IoT EHealth ecosystem based on WWAN

Hamza ZEMRANE
Mohammadia School of Engineering
Lab RIME
Rabat, Morroco, 10 000
zemranehamza93@gmail.com

Youssef BADDI
ESTSB, UCD
lab STIC
El Jadida, Morocco, 24 000
baddi.y@ucd.ac.ma

Abderrahim Hasbi
Mohammadia School of Engineering
Lab RIME
Rabat, Morroco, 10 000
ahasbi@gmail.com

***Abstract*—The Internet of Things is perceived today as a key opportunity for commercial development in different sectors of activity. Ehealth is a new IoT ecosystem where several microcomputer with health detection capabilities can diagnose the state of health of a patient, to deduce if his condition is stable or if a need for medical intervention very fast is obligatory, to prevent against any threat that can make us lose our patient. Our work consist of connecting three Ehealth microcomputers, each one relayed to ten health sensors and an alert button, to collect the health information of three different patients in movement, and send it to the medical server in the Internet for decision making, using an UTMS network in the network access layer, and the ATM network in the core layer. The simulation of our IoT Ehealth Ecosystem is done using the riverbed modeler academic edition 17.5, and lasts for 60 minutes, the performance study is done in the physical and data link layers, in the application layer in case of using a Voice and HTTP applications.**

***Index Terms*—Ehealth, Internet of Things (IoT), Wireless Sensor Network (WSN), Low Power Wide Area Network (LPWAN), Universal Mobile Telecommunications System (UMTS).**

I. INTRODUCTION

The goal of Internet of Things is to facilitate human, by building a smart environment, based on smart object that have the ability to autonomously generate data from the environment in which they are deployed and transmit this data to the Internet for decision making. In the perception layer of the architecture of the Internet of Things the Wireless Sensor Network are an effective way to collect the physical quantities from the environment, convert them on digital quantities process these information, and transmit them to the Internet for further processing. The WSN can be applied to the health care to create a smart IoT ecosystem on the health sector, the sensors used on the Ehealth can measure, record and transmit health information like: blood pressure, heart tension, glucose, temperature, position of the patient and others to the database server in reel time, to know the state of health of the patient and to warn if necessary emergency, hospital consultant, and the family of the patient for quick a intervention, to prevent against any health threat that can make us lose our patient and have a rapid reaction in case of a serious health problem. Our IoT EHealth ecosystem is based on several health sensors connected to a microcomputer and a Wireless Wide Area network to transmit the collected health information of the patients to the Internet, to store them in the database server, process them in a processing system dedicated to the health care, and share them between the different stakeholders in the health field. In this article we give in the section two: a definition of the Internet of Things, an overview of its architecture, and its protocols, in the section three: we give the modules that compose a WSN node, WSN topologies, and WSN protocols, in the section four: the state of the art on WWAN networks, where we compare LPWANs, cellular networks and the new networks based on the existing cellular networks, and we give a technical comparison between the different technologies, in the section five: we make an application of WSN in smart Healthcare, and we give the EHealth goals, types of applications and portable objects that will be used, social interest of EHealth, application and data used in EHealth, priority use cases, and the technical tools, in the section six: we make a simulation with the Riverbed Modeler Academic Edition 17.5 to analyze the performance of our ecosystem at the physical and data link layers using UMTS porotocol, in the case of using an HTTP application and in the case if using a voice application.

II. 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 a smart environment using smart objects that can autonomously generate data from the environment in which they are deployed and transmit this data to the Internet for decision-making. The IoT devices are usually wireless sensors, smart phones, RFID [1], smart homes [2], 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 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.

B. Architecture of IoT

The architecture of the IoT consists of the following layers:

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

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 [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, denomination of the requested service, and management of the services.

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.

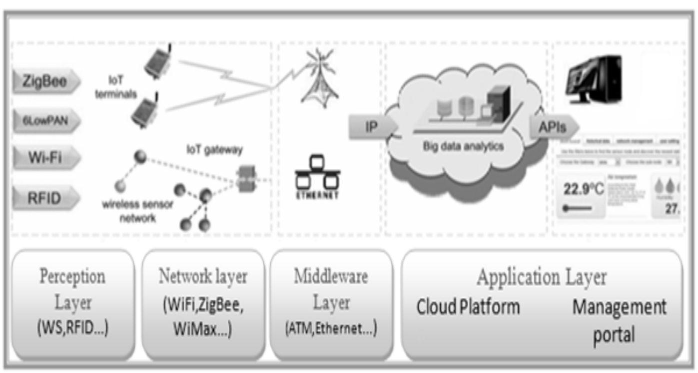

Fig. 1. Architecture of the Internet of Things

C. IoT protocols

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

- **Long-range networks :** such as Sigfox [8], LoRaWaN [5], or cellular technologies (GSM, 2G, 3G [9], 4G ...) are capable of transmitting 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 [6], Z-Wave, ZigBee [7], or Bluetooth Low Energy [4], allow data to be transferred over short distances, and are widely used in home automation or on the large wearable market.

