SCIREA Journal of Mathematics

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

December 19, 2019

Volume 4, Issue 6, December 2019

IoT Smart Home Ecosystem based on Multiprotocol Label Switching

Hamza ZEMRANE, Youssef BADDI, Abderrahim HASBI

Hamza ZEMRANE, Mohammadia School of Engineering, UM5, Lab RIME Rabat, Morocco, zemranehamza93@gmail.com, Web site: https://www.emi.ac.ma/

Dr.Youssef BADDI Higher school of technology Sidi Bennour UCD, Lab STIC El Jadida, Morocco, baddi.y@ucd.ac.ma, Web site: http://baddiyoussef.com/

Dr.Abderrahim HASBI, Mohammadia School of Engineering UM5, Lab RIME Ratab, Morocco ahasbi@gmail.com, Web site: https://www.emi.ac.ma/

Abstract

The development of Smart Cities that know our word today depends on the development of the IoT, in this context IoT are applied to develop and optimize may current and future sectors of activities like: health care, home automation, transportation, public services and others. The major issues of safety and comfort in traditional homes pushed us to detail and develop our own IoT Smart Home Ecosystem. Inside the home no one is safe from a fall, a cut, a poisoning, a burn, or a fire, as an example children are unfortunately the first victims of domestic accidents. The Smart Home can limit risks by integrating: smoke detectors, carbon monoxide detectors, alarms to trigger oneself when needed (PMR, for people with reduced mobility), motion detectors with alarm connected to the smartphones of your family member, remote surveillance cameras (for children and dependent persons). Equipped with many sensors and actuators, the Smart

Home can identify any potentially dangerous malfunction. The network architecture of IoT offers us a large number of network technologies to connect all the sensors and actuators to each other, and to transfer the collected information to the Internet, to choose the most suitable solution to use in our IoT Smart Home Ecosystem we did a study of the existing network solutions to go out with the WiFi network as a wireless solution and the Ethernet network as a wired solution. To allow access at the collected information to the right server located in the Internet with a quality of service grantee we were based on the MPLS network as a resent core Internetwork technology used by the operators.

Index Terms : Smart home, Internet of Things (IoT), IoT protocols, extended networks operators, Multiprotocol Label Switching (MPLS), Smart Cities.

1 INTRODUCTION

The IoT Smart Home Ecosystem also known under the name of the IoT Home Automation Ecosystem uses technol- ogy to make life easier for its inhabitants with respect of the environment. Everyone thanks to home automation can make their home more comfortable and secure to protect it from intruders, the children from accidents of every day, and even achieve great energy savings. If a simple audible alarm is sometimes not enough to deter burglars, clever solutions exist, and home security allows a real defense plan to be put in place. Depending on the needs (departure for holidays, weekends, nights), the user can anticipate scenarios: burglary, degradation of the garden, nocturnal revelers, etc. The necessary equipment are installed to respond to these scenarios: shutter closing, automatic watering, programmed lighting, etc. This can sim- ulate the presence of the user to discourage intrusions, or to trigger remote monitoring when he decide. The presence detection camera can generate an alert on a security service or even on the laptop, thanks to new applications with the video surveillance technology the user can be informed in real time and remotely if someone is trying to enter the home, he can then call a security company or the police. The technology used inside the smart home allows a programming of multiple devices to save energy consumption. The water heater can be activated one hour before the user arrival, and goes out when he leave, timer lighting and motion detector

prevent from forgetting to turn off the light, intelligent automatic watering can be programmed at night, the water does not evaporate, and the plants are not scorched by the sun. These programs can make us save energy and piece of mind. To connect all the sensors and the actuator inside the home between them in order to allow access at the collected home information to the gateway, who is in charge of retransmitting them via the Internet to the dedicated processing system hosted in the Web servers, the IoT network architecture offers us a large number of network technologies. Choosing the best network solution for our IoT Smart Home Ecosystem becomes then something that needs to be taken seriously. The comparative study that we made between the networks based on the network settings: physical support, topology, scope, debit, shows us that the wireless network WiFi and the wired network Ethernet are the two best solutions to applied on the IoT Smart Home Ecosystem. For the transmission of the home information from the local network to the right Web server via the Internet with a quality of service that varies depending on the types of data to be transmitted, we were based on a recent network used by the operators the MPLS core network that use label routing end traffic engineering for the QoS. The rest of the paper is organized as follows:

Section II talks about the Internet of Things, we give a definition of the IoT, its architecture, and we give examples of its domain of applications.

Section III talks about the IoT Smart Home Ecosystem, we define what is a domestic comfort, the home automation systems operation, we give a description of the information chain and the energy chain of a home automation systems based on the central heating of a house, and we give in general the component of a home automation system.

In Section IV we give the state of the art of the Network Layer of the IoT architecture, there is a lot of networks protocols for the IoT, we were based on some decision support settings to define the most suitable domain of application of each one (physical support, topology, scope, debit, synchronous) and we give a comparative table of IoT protocols based on these parameters.

In Section V we talk about the related work based on our last researches, where we can see the development of our work and the relation between this article and the others.

In Section VI we talk about the MPLS network and we detail the MPLS protocol mode of operation, we give the objective of MPLS, the concept of an MPLS network, and the MPLS terminology (architecture of the MPLS network, the label used in MPLS, the MPLS tables, and

the MPLS label distribution protocols: LDP,CRLDP, RSVP.).

In Section VII we make a simulation with the OPNET Network Simulator to study the network performance of our the IoT Smart Home Ecosystem were we compare a wireless solution using the WiFi protocol to a wired solution using Ethernet protocol, for the network layer of the IoT Ecosystem, for the Middle-ware layer we used the MPLS core network to send home information to right server, we analyze the performance of two protocol based on the network delay, the queries sent to the database by the sensors, in the case of using an HTTP application and in the case of using a Voice application.

2 INTERNET OF THINGS (IOT)

A. 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 smart environment using smart objects that can autonomously generate data from the environment in which they are deployed and transfer this data to the Internet for decision-making. The IoT devices are usually wireless sensors[1], smart phones, RFID[2], smart homes[3], and others connected 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 processing. These devices are deployed with a network architecture and a separate data processing application according to specific tasks in a particular area.

B. Architecture of IoT

The architecture of the IoT consists of the following layers:

1) *Perception layer:* Its 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 wireless transmission module to a sink or a network gateway. This layer consists of Wireless sensors[1], RFID[2], smart phones, wearable, smart cars, smart homes[3], and others.

2) *Network layer:* It transmits the digital information col- lect from the perception layer in

analog signal 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 [4], LoRaWAN [5], WiFi [6], ZigBee [7] and others.

3) *Middle-ware layer:* Several IoT devices in the same domain communicate with the same compatible device, this layer makes possible to extract the information sent from different hardware equipment, to translate it into a service information, for addressing, and denomination of the requested service.

4) *Application layer:* It serves as an interface for the user to access to the collected information from the perception layer and to manipulate them according to the demand of the specific domain and process them in a processing system.

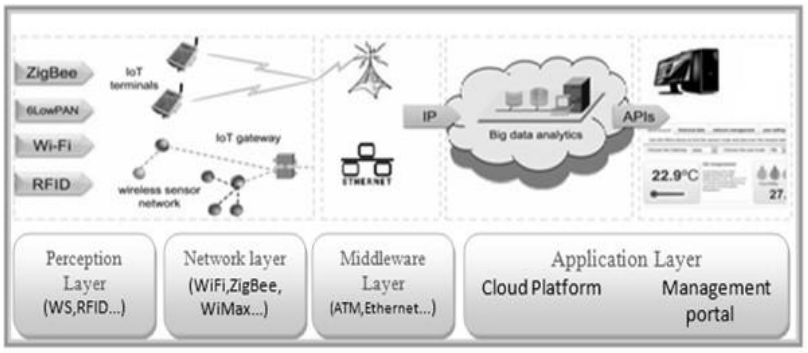

Fig. 1. Architecture of the Internet of Things

C. Domains of applications of the Internet of Things

There are a variety of application areas for the Internet of Things sectors, whether in the industrial world or in everyday life.

- **Medical applications [10]:** In the field of health, con- nected objects can serve several purposes. For example, they can be used as a monitoring device in form of a connected bracelet or connected watch which will make it possible to follow the physical activities of a patient at any time by informing for irregular signs. For people who take drugs connected objects can also inform when it's time to take the drugs. In addition, this could possibly inform the doctor of an emergency situation allowing him to locate the patient through the connected device.

- **Industrial applications [11]:** In the industrial world Internet of Things can considerably increase the perfor- mance and productivity of a factory. For example suppose that we have a

smart counter connected upstream of a production line and this counter lists in real time all the parts available in stock in a database, in case of shortage, it can automatically notify and send a message to the POAG system, which in turn will perform a procurement operation, for example.

- **Well-being and comfort [13]:** Home automation or smart home. Imagine for a moment that your thermostat is able to go on its own depending on the location of your car allowing you to warm up once you get home. Also, imagine that your fridge is informing you when you need to buy milk or that it can create a personalized shopping list based on your most purchased items. Or tell you when your food is about to expire.

