Congr. Int. en Ing. Electrónica. Mem. ELECTRO, Vol. 42 pp. 1-6 , Oct 2020, Chihuahua, Chih. México
http://electro.itchihuahua.edu.mx/memorias_electro/MemoriaElectro2018.zip
ISSN 1405-2172

A BLUETOOTH TESTBED FOR INTERNET OF THINGS

Mercado-Velázquez Andrés Aharhel[1], Escamilla-Ambrosio Ponciano Jorge[1], Rodríguez-Mota Abraham[1],
Ortiz-Rodríguez Floriberto[2]

[1] Centro de Investigación en Computación, Instituto Politécnico Nacional,
Av. Juan de Dios Bátiz, Esq. Miguel Othón de Mendizábal, Col. Nueva Industrial Vallejo, Alcaldía Gustavo
A. Madero, C.P. 07738, Ciudad de México, México.
andres@mevel.com.mx; pescamilla@cic.ipn.mx; arodrigm@cic.ipn.mx

[2] Escuela Superior de Ingeniería Mecánica y Eléctrica, Instituto Politécnico Nacional,
Unidad Profesional Adolfo López Mateos, Zacatenco, Av. Luis Enrique Erro S/N, Alcaldía Gustavo A.
Madero, C.P. 07738, Ciudad de México, México.
flortiz@ipn.mx

ABSTRACT.

The enormous number of Internet of Things applications demands to investigate the functionality of these systems. Hence, testing under real environments is of paramount importance to analyze the functionality of these systems. Taking this into consideration, the implementation of Internet of Things applications requires the integration of diverse testbeds, as Internet of Things solutions need to be thoroughly tested and fine-tuned before being offered to the market. In this work, a Bluetooth testbed for Internet of Things is presented. This testbed consists of a series of nodes that communicate to a gateway using the Bluetooth 4.1 BLE wireless communication protocol. This testbed will help to measure variables of interest to characterize the system's behavior. The importance of integrating this testbed, where different variables are analyzed in a real environment, is first to obtain data, and second to obtain their statistics to assess the performance of a network based on this technology under different conditions.

Keywords: Testbed, Internet of Things, Bluetooth, Smart Home.

RESUMEN.

El enorme número de aplicaciones que existen del Internet de las cosas exige investigar la funcionalidad de estos sistemas. Por lo tanto, realizar pruebas en entornos reales es de suma importancia para analizar la funcionalidad de estos sistemas. Teniendo esto en cuenta, la implementación de las aplicaciones del Internet de las cosas requiere la integración de diversas mesas de pruebas, ya que las soluciones del Internet de las cosas deben ser probadas y ajustadas minuciosamente antes de ser ofrecidas al mercado. En este trabajo, se presenta una mesa de pruebas para el Internet de las cosas que hace uso de la tecnología Bluetooth. Esta mesa de pruebas consiste en una serie de nodos que se comunican a un nodo principal en la red utilizando el protocolo de comunicación inalámbrica Bluetooth 4.1 BLE. Esta mesa de pruebas ayudará a medir variables de interés con el objetivo de caracterizar el comportamiento del sistema. La importancia de integrar una mesa de pruebas, donde se analizan diferentes variables en un entorno real, es primeramente obtener datos para luego obtener sus estadísticas y evaluar el rendimiento de una red basada en esta tecnología bajo diferentes condiciones.

Palabras Clave: Mesa de pruebas, Internet de las cosas, Bluetooth, Casa inteligente.

1. INTRODUCTION

The Internet of Things (IoT, also known as Internet of Everything) is referred as the interconnection of everyday objects to Internet [1]. IoT is increasing the presence of the Internet in all areas of human life, resulting in a network of devices that communicate with other devices and generate data that is useful to humans.

With the rapid advancement of technology, the IoT is opening enormous opportunities for a large number of new applications that promise to improve the quality of our lives. In recent years, the IoT has received a lot of attention from researchers and practitioners around the world.

