2-1-2018

Fault tolerance in WBAN applications

Malak Yousry ElSalamouny

School of Science and Engineering

Fault Tolerance in WBAN Applications

A Thesis Submitted to the

Electronics and Communications Engineering Department

in partial fulfillment of the requirements for

the degree of Master of Science

Submitted by: Malak ElSalamouny

under the supervision of

Prof. Hassanein Amer and Dr. Ramez Daoud

Submission Date: 6 January 2018

To my Family and Friends

Abstract

One of the most promising applications of IoT is Wireless Body Area Networks (WBANs) in medical applications. They allow physiological signals monitoring of patients without the presence of nearby medical personnel. Furthermore, WBANs enable feedback action to be taken either periodically or event-based following the Networked Control Systems (NCSs) techniques. This thesis first presents the architecture of a fault tolerant WBAN. Sensors data are sent over two redundant paths to be processed, analyzed and monitored. The two main communication protocols utilized in this system are Low power Wi-Fi (IEEE 802.11n) and Long Term Evolution (LTE). Riverbed Modeler is used to study the system's behavior. Simulation results are collected with 95% confidence analysis on 33 runs on different initial seeds. It is proven that the system is fully operational. It is then shown that the system can withstand interference and system's performance is quantified. Results indicate that the system succeeds in meeting all required control criteria in the presence of two different interference models.

The second contribution of this thesis is the design of an FPGA-based smart band for health monitoring applications in WBANs. This FPGA-based smart band has a softcore processor and its allocated SRAM block as well as auxiliary modules. A novel scheme for full initial configuration and Dynamic Partial Reconfiguration through the WLAN network is integrated into this design. Fault tolerance techniques are used to mitigate transient faults such as Single Event Upsets (SEUs) and Multiple Event Upsets (MEUs). The system is studied in a normal environment as well as in a harsh environment. System availability is then obtained using Markov Models and a case study is presented.

ACKNOWLEDGMENTS

I would like to acknowledge both of my supervisors: Prof. Hassanein Amer and Dr. Ramez Daoud for their great support throughout my thesis and courses and for allowing me to become part of the SEAD research group. This group gave me the true essence of high quality research skills apart from the knowledge gained from the weekly meetings. These meeting were more like gatherings which aim in sharing knowledge and providing innovative ideas that usually help in bringing new research topics. To name very few members who have positively impacted my personal and research development: Eng. Gehad Alkady, Eng. Hassan Halawa, Prof. Hany ElSayed.

Moreover, I would like thank my parents and young brother for baring me throughout my master's program and accepting the fact that I did not spend time with them or was not available when they needed me. For my career and academic mentors, I would like to thank Eng. Sarah Abu Nar, Dr. Lamia Khashan, Dr. Lamiaa Sayed and Eng. Rana ElKashlan for their continuous support. For my friend, classmate and work colleague, I would like to acknowledge Eng. Yasmine Adel who has been providing me with tremendous emotional support in my work, studies and life. Additionally, special recognition to my best friend in the UAE, Eng. Maha Kadadha, who was available "daily" for me with advices and endless genuine support in so many aspects. Special thanks to my professors in my undergraduate studies at Khalifa University, who were developing my academic and personal skills; prof. Raed Shubair, Dr. Paul Yoo, and Dr. Peng Yong Kong.

Finally, I would like to acknowledge the graduate program directors and professors who have shown great examples of Egyptian scholars: Dr. Ayman El Ezabi and Dr Karim Seddik, Dr. Watheq ElKharashi, Prof. Yehia Ismail, Prof. Ahmed Abu-Ouf, Dr. Yasser Gadallah and Prof. Salah ElHaggar.

List of Publications Out of This Thesis

M.Y. ElSalamouny, H.H.Halawa, R.M.Daoud, and H.H.Amer, "Performance of Fault Tolerant WBAN for Healthcare," 3rd International Conference on Engineering & MIS (ICEMIS), Monastir, Tunisia, May 2017, 4 pages.

M.Y. ElSalamouny, G.I. Alkady, I. Adly, R.M. Daoud, H.H. Amer, H. ElSayed, D.G. Mahmoud, H.A. Ismail, H.H. Halawa, "Highly Available FPGA-Based Smart Band for WBAN" 12th International Conference on Computer Engineering & Systems (ICCES), Cairo, Egypt, December 2017, 6 pages.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

WBAN – Wireless Body Area Network

WLAN – Wireless Local Area Network

NCS – Networked Control System

FPGA – Field Programmable Gate Array

SRAM – Static Read Only Memory

MCU– Microcontroller Unit

ASIC – Application Specific Integrated Circuit

FT– Fault Tolerance

DPR – Dynamic Partial Reconfiguration

PDR– Packet Delivery Ratio

LTE – Long Term Evolution

RSSI – Received Signal Strength Indication

EPC – Evolved Packet Core

WCNI– Wireless Configuration Network Interface

SEC-DED – Single Error Correction-Double Error Detection

IC – Integrated Circuit

SEU – Single Event Upsets

SET – Single Event Transients

MEU – Multiple Transient Upsets

AdDEU – Adjacent Double Event Upset

Chapter 1

Introduction

1.1 Background

Nowadays, with the high advancements in the wireless technology, the integration of such technology in many aspects in our lives became a necessity rather than a luxury especially in critical situations. A very prominent example is in healthcare systems. Not only will wireless healthcare systems ease the patient's mobility but it will also enable the patient's physiological signals to be monitored without the presence of nearby specialized doctor, nurse or medical health personnel. Therefore, this increases the efficiency and the quality of the medical service and transcends to the concept of Internet of Things (IoT). A Wireless Body Area Network (WBAN) is a system composed of a group of sensors that could be wearable or implanted inside the body. These sensors continuously or on intervals gather physiological signals and send them wirelessly to a data center or a server where data is processed and analyzed, and results could be monitored by the doctor.

There are many constraints in the wireless healthcare systems. One of the major issues is the reliability of the nodes and the sensed data while meeting the system requirements. In addition, the susceptibility of the system to interference should be taken into consideration. This is why applying the principles of Networked Control Systems (NCS) would be very convenient. This could also allow automated response to some wireless actuators based on the sensors readings.

Another point of interest is the study of Field Programmable Gate Arrays (FPGAs). FPGAs provide many advantages of both Microcontroller units (MCUs) and Application Specific Integrated Circuit (ASIC) designs. During the operation of a smart node (smart band as explained in chapter 4), the architecture of the node might be changed so its processor would behave differently. This is when the hardware reconfigurability of FPGAs becomes useful. Additionally, FPGAs could allow the recovery from design bugs that might occur also during the lifetime of node.

1.2 Contribution of this Thesis

This thesis presents a novel fault tolerant Wireless Body Area Network (WBAN) architecture in the communication links. The performance of the system is quantified with respect to the susceptibility of the WBAN to different types of interferences. Results and analysis show that the proposed system complies with the design standards of NCSs. The second contribution in this thesis is the design of fault tolerant FPGA-based smart band that could be reconfigurable during normal operation using a novel Wireless Configuration Network Interface (WCNI) FPGA scheme. The design is proposed with two working environments (normal, harsh) and availability of the system is shown to be very high in both.

1.3. Purpose/Objective of Study

This thesis focuses on tackling WBAN issues in the network layer, continuous-time operation, and some hint to the powering sources, in order to solve challenges of latency, data reliability, and low power wireless technology. This is done by presenting a novel WBAN architecture that follows NCS standards in addition to having fault tolerance in the communication links. In addition, the design of an FPGA fault tolerant smart band is presented with two different working environments to ensure the availability of the system. This will ensure a better healthcare service delivery and more reliable systems than the conventional ones.

1.4. Research Methods

The research focuses on design a WBAN system that can be implemented in a patient's house, elderly homes, or even hospitals or any place where the medical personnel is not physically available near the patient. The system should not only allow the doctor to monitor the subject's vital activities, but it also allows some feedback. Such feedback could be automatic as in controlling actuators on the subject's body, manual as the medical personnel overriding the automatic action, or simply sending some instructions to the patient or his/her relatives. Another important aspect is the fact that there might exist a need to change the underlying architecture of the WBAN smart band. The system should then allow reconfigurability while the system is still operational, for example, adding more processing. In addition, it should be prone to

faults that might affect the system performance if not mitigated with the required measures.

The architecture should follow the NCS requirements since health data are critical; therefore, the system is tested against several control loops for monitoring and actuation. For a better analysis of fault tolerant systems, the system is subjected to all possibilities depending on the available nodes and network links and the severity of the sensory data. The system is tested in an interference free medium, network congestion. Another source of interference could be the availability of another patient nearby the subject patient. Therefore, the proposed system should ensure no interference between the two patients while ensuring data reliability and latency criteria are met for each patient.

Regarding the second part of the thesis, the design for an FPGA-based smart band is presented. The smart band architecture should allow for reconfigurability through the wireless network using Dynamic Partial Reconfiguration (DPR). Therefore, the WCNI FPGA scheme is proposed. Moreover, in order to mitigate transient faults, several fault tolerant techniques are proposed and the system availability is calculated using Markov modeling.

1.5. Organization of the Thesis

The thesis is organized into five chapters. Chapter 2 illustrates the concept of WBAN, their applications, components, design challenges and research issue. In addition, previous work in the WBAN field is presented along with FPGAs in WBANs. Chapter 3 presents the novel WBAN architecture with the performance analysis and simulation results from Riverbed 18.0.3 [Riverbed 2017]. Chapter 4 introduces the design of an FPGA-based smart band that could be reconfigured using DPR and the proposed WCNI FPGA scheme. The design is tested in two different working environments for transient fault models. Modeling the system availability is done using SHARPE [SHARPE 2017]. Finally, a conclusion is added to summarize the key outcomes from each chapter and give recommendation for future work.

Chapter 2

Applications of WBANs and FPGAs in WBAN Systems

This chapter is dedicated in providing a detailed description on the concept of WBAN, its applications, components, design challenges and research issues. The typical system architecture consists of sensors, personal device and actuators. Various WBAN systems in the literature are briefly presented with their contributions, in order to provide the state-of-the-art when design WBAN system. In addition, they are used as the basis of research presented in this document. Then, Field Programmable Field Arrays (FPGAs) are presented with their advantages when compared to those of Microcontroller Units (MCU) and Application Specific Integrated Circuit (ASIC) specifically in the medical field. Finally, several types of FPGAs are introduced and Partial Reconfiguration is defined along with fault tolerance in FPGAs.

2.1 Background

Wireless Body Area Network (WBAN) is a system that consists of sensors, actuators, and a personal device (data sink) for the purpose of monitoring the person vital signs [Gusev 2017, Khan 2016, Huynh 2016, Barakah 2012, Latre´ 2011]. There are many applications for WBAN systems. Several challenges are faced when designing WBANs. In addition, there are many research fields that can work on overcoming some but not all of the challenges. Finally, an insight on Field Programmable Gate Array (FPGA) is presented along with its reliability issues to be used later in WBAN systems.

2.1.1. WBAN Positioning

In RF short range technologies, WBAN operates within 1-2 meters from the human body [Hughes 2016]. Another network is the Wireless Personal Area Network (WPAN) which can operate for up to 10 meters of range. Lastly Wireless Local Area

Network is concerned with networks of ranges reaching 30 meters. WBAN can be viewed as a special application of Wireless Sensor Networks (WSNs). Figure 2.1 shows the representation of the mentioned various networks and the Wide Area Network.

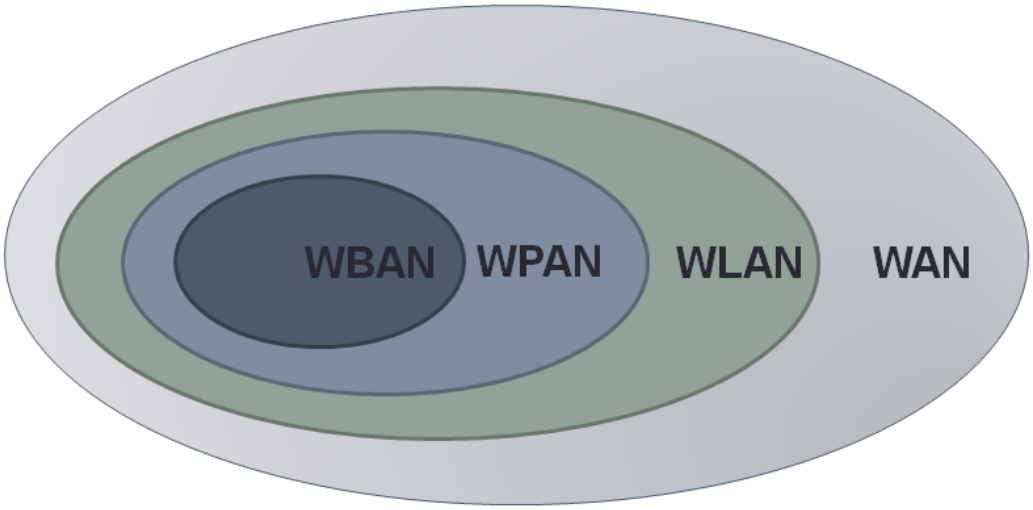

Figure 2.1: WBAN Positioning

2.1.2. Applications of WBAN

WBAN systems have many applications systems and are not limited to chronic medical conditions as data monitoring, illness diagnosis and treatment when possible. WBAN systems can be used in preventing accidents and in public safety in general. Moreover, training professional athletes could be enhanced by incorporating WBAN systems to decide which set of exercises are needed and examine heart and muscles response [Barakah 2012, Latre´ 2011].

In addition, it can be used in hazardous environments where workers are introduced to safety and health concerns as radiologists, nuclear power plants workers, firefighters, policemen, construction site workers, and military officers. Regarding the commercial use of WBAN systems, they can be used in consumer electronics as in virtual reality, gaming and in various appliances [Barakah 2012]. Lastly, WBAN systems can be used to in large scale research projects which aim in gathering physiological data of human beings and performing some statistics and analysis. Hence, WBAN systems lead to more efficient medical and health monitoring services while allowing flexibility to the subject person and his/her medical personnel without them being tied

to a certain machine or a certain place. Since the first application is the most common application, throughout the report, it is used to generalize the main application of WBAN but does not limit the proposed WBAN system to only this application.

2.1.2. WBAN Typical Architecture

A typical WBAN system is shown in figure 2.2. Sensors are connected to the central node via a wireless link protocol, the central node then aggregate that data to the hospital, the physician's handheld device, and the patient's relatives and so on.