III. WSN in IoT environment

Internet of Things can be defined as a paradigm where objects can communicate with each other in order to achieve a meaningful objective, the majority of those objects will be equipped with sensors and actuators, making the Wireless Sensor Network (WSN) a critical factor in the development of the IoT technology, WSN consists of sensors, with the ability of collecting and relaying the environmental information in an autonomous way. Unlike the wired solutions, WSN can be easier to deploy with a better flexibility and a reasonable cost. The wireless sensors are cheap, smart and with a limited resources. With the fact that IoT does not undertake an explicit communication technology, the integration of those wireless sensors in IoT networks will be a major factor in the development of IoT.

A. Sensor node

WSN can be defined as a network of sensor nodes, the hardware of each sensor node contains five modules.

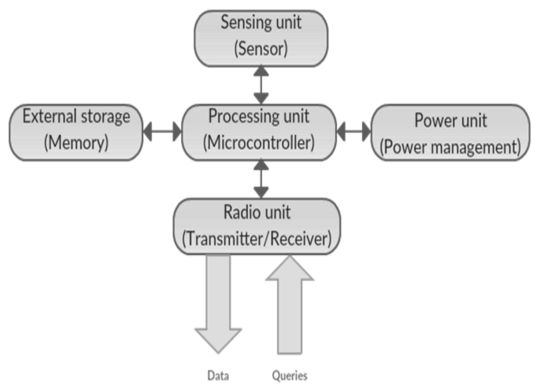

Fig. 2. Architecture of WSN node

- **Sensing unit :** collects information in a analog signal from the environment like: light, heat, movement, etc... and convert it to a digital signal.
- **Power unit :** offers the energy to other parts of the node.
- **Processing unit :** processes the data, the digital signal, sent by the sensing unit.
- **External storage :** two technologies of memory used here, a program memory which contains the system software (operating system, virtual machine, middleware, and application algorithms) and a non volatile user memory used for storing personal data.
- **Radio unit :** transfers the data to the control center trough a wireless medium.

B. WSN Protocols

Communications in WSN can be achieved over a wireless communication technologies, those ones differ depending on their link range, power requirement, mobility, and others.

- **Wireless Personal Area Networks (WPANs)**: is a short distance low powered network. IEEE has a specification which defines the physical and MAC layers for WPANs, we can cite 802.15.1 (Bluetooth) [4] as the most common protocol. **IEEE 802.15.1 :** Bluetooth smart or Bluetooth low energy (BLE) [4] is the recent version of Bluetooth suited for wireless personal area networks (WPANs) with an ultra-low power consumption and a lower communication range.
- **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. **WiFi [6]:** is a wireless communication technology for wireless local area networks with a high data rate and band with and a large coverage area.
- **Wireless Metropolitan Area Networks (WMANs)**: covers a geographic region area or region larger than WLANs, WMAN are based on the IEEE 802.16 standards as an example. **WiMAX protocol [10]:** is a wireless communication standard widely used on the gateway between the WSN and the Internet. The main goal of WiMAX [10] is to deliver wireless communication with quality of services (QoS) guarantees.
- **Wireless Wide Area Networks (WWANs)**: also called Cellular Network, Wireless local area networks often rely on Ethernet and short-range wireless routers, wireless WAN can use cellular network systems to send signals over a longer distance and lead to covers a large geographic area, we can cite GPRS, UMTS [11] and LTE [12] as the most popular. **General Packet Radio Service (GPRS):** is a best effort service derived from GSM in order to guaranty a certain level of QoS, with the introduction of packet data transport, data rate can reach 48Kbps.

TABLE I
WSN PROTOCOLS TECHNICAL DETAILS

	BLE	WiFi	WiMax	GSM
Layer	PHY and MAC	PHY and MAC	PHY and MAC	PHY and MAC
Range	10m	+100m	50km	35km-100km (per cell)
Type	WPAN	WLAN	WMAN	WWAN
Frequency	2.4GHz	2.4GHz, 5GHz	2GHz to 11GHz	850/900MHz - 1.8/1.9GHz
Data rate	1Mbps	54Mbps	70Mbps	14.4Kbps
Devices	7+	256+	1000+	Thousands

IV. STATE OF THE ART ON WWAN NETWORKS

A. LPWAN main actors: Sigfox and LoRaWAN

On the one hand the historical actor, Sigfox [8], French company of Toulouse. And on the other hand, LoRaWAN [5], an open protocol based on the chipset of the American company SEMTECH (whose technology was also initially developed in France). The French origin of these two options explains the presence of a strong ecosystem in France and in neighboring countries, including Belgium.

a) Sigfox: revolutionized the world of inter-object communications by offering low-speed connectivity that significantly reduced energy consumption from information-sharing. Sigfox [8] is positioned today as the first operator of long-range and low-speed network 100%100 dedicated to connected objects and has more than 1,500 relay antennas just on the French territory.

b) LoRaWAN: is a communication protocol initially developed by actors gathered around a consortium called the LoRa Alliance. The LoRaWAN [5] offers the advantage of having an interoperable standard. In fact, it allows communicating objects to connect to heterogeneous networks on private networks as well as on operated networks. The deployment of a private or operated LoRaWAN network [5] requires, as for the rest elsewhere, to be accompanied by service operators who master this communication protocol.