Thanks to the large number of IoT applications, the functionality of IoT networks must be studied before applying these systems to real-life environments. To overcome this critical hurdle the testbeds can support experimentation of IoT technologies and solutions, support the research and development of services and applications. In order to conduct an analysis of the capabilities of Bluetooth 4.1 technology in real application environments and thus determine whether it is the most suitable solution for different applications of the Internet of Things, the capabilities of this technology must be measured. These capabilities can be measured through testbeds implemented considering different real-life scenarios.

The objective of this work is to measure the effectiveness rate of messages received as a function of distance and average nodes current consumption of a Bluetooth 4.1 testbed for IoT under real environments.

The measurements performed in this paper aim to obtain information on two important properties of Bluetooth devices. The first one is the maximum distance (in meters) that each of the devices reaches in relation to the percentage of bytes received in a message sent between two network nodes. The second property analyzed is the energy consumption of the nodes that make up the battery powered IoT network, thus determining the average battery run-time in relation to its mAh capacity.

Some experiments performed with a Bluetooth testbed for IoT are presented in this paper. In addition, some general observations are given as well as some real-world tests.

The importance of creating testbeds where different variables are analyzed in a real environment is to obtain data which characterizes the behavior of a real network based on these technologies.

The proposed work aims to evaluate IoT solutions in realistic smart environments, by developing a functional IoT network that can be scaled to include different scenarios, diverse wireless technologies, and communications protocols.

Initially, this testbed is built to explore one research avenue in Internet of Things Cyber Security: Lightweight Moving Target Defence Strategies for IoT Cyber Security. This research is developed at the Cyber Security Laboratory, Centro de Investigación en Computación, Instituto Politécnico Nacional (CIC-IPN). However, the usefulness of this testbed is not limited for this research work, because the objective of this testbed is to be a scientific multi-user tool.

This works complements the previous work where a LoRa testbed was developed [5].

1.1. Bluetooth Low Energy.

Bluetooth Low Energy (BLE) is a low-power, short-range wireless technology that was first specified by Bluetooth Special Interest Group (SIG) as part of Bluetooth 4.0 in 2010 [6]. Since then, BLE has become a basic technology of IoT. In fact, BLE is suitable for typical resource-constrained devices in IoT (for example, small battery-powered sensors and actuators). However, compared to other IoT technologies, BLE is also widespread in consumer electronics devices such as smartphones. This feature of BLE facilitates the interaction between users and surrounding BLE devices, because smartphones can naturally become user interfaces and/or gateways in IoT scenarios [7].

For simplicity, BLE was originally designed to enable only star topology networks. However, this feature would limit the applicability of BLE in critical IoT application domains where star topology networks cannot ensure coverage of all expected areas. For example, many related wireless technologies in the field of smart homes (such as ZigBee, Z-Wave, and Thread) all support mesh topologies. In addition, the mesh topology provides path diversity, which provides inherent robustness, which allows us to better cope with the damage of radio propagation, interference, and equipment failure [7].

Since the release of version 4.0, several revisions of the Bluetooth specification have been released, including enhancements in data rate, payload, power consumption, and security. Table 1 summarizes the main differences between these versions. Bluetooth 4.0 explicitly prohibits peripheral devices and other central devices from simultaneously participating in multiple connections (or taking on multiple roles). Version 4.1 and higher have fundamentally changed the role that each device can play when there are multiple connections. In other words, regardless of its link layer role, the device can run multiple link layer instances simultaneously without restriction [8].

Table 1. Comparison of Bluetooth versions [8].

Version	4.0	4.1	4.2	5.0 and 5.1
Multi-roles	No	Yes		
PDU payload	Up to 31 bytes		Up to 255 bytes	
LE secure	No		Yes	
IoT support	Limited		Medium	High
Advertising channels	3 Channels			3 Primary Ch. 37 Secondary Ch
Data rate	1 Mbps			2 Mbps
Effective range	50 m (Line of Sight) 10 m (Indoor)			200 m (Line of Sight) 40 m (Indoor)
Battery life	Shorter			Longer

2. RELATED AND PREVIOUS WORK

Recently, a rapid increase in research has been observed in the different configurations and implementation of Bluetooth BLE testbeds in real application scenarios, as summarized in [2] where a research avenue in the area of Multi-vehicle Cooperative Driving is explored in the University of Gävle. Another testbed application is presented in [3], this research aims to obtain reliable drone-to-drone and drone-to-ground communications using Bluetooth technology. In [4] a design and implementation of a portable Smart Wireless Pedestrian Crossing Control System is presented; this work uses a Bluetooth testbed to validate in a real environment the developed system.