3 IOT SMART HOME ECOSYSTEM

The origin of the word home automation means a set of processes dedicated to the reduction (or elimination) of the effort and intervention of the person in the performance of a function. In the field of residential home automation, equip- ment are used to automate applications relating to: occupant safety, their communications, energy management (lighting and heating control), multimedia entertainment and others. We can therefore distinguish two areas of application of home automation:

- **The management of energy flows:** water, gas, electricity, when talking about domestic functions such as heating, lighting, ventilation, control of household appliances.

- **Data flow management:** telephone, radio, television, and computer.

This brain dedicated to the management of the house makes life easier and more enjoyable for its occupants. In addition, intelligent heating and lighting management can have a sig- nificant impact on energy conservation without compromising the comfort of the home.

A. Domestic comfort

1) A house that simplifies everyday life: All actions per- formed mechanically can be automated and integrated into pre-programmed scenarios. Eliminating tedious and repetitive gestures that can save us time and peace of mind.

- **The home speaks to us:** Transmissions of information via mobile phone, desktop PC or laptop by a voice message, an e-mail or SMS.

- **We talk to the home:** It can be to control the voice lighting circuits or to trigger scenarios. We can activate at a distance the heating, the alarm, the shutters, and others.

2) Autonomous house: The smart home allows a self su- pervision of the house system and reaction in case of need.

- **Supervision:** An autonomous house must be able to detect the changes of state of the systems to be monitored, in particular: breakdown of household appliances, mal- function of the heating system, change of weather condi- tions, power failure, attempted intrusion, risk household (leakage of water or gas, for example).

- **Reactivity:** examples of reactivity of the system: The banana awning rolls thanks to a wind or rain sensor. The shutters, on the south side, go down when it is too hot. The water supply is shut off automatically by a solenoid valve in case the watering system is triggered by the information provided by humidity sensors or a local weather forecasting system via the Internet, the intensity of the lighting adapts to the external brightness.

3) A secure house:

- **Ant-intrusion:** The objective is to set up a series of peripheral, perimeter and interior devices capable of de- tecting any intrusion or presence attempts. The detection causes a series of determined actions involving sound alarms, indoor or outdoor, as well as bright alarms. The central transmits the incidents to recipients (telephone central station).

- **Domestic hazards:** Here are some examples of domestic hazards: Fire, toxic fume release, freezer temperature increase, flood, gas leak.

B. Home automation systems operation

We distinguishes in every home automated system two fundamental parts which are: the Information Chain and the Energy Chain.

- **Information chain:** to operate, automatic system must be able to acquire setpoints from the user, but also the system itself and its environment, process these information and transmit orders to the energy chain.

- **Energy chain:** An automatic system must be supplied with energy to achieve its functions. The orders coming from the information chain lead to distribute the energy, to convert it and

finally to transmit it.

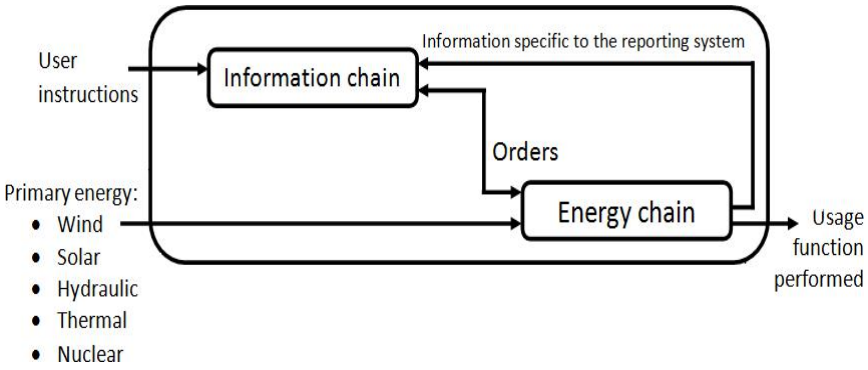

Fig. 2. Diagram of operation of an automated system

1) Example: The central heating of a house: A central heating system provides warmth to the whole interior of a building (or portion of a building) from one point to multiple rooms. When combined with other systems in order to control the building climate, the whole system may be an HVAC (heating, ventilation and air conditioning) system [14].

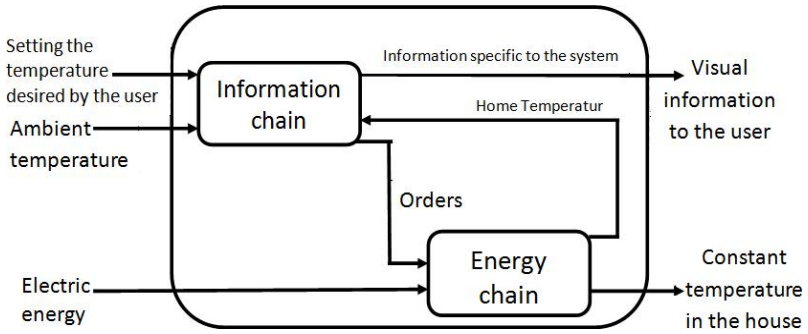

Fig. 3. Diagram of operation of the central heating of a house

Description of the Information Chain diagram:

- The information acquired via the temperature sensor, the button or the drive is sent directly as a signal based on a wireless or wired communication protocol at the input interface of the processing unit. Input interface is often used to adapt the signal.

- This processing unit can be a micro-controller, a local computer or a remote server.

- After the processing of the information by the algorithms designed by the operator, the result is flooded by the output interface of the processing unit using a wireless or wired communication protocol, in one hand, in the form of order to the Energy Chain, in the other hand, to communicate it to the user using an actuator [16] (display, speaker or indicator).

- The communication between the acquire part, the inter- faces of the processing unit, the communicating part and the distributing part of the Energy Chain is made often with wireless communication protocols, we distinguishes on our work a WLAN protocol [17].

Wireless Local Area Networks (WLANs): spans a relatively small area such as a building or a group of buildings, the most modern WLANs are based on IEEE

802.11 standards and marketed under the name of WiFi [6]. WiFi: is a wireless communication technology for wireless local area networks with a high data rate and band with and a large coverage area.

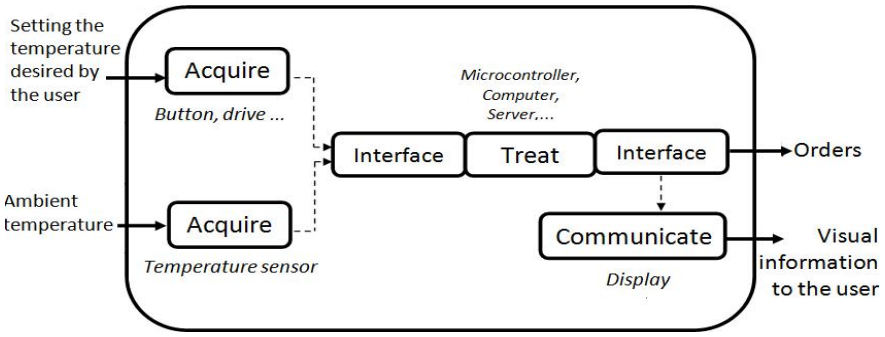

Fig. 4. Diagram of the information chain

Description of the Energy Chain diagram:

- It starts with a power box that receives input energy (primary energy: wind, solar, nuclear, ...) and produces an output energy: often via EDF in 230v or 400v which can be either an energy electric, pneumatic, hydraulic, or other.

- The distributing part allows the piloting of power energy. ”Power tap” for example: Contactor, solenoid valve, pneumatic distributor, relay, transistor, or other. This allows to have a controlled energy.

- The convert part makes it possible to transform the controlled energy by using a motor, a cylinder, a heating resistor, or other.

- The transmit part allows you to manipulate the transform- ing energy using a bevel gear, a reducer, or other.

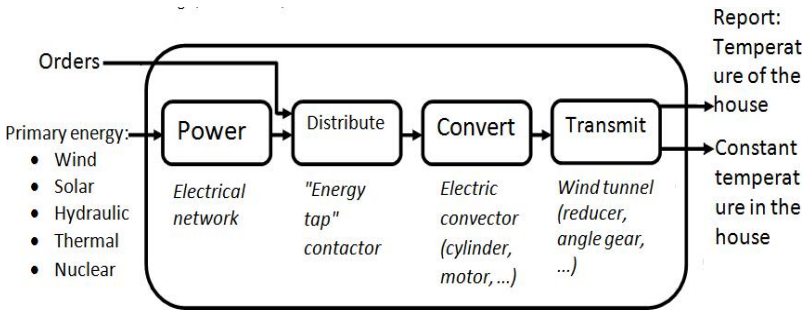

Fig. 5. Diagram of the energy chain

C. In general

Every automated home system is based on:

A sensor that is an element able to detect (with or without contact) a physical phenomenon in its environ- ment (presence or displacement of an object, heat, light,...) and to report this phenomenon to the programmable part in form of an input (for example logical input: 0 or 1), using a wireless communication protocol, in our simulation scenario we are based on the WiFi protocol[6], and for a wired solution we used the Ethernet protocol. We can find in the market a lot of sensors: smoke sensors, temperature sensors, presence sensors and other. There are three types of sensors in the market they can be: analog output sensors, digital output sensors or sensor with logic output.

