SCIREA Journal of Electrical Engineering

https://www.scirea.org/journal/DEE

November 7, 2019

Volume 4, Issue 4, August 2019

Comparison between IOT protocols: ZigBee and WiFi using the OPNET simulator

Hamza Zemrane[‡]

EMI, UM5, Rabat, Morroco

zemranehamza93@gmail.com (Hamza Zemrane)

Youssef Baddi[§]

ESTSB, UCD, El Jadida, Morroco

baddi.y@ucd.ac.ma (Youssef Baddi)

Abderrahim Hasbi

EMI, UM5, Rabat, Morroc

ahasbi@gmail.com (Abderrahim Hasbi)

Abstract

The Internet of things is perceived today as a key opportunity for commercial development in different sectors of activity that can be deployed in the local level as in the case of smart homes, at the regional level as in the case of health, or at the national level in the energy management sector. The IOT connectivity services are different depending on the use case, we find in this context a large number of constantly evolving protocols at the perception layer in the architecture of IOT networks, we distinguish in this article two of these protocols standardized by IEEE which are ZigBee and WiFi.

CCS CONCEPTS

•Computer systems organization → Embedded systems; Re-dundancy; Robotics; • Networks → Network reliability;

Keywords: Internet of Things, IOT architecture, ZigBee, WiFi, WSN

1. Introduction

The vision of the Internet of Things (IoT) is to build a smart environ-ment by using objects (wireless sensor[4], RFID[5], smart phone, wearables ...), which have the ability to collect information from the environment in which they are deployed, store it, process it, and transmit it using an Internet gateway for decision making. This vi-sion of the Internet of Things encompasses several building blocks that integrate and engage in multidisciplinary and interdisciplinary, business and technical domain activities. This involves interactions between the various entities of the IoT ecosystem, the information shared between the subsystems of the ecosystem is used for deci-sion making, the success of the IoT will depend on the evolution and development of these subsystems of the IoT ecosystem. Several communication protocols are then developed to improve the Inter-net of Things. In this article we detail on the second section the definition of Internet of Things, its architecture, and protocols, on the third section the IEEE 802.15.4 protocol (ZigBee [8]): its system structure, its topologies, its different frames, and the architecture of the protocol, on the fourth section the IEEE 802.11 protocol (WiFi): its modes, data transmission techniques and its physical frames, and on the fifth section the simulation of the two protocols using Opnet simulator.

2. INTERNET OF THINGS (IOT): DEFINITION, ARCHITECTURE, AND PROTOCOLS

2.1 Definition of IoT

We talk about the Internet of Things when the number of devices exceeds the number of people connected to the Internet, the goal of the Internet of Things is to facilitate human life by building a smart environment by using smart objects that have the ability to autonomously generate data from the environment in which they are deployed and to transmit that data to the Internet for decision-making. The IoT devices are usually wireless sensors[4], smart phones, RFID [5], smart homes, and others connect to the Internet via a plug-in connection module in a clever environment. These devices are used to collect information from the physical environment, and send it to the network edge for further process-ing. These devices are deployed with a network architecture and a separate data processing application according to the specific task in a particular area, for example using an intelligent health unit in a body to know the heartbeat, the position of the patient, blood pressure, temperature and others. The connected smart home management, to save energy, facilitates mobility, improved comfort through increased accessibility of domestic components.

2.2 Architecture of IoT

The architecture of the IoT consists of the following layers

2.2.1 Perception layer. It is composed of physical objects that have the ability to capture physical quantities (heat, humidity, vibration, radiation, and others) and transform them into digital magnitudes, process this information, store it and transmit it via a transmission module wireless to a sink or a network gateway. This layer consists of Wireless sensors, RFID[5], smart phones, wearables, smart cars, smart homes, and others.

2.2.2 Network layer. It transmits the digital information collect from the physical environment in analog format to a sink or the network gateway for further processing on this information. In this context we find a lot of technology on constant evolution as: Low Energy bluetooth[11], Lorawan[1], wifi, ZigBee [8] and others.

2.2.3 Application layer. It serves as an interface for the user to ac-cess information collected from the perception layer to manipulate them according to the demand of the specific domain and process them in a processing system.

2.2.4 Middle-ware layer. Several different IoT devices in the same domain communicate with the same compatible device, this layer makes possible to extract the information sent from different hard-ware equipment, to translate it into a service information, for ad-dressing, the denomination of the requested service, and manage-ment services.