c) The main difference: LoRaWAN [5] is open to all members of the alliance, that is to say that an object that can connect to a LoRaWAN network [5] can technically connect to another LoRaWAN network (change from one operator to another for commercial reasons or roaming agreements by taking advantage of alliance members). An IoT player with a fleet that is only Sigfox [8] compatible will remain dependent on the Sigfox [8] network deployment. Between the two, an actor like QoWisio in France has deployed a similar network to Sigfox [8] while promising its users a possible compatibility with LoRaWAN networks [5].

d) Technical resemblance: While the market approaches of Sigfox [8] and LoRaWAN [5] are different, they are, on the other hand, very similar from a technical point of view. Both operate on the same ISM 868 Mhz frequency band (in Europe), unregulated frequency. Data transmission can be done over long distances, up to 15-20 km. This makes it possible to deploy a network faster and at lower cost. The principle is that the sensor (Sigfox or LoRaWAN) broadcasts data packets, which are received by all antennas in view. A consolidation is performed by the network, which then communicates the unique message to any platform dedicated to data processing via a ”callback” mechanism.

The fact that this frequency band is free imposes restrictions on its use. No more than 1% use of the frequency band for a sensor. This translates to a maximum of 140 useful 12-byte messages (”payload”) that can be sent via the Sigfox [8] or LoRaWAN [5] network from the sensor (Uplink). Sending data to the sensor (Downlink) is very limited, however 4 messages of 8 bytes (”payload” useful) per day maximum for Sigfox [8].

Also to know, As the frequency is not regulated, it means that interferences between users can exist, which poses a problem to the guarantee of the quality of service (QoS). This is one of the arguments put forward by the promoters of the competing NB-IoT [13] technology, which operates on a regulated frequency, thus without interference. Beyond these two French-speaking networks, little by little new technologies are emerging that will soon become serious competitors. The standards of NarrowBand IoT [13] and LTE-M [12] are among them.

B. Cellular networks 2G, 3G, 4G

However the cell did not say its last word in the world of IoT. It could even be that the emergence of LPWAN networks is boosting cellular connectivity as we know it until now. The era of GPRS is already far behind us. Since 3G [9], then 4G has arrived bringing with them much higher data rates than can provide LPWAN networks. And the 5G, which has planned to see the day by the end of 2019 promises to multiply by 1,000 the performance of networks. Objects equipped with M2M (Machine to Machine) SIM cards thus have the capacity to collect and transmit large volumes of data. An important advantage in certain business uses such as the remote surveillance sector or the maintenance of industrial equipment. 3G [9] and 4G for real time and big data rates, Sigfox and LoRaWAN for low bit rates? It's not so simple anymore. Because recently operators 3G [9] and 4G begin to offer IoT 3GPP networks that use conventional infrastructure to connect frugal connected objects. Still, the advantage of proprietary IoT networks should be threatened by these new low-bandwidth LTE networks [12] says the research firm ABI Research. The firm anticipates that even though LPWANs using LoRaWAN, RPMA and Sigfox technologies are dominant today, the imminent commercialization of LPWAN cellular networks using LTE Cat-M1 [12], NB-IoT [13] and EC-GSM-IoT technologies will quickly compete in the heart of the ecosystem.

1) Networks based on existing cellular networks: LTE-M, NB-IoT: In recent years, IoT networks have been supplemented by solutions based on existing mobile networks, which have already been largely amortized by traditional telephony applications. Their standards are set by the 3GPP group, a guarantee of compatibility and interoperability between networks, thus promoting the adoption by the manufacturers of objects through the respect of a recognized global standard. Carried by dedicated frequencies and licensed (thus not congested), these networks are supposed to ensure a guarantee of transport of the data. We will note two protocols, coming directly from this approach, without surprise pushed by the telecom operators:

- **LTE-M [12]** imagined to be the M2M solution derived from LTE [12], is a very short-term evolution allowing, by removing what is not useful to the IoT, to create a more energy-efficient protocol while addressing significant bit rates (1Mb / sec).
- **NB-IoT [13]** for Narrow Band IoT, has been natively thought of as a true LPWAN protocol that is much closer to the LoraWAN [5] or Sigfox [8] protocols in terms of autonomy. Currently undergoing 3GPP standardization, the latter is today seen as the most serious competitor to LoRaWAN. It makes it possible to use a narrow part of the dedicated LTE [12] frequency band, using only a part of a frequency band allocated to a conventional mobile connection, for a limited but sufficient bit rate in the context of the objects communication. The deployment is also facilitated since it only requires a software update of the antennas already deployed for the 4G.

C. The difference between private networks and operated networks

Private IoT communications networks have many advantages, despite the fact that some of their functionalities are limited compared to operated networks. Private networks offer above all the freedom to no longer depend on a particular telecom operator. Especially since the deployment of a private network is not necessarily more expensive, if not the investment in the purchase of antennas to relay the communications of your objects. What can however be expensive is the management and maintenance of this network for someone who is not the core business.

On the other hand the operated network has the advantage of being a network 100% controlled by professional operators and thus to guarantee optimal performance and coverage. Added to this is a value-added service and more flexibility, in contrast to the private network that will offer the opportunity for your connected objects to communicate on a well-defined perimeter.

