UNIVERSITY OF THE WESTERN CAPE

INTERNET-OF-THINGS FOR CYBER HEALTHCARE (IoT4C): Information Dissemination, Systems' Interoperability and Security

by

Claude Kakoko Lubamba

A thesis submitted in partial fulfillment for the
degree of Master of Science

in the
Faculty of Science
Department of Computer Science

March 15, 2017

Declaration of Authorship

Signed: _____

Date: _____

"The only true wisdom is in knowing you know nothing."

Socrates

UNIVERSITY OF THE WESTERN CAPE

Abstract

Faculty of Science
Department of Computer Science

Master of Science

by Claude Kakoko Lubamba

Cyber Healthcare is becoming one of the fastest growing industries in the world due to an increasing elderly population and a more health conscious word population. On the other hand, IoT devices are emerging from niche areas to provide new services that we could not fathom without the technological advances made in IoT and healthcare fields [1]. Wireless Sensor Networking (WSN) is a promising approach to cyber healthcare as it can enable real-time monitoring of patients and early detection of emergency conditions and diseases [2, 3]. However, there are a number of issues that need to be addressed in order to benefit from the cyber healthcare promises.

The aim of this thesis is to develop efficient techniques for wireless sensor networks with the objective of supporting real-time healthcare monitoring and thus enhance public health service delivery in general by addressing the following key issues related to cyber healthcare systems:

- Cyber healthcare systems' field readiness
- Cyber healthcare systems' communication
- Cyber healthcare systems' interoperability
- Cyber healthcare systems' security

Acknowledgements

Foremost, I would like to express my sincere gratitude to my advisor and Supervisor Prof Antoine Bagula for the continuous support of my MSc study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me through research and writing of this thesis. I could not have imagined having a better advisor and mentor for my Masters study, without forgetting the whole computer science department for their encouragements, insightful comments, and hard questions.

I would also like to extend my sincere gratitude to the National Research Foundation (NRF) for granting me a bursary which allowed me to grow professionally and intellectually. Their bursary gave me the chance to study without having to worry about school fees and food.

I thank my fellow lab-mates for the stimulating discussions, for the sleepless nights we were working together before deadlines, and for all the fun we have had in the last four years.

Also I thank my friends and family Rosette Sifa, Ignace Bahati, and Chadrack Lubamba for the good vibe and good atmosphere in the house.

Last but not the least, I would like to thank my parents Jose Lubamba and Anny Ngolo for giving birth to me, and all together with Lubamba brothers and sisters for their unconditional love and financial, morale and spiritual supports throughout my whole life...

Publications

M Mandava, C Lubamba, A Ismail, A Bagula, and Herman Bagula. Cyber-healthcare for public healthcare in the developing world. In *2016 IEEE Symposium on Computers and Communication (ISCC)*, pages 14–19. IEEE, 2016.

A Bagula, C Lubamba, M Mandava, H Bagula, M Zennaro, and E Pietrosemoli. Cloud based patient prioritization as service in public health care. In *ITU Kaleidoscope: ICTs for a Sustainable World (ITU WT), 2016*, pages 1–8. IEEE, 2016.

Contents

List of Figures

List of Tables

Listings

Abbreviations

IoT	**I**nternet **O**f **T**hings
HL7	**H**ealth **L**evel 7
WSN	**W**ireless **S**ensor **N**etwork
WBAN	**W**ireless **B**ody **A**rea **N**etwork
EHR	**E**lectronic **H**ealth **R**ecords
OTAP	**O**ver **T**he **A**ir **P**rogramming
RFID	**R**adio **F**requency **I**dentification
RSSI	**R**ecieved **S**ignal **S**trength **I**ndicator
CSMA/CA	**C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **A**voidance

Dedicated to my parents Jose Lubamba and Anny Ngolo ....

Chapter 1

Introduction

Growing at an exceptional pace, the Internet-of-Things (IoT) is a complex network that connects billions of devices together with humans into a communication infrastructure that consists of many technologies, several platforms and also different protocols [4]. It is expected that by interconnecting millions of sensor network islands, the emerging IoT will bring a new dimension to the Internet by shifting its traditional internet "anywhere" and "any time" model of connectivity to enable access "anywhere", "anytime" and also using "anything" [4]. This will be achieved by outfitting the objects and appliances that we use daily with sensor devices and endowing them with an IP address. These IP addresses will transform these objects/appliances into smart objects that can access or be accessed by any other smart objects through the Internet or other emerging communication systems. As a result of recent technological advances made in the Internet-of-Things and healthcare fields [1], Cyber Healthcare is becoming one of the fastest growing industries in the world targeting the elderly population as well as a more health conscious world population. Wireless sensor networking (WSN) is a key player in Cyber Healthcare as it can enable real-time monitoring of patients and early detection of emergency conditions and diseases [2, 3] by capturing patients' vital signs, mapping these signs as patients' records and disseminating these records to cloud infrastructures where they are stored and processed to achieve situation recognition and decision support as services to communities. However, besides the ethical constraints resulting from healthcare processing, there are many challenges associated with the design and implementation of Cyber Healthcare WSN. These include issues related to the field readiness of the e-health bio-sensor devices used to capture the patients' vital signs, the integration of these vital signs as patient records into public healthcare systems and the secured dissemination of these records to processing places to enable both real-time and opportunistic access while guaranteeing data patient privacy. During this study, we revisit the issue of electronic healthcare (e-Health) to assess the relevance of using

Cyber Healthcare systems as a low cost and efficient alternative for public healthcare in both rural and urban settings of the developing world.

This project aimed to develop an efficient e-health wireless sensor networking model to support real-time healthcare monitoring by addressing the following issues:

- Vital signs capturing, mapping into medical records and integration into public healthcare storage systems using the HL7 standard.
- Real-time and Opportunistic dissemination of patient records to processing places using different wireless technologies and protocols.
- Privacy, security and confidentiality to protect medical records from being tempered with.

1.1 Problem Statements

The last decade have witnessed the rise of a flourishing e-health industry with mobile and ICT manufacturers such as Samsung, Apple and other companies releasing light weight bio-sensor devices which can read different vital signs and display these signs on a mobile device or a watch screen to provide services to the sport community. On the other hand, different other devices have recently emerged from a niche area initially focused on the elderly, namely commodity products used in the medical field to achieve patient monitoring. The emerging Cyber healthcare field can benefit from the integration of these bio-sensor devices to provide efficient health-care services and enhance patient monitoring and care. However, such integration raises many issues related to software openness, hardware and software compatibility and diversity and many others. The goal of this research was to develop a low cost and efficient e-health system that can be freely extended, manipulated and integrated into Cyber Health-care systems using the HL7 standard.

The following were problems that needed to be solved in this thesis:

- The field readiness of the bio-sensors (eHealth kit) needed to be determined. Given that the proposed system was intended to be deployed with real life systems to make real life healthcare decisions, it was very crucial to know whether this kit can be used for real life development, or it is just just a prototyping device.
- Secondly, we needed to investigate the after data collection process given that, the bio-sensors we used are not equipped with either storage capacities nor processing

capabilities. We needed to know whether we can rely on selected communication technologies to transport the data from collection points, to a centralized database, where the data will be used for different healthcare purposes.

- The next problem that was investigated in this thesis was related to network attacks. We needed to derive ways to prepare the system such that in cases of intrusion attacks, there is a mechanism that will allow the network to recover while excluding the corrupted node if there is any in the network.

- The last problem that was solved in this thesis was the problem of healthcare standards integration and systems' interoperability. We needed to know whether we can integrate a well known healthcare standard for exchanging patients' data into our proposed system, and if so, what are the pros and cons.

1.2 Background and Needs

The objectives of this study are firstly to improve the following aspects of eHealth: the security aspects, the standardization, and the systems interoperability aspects. And secondly, the research aims through investigation of environment monitoring sensors, to advise people with medical conditions about geographical locations with high levels of pollution that can affect their health, so that they can avoid these area. Note that this will be done if time is available, but mainly if resources are available, because the pollution monitoring sensors are very costly.

As an example, let's consider the number of elderly people and children of young ages in need of 24-hour medical attentions which has recently increased based on the results in [5, 6]. If the proposed system is implemented, it could solve this problem, and further even assist in ambulatory healthcare. There are also a large number of people with chronic health conditions [5], and if we could add air pollution mapping to the system, this could even further improve healthcare services.

Patients' data or Patients' electronic health records are very important and crucial information, especially as they are personal and confidential information and, it could be catastrophic if they get in unauthorized hands. With that in mind, comes the need for improving data communication security, and also the need to improve systems' confidentiality, in order to ensure that the data is safe and only available to authorized system users and medical practitioners. Given that our proposed network has nodes which transfer collected data, the investigation of security in this research will mainly focus on network intrusion, unwanted access detection and network recovery.

1.3 Purpose of the Study

The purpose of this study is to investigate ways to improve and enhance services delivery in healthcare industries, investigate ways to securely monitor patients remotely and also monitor the environment, by using powerful and emerging technologies. As already illustrated early in this chapter and as it will be noticed in the course of this thesis, the integration of healthcare services with Internet-of-Things features or vice-versa is refereed to as Cyber healthcare. The following are main points and also considered as pillar of the study that is undertaken in this thesis:

- Sensing Layer and Sensors Field-readiness: The purpose of investigating this topic is that of studying and determining the field-readiness of the eHealth sensor kit, and all its sensors. We wish to know whether these sensors are ready to be used in the real world and in real healthcare facilities or healthcare systems.
- The Information or Data Dissemination: This topic is investigated with a sole purpose of improving the way data are exchanged across different healthcare platforms and healthare systems. This is done by investigating the communication protocols used, the data overhead and also studying the behaviour of selected network performance parameters.
- The System Interoperability: Making patients' data available anywhere, anytime and to authorized persons being one of the goals of this thesis, there is also a question of how this data if formatted in order for it to be smoothly exchanged between various healthcare systems. Formatting data also comes with a cost, which will be discussed in the respective chapter of this thesis.
- Security: Lastly, the security will be also investigated. In any system or application where data is exchanged the need for security is vital to the deployment of the system. Note that the security of systems and of data transmission is a very huge and very wide research topic. However, this project will only focus on network intrusion attacks.

1.4 Objective(s) of the Study

The main objective if this study as the thesis title stipulate, is to investigate ways to improve healthcare by associating it with the internet of the thing (IoT). In order to

easily conduct this research, the main objective of this thesis was divided into sub-objectives which aligns with the purpose of the study in section 1.3. The following are the sub-objectives of the study conducted in this thesis:

- Most of cost efficient sensors that are in the market nowadays, are prototyping sensors and, in most cases, they are not designed to be deployed in real life applications. One of the objectives with this study is to investigate the field readiness of the sensors we used, and this is done through intense testing of these sensors where measurements are taken and compared with realistic facts. The field readiness will also be investigated in this project or research through performing multiple experiments and doing multiple reading with the sensors, on different subjects and in different circumstances. For example, the behaviour of vital signs varies in different circumstances such as, while sleeping, after physical exercises, in the morning, in the evening and so on. Our objective in this case is to investigate whether the readings of vital signs that we obtain from our sensors follow the same pattern similar to the results obtained with devices currently used in healthcare.

- Secondly, we will investigate the data communication amongst different healthcare systems and healthcare platforms. How is the data transferred from one system or platform to another. Investigating the communication devices and technologies used, will give to system's developer a clear idea in terms of range of communication, signal strength, and packets throughput ratio in both rural, and urban areas, as compared to the specifications supplied by the devices manufacturer. In general, the objective is to investigate selected network performance parameters.

- To add to what is discussed in the paragraph above, the IoT4C system that is proposed in this research, is a system that aims to connect multiple platforms, applications, systems and sub-systems. All of these entities exchanges data of different types. This research focuses on exchanging patients' records, which are complex, private and very confidential information. The different entity systems and sub-systems need to speak the same language in order for them to communicate. Given that our system will be interacting with other already existing systems, we have to format the data to be exchanged in a standard format such as the HL7 which we will discuss at a later stage of this thesis. The objective is to observe how much overhead does the process of formatting data in HL7 standards brings, in terms of storage space and packets time delay.

- The last point that will be investigated in this thesis is the security of systems. We will implement a defense mechanism against intrusion attacks, and test it performance.

1.5 Research Methods

Clifford Woody [7] stated that, research comprises defining and redefining problems, making reasonable hypotheses or suggesting solutions with the aim of deducting and reaching conclusions; and very carefully testing the conclusions deducted to decide whether they best fit the hypothesis formulated [7, 8]. In short, research is therefore, an original contribution to the existing stock of knowledge making for its advancement. It is the pursuit of truth with the help of study, observation, comparison and experiment. Research is the search of knowledge through objective and systematic methods of finding solutions to problems is research [8]. As such, the term research refers to a systematic method consisting of enunciating the problem, formulating an hypothesis, collecting the facts or data, analyzing the facts and reaching certain conclusions either in the form of solution(s) for the concerned problem or in certain generalizations for some theoretical construction. This section also covers a short explanation of types of research methods and methodologies that were used in the implementation of this proposed system [9].

There are four basic types of research, and other types can be derived from these basic types. They are the following:

- Descriptive vs Analytical research Methods : The first includes surveys and fact-finding inquiries of different kinds, whereas the analytical research uses facts and data that already exist and analyses them to make evaluations
- Applied vs Fundamental research Methods: Applied research aims at finding immediate solutions to any specific problem that a specific society/ business, or community is facing, and the fundamental research is usually undertaken for the sake of knowledge.
- Quantitative vs Qualitative research methods: As their names suggest, these types of research are concerned with phenomena, one involving measurement of some quantity characteristics and the other phenomena relating to quality.
- Conceptual vs Empirical Research Methods: The first methods is related to some abstract idea(s) or theory, and the Empirical is very appropriate when there is proof of certain variates affecting other variables in some way.

1.6 Research Question

If I may attempt to frame a research question for this thesis, I would say that this thesis endeavors to solve the problem of service delivery in public healthcare, ambulatory

healthcare, and environment monitoring. We wish to improve how these services are delivered and migrate from the traditional way to a modern way or a smart way, and this will be accomplished by coupling IoT technologies with traditional healthcare services, to obtain what is refereed to in this thesis as Internet-Of-Things for Cyber Healthcare (IoT4C). There are numerous areas of IoT in which research can be conducted in order to improve public healthcare service delivery. However, this thesis will focus on four main areas, which are aligned with our purpose of the study in section 1.3. They are the following:

- Automatic physiologic parameters capturing, why do we need this ? This is very important because of its automation, as it has the advantages of replacing the manual data capturing methods which is error-prone. Automated physio data capturing has a higher probability of providing error-free data capturing.
- After the physiological parameters have been captured, they need to be disseminated to doctors, and processing places where situation recognition or patient condition recognition are performed.
- The security of the physiological parameters during their communication from sensors, to the doctors, and processing places.
- Finally, the integration of the proposed design system into different public healthcare systems and platforms.

The above four points establish the four main chapter of this thesis. Each of these points is investigated separately, but their investigation converges to answering the main research question as stated above.

1.7 Research Methodology

The research we conducted is experimental research which leads to quantitative evaluation of the designed and developed prototype. This method is implemented in an incremental approach in order to implement potential solutions to actual problems. This means that the entire system is split into small manageable sub-systems, and these systems are built separately and independently as far as possible. Once these sub-systems are completely implemented, they are then assembled together in a bottom up approach to form the initial system, provided that they work, otherwise, they are refined. The implementation follows the flow in figure 1.1.

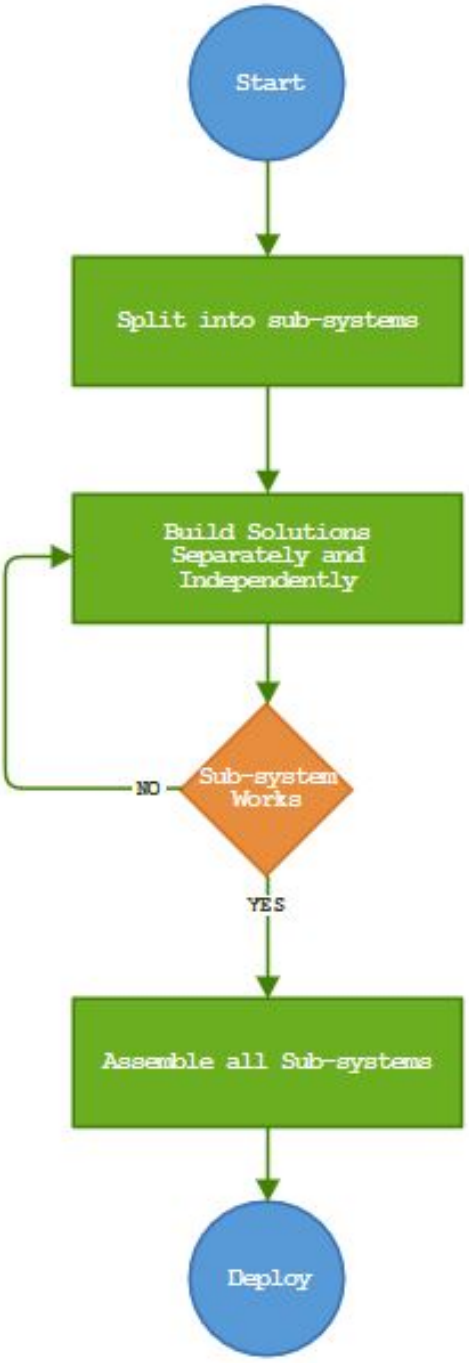

FIGURE 1.1: Implementation system flow

The process flow in figure 1.1, depicts the basic methodology that is used to implement the solutions to the problems illustrated in section 1.6 above. The presented process in figure 1.1, will assist in implementing the following solutions to the research questions:

- In our proposed solution we take advantage of the recent sensors and RFID technological advances to use an off-the-shelf eHealth kit for physiological parameters capture. This kit(s) provides multiple advantages such as :

  - Automated physiological parameters capture
  - Low probability of readings with errors
  - One single person can get multiple physiological parameters readings, etc ...

- Emerging communication technologies have provided lightweight communication platform for the wireless sensor networks (WSN) such as, Zigbee, and the lightweight version of WiFi, which are very suitable for sensor devices. These emerging communication technologies and platforms will be used in this research to achieve the dissemination of the physiological parameters from sensors to processing places.

- While both the Zigbee and WiFi have built-in security measures to protect the information carried by these types of communication technologies and protocols, to the best of our knowledge, these technologies do not cater for over-the-air attacks. We focused on OTAP security for the stated communication protocol and technologies.

- Lastly, there are many standards of electronic healthcare messages or data exchange that have been proposed for the interoperability of healthcare systems, which include also HL7. HL7 has been selected in this thesis as standard of interest for implementing the system interoperability.

1.8 Contributions and Outline

The main contribution made by this thesis, is that of proposing a cyber-healthcare framework and developing many of its main components to produce a prototype that will be developed further into matured and field-ready healthcare monitoring systems. The frame work is as depicted in figure 1.2

The depicted framework in figure 1.2 comprises 4 different layers and these layers, which are the application layer, the middle-ware layer, the dissemination layer or networking layer, and the sensing layer. These layers addresses the 4 research questions that we illustrated earlier in section 1.6 above.

The outline of the rest of chapters in this thesis is as follow:

- A chapter on literature reviews and related works

- Then follow four chapters each of which discuss respectively the four layers of our proposed frame-work (figure 1.2) which are the implementation of our proposed solutions in accordance with our research question

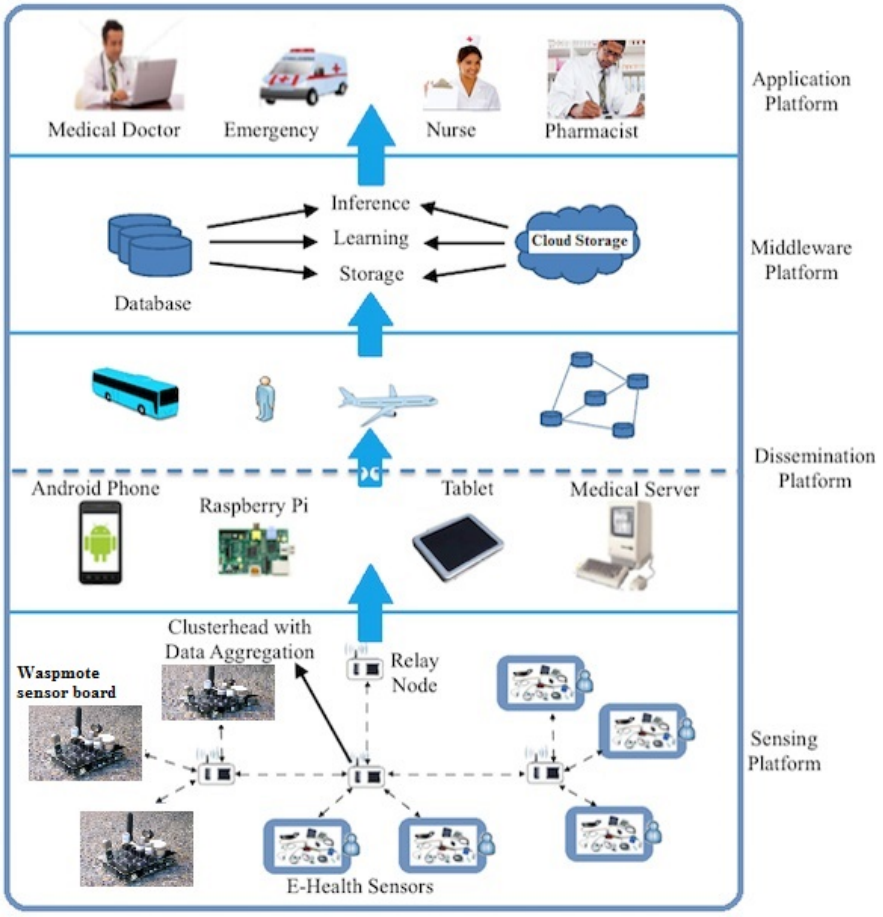

FIGURE 1.2: Cyber-healthcare Frame Work

- There after comes a chapter on the conclusion and the future work(s)

Chapter 2

Related Works

2.1 Internet-of-Things for Healthcare (IoT4C)

In [10], the authors presented a cloud centric version for a world wide implementation of Internet-Of-Things. They discussed the key enabling technologies and application domains that are likely to drive the Internet-Of-Things (IoT) research in the near future. They also presented a cloud implementation using *Aneka*, which is based on interaction of private and public clouds. They finally concluded their presented IoT vision by expanding on the need for convergence of the wireless sensor network (WSN), the internet and distributed computing directed at the technological research community.

In [11], the authors presented an implementation of a smart healthcare system in which they integrated healthcare with Internet-of-Things features into medical devices to improve the quality and effectiveness of services, bringing especially high value for elderly, patients with chronic conditions and those that require consistent supervision. They proposed a system which will suppress long waiting in the traditional public healthcare by providing patients' electronic health records available to authorized persons anywhere, anytime and also using anything. Their target was to establish 24*7 patients monitoring.

In [12], the authors proposed systems implementation that could very much improve healthcare service and revolutionize service delivery in elderly healthcare. They proposed the system such as Assisted Ambient Living (AAL), which encompasses technical systems to support elderly people in their daily routine to allow an independent and safe lifestyle for as long as possible. They also proposed another technique, the keep In Touch (KIT), which makes use of smart objects and technologies such as the Near Field Communication and Radio Frequency Identification, to facilitate tele-monitoring processes. They proposed systems that provides personal communication between elderly

people, their environment and relevant groups of care givers in an important aspect in Ambient Assisted Living (AAL). Through the combination of the Keep In Touch (KIT) and closed Loop Healthcare (CLH), a central AAL paradigm can be realized through the IoT, where the elderly live in their homes with smart objects, thus smart homes, communicating to the outside world in an intelligent and goal-oriented manner.

In [13], the authors proposed a framework for the Internet of Things communication as the main enabler for distributed worldwide healthcare applications. The work they presented started from the recent availability of the wireless medical sensor prototypes and the growing diffusion of electronic healthcare record databases, they analyze the requirements of a unified communication framework. Their investigation took the move by decomposing the storyline of a day in a selected subject's life. They finally presented the Internet of Things protocol stack and the advantages it brings to healthcare scenarios in terms of the identified requirements.

2.2 Sensing Layer

In [3] and [2], the authors worked on sensing using the eHealth kit which is very similar. However, the research done in this thesis concerning the sensing layer, adds more to what the two papers we mentioned above did. Our study on the sensing layer will only focus on the sensors' field-readiness. The authors in the two papers namely [2] and [3], conducted work and research on wireless sensors for healthcare and their research focuses were sensing and communication. They conducted experiments by doing multiple readings with sensor devices to check whether obtained values are in normal ranges, and in cases where values were unrealistic, they performed some calibrations in order to obtain values that are realistic or approximately close to the reality, given that the sensor used were prototyping sensors. We however concluded that, this research could have been done much better by performing readings or experiments in multiple scenarios such as:

- Collecting vital sign of a single individual in the morning, before bed, after gym, after exercising and early when he wakes up, and analysing this data taking into consideration the normal behaviour of the vital signs in each case.
- Collecting vital signs of multiple individuals and comparing their diversities while observing whether they all fall under normal ranges considering the health or medical status of the volunteers.