This work is a new branch of the LoRa testbed developed at CIC-IPN [5]. The objective of that work was to identify the kind of IoT applications for which LoRa technology is the most appropriate solution and to understand the capabilities of this technology in a real environment.

The previous research work focused on determining two important parameters of the LoRa communication protocol in two different scenarios. The first parameter was obtained from the implementation of the testbed for tracking vehicles in the Zacatenco IPN campus, this was the percentage of effectiveness of the messages received according to the distance. The second parameter obtained was the average power consumption of the network as a function of the number of nodes in the network and according to the type of activity that the network nodes perform (data sending, data reception, sleep mode), this parameter was measured in an IoT automatic irrigation system.

However, the present research work represents a new branch that aims to evaluate the Bluetooth BLE 4.1 technology in realistic intelligent environments under real-world conditions. In addition, it will allow the experimentation of more complex research paths, as well as diversifying the number of applicable scenarios.

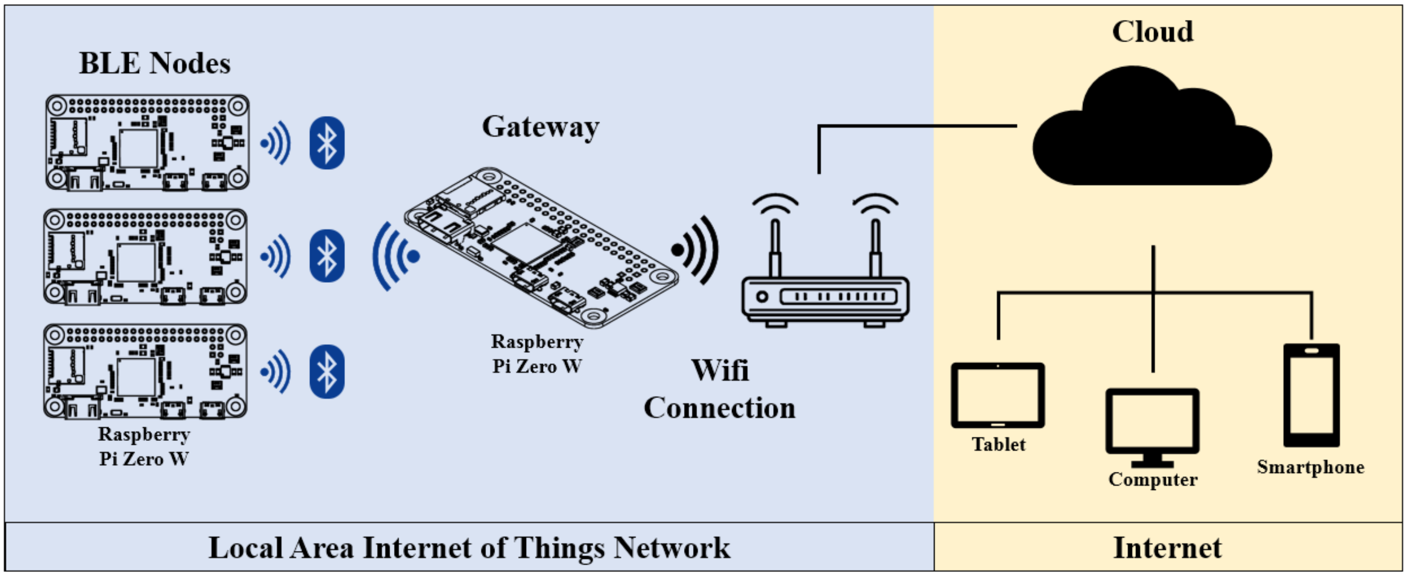

Figure 1. Bluetooth 4.1 BLE Testbed for Internet of Things.