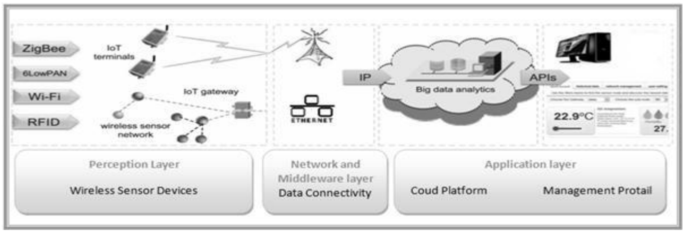


Figure 1: Architecture of the Internet of Things.

2.3 IoT protocols

For companies embarking on IoT, choosing the most suitable com-munication network to connect their objects to the Net can become deficient. There are two major categories of networks on the mar-ket:

- Long-range networks : such as Sigfox [9], LoRa [9] or cel-lular technologies (GSM, 2G, 3G, 4G ...) are capable of trans-mitting data from one device to another over vast distances. They are used by companies that want to connect kilometers of infrastructure to the Internet or in smart cities projects for example.
- Short-range networks : such as WiFi, Z-Wave[6], ZigBee[8], or Bluetooth Low Energy [11] allow data to be transferred over short distances, and are widely used in home automation or on the large wearable market.

3. ZIGBEE PROTOCOL: IEEE 802.15.4

Its specification is maintained by the Zigbee Alliance.It is a short-range protocol (WPAN or Wireless Personal Area Network)[12] by radio, Zigbee’s goal is to provide a way to create a simpler, cheaper WPAN network[12] than conventional technologies such as Bluetooth [11] or WiFi. Combining low-power operation, high security, robustness and high scalability with a large number of nodes, ZigBee/RF4CE [8] offers significant advantages in complex systems. This protocol is also in an ideal position to get wireless sensor networks in the IoT and M2M applications.

3.1 System structure, topologies and ZigBee frames

3.1.1 Structure of ZigBee system. The structure of the ZigBee[8] system consists of three different types of devices that are: ZigBee coordinator, ZigBee routers and ZigBee end devices.

- ZigBee coordinator (ZC) : is responsible for processing and storing information when receiving and transmitting data (One by Zigbee network, Initializes the network, Be-haves like a coordinator PAN 802.15.4, Behaves as a router once the network is initialized, Contains the entire stack).

- ZigBee routers (ZR) : act as intermediary devices that allow data to pass from one device to another (Optional network component, Associates with the ZC or with an already associated ZR, Behaves like a coordinator PAN 802.15.4, Participate in the routing of messages, Contains the entire stack).

- ZigBee end devices (ZED) : have limited functionality to communicate with parent nodes, so battery power is not consumed quickly (Optional network component, Does not allow associations, Does not participate in routing, Embark a light pile).

3.1.2 ZigBee topologies. The number of routers, coordinators and end devices depends on the type of the network topology, the IEEE 802.15.4 standard allows us three topology in the installation of a ZigBee network[8].

- Star topology : All the nodes (routers and terminals) com-municate only with the central node which is the coordinator, so to send a packet from one device to another, the packet must be routed by the coordinator. The problem in this topol-ogy is that if the link between the coordinator and the final device fails there are no other routes, the second problem is that all the packets in the network must pass through the coordinator, which increases the risk of congestion of the network.

- Tree topology : The "Zigbee coordinator" is in charge of starting the network, the coordinator can be linked to several routers and end devices, the routers can also be connected to other routers and end devices, respecting in hierarchy with the tree structure that contains the "Zigbee coordinator" at the top. The problem of this topology is that if a communi-cation link does not work there is no other route to reach the destination.

- Mesh topology : The coordinator is linked to other routers and end devices, and these routers can also be connected to other routers or end devices, allowing peer to peer peer communications. the advantage of this topology is that it al-lows a flexible propagation of the packets, if a link is blocked, other alternative routes can be used to route the packets.