The authors in [14], implemented a Ubiquitous Sensor Network (USN) for pollution monitoring, and their implementation was intended to be deployed in developing countries. They used Waspmote devices, with their sensor boards and sensors plugged on the board to prototype this implementation. Their architecture integrates different features that meet the requirements of developing countries [14]. Amongst these features, we focused on those that are of interest to our work, the opportunistic dissemination of data which is discussed in the sensing layer, and also the field-readiness of the sensors.

To assess the field readiness of the sensors and that of the communication protocols used, the authors in [14] conducted a number of experiments in terms of pollution monitoring and, they also assessed the data transmission. There are not really many ways of testing sensors' field-readiness, the most common way is to perform experiments and compare the reading results to those of the readings obtained using devices that are declared field-ready by recognized standards. In this project, similar to the work in [14] and the other two previous papers we discussed in the previous paragraph, we conducted numerous experiments and compared the obtained readings of both environment monitoring sensors and Healthcare sensors kit, firstly with the normal ranges of these data,(for example a normal person can not have a temperature above 50 degrees Celsius) and secondly in cases where it was possible, compared the readings with other readings obtained with trusted, expensive, accredited and recognized-to-be accurate devices that serves the same purpose as our devices.

The authors in [15] and [16] conducted a study on the improvement of readings obtained from sensors, and they used calibrations. Although the results obtained did not show 100% accuracy, the improvement on the results were very impressive and approximated the real results with a very small error. To improve the field-readiness, we will conduct the experiments in different conditions that can affect the readings or the performance of the equipment.

In [17], the authors presented an irrigation management system (IMS) which they implemented with wireless sensor networks (WSNs) and described in [17]. An IMS was set up and deployed in a township in a rural area of Malawi. The authors assessed the wireless sensor networks deployment field readiness in the proposed agricultural system, by investigating the performance of the communication's parameters such as the RSSI at different distances between nodes, and in different situations such as long and short maize plants surrounding the nodes. They also investigated other performance parameters such as the remaining battery power and the impact of the battery's performance on radio links. The experiments showed that they successfully implemented this system, and investigated performance parameters which led them to also conclude that the devices used were indeed field ready.

2.3 Networking Layer

Chronologically speaking, once the data is collected by devices such as sensors with low processing capabilities and low storage capacities, these data need to be transferred to where is will be processed or stored, and that is what this layer, or section of the project is about. Several scenarios of the implementation are discussed, scenarios such as the indoor and outdoor communication, the communication protocol used, the opportunistic and static communications and the packets throughput and packets delivery delays time. In paper [18], the authors considered studying variables or performance measures such as signal strength, payload, throughput and others through multiple experiments, and compared and analysed their performances. They evaluated the IEEE802.15.4 and the ZigBee performance with a special focus on application for industrial sensor networking [18]. They considered a couple of scenarios cases and in both cases with a star topology for the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) model, while investigating performance parameters such as the throughput, latency, packets loss and packets delivery delay time.

In [19], the authors conducted similar investigations, and also discussed a number of performance measures most of which are those discussed in the previous paragraph. In addition, they also added the energy consumption of the sensors. In this case they conducted the study for the IEEE802.15.4 and investigated the above mentioned performance parameters by conducting multiple experiments.

In [20], the authors proposed an accurate model for the slotted Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) access scheme for the IEEE802.15.4 standard for unacknowledged transmission mode. The authors conducted this research because the design of the 802.15.4 carrier sensing mechanism, that model the performance of the network in cases of non-acknowledged transmissions is not a very trivial extension. In [20] they derived a model and illustrated through simulations that could be extremely accurate. Guidelines were derived that optimized the energy, and the throughput performances of the sensor networks using the 802.15.4 standards.

In [21], the authors investigated the same performance parameters. The authors implemented s system for monitoring a vineyard. Arduino devices were scattered and ground-based located in the vineyard collecting information about the environment on the farm, and a drone hosting a gateway flew by every now and then to collect agricultural information collected by the sensor devices deployed in the vineyard. This implementation is referred to as Aerial opportunistic communication. The throughput, the packets loss and packets delivery delays were all investigated on altitudes to see which is the a most convenient height for the drone to fly at, and what is the maximum

and the minimum altitude it can fly at while also considering other factors such as trees and other things that can affect the behaviour or that can act as an obstruction on the drone's path. This seems relevant to our research because of the fact that the communication protocols are investigated in terms of height. Another study that conducted a similar experiment, but in terms of radius of communication, is the study in [22] and the authors concluded that the use of communication protocols with lower frequencies results in longer distances of coverage in term of data transfer, a claim that we will also investigate in our specific project.

In [23] the authors implemented a network simulator for the IEEE802.15.4, with which they conducted several sets of experiments to study its various features, which include: (1) the beacon enabled and the non-beacon enabled mode, (2) Carrier sense multiple access with collision avoidance (CSMA-CA), both unslotted and slotted , (3) direct, indirect and guaranteed time slot(GTS) data transmissions, (4) association, tree formation and network auto-configuration, and (5) orphaning and coordinator relocation. The authors in [23] also compared the IEEE802.15.4 and the IEEE802.11 under certain conditions such as in the non-beacon enabled mode, and under moderate data rate. They compared the efficiency of the communication standards, the overhead and the battery power consumption. They also discussed some issues that affect the networks, and that could degrade the network performance if they are not properly handled.

In [24], the authors presented a simulation-based performance evaluations of the new medium access protocol for the IEEE802.15.4 communication protocol and standards. They focused on the beacon-enabled mode, which they implemented in a star topology network. Key features were also described and discussed, and they also evaluated the performance parameters such as the throughput, the packets delivery delay, the energy consumption, and others. Another important topic that was addressed in this paper is the analysis that compared the energy costs of beacon tracking and non-tracking modes for synchronization, and showed that the best choice is totally dependent on the combination of duty cycles and data rates.

In [25] The authors in this paper presents an analysis of the IEEE802.15.4 performance, in a low power, low data rate wireless standard. The study was done in relation to the medical sensor body area network. An emerging application of WSN with particular performance constraints, which include power consumption, robustness and security, and physical size is presented by the authors. They performed their analysis in a star topology network on the IEEE802.15.4 communication standard at 2.4 GHz, for WBAN, which consisted of wearable or desk-mounted coordinators outside of the body with up to 10 body implanted sensors. They mainly considered the long-term power consumption

of devices, since for practical and medical reasons, implanted medical devices and sensors must function for 10 to 15 years without battery replacement or charging.

In this study most of the performance measures are similar to what has already been done or investigated by other researchers, studying them in, different locations or different cities where the atmosphere and weather may generate a different scenario which might have an influence on the performances of these communication protocols. That is the specific focus of this study regarding the networking layer of this implementation.

2.4 Application Layer

By definition, the application layer is the layer of the generic protocol of the TCP/IP protocol suite, which consists of protocols which the main focus of which is the process-to-process communication across an IP network, and provides a firm communication interface and end-user services. The application layer itself is a vast research topic many aspects of which can be investigated. In this research however, we mainly focus on the network attacks, attack preventions, attack mitigation, and we also investigate the security provided by the communication protocol devices we used, IEEE802.15.4/ZigBee and the Wifi.

2.4.1 The Over-the-air Attacks & Security Modes on Waspmotes and Arduino

Over-the-air programming (OTAP) is a methods of sharing configuration settings, new software, and even updating encryption keys to devices like cellphones or secure voice communication equipment[26]. It has important features, where one central location can propagate updates to all the users who are not able to refuse, defeat, or alter the update, and the update applies immediately to everyone on the communication channel [26]. In OTAP communication a user may be able to "refuse OTAP" but, the "Channel manager" can also "remove" them from the channel automatically [26].

In [27] the authors investigated a fire emergency and gas detection system based on WSNs project for both indoor and outdoor environments. The main challenges which are addressed in this paper include, the management of nodes, the provision of algorithms, the risk modelling and analysis, and the OTAP. The implementation is done considering the fact that the WSNs can be deployed both indoors and outdoors. They used remote access in order to enable users to monitor various network activities such as retrieving sensor measurements (gas concentrations), and network status parameters

(power levels,active nodes, etc.). These capabilities are possible with OTAP [27], they also used Email server, twitter integration and GPRS communication for data retrieving and acquiring information about certain performance measures (signal strength, power level, etc ..).

In [28], the authors investigated a project titled "A Living Smart City: Dynamically Changing Nodes Behavior through over-the-air-programming",and as it can be deduced from its title, the paper discusses an implementation of an IoT smart city project, where they use OTAP to change and modify nodes' behaviours. They presented a deployed facility, emphasizing on the possibility of experimenting on a larger testbed, through the re-programming of the IoT devices deployed [28]. In our project, we considered the implementation investigated by the authors in [27, 28] and [26] to try and see how we can add and improve on what they did.

In our project, the use of OTAP is a bit similar to that of [28], we use the OTAP for updating security and encryption keys by issuing commands and controls node behaviours, but mainly for intrusion detection and network-nodes restructuring if an attack is detected. For instance, if one node in the network is attacked or an attack is detected or even if a node is suspected of being corrupted, a OTAP command is issued either to restructure the network or to reset the node. The OTAP command can also be scheduled to be issued in cases of for example node quick depletion because of too much traffic in data transmission. This OTAP command can be issued to restructure the network such that all nodes with lower power do less work than the ones with higher energy level. Firmware, update and also other data such as those in [27, 28] can also be sent using over-the-air-programming.

In [29], the authors present a feasibility study of the performance of impersonation attacks on the modulation-based and transient-based Radio Frequency (RF) fingerprinting techniques. They also state that both of these techniques are vulnerable to impersonation attacks; but the transient-based techniques are harder to reproduce due to the effects of the wireless channel and antenna in their recording process. They assess the feasibility of performing the impersonation attacks by doing extensive measurements as well as a number of simulations using collected data from different wireless devices. They then discuss the implication of their findings and how they affect current devices, identification techniques and other related applications.

In [30], the authors present a security overhead analysis for the MAC layer in the 802.15.4 WSN. They further conducted a survey security mechanisms which they define in the specification, including security objectives, security suites, modes, encryption, and authentication. They also identify security vulnerabilities and attacks, and propose some enhancements to improve security and to prevent from attacks such as denial-of-service

attack, reply-protection attacks, same-nonce attacks, ACK attacks, and others. Their results show that, for example , with the 128-bit key length and 100 MIPS, the encryption overhead reaches to up to 10.28 μs micro seconds per block, and with 100 MIPS and 1500-byte payload, the encryption overhead reaches to actually higher than 5782.5s.

Security is one of the big topics researched in the IoT and especially in the WSNs [31–34], and with that in mind, it is very important to be aware of all the short-falls that are involved when talking or discussing the issues related to security. This work focuses on the security at the node level and also the security in the communication between the node and the sink-node & gateway. Cryptography is one of the regularly adopted solutions. It could be difficult to apply longer keys for very secure communication because longer encryption keys require more processing capabilities. However, strong computing and processing capabilities are a short-fall that we find at the bottom level or sensor layer when dealing with sensors. Therefore, we apply solutions proposed in the papers [31] and also try to combine the solution proposed respectively in [34] and [33]. This is done while trying our most best to minimize the overheard of the data because this could possibly cause other problems.

Another important type of attack for which it is very important to prepare for, is the system attack by signal jamming. Apart from attempting to access data fraudulently, attackers can also prevent these data from travelling from the sensors to the gateway or from the gateway to the data storage by jamming the communication's signal. This type of attack has not been thoroughly researched and only a few solutions are proposed. Most of the publications that have been written, only discuss the problems, chances and possibilities of it occurring in a network of communicating sensors, actuators and gateways. There are also a small number of papers that we came across, that gave us the thumbs up for tackling this problem. Researchers such as [35], propose channel switching as a solution to avoid signal jamming and interference. The study was conducted by simulating certain nodes in the network to make them believe they are jammed since they could not use a real jammer. Other researchers [36–38] discuss the topic of jamming. However, we instead considered the research in [39] in which the researcher proposes Multi-Channel Ration (MCR) decoding [39]. This approach consists of using multiple antennas, in this case two, to defend and recover from a jamming attack. The receiver and transmitter use one antenna to respectively receive and transmit data, once the signal is jammed in the communication with that antenna, the communication switches to the other antenna for both temporary transmission and reception, and mainly for recovery from the attack. In this project, since the devices we use are mono-antenna devices and they do not provide us with the possibility of self adding extra antenna, we use two approaches, the use of two communication devices of which both are of the same type, and the use of two communication devices of different types. One of the two

devices is always in sleep mode until it detects unusual behaviors or jamming attack, then it wakes up and starts transmitting and recovering the node from which ever defect it has.

In [40] and [41], the authors present mathematical and statistical models for optimal jamming attacks and network defence policies in WSN. They present a scenario in which an advanced and sophisticated jammer jams a network, controls the jamming probability, and affects the transmission range, which leads to defective and corrupted communication links. Once the jammer is detected, it ceases, and the detection is done by node monitoring in the network. Their work consist of a mathematical sensor network model, and statistical attacker model, and a model for attack detection. Based on their obtained result, with a controllable jammer, their derived solution seems to be very useful and interesting, but also complex and it requires strong computation capabilities if deployed.

2.5 System Interoperability and Patients' EHR Messaging Standards.

Another very important aspect of this research are the Systems' interoperability and patients electronic healthcare records messaging standards.

In [42], the authors investigated a project titled, "HL7 ontology and mobile agents for interoperability in heterogeneous medical information systems. They proposed a system that they called the electronic Medical Agent System (eMAGS), which is a multiple agent system based on the HL7 messaging standards, to simplify the flow of patients' data across healthcare organizations. Orgun and Vu [42], have illustrated a system that uses existing healthcare messaging standards (HL7) to convert data into a frame-based representation of this data with unique ID's and synonyms for each type or concept [42]. They used the IDs to obtain a linking system between the message structures required for various HL7 events and synonyms with the objective of identifying the variations by which these concepts are referred to in the different healthcare systems.

In a work produced in [42], they also made use of open source tools and application such as Protégé-2000, which is an open source tool, as we stated, that assists users in the construction of large scale electronic knowledge bases. This tool is a built-in user interface that allows developers to edit and create domain ontology. Other tools are SNOMED, UMLS, XPETAL, XSLT, etc. . . , for decision-making and some machine learning in handling frames, HL7 frames, and messages.

In [43], the authors discuss in detail the HL7 or Health Level Seven. They explain all the different types of HL7 and of HL7 messages, ranging from the ADT message, ACK

message (Acknowledgement message), BAR (Add/change billing account message), to the VXX (Response for vaccination query with multiple PID matches). There are over 100 different types of HL7 messages, and each message type is made of multiple segments. This information is free and can be found online at the URL: https://www.hl7.org/special/committees/vocab/V26_Appendix_A.pdf.

In [44], the authors suggest an architectural model of a system which targets two departments in the healthcare industry, the Obstetric Pediatric and The Gynecology [44]. The authors, suggest systems' interoperability or the interoperability of systems as a solution to obtain a better access to patients' data. With that in mind, authors decided to deploy and test their system on a cloud, because of its scalable properties [44], and the fact that the cloud is easily accessible and can make the access to patients' data by authorized persons possible, anywhere, anytime. After testing and experimenting, the authors stated that the scalability in cloud computing makes it a perfect platform for implementing systems' interoperability, and especially in the healthcare domain.

In [45], the authors conducted research on an implementation such as the one in the previous paragraph by [44]. They conducted research on implementing a cloud computing system for healthcare organizations, and the focus of this research was on an integrated model for exchanging patient medical healthcare records, in a standard formatted and internationally agreed manner, which are basically the HL7 standards. The study in [45] investigated the issues that healthcare organizations encounter in their usage of various IT applications and infrastructures which are mostly in need of updates as a result of the fast growing healthcare industry and healthcare services. They then suggest a design of a cloud-based and integrated e-Medical records system which uses HL7. In [46], the authors discuss the privacy, security and requirements for healthcare in cloud computing. Another paper that we were interested in is the [47], in which the authors discuss a case study of cloud security in healthcare.

In [48], the authors describe and evaluate the recent and ongoing large-scaled activities which are related to systems' interoperability and system integration of networked clinical research. The paper [48] covers the following topics: the open source/open community approach, acceptance of e-Source in clinical research, the necessity for general IT-conception, interoperability of the electronic health record (EHR) and electronic data capture and harmonization and the bridging of standards for technical and sematic interoperability. Programs and National infrastructures have been set up to offer general IT-conceptions with regard to the direct planning and development of software tools (e.g. TMF, caBIG, NIHR). In order to attain technical and semantic interoperability, current standards (e.g. CDISC) have to be coordinated and linked. Major groups have been made to offer semantical interoperability (e.g. HL7 RCRIM under the joint leadership

of HL7, CDISC and FDA, or BRIDG covering CDISC, HL7, FDA, NCI) and to provide core sets of data collection fields (CDASH). The vital tasks for healthcare informatics within the next ten years will now be the expansion and implementation of surrounding IT conceptions, strong support of the open community and the open source approach, the acceptance of e-Source in clinical research, the unbending continuity of standardization and the bridging of technical standards and the prevalent use of electronic health record systems

In the book [49], the authors presented a lot of information on the principles of interoperability with the patient messaging protocol health level seven(HL7), and the SNOMED as presented. This book contains a lot of information which can be very important when implementing systems that are intended to be integrated into public healthcare systems and platforms. This book provided us with a lot of information throughout the writing of this thesis.

The authors in the paper [50] presents a solution to the integration of information systems, because, one of the priorities of the national healthcare authority is to meet organizational, clinical and managerial needs. Current practice indicates that the most favorable approach to achieve a regional healthcare information system (RHIS) is to use a health level 7 (HL7) message-based communication system implemented by an asynchronous common communication infrastructure between healthcare systems and platforms. The RHIS is a wide-ranging and integrated information system at a regional level that comprises all types of healthcare levels. It can also be expanded to a national, and international level. It comprises interoperability issues that cover most of the necessary components, and that are competent to work efficiently in a secure wide area network to guarantee data privacy and confidentiality. The authors in [50] also investigated another important feature of the proposed solution, which is to create an interoperability framework that can be replicated from one healthcare institution to another. In that sense, shared interoperability messages can be used to join heterogeneous information systems. In response to this approach, more than 10 different groups have submitted proposals to the Greek government and the anticipated interoperability' framework appears to be broadly accepted as a solution to improve information and communication technologies developments in the healthcare sector in Greece.

Chapter 3

Sensing Layer and Sensors' Field-readiness

3.1 Introduction

As we stated in chapter 1, the first research question is covered in this chapter and potential solutions related to the concerned research question are implemented. Their usefulness lies in the fact that the capturing of automatic physiological parameters presents very high advantages, that guarantees error-free physiological data capture in contrast to the manual data capture which is associated with a high probability of producing error-prone readings that can be misleading. This project draws on the recent advanced technology in wireless sensor devices and RFID technologies to create a lightweight, cost-efficient and low-power, off-the-shelf eHealth sensor kit for capturing physiological parameters. This kit coupled with communication technologies, provides multiple advantages compared to the traditional manual system used to capture patients' physiological data. Some articles which are listed above the introduction have helped in the implementation of the sensors' field-readiness.

3.2 The Sensor eHealth Kit

The e-Health sensor kit depicted in figure 3.1, is a platform that allows Arduino and Raspberry Pi users to implement biometric and medical applications where body monitoring is needed by using 10 different sensors that measure: pulse, oxygen in blood (SPO2), airflow (breathing), body temperature, electrocardiogram (ECG), glucometer, galvanic skin response (GSR - sweating), blood pressure (sphygmomanometer), patient position (accelerometer) and muscle/electromyography (EMG) [51].

FIGURE 3.1: The e-Health sensor kit with sensors attached.

Due to the nature of certain sensors and their requirements in order to operate, we will not be able to test certain sensors' field-readiness. The muscle sensor and the electrocardiogram (ECG) sensor require three different types of leads for each experiment which cannot be sourced locally and, up to now, are merely sold together with the whole kit. The glucometer sensor requires real blood, which would involve drawing and handling blood from volunteer subjects, which we could not do, as this research does not cover the insurance of this type of experiment we do not have the expertise or clearance to conduct this type of medical experiment. For these reasons, the stated sensors could not be investigated during this research.

3.2.1 eHealth Sensor Kit Usage Settings

Figures 3.1 and 3.2 are perfect illustrations of how the sensors are plugged into the eHealth shield. Each sensor has its own function for reading physiological parameters, and to allow all of them to read at once, their functions for reading are combined in a single script. They will be able to read vital signs when placed on the body. More details on the use of this kit can be found on the manufacturer's website `http://cooking-hacks.com/`, the document [51] and also in the documentation on the Participatory health-care project we conducted in 2014 [3].

The Software side of the usage of this kit requires an Arduino IDE for use with Arduino, as well as the Raspberry Pi operating system in which the e-Health library must be imported. A GCC compiler must be installed on the machine in order for the code to compile. The eHealth shield into which all the sensors are plugged (Figure 3.1) is

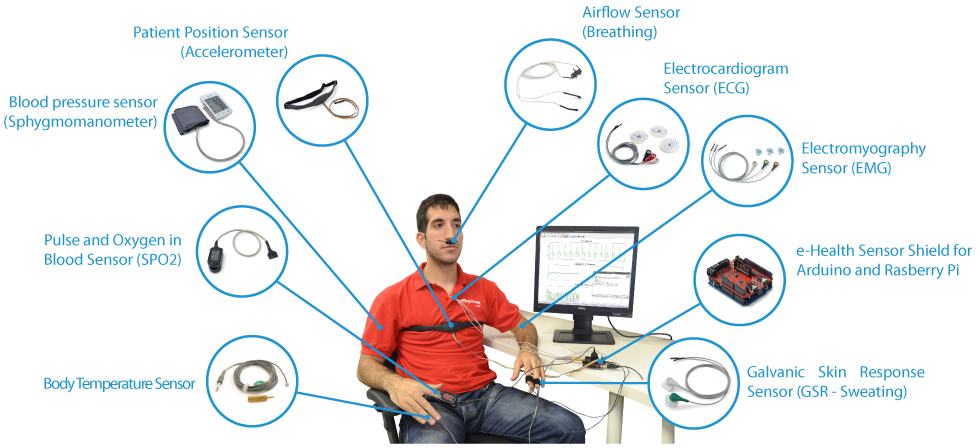

FIGURE 3.2: The e-Health sensor kit usage on a human body.

compatible with both the Arduino and the Raspberry Pi via the e-Health shield to raspberry Pi bridging shield (Figure 3.4).

The code is then compiled to check for errors and if it is found to be error-free by the compiler, it is then cleared for upload. Once the code is uploaded on the Arduino, it will remain embedded until another code is uploaded or, until the device is formatted. To execute the code on the Arduino, the device needs only to be turned on for the result to be directly displayed through the serial monitor or using an LCD display. Note that there are many types of Arduino IDE and each one of them is compatible with a specific Arduino hardware. For the Arduino Uno rev 3 that is used for the implementation of this project, every Arduino IDE of version 1.0.X (where x varies from 0 to the last digit of the last version) works and is compatible with the eHealth library.

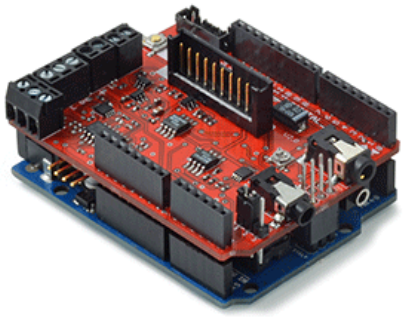

FIGURE 3.3: eHealth shield on Arduino Uno Rev 3

FIGURE 3.4: eHealth shield on Raspberry Pi

The Arduino IDE is a user-friendly development tool that allows the user to write and compile code for the Arduino micro-controller. The Integrated development tool (IDE) that we used for this project is the version 1.0.5r. The sketch (code) is uploaded to the Arduino via a serial port, usually a USB port. The main class of the sketch comprised

of two parts: one that runs once when the sketch starts, and another part that loops indefinitely until the sketch is stopped or interrupted. The top part of the sketch is reserved for variables declarations and external class importation, see listing 3.1.

Every sensor that is used has its own specifications which are described in further detail in the Participatory health-care project conducted in 2014[3, 52], and are also available on the manufacturer's website `http://coocking-hacks.com`. The work we conducted on the participatory health care project [3, 52] provides very useful information concerning hardware and software settings and configurations. However, in this thesis we only provide brief descriptions which enable the reader to get a general idea of the equipment.

```
1
2 // Class Importations or inclusion goes here
3 // Variable declarations goes here
4 void setup() {
5 // Code here ... all that needs to run once
6 }
7
8 void loop() {
9   // All code that needs to run in a loop goes here
10 }
```

LISTING 3.1: Arduino skeleton code explained

The e-Health sensor kit has nine different sensors as illustrated in Figure 3.2, some of which read more than one clinic measurement, mainly all vital signs. Each sensor is tested individually and the results are compared, analyzed and finally a conclusion is drawn. Table 3.1 below presents all nine sensors and the clinical measurement they produce, including those we will not be testing as stated earlier.