3. BLUETOOTH 4.1 BLE TESTBED FEATURES

3.1. Testbed architecture.

In this work we present a Bluetooth 4.1 BLE testbed, which is initially presented in a star network topology, but with the ability to configure the characteristics of the network to different types of topologies depending on the application scenario. This network consists of a series of nodes that communicate to a gateway using Bluetooth 4.1 BLE technology. The nodes of this network send and receive information from the gateway, after that, the gateway communicates to a private web server in the cloud, where data can be viewed, processed, analyzed and stored.

Figure 1 shows the general configuration of the network and devices. The gateway (or multiple gateways depending on the network topology) sends and receives information from the cloud and this is responsible for being the bridge between nodes and the private web application from which the information of the nodes is viewed, processed, analyzed and stored, and also some actuators connected to the network are manipulated.

3.2. Hardware.

The nodes and the gateway of the testbed's local area IoT network are implemented with Raspberry Pi Zero W.

The Raspberry Pi (RPi) is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi Foundation. The RPI is a single board where all the essential circuits of a computer are contained, such as the Central Processing Unit (CPU), the Graphics Processing Unit (GPU), and several input, output and processing circuits [9]. The availability of features such as the General-Purpose Input Output (GPIO) pins make the computer amenable to programming hardware, as well as driving electronic circuitry and collect data through various means. Additionally, the RPi is a low-cost computer that has the ability to interact with the outside world and has been used in a wide array of digital maker projects. The RPi cards are used in IoT projects and by researchers around the world. Since its launch in 2012, the RPi has been a popular tool for developing testbeds in various research projects.

For its small size and capabilities, the RPi Zero W is selected in this research in order to achieve the same behavior as the common IoT devices installed in smart houses. RPi Zero W is a small development board that uses the Broadcom BCM2835 SoC as the main processer and which consists of the ARM11 CPU operating at 1GHz, 512MB of DRAM, MicroSD card slot, Camera Serial Interface and 2.4GHz 802.11n wireless LAN and Bluetooth 4.1 BLE transceiver. This board runs the Raspbian Linux operating system based on Debian Stretch Linux.

4. APPLICATION SCENARIO

4.1. A Lightweight Moving Target Defence Strategy for IoT Cyber Security.

In order to evaluate and quantify the performance of an IoT network under real world conditions, the testbed was implemented in one application scenario. This scenario has been proposed in the context of cyber security in IoT.

Consequently, the testbed was implemented for the research work “A Lightweight Moving Target Defence Strategy for IoT Cyber Security”.

As it was mentioned in the previous sections, “A Lightweight Moving Target Defence Strategy for IoT Cyber Security” is a research work that is being developed at the Cyber Security Laboratory of CIC-IPN. This work proposes the designing, implementation, and evaluation of a Lightweight Moving Target Defense (LMTD) strategy considering the IoT specific characteristics, using distributed computing in order to achieve a balance between performance, cyber security and required system resources.

To evaluate the LMTD strategy, it is necessary to generate real operating conditions of an IoT system. In that sense, this testbed provides a rigorous, transparent, and repeatable verification of objectives proposed in the research work mentioned above.

The application scenario chosen in the research work "A Lightweight Moving Target Defence Strategy for IoT Cyber Security" is a smart home. In this smart home, different network nodes collect environmental information and conditions inside and outside of a home, variables such as ambient temperature, humidity and air quality are measured and sent through the IoT network layer to an Internet web application where they can be monitored remotely.

The objective of implementing this testbed in this research work is to quantify the operability of the use of the Bluetooth communication protocol in a smart home application scenario, to measure the real limitations of Bluetooth 4.1 BLE under real operating conditions.

5. TESTBED PERFORMANCE

Testing performed in this work aims to measure the real behavior and capabilities of two properties of Bluetooth 4.1 BLE technology.

The first property is the maximum distance (in meters) reached from gateway to testbed's local area IoT network nodes, i.e., to analyze the network behavior when data is sent from nodes to gateway through different distances inside and outside home. Consequently, this means to obtain the maximum distance in relation to effectiveness rate of messages received between gateway and nodes in the network.

The second property analyzed is the energy efficiency of battery powered IoT nodes in the network. Once this information is obtained, it is possible to determine the average battery run-time in relation to its capacity in mAh, both in reception and data transmission conditions.