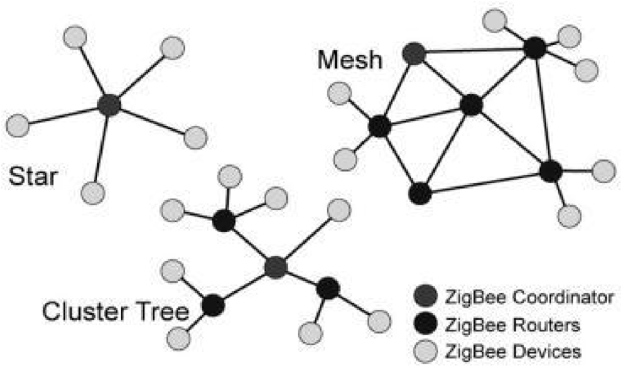


Figure 2: ZigBee topologi

Frequency band	Availability	Number of channels	Maximum speed
868 Mhz	Europe	1	20Kbit/s
915 Mhz	Americas and Australia	10	40Kbit/s
2.4 Ghz	Available every-where	16	250Kbit/s

Table 1: Usable frequency band deifies by 802.15

3.1.3 Zigbee frames. Zigbee frames have a maximum size of 128 bytes including protocol overhead. There is therefore a total of 104 bytes of data. The IEEE 802.15.4 MAC defined 4 frames structure:

- "Beacon" or SuperFrame frame : are used to synchronize nodes, to identify the network, and to describe the structure of "superframes".
- Data frame : used for all data transfers.
- Confirmation frame: used to confirm that a data frame has been received successfully.
- MAC control frame : used to manage all MAC control transfers.

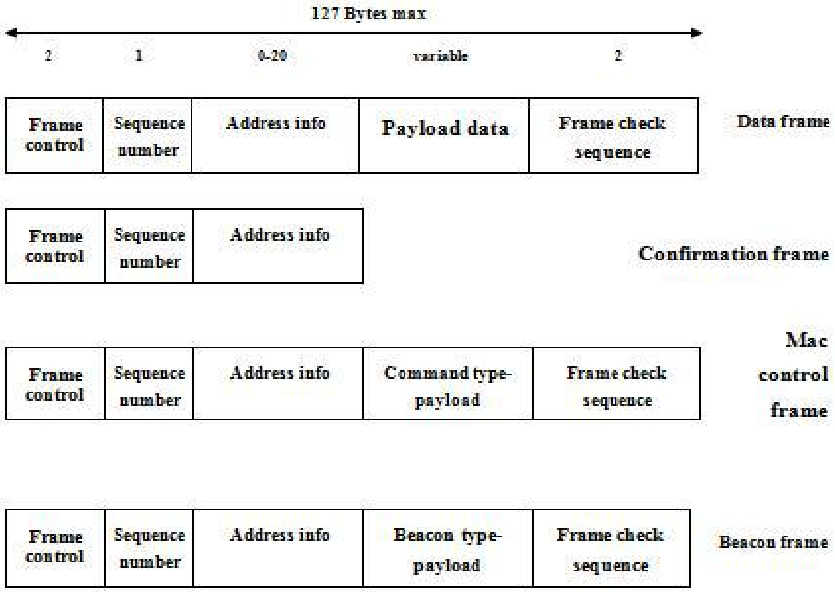


Figure 3: ZigBee MAC layer Frames

3.2 Architecture of ZigBee protocol

The ZigBee [8] protocol architecture consists of multiple layers, IEEE 802.15.4 is defined by physical layers, and Mac while this protocol is complete by the accumulation of network layers and ZigBee application.

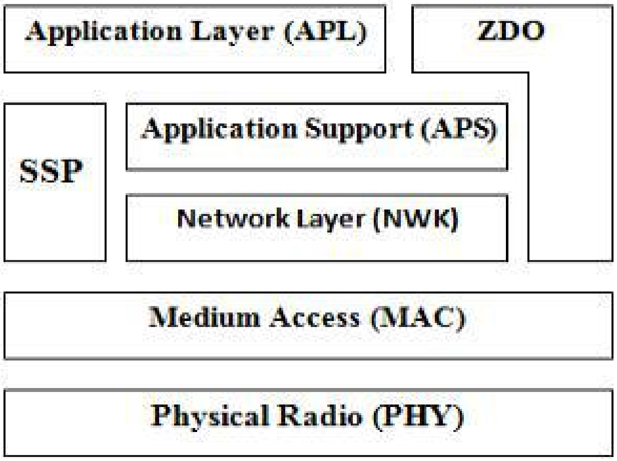
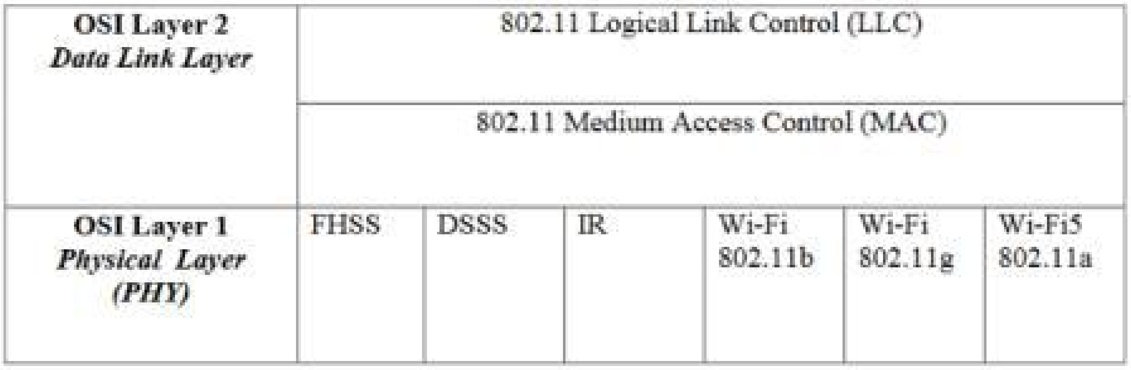