Finally, in terms of information security, the two alternatives are equal. If the operated network offers a data security solution 100% controlled by the operators, the private network offers the possibility of deploying its own network while remaining fully sovereign of the data that transit and the use made of it. An alternative often favored by cities who want to deploy their own infrastructure of connected objects on the territory.

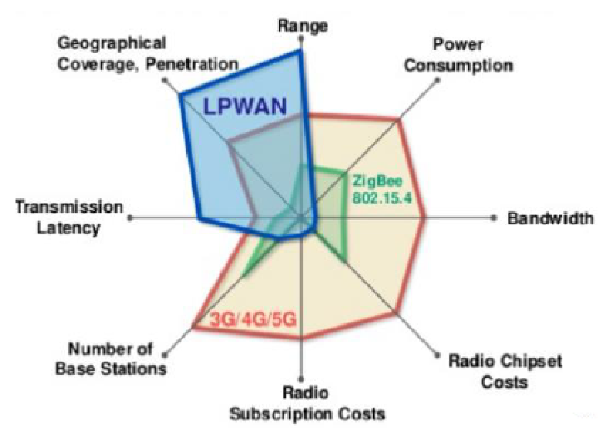

Fig. 3. Performance comparison between the cellular and LPWAN networks

TABLE II
COMPARISON OF EXISTING WWAN TECHNOLOGIES (SOURCE: MULTITECH)

Features	LoRaWAN	Sigfox	LTE Cat-M1 2017 (Rel13)	LTE Cat-M2 NB-IoT 2018 Rel13+
Frequency band	433 / 470 / 780 / 868 / 915 MHz ISM	868 / 915 MHz ISM	Licensed Spectrum (700 MHz-2.5GHZ+)	Licensed Spectrum (700 MHz-2.5GHZ+)
Modulation	DSS with Chirp	UNB / GFSK - BPSK	OFDMA	OFDMA
Bandwidth	125 - 500 KHz	100 Hz (EU) / 600 Hz (NAM)	1.4 MHz	200 KHz
Max data rate	293 - 50K bps	100 bps (EU) / 600 bps (NAM) 6 12 / 8 bytes Max	380 Kbps	250 Kbps going down / 22 kbps upload
Maximum number of messages per day	Unlimited, but some operators may limit	upload 140 msgs / day, download: 4 msgs / day	Not Known	Not Known
Maximum power	14-30 dBm	14-22 dBm	23 dBm	20 dBm
Liaison statement	153-161 dB	149-161 dB	155 dB + down	160 dB+
Communication channel	half-duplex	Limited half-duplex	half-duplex	half-duplex

D. The needs and cases of customer use, key to the development of IoT

The question of choosing the IoT network only makes sense for a given customer use case. Only the in-depth study of customer use cases to which optimized IoT solutions will have to answer we will dictate the choice of the most suitable networks. At a time when massive deployments of IoT networks are in full swing and interoperability is no longer a technological barrier, customers must now be supported upstream of their IoT program, on the expression of their needs as well as mastering IoT solutions on the market in order to choose the best solutions suited to their needs. Even if the packaged solution can be a guarantee of guarantee and simplicity of integration, gaps or limits can appear between the expected services and the services rendered end-to-end by the IoT networks. Thus a better understanding and control of the uses associated with an evaluation of their real gain would make it possible to democratize the IoT for the companies, and would probably help them to better transform the many IoT proof of concept (PoC) that the ecosystem knows into real industrial success.

V. APPLICATION OF WSN IN SMART HEALTHCARE

A. EHealth goals

Achieve better health and comfort in health care by facilitating effective and efficient care support using computer applications. Create a care sector framework to integrate financial and organizational applications into existing and new care arrangements. Make services via a platform available for mobile applications. Support the quality and accessibility of the health app. Support for care using health apps.

B. Types of applications and portable objects that will be used in EHealth

We will rely on applications and electronic devices that have the following characteristics: Communication-oriented applications (Applications that allow patients to directly ask online questions to a healthcare provider (telecoaching). Application allowing patients to access their electronic patient record, directly). Application as a reference book for patient health information (for health care providers and patients). Application and electronic monitoring accessories: applications and accessories that measure, record and transmit health parameters to a database. Medical devices: applications and electronic accessories for diagnostic purposes. Training application: application used for (continuing) training of healthcare providers or patients.

C. Social interest of EHealth

Improve the quality of care with a focus on prevention. Support care anytime, anywhere for both the patient and the caregiver. Increase the patient's autonomy. Promote technological innovation and entrepreneurship.

D. Application and data

- The data is:
  - Registered and processed locally in the mobile device (micro-computer)
  - Transmitted by the mobile device to a central platform for aggregating, processing and transmitting data.
- The purposes of data generation: we will set up a micro-computer with more than ten health sensors (blood pressure, heart rate, temperature, position of the patient, glucometer, sound, others and even a button alert), all signals generated will be processed by the sensor itself locally and transmitted to a database for further processing.