5.1. Distance tests.

In order to determine the maximum distance reached by Bluetooth communication between a gateway and network nodes, tests were carried out to send and receive data indoors and outdoors. Five-volts DC batteries were used as power source in network devices.

Data frames sent from nodes to gateway consist of a maximum of 20 bytes information per message, because a message of greater length in all tests generated a distortion in received data, i.e. more than 20 bytes messages in all cases did not match with received messages. For the above reason, in all tests presented in this work, 20 bytes information per message are taken as the base number.

Figure 2 presents the results obtained from the tests performed. In the chart we can observe that there is a direct relationship between distance and the number of bytes received with respect to the bytes sent, in other words, there is a decrease in the effectiveness rate of the messages received as the distance in meters between the sender and the receiver increases.

Let ρ be the effectiveness rate in percent, then we can have,

$$\rho = \frac{\lambda}{\mu} \tag{1}$$

Where λ is the number of bytes received and μ is the number of bytes sent. With Eq. (1), the effectiveness rate is calculated.

Figure 2 shows that ρ suffers a decrease for messages transmitted outdoors, as well as messages sent indoors; however, if proper analysis is performed and if a tangent line is drawn on the indoors curve at any of its points, then it results that the slope in this line is greater than the slope calculated in a line drawn at the same level in the Y-axis on the outdoors curve. In other words, the instantaneous rate of change calculated at any point on the indoors curve is higher than the instantaneous rate of change calculated at the same level on the Y-axis on the outdoors curve.

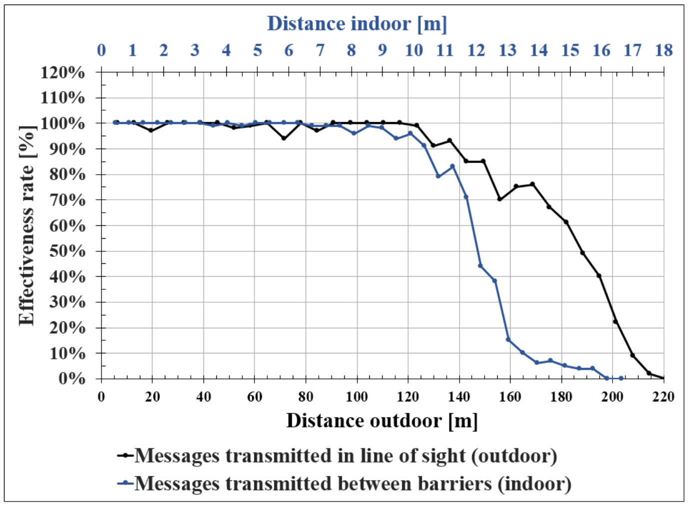

Figure 2. Effectiveness rate of messages received as a function of distance.

5.2. Network energy efficiency tests

In order to obtain the energy consumption levels reached by the network nodes which communicate using the Bluetooth BLE protocol to the network gateway, electrical current measurements were made during the sending and receiving of data.

Figure 3 shows the electrical diagram used to measure the electrical current in the testbed nodes.

While there are several methods of measuring current, the most common method is to perform an indirect measurement by measuring the voltage across a precision resistor and using Ohm's law to measure the current across the resistor.

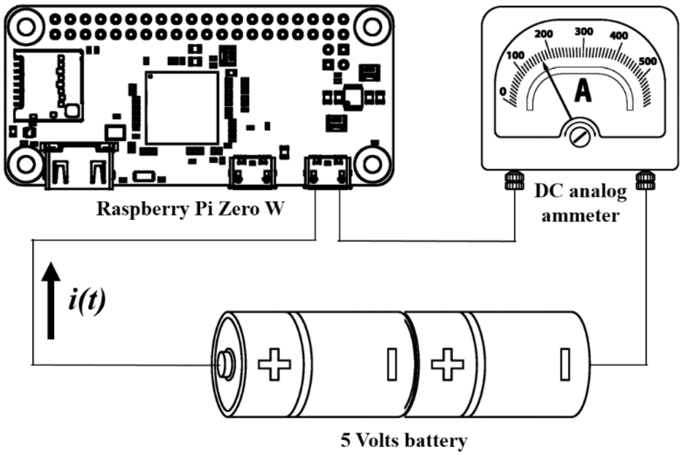

Figure 3. Electrical diagram for current measurement of testbed nodes

In order to measure the electrical current of the network nodes, direct measurements were made in this work with the help of an ammeter. This measuring device is essentially a voltmeter with a precision resistance. The ammeter uses Ohm's law to obtain the value of the current flowing through the circuit.