Figure 4: Architecture of ZigBee protocol

- The physical layer : This layer performs modulation and demodulation operations respectively on the transmit and receive signals.
- The MAC layer : It is responsible for the reliable transmis-sion of data by accessing different networks with Carrier Detection Multiple Access (CSMA) collision avoidance. It also transmits beacon frames to synchronize communication.
- The network layer : it supports all network-related opera-tions, such as network and device configuration, connecting and disconnecting end devices from the network, routing.
- The sub-layer application support : Enables the neces-sary services for the ZigBee device object and application objects to interface with network layers for data manage-ment services.
- Application Layer : It provides two types of data services as a pair of key values and generic message services. The message is a structure defined by the developer, while the key-value pair is used to get the attributes in the application's objects. ZDO is the interface between the APS layer and the application objects.He is responsible for detecting, initiating, and linking other network devices.

4. WIFI PROTOCOL: IEEE 802.11

The IEEE 802.11 standard defines the first two layers (low) of the OSI model, namely the physical layer and the data link layer. The latter is itself subdivided into two sub-layers, the LLC sublayer (Logical Link Control) and the MAC layer (Medium Access Control). The following figure illustrates the model architecture proposed by the 802.11 work-group compared to the OSI model. One of the peculiarities of this standard is that it offers several variants at the physical level, while the link part is unified.



OSI Layer 2 ***Data Link Layer***	802.11 Logical Link Control (LLC)					
	802.11 Medium Access Control (MAC)					
OSI Layer 1 ***Physical Layer (PHY)***	FHSS	DSSS	IR	Wi-Fi 802.11b	Wi-Fi 802.11g	Wi-Fi5 802.11a

Figure 5: WiFi layers

4.1 Topology and data transmission

4.1.1 Operating mode.

- Infrastructure : The infrastructure mode[2] is based on a special station called Access Point (AP). This mode allows WiFi stations to connect to a network (usually Ethernet) via an access point. It allows a WiFi station to connect to another wiFi station via their common AP. A WiFi station associated with another AP can also interconnect. All AP radio rang stations form a Basic Service Set (BSS). Each BBS is identified by a 6-byte BSSID (BSS Identifier) that corresponds to the MAC address of the AP.

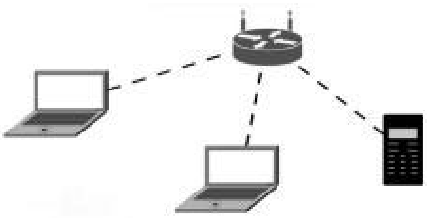


Figure 6: Infrastructure topology

- Ad-Hoc : In ad hoc mode [3] the client wireless machines connect to each other in order to constitute a point-to-point network (peer to peer), that is to say a network in which each machine plays at the same time the role client and the role of access point. The set formed by the various stations is called a set of independent basic service set (IBSS). In an ad hoc network, the scope of the independent BSS is determined by the scope of each station. This means that if two of the network stations are out of reach of each other, they will not be able to communicate even if they "see" other stations.