– **Analog output sensor [18]:** Output in the form of a voltage which varies according to the input to be measured, for example the temperature sensor.

– **Digital output sensor [19]:** Output as a continuation of 0 and 1, 1 bit can be coded on 1 byte (contains 8 bits), example the Anemometer.

– **Sensor with logic output [20]:** Output in the form of 0 or 1, also called ”all or nothing” sensor, for example Infrared barrier, push button, limit switch, presence sensor, and others.

- For the programmed system or the programmable part, in our IoT Smart Home ecosystem we used a remote server installed in the Internet, so we can know the state of our house even if we are not in the house, the programmable part requires an operator, is a person who gives instructions to the system and who is able to understand the signals that the system returns. In programming, a sensor is in logical state 1 when it is active (it picks up something) and conversely in state 0 if it captures nothing.

- The actuators [16] can not be connected directly to the output of the control part. It's the utility of an interface, which plays the role of "switch" controlled by the control part. It manages all these exchanges of information.

- The result of the programmable part is sent to the actua- tors [16] (cylinder, motor, siren or loudspeaker, indicator or display,...) via the interface, using also often a wireless communication protocol, in the form of an input (logic: 0 or 1), the actuators execute consequently the orders received from the programmable part.

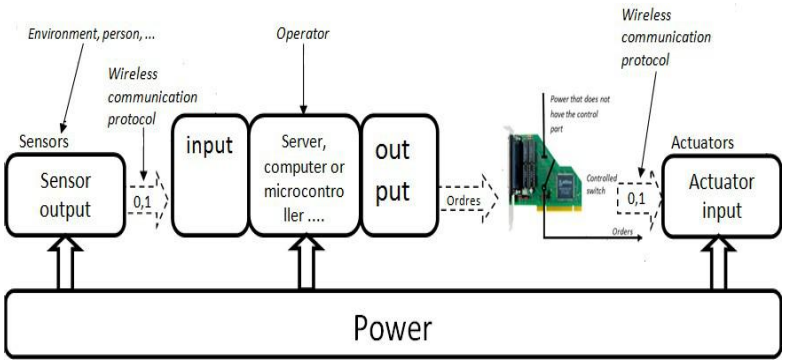

Fig. 6. Diagram of a Home Automation System

4 STATE OF THE ART ON NETWORK LAYER OF THE IOT ARCHITECTURE

In the field of wireless and wired networks, a commu- nication protocol defines the rules and the communication procedures of the physical and MAC layers of the OSI model on a medium or physical channel. It allows to connect an object to a wired or wireless network. In addition, if this network includes a gateway, that is to say a device connected to both the network and the Internet, then this object [21] can transmit and receive data to the Internet.

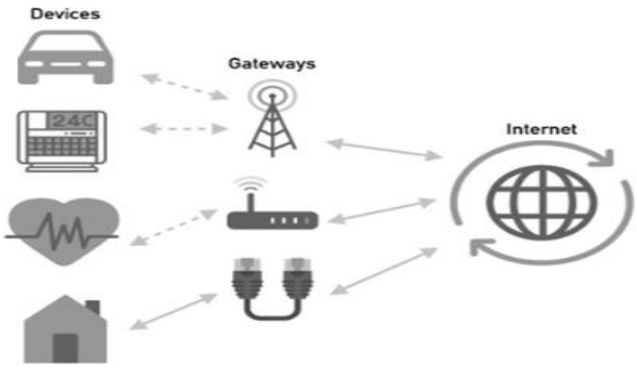

Fig. 7. Principle of a connected object

When talking about connecting object [21] it usually evokes wireless communications and technologies such as WiFi [6], Bluetooth or cellular. However, this is only the tip of the iceberg because there are several physical media and dozens of protocols with different characteristics (throughput, range, power consumption, price, etc.).

A. Decision Support Settings

It is important to know certain parameters that make it possible to understand the operation of the protocols and to provide elements of answer.

1) Physical support: A physical medium is through which the transmission of information is carried out. This can be divided into two categories:

- Wireless communications: This includes radio communi- cations (cellular, Bluetooth, WiFi, SigFox [8], LoRaWAN

[5] ...) but also bright communications (the Li-Fi protocol uses the frequencies of the light spectrum to transmit information), this type of communication is used in hospital environments [22] because it avoids the nuisance caused by radio communications.

- Wired communications: The wired communications in the IoT are mainly carried out on the three supports:

– Twisted pair cable (for Ethernet networks) [23]: widely used in office environments, such as remote printers.

– CPL: it is particularly used in home automation and in smart meters.

– Optical fiber [24]: ideal for very high speed commu- nications.

2) Topology: The topology is also one of the parameters to take into account in our evaluation. Indeed, it corresponds to the logical architecture of a network, defining the links between the objects [21] of the network and a possible hierarchy between them. The main typologies used in telecom- munications are:

Mesh Topology [25]: In a Mesh topology, an object called a node is connected to one or more other nodes of the same network. This forms a mesh in which an emitted data is relayed potentially by several nodes before reaching its destination, this is called a route. As time goes by, nodes can establish new routes based on their states (for example, failures) and characteristics of the physical medium (for example, a decrease in noise). It is also possible to prioritize a mesh topology [25] to define levels in order to manage the network more easily. In this case, the parent node is the master of the network. This is called cluster tree. This topology is widely used in home automation, where some objects fail to connect to the gateway because of distance or noise and surrounding obstacles. This is also applied to smart metering, for example in the framework of the Linky project led by Enedis.

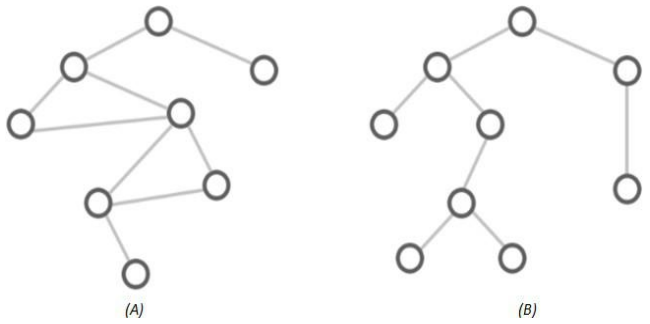

Fig. 8. Mesh topology classical (A) and hierarchical (B)

- Star topology [26]: The objects [21] are connected to a gateway called hub or router. Its role is to ensure communication between the nodes of the network. This type of topology makes it easy to add or remove nodes without impacting the rest of the network. In addition, all the intelligence of the network is concentrated on a single node which makes it possible to manage the network more easily. However, if the hub is experiencing a technical problem, then the entire network is down. This

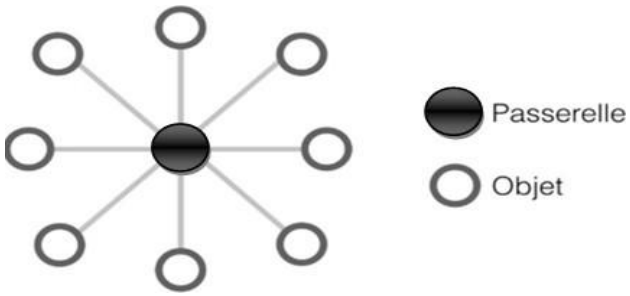

Fig. 9. Star topology

type of topology is widely used in indoor environments (especially with WiFi) or in the context of portable technologies (clothing, bracelets, etc. connected) where the smartphone acts as a gateway.

- Cell topology [27]: A cellular topology is based on a division of a territory into zones called cells. The radius of a cell can range from a few hundred meters (urban) to several kilometers (rural). At the heart of the cell, an antenna provides the radio link between objects [21] and the Internet. The principle is synthesized in the following figure where each cell uses a radio frequency band different from neighboring cells. This type of topology is the basis of mobile networks (eg 2G/GSM, 3G/UMTS, 4G/LTE [28], 5G [29] and 6G).

Fig. 10. Cell topology

- Broadcast topology: In this type of topology, an object transmits a message without specifying a particular re- cipient. What makes the message is analyzed by all the objects that have received the message correctly, that's why we talk about broadcast as shown in the image below. This operation is suitable when you want to reach several devices without distinction, this is for example the case of LoRaWAN [5] and Sigfox protocols [8].