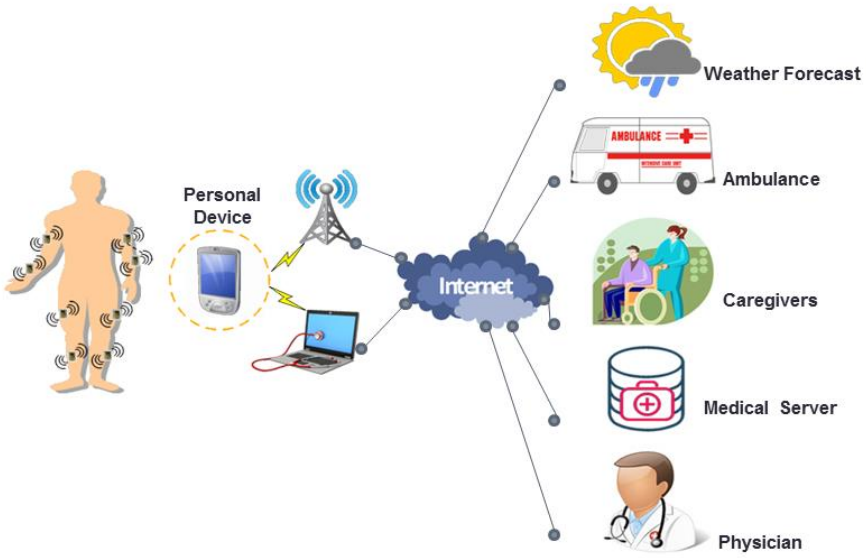

Figure 2.2: WBAN Existing Architecture

2.1.3. WBAN System Components

As mentioned earlier, a WBAN consists of wireless sensor nodes, wireless actuator nodes, and a personal device (PD) that gathers the sensors data and sends the necessary information to the actuators or the monitor system.

2.1.3.1. Wireless Sensor Node (S)

It is a device that collects vital physiological signals and converts them to data to be sent wirelessly. It consists of a physiological sensor, a microcontroller and a wireless network interface. In the Table 2.1 below, a list of most common vital WBAN sensors is shown according to [Barakah 2012, Latre´ 2011]. Another list of WBAN sensors are shown in Table 2.2 as in [Khan 2008].

Table 2.1: WBAN Sensors (1)

Application	Data Rate	Bandwidth	Accuracy
ECG (12 leads)	288 kbps	100-1000 Hz	12 bits
ECG (6 leads)	71 kbps	100-500 Hz	12 bits
EMG	320 kbps	0-10,000 Hz	16 bits
EEG (12 leads)	43.2 kbps	0-150 Hz	12 bits
Blood saturation	16 bps	0-1 Hz	8 bits
Glucose monitoring	1600 bps	0-50 Hz	16 bits
Temperature	120 bps	0-1 Hz	8 bits
Motion sensor	35 kbps	0-500 Hz	12 bits
Cochlear implant	100 kbps		
Artificial retina	50-700 kbps		
Audio	1 Mbps		
Voice	50-10 Mbps		

Table 2.1: WBAN Sensors (2)

Physiological Signal	Parameter range	Data arrival time (sec)	Sample Size (bits)	Data rate (kbs)
Blood flow	1-300 ml/s	0.025	12	0.48
ECG signal	0.5-4 mV	0.002	12	6.0
Respiratory rate	2-50breaths/min	0.05	12	0.24
Blood Pressure	10-400 mm Hg	0.01	12	1.2
Blood pH	6.8-7.8 pH units	0.25	12	.048
Nerve Potentials	0.01-3 mV	5E-05	12	240
Body Temperature	32-40 ^{0}C	5	12	.0024

2.1.3.2. Wireless Actuator Node (A)

It is a device that takes the response and performs a certain physical action. For example, drug delivery device receives action to pump the drug up to a certain extent [Fong 2015] and pacemakers exert an electrical signal to the targeted lead [Rotariu 2012]

2.1.3.3. Wireless Personal Device (PD)

This is a control unit that collects data and acts as a gateway or a sink. It can be a personal digital assistant (PDA) or a smartphone. The main task for this device is collect data from the sensors sends them to a control node then receives the proper action and forwards it to the targeted actuator.

2.1.4. Challenges

There are various challenges that occur when designing a WBAN. To list a few that would be considered in this paper, the challenges [Kraemer 2017, Barakah 2012] are:

1. Latency
2. Data Accuracy
3. Mobility
4. Power Consumption
5. Biocompatibility
6. Wireless Technology: low power technology
7. Security

2.1.5. Research Issues

According to [Kraemer 2017, Barakah 2012], there are many open research issues that could be tackled when designing WBAN systems. They include:

1. Physical layer
2. Data Link layer
3. Network layer
4. Physical characteristics of the electronic circuits of the sensors and the actuators
5. Resource management
6. Powering source
7. Energy issues
8. Computational power
9. Material constraints
10. Security
11. Continuous-time operation
12. Usability
13. Quality of Service (QoS)
14. Signal and path performance

In the next subsection, various related works on WBAN systems addressing one or more of the previous mentioned research issues and challenges.

2.2. Tackling Some WBANs Design Issues

In [Khan 2008], the performance of WBANs in a hospital network was evaluated in various patient monitoring environments. Each wireless sensor on the patient sends to hospital's service node via IEEE802.15.4/ZigBee. The server then sends the data over the Internet with reasonable delays. Since the packets from each sensor is short in size and are sent continuously, this increases the transmission delays; thus decreasing the system's efficiency. It is recommended to gather sensors data in one master node before transmission.

Solving the issues of energy consumption, and QoS of WBANs, [See 2012] presented a study of the best location for the transmitter node (sensor) to achieve the best link reliability with receiver node fixed on the wrist. This was studied while the patient is stationary, walking or jogging with respect to Packet Delivery Ration (PDR) and Received Signal Strength Indicator (RSSI).

Similarly, [Khan 2016] presented WBAN architecture to find the optimal placement of the gateway node on the human body. The gateway is defined as the node which gathers all sensors data and sends them to the medical servers or doctors. Finding the optimal placement was studied against three different human postures; walking, standing, and sitting with respect to the end-to-end delay, Packet Delivery Ratio (PDR), back-off duration and nodes power consumption. There were seven suggested placements of the gateway as shown in figure 2.3. As per the simulation results, node 5 placement has shown the lowest delay in walking posture, while node 7 had the lowest delay in sitting and standing positions.

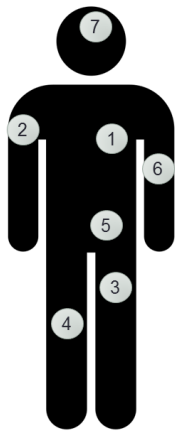

Figure 2.3: Gateway Node Placement

In [Huynh 2016], a WBAN system for healthcare monitoring application based on ZigBee standard was proposed to solve the issue of energy consumption as in the idle or sleep mode. The sensors send data to a WBAN coordinator which in turns sends data to a WBAN gateway. Similarly, the gateway communicates with the medical monitor system. This design did not consider the actuators needed in a WBAN system.

With the use of IEEE802.15.4/ZigBee in WBAN systems, the issue of coexistence occurs especially for mobile nodes (dynamic coexistence) in WBANs. This happens when more than one patient are in the same location which could affect the WBAN functionality and efficiency. Therefore, [Deylami 2014] presented a Dynamic Coexistence Management (DCM) to increase the reliability of the monitoring data for the patients.

Considering the introduction of wireless actuators, [Rotariu 2012] presented a design of a monitoring system for patients with cardiac wireless pacemakers. The system relies on low power transmission and signal repeaters to amplify the signal to be sent to a personal computer through the access point; however, this system is only applicable for indoor environments. Thus, this limits the mobility of the patient. Regarding wireless drug delivery, [Fong 2015] presented two prototypes for micro-electro-mechanical system to allow for localized and precise drug injection based on external RF signal.

Unlike WBANs for health monitoring applications, [Youssef 2015] presented a WBAN model for firefighters taken into account the environmental conditions and their health status in critical situations. Figure 2.4 shows the proposed system architecture. Another interesting WBAN application, [Saleh 2015] presented a design for a prosthetic arm for real time actuation of motors in the upper arm (Sensor1), elbow (Sensor2) and wrist (Sensor3). Each location consists of four sensors (Torque, Position, Current, and Temperature). The communication links have been subjected to external interference while succeeding to follow the systems benchmarks. Figure 2.5 shows the ZigBee channel allocations in the prosthetic arm proposed in [Saleh 2015].

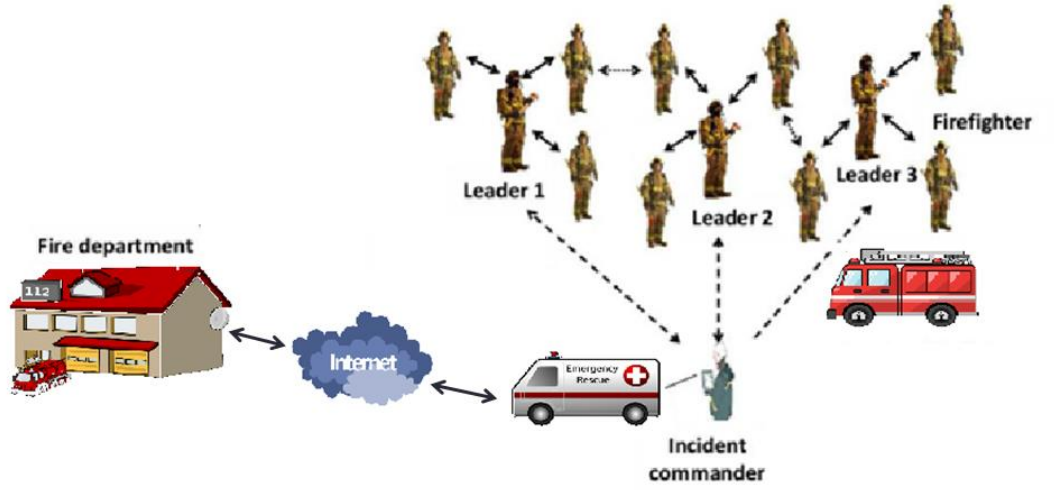

Figure 2.4: Firefighters WBAN Architecture

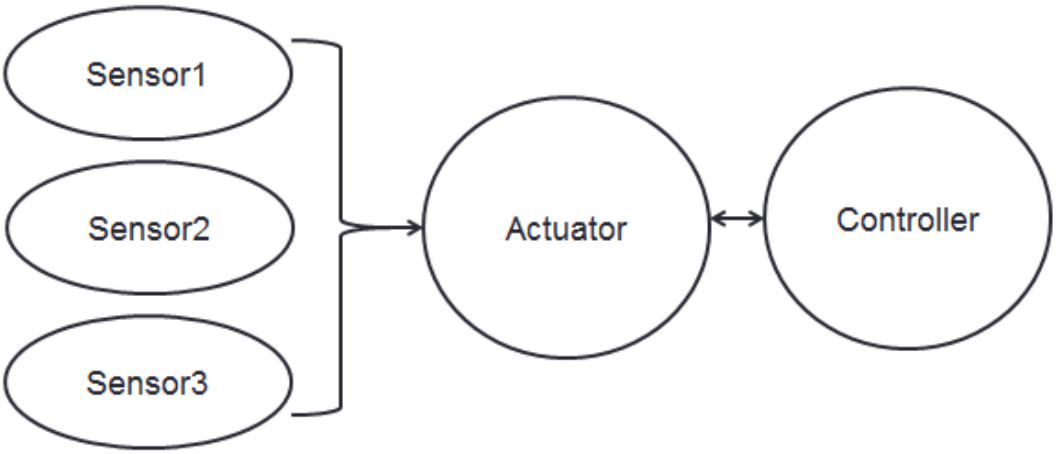

Figure 1.5: Channel Allocation in the Robotic Arm

In order to study the effect of interference, [Abdel Reheem 2012] has presented three techniques of interferences that could be used to evaluate the performance of WBANs. The techniques are network congestion, medium congestion and jammers. Network congestion represents two interfering nodes communicating with close proximity to the main patient for example sharing the same communication standard. For

medium congestion, the two interferers share the same channels allocated for the patient. Finally, for the jammers, it is an intentional interference which could result from surrounding ambient factors that might deteriorate the wireless sensors data for example.

2.3. FPGA in WBAN Systems

2.3.1. FPGA Definition and Types

Another point of interest is the Field Programmable Gate Arrays (FPGAs) and how to integrate them in a WBAN system. FPGA is semiconductor prefabricated silicon device that can be configured as digital circuit design system. Nowadays, FPGAs are used in various applications including automotive and space industries, and in communication networks that require high data processing. In addition, current FPGA solutions provide the system designer to lower the medical system's size, power consumption and cost [Xillinx Medical].

FPGAs have been long known for many advantages compared to the conventional Microcontroller Units (MCU), as for better performance in processing signals with high data rates which eventually leads to lower power consumption of the FPGA nodes. This is a very crucial property needed in WBAN designs especially when using sensors with high data rates like Electrocardiography (ECG), Electromyography (EMG), and Electroencephalogram (EEG). In specific, [Mills 2016] used an algorithm on EEG signals and implemented it an MCU, FPGA, and ASIC. Results have shown that FPGA outperforms in MCU in computational power of bitwise operations. Even though FPGA was used as a prototype for an ASIC which explains high power consumption of the FPGA when compared to that of ASIC, advantages of using an FPGA rather than ASIC is presented below.

When comparing the performance of FPGAs to that of Application Specific Integrated Circuit (ASIC) designs, the FPGAs allow for software/hardware reconfiguration while the system is operating. Unlike in ASIC designs, the software cannot be updates and the ASIC chip should be redesigned. This comes at the expenses of the higher cost of the WBAN using FPGA over that using ASIC in large scale production. In addition, larger area and more power consumption compared are the drawbacks of such configuration flexibility in FGPA designs. However, if the design of the WBAN is customized based on each person medical state, it is favorable to a have configura-

ble system especially in processing [Maricau 2013]. From an economical perspective, FPGA-based systems have faster time to market when compared to that of ASIC [Xilinx 2017].

Nowadays, FPGAs are used in various biomedical applications that are not limited to imaging purposes. FPGAs are used in several medical devices and equipment as electro surgery, heart assistive (pacemakers), automatic external defibrillators and biosensors. Moreover, they are used in portable patient monitoring systems and drug delivery systems [Maricau 2013].

2.3.2. Types of FPGAs

There are several types of FPGA based on the memory technologies as anti-fuse based FPGA, Static (SRAM) based FPGA, and Flash-based FPGA. Anti-fuse based FPGA uses modified CMOS technology which lessens parasitic resistance and capacitance, hence, decreasing the area. The drawback of this FPGA type is that it cannot be reprogrammed. Flash-based FPGA relies on nonvolatile memory which provides more area efficiency when compared with that of other technologies; however, reconfiguration and reprogramming cannot be performed for infinite times. Finally, the SRAM based FPGA uses static memory cells to program configurable logic blocks (CLBs) that are connected by interconnects in addition to I/O blocks which are both programmable as shown in figure 2.6 [Brown 1996, Xillinx 2017]. FPGA solutions provide to lower the medical system's size, power consumption and cost [Xillinx Medical]. There are various FPGA designs among which SRAM-based ones are more favored since they provide high performance needed to perform signal processing, reconfigurability when the system evolves and finally reduced development cost [Baig 2012, Xillinx 2017].