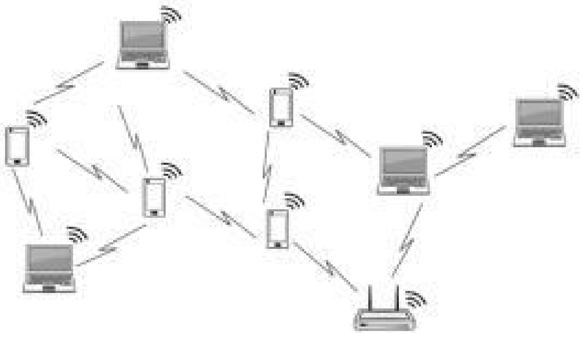


Figure 7: Ad-hoc topology

4.2 Data transmission techniques

4.2.1 The transmission channels. The transmission channels: The transmission channel is a narrow frequency band that can be used for communication. The governments propose frequency bands for free use. The bodies responsible for regulating the use of radio fre-quencies are: ETSI (European Telecommunications Standards Insti-tute) in Europe, the Federal Communications Commission (FCC) in the United States,and MKK (Kensa-kentei Kyokai) in Japan. United States released three frequency bands for Industry, Science and Medicine. These frequency bands, called ISM (Industrial, Scientific, and Medical), are the bands 902-928 MHz, 2.400-2.4835 GHz, 5.725-5.850 GHz. In Europe the 890 to 915 MHz band is used for mobile communications (GSM), so only the bands 2,400 to 2,44835 GHz and 5,725 to 5,850 GHz are available for amateur radio use.

4.2.2 Transmission technologies. Local radio networks use radio or infrared waves to transmit data. The technique originally used for radio transmissions is called narrow-band transmission; it consists of passing different communications over different channels. The physical layer of the 802.11 standard thus initially defines several transmission techniques to limit the problems due to interference: The technique of frequency hopping spread spectrum,The technique of direct sequence spread spectrum, Infrared technology.

The narrow-band technique. The narrow band technique consists in using a specific radio frequency for the transmission and recep-tion of data. The frequency band used should be as small as possible to limit interference on adjacent bands.

The technique of frequency hopping spread spectrum. The Fre-quency Hopping Spread Spectrum (FHSS) technique [7] consists of splitting the wide frequency band into a minimum of 75 channels, then transmit using a known channel combination of all stations in the cell. In the 802.11 standard, the 2.4 - 2.4835 GHz frequency band makes it possible to create 79 channels of 1 MHz. The transmission is done by emitting successively on one channel then on another for a short period of time (about 400 ms), which allows a given moment to transmit a more easily recognizable signal on a given frequency.

The technique of direct sequence spread spectrum. Direct Sequence Spread Spectrum (DSSS)[10] is the technique of transmitting for each bit a Barker sequence of bits. The physical layer of the 802.11 standard defines an 11-bit sequence (10110111000) to represent a 1 and its complement (01001000111) to encode a 0. Each bit encoded with the sequence is called chip or chipping code.

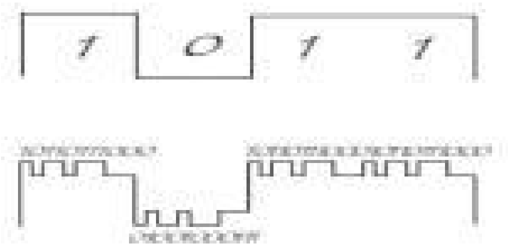


Figure 8: The technique of direct sequence spread spectrum

Infrared technology. The IEEE 802.11 standard also provides an alternative to using radio waves: infrared light. The main charac-teristic of infrared technology is the use of a light wave for data transmission. Thus the transmissions are uni-directional. The non-dissipative nature of the light waves provides a higher level of security. It is possible thanks to the infrared technology to obtain rates ranging from 1 to 2Mbit/s using a modulation called PPM (pulse position modulation).

4.3 WiFi physical frames

Data packets from the network layer are encapsulated at level 2 by a MAC header, forming a Mac Protocol Data Unit (MPDU). This MPDU is then encapsulated in a second frame at level 1 (physical) to allow transmission on the media this set forms a (PLCP-PDU).

Frame FHSS used in the IEEE 802.11. .

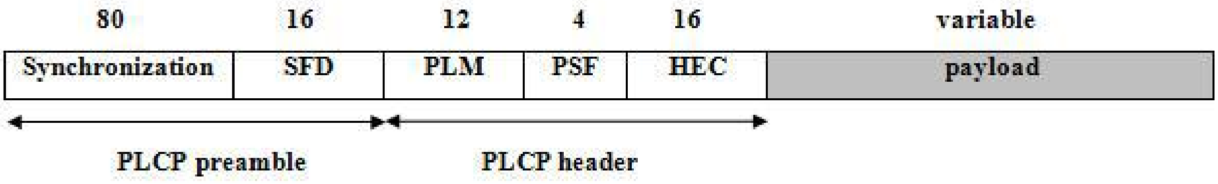


Figure 9: FHSS frame bit size

Frame DSSS used in the IEEE 802.11 b. .