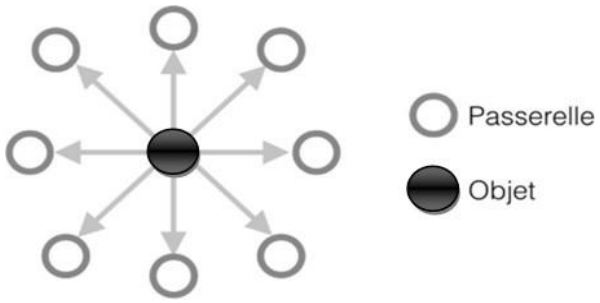

Fig. 11. Broadcast topology

3) Scope: The transmission range of a signal is the maxi- mum distance at which a receiver is able to decode the signal, it can be divided into three categories:

- Short: a few meters to a hundred meters
- Average: hundreds of meters to a few kilometers
- Long: up to several tens of kilometers

The range of a signal depends both on the value of the maximum transmission power provided by the protocol and on the physical environment. In fact, apart from radio com- munications that make it possible to reach very long distances, the physical environments that we have mentioned above only allow signals to be broadcast up to a few hundred meters away. To overcome this limitation, a set of repeaters are generally deployed to relay the signal. Therefore, it is important to judge how far your object [21] will be from the nearest bridge. Depending on this value, it will be obvious that some protocols will be more suitable than others.

4) Debit: The flow is mainly limited by the modulation of the signal and the width of the frequency band: the wider it is, the higher is the flow rate. This is explained by the fact that there are several frequencies on which it is possible to transmit or receive several bits of information simultaneously. One example is the NB-IoT protocol [28], which operates on the same frequencies as the LTE protocol [28], but on a narrower band. As for the scope, we can also identify flow categories:

- Low bit rate: up to several tens of bit/s.
- Medium throughput: up to several hundred Kbit/s.
- Broadband: Several hundred Kbit/s and up to several tens of Mbps.

- Very high speed: Several hundred Mbps or even several Gbit/s.

5) Comparative: The tables below groups together the main protocols used in IoT projects, and in column the parameters that we defined previously.

TABLE I TECHNICAL COMPARISON BETWEEN THE PROTOCOLS USED IN IOT

Technology	**Physical support**	**Topology**	**Scope**	**Debit**
3G	Wireless	Cellular	Average	Broadband
4G	Wireless	Cellular	Average	Very high speed
LTE-M	Wireless	Cellular	Long	Medium throughput
SIgfox	Wireless	Broadcast	Long	Low bit rate
NBIoT	Wireless	Cellular	Long	Low bit rate
WiFi	Wireless	Star	Short	Very high speed
ZigBee	Wireless	Mesh	Short	Low bit rate
NFC	Wireless	Star	Short	Medium throughput
LiFi	Wireless	Star	Short	Broadband
Optical fiber	wired	Mesh	Average	Very high speed
CPL	wired	Mesh	Average	Medium throughput

5 RELATED WORK

In the article [9] we talk about the network architecture of the Internet of Things in general, and we define the four main layers that are: the perception layer, the network layer, the midelware layer, and the application layer. We define after the SDN technology that allows to remove the control function present in the network infrastructure equipment that can be: RFIDs, sensors, switches, routers or even firewalls, and centralize it it into a single controller, the network equipment are thus responsible only for the data transfer function, leaving the data control at the upper layer: the control layer where the SDN controller is located. With the combination of these two network technologies we came out with a new SDN-based IoT architecture (SDIoT) that take advantage of the global view of the network by the SDN controller to determinate the optimal network polices depending on the types of data that the network have to transmit, and convert those policies on network instruction and implement them directly on the network equipment. The SDIoT architecture reduce the con- sumption of network resources and increase its performance. Without taking about any communication protocol used in the IoT in particular.

In the article [12] we focus on perception layer of the IoT architecture which is composed of objects that can collect information from the physical environment in analog signal, convert it into digital signal, process this information, stoke it, and finally transmit it to the dedicated server hosted in the Internet for decision-making, these objects can be smart phones, RFID, smart cars, Wearables and others, in this article [12] we distinguish the wireless sensor networks that have a very high faculty of perception and transmission of the collected data from the physical environment through the network. A wireless sensor network is composed mainly of wireless sensors, a wireless sensor is composed of: Sensing unit, Power unit, Processing unit, External storage, and Radio unit. For the transmission of the collected information we distinguish:

- Wireless Personal Area Networks (WPANs) like the ZigBee protocol.
- Wireless Local Area Networks (WLANs) like the WiFi protocol.
- Wireless Metropolitan Area Networks (WMANs) like the WIMAX protocol.
- Wireless Wide Area Networks (WWANs) for example, cellular networks: 4G LTM, 5G, or LPWAN networks such as: SIGFOX and LORAWAN.

In this work [12] we have detailed the operation mode of the WIMAX protocol and we analysed

its performance, always without a direct application of IoT in a particular field.

In the article [15] we applied the IoT to the health care sector to create a new IoT Ehealth ecosystem, based on the Arduino microcomputer that allows to collect health information from a patient and send it to the Internet for decision making. The microcomputer can gather ten health sensors (blood pres- sure, cardiac, temperature, position of the patient, glucometer, sound, others and even a warning button), the set of signals generated by the sensing units will be processed locally by the processing unit of the microcomputer then transmitted through the access and core network to the health processing system hosted on the Web server located in the Internet. Our IoT Ehealth ecosystem can make us prevent against any threat that can make us to lose our patient and allows a quick intervention of the emergency in case of need. This time to allow access at the collected heath information to the right server in the Internet, to be shared by the family of the patient, the hospital which contains the specialists and the emergency center, we were based on the WWAN network which makes it possible to cover a large geographical area, and especially the UMTS cellular. In this article [15] we talk about UMTS in the IoT network layer as a protocol that allow access at the health information of the patient to the Internet, but we dont talk about the routing of this information inside the IoT Midelware layer.

In this article we talk about the IoT Smart Home ecosystem that make the traditional homes more secure and enjoyable for its occupant. To collect the information from the home sensors we used the WiFi and the Ethernet networks and we compared their performance, this time we detail the middle-ware layer that interconnect between different networks and allow data to be transferred to the right server via the Internet with a grantee of the quality of service, we distinguished the MPLS network, in the next section we detail the mode of operation of the MPLS network, which is a resent technology used by the operators that allows data to be transferred with quality of service based on label switching and traffic engineering.

6 MPLS PROTOCOL: MODE OF OPERATION

A. Objective of MPLS

Initially MPLS (Multi-Protocol Label Switching) [33] was deployed to reduce packet processing time in routers to gain performance.

Currently MPLS offers traffic engineering (MPLS-TE) and the implementation of effective VPN.

MPLS allow the construction of efficient optical networks (GMPLS and -MPLS).

B. The concept of an MPLS network

MPLS allows a strict separation between routing and for- warding.

Layer 3 is actually responsible for routing, and layer 2 is responsible for forwarding.

Routing consists of processing information to build a routing table. Forwarding makes the passage of a packet received on an input port to the correct output port based on a table of forwarding.

MPLS [33] is intended to be at the top of multiple link layers, specifications currently exist for the following link layers:

- ATM [30]: label contained in the VCI / VPI field of the ATM header.
- Frame Relay [31]: label contained in the DLCI field of the FR header.
- PPP [32] / LAN: uses a 'shim' header inserted between L2 headers and L3.

Translation between different types of link layers must be supported, MPLS can be interfaced with several Layer 3 protocols IPV4, IPV6, IPX, ...) or layer 2 (ATM, FR, PPP

...).

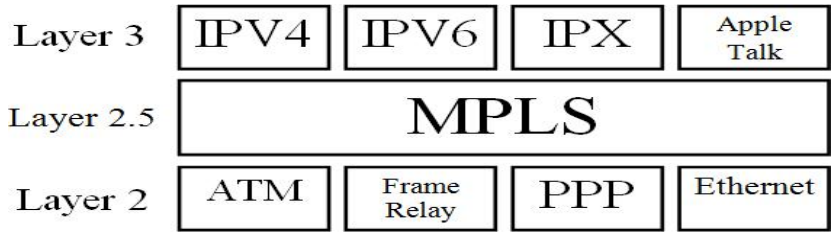

Fig. 12. The layer of the MPLS protocol

C. MPLS terminology

1) Architecture of the MPLS network:

- **LSP Label switch path :** Path established through the MPLS domain. Packets associated with the same FEC by the Ingress LER will follow the same path up to Egress LER. (Virtual circuit concept), independently of the Layer

3 protocol. These paths can be statically or dynamically established.

- **Ingress LSR :** Examine incoming IP packets, classify the package in an FEC, and generates the MPLS header and assigns it the original label.

- **Egress LSR:** Removes the MPLS header.

- **LSR :** These are routers that switch Labels inside the MPLS network. Routes MPLS packets using tag switch- ing, able to route native IP packets, execute one or more IP routing protocol, participates in MPLS control protocols.

- **Forwarding Equivalence Class FEC :** The FEC de- termines which packets will be associated with an LSP. Currently, an FEC establishes an association based on the IP address destination. Ex: For all the packets having as destination the network B.0 put label 50. An FEC can also establish an association based on another field or combination of fields. Ex: For all packets destined for the B.0 network, whose ToS = 6 field, whose destination TCP port is 503 and coming from the input interface 2, set tag 60. The association is governed by Ingress LER.