TABLE 3.1: Sensors and vital signs

Sensor	Vital Sign(s)
nasal / mouth airflow sensor (Breathing)	Breathing rate
Pulse and SPO2	Pulse and Oxygen concentration in blood
Blood Pressure Sensor	Systolic, Diastolic blood pressure and Pulse
Temperature Sensor	Body Temperature
Position Sensor	Patient Position
Galvanic Skin response Sensor	Electrical conductance of the skin

3.3 Field-readiness Tests and Experiments

Nowadays many devices that are used in IoT research are prototyping devices. They are mainly used due to their affordable cost, with the idea of producing good research products with cheap equipment. In this section the experiments of sensors, some in groups and others individually, and this in parallel with the research questions concerned and the proposed solution in 1. The next section discusses the first concerned sensor is discussed.

3.3.1 The Nasal/Mouth Airflow Sensor

The Airflow sensor, as listed in table 3.1, is a device used to measure the breathing rate in a patient in need of respiratory help. This device consists of a flexible thread which fits behind the ears, and a set of two prongs which is placed in the nostrils. Breathing is measured by these prongs. The specifically designed cannula/holder allows the thermocouple sensor to be placed in the optimal position to accurately sense the oral/nasal thermal airflow changes as well as the nasal air temperature. This sensor is comfortable, adjustable and easy to install figure 3.5.

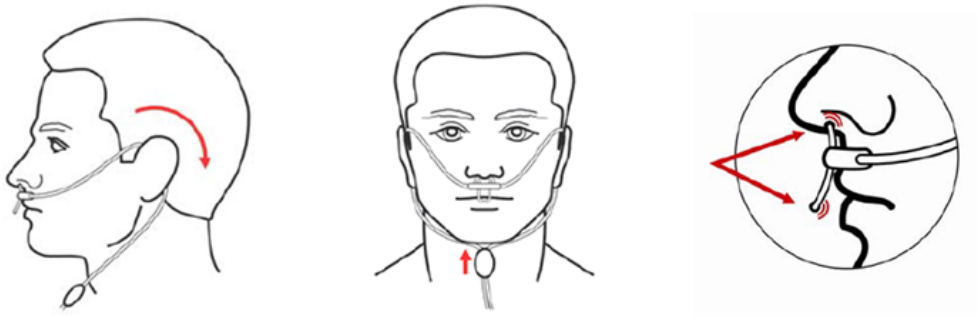

FIGURE 3.5: The e-Health sensor kit's Nasal/ Airflow sensor

Experiment Configuration and Setup

To test this sensor, the following are needed:

- An Arduino (In this case the Arduino Rev3)
- A eHealth shield (In this case eHealth kit V2.0)
- Octave or Kst for visualization and plotting.
- A nasal/mouth airflow sensor customized for the eHealth shield
- A volunteer subject to test on

- And on the software side, the Arduino IDE, and any serial reader or monitor software

The airflow sensor is plugged or connected to the eHealth shield by an analog input, and when the function for reading is called, it returns values from 0 to 1024. Another function returns values directly in wave forms when called, which can be seen using serial monitors. This sensor can be very useful in monitoring patients with Apnea problems, which can lead to brain failure or even death. Apnea is defined as the lack or suspension of external breathing. It can occur voluntarily by blocking the nasal orifices and shutting the mouth, it can also occur mechanically, by strangulation, or as a consequence of trauma or neurological disease. The nasal/mouth airflow sensor device can also be used to measure the rate at which a person breathes, which is particularly pertinent to a patient in need of respiratory help.

```
#include < eHealth.h >
void setup(){
  Serial.begin(115200);
}

void loop(){
  int air = eHealth.getAirFlow();//Returns values from 0 to 1024
  eHealth.airFlowWave(air); // print the values in wave forms
}
```

Listing 3.2: eHealth library's airflow functions usage

One way to find out whether there is a problem with a patient's breathing, is by checking the gaps between inhalation (breathing in) and exhalation (breathing out), as longer gaps are signs of respiratory trouble. With this in mind, this sensor can be used to monitor and record the length of the gaps between respiratory phases. If the difference is above the threshold, an alert is then generated. Listing 3.2 is an example of a code that tracks the air flow of an individual.

Subject One Experiment

Having prepared everything needed to conduct a reading, we then used this sensor to collect respiratory data. The subject was in a resting position, sitting a sofa. The results of this experiment, as depicted in figure 3.6, show that the subject successively inhaled and exhaled, displayed by the fluctuations of the graph. The behaviour of the curve is sufficient to say that the sensor can be used to check whether a subject is breathing or not. However, this is not sufficient to conclude on the field-readiness of the device.

Subject Two Experiment

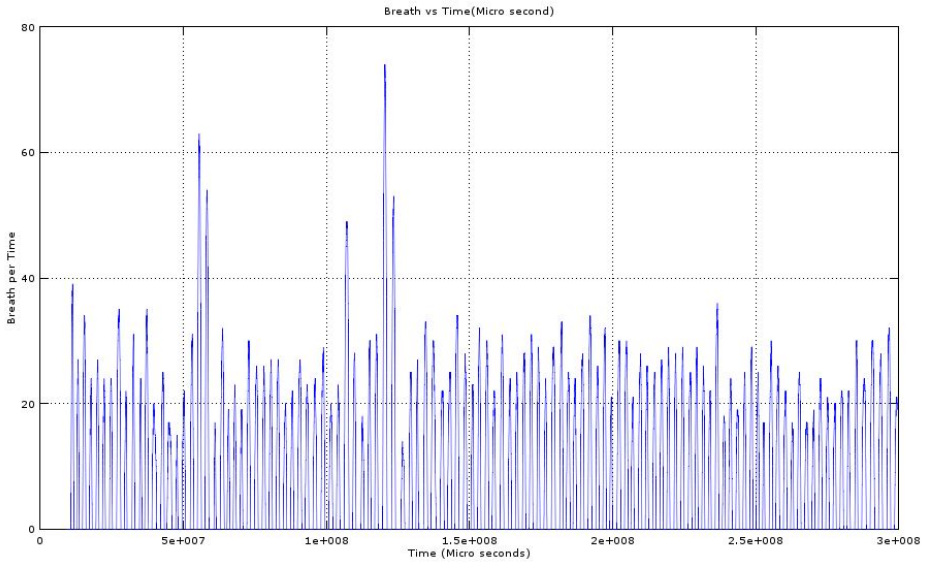

FIGURE 3.6: First experiment and test of the airflow sensor

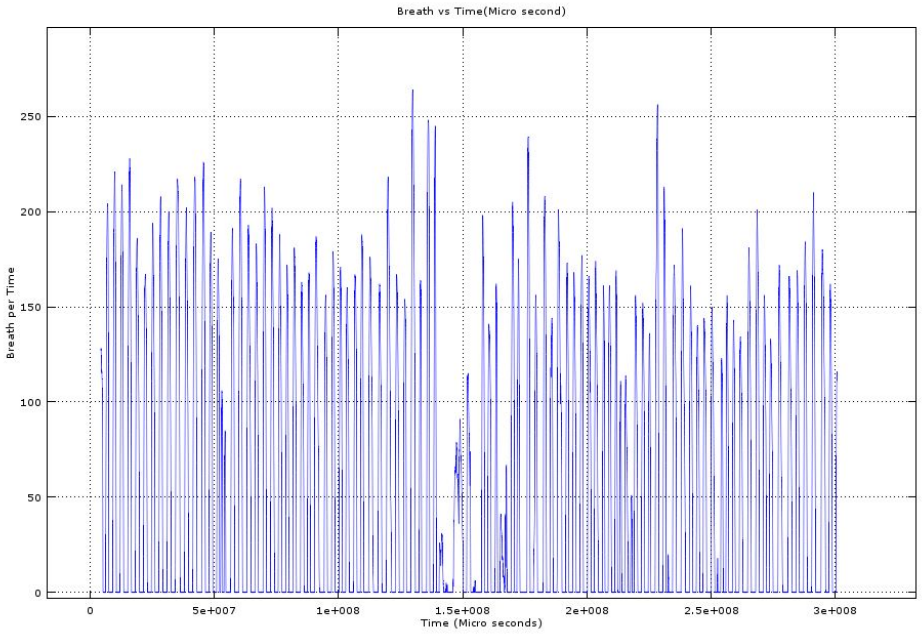

FIGURE 3.7: Second experiment and test of the airflow sensor

In addition to the previous experiment, another experiment was carried out to check the consistency of the result that the device produces. Another subject had the airflow sensor placed in the correct location for usage and we collected respiratory data to compare them in terms consistencies and realism of obtained data. From figure 3.7 it can be seen that the behavior of the curve in the graph is similar to that of figure 3.6, with peaks and troughs. However, the axis boundaries are different from those in figure 3.6.

Observation

The sensor seems to work with two subjects and the results appear to be consistent in terms of data behaviors. The diversity of the amplitude in the graphs is possibly due to the fact that every subject is unique and each person has his own unique way of breathing. With that said, this sensor is better for prototyping, but in cases of major necessities the airflow sensor can also be used in healthcare monitoring to produce meaningful data that can be used. The actual design of the sensor is by far not field-ready, but sufficient for a prototyping sensor. The wires connecting the prongs to the Arduino could be made longer to allow patient movement without disturbing the plugged devices.

After a number of experiments we also observed that the precision in the readings of the sensors is very relative to the position of the prongs in the nasal orifices. Given that the prongs of the sensors measure the pressure at which the air is exhaled from the nasal orifices, the way they are placed is very important and plays a vital role in the precision of the obtained data. Two experiments were carried out—one with the prong placed directly inside the nose, and the second with the prong differently placed to the previous. The data we obtained followed the same pattern; in both cases the plot reassembled the sinusoid squeezed. However, these two experiments differed in the ranges or the amplitudes that were produced; when the prongs are placed very closely and directly in the nasal orifices, the data has higher amplitudes, and in the other case, the data appears to have lower amplitudes.

3.3.2 The Blood Pressure, Pulse and Temperature Sensor

With the help of a specialist in public health and a healthcare specialist, the above mentioned three sensors were also investigated at the same time. These sensors also read measurements that are considered to be vital signs. The Blood pressure sensor reads the systolic blood pressure, diastolic blood pressure and pulse. The pulse sensor reads the pulse and the oxygen saturation in blood (SPO_2), and finally the temperature sensor reads body temperature.

Experiments and tests were conducted with single and multiple subjects. For one subject, the physiological measurements or vital parameters were collected at four different points: in the morning when the subject woke up; after the subject had exercised; in the evening; and after the subject had done some jogging and running. Table 3.2, presents the data collected from our first subject. The blood pressure readings fell in the normal range for an average healthy person who does not have blood pressure problems. The pulse increased with exercise and also fell under a normal range for an average healthy person. A second experiment was conducted with a second subject (see table

TABLE 3.2: Sensor Field Readiness: Daily Activities Monitoring (Subject one)

Days/ Vital signs	Morning	After Exercise	Evening	After running
Systolic blood pressure	Max: 120mmHg Min: 120 mmHg Av: 120 mmHg Range:N/A	Max: 111mmHg Min: 110 mmHg Av: 110.5 mmHg Range:(110,111) mmHg	Max: 133mmHg Min: 129 mmHg Av: 131 mmHg Range:(129,133) mmHg	Max: 111mmHg Min: 111 mmHg Av: 111 mmHg Range:N/A
Diastolic blood pressure	Max: 81mmHg Min: 80mmHg Av : 80.5 mmHg Range: (80 -81)mmHg	Max: 73mHg Min: 71mmHg Av: 72mmHg Range: (71-73) mmHg	Max: 83mmHg Min: 69mmHg Av : 75mmHg Range:(69-81) mmHg	Max: 84mmHg Min: 77mmHg Av : 80.5mmHg Range: (77 -84) mmHg
Pulse	Max: 75 bpm Min: 58 bpm Av : 65.5 bpm Range: (58, 75) bpm	Max: 62 bpm Min: 56 bpm Av : 59 bpm Range: (56,62) bpm	Max: 72 bpm Min: 59 bpm Av : 65.5 bpm Range: (59, 72) bpm	Max: 60 bpm Min: 52 bpm Av : 56 bpm Range: (52,60) bpm
SPO2	Max: 99% Min: 99 % Average: 99% Range: -	Max: 93% Min: 89 % Average: 91% Range:(89-93)	Max: 99% Min: 95 % Average: 97% Range: (95-97)	Max: 94% Min: 89 % Average: 91.5% Range:(94-99)
Temp (^oC)	Max:36.10 Min:36.06 Average:36.08 Range: 36.54 – 36.80	Max:36.83 Min:36.65 Average:36.75 Range: 36.65 – 36.83	Max:36.08 Min:36.06 Average:36.07 Range: 36.73 – 36.75	Max:36.81 Min:36.59 Average:36.80 Range: 36.59 – 36.81

3.3) and the pattern was the same, although the resulting values were not similar. This is expected as every individual or subject is different. With exercising, most of the parameters change by mostly decreasing, but in other cases with a different subject, they increase. In the morning they are lower than in the evening where they increase in most cases because the subject was probably busy during the day with daily activities which are in most cases more like exercising.

TABLE 3.3: Sensor Field Readiness: Daily Activities Monitoring (Subject two)

Days/ Vital signs	Morning	After Exercise	Evening	After running
Systolic blood pressure	Max: 113mmHg Min: 112 mmHg Av: 112.5 mmHg Range:(112,113) mmHg	Max: 127mmHg Min: 119 mmHg Av: 123 mmHg Range:(119,127) mmHg	Max: 121mmHg Min: 115 mmHg Av: 118 mmHg Range:(115,121) mmHg	Max: 120mmHg Min: 117 mmHg Av: 118.5 mmHg Range:(117,120) mmHg
Diastolic blood pressure	Max: 83mmHg Min: 77mmHg Av : 80mmHg Range: (77 -83)mmHg	Max: 79mmHg Min: 78mmHg Av: 78.5mmHg Range: (78-79) mmHg	Max: 81mmHg Min: 69mmHg Av : 75mmHg Range:(69-81) mmHg	Max: 84mmHg Min: 77mmHg Av : 80.5mmHg Range: (77 -84) mmHg
Pulse	Max: 69 bpm Min: 59 bpm Av : 64 bpm Range: (56, 69) bpm	Max: 73 bpm Min: 61 bpm Av : 67 bpm Range: (61,73) bpm	Max: 69 bpm Min: 59 bpm Av : 64 bpm Range: (56, 69) bpm	Max: 79 bpm Min: 68 bpm Av : 73.5 bpm Range: (68,79) bpm
SPO2	Max: 99% Min: 99 % Average: 99% Range: -	Max: 93% Min: 89 % Average: 91% Range:(89-93)	Max: 97% Min: 95 % Average: 96% Range: (95-97)	Max: 99% Min: 94 % Average: 96.5% Range:(94-99)
Temp (^oC)	Max:36.80 Min:36.54 Average:36.64 Range: 36.54 – 36.80	Max:36.83 Min:36.65 Average:36.75 Range: 36.65 – 36.83	Max:36.75 Min:36.73 Average:36.74 Range: 36.73 – 36.75	Max:36.81 Min:36.59 Average:36.80 Range: 36.59 – 36.81

To simplify the way the data in table 3.2 is visualized, we plotted the results of the experiment in table 3.2, so that the pattern can easily be visualized. Figure 3.8 presents a plot of averaged readings of vital parameters obtained using some eHealth sensor kits. Normally, the desired systolic blood pressure is supposed to be greater than or equal to 90 mm Hg and less than or equal to 120 mm Hg. Diastolic blood pressure should normally be greater than or equal to 60 mmHg and lower than or equal to 80 mm Hg. Note that a reading lower than this range indicates low blood pressure.

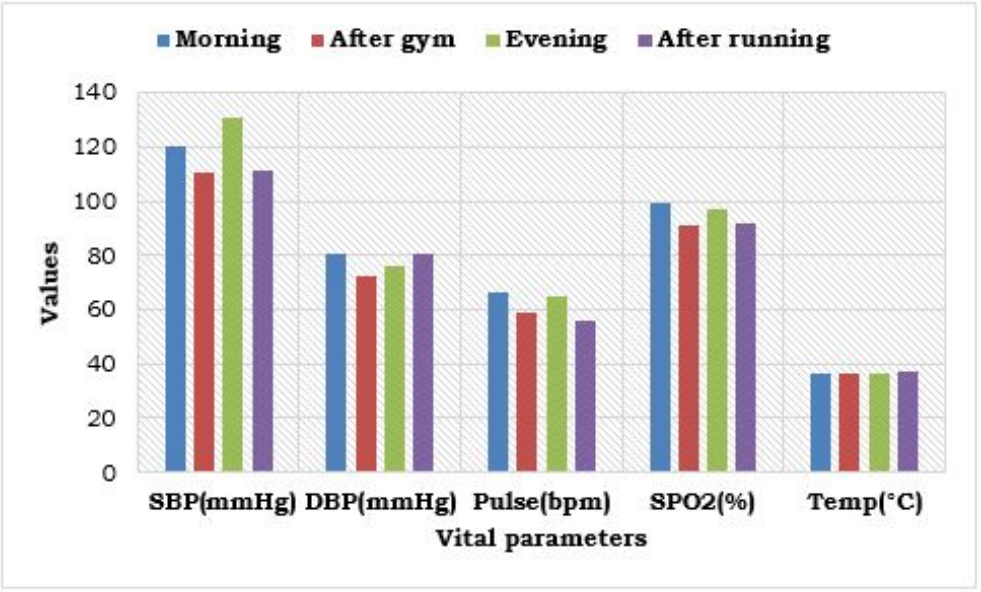

FIGURE 3.8: Detailed field readiness deducted from table 3.2

In figure 3.8 above, we can see that the blood pressure is very normal in both cases, except when the testing subject exercises. This is expected because the blood flow increases and the pressure increases as well. After the experiments which lead us to the above two tables 3.2 and 3.3, we conducted one more experiment, but this time over four consecutive days. Data was collected every day between 17:00 and 19:00 and was averaged both for each day, and for the total of four consecutive days.

TABLE 3.4: Sensor Field Readiness: Four days Activities Monitoring (Subject one)

Days/ Vital signs	Day 1	Day 2	Day 3	Day 4
Systolic blood pressure	Max: 134 mmHg Min: 132 mmHg Av: 133.5 mmHg Range:(132, 134) mmHg	Max: 131mmHg Min: 129 mmHg Av: 130 mmHg Range:(129,131) mmHg	Max: 134 mmHg Min: 131 mmHg Av: 118 mmHg Range:(131,134) mmHg	Max: 130 mmHg Min: 126 mmHg Av: 128 mmHg Range:(126,130) mmHg
Diastolic blood pressure	Max: 79 mmHg Min: 78 mmHg Av : 78.5mmHg Range: (78, 79)mmHg	Max: 82 mmHg Min: 76 mmHg Av: 79 mmHg Range: (82, 76) mmHg	Max: 81 mmHg Min: 75 mmHg Av : 78 mmHg Range:(81, 75) mmHg	Max: 83 mmHg Min: 63 mmHg Av : 73 mmHg Range: (83, 63) mmHg
Pulse	Max: 88 bpm Min: 82 bpm Av : 83 bpm Range: (82, 88)bpm	Max: 79 bpm Min: 67 bpm Av : 73 bpm Range: (67,79) bpm	Max: 73 bpm Min: 67 bpm Av : 70 bpm Range: (67, 73) bpm	Max: 74 bpm Min: 66 bpm Av : 70 bpm Range: (66,74) bpm
SPO2	Max: 99% Min: 95 % Average: 99% Range: (95, 99)%	Max: 93% Min: 89 % Average: 91% Range:(89-93)	Max: 97% Min: 95 % Average: 96% Range: (95-97)	Max: 95% Min: 93 % Average: 94% Range:(94-99)
Temp (^oC)	Max:36.87 Min:36.53 Average:36.70 Range:(36.53,36.87)	Max:37.06 Min:36.64 Average:36.85 Range:(36.06,36.64)	Max:36.98 Min:36.92 Average:36.95 Range: 36.92 – 36.98	Max:36.99 Min:36.91 Average:36.95 Range: 36.91 – 36.99

Table 3.4, displays averaged readings for one subject who was recently diagnosed with early blood pressure problems. As it can be clearly seen from figure 3.9 and which we deduced from table 3.4, the systolic blood pressure is largely above the normal measurement, which is of 120 mm Hg. This high blood pressure reading correlates with the diagnosis that the subject received of early hypertension or pre-hypertension.

However, other parameter's readings are reliable since they fall under the normal and valid ranges.

The sensors investigated in this section appear ready to be used in the healthcare environment based on the results presented in tables 3.2, 3.3 and 3.4, and after consulting couple of professional medical practitioners, the obtained results were confirmed to be valid, reliable and appear to be fairly good. Like any other electronic devices, there are still some little flaws that can be found in these sensors and that can be fixed to make the devices much more reliable, but to the best of our knowledge and based on our experiments, the devices can be used in healthcare practices.

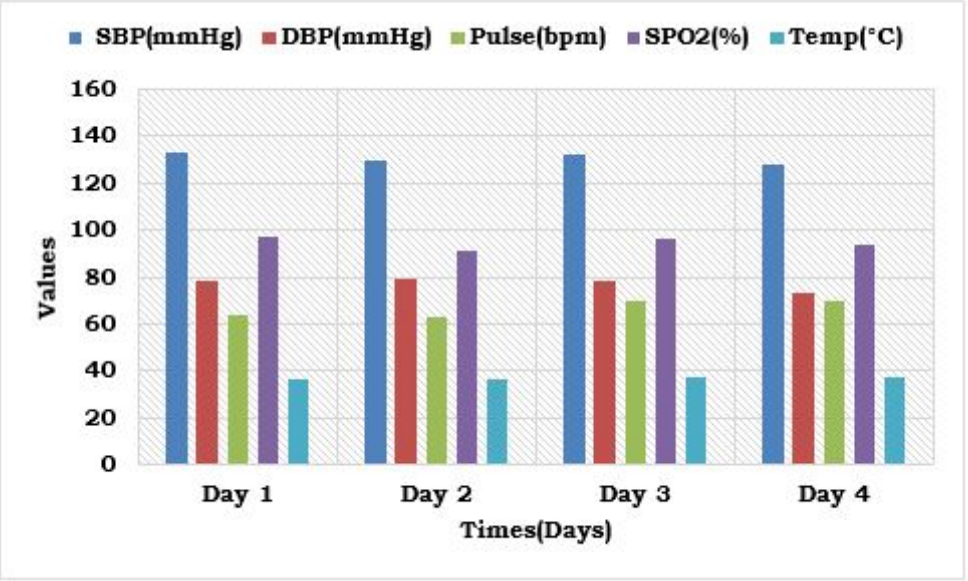

FIGURE 3.9: Detailed field readiness deducted from table 3.4

3.3.3 The patient Position Sensor

The patient position sensor as seen on figure 3.1, is a sensor that tracks the position of the patient wearing it. It is a very important sensor because the data obtained from it can indicate, for example, whether the patient has fallen, or whether he has taken in a position that is not good for his condition while asleep. This sensor is worn or attached to the chest. The Patient position sensor is designed to recognize only 5 different positions as shown in figure 3.10, which are the main positions for a patient in a hospital bed. This is also a major weakness of the sensor, because it can only recognize the 5 positions below. More information about this sensor's specifications can be found in our previous work [2, 3] and more details can be also found at the sensor provider's website `https://www.cooking-hacks.com`.

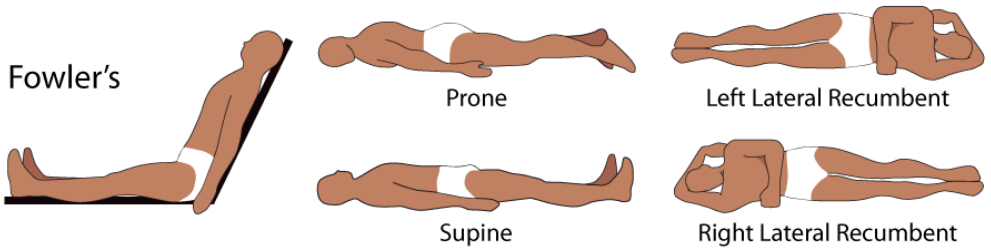

FIGURE 3.10: Patient position sensor

Experimentation with this sensor shows that out of 7 tests for each position the sensor recognized 100% for each position (Fowler, Prone, Supine, right and left lateral recumbent). However, when we tested other positions unknown to the sensor, and which are not lying down positions, such as squatting, the sensor detected some as unknown and some as one of the five positions (see figure 3.10) close to the position being tested.

TABLE 3.5: Test of ten experiments of each specific position with the patient position sensor

Positions	Prone	Supine	Fowler	Right LR	Left LR	Others
Passed	10/10	10/10	10/10	10/10	10/10	7/10
Failed	0/10	0/10	0/10	0/10	0/10	3/10
Pass Accuracy	100%	100%	100%	100%	100%	70%

Table 3.5, shows tests that we conducted with the patient position sensors. As can be seen, all the recognized positions were passed with an accuracy of 100%, but not the unknown positions. In the unknown positions, we had three standing positions, three bending positions, three squatting positions, and one sitting position with the chest leaning more forwards. The obtained results are as follows: the three standing positions, two of the bending positions and two of the squatting positions, were respectively recognized as standing or sitting positions or Fowler position.