E. Priority use cases

- **Cardiovascular diseases:** risk management and care (lipids, weight, blood pressure).
- **Diabetes:** telemonitoring, point-of-care testing and digital support of integrated care.
- **Mental health care:** remote care and psychotherapy, therapeutic compliance, combination with mobile teams...
- **Chronic pain:** multidisciplinary approach to chronic pain in specialized pain centers with patient monitoring: effort, sleep quality, pain intensity, and therapeutic compliance.
- **Apoplexy (stroke):** applications for acute care using high-speed, specialized treatment for home rehabilitation, reintegration, mobile access, self-management and empowerment of the patient and the environment.

F. Technical tools: The micro computer and the shield used

We will use the MySignals shield directly over the Arduino micro computer.

Fig. 4. Micro computer Arduino

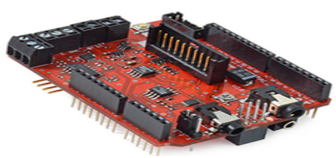

Fig. 5. MySignals shield

Our shield that allows to gather all these sensors is composed as follows:

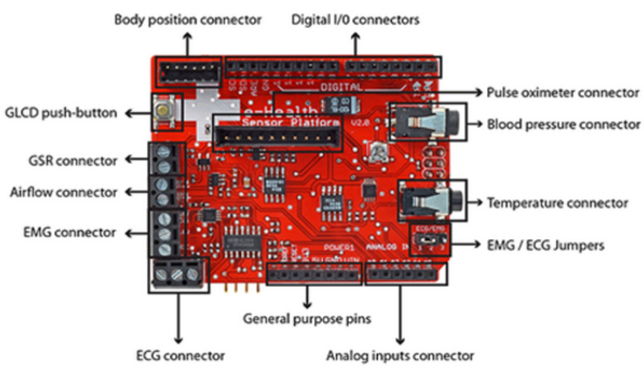

Fig. 6. MySignals shield seen from above

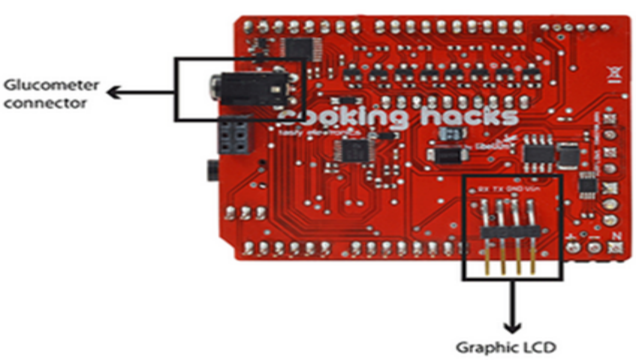

Fig. 7. MySignals shield seen from below

The shield MySignals can gather ten health sensors (blood pressure, cardiac, temperature, position of the patient, glucometer, sound, others and even a warning button), the set of signals generated will be processed by the sensor itself locally then transmitted through the access and core network to a database located in the Internet, for further processing. The patient will be connected to the micro computer as follows:

Fig. 8. Patient connected to the micro computer

The proposed network topology allows doctors and emergency services to know the health status of patients in real time or that allows them to be alerted if thresholds are exceeded, the network topology is based on the cellular network 3G [9] for data transmission.

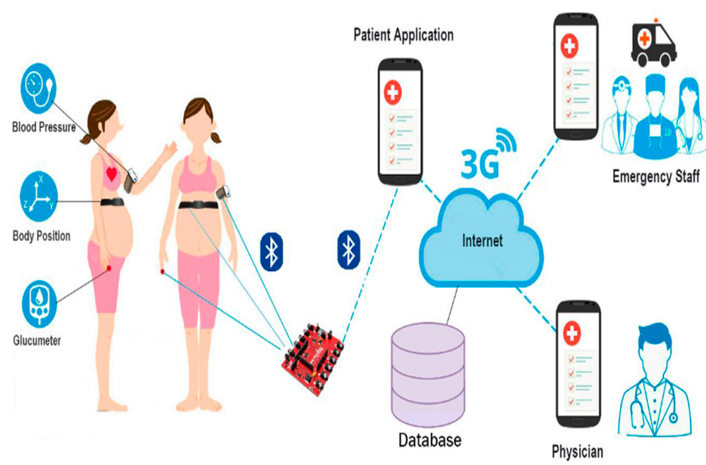

Fig. 9. Network topology for data transmission based on UTMS

VI. Simulation Scenario and Performance Analysis

Our simulation consist of connecting a three microcomputers relayed with ten health sensors and an alert button, to patients in movement, to extract the health information and send it to the right medical server in the Internet for decision making, through an ATM core network and three UTMS base stations in the access layer. The simulation of our IoT Ehealth Ecosystem takes 60 minutes using the Riverbed Modeler Academic Edition 17.5. The performance analysis is done on the physical and data link layer, and in the application layer using a Voice and HTTP applications.