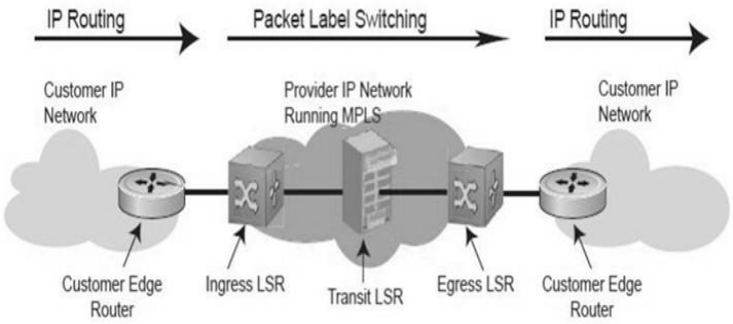

Fig. 13. Architecture of the MPLS network

2) The basic principle of MPLS:

- In MPLS the IP header of the packet is analyzed once by the Router at the entrance of the network (ILSR).

- The Ingress Router assigns to each packet a class ”FEC” Forwarding Equivalent Class, identified by a ”Label”, the other routers switch the packet according to the Label without analyzing IP header.

- FEC is associated with a group of IP packets having the same properties (class of service, destination address, ...). All packages having the same FEC are going the same way and enjoy the

same treatment.

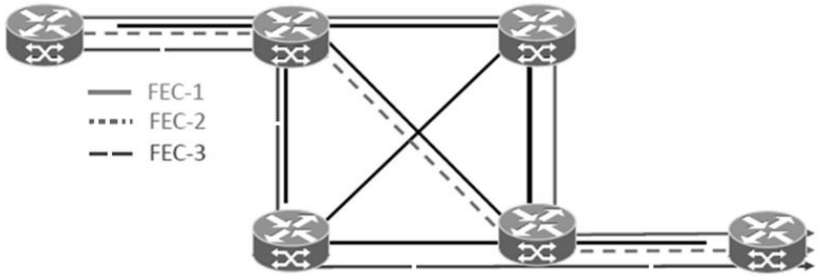

Fig. 14. Traffic specification of the MPLS network

3) *The label used in MPLS:* The MPLS header is a 32 bit identifier for identifying an FEC, the label has a local meaning,it transported either: in a ”shim” header between the headers of layers 2 and 3, or as an existing field of the layer 2 header such as VPI / VCI in the ATM or DLCI for Frame Relay, the Ingress switches add a label to the IP packets and the MPLS switches (LSR) transfer them based on of the value of the label, the Egress switches deletes the labels and routes them to the base of the IP address.

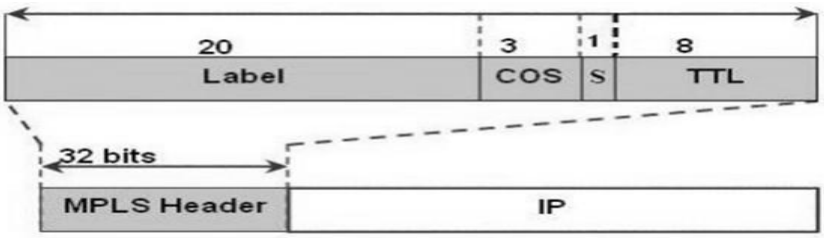

Fig. 15. Composition of the MPLS Header

4) *Label distribution:*

- LSRs rely on label information to switch packets through the MPLS backbone.
- Each router, when it receives a tagged packet, uses the label to determine the interface and the output label.
- For this purpose, label distribution protocols are used such as: Label Description Protocol (LDP), Border Gate- way Protocol (BGT-TE), Resource Reservation Protocol (RSVP-TE), Constraint-based Routing LDP (CR-LDP)...

. These protocols cooperate with higher-level IS-IS rout- ing protocols, OSPF, RIP, BGP,...

- LDP remains the most used in MPLS.

a) *Label Distribution Protocol LDP:* This protocol [34] defines a set of procedures and messages by which an LSR informs an other of the label attributed to a FEC. LSRs use this protocol to build the LSP across the network by getting based on the routing tables.

b) *Constraint-based Routed-LDP CR-LDP:* Extends Pro- tocol LDP to build LSPs with some constraints of traffic or QoS. Some fields are added to the protocol LDP describing the characteristics of the connection: Peak, Comitted, Excess.

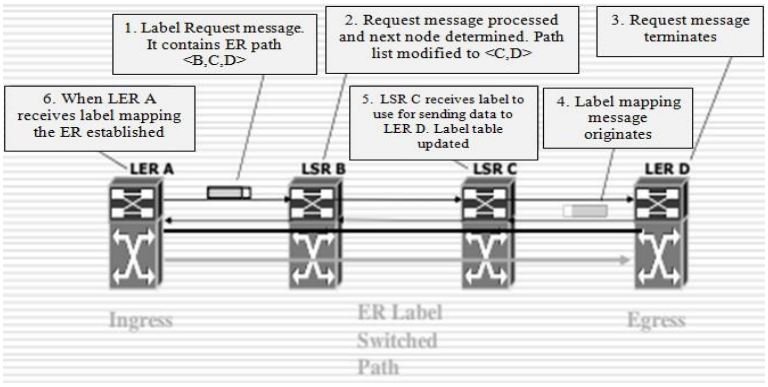

Fig. 16. Constraint-based Routed-LDP

c) *The Resource Reservation Protocol RSVP-TE:* RSVP has been modified to support QoS management capabilities within an MPLS network. With RSVP-TE, the recipient claims a path to the source with clean traffic conditions.

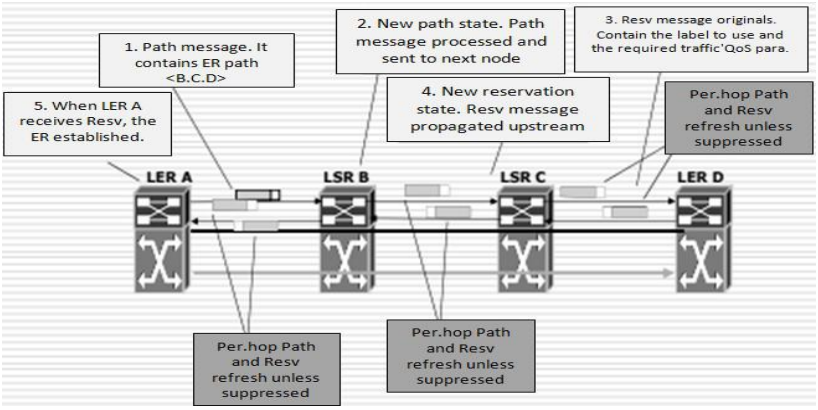

Fig. 17. The Resource Reservation Protocol

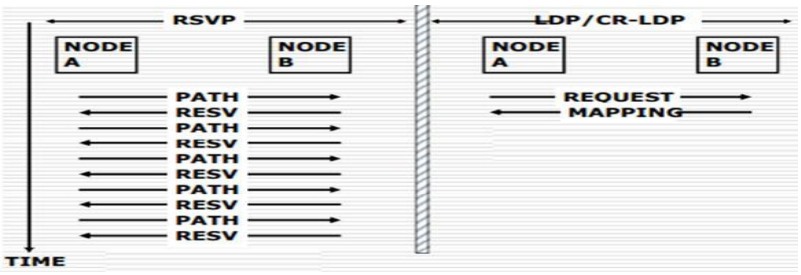

Fig. 18. Comparison between RSVP and LDP/CRLDP the protocols

7 SIMULATION AND PERFORMANCE STUDY OF THE IOT SMART HOME ECOSYSTEM

Our IoT Smart Home solution we compare a wireless net- work (WiFi protocol) and a wired network (Ethernet protocol [35]) in the network layer, to collect the home information sent by the different home sensors. We used five sensors, that can be a smoke sensor, a light sensor, a glass breaking sensor, a temperature sensor, and a garage door sensor.

The information generated by the sensors are sent through the gateway to enter to the MPLS core network, witch is the middleware layer in the Internet of Things architecture [36]. The Ingress LER add different labels to the parquets depending on the IP address of destination and the nature of the traffic. We have configured the the traffic engineering in our MPLS core network to route the HTTP traffic [37] and the data base queries using the green LSP (Label switch path), and to route the voice traffic [38] through the red LSP.

After label switching in the MPLS core network the traffic can enter to an other network via an other gateway, that contain the Web Server were it hosted the processing system of our Smart Home and contain also the data base management system, and the voice server responsible for the voice communication between the user and the automated home equipment.

When the programmable part of our solution detects an abnormal event such as a broken window, a lot of smoke, a not normal fall or increase of temperature, light on in the morning or after the time of sleep, or an not justify opening on the garage door, it can immediately active the right actuator [16], and warn the user on his laptop and his smart phone. Our simulation is done with the OPNET network simulator, it begin at 05:50:00 pm and ends at 06:48:20 pm, and it takes about fifty minutes.