As shown in figure 3, the procedure consists of interrupting the flow of electrons in the circuit and connecting the ammeter as a bridge in the circuit through which the current flow passes.

Table 2 shows the data obtained from the average current consumption measurement under sending and receiving 20 bytes information messages every 5 seconds for all devices.

Table 2. Average BLE node current consumption

BLE Node		Average current consumption (mA)	Battery Life of a 4,000mAh battery (Hrs)
Raspberry Pi Zero W	Sending data every 5 seconds via Bluetooth communication protocol	240	16.6
	Receiving data every 5 seconds via Bluetooth communication protocol	185	21
	Without sending or receiving data	165	24.2

The point of estimating the 4000 mAh battery average lifetime in hours is to provide a more comprehensive overview of the RPi Zero W capabilities in real work conditions using the Bluetooth communication technology. In that sense, once these capabilities have been analyzed, the testbed can be helpful to take a more accurate decision when considering what type of wireless communication technology is most suitable for each project.

As it is shown in figure 4, the power consumption of BLE nodes in the local area IoT network increases as it uses Bluetooth technology to communicate with the gateway. If the network node is receiving information from the gateway and is in listen-only mode, the average power consumption increases by 12% compared to the average power consumption when the node was not sending or receiving data. Likewise, when the network node is sending messages to the gateway, the average power consumption increases by 45% compared to the average power consumption when it was not sending or receiving data.

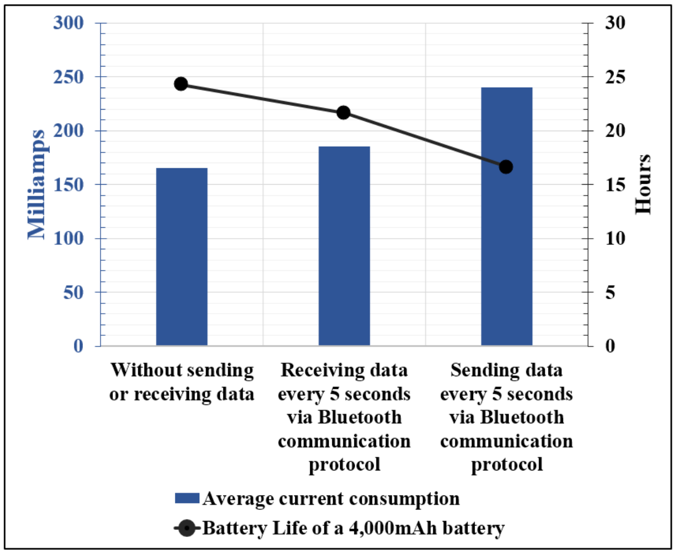

Figure 4. Average BLE node current consumption

The results obtained and shown in figure 4 were predictable considering that every electrical device demands more current as it performs more tasks or makes use of other features of its own system, i.e., BLE nodes in the network consume 45% more electrical current when they are sending messages to the gateway than when they are not receiving or sending any data.

It is important to note that the power consumption of the RPi Zero W needed to operate is significant. Despite its size, the RPi Zero W uses an ARM processor architecture, which runs an operating system and the functions derived from it. Also, RPi runs parallel programming which is controlled by an operating system task manager, among other features.

6. CONCLUSIONS

This testbed shows the real Bluetooth 4.1 BLE technology message transmission and reception capabilities as a function of the maximum distance reached indoors and outdoors under different parameters and conditions.

In addition, the energy efficiency of the RPi Zero W nodes was measured through the testbed using the inbuilt Bluetooth module. The average power consumption measurements show that when the IoT nodes send data to the gateway there is a 45% increase in power consumption compared to the average power consumption when the node was not sending or receiving data. Likewise, when the IoT node is receiving information from the gateway, the average power consumption increases by 12% compared to the average power consumption when it was not sending or receiving data.