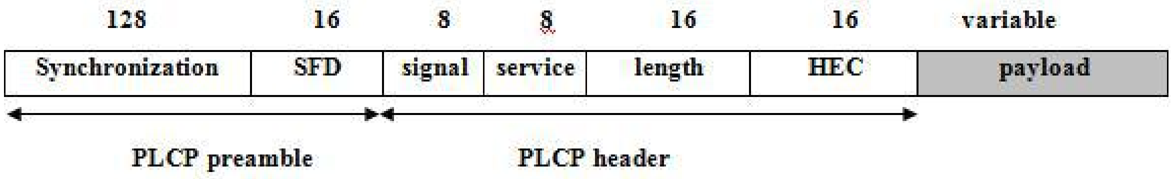


Figure 10: DSSS frame bit size

Frame OFDM used in the IEEE 802.11a end the IEEE 802.11g. .

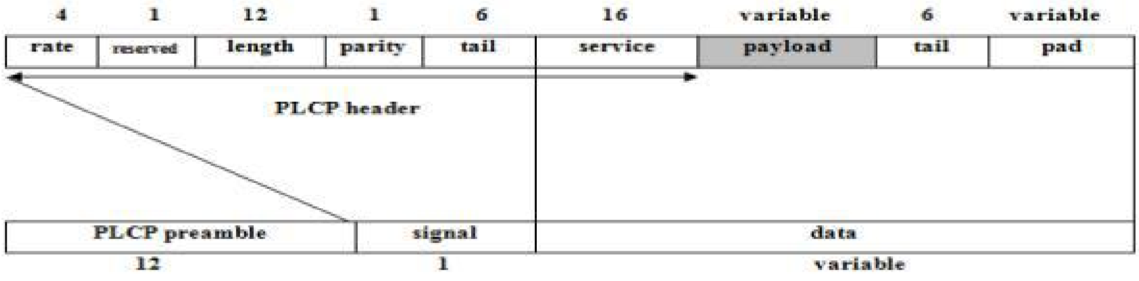


Figure 11: OFDM frame bit size

5. SIMULATION WITH OPNET FOR ZIGBEE AND WIFI

Table 2: Technical comparison between the two protocols

Protocol	ZigBee	WiFi
IEEE	802.14.5	802.11
Memory need	4-32KByte	1MByte+
Autonomy of the battery	Years	Hours
Maximum network nodes	65 000+	256+
Speed of transfer	20-250kbps	320-100
		Mbps
Scope	100m	300m
Security method	23-34-128 bit AES	SSID
Application	Remote control Mea-	Wireless
	surement, control	LAN

5.1 ZigBee: IEEE 802.15.4

5.1.1 Simulation scenario. The following simulation consists of a ZigBee coordinator that starts the network, routers, and end devices, forming three possible scenarios for simulating a star topology, a tree topology, and a mesh topology. The objective of this simulation is to analyze the performance of a ZigBee network in the context of the Internet of things, according to the following parameters.

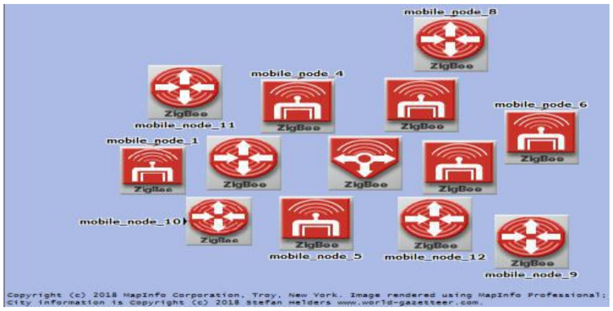


Figure 12: ZigBee scenario

5.1.2 Results.

Application layer end to end delay. Time interval between when a message is queued for transmission at the physical layer until received at the receiving node.

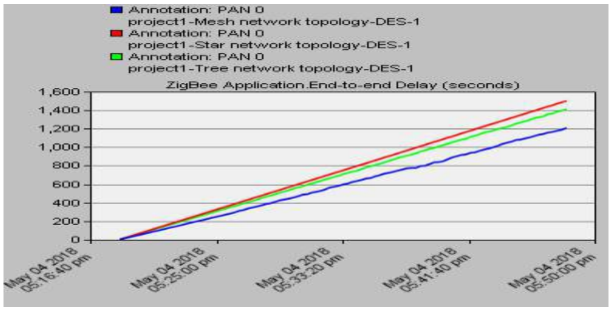


Figure 13: Average end to end delay by seconds

Network layer number of Hops. It’ s the number of times a packet travels from the source through the intermediate nodes to reach the destination.