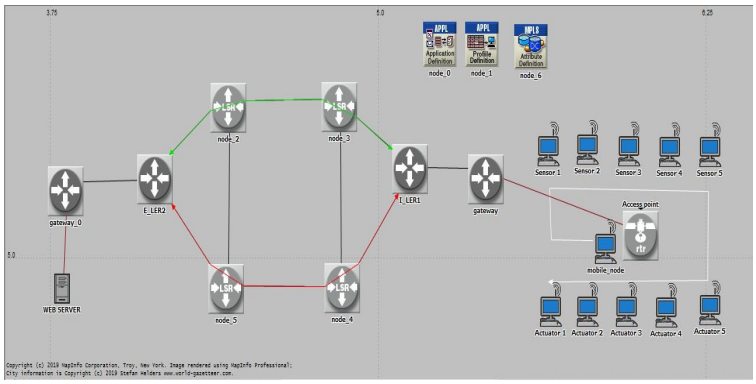

Fig. 19. Simulation scenario using WiFi based on MPLS

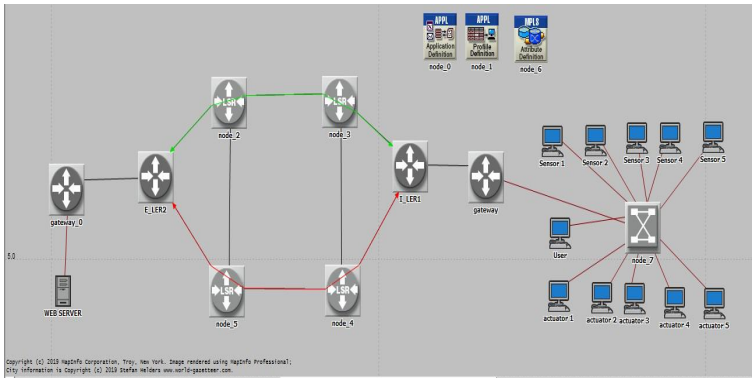

Fig. 20. Simulation scenario using Ethernet based on MPLS

A. Performance study of the WiFi protocol

1) *WiFi throughput:* Throughput refers to how much data can be transferred from one location to another in a given amount of time. It is used to measure the performance our WiFi network. The curve starts at 05:54:00 pm at 450000 bits / sec, after it does a little variation around this value, then it stabilizes until the end of the simulation.

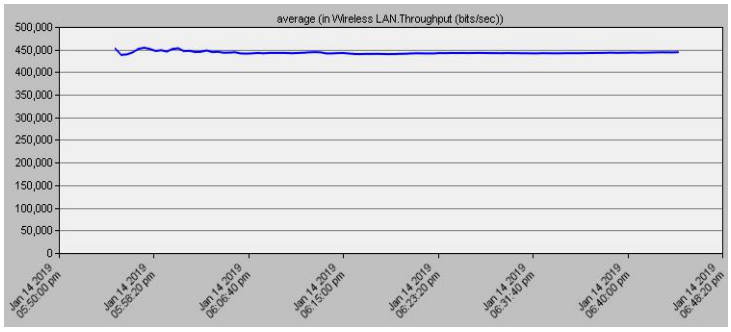

Fig. 21. Average of the WiFi throughput (bits/sec)

2) *WiFi Media Access Delay:* We measure access delay as the time from when the data reaches

the MAC layer until it is successfully transmitted out on the wireless medium. The reason for studying average access delay is that many real-time applications have a maximum tolerable delay, after which the data will be useless. The curve starts at 05:54:00 pm at a little less than 0.20 sec, then it starts to increase until reaching 0.225 sec and then stays on this value until the end of the simulation.

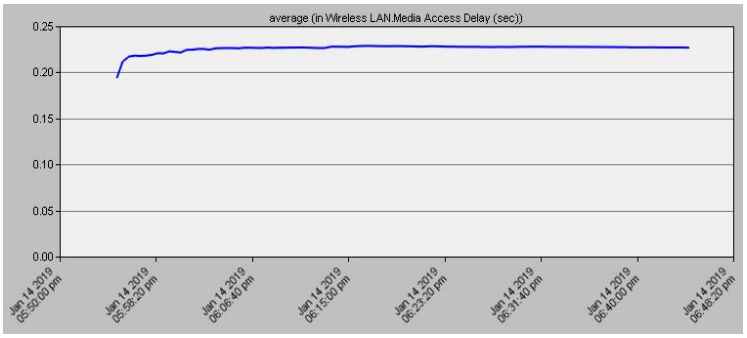

Fig. 22. Average of the WiFi media access delay (sec)

3) WiFi load: It's the number of frames that transit over the wireless network as a function of time. This curve starts at 05:54:00 pm to slightly more than 800,000 bits / sec then it makes a small evolution at 850000 bits / sec where it stabilizes is remains on this value until the end of the simulation.

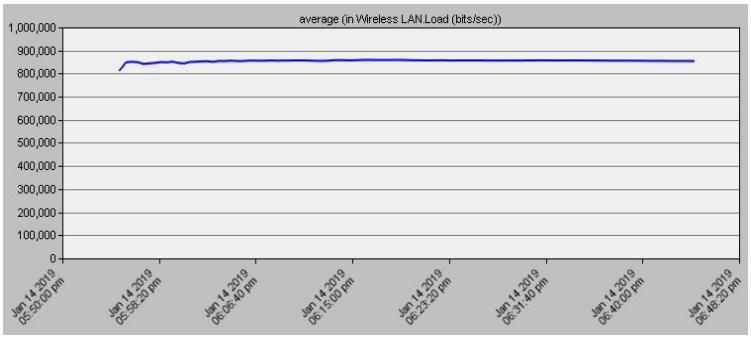

Fig. 23. Average of the WiFi load (bits/sec)

B. Performance comparison between WiFi and Ethernet based on the MPLS core Network

1) WiFi and Ethernet delay: Specifies how long it takes for a bit of data to travel across the local network from one node or endpoint to another. The two curves start around 05:54:00 pm, the curve that represents the Ethernet protocol starts slightly more than 0.00030 sec, it makes some variation then it stabilizes on this value until the end of the simulation. The curve that represents the WiFi protocol starts at 0.45 sec it make after an increase to reach 0.6 sec where it

stabilizes until the end of the simulation.

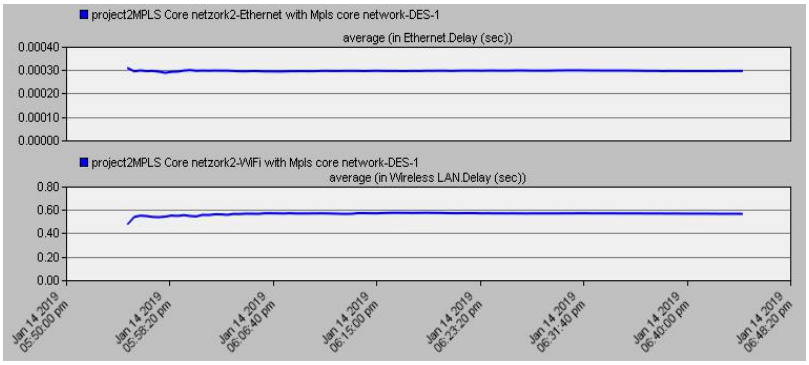

Fig. 24. Comparison between WiFi and Ethernet delay (sec)

2) Database queries: it's the comparison between the num- ber of queries sent by the sensors, to the database in the WEB server. Both curve starts around 05:54:00 pm. The curve that represents the Ethernet traffic starts at slightly more than 20 000 bytes / sec after it increases considerably to reach 32500 bytes / sec around 06:23:00 pm then it tries to stay on this value until the end of the simulation. The curve that represents the WiFi protocol starts slightly less than 20000 bytes / sec then makes a dimunission to receive 5000 bytes / sec until 06:06:40 pm after it continues dimunission to tend towards 0 to the end of the simulation.

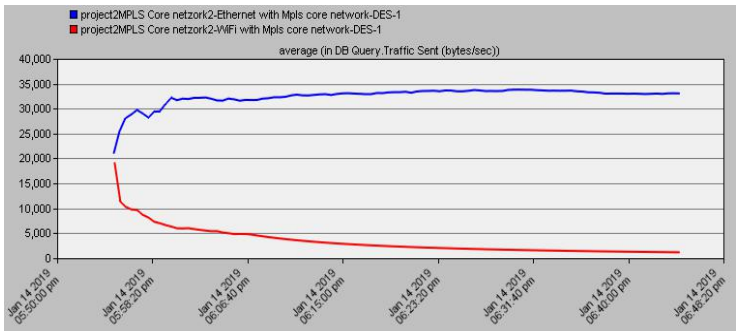

Fig. 25. Average of the queries sent to the Database (bytes/sec)

3) Using a HTTP application:

a) The HTTP traffic sent: Its the average of the number of bytes/sec of an HTTP application, sent by the sensors to the home processing system located in the Web server. The curve that represents the HTTP traffic send using the Ethernet protocol starts with 4500 bytes / sec after it decays to reach 2000 bytes / sec until 06:15:00 pm then it is still a slight decrease to reach 19000 bytes / sec end of the simulation. For the curve that represents the HTTP traffic it starts at 4500

bytes / sec after it makes a fast fall to reach 2000 bytes / sec at 05:56:00 pm then it still slings to get 1000 bytes / sec at 06:06:40 pm and after until the end of the simulation it makes a slight dimunition.