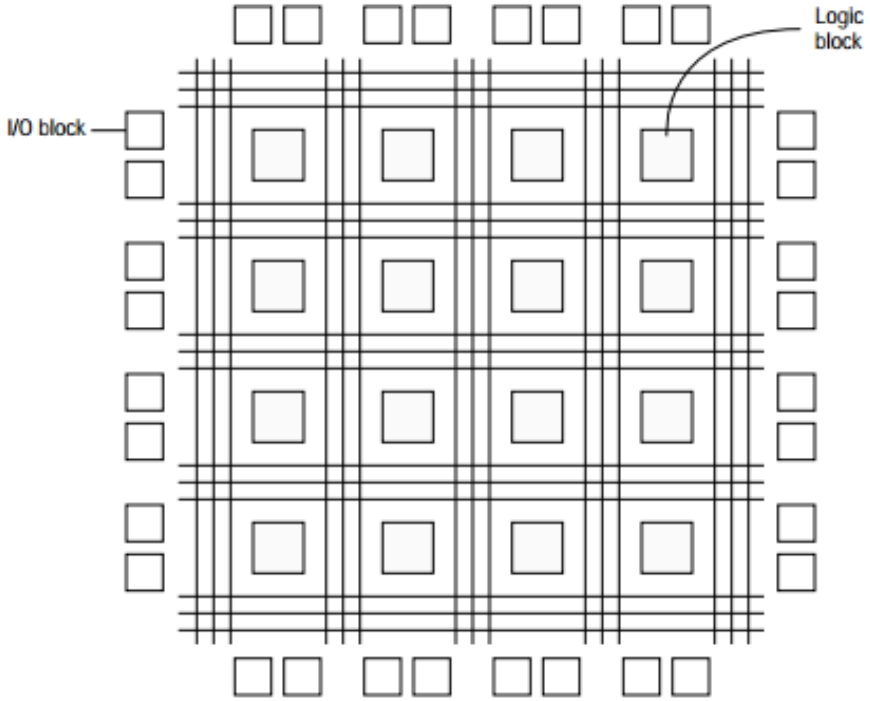

Figure 2.6: FPGA Architecture [Brown 1996]

2.2.1. Partial Reconfiguration (PR)

One of the main advantages of the use of FPGAs is its flexibility to reprogram the design without having to go through the fabrication process. In addition, the FPGAs functionality to perform Partial Reconfiguration (PR) allows to partially re-configuring a location on the FPGA using a partial BIT file without affecting the normal static operations [Xilinx 2017]. Thus, PR modifies subset logic by downloading partial configuration file of an FPGA design [Xilinx 2017]. Figure 2.7 shows how partial reconfiguration is performed. When implementing a system on an FPGA, the logic is predefined by the developer to be either static logic or reconfigurable logic. The static logic remains unaffected when PR is performed on Block A. A1.bit, A2.bit, A3.bit and A4.bit are examples of BIT files that can be downloaded and reprogrammed into the FPGA.

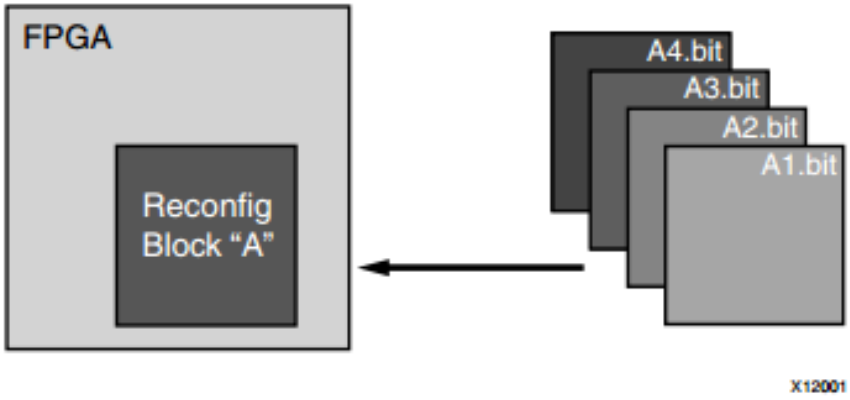

Figure 2.7: Partial Reconfiguration [Xilinx 2017]

PR is divided to two categories, static partial reconfiguration and Dynamic Partial Reconfiguration (DPR). Static partial reconfiguration requires the normal FPGA operations to be stopped until the reconfiguration is completed, while DPR is performing PR while the other static logic is still operational [Savani 2011].

2.2.2. Fault Tolerance in FPGA

Fault tolerance is a very essential aspect to be considered when designing WBAN systems. When using FPGAs in WBANs, system faults are needed to be considered to ensure no safety critical situation occurring. There are two types of faults in FPGAs, transient and permanent faults. Permanent faults on the other hand, cause an non recoverable damage to the FPGA's silicon. They include Electromigration (EM), Hot Carrier Injection (HCI), and Time Dependent Dielectric Breakdown (TDDB), electro-migration and hot carrier effect work on damaging the semiconductors and with aging effects could lead to permanent faults [Baige 2012, Gauar 2010, Maricau 2013]. Electromigration (EM) occurs in metals as in interconnects and vias when high density current collide with the metal atoms creating voids and hillocks.

This could deteriorate the current flow in the metal and will eventually lead to permanent non recoverable faults [Maricau 2013]. Hot Carrier Injection (HCI) occurs when a 'lucky' electron escapes from the channel to the dielectric material reducing the efficiency of the channel and this could eventually leads to a permanent deformation of the channel. Finally, regarding Time Dependent Dielectric Breakdown (TDDB), it is when high electric field occurs from the substrate to the dielectric

which could permanently damage the dielectric material [Maricau 2013]. Solving such permanent faults that occur with aging require proper system design, enhanced material selection as metals and dielectrics and providing redundancy in case of a permanent failure in a module.

On the other hand, transient faults are those that occur during the useful life of the modules such that they will momentarily change the system behavior but will not cause permanent damage to the FPGA fabric. In order to recover from transient faults, reconfiguration is done on the faulty module [Alkady 2015]. These faults include on-chip crosstalk noise, simultaneous switching noise (SSN) as substrate noise, energetic particles and radiated external Electromagnetic Interference (EMI) [Maricau 2013]. Transient faults include Single Event Upsets (SEUs), Single Event Transients (SETs), and Multiple Transient Upsets (MEUs). In particular, external radiation causes a change in the depletion region in the CMOS channel; thus, this could flip the logic from '1' to '0' or from '0' to '1'. An illustration on this phenomenon (SEU) is shown in figure 2.8 according to [Savani 2011].

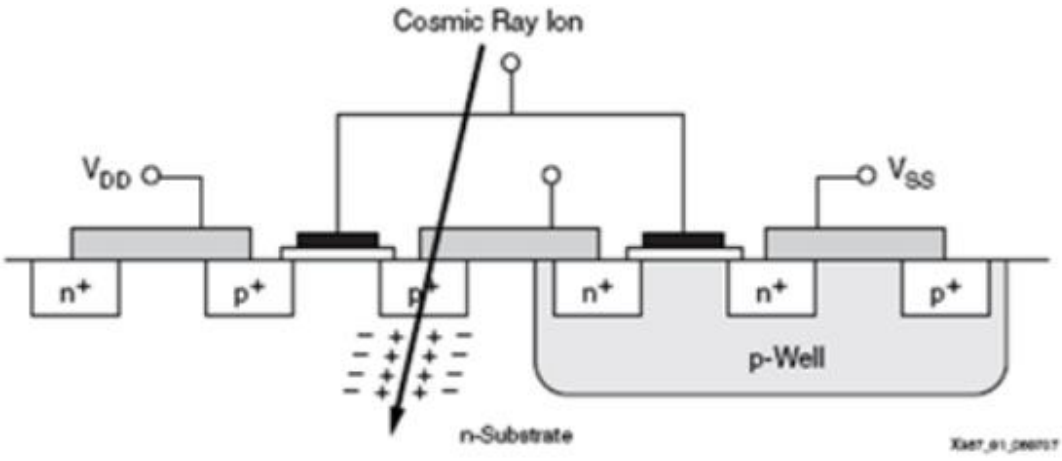

Figure 2.8: SEU in FPGA

In [Alkady 2017], ways to mitigate SEUs and some MEU effects are done using fault-tolerant FPGAs techniques as N-Modular Redundancy (NMR) and reconfiguring the faulty modules using Dynamic Partial Reconfiguration (DPR). The research focused on solving the issue of transient faults. This is due to the fact that the probability of transient faults is more than that of permanent faults, in addition, transient faults could give a wrong indication of the output which is an effect that could

cause major problems in systems like WBANs with hard real time constraints. In the next chapter, WBAN architecture is presented and according to this design, a smart band using FPGA is proposed in the following chapter.

Chapter 3

Performance of Wireless Body Area Network (WBAN)

This Chapter introduces the WBAN system architecture developed and analyzed using on Riverbed 18.0.3 previously named as OPNET Modeler Suite [Riverbed 2017]. It is a powerful network simulator used in testing technology designs, increasing network R&D productivity, developing customized wireless protocols and technologies, and finally evaluating any enhancements in the existing protocols. The first section explains in details the system architecture and all of the necessary system parameters. The second section illustrates the definitions of some possible scenarios at which the architecture is examined against. Finally, simulation results of the system are analyzed in no interference medium, network congestion and with identical system with close proximity to the original.

3.1. System Architecture

The proposed system consists of wireless sensors and actuators either wearable or implanted on a patient's body connected to a smart wrist-band. The smart band gathers sensors data and sends the aggregated data to the access point available in the patient's house. In addition, a duplicate of the sensors data is sent to the patient's smartphone. The smartphone has special software processes the received sensors data coming from the smart band. Then, the smartphone generates response/action to be sent back to the smart band which in turns controls the actuators. Meanwhile, the two copies of the aggregated sensors data received by the access point and the smartphone along with the action taken by the smartphone are passed to the control node (CN) where the doctor or the hospital is located. This is done for monitoring purposes or for taking over the action taken by the smartphone when needed or for performing the necessary actions in case of emergencies. For instance, if an emergency occurs, the medical personnel could send the ambulance or inform the patient's relatives or healthcare personnel with the necessary instructions.

In this system, it is assumed that the sensors and the actuators are located 1m away from the smart band. Moreover, the distance between the smart band and the smartphone is 3m and the distance between the patient's smart band and the access point is 10m. Figure 3.1 shows the architecture of the proposed WBAN system.

The two main communication technologies that are used in this architecture are low-power IEEE802.11n and LTE. Low-Power IEEE802.11n Wi-Fi is used for short-range communications as with the networks with close proximity to the patient. The choice of IEEE802.11n is due to its high data rate and the two frequency bands it supports; 2.4GHz and 5GHz. Therefore, this enables higher bandwidth and more non-interfering channels to be used especially when assuming that the patient is living with family members who are connected to the same AP. On the other hand, LTE is used for long range communications as with the link between the smartphone and the CN. The use of LTE capability in the smartphone increases the mobility of the patient and enables health monitoring in areas with no Wi-Fi coverage. Figure 3.2 shows the channel allocation of the various links. Symbols Ss' and 'As' stand for sensors, actuators, respectively, while symbol 'B' represents the smart band, and 'Ph' is the smartphone.

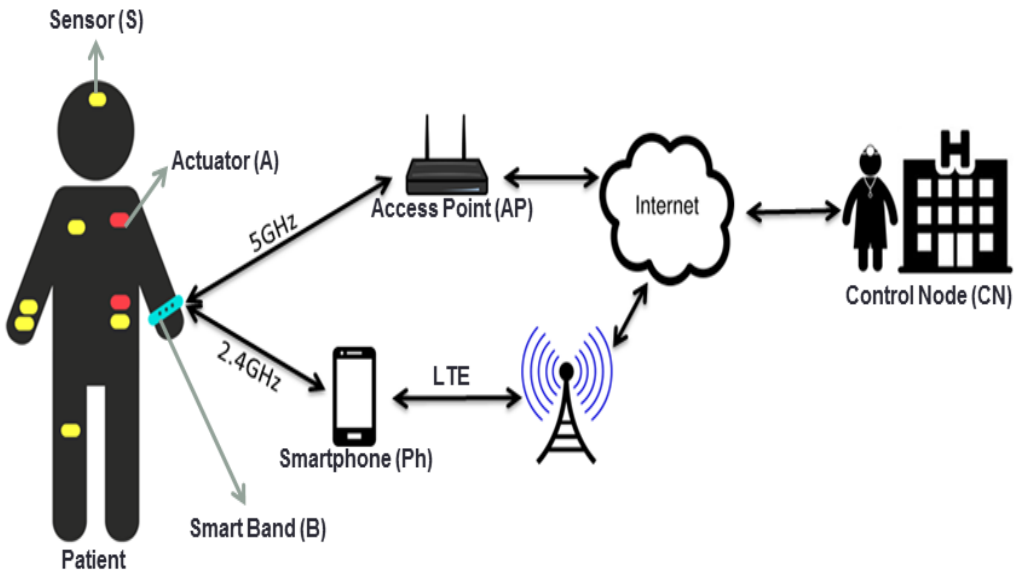

Figure 3.1: Proposed System Architecture

The system consists of six sensors [Latre´ 2011], shown in Table 3.1, connected to the smart band via Ch1 (IEEE 802.11n-2.4GHz). The actuators are connected to the smart band on Ch6 (IEEE802.11n-2.4GHz). The smart band, then, communicates with the smartphone on Ch11 (IEEE802.11n-2.4GHz) and with the access point on Ch40 (IEEE802.11n-5GHz). Thus, the choice of channels ensures no interference between the different links. As mentioned earlier, LTE is solely used for the communication link between the smartphone and the CN. The access point, and the eNodeB at which the patient's smartphone is connected to an Evolved Packet Core (EPC) which in turns is connected to a cloud node that also connects to the CN. The cloud node represents communication over the Internet. This allows the medical personnel to monitor patient's health activity and take actions when needed from anywhere in the world without the need of being physically available in a certain location.

Table 3.1: System Data Rates

Node	***Data Rate***
Blood Saturation Sensing Temperature Sensing Glucose level Sensing Motion Sensing Electroencephalogram (EEG) Electrocardiography (ECG)	1Byte/sec, 1Byte/sec, 100Bytes/sec, 1kBytes/sec, 0.33kBytes/sec, 1kBytes/sec
Actuators (A1, A2)	2Bytes/sec
Band (B) to Smartphone (Ph) or Band (B) to Access Point (AP)	2436Bytes/sec
Access Point (AP) to Control Node (CN)	2436Bytes/sec
Smartphone (Ph) to Control Node (CN)	2436Bytes/sec
Response Packet (R)	1Byte/sec

Figure 3.2, shows the different channel allocations ignoring the link of the access point, LTE infrastructure and the gateways. The arrow direction shows the source and destination of the packets. For the link between the smart band and the phone, the forward arrow represents the sensors data sent to the CN while the backward arrow represents the needed action to the actuators or the overriding response from the CN to smart band. The forward arrow from the smart band to the phone represents the sensors data while the backwards arrow represents the action made on the smartphone by the application installed on the phone. The two forward LTE links between the smartphone and the CN represent the sensors data along with the same action taken by the phone to the smart band. Finally, the backward LTE link indicates the overriding response to the smartphone.