3.3.4 The Galvanic Skin Response Sensor (GSR-Sweating)

The Galvanic Skin Response (GSR) also known as the Skin conductance, is a method that is used to measure the skin's electrical conductance [53]. The skin's electrical conductance varies with its moisture level. The relevance of this comes from the fact that the sweat glands are controlled by the sympathetic nervous system. Moments such as those of strong shock and emotions, change the skin's electrical resistance [53]. A sensor (Figure 3.11) that detects these kinds of moments can also be used in lie detection and assist in polygraph tests. In order to obtain better results, the sensor sometimes needs calibration and information about how to do it can be found in our previous work in [3] and more in-depth information on calibration can also be found on

the supplier's website https://www.cooking-hacks.com/documentation/tutorials/eHealth-biometric-sensor-platform-Arduino-raspberry-pi-medical/

FIGURE 3.11: The Galvanic Skin Response(GSR) Sensor

Testing this sensor was a difficult task because real moments of emotions or shock need to be generated spontaneously while the sensor is connected to the user, and that was not only difficult to get but it is also not ethical to manipulate the feelings of a volunteer subject. For these reasons we could not actually use this sensor to get real values. Instead, we moisturized our fingers to get them wet, and as soon as we placed the sensors on the subject's fingers and executed the code we obtained values. But we still could not generate the moment that impacts on feelings or puts the body in a state of shock or emotion.

3.4 Conclusion

To bring this chapter to a close, the eHealth kit, with all its sensors, is not yet field-ready to be used in real hospitals and healthcare institutions. It is, however, ready for prototyping and its implementation of application has high potential. With modification and small improvements such as packaging and extension of wiring, the sensors could reach field-readiness. The kit is designed to test and implement prototypes and provide proof of concepts of eHealth application. Its main purpose is to promote the IoT and the use of technologies in the healthcare industry. This observation is mainly based on the following aspects:

- The way the kit is wrapped: It is almost impossible to handle all the sensors due to the way the whole kit is wrapped and the way the cables stick out from the Arduino micro-controller and the eHealth kit.
- The cabling of the sensors : Most of the cables that allow connections between the sensors and the micro-controller (see figure 3.1) are too short and would not be

long enough for an adult patient to use, given that some sensors are attached to the head (airflow sensor) and some may be attached to the foot(body temperature sensor).

Taking into consideration the above, an improved version of these sensors—in terms of cabling size or length—micro-controller and eHealth shield wrapping could assist in further developing the device to be field-ready for usage in ambulatory healthcare, clinics, hospitals, and other healthcare facilities. That being said, some sensors which form the kits are on their own field-ready in terms of physiological readings accuracy and consistency.

Chapter 4

Networking Layer and Data Dissemination

4.1 Introduction

Data dissemination, is an inevitable aspect in software system development especially when dealing with devices that are low in processing capabilities and low in storage capacities, devices such as sensors. After sensors have captured the physiological measurement, this data need to be disseminated to doctors and processing places where the data will be used for situation recognition or patient situation recognition. In this chapter another research question listed in chapter 1 is discussed. Emerging communication technologies which are considered to be lightweight are used to provide better communication platforms for wireless sensor networks (WSN), technologies such as ZigBee and WiFi light. The last two stated emerging communication technologies and platforms are investigated in this chapter, and a number of networking performance parameters are investigated to assess how the data will be disseminated from the sensing layer of the system to the processing layer.

4.2 Waspmote

In this chapter, instead of eHealth kit on Arduino, we used Waspmote devices for testing the network performance parameters. The reason Waspmotes (see figure 4.1) were used instead of Arduino & eHealth kit is that, eHealth kit are very expensive, and getting enough of these kits necessary for experiments could require a lot financially. On the other hand Waspmotes, although they are also expensive, we have in our possession

enough to create a small testbed network for experimenting. In terms of functions, Waspmote are just Arduino wrapped differently, which is another reason we instead used what we have to experiment and conclude with approximations.

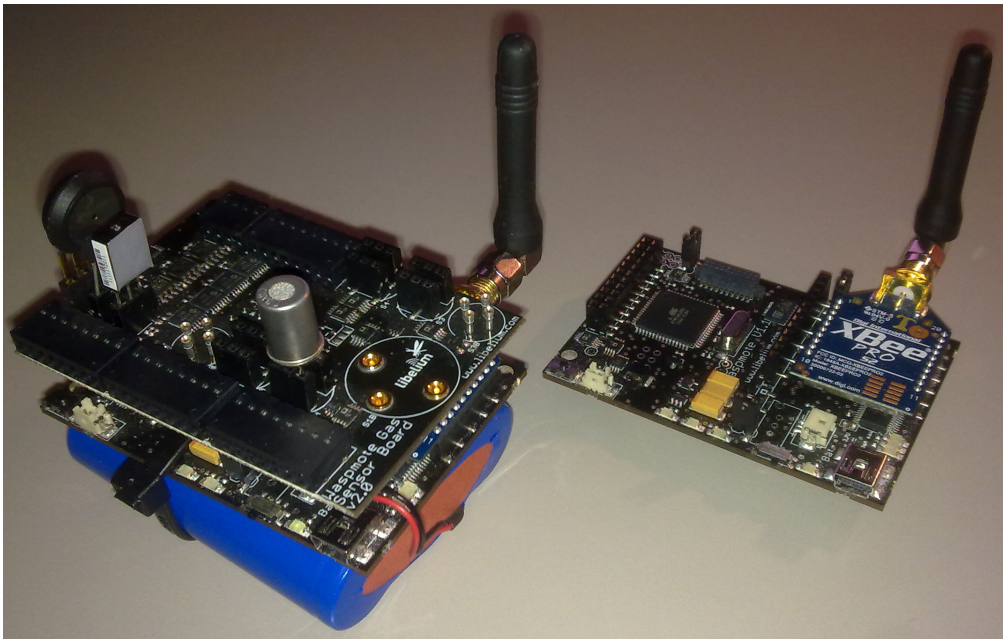

FIGURE 4.1: Waspmote device connected to a Waspmote battery, with a sensor board

By definition, Waspmote devices are open source wireless sensor platforms, specially focused on the implementation of low consumption modes which allows the sensor nodes ("motes") to be completely autonomous, that is battery powered, and rechargeable by customized solar panels [14]. Lifetime of Waspmote sensor nodes may go from 1 to 5 years depending on the duty cycle and the radio used [14].

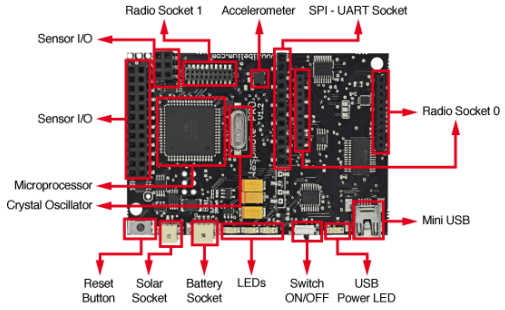

FIGURE 4.2: Front view of Waspmote device described

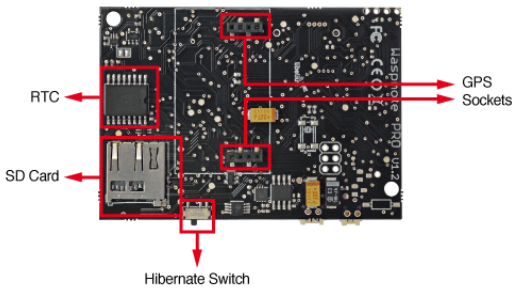

FIGURE 4.3: Back view of Waspmote device described

As described by the front view figure 4.2, and the back view figure 4.3, Waspmote devices are sensor devices which are specially oriented to developers. Similarly to the Arduino, the Waspmote devices work with different communication protocols such as:

the IEEE802.15.4, ZigBee, Bluetooth, WiFi, and 3G/GPRS. Necessary information regarding Waspmotes usage, specifications, software and hardware requirements can be freely obtained from the libelium official website http://www.libelium.com/products/waspmote/overview/.

4.3 The Communication Technologies

Communication technologies and protocols, are devices and protocols used to transfer data. In this thesis, we used the IEEE802.11/WiFi, and the IEEE802.15.4/ZigBee communication protocols. We used devices manufactured by "DIGI". Important information about these devices and their manufacturer can be found on their websites www.digi.com.

FIGURE 4.4: Xbee S1

FIGURE 4.5: Xbee S2

FIGURE 4.6: xbee S6

The figures above are depictions of the devices that we use as communication technologies in this research. Figure 4.4 depicts the xbee series 1 or xbee S1, which can only be configured as IEEE802.15.4 and in a setup for mesh communication(xbee digi mesh). The xbee S1 can act as both, router and end-device depending in how they are configured. On the other-hand, the xbee series 2 or S2 as illustrated in figure 4.5, is simply an updated version of the Se xbee device, which therefore can be configured as both IEEE802.15.4 and ZigBee communication protocol, it can also be set to operate in all topologies including mesh networking, and devices in the network. Like the S1, it can be router or an end-device as well as coordinator for ZigBee mode. The last illustration is that of the xbee S6(figure 4.6). The xbee S6 is a device that was designed to host the IEEE802.11 communication protocol.

The xbee S1 and S2 both communicate on the physical layer, and therefore they use media access control(MAC) address to communicate. On the other-hand, the xbee S6 communicates on the IP or networking layer, therefore they need to be assigned IP addresses, unlike the xbee s1 & s2 that have original and unique MAC addresses which they use to communicate. As we have already stated in the paragraph above, these

devices can be configured in any kind of topology, including a mesh, which is mostly used in this thesis. The devices can be configured using the xctu which is discussed in section 4.3.1, or the devices can also be configured using any serial terminal software which can access the machine's USB ports.

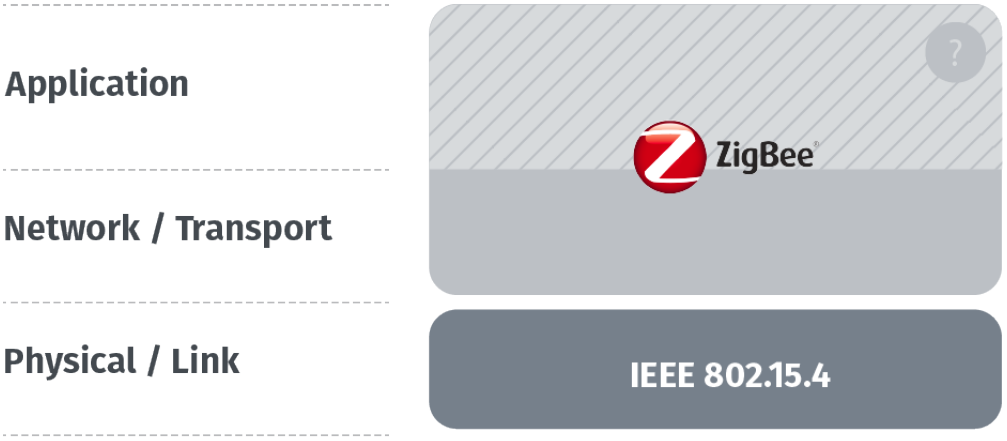

FIGURE 4.7: Osi versus IEEE802.15.4 and Zigbee model

In Figure 4.7, we illustrate how the IEEE802.15.4/ZigBee stack matches the OSI stack. The IEEE802.15.4 communicate on the physical layer using only MAC addresses. The ZigBee stack is built on top of the IEEE802.15.4 standards, and it uses its model, in which the network Layer has direct access to the MAC address and the MAC layer overall. The ZigBee Network layer provides to the network with topologies, MAC addresses management, discovery protocol, routing and security services. Applications are built on the ZigBee stack through the application interface (API). The ZigBee Alliance also has an application profiles for specific application categories, which allow standardization of the functionality, which also improve compliance and interoperability among different vendors' products. Note that the ZigBee stack doesn't use all the features of the IEEE802.15.4 standard MAC.

4.3.1 The X-CTU Software

X-CTU software is a user-friendly open source software for configuring and managing the xbee devices. Like their xbee devices, the software is also provided by DIGI and can be freely downloaded from `http://www.digi.com/products/xbee-rf-solutions/xctu-software/xctu`. The xctu can be used to set different parameters such as network ID, destination node MAC address and communication mode(broadcast, multicast or unicast), enable encryption, updating firmwares, etc... [54]. The devices can also be configured with any serial terminal in what is called the "AT", by issuing AT commands. Once the command "+++" is issued and the device returns "OK" to the terminal, it

means it is ready to be configured in "AT" mode. Commands such as "setSSID", etc... can be issued to set and get certain specific variables.

The software is very user-friendly and specially easy to use, and the newer the version, the better and the more user friendly it is. Multiple devices are configured with the same network ID, and configured to communicate in broadcast mode. With a single device connected to a single port on a machine running the X-CTU software, it is possible to scan all the live nodes in the range of communication. These are just couple of few things that the X-CTU software can do. More detailed information can be found at http://www.digi.com/products/xbee-rf-solutions/xctu-software/xctu.

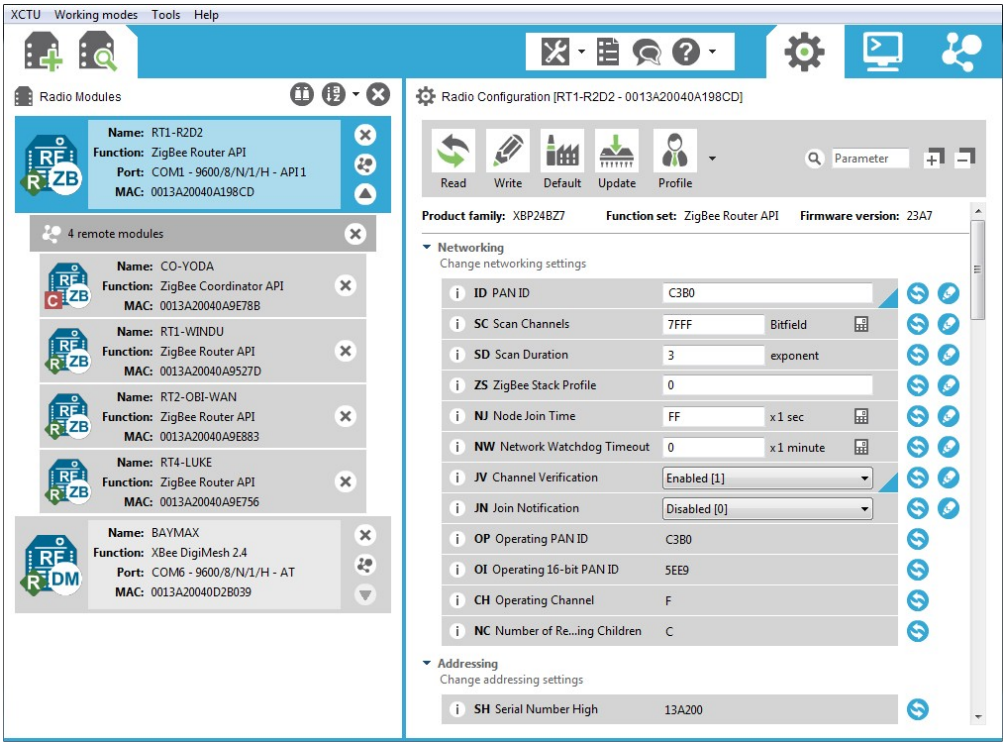

FIGURE 4.8: Basic x-ctu layout of the home screen

When looking at figure 4.8, on the left side of the figure, we can see that multiple zigbee devices are connected and that the zigbee device with MAC address 0013A20040A198CD, has discovered 4 more devices or modules in its entourage. The modules labelled with a green "R" are routers and those with a red "C" are coordinators. On the the top right side of the figure, there are tabs and from the right side to the left side are the network working mode, the console working mode, and the configuration working mode. After the configuration working mode, there is a palette menu of 4 icons of which one is for seeking help, one for comments and suggestion and the other two are respectively mainly for frames generation and communication testings [54].

On the left most side of the screen in figure 4.8 are two of the principal features of the software, namely the keys to any use of the software, as they are the way of adding

devices once they are plugged to a machine running the software. The add "+" sign is for adding a device from a specific USB port. Once the button is clicked, a window opens from which the user can choose the port to which the device they want to add is connected, the baud-rate and other specifications. Next to the add button, is the search button which is very helpful because once clicked, it gives the user the possibility of adding as many devices as possible as long as they are all connected to the machine from which the software is ran. Unlike the add "+" button which allows the user to select one option for every selection, the search button allows the user to select multiple devices (from USB ports) to add at once. It is basically a multiple add button.

4.3.2 The IEEE802.15.4/ZigBee

The ZigBee is high-level communication protocol used to deploy small low-power digital radios in a personal area network (PAN) [55]. It is a IEEE802.15.4-based communication protocol. The Zigbee technology as defined by the ZigBee alliance, is intended to be cost-less and simpler to use than other wireless personal area networks(WPANs), such as the IEEE802.11, or the Bleutooth. It is also designed for short-range low-rate wireless data dissemination [55].

On the other hand, the IEEE802.15.4 is a standard of communication that specifies the MAC layer as well as the physical layer for low-rate WPANs. This standard is well looked after and maintained by the IEEE802.15.4 working group, which defined it in early 2003 [56]. These standards and specifications are the basis for the zigbee communication protocol [57], the ISA100.11a [58], Miwi, WirelessHART, and Thread specifications, and each of which additionally lengthens the standard by merging the upper layers which are not defined in IEEE 802.15.4. Alternatively, it can be used with 6LoWPAN as a Network Adaptation Layer and standard Internet protocol and/or IETF RFCs defining the upper layers with proper granularity to build a wireless embedded Internet. See figure 4.7 above for details on the layering of the zigbee/ IEEE802.15.4. The IEEE802.15.4 operates in multiple frequencies most of which (the 800 MHz and 900 MHz) only operate in the European and American regions). The 2.4 GHz operates all over the world.

4.3.3 The IEEE802.11/WiFi

WiFi is a communication technology where devices of electronic nature are used to connect to a wireless network [59]. These networks are usually password protected, but may also be open, which allows any device within the range of the network to access the resources of the wireless local area network (WLAN) [59]. The WiFi Alliance defines

it(WiFi), as any "WLAN" product based on the IEEE802.11 standards [59]. Devices that can use the WiFi includes computers, tablets, cellphones, printers, and also devices such as xbee S6 devices.

WiFi is a very common communication technology used nowadays for device communication and data transfer. However, because of its low cost and efficiency in battery usage, the IEEE802.15.4 communication protocol is taking over slowly but surely as the best communication technology for data transfer. This is because it does not also require huge infrastructure to be deployed, especially when deployed in the IoT domain, the zigbee and IEEE802.15.4 are much better than the WiFi even with regards to their battery consumption as we will see in the sections to come.

4.3.4 IEEE802.15.4/ZigBee vs IEEE802.11/WiFi

Below in table 4.1, is a list of properties that seems to differentiate the 802.15.4 communication protocol from the 802.11 communication protocol. There a lot of parameters to consider when comparing IEEE802.15.4 and IEEE802.11 but, in this thesis we considered only those listed in table 4.1. Note also that, there are many types of IEEE802.11, there are the a, b, n and the g types of communication standards, but in this table only the IEEE802.11n is used.

Properties	802.15.4	802.11n
Ranges	75m	240m
Frequency	800Mhz, 900MHz, 2.4GHz	2.4 and 5 GHz
channels	16 (for the 2.4 GHz) and 1 (for the rest)	14
Data rate	250 kbps(for the 2.4 GHz), 40 kbps(for the rest)	248 Mbps
Type	PAN	LAN

TABLE 4.1: IEEE802.15.4 protocol versus IEEE802.11 protocol table

4.4 Experiments & Results

4.4.1 Power Consumption

Power consumption is one of the big issues not to be overlooked when implementing and deploying IoT applications because in most cases, devices on the network are individually deployed and are either rechargeable by solar power storage, or a limited source of power which, if exhausted, the device will no longer serves the purpose for which it was deployed for. Therefore, it is very important need to implement the system in such a way that it drains less power while doing more of the job the device was deployed to do.

The performance parameters of the IEEE802.15.4 and the IEEE802.11 are compared in this section especially with regard to power consumption. For these experiments, we used waspmote devices which run on rechargeable batteries. Given the price of a single eHealth kit, the quantity needed to conduct the experiments in this chapter, and also the facts that Waspmote are just Arduino well wrapped, we used Waspmote devices to experiment communication and data dissemination instead of Arduino and eHealth kit. A code for broadcasting a simple hello packet and resending an acknowledgement once a packet is received was implemented and uploaded on the waspmote. The motes were then stripped from their recharging source and were left to run on their limited source of power continually over night while storing information about their battery status in files on the SD card.

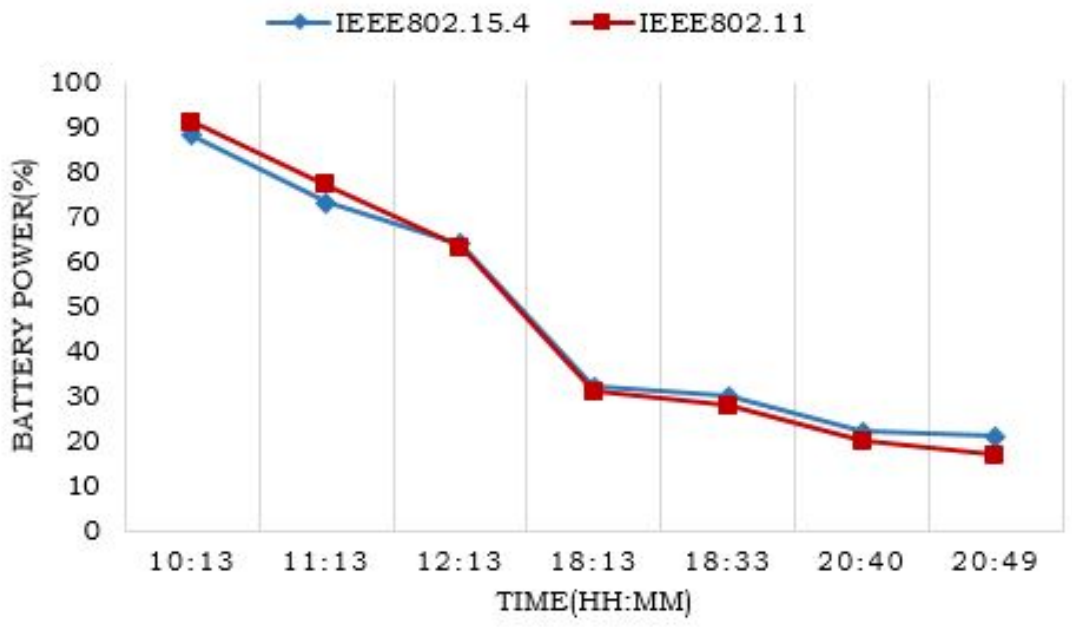

FIGURE 4.9: IEEE802.15.4 vs IEEE802.11 Power Consumption

As depicted in figure 4.9, the waspmotes ran on batteries for over 10 hours. Although the waspmote deployed with xbee S6 started with a high percentage of battery power, it ended with lower remaining battery power. Figure 4.6 above confirms that the IEEE802.15.4 does not consume much power while communicating and transferring data using wireless, unlike the IEEE802.11. This can be observed by the fact that at the time of 10 : 13 when the experiment started, the IEEE802.11 started with a slight higher percentage of battery power, however, when the experiment was terminated, the IEEE802.15.4 had more remaining battery power. The speed at which the power is drained from the batteries is also very high because the motes run continuously for ten hours or more. If they are configured to operate in a sleep and wake mode, they can

actually achieve over 10 hours or perhaps double this if the mote is set to sleep after a certain time of working and continue the cycle.

4.4.2 Signal Strength (RSSI)

The received signal strength indicator, also known as RSSI, by definition in telecommunication, is a measurement of the power present in the received radio signal[60]. The RSSI is usually invisible to a human eye of the user, and cannot be physically felt by the users of a receiving device. Yet, because it can vary greatly and have a negative effect on the communication between wireless devices, both the IEEE802.11 and the IEEE802.15.4 often make the measurement available to the users [60]. In this section, we present an investigation on the RSSI measurements collected while testing and comparing our two communication protocols.

4.4.2.1 The Static Communication

The investigation consisted of sending simple packets from a single device to multiple receiving devices situated at a certain distance, then collecting information about the power of the signal and attaching it to the acknowledgement that is returned to the source. Note that the packets sent in this case were made up of basic node information, like on board waspmote temperature, remaining battery power, node MAC address, node ID, node name and a simple hello string.

Given factors that can affect the communication and specially the communication with the IEEE802.15.4 and the zigbee, we considered testing the communication, "outdoors", with a clear line of sight for both communication protocols concerned here, then afterwards we tested them "indoors" introducing the factor and the impact of the number of wall(s) between the sending devices and the device(s) on the receiving side. All the experiments were conducted with the main goal of optimizing the solution by maximizing the services in terms of better communication, while minimizing the cost of the latter. After running a number of experiments, the average result of all experiments is as shown is figure 4.10 below.