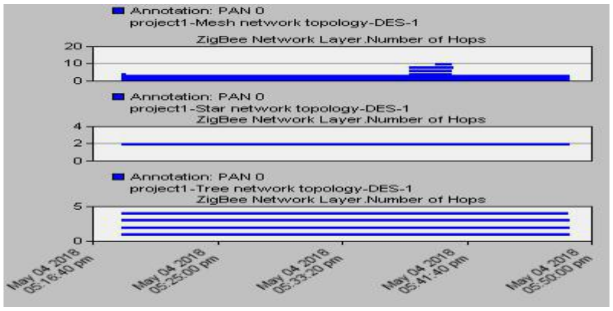


Figure 14: Number of Hops

MAC layer media Access delay. Data parquets are transited from the network interface card to the shred channel using the mac media access layer.

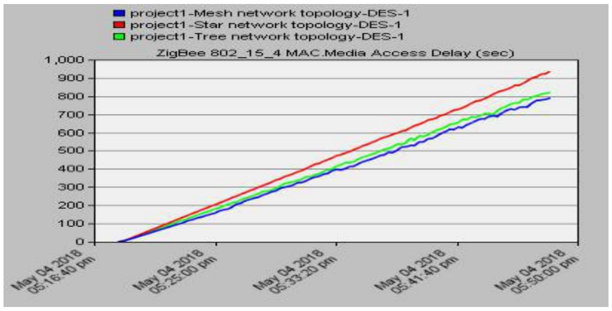


Figure 15: Media Access delay by seconds

5.2 WiFi: IEEE 802.11

5.2.1 Simulation scenario. The following simulation consists of a wireless Wifi access point, a router that acts as the gateway, an HTTP server that contains the application used by end users in mobile stations. The objective of this simulation is to analyze the performance of a WiFi network in the context of the Internet of Things, according to the following parameters.

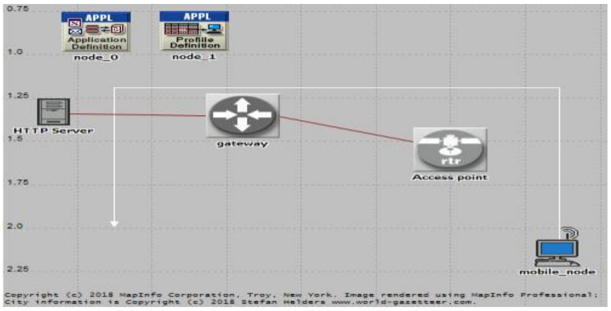

0.75
1.0
1.25
1.5
1.75
2.0
2.25
APPL
Application Definition
node_0
APPL
Profile Definition
node_1
HTTP Server
gateway
rtr
Access point
mobile_node
Copyright (c) 2018 MapInfo Corporation, Troy, New York. Image rendered using MapInfo Professional;
City information is Copyright (c) 2018 Stefan Helders www.world-gazetteer.com.

Figure 16: WiFi scenario

5.2.2 Results.

Application HTTP Traffic sent end received. Its the comparison between the number of bytes of HTTP application sent and received from the source to the destination.

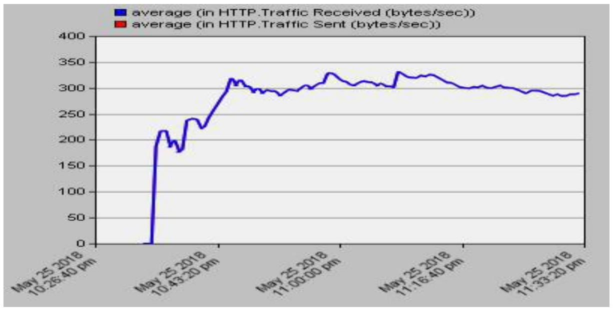


Figure 17: HTTP Traffic sent and received by bytes/s

Wireless LAN Media Access delay. Provide an addressing mecha-nism and channel access so that each wireless node available on a network can communicate with other wireless nodes available on the network.