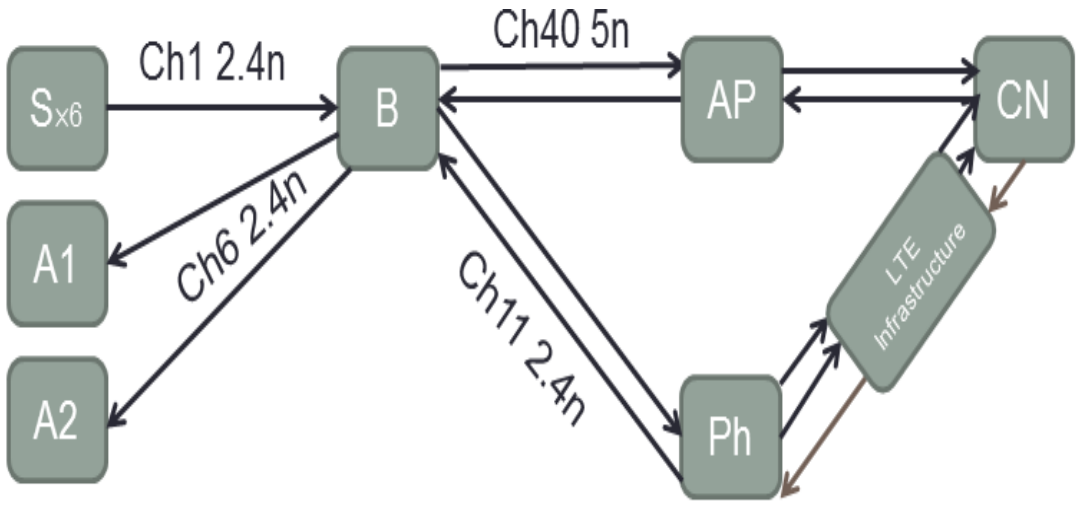

Figure 3.2: System Channel Allocations

Regarding the payloads, since the patient's data is considered control signals, UDP is used to send the data in this system [Abdel Reheem 2012]. In Table 3.2, the sensors data include most but not all vital signals that a doctor needs to monitor selectively or collectively. For the worst case analysis, all of the provided most common six sensors are taken to be operational at the same time whether the signals are needed to be monitored or not. Similar argument is made with the actuators that could be wireless pacemaker devices, drug pumps, defibrillators, etc [Rotariu 2012, Fong 2015]. The data sent from smart band data is the aggregated sensors data over one second. This data is sent to both the smartphone and the access point which in turn send the two sets of data to the CN. The response packet from any node to another is set to be 1Byte/sec.

3.2. Test Scenarios Definitions

Since reliability is a major challenge in NCSs and especially when dealing with human's health as in WBAN, duplicated paths for the sensors data are added to the system. As previously mentioned, the sensors data are sent to both the access point and the smartphone. As a result, if one links fails, the other path is present for the controller to receive sensors data, process them and send the required action to the actuators. The controller is either the smartphone or the CN which has the same software installed on the smartphone. Therefore, the CN could overtake the action in case of the smartphone failure. It is worth mentioning that fault tolerance is not considered on the sensors and actuators levels. The only assumption made is that they could be powered by piezo-cells or wireless charging to allow more durability of the system [Adly 2016]. The smart band fault tolerance is going to be introduced in the next chapter. For the CN level, it is assumed that it is a very robust machine that carries out the required tasks.

In order to properly define the system's functionality, hence quantify its performance, there are several scenarios simulated based on the severity of the patient's condition and accordingly produce the proper response and based on the availability of the functioning nodes that would send and receive information. In Table 3.2, the definition of nine scenarios is shown where each scenario is represented by (XY) as in [ElSalamouny1 2017]. Symbol X represents the status of the nodes, while symbol Y represents whether an action in needed or not depending on severity of the sensors data whether it requires no action or action from the phone or the CN.

Table 3.2: Scenarios Definition

X	***Functioning Nodes***	***Y***	***Severity of The Sensors Data***
1	All nodes are working	1	No action is needed
2	The access point fails	2	Action is needed by smartphone
3	The smartphone fails	3	Action is needed by CN

In specific, the scenario denoted by (11) as shown in figure 3.3 indicates no failure in the access point or the smartphone along with the fact that the sensors data are showing normal behavior and hence, no action is required by the actuators. Therefore, when the data are sent from the sensors to the smartphone through the smart band, the smartphone will process the data and produce a response to the CN indicating that no action has been taken because the data shows normal status. As mentioned earlier, the access point and the smartphone send the sensors data to the CN and this applies to all scenarios with X=1.

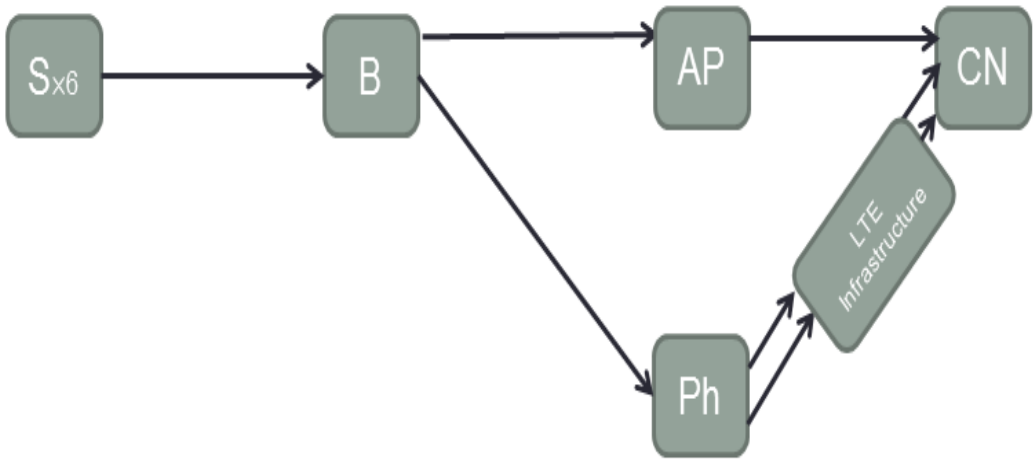

Figure 3.3: Scenario (11) Definition

Similarly, in scenario (12), no node failure is observed; however, an action is required by the phone. Therefore, a response packet is sent from the smartphone to the smart band which, accordingly, gives a signal to enable the targeted actuator. Meanwhile, the CN receives the same response packet from the smartphone so that it ensures that the proper action was taken. For scenario (13), if the CN needs to override the action as done in scenario (12), it can send a response packet to the smart band via the access point Wi-Fi access point link.

Scenario (21) indicates a failure in the access point and no action is required to the actuators. In this scenario, only one copy of the sensors data is sent from the smart band to the smartphone. Hence, the CN receives one copy of the sensors data along with the no response packet generated by the smartphone. As for scenario (22), where the access point fails and an action is required, the smartphone receives the sensors data

through the smart band. The smartphone could, then, generate the required response and send it back to the smart band which in turns gives the signal to the targeted actuator. Similarly, the response packet of the action taken by the smartphone is sent to the CN. Scenario (23) as shown in figure 3.4 is similar to the previous scenario; however, the medical personnel need(s) to either overtake the action done by the smartphone or simply notify the patient that the access point has failed. The CN action could be just sent through the smartphone LTE link.

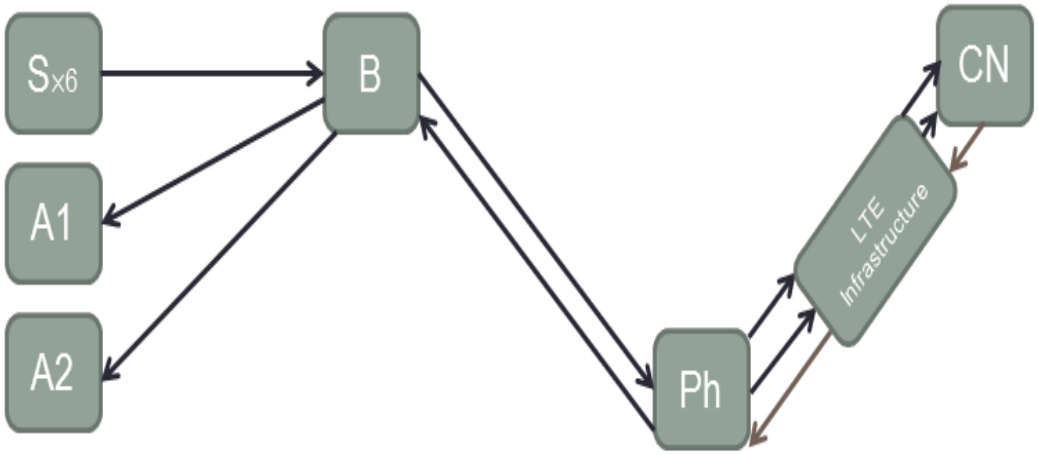

Figure 3.4: Scenario (23) Definition

When the smartphone fails as with scenarios with X=3, scenario (31) indicates that sensors data shows normal behavior and no action is required. Therefore, the smart band aggregates the sensors data to the access point which, accordingly, sends them to the CN. As for scenario (32) shown in figure 3.5, where an action is needed, the CN receives the data from the access point and waits for the response packet and the data from the other link. If the data does not arrive, the software at the CN will generate the needed response and forwards it back to the smart band via the access point link. The smart band, then, gives a signal to the targeted actuator. Unlike in scenario 32, in scenario (33), the medical personnel would need to override the action taken by the software or send signal notifying the patient or emergency contacts (as the patient's relatives) that the smartphone is not functioning.

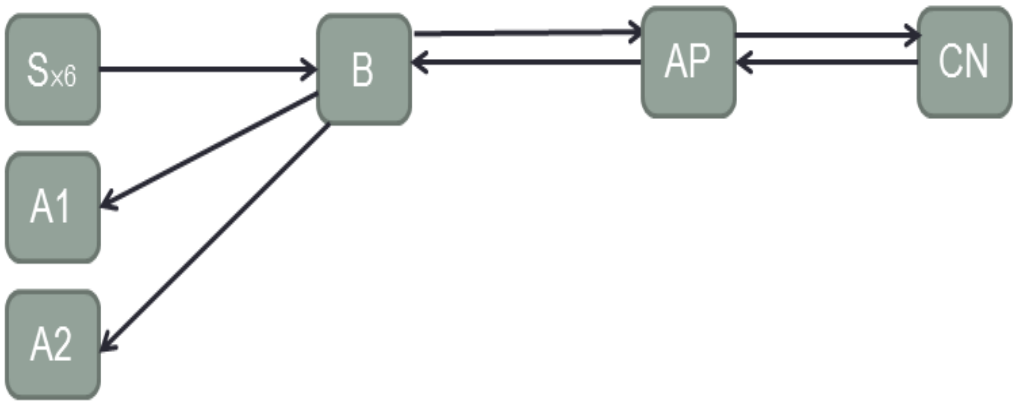

Figure 3.5: Scenario (32) Definition

In order to define system deadlines from as per the real time system constraints, four loops are defined as shown Table 3.3. By using the term 'closed loop', it means sensors data send to the controller then a local decision is made and sent to the actuators. The controller could be either the smartphone as in closed loop1 or the CN as in closed loop 2. The closed loops represent data gathering, processing and decision making while the opens loops represent data and monitoring. Accordingly, open loop allows monitoring the sensors data from the sensors and the decision from the smartphone (if taken) to the CN. Therefore, open loop1 indicates monitoring sensors data coming from the smartphone while open loop 2 indicates monitoring via the access point. The system ensures that each scenario from the nine scenarios has a minimum of one closed loop and one open loop except for the scenarios with Y=1 where no action is needed and in other words a closed loop is invalid.

Table 3.3: Control Loops Definition

Loop Definition	***Loop Links***
Closed Loop 1	Ss → B → Ph → B → As
Closed Loop 2	Ss → B → AP → CN → B → As
Open Loop 1	Ss → B → Ph → CN
Open Loop 2	Ss → B → AP → CN

According to the nine defined scenarios, the system is evaluated based on the total end-to-end delay and the packet loss ratio for each link using Riverbed 18.0.3 [Riverbed 2017]. As mentioned earlier, as all of the data in this system is sent using UDP, video conferencing statistics are used to check these parameters. Since the cloud topology is varied and is not of an interest in this research, an IP cloud node is used in the simulation. However, in order to accurately model its effect on the system, scenario (13), which has all of the control loops satisfied, is later used with changes in the cloud parameters. The cloud parameters are 100ms packet delay and a 0.1% packet loss ratio [Sethi 2012].

In order to model low-power 802.11n on Riverbed, the transmission power was considered to be 1mW and its receiver sensitivity is -95dBm [Riverbed 2017, Wi-Fi Alliance® 2016, Perez 2015]. Moreover, a maximum data rate of (65Mbps) is used as provided by the simulator. When applying the interference on the links, the interferer nodes had transmission power of 5mW with the same receiver sensitivity [Abdel Re-heem 2012]. For the WLAN and the LTE communications, the parameters of nodes are shown in Table 3.4.

Table 3.4: WLAN and LTE Parameters

WLAN Node Parameters	
HT PHY 2.4GHz (802.11n)	HT PHY 2.4GHz (802.11n) or HT PHY 5GHz (802.11n)
Data Rate (bps)	65Mbps
Channel Settings	Ch1, Ch6, or Ch11 for 2.4GHz (802.11n) or Ch40 for 5GHz (802.11n)
Transmit Power (W)	0.001W
Packet Reception-Power Threshold (dBm)	-95dBm
UE Node Parameters	
Antenna Gain (dBi)	-1dBi
Maximum Transmit Power (W)	0.5W
Receiver Sensitivity (dBm)	-200dBm
eNodeB Node Parameters	
PHY Profile	LTE 20MHz FDD
Antenna Gain (dBi)	15dBi
Maximum Transmit Power (W)	0.5W
Receiver Sensitivity (dBm)	-200dBm

3.3. Performance Analysis and Simulation Results

All of the simulation results are evaluated on 33 runs with different initial seeds and confidence analysis of 95% on the data averages of all runs. The proposed healthcare system is tested in with no interference medium with the introduction of the IP cloud parameters on scenario (13) as it is the most congested scenario with links. Then, the same scenario is tested with network congestion and finally, another patient WBAN system is added to the model as a source of interference.

3.3.1. No-Interference Model

Simulating the no-interference model on Riverbed with all of the necessary parameters for the nine separate scenarios, each link's end-to-end delays for each scenario is obtained with confidence of 95% on the average of the 33 runs. The maximum of each link's confidence interval shown in Table 3.5 [ElSalamouny1 2017] is added as in Table 3.6 to find the total end-to-end delay of each loop as shown in Table 3.7 based on the loop definitions in Table 3.3. It could be observed that the link delays in each scenario slightly differ as in S→B link. This is due to the simulator's failure to accurately model the values in the micro seconds scale.