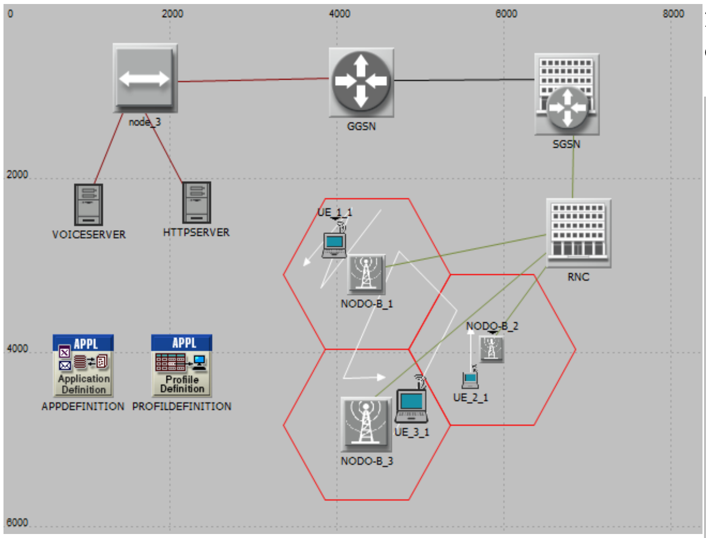

Fig. 10. The simulation scenario of UMTS

1) The performance study of the Ecosystem:

a) UMTS Downlink and Uplink tunnel delay: Its the time of encapsulation of data in the UMTS protocol by seconds on the Downlink and the Uplink. The two curves are more or less stable, their evolution begin around 10:40 pm, the Uplink curve starts with 0.000040 seconds and it is at 0.000040 seconds towards the end of the simulation. For the Downlink curve it starts with 0.000015 second and stays at this value until the end of the simulation.

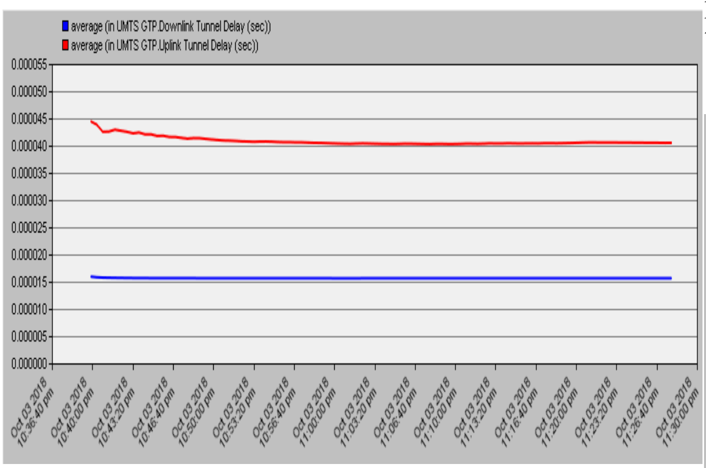

Fig. 11. The UMTS tunnel delay

b) The UMTS traffic received on the Downlink and Uplink: Here we have two curves that represent the UMTS Uplink traffic and the UMTS Downlink traffic received by packets per second. We see that the two curves start their increases at 10:40 pm, the curve of the received Downlink traffic gets 350 packets per second at 10:53:20 pm and then it continues to increase up to 390 packets per second towards the end of the simulation. The received Uplink traffic curve has 200 packets per second at 10:49 pm and then tries to stabilize on that value until the end of the simulation.

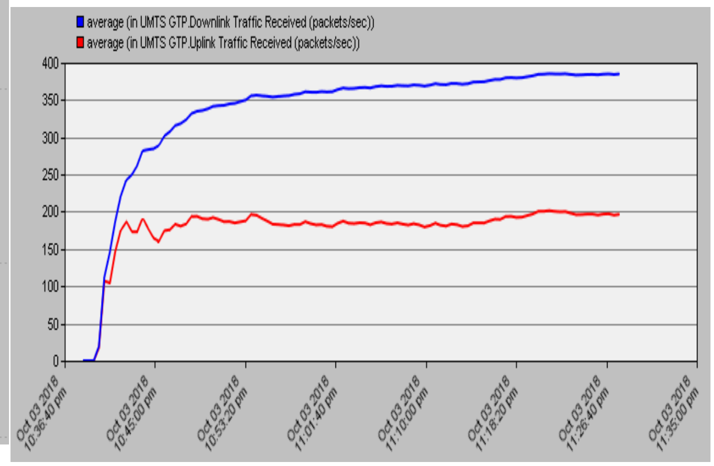

Fig. 12. The UMTS traffic received

c) UMTS Handover: UMTS Handover Pilot channel by cell (Ec/No), Ec: represents the amount of energy, No: spectral density of the noise, Unit: Watts/Hz (or mWatts/Hz), Ec/No: Energy on the spectral noise density, Unit: dB. We analyze only the behavior of UE3-1 which knows a lot of movements between the cells during the simulation. At the beginning the dB for Nodo-B-3 is in first position it is at more than 5 then it stars to decrease, after it is the dB of the Nodo-B-2 which takes the first position when UE3.1 passes to the cell 2 then when it goes to cell 1 the dB of Nodo-B-1 takes the first position and stars to decreases when U3.1 leaves cell 1 to go to cell 3.