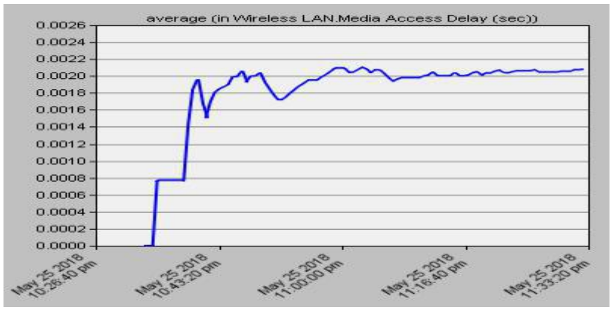


Figure 18: Wireless LAN Media Access delay by seconds

Physical Wireless LAN throughput. Is the useful transmission rate of the network over a communication channel (messages suc-cessfully received)

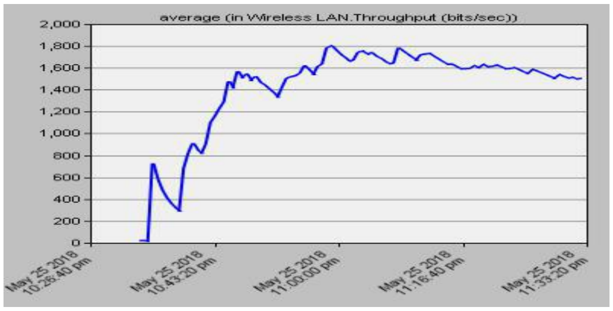


Figure 19: Wireless LAN throughput by bits/seconds

6. CONCLUSIONS

WiFi and ZigBee are two protocol widely used in the short range networks for the creation of WPAN [12] for services that use the Internet of Things, WiFi is a protocol that is defined at the data link layer and the physical layer, unlike ZigBee [8], which makes an abstraction of the network and transport layers, the ZigBee [8] protocol makes it possible to do the routing and also to ensure the forwarding of the end-to-end packets, our future work will be to improve these two protocols which are defined in perceptual level in the IoT network architecture using Software Defined Application (SDN) technology which allows to decouple the control function in the equipments and to centralize it at the level of a single controller.

REFERENCES

[1] Ferran Adelantado, Xavier Vilajosana, Pere Tuset-Peiro, Borja Martinez, Joan Melia-Segui, and Thomas Watteyne. 2017. Understanding the limits of LoRaWAN. IEEE Communications magazine 55, 9 (2017), 34–40.

[2] Bharathan Balaji, Jian Xu, Anthony Nwokafor, Rajesh Gupta, and Yuvraj Agarwal. 2013. Sentinel: occupancy based HVAC actuation using existing WiFi infrastruc-ture within commercial buildings. In Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems. ACM, 17.

[3] Min Chen, Yixue Hao, Yong Li, Chin-Feng Lai, and Di Wu. 2015. On the com-putation offloading at ad hoc cloudlet: architecture and service modes. IEEE Communications Magazine 53, 6 (2015), 18–24.

[4] Long Cheng, Jianwei Niu, Chengwen Luo, Lei Shu, Linghe Kong, Zhiwei Zhao, and Yu Gu. 2018. Towards minimum-delay and energy-efficient flooding in low-duty-cycle wireless sensor networks. Computer Networks 134 (2018), 66–77.

[5] Klaus Finkenzeller. 2010. RFID handbook: fundamentals and applications in con-tactless smart cards, radio frequency identification and near-field communication. John Wiley & Sons.

[6] Behrang Fouladi and Sahand Ghanoun. 2013. Security evaluation of the Z-Wave wireless protocol. Black hat USA 24 (2013), 1–2.

[7] Sterling Hughes, Jana Van Greunen, Raj Vaswani, et al. 2013. Creation and use of unique hopping sequences in a frequency-hopping spread spectrum (FHSS) wireless communications network. US Patent 8,442,092.

[8] Manijeh Keshtgari and Amene Deljoo. 2011. A wireless sensor network solution for precision agriculture based on zigbee technology. (2011).

[9] Mads Lauridsen, Benny Vejlgaard, István Z Kovács, Huan Nguyen, and Preben Mogensen. 2017. Interference measurements in the European 868 MHz ISM band with focus on LoRa

and SigFox. In Wireless Communications and Networking Conference (WCNC), 2017 IEEE. IEEE, 1–6.

[10] Yao Liu, Peng Ning, Huaiyu Dai, and An Liu. 2010. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In INFOCOM, 2010 Proceedings IEEE. IEEE, 1–9.

[11] Mike Ryan et al. 2013. Bluetooth: With Low Energy Comes Low Security. WOOT 13 (2013), 4–4.

[12] Su-Khiong Yong, Pengfei Xia, and Alberto Valdes-Garcia. 2011. 60GHz Technology for Gbps WLAN and WPAN: from Theory to Practice. John Wiley & Sons.