The results show that for closed loop1, the maximum delay for all scenarios is 968μs which is the total delay in the Wi-Fi links. Similarly, for the closed loop 2, the maximum delay is 37.6ms for scenarios 13, 32, and 33 which is the total delay of the Wi-Fi and the LTE links as in scenario (32) where the CN needs to wait for LTE link (represented by the smartphone) to send response packet and the data. For scenario 23, the delay in the closed loop 2 is remarkably higher than other scenarios due to the fact that the CN can only override action through the LTE link which is usually slower than the Wi-Fi link. In all scenarios, there is zero packet loss. Based on these results, the system has a significant lesser end to end delay than sampling period of the smart band which is 1s.

Table 3.5: System Link Delays

	11	**12**	**13**	**21**	**22**	**23**	**31**	**32**	**33**
A1		48.8 µs	69.3 µs		64.1 µs	77.7 µs		64.1 µs	64.1 µs
A2		63.4 µs	57.8 µs		66.3 µs	70.2 µs		69.1 µs	69.1 µs
S-B	59.2 µs	64.5 µs	65.7 µs	61.6 µs	57.8 µs	54.1 µs	60.7 µs	62 µs	62 µs
B-CN	597 µs	597 µs	608 µs				597 µs	634 µs	630 µs
B-Ph	580 µs	627 µs	605 µs	580 µs	631 µs	627 µs			
Ph-CN	14.5 ms	14.5 ms	14.5 ms	14.5 ms	14.5 ms	17.1 ms			
Ph-CN(R)	13.3 ms	13.3 ms	13.3 ms	13.3 ms	13.2 ms	16.3 ms			
Ph-B(R)		179 µs	142 µs		213 µs	18.5 µs			
CN-B(R)			188 µs					220 µs	220 µs
CN-Ph(R)						19.6 ms			

Table 3.6: Loop End to End Delay Calculations

	Closed Loop1	Closed Loop 2	Open Loop 1	Open Loop 2
11			S-B, B-Ph, Ph-CN	S-B, B-CN
12	S-B, B-Ph, Ph-B, max(A1,A2)		S-B, B-Ph, Ph-CN	S-B, B-CN
13	S-B, B-Ph, Ph-B, max(A1,A2)	S-B, B-CN, CN-B, max (A1,A2)	S-B, B-Ph, Ph-CN	S-B, B-CN
21			S-B, B-Ph, Ph-CN	
22	S-B, B-Ph, Ph-B, max(A1,A2)		S-B, B-Ph, Ph-CN	
23	S-B, B-Ph, Ph-B, max(A1,A2)	S-B, B-Ph, Ph-CN, CN-P, P-B, max(A1,A2)	S-B, B-Ph, Ph-CN	
31				S-B, B-CN
32		S-B, B-CN, CN-B, max(A1,A2)		S-B, B-CN
33		S-B, B-CN, CN-B, max(A1,A2)		S-B, B-CN

Regarding the monitoring loops, open loop1 has an average delay in all scenarios of 17.78ms that is the summation of the Wi-Fi and LTE delay links. Finally for monitoring open loop2 through the Wi-Fi access point, the maximum delay is 696µs which presents delays in the Wi-Fi links. Figures from 3.6-3.10 show the end-to-end delay of several runs where the horizontal axis represents time (minuets) while the vertical axis is the end-to-end delay (in seconds). Figure 3.6 shows the simulation results for 10 runs for the Ph→CN (Response) link of scenario (11), while figure 3.7 [ElSalamouny1 2017] shows the output of 10 runs, however, for the B→Ph link in scenario (12). Figure 3.8 illustrates the output of 10 runs of the S→B link of scenario (21), while figure 3.9 shows that for Ph→CN link of scenario (23). Lastly, figure 3.10 shows the output results of the B→CN of scenario (33).

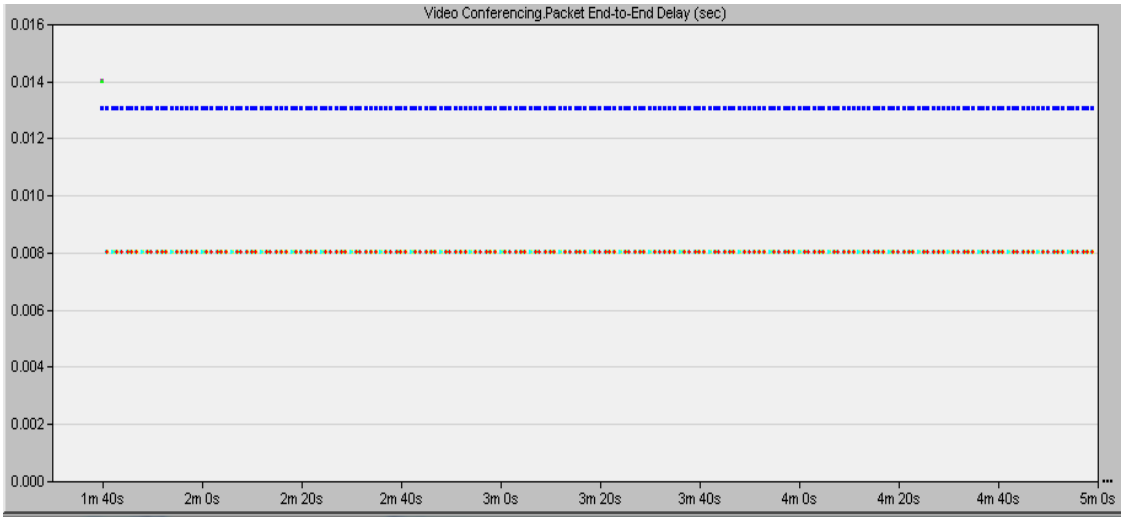

Figure 2.6: Ph-->CN (Response) Scenario (11)

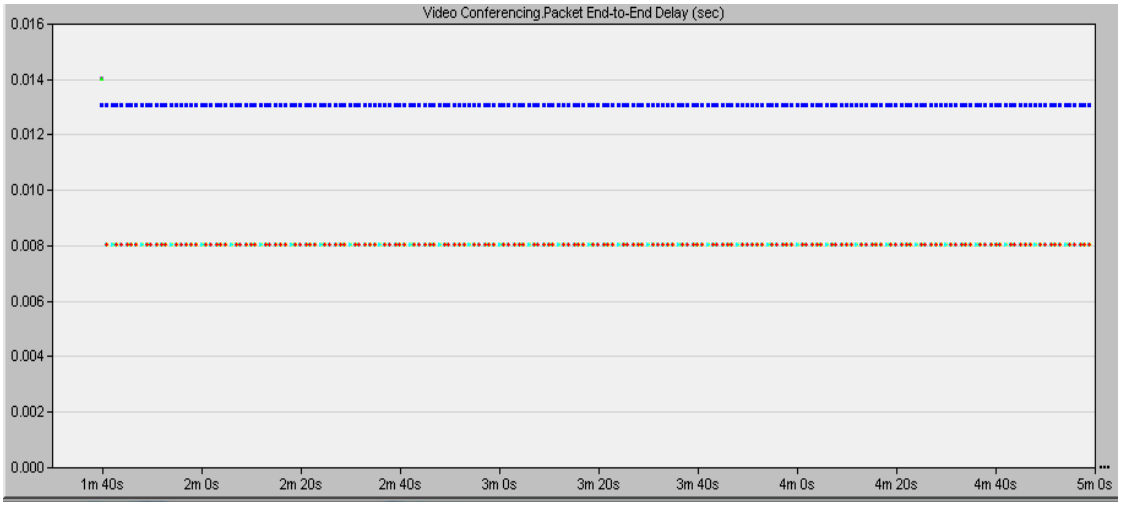

Figure 3.7: B-->P Scenario (12)

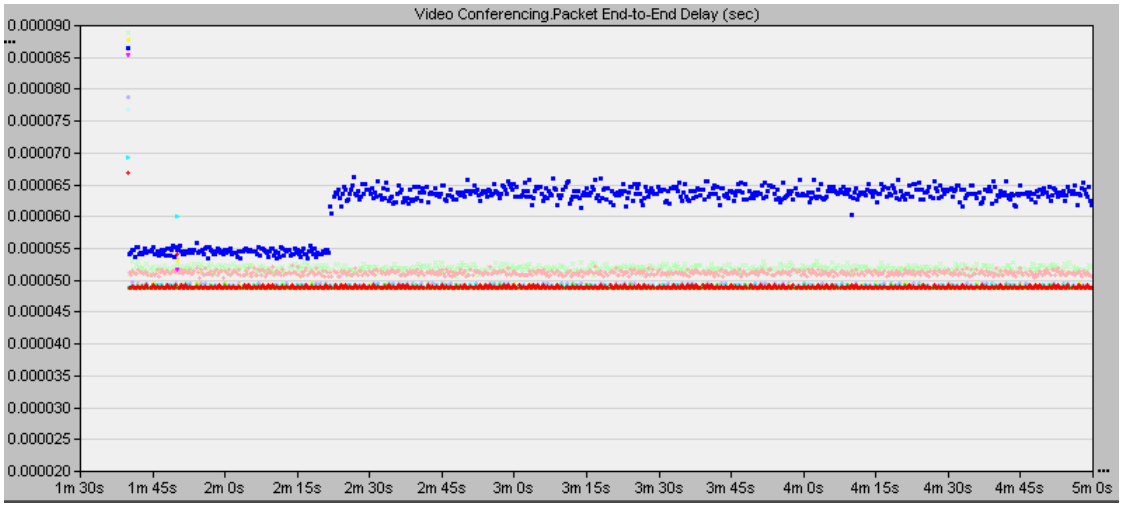

Figure 3.8: S-->B Scenario (21)

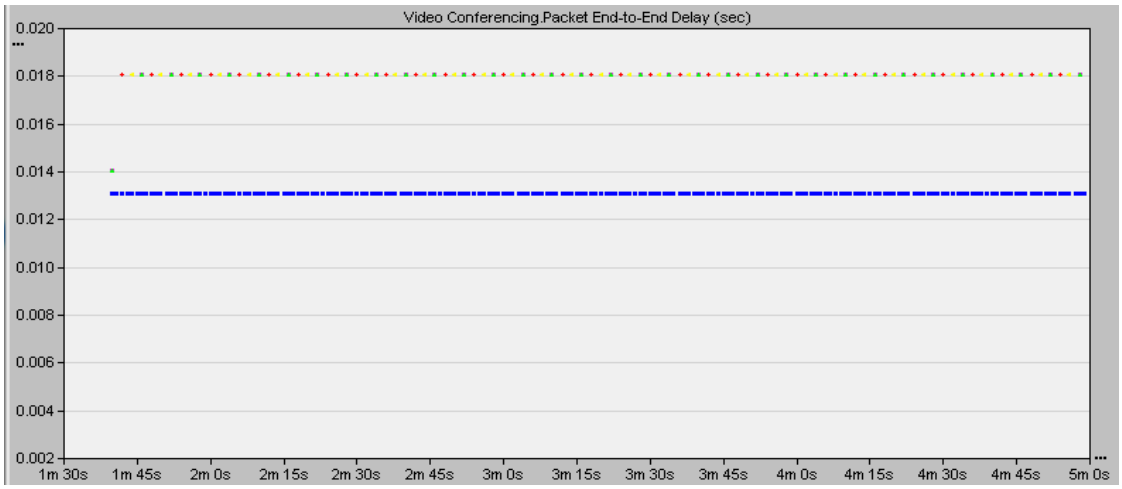

Figure 3.9: Ph-->CN Scenario (23)

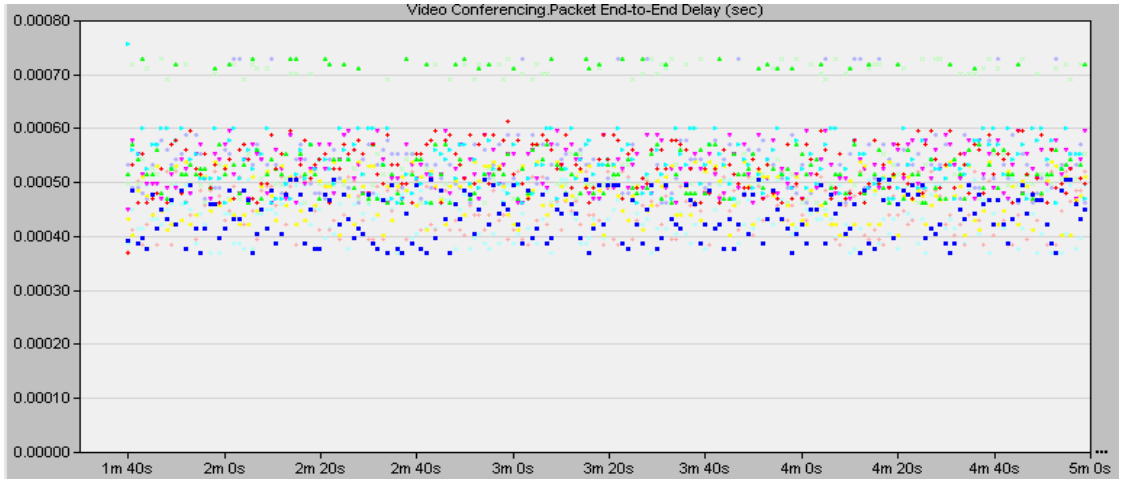

Figure 3.10: B-->CN Scenario (33)

Table 3.7: Loop Delays

	Closed Loop1	Closed Loop2	Open Loop1	Open Loop2
11			15.14ms	656.2µs
12	933.9µs		15.19ms	661.5µs
13	882µs	931µs	15.17ms	673.7µs
21			15.14ms	
22	968.1µs		15.19ms	
23	943.8µs	37.6ms	17.78ms	
31				657.7µs
32		985.1ms		696µs
33		981.1ms		692µs

Figure 3.11 shows the Riverbed Model of the WBAN architecture. As shown on the upward left-most corner is the model for the six sensors and two actuators connected to the smart band. Below is the model for the smartphone. On the right side, there is the access point (AP) connected to the IP Cloud which is also connected to the EPC and the CN. The Evolved Packet Core (EPC) along with the eNodeB fall within the LTE infrastructure.

In order to analyze the impact of latency and packet loss over the Internet on the proposed system, the most congested scenario (13) is simulated with an additional 100ms packet latency and a 1% packet discard ratio [Perez 2015]. Figure 3.12 shows the Riverbed results on several runs with no changes in the Internet parameters and after exerting the changes the communication link between the AP and the CN. Results show an offset of 100ms made on the total end-to-end delay when compared to that with no modified cloud.