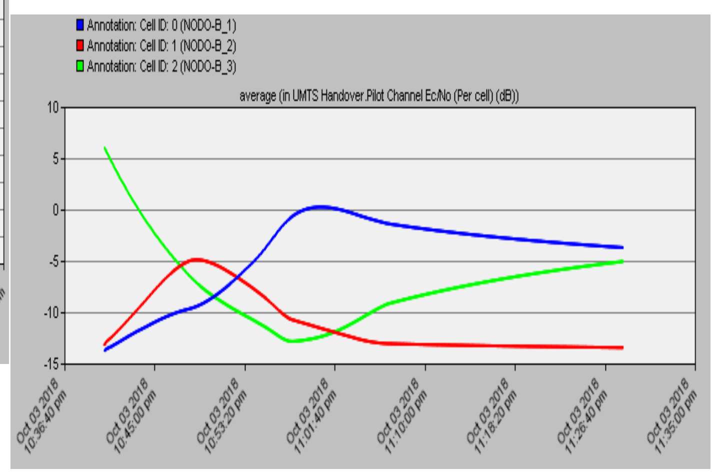

Fig. 13. The UMTS Handover for UE3-1

2) The performance study of the Voice application:

a) The voice Jitter: Is the difference in end-to-end transmission delay between selected voice packets in the same packet stream, without taking into account any lost packets. The curve is on 0.007 second at 10:40 pm then it decrease rapidly to 0.001 second at 10:42 pm where it stabilizes and keeps this value until the end of the simulation.

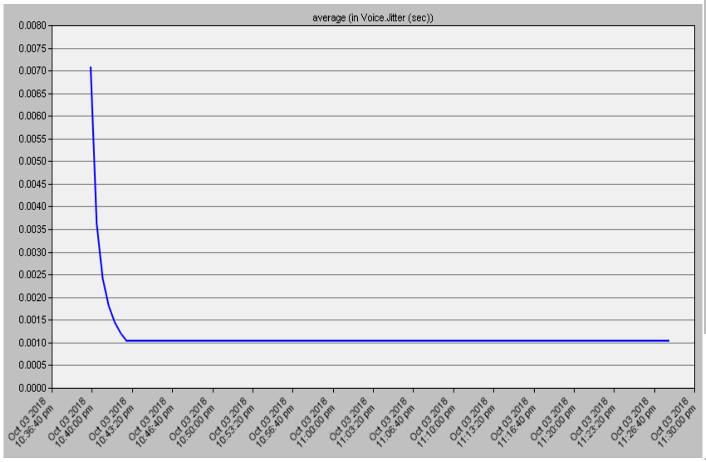

Fig. 14. The average of the voice Jitter

b) The voice packet end to end delay: Its the time interval between when the voice packet is queued for transmission at the physical layer until received at the receiving node. the curve is on 1.25 seconds at 10:40 pm then its starts to increase slowly to 1.59 second at 10:42pm where it stabilizes and keeps this value until the end of the simulation.

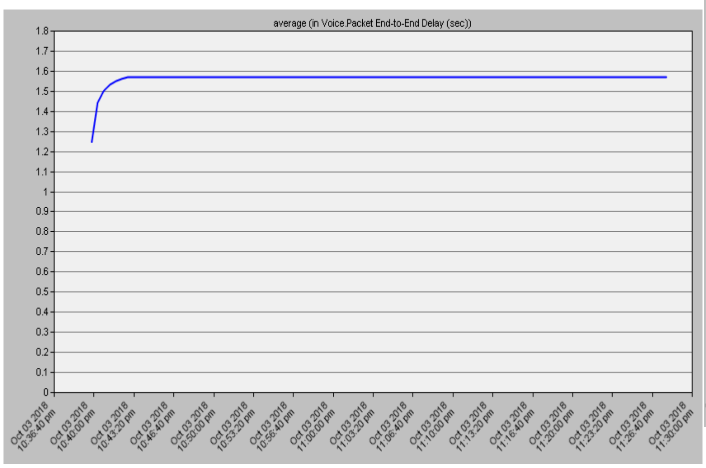

Fig. 15. The average of the voice packet end to end delay

3) The performance study of the HTTP application:

a) HTTP object response time: We analyze the average response time to an HTTP request we see that the curve increases towards 10:40 pm to reach 0.58 second then it increases unsteadily up to more than 1 second at 10:50 pm then it continues its unstable increase until 2 seconds towards the end of the simulation.

b) The HTTP traffic sent and received: We notice that the two curves at the beginning are superimposed and they

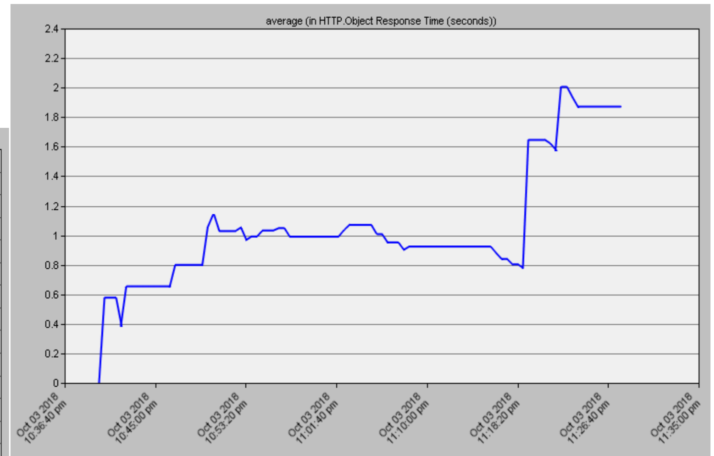

Fig. 16. The average of the HTTP object response time

reach up to 0.15 packet per second at 10:40 pm then they start to decrease until 0.032 packet per second at 10:49 pm, after that time the two curves separate and increase so that the curve of the traffic sent reaches 0.07 packet per second and that the curve of the traffic received reaches 0.062 packet per second at 10:57 pm, the two curves remain always separated but keep a few near the same rate of separation so that the curve of the traffic sent reaches 0.75 packet per second and the curve of the traffic received reaches 0.065 packets per second towards the end of the simulation.