As can be seen in figure 4.10, for the IEEE802.15.4, as the distance increases, the signal strength becomes weaker and the quality of communication becomes poorer. On the other than because we connected the xbee S6 devices to an existing access point to test the signal strength, the coverage of communication became wider. and therefore for the first 15 m the signal strength stayed stable around -66dBm. But if the communicating devices are placed further away from the access points, the signal strength start

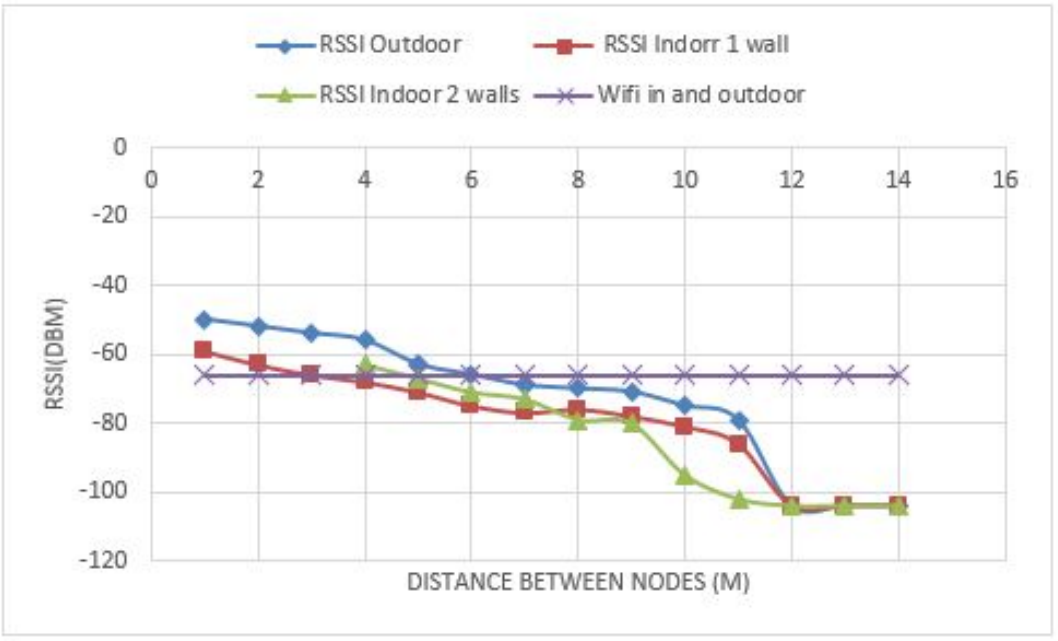

FIGURE 4.10: IEEE802.15.4 vs IEEE802.11 Indoor, and Outdoor RSSI

decreasing at a certain distance. The specifications of each device are main keys to the indications of the approximation of the each device's range of communication.

Although the device's specifications may give indications on how far these devices can range in communication, it is unlikely that you will get results similar to the ones given by the device's specifications, and this is because the devices were originally tested in a controlled environment which we could not simulate or generate. Therefore, the results obtained in this research are not definitive, and are very relative to the area in which the device(s) is(are) tested. For this project, since the aim is to deploy these devices in clinics, hospitals, healthcare facilities or public places, in cases of pollution monitoring, we decided to test the devices in a very normal place where people living their day to day lives, which means that at least one other devices that can interfere with our test was used.

Whether it was indoor with one, two or three walls, or outdoors, every time we experimented with the devices and tested the communication in terms of signal strength on the receiving side, we obtained different results for each experiment, even if the circumstances were similar. The results in figure 4.10 above were obtained by averaging the results of the six experiments conducted.

4.4.2.2 Opportunistic Communication

After, investigating the RSSI for the static communication, we shifted our focus to investigating the behaviour of the RSSI in opportunistic communication scenarios. As we have already indicated earlier, opportunistic communication in this study refers to the kind of communication in which either the sender or the receiver is moving while transferring or receiving data. In this project, two types of the opportunistic communication are considered, ground-based opportunistic communication, and aerial opportunistic communication.

Ground-based Communication

Ground-based opportunistic communication investigates the types of opportunistic communication, in which both the sender and receiver are at the ground level. A basic example could be that of a public transport bus collecting or transmitting information everyday as it goes through it normal daily route in which receiving or transmitting devices are deployed alongside the bus route.

In one experiment, a transmitting device was attached to a moving person at the slow walking, fast walking and running speed transmitting information to deployed and ready-to-receive devices, and in the other experiment a receiving device was attached to the person, travelling at the same speed as in the previous case, but in this case collecting data from deployed sensors along the path. Figure 4.11 below depicts the information about the behaviour of the devices in terms of signal strength. All experiments conducted with the IEEE802.11, resulted in signal strengths with a minimum of - 41 dBm and a maximum of -51 dBm. Therefore, once more, the IEEE802.11 out performs the IEE802.15.4, in terms of signal strength.

Aerial Communication

Aerial communication, in this case refers to the communication where either the sender or the receiver devices are attach to a drone or any other object flying at a lower altitude, lower than 20 metres. The aim of this experiment was to investigate how far in terms of altitude the different communication protocols investigated here can freely communicate. Figure 4.12 shows the results of our investigation

With regards to the multiple experiments that we conducted, the results of the received signal strength (RSSI) are as shown in figure 4.11. Again, it is possible that if these experiments were conducted in a different area, they could result in obtaining different results, but for the experiment we conducted, at each distance, the received signal strength, fell in the range Minimum RSSI (-dBM) and maximum RSSI (-dBm)

FIGURE 4.11: IEEE802.15.4 ground-based RSSI comparison

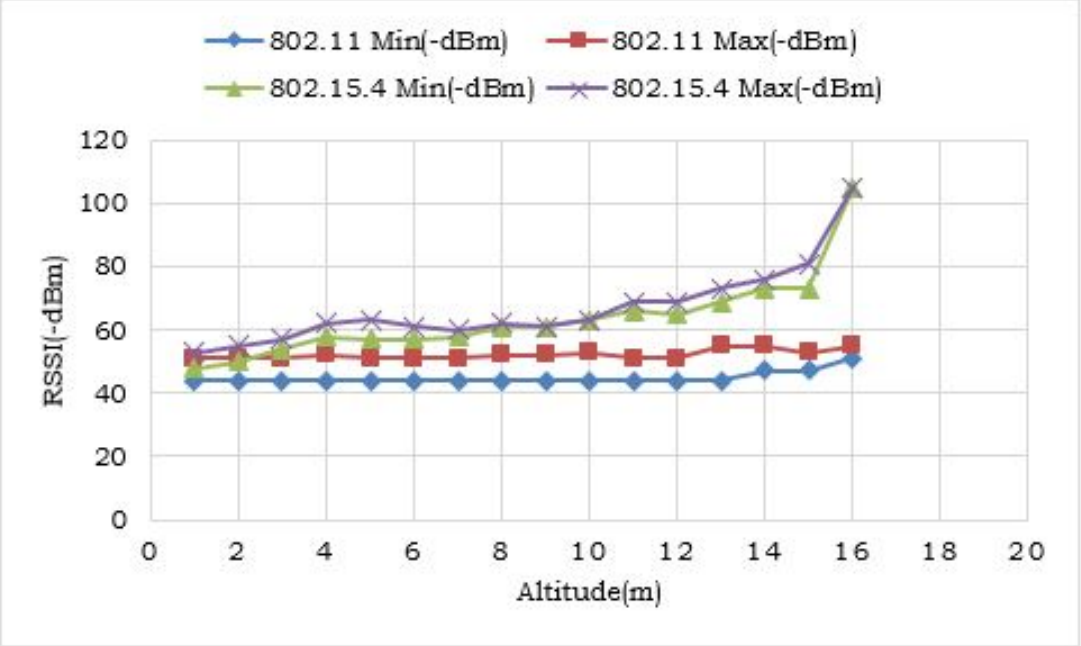

FIGURE 4.12: IEEE802.15.4 signal strength ranges in aerial communication using drone

4.4.3 Throughput and Packets delays

The throughput is defined as the measure of how many units of data or information a system can process in a given amount of time [61]. This concept is broadly applied to systems ranging from countless features of computer and networking systems, to

organizations. Other related measures includes, the RSSI as discussed in the section above, the packets delay, etc ... In order to study this feature, the investigation is divided into two parts, static communication, in which, as we have already stated, both the sending and receiving devices are static, and opportunistic communication, where either, or both of the sending device(s) and(or) receiving devices are mobile and constantly in motion while transmitting data.

4.4.3.1 Static Communication

Static communication covers all types of communication in which both the sending devices and the receiving devices are fixed at one location. This communication is very common in the IoT domain nowadays. This communication can be a point to point communication or even a point to multiples other points communication. The topology of the network can vary from tree, star, mesh or a mixture of different topologies. In this project, the static communication of the IEEE802.15.4 communication protocol of the 2.4GHz is investigated and compared to the results of the IEEE802.11. The communication is also based on the location of either the sender or the receiver devices, for example if this communication takes place inside buildings, we refer to it as indoor communication and if it takes place in an open spaces with a clear line of sight, we, refer to it as outdoor communication. In the next section, indoor communication is discussed.

Experiment results and setup

In this chapter, the setups for every experiment that aims to test the connection or any communication's performance parameters, are very similar. They all involve one or multiple devices sending data to one or also multiple devices. Regarding the throughput, a fixed number of packets were sent, from one device to multiple devices situated at different distances ranging from 1 metre to the distance where the data can not be received anymore. The number of received packets was then recorded. In figure 4.13, a graph of the ratio of received packets per sent packets, by distance or range of communication is presented.

As with the RSSI, for the IEEE802.11 or WiFi, we connected to an existing access point that we created with a mobile device, and the network coverage seemed to be far larger than that of the IEEE802.15.4, and hence resulted in higher throughput as the distance or communication range increased. The throughput, like with the RSSI, is relative to the area in which the devices are deployed. It is more likely that, if this experiment was conducted on a farm or in the mountains or somewhere where there are fewer sources of interference, much better results could be obtained.

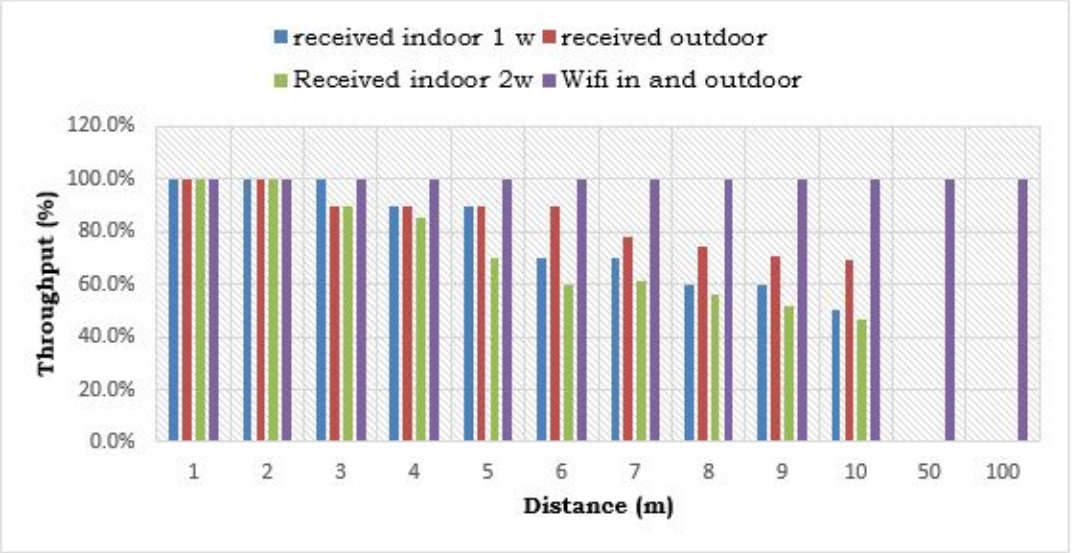

FIGURE 4.13: IEEE802.15.4 vs IEEE802.11 Indoor, and Outdoor throughput

The WiFi/IEEE802.11 without question outperformed the IEEE802.15.4/ZigBee in terms of throughput, more sent packets from the sender's side arrived and were delivered to the receiver's side in the IEEE802.11 than in the IEEE802.15.4. However, as we progress with the study, and after we have studied all parameters, we may discover that the IEEE802.11 is actually better than the IEEE802.15.4. Only in certain cases, by combining the different performance parameters and by maybe optimizing the cost of communication.

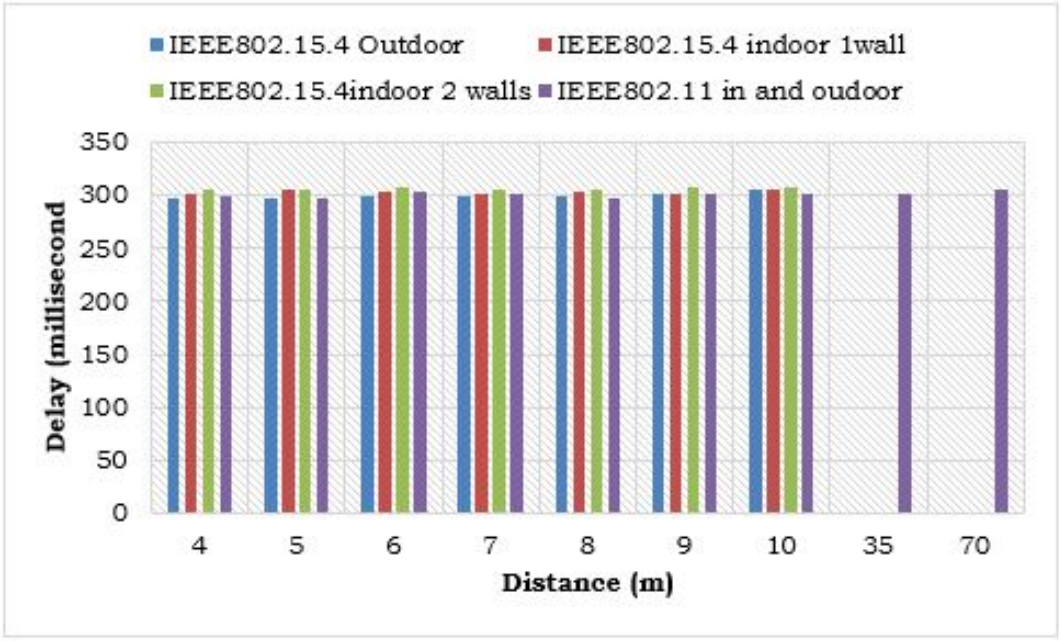

FIGURE 4.14: IEEE802.15.4 vs IEEE802.11 Indoor, and Outdoor Packets delays

Figure 4.14 depicts a summarized graph of a comparison of the packets delivery delay time of the IEEE80.15.4 and the IEEE802.11 in both indoors with walls, and outdoors configuration. Once again, the IEEE802.11 outperformed the 802.15.4 because of its consistency in packets delays and the average packets' delay time. Again it is very important to state that these results are very relative to the time at which the experiment was conducted, and also very relative to the area in which the experiment was conducted. We say relative to the time and the area because, for example, if deployed in residential areas, people often cook, and use appliances like microwaves which are very strong in interference. and if the experiment is conducted during this time, the results could be very different. The above results in figure 4.14 are an average of results from experiments conducted at different times in a couple of areas. That is why we suppose that these results are a close approximation to what can happen in most cases if a system is deployed with the devices discussed in this research.

4.4.3.2 Opportunistic Communication

Opportunistic communication in this study refers to any sort of communication that involves one or more communication device(s) or technology(ies) communicating or exchanging data with one or more other devices, while either the sender(s) or the receiver(s) or both, are in motion while the data exchange is taking place. This type of communication can be very useful in applications such as smart parking, smart farming, or even environment monitoring, where nodes collecting environmental data are planted all around the area of interest, and mobile objects such as cars and buses mounted with receiving device can, on their daily driving routing, collect information of interest about the environment of the concerned area of interest. The study conducted here involves opportunistic communication where a person(running, slow walking, fast walking) and a drone(hovering over sender devices) are considered as data collectors.

Given the nature of this type of communication, it is very likely that it will take place mostly outdoors, which is why all the experiments in this section were conducted outdoors. Two types of experiments were carried out:

- The experiment with either transmitting or receiving devices placed on a person's body.
- The experiment with either the transmitting or the receiving device(s) mounted on a drone.

Ground-based Communication(Slow walk, Fast walk, Run)

A. IEEE802.15.4/ZigBee

In the first experiment, we had couple of receiving devices carried by a person walking/running past sending devices, and vice-versa. In the case mobile clinics users with eHealth kits could be moving in very remote areas collecting data about certain patients, and all along their path, gateways and xbee data receivers could be placed for data transmission as they collected. In the same way, information about environment, or in a smart farm can be collected and stored in a SD card, and from time to time a gateway can pass by and if one of these devices detects the presence of a gateway, it triggers data transfer. Series of experiments were conducted similarly to the static experiments but this time adding the mobility of at least one communicating device.

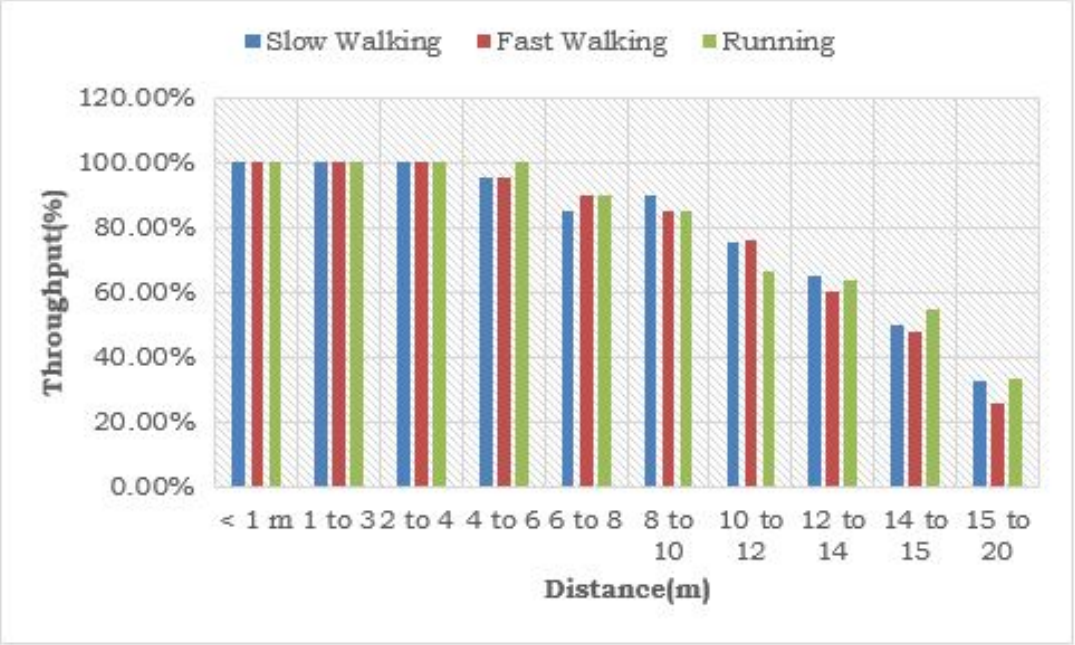

FIGURE 4.15: IEEE802.15.4 Throughput experiment one

Figure 4.15 is a graph of collected information regarding data throughput, and as can be seen from the figure, in a communication range of up to 15 metres, the throughput is slightly higher than 50%, which is a good thing, but still not for enough for implementation in sectors like eHealth, because of the nature of the data and the use of it to make huge decisions which could cost lives. Logically speaking, when communicating devices are in slow motion, it is probable that they can efficiently transmit data as compared to communicating devices in fast motion or very fast motion, and this is because, slow motion is relatively close to no motion at all, and the higher the speed of motion, the further it is from static or no motion. However, the data obtained in figure 4.15, does not follow these rules in all cases. In same cases, for example at the communication distance of 12 to 20 metres, when either one of the communication devices is in fast motion, it actually obtained a higher percentage of throughput compared to the one in

the middle or average speed motion, and this is probably because they might have been interference when we experimented on the communication in slow motion, which was probably not there when we investigated the communication while running.

To further investigate the behaviour discussed in the previous chapter, another experiment was conducted on the same day, at the same time in same area, and the results although different, followed the same pattern. Figure 4.16, is a representation of the obtained results or the experiment output.

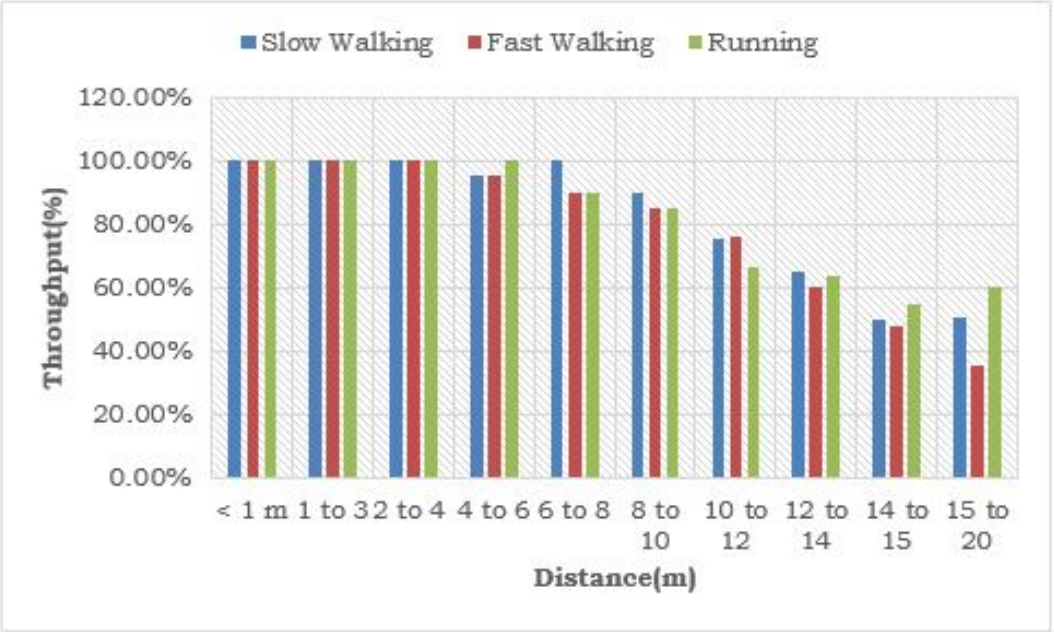

FIGURE 4.16: IEEE802.15.4 Throughput experiment two

B. The IEEE802.11/ WiFi

With the aim of comparing the performances of both the IEEE802.15.4 and the IEEE802.11, another series of experiment were conducted, but this time with the IEEE802.11. The setup was also similar to that of the experiment in the section above. Once again, and in a different scenario, we have discovered that the IEEE802.11 outperformed the IEEE802.15.4 in terms of range of communication or communication coverage. Figure 4.17 depicts the results of the first experiment.

As the figure stipulates, the coverage range in similar scenarios as in the previous section above, has extended to up to 50 metres in open site, outdoor communication. However, at longer distances, the throughput percentages drops and becomes very poor and intolerable for a system that collects critical data for critical decision-making. Note that this experiment was conducted with the xbee S6, and they are devices that need to connect

to an existing access point in order for them to communicate. For this specific experiment we created an access point with an android device, to which we connected the devices to allow them to exchange data. The strength and weaknesses of the properties of the created access point may also play a major role in the behaviour of the throughput parameters.

FIGURE 4.17: IEEE802.11 Throughput experiment one

To test the impacts of the access point in the communication, and in order to find out whether the specifications of the access points influences the throughput, we conducted another experiment in parallel with the experiment the data of which are shown in Figure 4.17, but in this case, we used an existing access point in the area, with higher quality devices and a high performing antenna, and the results were as in figure 4.18. With a much better access point, the results seemed to improve and much better results were obtained. The difference might be very small in many cases, but it can turn out to be very important in some cases. For example, if the difference is 10% or if the throughput increased with 10%, this could mean 100% throughput for all previously 90% obtained throughput. However in a case below 40% the difference might also turn out to be meaningless, because the change in throughput is still below 50%, even though 50% is not the average throughout percentage for critical decision-making data exchange.