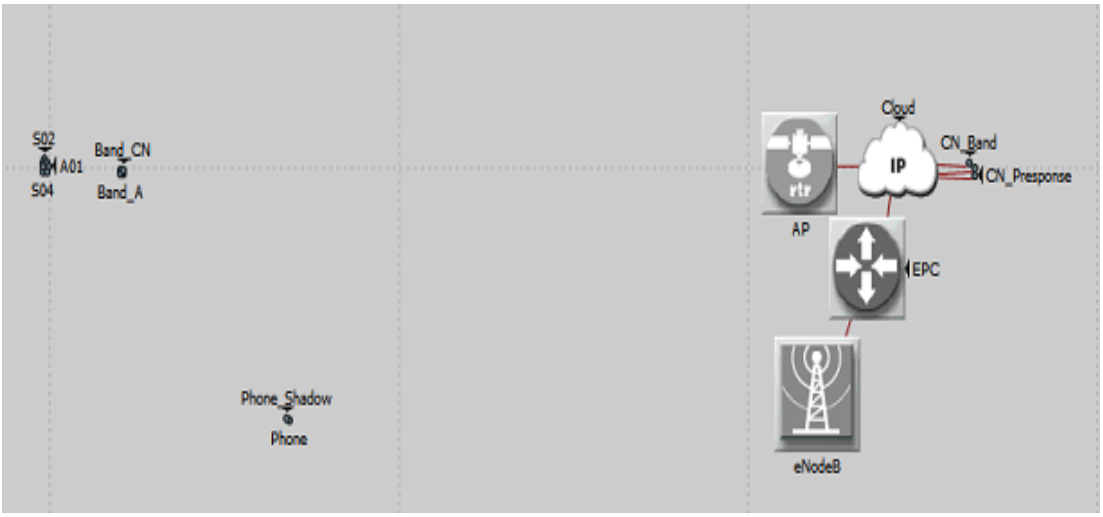

Figure 3.11: Riverbed Model

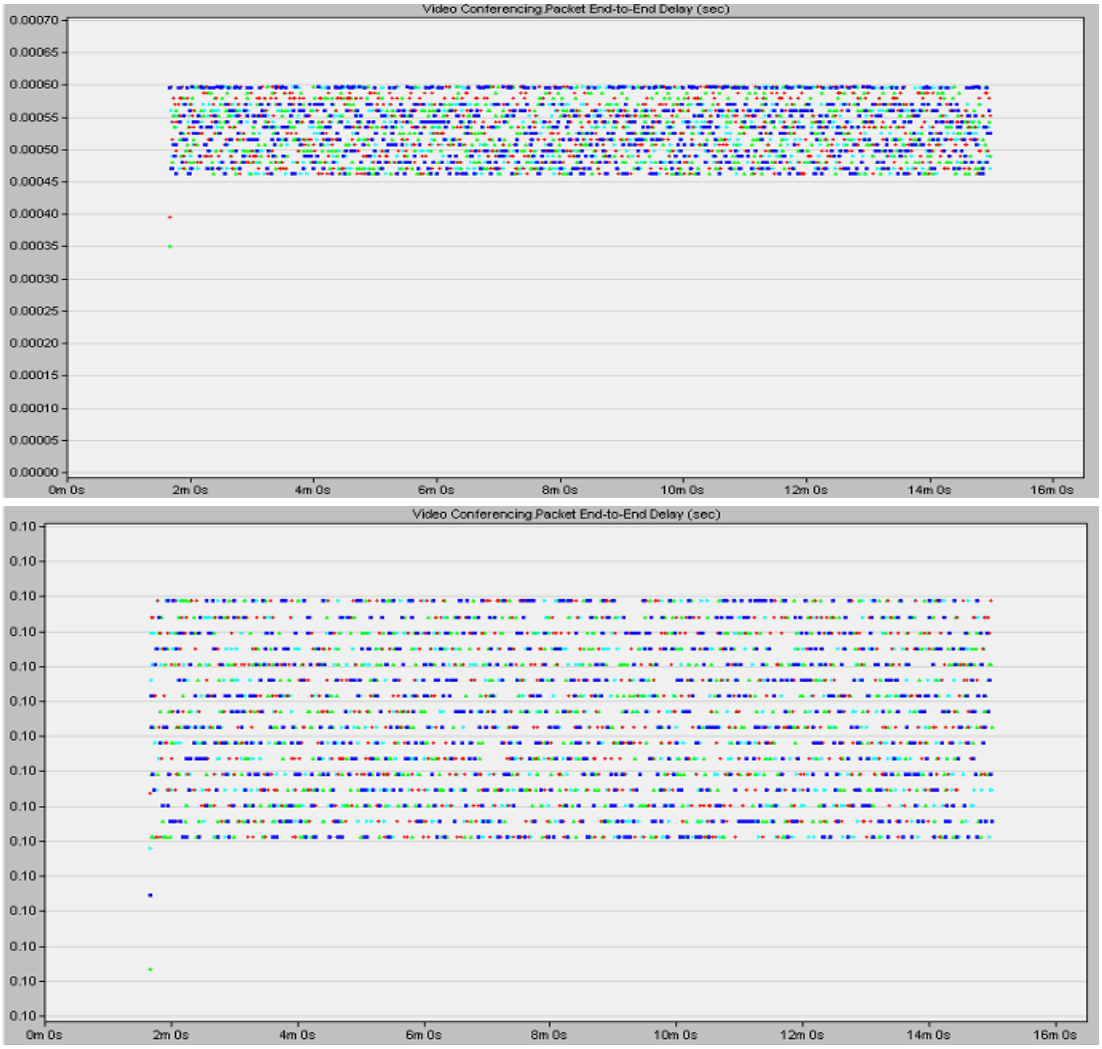

Figure 3.12: End-to-end delay AP–CN without, and with IP Cloud node modifications

3.3.2. Network Congestion

In order to ensure that the system can be prone to interference, network congestion is used [Abdel Reheem 2012, Saleh 2015]. For the Wi-Fi interference model, two interfering nodes are added to each Wi-Fi link with the same frequency channel and are placed perpendicular to the existing link. The two interfering nodes send FTP files. For example, the Wi-Fi link between the sensors and the smart band is on Ch1. Therefore, two interfering nodes, communicating on the same channel (Ch1), are placed perpendicular to the axis of the original link between the sensors and the smart band as shown in Figure 3.13. Therefore, there is four pairs of interferers for the Wi-Fi communication links used (Ch1, Ch6, Ch11, Ch40). Figure 3.14 shows the interference Riverbed model for Ch40.

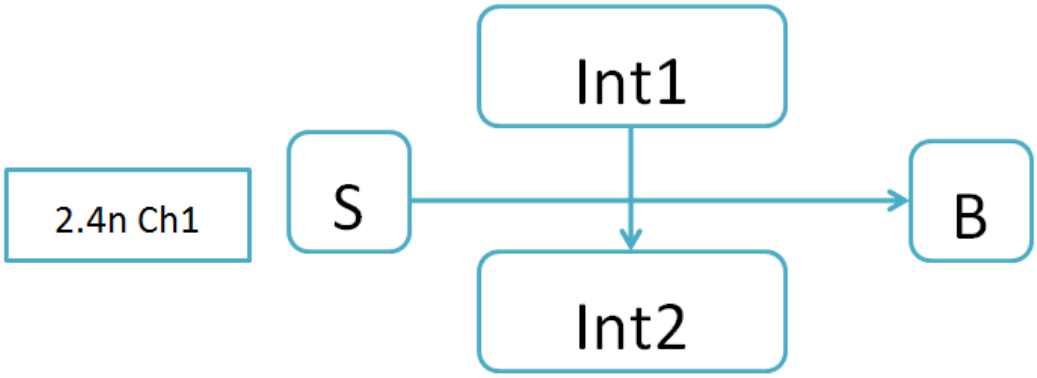

Figure 3.13: Interfere Nodes Placement

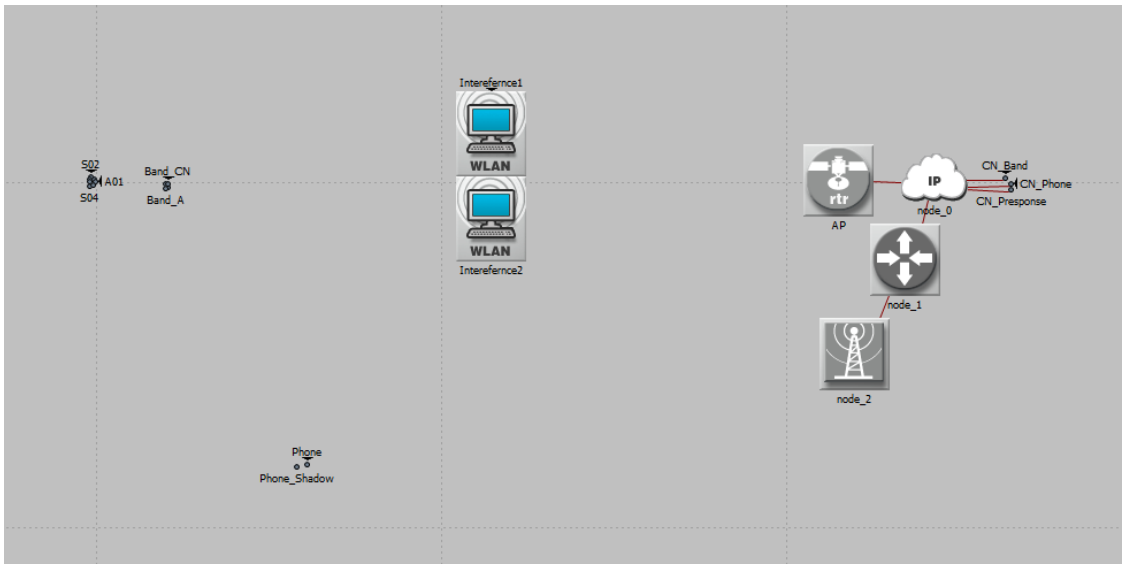

Figure 3.14: Riverbed Model Interferers on Ch40

Table 3.8: Communication Links Interference

Communication Link	*Interferers Maximum Data Rate*
Wi-Fi Ch1	470kBytes/sec
Wi-Fi Ch6	475kBytes/sec
Wi-Fi Ch11	475kBytes/sec
Wi-Fi Ch40	475kBytes/sec
LTE	850kBytes/sec

The simulation results, in Table 3.8, show that the maximum data rate that could be sent on Ch1, without affecting the packet delivery of the data from the sensors to the smart band while slightly increasing the end-to-end delay, is 470kBytes/sec. For Ch6 interference, the maximum data rate is 475kBytes/sec with no packet loss from the smart band to the actuators and a tolerable increase in the end-to-end delay. Similarly for Ch11, the maximum data rate, which could be transmitted by the interfering nodes without affecting the packet delivery with a small increase in the end-to-end delay between the smart band and the smartphone, is 475kBytes/sec. Finally for Ch40, the maximum data rate is 475kBytes/sec without affecting the packet received with a minor change in the end-to-end delay.

As an example for LTE interference model, 10 LTE supported workstations are connected to the same eNodeB where the patient is connected to. The workstations send FTP files to a common Ethernet workstation connected to the cloud. The maximum data rate per each workstation that could be sent without affecting the connection between the patient's smartphone and the CN is 850kBytes/sec.

3.3.3. Two-Patient-Model

Another interference model that is studied on the proposed system is the introduction of another patient with the same sensors, actuators and smartphone, and in close proximity to the main patient (2m away). The new model should ensure that the second patient's data should not interfere with that of the original patient causing loss

of data or increasing the delay to exceed the system requirements. Similarly, the second patient should have reliable system as the original patient. The two patients are connected to the same access point and the data is sent to a common CN as shown in figure 3.15. The channel allocation is unchanged for each communication link. Table.3.9 shows the end-to-end delays for each link while Table 3.10 shows that for each loop definition. From simulation results, there is almost zero packet loss ratio along with a slight increase in the loop delays for each patient; however, delays are still within the system requirements of 1s. Figure 3.16, shows the results of various runs for the Wi-Fi link between the band of each patient and the CN. Figure 3.17 shows the Riverbed model for the two patients.

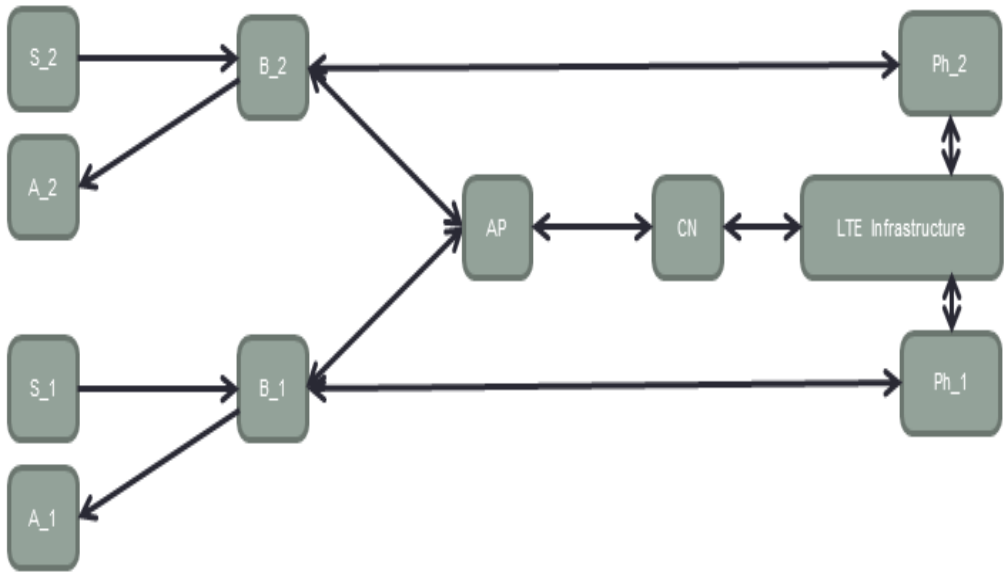

Figure 3.15: Two-Patient Model

Table 2.9: Two-Patient-Model Link Delays

	Patient 1	Patient 2
A1	60.6µs	57.9µs
A2	59.4µs	50.4µs
S-B	115µs	110µs
B-CN	668µs	644µs
B-Ph	635µs	664µs
Ph-CN	13.5ms	13.4ms
Ph-CN(R)	13.1ms	12.9ms
Ph-B(R)	247µs	188µs
CN-B(R)	222µs	196µs

Table 3.10: Two-Patient-Model

	Closed Loop 1	Closed Loop 2	Open Loop 1	Open Loop 2
Patient1	10.57ms	14.57ms	14.25ms	783µs
Patient2	10.16ms	14.40ms	14.18ms	754µs

