *25*, 112–119. [[CrossRef](#)]

28. El-Mougy, A.; Ibnkahla, M.; Hattab, G.; Ejaz, W. Reconfigurable wireless networks. *Proc. IEEE* **2015**, *103*, 1125–1158. [[CrossRef](#)]
29. Choi, Y.S.; Shirani-Mehr, H. Simultaneous transmission and reception: Algorithm, design and system level performance. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 5992–6010. [[CrossRef](#)]
30. Ping, L.; Liu, L.; Wu, K.; Leung, W.K. Interleave division multiple-access. *IEEE Trans. Wirel. Commun.* **2006**, *5*, 938–947. [[CrossRef](#)]
31. Velazquez-Gutierrez, J.M. Reception of Multiple Users in Reconfigurable Wireless Networks. Ph.D. Thesis, Tecnológico de Monterrey, Monterrey, Mexico, 2018.
32. Hong, J.P.; Choi, W.; Rao, B.D. Sparsity controlled random multiple access with compressed sensing. *IEEE Trans. Wirel. Commun.* **2014**, *14*, 998–1010. [[CrossRef](#)]
33. Fang, F.; Zhang, H.; Cheng, J.; Leung, V.C. Energy-efficient resource allocation for downlink non-orthogonal multiple access network. *IEEE Trans. Commun.* **2016**, *64*, 3722–3732. [[CrossRef](#)]
34. Khedr, M.E.; Zaghoul, M.S.; El-Desouky, M.I. Wireless Adhoc Multi Access Networks Optimization Using OSPF Routing Protocol Based On Cisco Devices. *Int. J. Comput. Netw. Commun.* **2015**, *7*, 59. [[CrossRef](#)]
35. Wang, D.; Gao, X.; You, X.; Han, B. Channel Estimation Algorithms for Broadband MIMO-OFDM Systems. *Acta Electron. Sin.* **2005**, *33*, 1254.
36. Mahfoudh, S.; Minet, P. Survey of energy efficient strategies in wireless ad hoc and sensor networks. In Proceedings of the Seventh International Conference on Networking (icn 2008), Cancun, Mexico, 13–18 April 2008; pp. 1–7.
37. Raya, M.; Hubaux, J.P. Securing vehicular ad hoc networks. *J. Comput. Secur.* **2007**, *15*, 39–68. [[CrossRef](#)]
38. Xiao, Y.; Chen, H.; Yang, S.; Lin, Y.B.; Du, D.Z. *Wireless Network Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2009.
39. Du, D.Z.; Ko, K.I. *Theory of Computational Complexity*; John Wiley & Sons: Hoboken, NJ, USA, 2011; Volume 58.
40. Alazzawi, L.; Elkateeb, A.; others. Performance evaluation of the WSN routing protocols scalability. *J. Comput. Syst. Netw. Commun.* **2009**, *2008*, 481046.
41. Fauzia, S.; Fatima, K. Performance evaluation of AODV routing protocol for free space optical mobile Ad-Hoc networks. In *The International Symposium on Intelligent Systems Technologies and Applications; Advances in Intelligent Systems and Computing*; Springer: Cham, Switzerland, 2018; Volume 683, pp. 74–83.
42. Babayo, A.A.; Anisi, M.H.; Ali, I. A Review on energy management schemes in energy harvesting wireless sensor networks. *Renew. Sustain. Energy Rev.* **2017**, *76*, 1176–1184. [[CrossRef](#)]
43. Tuah, N.; Ismail, M.; Haron, A.R. Energy consumption and lifetime analysis for heterogeneous Wireless Sensor Network. In Proceedings of the 2013 IEEE TENCON Spring Conference, Sydney, Australia, 17–19 April 2013; pp. 188–193.



© 2019 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/>).