Aerial Communication

A. The IEEE802.15.4/ZigBee

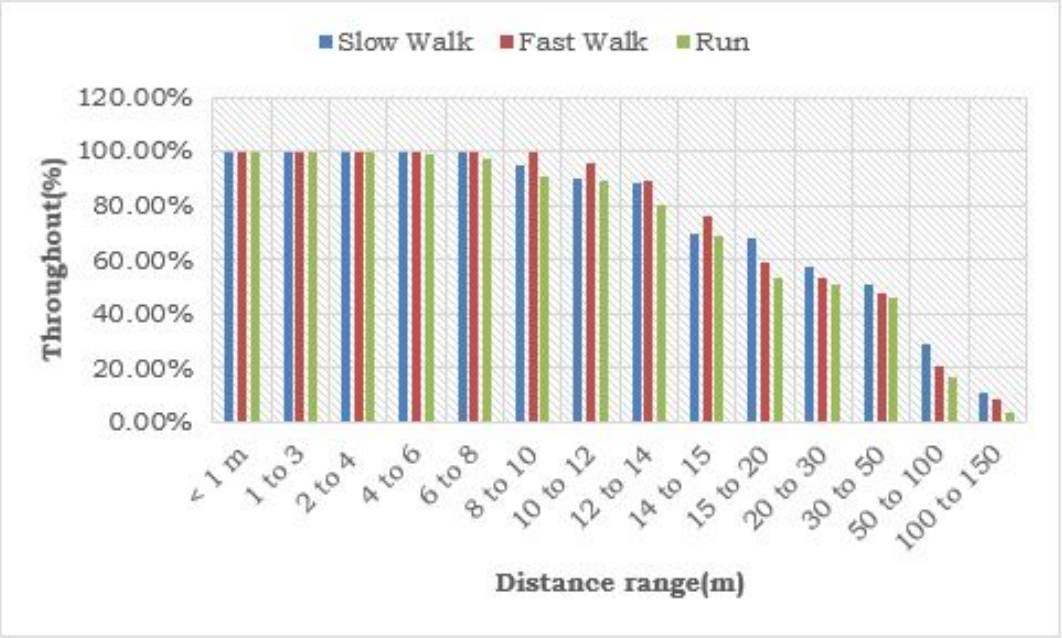

FIGURE 4.18: IEEE802.11 Throughput experiment two

In this section, we explain works and experiments conducted where whether the data transmitter or the data receiver is attached on a drone. The aim of this research or experiments is to investigate another aspect of opportunistic communication. Two types of experiments were conducted in which, respectively, the sending devices were attached to the drone, and the receiving device was attached to the Drone. Data about packets throughput per altitudes were collected as part of the experiment.

In these experiments elevations or height are considered with approximation because drones do not fly in a straight line and at an exact height. There are factors that have a major impact on the drone's flight. The wind and the weight of the devices attached to the drone make a difference and also in some cases, the drone will have to either fly at an elevated altitude or at a lower altitude to avoid obstructions and obstacles.

Figure 4.19 shows 4 different experiments conducted with drones. In two of these experiments the drone had a receiver mounted on, and in the remaining two a sending devices was attached to the drone. The experiments were conducted per communication technologies, and this section only covers the experiments with the IEEE802.15.4. As figure 4.19 shows, in both cases, when the drone acts as a receiver to collect information from deployed sensors in specific areas, it performs much better then when the drone collects data by flying above the ground-based receivers.

Note also that these results are not definitive, because of the conditions in which the experiment was conducted. The drones do not have a static flight, therefore information

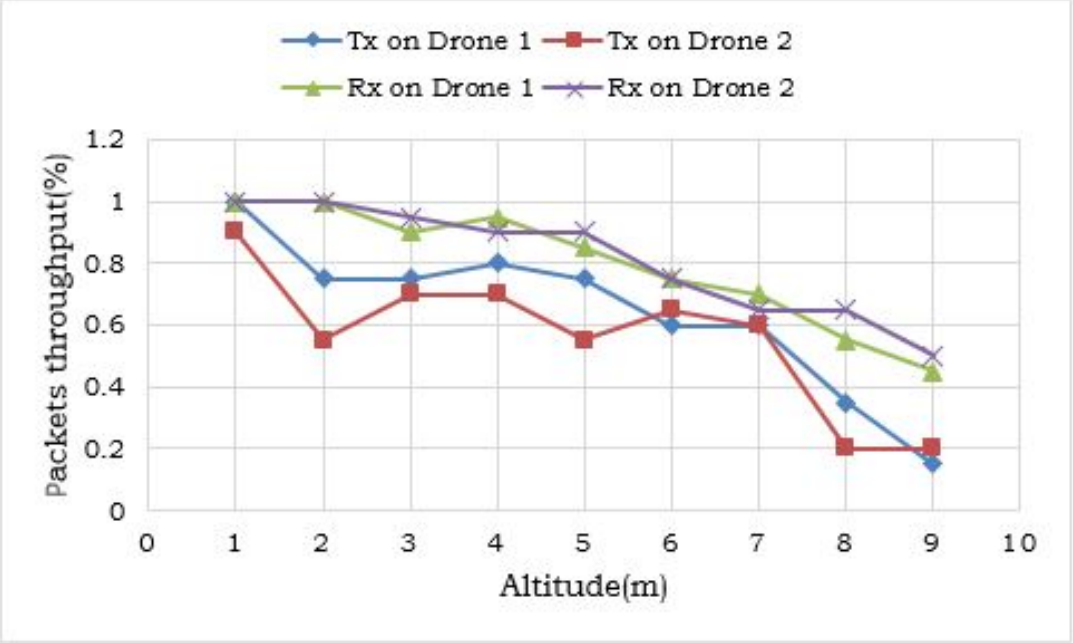

FIGURE 4.19: IEEE802.15.4 throughput results with drones

about altitudes is not very exact and accurate. Flying a drone on a straight line parallel to the ground at a fixed altitude is nearly impossible, which is why data about the altitude should be considered in ranges, instead of 1 metres of elevation. We for example considered a range [1-3]. This can result in the graph shifting up or down by one unit or 10% throughput data delivery.

B. The IEEE802.11/WiFi

After the experiment with the IEEE802.15.4 shown in figure 4.19, we them conducted another experiment with WiFi light/IEEE802.11. Figure 4.17 depicts the results of the four experiments conducted. Altitude wise, the results are much better compared to the results obtained with the IEEE802.15.4 shown in figure 4.19. From the experiments shown in figure 4.19, we noticed that, at least one of each type received up to all 100% data transmitted either by the drone as the transmitting device, or with the drone as receiver.The IEEE802.11 once again in this respect, performed much better than the IEEE802.15.4.

In terms of altitudes, at an elevation of up to 15 metres above ground, at least two of the four experiments, of which two of each type(see figure 4.20) received 100% of all the data transmitted, and the rest received at least 90% or more of the transmitted data, which is a very much better packets throughput, and very desirable when deploying networking systems, especially Internet-of-Things(IoT) systems in general. However, this is not

the only performance parameter to consider when considering the deployment of a cost efficient wireless sensor network.

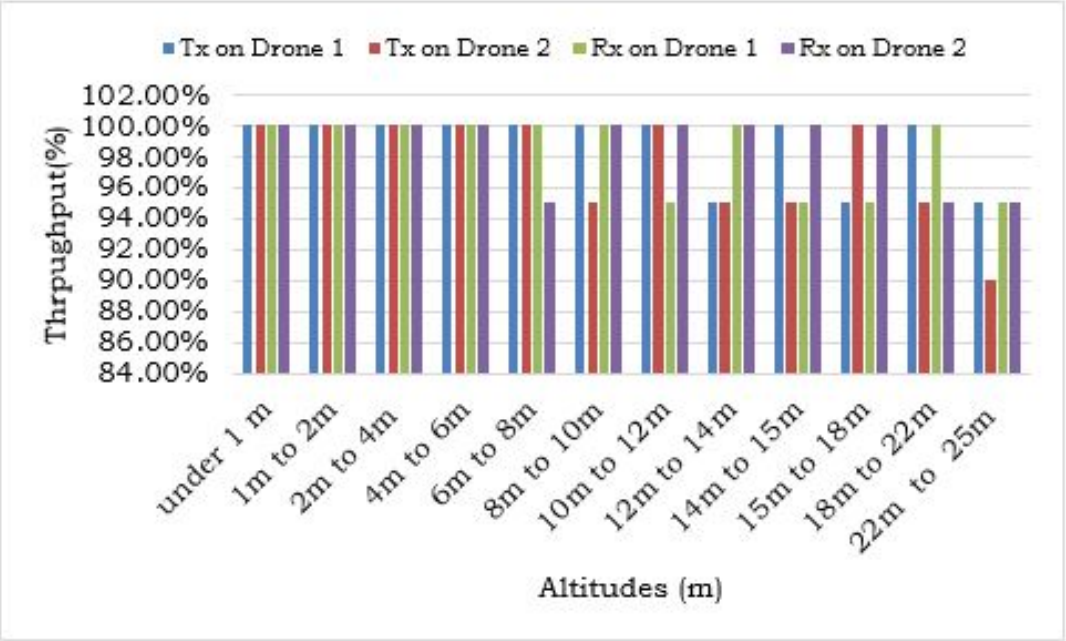

FIGURE 4.20: IEEE802.15.4 throughput results with drones

4.5 Conclusion

As we stated early sections of this chapter, the investigation of certain networking performance parameters is very important because, in order to deploy any type of networking, investigation on how it will perform in the area and conditions is very important. When deploying IoT systems or any other smart systems especially for monitoring, it is very important to bear in mind that, these systems are mostly deployed to work unattended or also deployed to work attended on a very lower frequency. The reason certain performance parameters weigh more than other was because of the way each affect the network and how they affect other performance parameters.

If we consider the cost of regularly attending sensors which are for example deployed for monitoring the presence of a certain gas in a certain area, we will probably come to a point where preference will be given to applications or systems that are self sustaining.

That leads us to consider the power consumption of the motes deployed. Sensors or devices with a low rate of power consumption can actually be classified as devices that perform better even when in certain performance parameters they do not yield excellent results. There is a trade-off between performance parameters that need to be satisfied

in order to obtain a system or systems that are as efficient in power consumption as they are in other parameters.

Chapter 5

Application Layer and Intrusion Detection

5.1 Introduction

Cyber-healthcare [52, 62] is emerging as a new field of medicine that relies on the sensor/actuator and wireless networking technologies to collect patients' vital signs and disseminate these signs to processing places where situation recognition is achieved and decisions taken about patients' treatment. However, owing to their communication model, wireless networks are burdened by many vulnerabilities[41]. These include exposure to security attacks, which in the case of healthcare systems, can have a more damaging than positive impact on the health of those who should benefit from these systems. Some of these vulnerabilities include intrusion and jamming attacks [31, 32] leading to information leaking, unauthorized access to information and data by people with technical means to eavesdrop in an unprotected communication. Some of these attacks simply target the stability of the network to prevent communication between nodes, mostly for personal mischievous reasons.

Furthermore, wireless sensor networks are more vulnerable to these security vulnerabilities due to their limitations in computation and storage capabilities as well as their limited battery life when deployed unattended [35]. Securing a wireless sensor network against intrusion and other forms of attacks is therefore a more challenging endeavour as it requires taking into account much more parameters and devising additional security measures than when dealing with other wireless networks [37]. In this chapter, we present one of the solutions to the problems of jamming attacks and intrusions for a network of low-cost, and low power devices. The solutions proposed in this chapter

is implemented and tested on a network of Waspmote devices communicating over the IEEE802.15.4 protocol and running on limited battery power.

5.1.1 Contribution

In this chapter, we revisit the issue of network security management to assess the relevance of using over-the-air intrusion detection and mitigation for securing a cyber-healthcare network infrastructure. We consider a local intrusion detection model where each node of a cyber-healthcare sensor network can detect intrusion by using local information collected from neighbours. We apply a probabilistic mitigation model where upon intrusion, the nodes of a sensor network compute the next channel to hop to using a distributed method that relies on the signal strength found in the channels.

5.2 The Channel Surfing Model

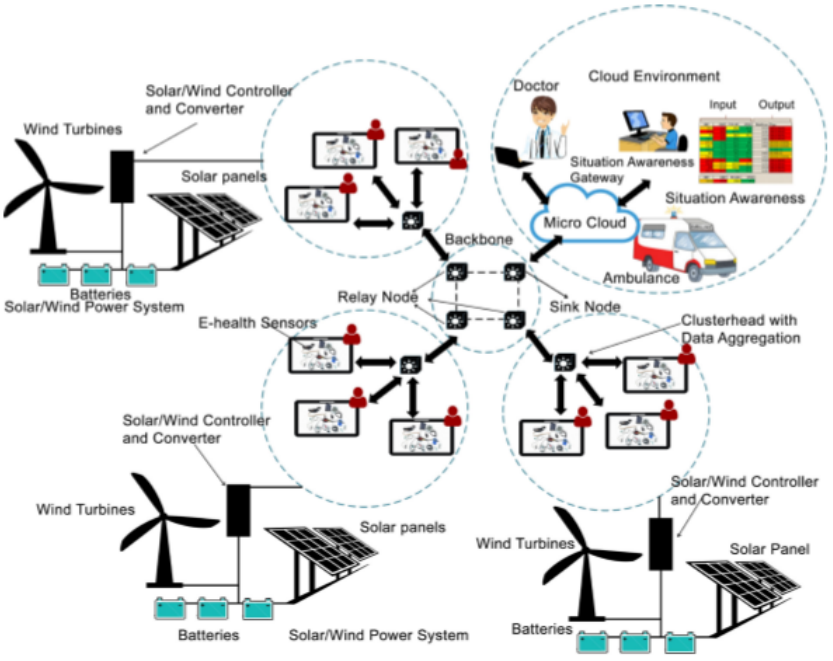

FIGURE 5.1: The Cyber Healthcare Model

We also consider in this chapter a "Cyber Health Care" model depicted by Figure 5.1, where sensors are grouped into separated health kiosks which are interconnected by a wireless sensor network using the zigbee/802.15.4 or WiFi protocol. In such a network configuration, potential intrusions/attacks may arise from (i) a node reporting application parameters such as bio-sensor values which are beyond the range known by neighbour nodes ; (ii) a node revealing abnormal communication parameters such as the

signal strength which has moved beyond known physical parameters and; (iii) network parameters such as the node weight, revealing abnormal routing values under periodic updates of the network when using collection tree protocols such as in [63, 64].

5.2.1 Model Formulation

The channel surfing problem consists of finding and energy efficient routing such that:

1. The energy in the running channel is below a given threshold
2. All nodes use the same communication channel
3. The most efficient channel used by the network before intrusion is not the same as the channel used by the network after intrusion
4. The channel used after intrusion detection is the most energy efficient channel selected by all nodes through voting

5.2.2 The Channel Surfing Algorithm

Research work has been conducted to address security issues related to jamming attacks. Solutions were proposed using channel surfing as a way of mitigating these attacks. Channel surfing consists of switching to another, not only available, but also more efficient in case of an attack or when a nodes in the network suspects a suspicious behaviour from its neighbours. In most cases the choice of the next channel to hop to has been made based on simple mathematical and statistical computations, baring in mind the limited capabilities that sensors have and their inability to perform huge and complex computations. A high level description of the *preplanned channel surfing* proposed in This chapter is as follows. The channel surfing algorithm we considered in this thesis consists of computing the next channel to hop to on the fly when intrusion happens, and it leads to a reactive channel surfing algorithm presented below.

Channel Surfing

Build routing tables. At each beaconing time do

- Broadcast Hello messages to discover neighbours
- receive acknowledgement from neighbours
- build routing tables

Intrusion detection. Upon anomaly detection do

- Detect attack from neighbor
- Selectively broadcast the anomaly to selected neighbours

Compute and hop to new channel. After intrusion detection do

- Surfe all channels to detect signal strength
- Collect signal channel quality (Q)
- Compute probabilities (scores)
- Select the next channel to hop to
- Hop to new channel

5.2.3 The Intrusion detection Algorithm

In this section, we present a basic and simple algorithm for the proposed intrusion detection protocol. The protocol consist of two basic parts, the network initialization, and the intrusion detection part. The initializing of the network is simply the process of each node taking notice of its neighbours and storing their information table while avoiding duplication of entries in the later table (see algorithm 1).

Algorithm 1: Network initialization algorithm

```
1  Let N be the Network of n nodes and i be the current node;
2  Let k be a node in the network N;
3  Let assume that all nodes in N are configured to communicate in the channel ch;
4  Let also assume that MAC_TABLE has n entries and specifies the node i at time t;
5  for each node k ∈ N do
       // Broadcast HELLO to all neighbors
6      for All neighbors i ≠ k do
7          t+ = 1;
8          if (MAC(k) ∈ MAC_TABLE(i, t)) then
9              MAC_TABLE(i, t) ← MAC(k) ;
10     for node k in N do
11         check if all nodes has its neighbor's MAC stored;
```

As is performed in algorithm 1, each and every node(s) in the network make acquittance with its neighbors and with all other nodes in the network. To start the initialization, each node broadcast a HELLO message signed with its MAC address, and every other nodes in the network, which receives the broadcast message, stores the signature MAC address in a table that will be used as a table of reference in the intrusion detection Algorithm. Algorithm 2 is the representation of how the main processes of our proposed protocol implementation flows. In the presented algorithm, note that certain parts are just represented as a one line pseudo-code, where in fact they are long and complex mathematical or statistical computations.

Algorithm 2: Intrusion detection algorithm

```
1 while All node devices are ON do
2     if Suspicious behaviour or attack is detected then
3         BroadcastAttackAlert();
4         C = computeNextChannel();
5         setChannel(C);
```

5.2.4 Next Channel Computation

Certain important and very useful assumptions need to be made taking into consideration key communication performance parameters in order to compute the next communication channel, which must also be feasible for a better communication amongst every nodes in the network. In most communication devices and in most communication, a RSSI of $-30dBm$ or higher is a very feasible communication [65], which usually deliver in almost all cases 100% of all the send packets which as much as 0% packets loss [66]. Subsequently, any communication with RSSI of $-100dBm$ or lower is generally not such a good communication and in most cases, it has a higher percentage of packets lot, which reaches in certain cases, as much as 100% of packets loss [67].

5.2.4.1 Channel Quality

The Quality of the RSSI is also very much influenced in big part by the distance between communicating device. However, there are other things such as the devices' specifications, which include the device's range of communication, its antenna gain and its reaction against interference [65, 66]. Let $Q_{N,d}(ch, i)$ denote the quality of the network in terms of signal strength as sensed by node i when communicating using the channel ch. Then, building upon the previous observations, $Q_{N,d}(ch, i)$can be defined by:

$$Q_{N,d}(ch,i) = \begin{cases} 100\% & RSSI \geq -30dBm \\ 0\% & RSSI \leq -100dBm \\ 1.4285 \times (RSSI + 100)\% & \text{Otherwise.} \end{cases} \tag{5.1}$$

where $Q_{N,d}(ch, i)$ denote the quality of the links as sensed by node i when communicating in channel ch, N denote the network, d denote the distance between every communicating nodes assuming that the later is equal and $RSSI$ is the Received Signal Strength Indicator in channel ch. Note that, as suggested earlier, these formulas are true and usable, only if firstly all the devices in the network can communicate, and if all the devices in the network are similar and have similar specifications and characteristics. Note also that since the quality of the network $Q_{N,d}(ch, i)$ is expressed in percentages,

it can easily be transformed into probabilities by multiplying $Q_{N,d}(ch, i)$ by $\frac{1}{100}$ to produce a probability parameter$P_{rb}(i, d, ch)$ expressing the goodness of the channel ch as detected by node i. It is expressed by

$$P_{rb}(i, d, ch) = \frac{Q_{N,d}(ch, i)}{100} \tag{5.2}$$

which represents positive rational number within the interval $[0, 1]$.

5.2.4.2 Channel Scoring

Let denote by $P_{rb}(ch, d)$ the probability of a channel to be selected as the next channel in case of attack intrusion. In the network N of n nodes, the average probability of a certain channel ch to be the next channel of communication is then given by :

$$P_{rb}(ch, d) = \frac{1}{n} \times \sum_{i=1}^{n} P_{rb}(i, d, ch) \tag{5.3}$$

Where $P_{rb}(ch, d)$ is the probability of the channel ch of a node communicating to other nodes situated in a range of d meters will be chosen, $P_{rb}(i, d, ch)$ is the probability that the signal of the channel ch as sensed by node i is good and n is the total number of nodes in the network while d is the averaged distance distance between nodes.

5.3 Experimental results

Sets of experiments were conducted using a set of five(5) waspmote devices connected in a network with one of them playing the role of unwanted intruder trying to jam the other four(4) devices. The objective was to investigate the performance of the proposed distributed algorithm with respect to the following:

1. The time taken by all nodes to adapt to the new channel.
2. The intrusion detection efficiency and,
3. The channel scoring efficiency.

5.3.1 New Channel Joining Time

As illustrated in the section above, one of the important parameter that needed to be investigated here is the "New Channel Joining Time" which is the time between the detection of an intrusion, and the time that all device join the new network channel.

Waspmotes				
Nodes / Experiments	Node 1	Node 2	Node 3	Node 4
Experiment 1	201 ms	∞	302 ms	326 ms
Experiment 2	292 ms	429 ms	298 ms	269 ms
Experiment 3	331 ms	317 ms	272 ms	315 ms
Experiment 4	219 ms	197 ms	308 ms	301 ms
Experiment 5	321 ms	471 ms	331 ms	306 ms
Experiment 6	421 ms	395 ms	239 ms	296 ms

TABLE 5.1: Channel joining time

We conducted a number of experiments but recorded and presented only a sample of 6 experiments shown in table 5.1. The joining time of nodes is dependent of different types of interferences that can affect communication and differs from one node to another. We considered the case where all nodes are in a star topology and can directly talk to the sink node and gateway.

In most cases of our experiments, the channel joining time is slightly dependent of the position of the node compared to the node that has discovered the attack first. If a node is directly communicating in single hop with the node that discovered the attack, then this node will compute the next channel of communication as soon as it receives the attack notification. On the other-hand, if there is two or more hops between the node that detected the attack first and a certain node A, the node A will probably receive the attack notification with a small delay which will be carried out through the whole process and cause a probable lengthening of the channel joining time. This is in agreement with the experiments in table 5.1, which reveals that different experiments yield different joining times for different nodes in the network.

5.3.2 Intrusion detection efficiency

One of the main aim of this chapter was to assess whether the intrusion detection protocol implemented provided positive results. The experiments as in the previous section, were conducted with waspmote devices(4 devices) and one more waspmote that we used to simulate an intrusion. The results were shown in table 5.2 were produced. Out of 10 selected experiments we conducted in urban area with people living their day to day life, and using wireless devices that can greatly harm our communication

through interferences. The results reveal that up the 80% of all attacks we generated were detected. This was a great success rate for experiments conducted in an area full of possible interferences.

Intrusion Detection			
Experiments	Detected	By What Node	Node joined
Experiment 1	Yes	Node 3 & 1	All
Experiment 2	Yes	Node 2	All
Experiment 3	Yes	Node 1	All
Experiment 4	No(1)	Node 2	1(Node 2)
Experiment 5	Yes	Node 3 & 4	All
Experiment 6	Yes	Node 3	All
Experiment 7	Yes	Node 4	All
Experiment 8	Yes	Node 4	All
Experiment 9	No(0)	None	None
Experiment 10	Yes	Node 3	All

TABLE 5.2: Intrusion detection

Referring to table 5.2, the intrusion detection efficiency computed by considering the following:

1. The number of detected intrusion over the number of experiments and,
2. The number of nodes that joined the new channel.

5.3.3 Channel Scoring efficiency

Channel scoring refers to the process by which every node in the network accurately scores each communicating channel according to equation 5.2, and from their scoring the average score of each channel is then computed using equation 5.3

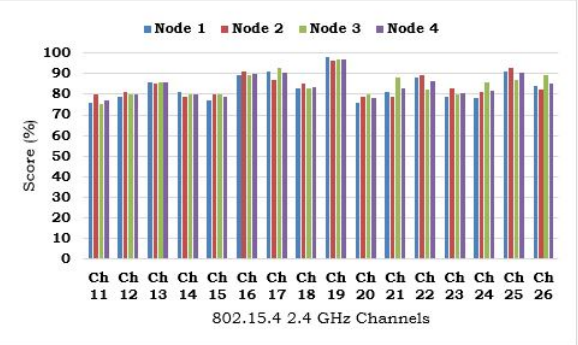

FIGURE 5.2: 802.15.4 2.4 GHz channels scoring

Similarly to previous sections, we also conducted a number of experiments to evaluate the channel scoring efficiency and reported the results in figure 5.2 which shows that:

- A marginal different is revealed between the scores provided by different nodes and,
- The channel surfing process will prioritize channel 19 first (see figure 5.2), then in case of another attack, if the scoring chart remains the same, the next channel of communication that is very luckily to be selected is either the 16^{th}, the 17^{th} or the 25^{th}, and the process continues in case of another attack.

5.4 Conclusion and future work

The protocol we proposed in this chapter, as we tested with different experiments presented in figure 5.2 and in tables 5.1 and 5.2, worked as we expected. It did not however work to our full expectation. As table 5.2 shows, out of the 10 experiments we conducted with simulated intrusion attacks, 80% of them were successfully detected, and only 20% where either not detected, or detected but nodes did not join the new channel.

Chapter 6

System Interoperability and Patients' EHR Messaging Standards

6.1 Introduction

Patient data or patient health information has been nowadays made much more available to authorized persons as a result of the fast advancing communication technologies and the inclusion of Internet of the Things (IoT) technologies in the healthcare industry. The inclusion and advancement of the IoT in the healthcare domain have led to the inclusion of cloud systems and cloud infrastructures allowing patient electronic health records (EHR) to be accessible by authorized healthcare practitioners, patients and pharmacist anywhere, anytime and sometimes using anything. Some of the advantages of a cloud based healthcare include the following:

1. Better patient care through a unified patient medical record
2. Cost reduction through a collaborative economic environment with shared overhead costs
3. Resources availability through remote medical services
4. Improved healthcare quality through aggregation of medical data and online access
5. Research support through an integrated repository of millions of patients cases uniformly and globally accessible.
6. Strategic planning support by using the eHealth budgeting for healthcare services

However, having patient data stored in multiple cloud infrastructures and systems exchanging this data requires certain rules and regulation to ensure that the exchange is performed uniformly, consistently and in a standardized way. The health level seven (HL7), as defined in [42, 43, 68], is a set of rules, standards, formats and definitions for exchanging and developing electronic health records (EHRs) between different medical applications. It defines a format for the transmission of health-related information. In this chapter, we discuss the HL7 standards and investigate the different resources and parameters that are affected by the HL7 formatting process with the objective of evaluating the routing overhead associated with the HL7 when deployed in a lightweight setting environment.