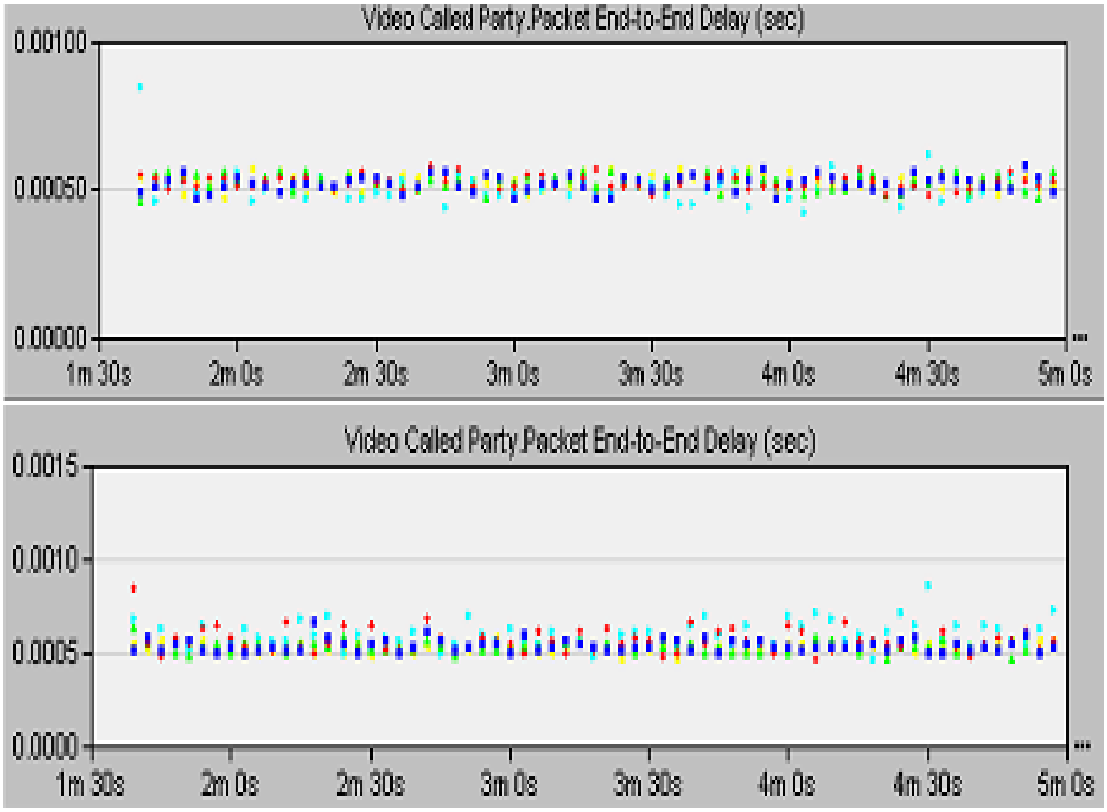

Figure 3.16: Patient1 and Patient2 End-to-end Delay Band-CN

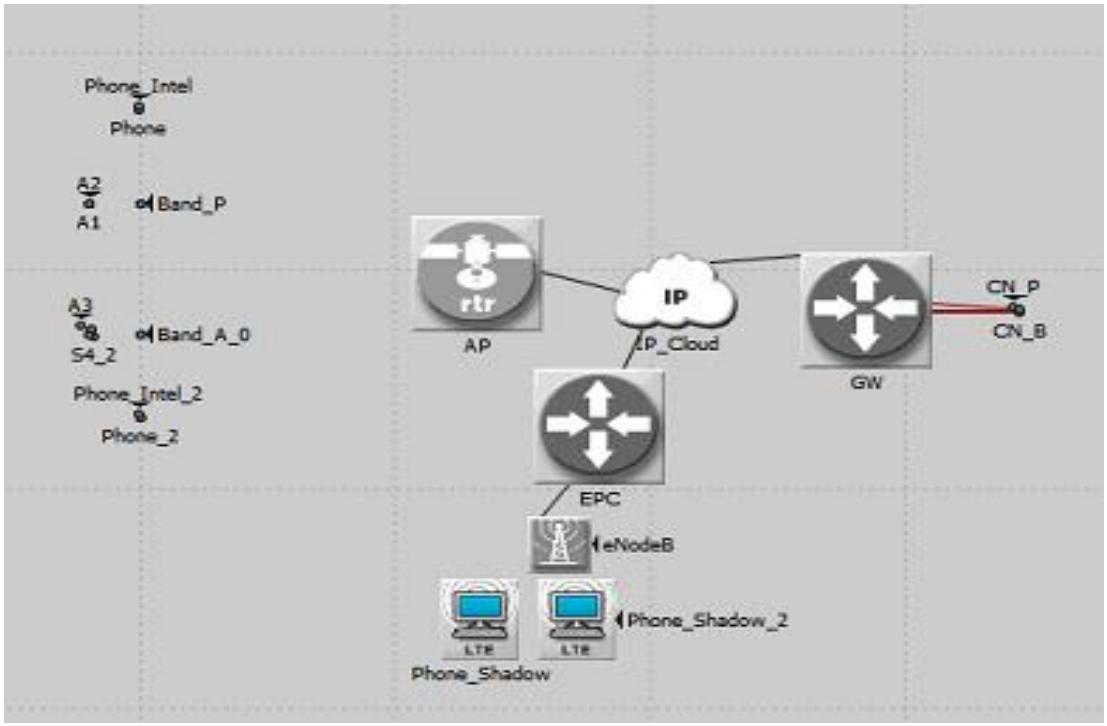

Figure 3.17: Riverbed Model for the two patients

Chapter 4

FPGA-Based Smart band for WBAN

This chapter presents the design architecture of an FPGA-based smart band. In addition, more justification using for FPGAs in this specific WBAN design. Given that the smart band could be viewed as a system's single point of failure, fault tolerance on the smart band level is studied in two working environments. The availability of the smart band is then quantified using Markov modeling. Previously, the application of WBAN was limited to patients' health monitoring. Here, more generic design is proposed to accommodate all types of WBAN applications.

4.1. FPGA-Based Smart Band Motivation

Apart from the various reasons of using FPGAs in general, there are specific justifications to use them in the WBAN system mentioned before. Firstly, during the operation time of the smart band, there might exist a need to change the underlying architecture of the smart-band. For example, the processor could be replaced with another one to allow advanced processing capabilities or reduced power consumption depending on the person's health status and the required measures. In specific, adding new sensors with higher data rates than the original's processor capabilities, or require DSP processing would require the smart band to be changed. Therefore by using FPGAs in smart bands, changing the hardware architecture could be done using Dynamic Partial Reconfiguration (DPR) capability. Hence, this makes the use of FPGAs more convenient in a WBAN system.

Secondly, FPGAs have the ability to reconfigure the hardware if design errors are detected, especially, after the smart band has been activated and used. Thirdly, for power saving purposes, FPGAs enable downloading several modes of operation (sleeping mode, walking mode, running mode) based on the needed mode. The most important feature is that the smart band is operational during any of the reconfiguration processes. Thus, the need for visiting the medical personnel could be potentially re-

duced, such that the visits would include updating or upgrading the smart band or even changing the smart band during its normal lifetime.

Based on the reasons mentioned above, the smart bands, which are originally either MCU-based or ASIC-based are replaced with FPGA-based ones. The FPGA-based smart band design is studied in two working environments; normal environment for health monitoring as patients' or elderly houses, harsh environment as workers dealing with hazardous environments as nuclear power plants, aviation, construction workers, medical personnel working in areas with high radiations (X-ray).

4.2. FPGA-Based Smart Band Components

This section presents the design FPGA-based smart band with respect to the operation of the processor and its allocated memory along with the necessary hardware modules. A wireless network interface is proposed and is used to pull configuration files and perform initial full configuration at power up or Dynamic Partial Reconfiguration (DPR). Fault tolerant techniques on the processor, memory and the modules level are presented in order to mitigate transient faults in the two working environments.

4.2.1. FPGA-Based Smart Band Design

Soft-core processors when compared to hardwired processors provide more design flexibility; therefore, the proposed smart band design consists of a soft-core processor, as MicroBlaze™ from Xilinx [Xillinx 2017, Kale 2016]. The choice of MicroBlaze™ softcore processor is due to the fact that it could be easily implemented in low cost FPGAs [Shanehsazzadeh 2017]. The processor and an assigned memory block are denoted as (PM) module. Modules (M) such as Network Interface controller, General Purpose Input/Output (GPIO) controller, Direct Memory Access (DMA) controller, etc are other hardware auxiliary modules that may be needed.

For instance, depending on the number of connected sensors and their data rates, the DMA controller could become useful. As a result, without the CPU intervention and processing overheads, the smart band could directly transfer data from/to the network controller [Shanehsazzadeh 2017].

Depending on the necessary operation mode of the FPGA based smart band, the appropriate partial configuration file is downloaded using the DPR technique. In [Alkady 2017], a proposed scheme in industrial applications for configuring or updating an FPGA was presented. The scheme utilizes an Ethernet interface and does not require external memory, in addition, it allows for Dynamic Partial Reconfiguration (DPR) and full initial configuration. Based on this scheme, modifications on this design are done to accommodate for the wireless capabilities needed in the smart band design. Figure 4.1, as in [Alkady 2017] shows the Ethernet FPGA scheme.

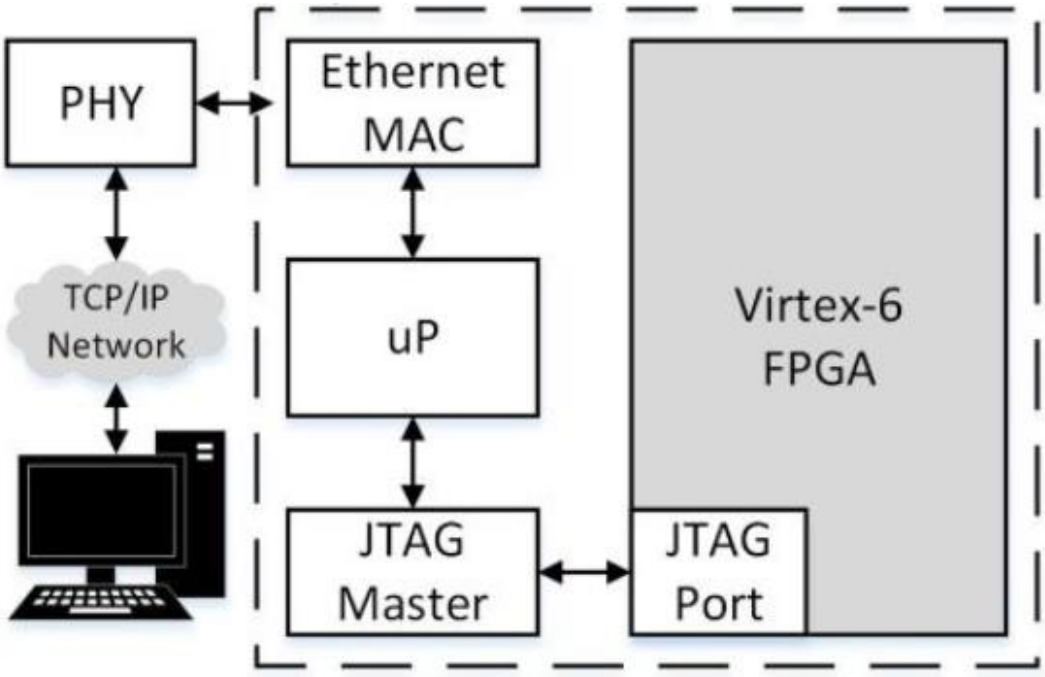

Figure 4.1: Ethernet FPGA Scheme

4.2.2. Wireless Configuration Network Interface (WCNI)

In normal FPGA based systems, external memories are needed to save the configuration files. This is apart from the additional dedicated circuitry needed to provide the connectivity to download these files. Thus, the off-chip components needed to configure the system increase, hence, increasing the area. This is something undesirable or inconvenient in the smart band since size and mobility are main issues.

Another medication is proposed based on the scheme in [Alkady 2017] to enable wireless configuration without external memory to hold the configuration files; thus reducing the area. Similarly, Dynamic Partial Reconfiguration (DPR) and full initial configuration from the network are enabled. DPR is used to perform any of the config-

uration updates on the smart band mentioned earlier, while the full initial configuration is used in the smart band powering up process.

In order to handle configuration processes, the modification employs an FPGA Wireless Configuration Network Interface (WCNI). The WCNI allows pulling the configuration data through the Wi-Fi network which are either stored on the smartphone or on the CN (for example the hospital). Then, in order to allow flexibility in the deployment, the WCNI directly downloads the configuration file to the targeted block. The WCNI, as shown in figure 4.2 [ElSalamouny2 2017], consists of a lightweight WLAN Media Access Controller (MAC), along with to a small hardwired processor and a Joint Test Action Group (JTAG) core. JTAG is usually used for testing and verifying circuits after manufacturing.

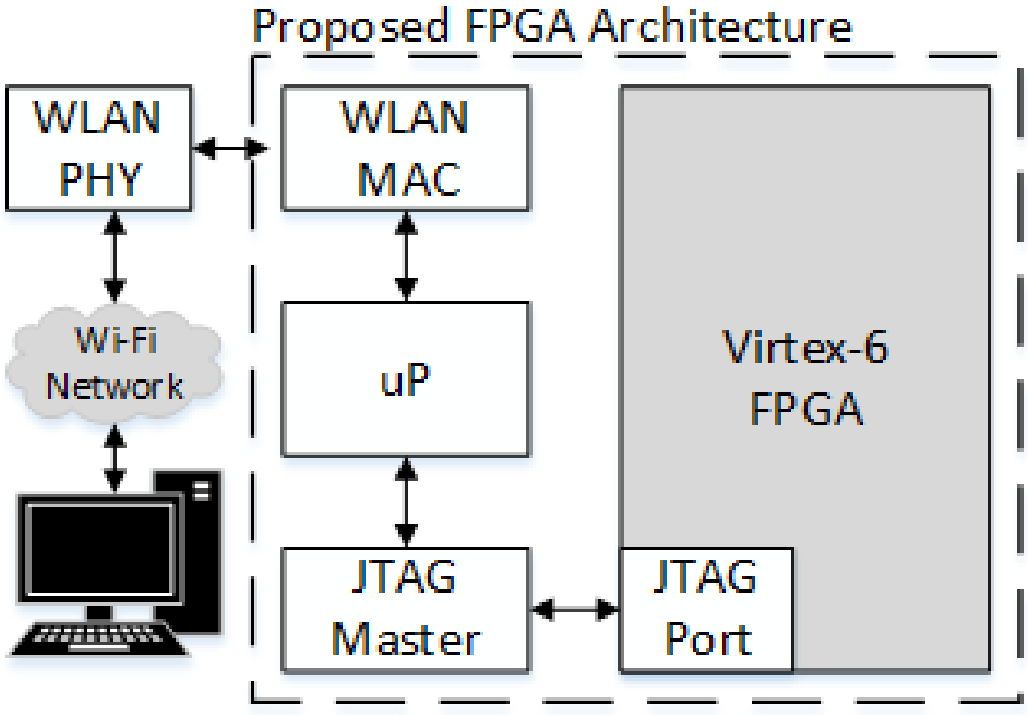

Figure 4.2: Proposed FPGA Architecture (WCNI)

4.2.3. Fault-Tolerant FPGA-Based Smart Band Design

Since the probability of transient faults is higher than that of permanent faults, transient faults are only considered in the FPGA-based smart band. In order to mitigate transient faults, fault tolerant techniques are used depending on the fault model for each working environment. The normal environment is prone to SEUs while the other one is more susceptible to SEUs and MEUs, in specific, Double Event Upsets (AdDEUs)

which affects two adjacent bits simultaneously [ElKady 2017, Terada 2015]. System recovery is done through Dynamic Partial Reconfiguration (DPR) on the processor, and its associated memory or modules though Wireless Configuration Network Interface (WCNI) scheme explained earlier.