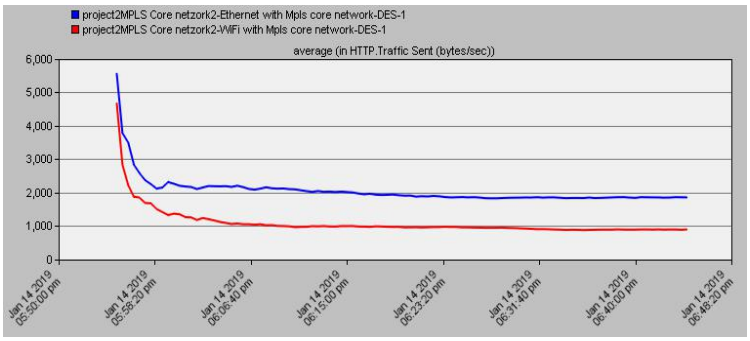

Fig. 26. Average of the HTTP traffic sent (bytes/sec)

b) *The HTTP traffic received:* Its the average of the number of bytes/sec of an HTTP application, received by the home processing system located in the Web server through the MPLS core network. For the HTTP traffic received is more or less the same as the HTTP traffic send, the curves that represent the Ethernet and WiFi protocols make the same rate of vaiations, we just notice that for the curve that represents the WiFi protocol is a faster fall to wait for less than 1000 bytes / sec at 06:06:40 pm it draws after up to 600 bytes / sec towards the end of the simulation.

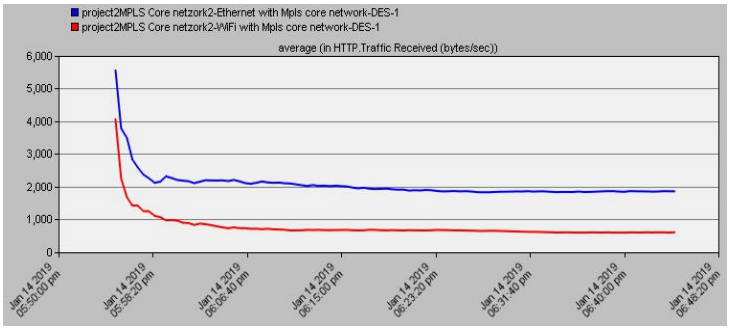

Fig. 27. Average of the HTTP traffic received (bytes/sec)

4) *Using a Voice application:*

a) *Packet end to end delay for a voice application:* Is the difference in end-to-end one-way delay between selected packets in a flow with any lost packets being ignored, for a voice application used by the sensors and the actuators. The two curve starts around 05:54:00 pm, the curve that represents you the Ethernet protocol it remains on the same value 0.060 sec throughout

the simulation, for the curve that represents the WiFi protocol it starts at a value a little less then 0.60 sec afte it makes a slight increase until the end of a simulatoin.

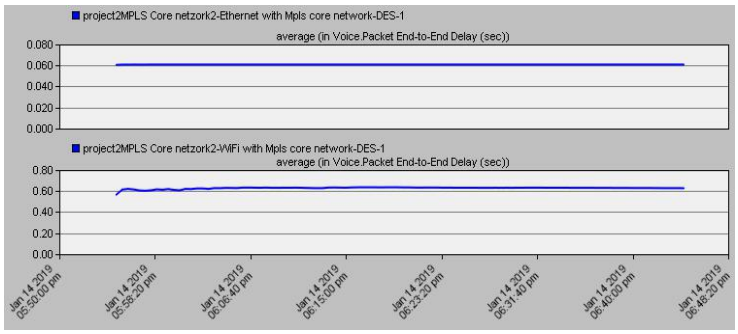

Fig. 28. Average of the voice packet end to end delay (sec)

b) *The voice traffic sent:* Its the the amount of the voice bytes/sec sent from the sensors to the processing system in the WEB server to the end of the simulation. The curve that represents the Ethernet protocol starts at a little less than 60000 bytes / sec, the curve that reprensents the WiFi protocol starts at a little more than 60000 byes / sec, the two curves have the same rate of variation and they overlap vres 06:06:40 pm to the value 70000 bytes / sec where it stabilizes until the end of the simulation.

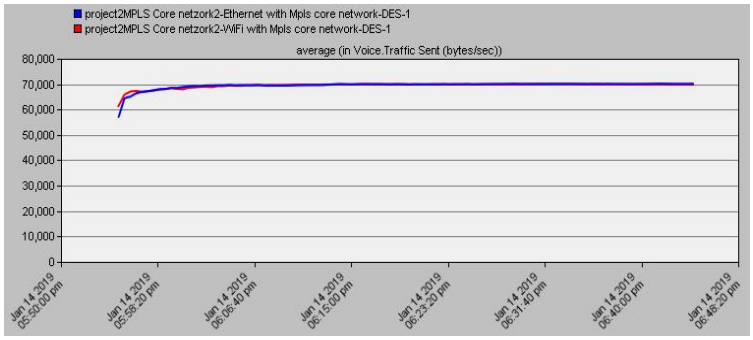

Fig. 29. Average of the voice traffic sent (bytes/sec)

c) *The voice traffic received:* Its the number of the amount of the voice bytes/sec received by the processing system in the WEB server to the end of the simulation. Both curves start at 05:54:00 pm. The curve representing the Ethernet traffic starts at more than 50000 bytes / sec and then increases to reach 70000 bytes / sec at 06:06:40 pm where it stabilizes and remains on this value until the end of the simulation. The curve that represents the WiFi protocol starts at more than 30000 bytes / sec then it makes a slight increase to 35000 bytes / sec where it stabilizes and stays on this value until the end of the simulation.

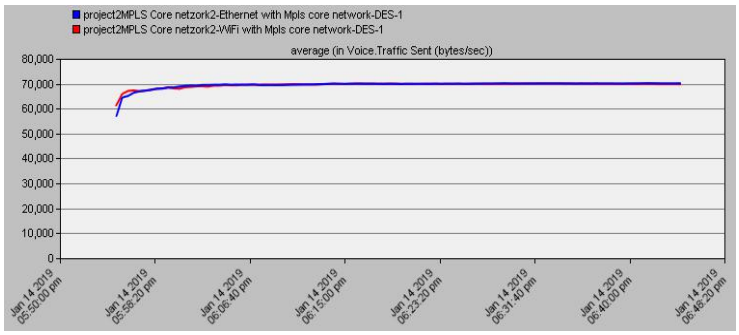

Fig. 30. Average of the voice traffic received (bytes/sec)

d) *The Voice MOS:* Is the Mean Opinion Score it's a measure of the quality used in telephony to express the quality of the voice applications. The two curves that represent the Ethernet and WiFi protocols are superimposed on this graph and stabilize on the same value 3.75 until the end of the simulation.

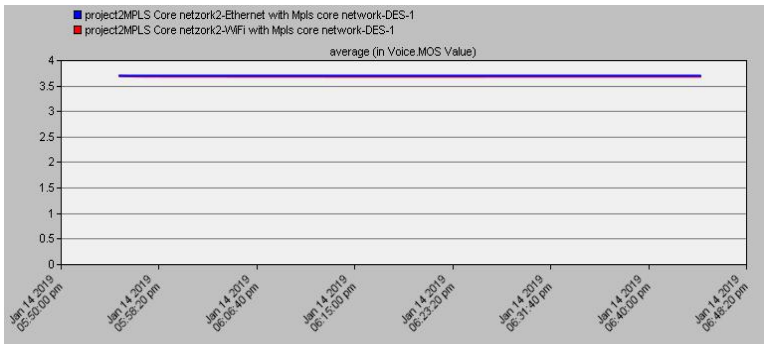

Fig. 31. Average of the Voice MOS

8 CONCLUSION

Smart cities today news an interconnection between a lot new of IoT ecosystems and an interoperability between a lot of network infrastructures, the IoT Smart home ecosystem is a part of this big development. The IoT Smart home ecosystem make the traditional homes more secure and enjoybel for its occupants, and for this its based on a lot of sensors and actuators. To connected all this sensors and actuators to each other and to the gateway we were based on a wired and a wireless technologies, the Ethernet protocol and the WiFi protocol, and to allow access at the collected home information to the right web server located in the Internet we were based on the MPLS core network. The performance study of the two technologies based on the same MPLS core network make the Ethernet protocol reacts better than the WiFi protocol in

the processing of a large amount of data but reduces the mobility of the user inside the home, taking into account that the generation of data by the sensors can be calculated and regulated in a Smart Home so as not to decrease performance in the case of using a WiFi network, the Wifi protocol remains the best solution for the future of the Smart Home.