6.2 The HL7 Standards

HL7 and its members provide a framework (and related standards) for the interchange, integration, distribution, and recovery of electronic health information. These standards define how information is wrapped and transferred from one party to another, setting the language, structure and data types required for all-in-one integration between systems. HL7 standards support clinical practice and the management, delivery, and evaluation of health services, and are acknowledged as the most frequently used in the world [42, 43]. HL7 standards are grouped into reference categories:

- Section 1: Primary Standards - They are considered the most popular standards category for system integrations, system compliance and system inter-operability. The most used and highly demanded standards are in this category [43].
- Section 2: Foundational Standards - These standards define the fundamental tools and basics building blocks used to build standards, and the important technology infrastructure that must be used by implementers of the HL7 standards [43].
- Section 3: Clinical and Administrative Domains - Information that are related to messaging and documents standards for clinical specialties are in this section. They are usually implemented once the section 1 standards for the organization are in place [43].
- Section 4: EHR Profiles - The electronic health records profile standards offers functions models and profiles that facilitate the construction of management of EHR [43].
- Section 5: Implementation Guides - Provides guidance for implementation and/or support documents created to be used in conjunction with standards that already

exist. Every documents in this section, provides extra material for a parent standards [43].

- Section 6: Rules and References - Provides programming structures, guidelines for software and standards development, and technical specifications for implementing the HL7 [43].
- Section 7: Education & Awareness - This section covers the HL7's Draft standards for Trial Used (DSTU) and current projects, as well as important resources and tools to improve the understanding and adoption of the principals of HL7 standards [43].

The implementation discussed in this chapter, is mainly in the primary standards and a little bit in the EHR profiles.

6.3 HL7 Message Types and Descriptions

The HL7 standards has over 150 different messages types, for example ACK (general acknowledgement), an ADT(Admission discharge transfer message), BPS (Blood product dispense status message), BRT (Blood product transfusion/disposition acknowledgement message), etc. Each message type is made of segments and each segment occupy a line or more in typical HL7 message type. Similarly to the number of message types, there are also over hundred different segments that can be added in a single HL7 message type. For example, the ABS (abstract segment), the ACC (accident segment), the MSH (message header segment) which is always and must be the first part of every HL7 message, the OBR (Observation request), the OBX (Observation results), etc [44, 45]. The ADT message,is one of the most frequently used HL7 message type. It covers a lot of use cases such as patient admissions, cancellation of admits, patient data merging, etc [69, 70]. This is the reason this message types has a long list of event with are technically called segments in HL7. The full list of the HL7 v2 or higher can be accessed in [43]. Note that, this project and mainly this chapter's discussion focuses only on the ADT type message which implementation can be generalized to other types of message. However it is likely a whole system for interoperable system can be build and operate only with the ADT types of message to exchange all the necessary patients' data.

ADT messages are made of segments, and an ADT message has 51 different message sub-types titled A01 to A51, which can be found in [43]. The basic ADT message type is the A01 type, which is the patient admission and visit notification message. Each ADT message types are formed of segments and the number of total possible segment

is large, and some of the segments can appear twice and more in a single type ADT or other message type.

6.3.1 Mandated Structure of the ADT Message

The HL7 set of standards recommend and mandates that messages follow a specific structure, and this structure is designed as the "Mandated structure" [43]. The mandated structure mainly focuses on which segments are needed for which type of HL7 message and HL7 sub-message, and the sequences in which these segments come.

6.3.2 HL7 segments

A segment is a collection of fields that contain various types of data. Each segment exists individually and can be used in various messages, various sequences, throughout the HL7 standard. Segments may be required for a particular message or they may be optional [43, 44]. Each segment is identified by a unique three-character code called "Segment ID". The segment ID codes beginning with the letter Z are reserved for locally defined Z-segments that are not part of the HL7 standards [43].

TABLE 6.1: List of most commonly used segments

Segment ID	Meaning
DG1	Diagnosis
EVN	Event types
GT1	Guarantor
IN1	Insurance
MSH	Message header
NTE	Notes and comments
OBR	Observation request
OBX	Observation results
AL	Allergies
COR	Common order
PID	Patient identification
FT1(for DFT types)	Financial transaction

One or more segments from a message can be removed if desired. However, because HL7 rules state that unused or unexpected segment should be ignored, most system will overlook the unused segments without causing any problem. With that being said, it is therefore not necessary to manually remove unused segment manually [43]. However, unused segments might be removed in cases where their presence conflicts with of the trading partners' system when receiving a message containing this segment(s). The most commonly utilized segments in most healthcare systems are those in table 6.1.

A basic sample of an HL7 example of an HL7 message can be visualized in figure 6.1 where every single HL7 message start with the message header "*MSH*" which contains the message type which in this case is "*ADT*01", the software version, the company name, the HL7 version in this case 2.4, and other information about the system that is sending that specific message. After the "*MSH*", then follows the event "*EVN*" which contains the event date and time or the date and time the event took place. In third comes the "*PID*", the patient identification, which contain all important information of the patient, full-name, date of birth, address, phone contact, parent ID number.

```
MSH|^~\&|AccMgr|1|||20120123495123||ADT^A01|5
EVN|A01|20050110045502|||||
PID|1||10006579^^^1^MRN^1||DOE^JOHN^Q||192412
NK1|1|TSTORTECH^DAWN^|DAUGHTER|8729 W AURORA
NK1|2|TSTORTECH^DAWN^|PATIENT REPRESENTATIVE|
NK1|3|||3333 W GOOD HOPE RD^^MILWAUKEE^WI^532
PV1|1|I|PREOP^101^1^1^^^S|3|||37^SMITH^JOE^Q^
PV2|||||||20150722100000||||Hospital Encount
OBX|1|TX|||The patient gets 6 hours of sleep
NTE|1||This is a Display Note.
NTE|2||This is also a Display Note.
OBX|2|TX|||The patient takes aspirin for a he
NTE|1||This is a Display Note.
NTE|2||This is also a Display Note.
GT1|1|8291|DOE^JOHN^Q|^^|111^MAIN ST^^SOMEWHE
DG1|1|I9|71596^OSTEOARTHROS NOS-L/LEG ^I9|OST
IN1|1|MEDICARE|3|MEDICARE|^^^^^|^^|||||MyComp
IN2|1||123121234^^^|MyCompany LLC|||123121234
IN1|2|NON-PRIMARY|9|MEDICAL MUTUAL CALIF.|PO
```

FIGURE 6.1: HL7 basic message

After the "*PID*", follows the "*NK*1", which contains the next of kin information, this segment can be repeated because, it is possible that a patient has more than one next of kin, then comes the "*PV*1" (patient visit information segment) which can be also repeated. Much more segments can follow the "Mandated structure" of the specific message.

6.4 HL7 for Cloud Computing and Interoperability

Figure 6.2 depicts a cloud-based cyber-healthcare environment where:

1. Different digital healthcare systems are used to collect patients' data

2. Patient data is stored in different cloud environment endowed with storage and processing capabilities, and

3. Different stakeholders are provided with different services through the cloud environment over the HL7 standards.

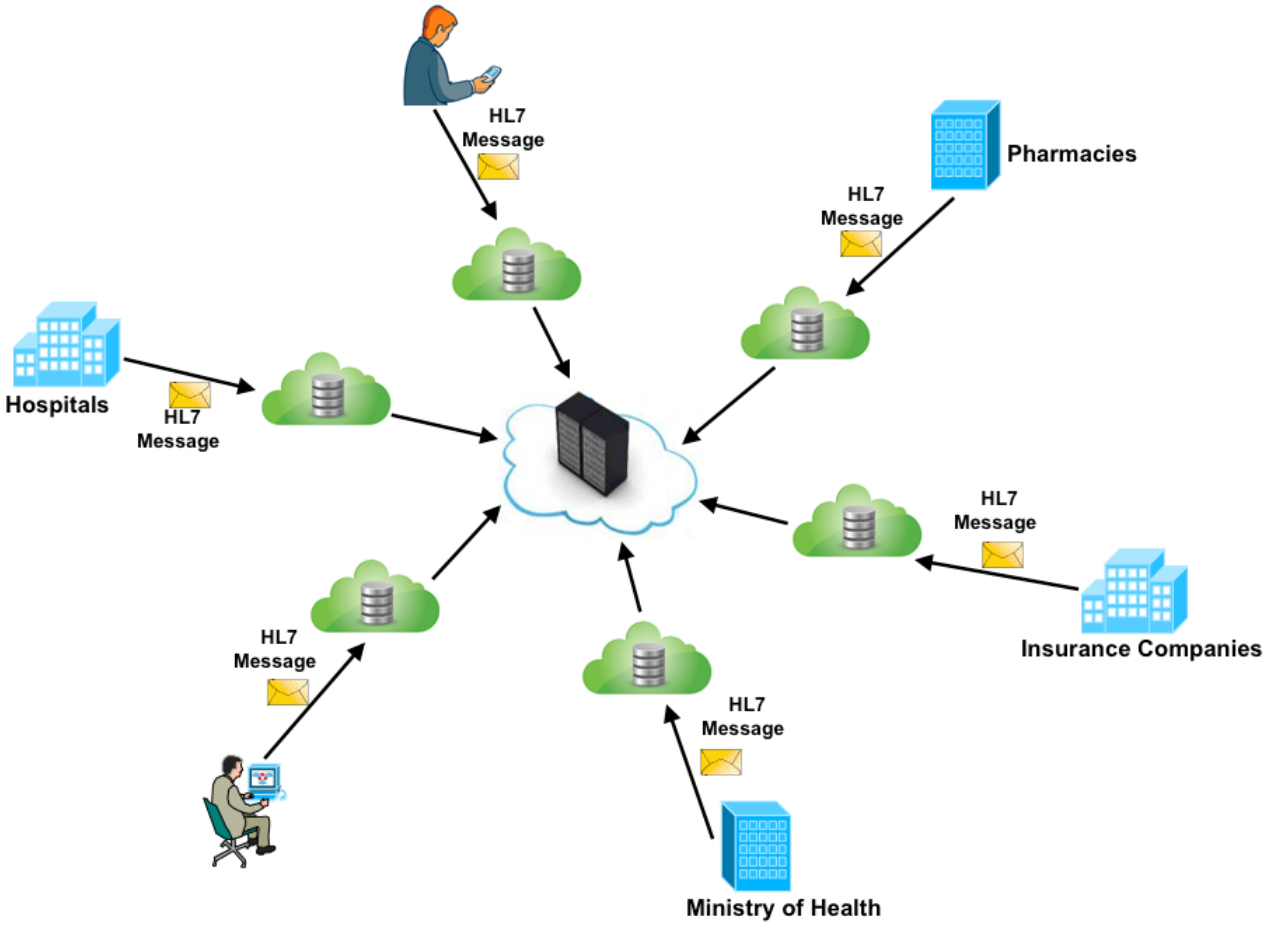

FIGURE 6.2: The Test Network

HL7 formatted data are very complex and formatting complex data comes with more issues such as packets overheads in terms of size and data transmission delays. Baring this in mind, we decided that, it would be resource wasting to implement HL7 in the communication between sensors and gateway or to database. Therefore, HL7 was implemented at the application layer, where data is exchanged among different cloud infrastructure with the aim of achieving more efficient interoperability of the healthcare information systems [44].

6.4.1 What is XML data and How is it related to HL7 ?

The Extensible Markup Language (XML) is a markup language which is a description of a set of rules for encoding documents in a format that is both human-readable and

machine-readable [71]. The XML is discussed in this section, because, most of the existing open source softwares take as input data into XML format before converting them into HL7 format. Listing 7.1, present a piece of XML code that demonstrates how data is encoded into XML. More information about XML and friendly tutorials can be found http://www.w3schools.com/xml/

.

```
<?xml version="1.0" encoding="utf-8"?>
<root>
    <row>
        <Msg_header>Patient admin, software version xxx </Msg_header>
        <Event_date> date and time </Event_date>
        <Patient ID> full-name, DOB, sex, age, ethnicity, address, tel </
    Patient ID>
        <Observation_1>Height 184 cm</Observation_1>
        <Observation_2>Weight 70kg</Observation_2>
        <visit information>Name of visitor and relation to patient</visit
    information>
        <Allergies>Aspirin</Allergies>
        <Diagnosis>Chest pain for examples<Diagnosis>
    </row>
    <row>
        <Msg_header>Patient admin, software version xxx </Msg_header>
        <Event_date> date and time </Event_date>
        <Patient ID> full-name, DOB, sex, age, ethnicity, address, tel </
    Patient ID>
        <Observation_1>Yellow eyes</Observation_1>
        <Observation_2>Weight loss</Observation_2>
        <visit information>Name of visitor and relation to patient</visit
    information>
        <Allergies>Panado</Allergies>
        <Diagnosis>Chest pain for examples<Diagnosis>
    </row>

</root>
```

Listing 6.1: Example of a XML Data format

6.4.2 XML relevance in Systems Interoperability

The XML is relevant mainly because of it relationship with most of HL7 converter softwares. In order to transform data into HL7 format, the data needs to be in XML form, which is a machine-readable language. For the purpose of the study, we looked at the "Altova MapForce" [72] because of it free trial. The altova MapForce is a any-to-any data mapping, conversion and integration tool that maps data between any combination

of XML, database, etc ..., then converts it into the desired format [72]. Chameleon and Iguana interface engine [73] is also one of those applications that has been implemented years ago for similar purposes and has been used widely world wide in most of the healthcare applications [73]. The Iguana is also able to support several data formats to allow you to receive, transform and route any data he/she wants [73].

The above two mentioned interfaces are special cases that show the importance and relevant to the XML in the implementation of any HL7 friendly systems. Whether the data is collected directly by sensors using the eHealth kit, or whether it is manually collected by a nurse, these data, needs to be transformed into XML, to enable the two interfaces stated above and many more to easily understand the data and convert it into HL7. Alternatively to the conversion issue, solution could be implementing our own application that directly convert from normal files or even from EHR files to HL7, but this would be not only time and resources wasting but also would result in trying to reinvent the wheel.

6.5 Performance Evaluation

As previously stated, integrating the HL7 standards into a eHealth systems comes with high prices specially when lightweight devices and communication are at stake. We considered two main performance parameters resulting from the increment in data size and processing associated with the HL7 protocol:

- Data overheads and,
- Delay overheads

To evaluate the performance of the proposed system, we considered a downscaled version of the system proposed in figure 6.2 where:

1. Patient's data is generated by eHealth and mobiles devices and,
2. Communication between the involved entities is performed through lightweight communication protocols such as the 802.15.4/ZigBee and the lightweight version of the WiFi protocol.

Such a system is typical for deployments in rural areas of the developing regions where power supply is either into meltdown or unavailable.

6.5.1 Overhead in Terms of Data Size

The first parameter that is investigated in this chapter is the file size or data size. We conducted an experiment to investigate how much the data is altered firstly from plain text data to XML and then from XML to HL7. The experiment consisted of recording sample patient information collected respectively in the plain text form, XML form and in HL7 format. Starting with one patient's record, then two, until we get to hundreds patients basics EHR. The data in the later three different format were analysed to found out the difference in packets size and how it scales.

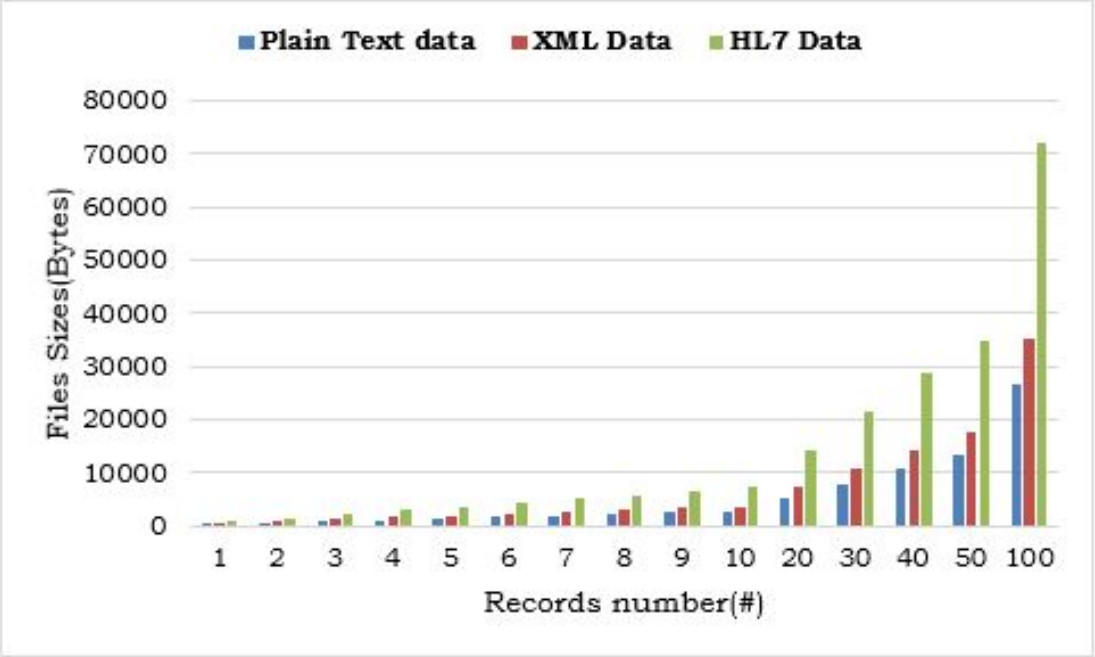

FIGURE 6.3: Data size Overhead

Figure 6.3 shows the results of the experiment we conducted. As revealed by the figure, converting the plain text data into XML format data increases the size of the data, and the impact is the same with converting data from XML to HL7, but in the later case the increment in data size is close to the double of the original size of the XML. This means that, it is more than twice the original data size(in Bytes) in plain text format.

Large data do not only require large storage capacities, but also advanced and improved data management systems as well as data handling mechanism which can easily handle large data. Sensors are lightweight devices that do not have these these two capabilities, enough storage capacity and the processing capability. It is therefore encouraged to implement the HL7 standardization at the cloud layer rather that the sensing layer.

6.5.2 Packets Delivery Delay or HL7 Over-head's Delay

Another parameter that is investigated because of it crucial importance, is the data delay or packets delay. We considered in this chapter investigating the data delivery delay in both single and multiple hops communication. The experiment where conducted over the 802.15.5/ZigBee and also over the lightweight version of WiFi protocol. All the experiments were conducted using waspmote devices. The next subsections discuss the packet delivery delay respectively for the single hop and multiple hops for the main two communication protocols discussed in this thesis.

6.5.2.1 Single hop IEEE802.15.4/ZigBee vs IEEE802.11/WiFi

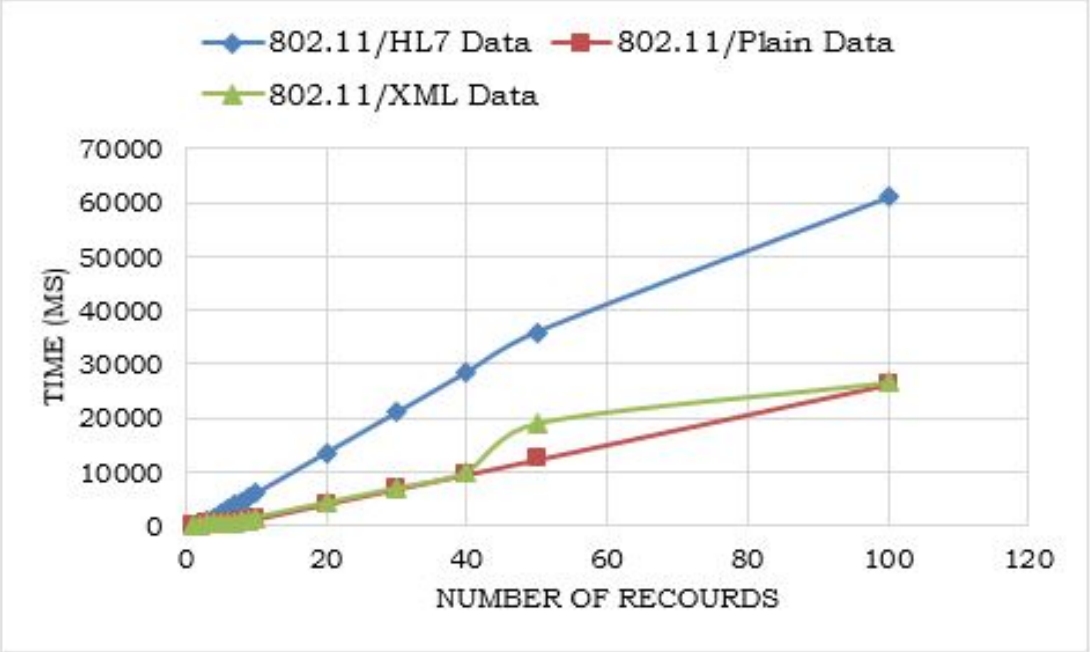

FIGURE 6.4: 802.11/WiFi Single hop Data delay Overhead

This section reports on an experiment which we conducted with all communicating nodes or devices situated one hop away from each other. A number of devices was configured as senders, while others were setup as receiving devices communicating with the sensors firstly in uni-cast mode, thereafter in broadcast mode. The results were fairly similar and the slight difference was due to the fact the experiment was undertaken in a crowded urban environment and not in a controlled environment which would have provided us with identical conditions every time an experiment was conducted.All the results where closely similar and we averaged them to give an idea of how the performance pattern looks like in terms of impact of difference.

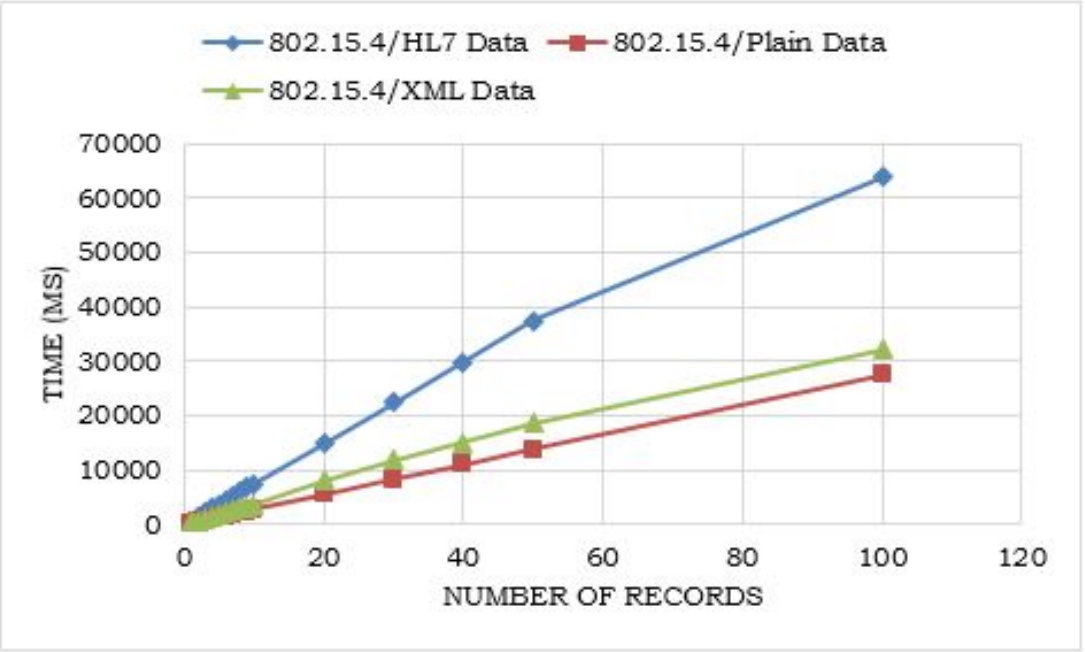

FIGURE 6.5: 802.15.4/ZigBee Single hop Data delay Overhead

The figures 6.4 and 6.5 represent the results of the experiment conducted. As it is revealed in the two figures, exchanging data in a plain text form takes less time than communicating data in XML format. The same applies to communicating data in XML form which also takes less time than communicating data in HL7 form. This indeed confirms how much overhead does mapping data from XML to HL7 brings. These results give important information that need to be taken in consideration when trying to implement HL7 friendly systems. These results also reveal the difference between outbound standardization where patients' data is transformed into plain text before being transported to the cloud layer and inbound standardization where EHRs are transformed into HL7 format before being transported to the cloud infrastructure where standardized services are provided. Both figures reveal similar performance patterns where the transformation process from text to XML and/or HL7 induces communication delay.