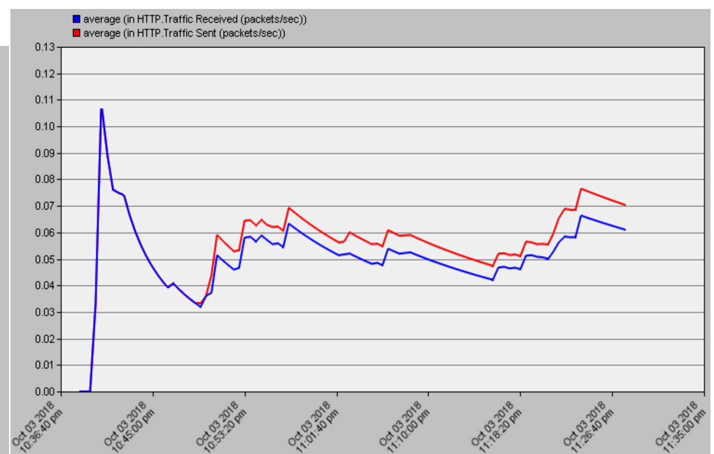

Fig. 17. The average of the HTTP traffic sent and received

VII. Conclusion

Currently many smart cities like: Amsterdam Smart City, Smart City Lyon, and Dubai Internet City and others are expressing a massive generation of data, as well as the establishment of many network infrastructure as a part of the use of the Internet of Things. The Internet of Things is applied to improve many current and future sectors of activity like home automation, transportation, public services and others.we focus in your article on the health care sector.

The new IoT EHealth ecosystem is designed to prevent against any health threats that can make us lose our patient, and to react rapidly in case of a serious health problem. Our IoT EHealth ecosystem can measure, record and transmit, health information of the patient to the Internet and can warn emergency, hospital, and the family of the patient if necessary for a quick intervention. The EHealth ecosystem is based on a micro computer connected to ten health sensors and even an alert button, all the information generated by the sensors are transmitted through the Internet to the data base server and the processing system server. To allow access at the health information to the Internet we were based on the WWANs especially the UMTS network. To study the performance of our IoT EHealth ecosystem we used the Riverbed Modeler Academic Edition 17.5 to make a simulation scenario based on the UMTS and ATM networks, the simulation allow us to analyze the performance at the physical and data link layers using UMTS protocol, the performance in the case of using a voice application and the performance in the case of using an HTTP application.

REFERENCES

[1] HILLIER, Aaron. Modifying Commercial RFID Tags using Polydimethylsiloxane based Polymers for Sensing Purposes. 2020. Thse de doctorat. University of Kent,.

[2] 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.

[3] ZEMRANE, Hamza, BADDI, Youssef, et HASBI, Abderrahim. Mobile AdHoc networks for Intelligent Transportation System: Comparative Analysis of the Routing protocols. Procedia Computer Science, 2019, vol. 160, p. 758-765.

[4] TEKLER, Zeynep Duygu, LOW, Raymond, GUNAY, Burak, et al. A scalable Bluetooth Low Energy approach to identify occupancy patterns and profiles in office spaces. Building and Environment, 2020, vol. 171, p. 106681.

[5] YEGIN, Alper, KRAMP, Thorsten, DUFOUR, Pierre, et al. LoRaWAN protocol: specifications, security, and capabilities. In : LPWAN Technologies for IoT and M2M Applications. Academic Press, 2020. p. 37-63.

[6] ZEMRANE, Hamza, BADDI, Youssef, et HASBI, Abderrahim. Comparison between IOT protocols: ZigBee and WiFi using the OPNET simulator. In : Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications. 2018. p. 1-6.

[7] QIN, Zhenquan, SUN, Yingxiao, HU, Junyu, et al. Enhancing Efficient Link Performance in ZigBee Under Cross-Technology Interference. Mobile Networks and Applications, 2020, vol. 25, no 1, p. 68-81.

[8] FOURTET, Christophe et PONSARD, Benot. An introduction to Sigfox radio system. In : LPWAN Technologies for IoT and M2M Applications. Academic Press, 2020. p. 103-118.

[9] 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. 2019. p. 1-8.

[10] 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 Computing Technologies and Applications (Cloudtech). IEEE, 2018. p. 1-8.

[11] ISLAM, Muhammad Khaledul et WIRTANEN, Jeffery. Method and system for signaling release cause indication in a UMTS network. U.S. Patent No 10,582,562, 3 mars 2020.

[12] MALLADI, Durga Prasad, WEI, Yongbin, HORN, Gavin B., et al. Long term evoluton (LTE) user equipment relays having a licensed wireless or wired backhaul link and an unlicensed access link. U.S. Patent No 10,588,101, 10 mars 2020.