This work can be a starting point for the development of similar projects seeking to use Bluetooth BLE 4.1 short-range wireless transmission technology in Internet of Things networks.

7. FUTURE WORKS

7.1. Pentesting Tests and Cybersecurity Requirements Analysis

This testbed is a tool that can be used in a practical way for different purposes.

One of them is the vulnerabilities detection of the Bluetooth BLE 4.1 communication protocol through penetration tests performed in different points of the network. Also, these tests will allow to obtain security requirements to harden the network and increase the security of the system.

7.2. A LoRaWAN, Bluetooth 4.1, 802.11 bgn Wireless LAN (WiFi) and ZigBee Testbed for IoT

The heterogeneity of IoT that limits the interconnection and functionality of the communication protocols of these networks is one of the first problems for testing IoT systems today. To solve this problem and expand the capabilities of this testbed it is proposed as a future work to integrate LoRaWAN, 802.11 b/g/n wireless LAN (WiFi) and ZigBee communication protocols to the current Bluetooth 4.1 BLE testbed presented in this work.

This research work would represent an improvement towards a more complete testbed where some of the most used wireless communication protocols in IoT systems are considered. In addition, it will allow the experimentation of more complex research avenues, as well as diversify the number of applicable scenarios.

ACKNOWLEDGMENT

The first authors acknowledge the support of CONACYT to carry out this research. Acknowledge is also given to IPN-SIP for its support to carry out this research under grant SIP-20200480 and SIP-20200481.

REFERENCES

[1] A. Sunyaev, “The Internet of Things,” in Internet Computing, Springer International Publishing, 2020, pp. 301–337 [Online]. Available: http://dx.doi.org/10.1007/978-3-030-34957-8_10

[2] A. Bemani, N. Bjorsell, “Cyber-Physical Control of Indoor Multi-vehicle Testbed for Cooperative Driving,” arXiv preprint arXiv:2006.04421, Jun, 2020 [Online]. Available: https://arxiv.org/abs/2006.04421

[3] K. Li, N. Lu, P. Zhang, W. Ni, and E. Tovar, “Poster Abstract: Multi-Drone Assisted Internet of Things Testbed Based on Bluetooth 5 Communications,” in 2020 19th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), 2020 [Online]. Available: http://dx.doi.org/10.1109/IPSN48710.2020.00-14

[4] W. K. Saad, Y. Hashim, and W. A. Jabbar, “Design and Implementation of Portable Smart Wireless Pedestrian Crossing Control System,” IEEE Access, vol. 8, pp. 106109–106120, 2020, doi: 10.1109/access.2020.3000014. [Online]. Available: http://dx.doi.org/10.1109/ACCESS.2020.3000014

[5] A. A. Mercado-Velázquez, P. J. Escamilla-Ambrosio, F. Ortiz-Rodríguez, A. J. Rosales-Silva, N. Muñoz-Aguirre, “Mesa de pruebas para el protocolo LoRa”, SOMI XXXIV Congreso de instrumentación, Morelia, 2019.

[6] D. Hortelano et al., “From Sensor Networks to Internet of Things. Bluetooth Low Energy, a Standard for this Evolution,” Sensors, vol. 17, no. 2, Feb. 2017, Art. No. 372.

[7] S. M. Darroudi, C. Gomez, and J. Crowcroft, “Bluetooth Low Energy Mesh Networks: A Standards Perspective,” IEEE Communications Magazine, vol. 58, no. 4, pp. 95–101, Apr. 2020, doi: 10.1109/mcom.001.1900523. [Online]. Available: http://dx.doi.org/10.1109/MCOM.001.1900523

[8] J. Yang, C. Poellabauer, P. Mitra, and C. Neubecker, “Beyond beaconing: Emerging applications and challenges of BLE,” Ad Hoc Networks, vol. 97, p. 102015, Feb. 2020, doi: 10.1016/j.adhoc.2019.102015. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2019.102015

[9] E. Upton, J. Duntemann, R. Roberts, T. Mamtora, B. Everard, “Learning Computer Architecture with Raspberry Pi”, Wiley: Indianapolis, September 2016.