6.5.2.2 Multiple hops IEEE802.15.4/ZigBee vs IEEE802.11/WiFi

The experiments conducted with network of nodes located one hop away from each other (figure 6.4 and 6.5) were complemented by another set of experiments of the same type, but this time with sender and receiver node devices located more than one hop away, communication in a crowded urban area highly exposed to interference.

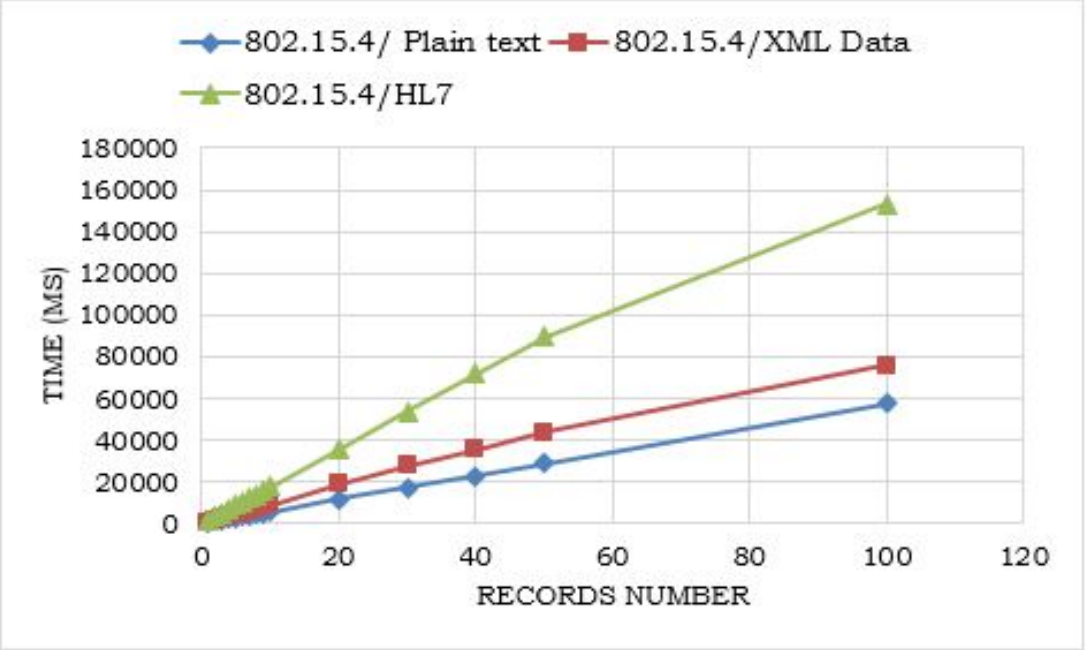

FIGURE 6.6: 802.15.4/ZigBee Multiple hops Data delay Overhead

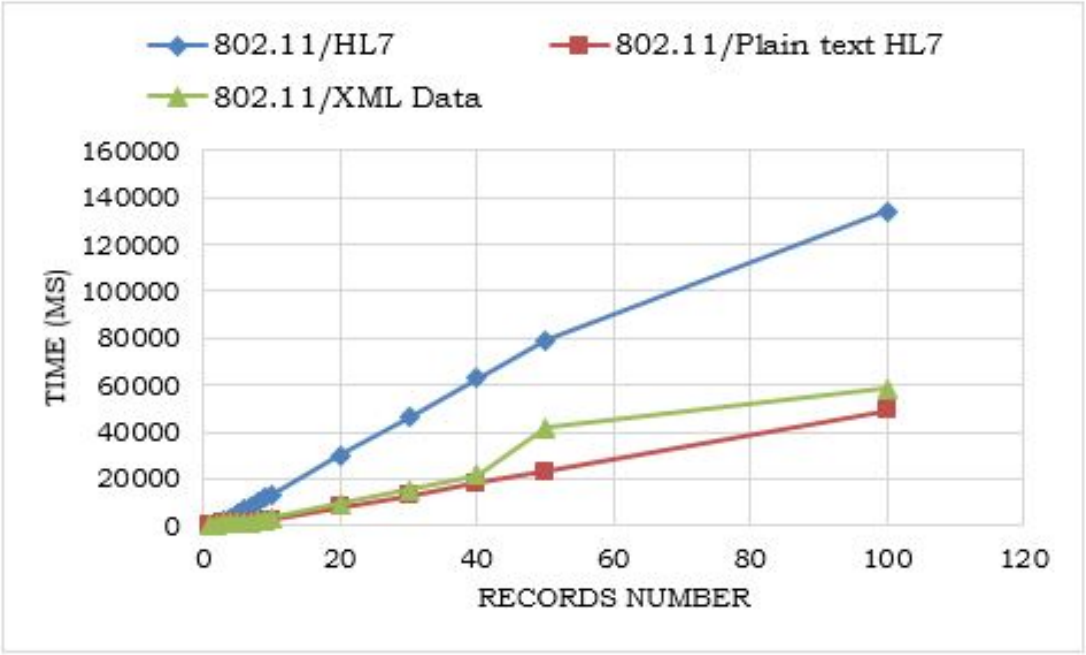

FIGURE 6.7: 802.11/WiFi Multiple hops Data delay Overhead

The result of the experiments presented in figure 6.6 and figure 6.7 were all averaged from a set of a sample of 5 experiments. The results reveal that multiple hops communication takes slightly more time than single hop communication. However looking at the performance pattern, they are very similar to those of the single hop communication respectively presented in figure 6.4 and figure 6.5.

6.6 Conclusion

The aim of this chapter was to investigate how much overhead does the HL7 implementation brings to a cloud-based healthcare system. It was only logically obvious to assume that as more fields and information are added to the original data, more overhead will be observed in size, and more time it will probably take for packets to be delivered. All the experiments that we conducted in this chapter support this hypothesis and indeed confirms that mapping data from plain normal text to XML form, and from XML to HL7 comes with a cost of increment in both storage size and data delivery time. The results presented in this chapter also raise the issue of the trade-off between in-bound and out-bound standardization which is still an open issue when dealing with lightweight communication.

Chapter 7

Conclusion and Future Works

7.1 Conclusion

This thesis has revisited the issue of cyber-healthcare by raising and providing answers to four(4) main points of this thesis's research question which, to the best of out knowledge, are the pillars of current research conducted in the field of cyber-healthcare. This chapter presents the conclusions drawn from different experiments which were conducted in order to provide answers to the research question.

Field readiness of eHealth sensor kit- On the question of automatic physiological parameters capturing and sensors, we investigated the eHealth sensor kit to evaluate whether the kit and all it sensors are field ready. Reading from most of the sensors indicated that the sensors can be trusted and information obtained from these sensors could be used to make crucial medical decision. Note however that, the physical aspect of the kit does not tell the same story. The way these sensors are wrapped and presented tells that the kit was designed mainly to be used in prototyping and system testing, and not as end-products. The eHealth kit that we investigated in chapter 3, as depicted in figure 3.1 and 3.2, does not provide proper connections and 3 out of 5 time the connection of one or more sensors disconnected while we conducted experiments due to test subject's movements. With that in mind, we concluded that this kit is designed for prototyping. However, if the sensors cabling and connections are catered for and the eHealth shield is well packaged, the whole set could be used in public healthcare facilities and provide reliable and accurate readings, which can be used in important decision making to provide better healthcare services.

Data dissemination- We conducted numerous experiments in chapter 4 on the 802.15.4 and ZigBee and the IEEE802.11/WiFi communication protocols and compared their performance. All the experiment in chapter 4, the RSSI, throughput, and packets delivery

delay time as performances parameters. We compared these performance parameters in different scenarios, both indoor and outdoor communication and using unmanned aerial vehicles (UAV) communicating with sensors. Different types of motions were also considered like: walking and running. The results obtained in the experiments conducted revealed that, the 802.11/WiFi outperformed the 802.15.4/ZigBee in most of the performance parameters. However, the 802.15.4/ZigBee could be preferred because of its cost efficiency, lightweight battery power usage and especially its design which is IoT and WSNs friendly.

Cyber-healthcare security- We implemented an intrusion detection protocol for securing the transmission of the physiological data from different entities such as sensors, gateways, central databases, and other processing places. These security measures were implemented to complement the already existing security measures available on the IEEE802.15.4/ZigBee and the lightweight version of WiFi as they were protocol of interest. To the best of our knowledge, the existing security measures do not cater for attacks such as over-the-air attacks that we focused on in our implemented protocol in chapter 5. The results of our experiment in table 5.1 and 5.2 shows that our protocol performed well, although it was not 100% accurate. The algorithm behind our proposed protocol is open to improvements, since with more resources, would have had a larger testbed with a lot more devices to work with. This would have offered more data and increase the protocol's accuracy.

Cyber-healthcare interoperability- The last pillar of the research we conducted in this thesis, which is also the last or fourth research question discussed in depth in chapter 6. It concerns the integration of our design into public healthcare systems. Amongst a multitude of healthcare standards that have been proposed in different previous researches for system interoperability of healthcare systems, chapter 6 of our thesis presented a study of the impacts of HL7 in system interoperability. In chapter 6, we also investigated performance parameters related to the overhead that formatted HL7 messages bring and how they affect the data communication process. We conducted experiments for both single and multiple hops communication, and the results revealed that implementing HL7 comes with a cost.

7.2 Future Work

The work presented in this thesis could be extended in the following area:

1. ***Cyber-healthcare security-*** The results presented in this chapter could be improved to increase the intrusion detection accuracy because the target is to achieve

between 98% and 100% of intrusion detection accuracy, specially because this project's implementation targets healthcare systems.

2. ***Cyber-healthcare interoperability-*** The research conducted in chapter 6 could be complemented by further investigating the implementation of the interoperability at different layer and cloud infrastructures could also be added.

3. ***Cyber-healthcare privacy-*** Beside security requirements, cyber-healthcare systems require privacy which can be achieved through anonymization, thus integration of efficient anonymization algorithms in the proposed cyber-healthcare framework has been planned for future work.

Bibliography

[1] T Yoshikawa Thomas and Shobita Rajagopalan. Tuberculosis and aging: a global health problem. *Clinical infectious diseases*, 33(7):1034–1039, 2001.

[2] Zola Madolo, Ditiro Maubane, and Antoine Bangula. Participatory health care system. 2013.

[3] Claude Kakoko Lubamba. Participatory healthcare system (sensing and data dissemination). 2014.

[4] Jaewoo Kim, Jaiyong Lee, Jaeho Kim, and Jaeseok Yun. M2m service platforms: survey, issues, and enabling technologies. *Communications Surveys & Tutorials, IEEE*, 16(1):61–76, 2014.

[5] Arnold G Zermansky, Duncan R Petty, David K Raynor, Nick Freemantle, Andy Vail, and Catherine J Lowe. Randomised controlled trial of clinical medication review by a pharmacist of elderly patients receiving repeat prescriptions in general practice. *Bmj*, 323(7325):1340, 2001.

[6] Jayne Steadman, Nora Donaldson, and Lalit Kalra. A randomized controlled trial of an enhanced balance training program to improve mobility and reduce falls in elderly patients. *Journal of the American Geriatrics Society*, 51(6):847–852, 2003.

[7] Chakravanti Rajagopalachari Kothari. *Research methodology: Methods and techniques*. New Age International, 2004.

[8] Corrine Glesne, Alan Peshkin, et al. *Becoming qualitative researchers: An introduction*. Longman White Plains, NY, 1992.

[9] Meredith Damien Gall, Walter R Borg, and Joyce P Gall. *Educational research: An introduction* . Longman Publishing, 1996.

[10] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7):1645–1660, 2013.

[11] Yesha Bhatt and Chintan Bhatt. Internet of things in healthcare. In *Internet of Things and Big Data Technologies for Next Generation Healthcare*, pages 13–33. Springer, 2017.

[12] Angelika Dohr, R Modre-Opsrian, Mario Drobics, Dieter Hayn, and Günter Schreier. The internet of things for ambient assisted living. In *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on*, pages 804–809. Ieee, 2010.

[13] Nicola Bui and Michele Zorzi. Health care applications: a solution based on the internet of things. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*, page 131. ACM, 2011.

[14] Antoine Bagula, Marco Zennaro, Gordon Inggs, Simon Scott, and David Gascon. Ubiquitous sensor networking for development (usn4d): An application to pollution monitoring. *Sensors*, 12(1):391–414, 2012.

[15] Muthoni Masinde and Antoine Bagula. A calibration report for wireless sensor-based weatherboards. *Journal of Sensor and Actuator Networks*, 4(1):30–49, 2015.

[16] Muthoni Masinde. An assessment of field readiness for wireless sensor based weatherboards—a calibration report. In *Industrial Informatics (INDIN), 2014 12th IEEE International Conference on*, pages 604–610. IEEE, 2014.

[17] Million Mafuta, Marco Zennaro, Antoine Bagula, Graham Ault, Harry Gombachika, and Timothy Chadza. Successful deployment of a wireless sensor network for precision agriculture in malawi. In *Networked Embedded Systems for Every Application (NESEA), 2012 IEEE 3rd International Conference on*, pages 1–7. IEEE, 2012.

[18] Lamia Chaari and Lotfi Kamoun. Performance analysis of ieee 802.15. 4/zigbee standard under real time constraints. *International Journal of Computer Networks & Communications*, 3(5):235, 2011.

[19] MM Chandane, SG Bhirud, and SV Bonde. Performance analysis of ieee 802.15. 4. *International Journal of Computer Applications (0975–8887)*, 2012.

[20] Sofie Pollin, Mustafa Ergen, Sinem Coleri Ergen, Bruno Bougard, Liesbet Van der Perre, Ingrid Moerman, Ahmad Bahai, Pravin Varaiya, and Francky Catthoor. Performance analysis of slotted carrier sense ieee 802.15. 4 medium access layer. *Wireless Communications, IEEE Transactions on*, 7(9):3359–3371, 2008.

[21] João Valente, David Sanz, Antonio Barrientos, Jaime del Cerro, Ángela Ribeiro, and Claudio Rossi. An air-ground wireless sensor network for crop monitoring. *Sensors*, 11(6):6088–6108, 2011.

[22] Andrea Goldsmith. *Wireless communications*. Cambridge university press, 2005.

[23] Jianliang Zheng and Myung J Lee. A comprehensive performance study of ieee 802.15. 4, 2004.

[24] Gang Lu, Bhaskar Krishnamachari, and Cauligi S Raghavendra. Performance evaluation of the ieee 802.15. 4 mac for low-rate low-power wireless networks. In *Performance, Computing, and Communications, 2004 IEEE International Conference on*, pages 701–706. IEEE, 2004.

[25] Nick F Timmons and William G Scanlon. Analysis of the performance of ieee 802.15. 4 for medical sensor body area networking. In *Sensor and ad hoc communications and networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on*, pages 16–24. IEEE, 2004.

[26] Edward G Tiedemann Jr, Irfan Khan, and Alejandro R Holcman. Method and system for over-the-air (ota) service programming, April 30 2002. US Patent 6,381,454.

[27] Amro Qandour, Daryoush Habibi, and Iftekhar Ahmad. Wireless sensor networks for fire emergency and gas detection. In *Networking, Sensing and Control (ICNSC), 2012 9th IEEE International Conference on*, pages 250–255. IEEE, 2012.

[28] Jose Antonio Galache, Pablo Sotres, Juan R Santana, Veronica Gutierrez, Luis Sanchez, and Luis Muñoz. A living smart city: Dynamically changing nodes behavior through over the air programming. In *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on*, pages 1271–1276. IEEE, 2013.

[29] Boris Danev, Heinrich Luecken, Srdjan Capkun, and Karim El Defrawy. Attacks on physical-layer identification. In *Proceedings of the third ACM conference on Wireless network security*, pages 89–98. ACM, 2010.

[30] Yang Xiao, Hsiao-Hwa Chen, Bo Sun, Ruhai Wang, and Sakshi Sethi. Mac security and security overhead analysis in the ieee 802.15. 4 wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, 2006(1):1–12, 2006.

[31] Javier López and Jianying Zhou. *Wireless sensor network security*, volume 1. IOS Press, 2008.

[32] Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong. Security in wireless sensor networks: issues and challenges. In *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, volume 2, pages 6–pp. IEEE, 2006.

[33] Kashif Saleem, Norsheila Fisal, Sharifah Hafizah, and Rozeha A Rashid. An intelligent information security mechanism for the network layer of wsn: Biosarp. In *Computational intelligence in security for information systems*, pages 118–126. Springer, 2011.

[34] Mohamed Hossam Ahmed, Syed Wasi Alam, Nauman Qureshi, and Irum Baig. Security for wsn based on elliptic curve cryptography. In *Computer Networks and Information Technology (ICCNIT), 2011 International Conference on*, pages 75–79. IEEE, 2011.

[35] Wenyuan Xu, Wade Trappe, and Yanyong Zhang. Channel surfing: defending wireless sensor networks from interference. In *Proceedings of the 6th international conference on Information processing in sensor networks*, pages 499–508. ACM, 2007.

[36] David R Raymond and Scott F Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. *Pervasive Computing, IEEE*, 7(1):74–81, 2008.

[37] Anthony D Wood, John A Stankovic, and Gang Zhou. Deejam: Defeating energy-efficient jamming in ieee 802.15. 4-based wireless networks. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on*, pages 60–69. IEEE, 2007.

[38] Bruce DeBruhl and Patrick Tague. Digital filter design for jamming mitigation in 802.15. 4 communication. In *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*, pages 1–6. IEEE, 2011.

[39] Wenbo Shen, Peng Ning, Xiaofan He, Huaiyu Dai, and Yao Liu. Mcr decoding: A mimo approach for defending against wireless jamming attacks. In *Communications and Network Security (CNS), 2014 IEEE Conference on*, pages 133–138. IEEE, 2014.

[40] Mingyan Li, Iordanis Koutsopoulos, and Radha Poovendran. Optimal jamming attacks and network defense policies in wireless sensor networks. In *IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications*, pages 1307–1315. IEEE, 2007.

[41] Mingyan Li, Iordanis Koutsopoulos, and Radha Poovendran. Optimal jamming attack strategies and network defense policies in wireless sensor networks. *IEEE Transactions on Mobile Computing*, 9(8):1119–1133, 2010.

[42] B Orgun and J Vu. Hl7 ontology and mobile agents for interoperability in heterogeneous medical information systems. *Computers in biology and medicine*, 36(7): 817–836, 2006.

[43] J Quinn. An hl7 (health level seven) overview. *Journal of AHIMA/American Health Information Management Association*, 70(7):32–4, 1998.

[44] Oana-Sorina Lupşe, Mihaela Marcella Vida, and L Tivadar. Cloud computing and interoperability in healthcare information systems. In *The First International Conference on Intelligent Systems and Applications*, pages 81–85, 2012.

[45] Bens Pardamean and Rizal Ricky Rumanda. Integrated model of cloud-based e-medical record for health care organizations. In *10th WSEAS international conference on e-activities*, pages 157–162, 2011.

[46] Goce Gavrilov and Vladimir Trajkovik. Security and privacy issues and requirements for healthcare cloud computing. *ICT Innovations*, pages 143–152, 2012.

[47] Michael Johnstone. Cloud security: A case study in telemedicine. 2012.

[48] Christian Ohmann and Wolfgang Kuchinke. Future developments of medical informatics from the viewpoint of networked clinical research. *Methods of information in medicine*, 48(1):45–54, 2009.

[49] Tim Benson. *Principles of health interoperability HL7 and SNOMED*. Springer Science & Business Media, 2012.

[50] A Berler, S Pavlopoulos, and D Koutsouris. Design of an interoperability framework in a regional healthcare system. In *Engineering in Medicine and Biology Society, 2004. IEMBS'04. 26th Annual International Conference of the IEEE*, volume 2, pages 3093–3096. IEEE, 2004.

[51] Rmesh Sahoo and Srinivas Sethi. Functional analysis of mental stress based on physiological data of gsr sensor. In *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1*, pages 109–117. Springer, 2015.

[52] M Mandava, C Lubamba, A Ismail, A Bagula, and Herman Bagula. Cyber-healthcare for public healthcare in the developing world. In *2016 IEEE Symposium on Computers and Communication (ISCC)*, pages 14–19. IEEE, 2016.

[53] María Viqueira Villarejo, Begoña García Zapirain, and Amaia Méndez Zorrilla. A stress sensor based on galvanic skin response (gsr) controlled by zigbee. *Sensors*, 12(5):6075–6101, 2012.

[54] Kuang-Yow Lian, Sung-Jung Hsiao, and Wen-Tsai Sung. Intelligent multi-sensor control system based on innovative technology integration via zigbee and wi-fi networks. *Journal of network and computer applications*, 36(2):756–767, 2013.

[55] Axel Sikora and Voicu F Groza. Coexistence of ieee802. 15.4 with other systems in the 2.4 ghz-ism-band. In *2005 IEEE Instrumentationand Measurement Technology Conference Proceedings*, volume 3, pages 1786–1791. IEEE, 2005.

[56] IEEE 802 LAN/MAN Standards Committee et al. Ieee 802.15 wpan^{TM} task group 4 (tg4). *saatavilla WWW-muodossa¡ URL: http://www. ieee802. org/15/pub/TG4. html*, 11, 2006.

[57] David Gascón. Security in 802.15. 4 and zigbee networks, 2009.

[58] Xiaohang Chen. Low-power mac design for m2m communications in cellular networks: Protocols and algorithms. 2013.

[59] Marieke Fijnvandraat and Harry Bouwman. Flexibility and broadband evolution. *Telecommunications Policy*, 30(8):424–444, 2006.

[60] Martin Sauter. Mobility management in the cell-dch state. *From GSM to LTE: An Introduction to Mobile Networks and Mobile Broadband (eBook). John Wiley & Sons*, page 160, 2010.

[61] David Stanislowski, Xavier Vilajosana, Qin Wang, Thomas Watteyne, and Kristofer SJ Pister. Adaptive synchronization in ieee802. 15.4 e networks. *IEEE Transactions on Industrial Informatics*, 10(1):795–802, 2014.

[62] A Bagula, C Lubamba, M Mandava, H Bagula, M Zennaro, and E Pietrosemoli. Cloud based patient prioritization as service in public health care. In *ITU Kaleidoscope: ICTs for a Sustainable World (ITU WT), 2016*, pages 1–8. IEEE, 2016.

[63] Antoine B Bagula, Djamel Djenouri, and Elmouatezbillah Karbab. Ubiquitous sensor network management: The least interference beaconing model. In *PIMRC*, pages 2352–2356, 2013.

[64] Lutando Ngqakaza and Antoine Bagula. Least path interference beaconing protocol (libp): A frugal routing protocol for the internet-of-things. In *International Conference on Wired/Wireless Internet Communications*, pages 148–161. Springer, 2014.

[65] Emanuele Goldoni, Alberto Savioli, Marco Risi, and Paolo Gamba. Experimental analysis of rssi-based indoor localization with ieee 802.15. 4. In *Wireless Conference (EW), 2010 European*, pages 71–77. IEEE, 2010.

[66] Ilku Nam, Kyudon Choi, Joonhee Lee, Hyouk-Kyu Cha, Bo-Ik Seo, Kuduck Kwon, and Kwyro Lee. A 2.4-ghz low-power low-if receiver and direct-conversion transmitter in 0.18-cmos for ieee 802.15. 4 wpan applications. *IEEE Transactions on Microwave Theory and Techniques*, 55(4):682–689, 2007.

[67] Wei Yuan, Xiangyu Wang, and Jean-Paul MG Linnartz. A coexistence model of ieee 802.15. 4 and ieee 802.11 b/g. In *2007 14th IEEE Symposium on Communications and Vehicular Technology in the Benelux*, pages 1–5. IEEE, 2007.

[68] FJ Van Wingerde, James Schindler, Peter Kilbridge, P Szolovits, C Safran, D Rind, S Murphy, G Octo Barnett, and IS Kohane. Using hl7 and the world wide web for unifying patient data from remote databases. In *Proceedings of the AMIA Annual Fall Symposium*, page 643. American Medical Informatics Association, 1996.

[69] Kazuhiko Ohe and Shigekoto Kaihara. Implementation of hl7 to client-server hospital information system (his) in the university of tokyo hospital. *Journal of medical systems*, 20(4):197–205, 1996.

[70] Teeradache Viangteeravat, Matthew N Anyanwu, Venkateswara Ra Nagisetty, Emin Kuscu, Mark Eijiro Sakauye, and Duojiao Wu. Clinical data integration of distributed data sources using health level seven (hl7) v3-rim mapping. *Journal of clinical bioinformatics*, 1(1):1, 2011.

[71] Albrecht Schmidt, Florian Waas, Martin Kersten, Michael J Carey, Ioana Manolescu, and Ralph Busse. Xmark: A benchmark for xml data management. In *Proceedings of the 28th international conference on Very Large Data Bases*, pages 974–985. VLDB Endowment, 2002.

[72] Bogdan Alexe, Wang-Chiew Tan, and Yannis Velegrakis. Comparing and evaluating mapping systems with stbenchmark. *Proceedings of the VLDB Endowment*, 1(2): 1468–1471, 2008.

[73] Hwa Sun Kim, Hune Cho, and In Keun Lee. The development of a graphical user interface engine for the convenient use of the hl7 version 2. x interface engine. *Healthcare informatics research*, 17(4):214–223, 2011.