REFERENCES

[1] BHUSHAN, Bharat et SAHOO, G. Routing Protocols in Wireless Sensor Networks. In : Computational Intelligence in Sensor Networks. Springer, Berlin, Heidelberg, 2019. p. 215-248.

[2] ZUMSTEG, Philip et QU, Huyu. Reading RFID tags in defined spatial locations. U.S. Patent Application No 10/248,817, 2 avr. 2019.

[3] BRADFIELD, Kelvin et ALLEN, Chris. User Perceptions of and Needs for Smart Home Technology in South Africa. In : Advances in Informatics and Computing in Civil and Construction Engineering. Springer, Cham, 2019. p. 255-262.

[4] DARROUDI, Seyed Mahdi, CALDERA-SÀ NCHEZ, Raül, et GOMEZ, Carles. Bluetooth Mesh Energy Consumption: A Model. Sensors, 2019, vol. 19, no 5, p. 1238.

[5] BASFORD, Philip J., JOHNSTON, Steven, APETROAIE-CRISTEA, Mihaela, et al. LoRaWAN for city scale IoT deployments. 2019.

[6] NAIK, Sulochan et D'SOUZA, Meenakshi. Efficient Power Saving Method for WiFi Direct Devices in IoT based on Hidden Markov Model. In : 2019 11th International Conference on Communication Systems Networks (COMSNETS). IEEE, 2019. p. 565-567.

[7] CHANG, Hong-Yi. A connectivity-increasing mechanism of ZigBee- based IoT devices for wireless multimedia sensor networks. Multimedia Tools and Applications, 2019, vol. 78, no 5, p. 5137-5154.

[8] MEKKI, Kais, BAJIC, Eddy, CHAXEL, Frederic, et al. A comparative study of LPWAN technologies for large-scale IoT deployment. ICT Express, 2019, vol. 5, no 1, p. 1-7.

[9] ZEMRANE, Hamza, BADDI, Youssef, et HASBI, Abderrahim. SDN- Based Solutions to Improve IOT: Survey. In : 2018 IEEE 5th International Congress on Information Science and Technology (CiSt). IEEE, 2018. p. 588-593.

[10] Zhang, Y., Sun, L., Song, H., et al. Ubiquitous WSN for healthcare: recent advances and

future prospects. IEEE Internet Things J. 1(4), pp. 311–318 (2014)

[11] HUANG, Junqin, KONG, Linghe, CHEN, Guihai, et al. Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mecha- nism. IEEE Transactions on Industrial Informatics, 2019.

[12] ZEMRANE, Hamza, ABBOU, Aiman Nait, BADDI, Youssef, et al. Wireless Sensor Networks as part of IOT: Performance study of WiMax- Mobil protocol. In : 2018 4th International Conference on Cloud Com- puting Technologies and Applications (Cloudtech). IEEE, 2018. p. 1-8.

[13] ZEMRANE, Hamza, BADDI, Youssef, et HASBI, Abderrahim. Internet of Things Smart Home Ecosystem. In : Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks. Springer, Cham, 2020. p. 101-125.

[14] WILSON, Mark W. Cooking appliance control of residential heating, ventilation and/or air conditioning (hvac) system. U.S. Patent Application No 15/637,916, 3 janv. 2019.

[15] ZEMRANE, Hamza, BADDI, Youssef, et HASBI, Abderrahim. Ehealth smart application of WSN on WWAN. In : Proceedings of the 2nd International Conference on Networking, Information Systems Security. ACM, 2019. p. 26.

[16] RODGER, Sean, RODGER, Erwin, KOCH, Rob, et al. Actuator position sensing. U.S. Patent Application No 10/222,233, 5 mars 2019.

[17] CHEW, Daniel. Protocols of the Wireless Internet of Things. 2019.

[18] DAI, Feng, REBER, Daniel, et EMERY, Jean-Christophe. Analog sensor with digital compensation function. U.S. Patent Application No 10/215,617, 26 février 2019.

[19] CRAWLEY, Martin, SMITH, Michael G., GROSS, Irwin, et al. Ap- paratus having a digital infrared sensor. U.S. Patent Application No 16/127,182, 3 janv. 2019.

[20] STEWART, David A. Sensor logic control of gun camera. U.S. Patent Application No 16/193,458, 16 mai 2019.

[21] LAPUT, Gierad et HARRISON, Chris. SurfaceSight: A New Spin on Touch, User, and Object Sensing for IoT Experiences. In : Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. ACM, 2019. p. 329.

[22] KANG, Seungjin, BAEK, Hyunyoung, JUNG, Eunja, et al. Survey on the demand for adoption of Internet of Things (IoT)-based services in hospitals: Investigation of nurses' perception in a tertiary university hospital. Applied Nursing Research, 2019.

[23] MILLER, Joshua E., READ, Jon, OLIVERAS, Ovidio M., et al. Cu- mulative distribution of ballistic impact failures of common twisted-pair data cables at orbital speeds. International Journal of Impact Engineering, 2019, vol. 124, p. 61-66.

[24] DÍAZ, Camilo AR, LEITÃO, Cátia, MARQUES, Carlos A., et al. IoToF: A Long-Reach Fully Passive Low-Rate Upstream PHY for IoT over Fiber. Electronics, 2019, vol. 8, no 3, p. 359.

[25] YIN, Junjie, YANG, Zheng, CAO, Hao, et al. A Survey on Bluetooth 5.0 and Mesh: New Milestones of IoT. ACM Transactions on Sensor Networks (TOSN), 2019, vol. 15, no 3, p. 28.

[26] INVIDIA, Lorenzo, OLIVA, Silvio Lucio, PALMIERI, Andrea, et al. An IoT-oriented Fast Prototyping Platform for BLE-based Star Topology Networks. Journal of Communications Software and Systems, 2019, vol. 15, no 2.

[27] HUANG, Xina, ZHANG, Sheng, HU, Quandong, et al. Coupling Effect of Unit Cell Topology and Forming Orientation on the Ti6Al4V Porous Structures Fabricated Using Selective Laser Melting. Advanced Engineer- ing Materials, 2019, vol. 21, no 2, p. 1800737.

[28] LIU, Sicong, XIAO, Liang, HAN, Zhu, et al. Eliminating NB-IoT Interference to LTE System: a Sparse Machine Learning Based Approach. IEEE Internet of Things Journal, 2019.

[29] FROYTLOG, Anders, FOSS, Thomas, BAKKER, Ole, et al. Ultra-Low Power Wake-up Radio for 5G IoT. IEEE Communications Magazine, 2019.

[30] SAIRAM, Kanduri, SINGH, Chandra, VAMSI, P. Sai, et al. Broadband Services Implementation by Using Survivable ATM Architecture. Avail- able at SSRN 3355302, 2019.

[31] KURNIATI, Kurniati et DASMEN, Rahmat Novrianda. The Simulation of Access Control List (ACLs) Network Security for Frame Relay Net- work at PT. KAI Palembang. Lontar Komputer: Jurnal Ilmiah Teknologi Informasi, 2019, p. 49-61.

[32] LI, Qi, YUAN, Yitong, et YUAN, Jin. Research on the Construction of the Old Age Institutions in Shanxi Province Based on PPP Model. 2019.

[33] CHUNDURI, Uma S., TANTSURA, Evgeny, et AMMIREDDY, Amar- nath. Ospf extensions for flexible path stitchng and selection for traffic transiting segment routing and mpls networks. U.S. Patent Application No 16/077,837, 21 février 2019.

[34] BASHANDY, Ahmed R., FILSFILS, Clarence, et WARD, David D. Segment routing over label distribution protocol. U.S. Patent Application No 10/270,664, 23 avr. 2019.

[35] PANDEY, Bishwajeet, FARULLA, Giuseppe Airo, INDACO, Marco, et al. Design and Review of Water Management System Using Ethernet, Wi-Fi 802.11 n, Modbus, and Other Communication Standards. Wireless Personal Communications, 2019, vol. 106, no 4, p. 1677-1699.

[36] KAUR, Kiranpreet et SHARMA, Anil. Interoperability Among Internet of Things (IoT) Components Using Model-Driven Architecture Approach. In : Information and Communication Technology for Competitive Strate- gies. Springer, Singapore, 2019. p. 519-534.

[37] DA CRUZ, Mauro AA, RODRIGUES, Joel JPC, LORENZ, Pascal, et al. A proposal for bridging application layer protocols to HTTP on IoT solutions. Future Generation Computer Systems, 2019, vol. 97, p. 145- 152.

[38] KUMAR, Vinay, MOHAN, Sujay, et KUMAR, Rakesh. A Voice Based One Step Solution for Bulk IoT Device Onboarding. In : 2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC). IEEE, 2019. p. 1-6.