In order to improve the availability of the smart band FPGA design, transient faults are overcome using a watchdog signal sent from the softcore processor to the WCNI processor (μP). Moreover, the processor's associated memory is protected by Single Error Correction-Double Error Detection (SEC-DED) technique such that single errors are detected and corrected while double errors are detected only. Therefore, the WCNI processor is triggered and the PM module is partially reconfigured (using DPR) if a transient fault (SEU or AdDEU) occurs. The reconfiguration is done on the same location.

Unlike in [Alkady 2017], where two processors (main and standby) are operational while the main processor is being reconfigured which could decrease the battery life if implemented on the proposed smart band. This assumes that it is acceptable in the FPGA based smart band design that one sample of sensors data is lost since the time to perform DPR is 560ms [Alkady 2017, Kale 2016]. Figure 4.3 shows the FT FPGA-based smart band where µP is the hardwired processor of the WCNI and the modules are in the normal environment while Figure 4.4 shows that in the harsh environment.

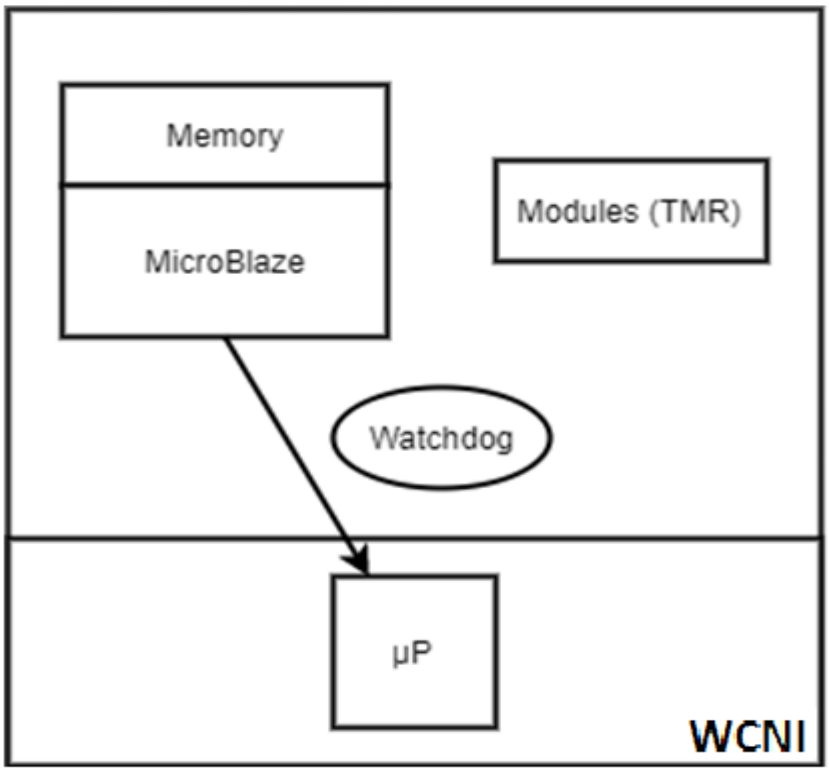

Figure 4.3: FT FPGA-based Smart Band Normal Environment

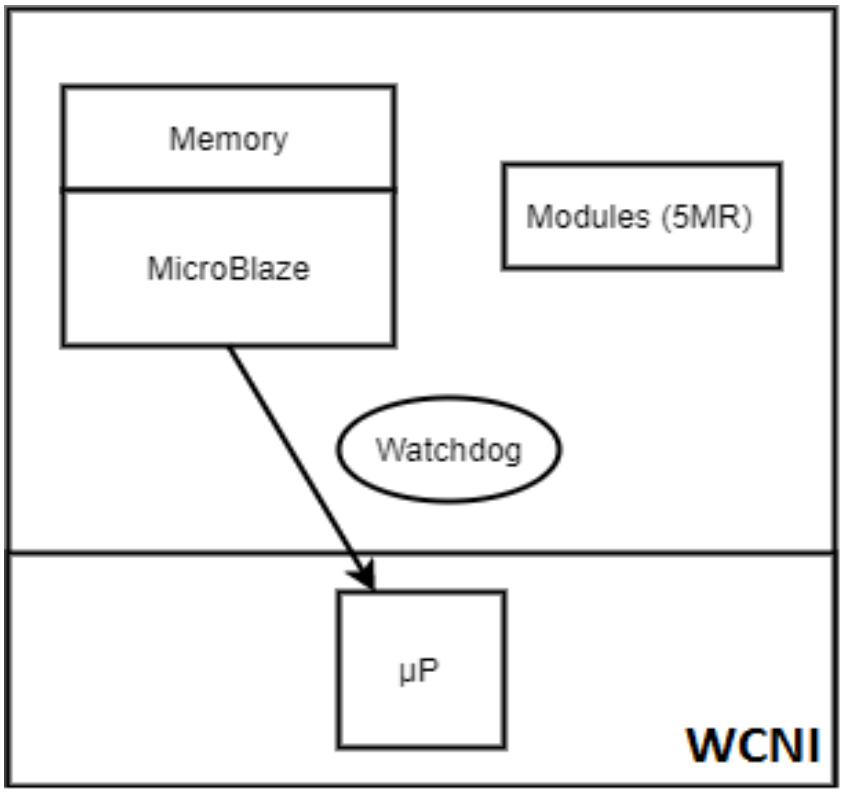

Figure 4.4: FT FPGA-based Smart Band Harsh Environment

Depending on the working environment, the FT design for the hardware modules is done using different FT techniques. Since in the clean environment design, only SEUs are considered. Therefore, the M modules are protected by using Triple Modular Redundancy (TMR). This technique uses three identical of the M modules connected to a majority voter. Since the voter is a single point of failure, it allocated in the WCNI's hardwired processor which is more reliable. Therefore, if one module fails, the other two operating modules cover this error and the correct output is generated. When the modules fail, hence, the system fails. As in [Alkady 2016], TMR reliability is increased by performing DPR to reconfigure the faulty module. This technique is also used in this design.

On the contrary, in the harsh environment module design, the probability of SEUs or AdDEUs is more likely to occur. Thus, the proposed M modules are protected using 5MR. Similar to the TMR, five duplicates of the M modules are connected to an error detection and recovery mechanism. This mechanism is presented in [Lala 1985] and is located in the hardwired processor in the WCNI as that of the TMR voter. The 5MR system can overcome three consecutive single-bit-failures (S) in three M modules. It can also withstand a double failure (D) in two M modules, followed by a single-bit-failure in a third M module [Lala 1985]. As in TMR modules, 5MR modules can operate with a minimum of two modules.

Since the error detection and recovery mechanism is implemented in the hardwired processor of the WCNI, another 5MR scheme can be emerged. In other words, the five outputs from the five identical modules are connected to an advanced voter system implemented inside the hardwired processor.

Depending on the failures occurring, the processor with its special voter changes the number of modules taken for the output. Therefore, this system withstands the same faults tolerated by the previous one. When three consecutive failures occur, the special voter goes from being a majority voter for five modules to being a voter for four then three and then only two modules remain.

For instance, when one module fails, the failed module is discarded by the voter. Then the voting is done on the remaining four modules. When double failure in two modules occurs, these two failed modules are discarded and the voter only considers the remaining operating three. If a single failure is detected followed by a double fail-

ure, at this instance, the system is unable to decide which two modules are faulty and which are not. Therefore, the system fails with this sequence of faults.

In the two 5MR mechanisms, similar to that in TMR technique, when one or more modules fails, DPR is used to recover the faulty module(s). This is while the other remaining operating modules generate the output when possible. Therefore, since the voting mechanism lies in the WCNI hardwired processor as a software, the NMR systems are no more detecting and masking the faults. However, they can detect and exclude the faulty module(s) in addition to recovering them using DPR. Figure 4.5 shows the flow chart of the TMR fault tolerant technique while figure 4.6 shows that for 5MR as in [ElSalamouny2 2017].

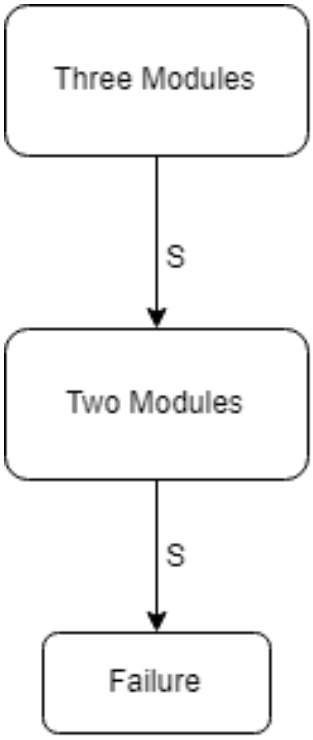

Figure 4.5: TMR Flow Chart

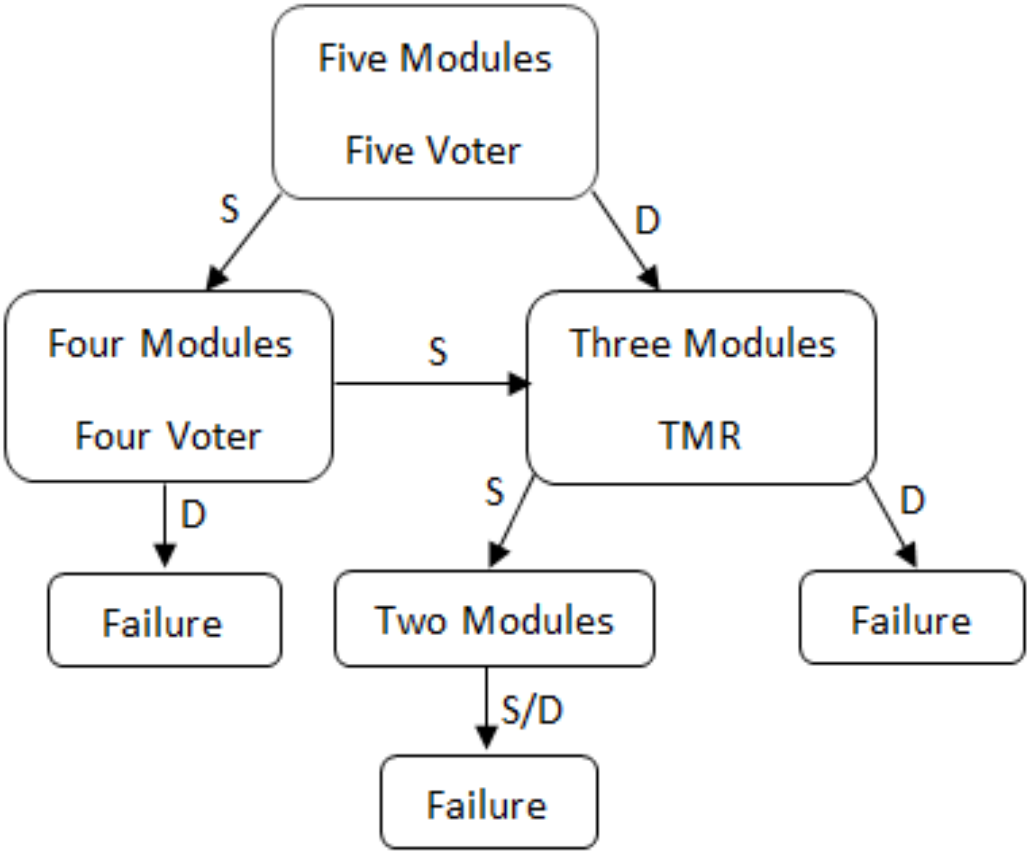

Figure 4.6: 5MR Flow Chart

4.3. System Availability

In order to properly evaluate the FT models proposed in the smart band, the availability of each system is examined and quantified using Markov modeling. The availability of the PM module, the M modules in both clean and harsh environment are shown.

4.3.1 PM Module

As mentioned before regarding the PM module, when an SEU or an AdDEU transient fault is discovered in the processor (P) or a double failure in the processor associated memory block, DPR is performed on the whole (PM) block. The double failure on the memory is only considered because already the memory is protected by SEC-DED. The Markov availability model as shown in Figure 4.7 consists of two states; the (Up) state which represents the operational block while the (Down) state

represents failure in the block. The system changes from the Up state to the Down state with a failure rate of λ_{soft} and λ_{mem_D}. (λ_{soft}) indicates the failure rate of the softcore processor while (λ_{mem_D}) indicates the failure rate of double bit errors in the memory. The recovery rate is denoted by μ which is the reciprocal of the mean time to perform DPR on the same PM block.

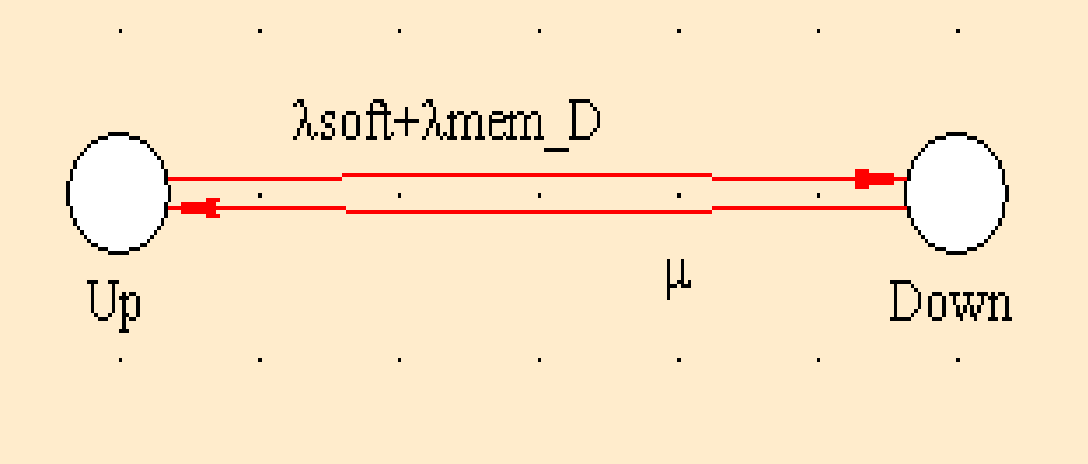

Figure 4.7: PM Module Markov Model

4.3.2. M Modules for the Clean Environment (TMR)

Since only SEUs are considered in the clean environment, the TMR technique relies on having three identical copies of the same module connected to a majority voter circuit. Figure 4.8 shows the Markov model for TMR such that state '3' indicates all modules are functioning while state '2' means only two operational modules in the system. Finally, state 'F' represents the failed state where either one module or no module is functional. Since the modules are identical, if any module fails, it fails with a common failure rate of λ_M and similarly recovers with a rate of μ_{m1} using DPR. μ_{m1} is the recovery rate of one module (M). In other words, in state '3', if any one of the three operational modules fails, the systems goes to state '2' with a failure rate of $3\lambda_M$. The faulty module can be recovered with a recovery rate of μ_{m1} using DPR. Moving to state '2', if another module fails before the first faulty module is completely restored, the system then goes to a system failure state 'F' with a failure rate of $2\lambda_M$. Hence, DPR is performed on all of three modules going to state '3' with a recovery rate of three (M) modules μ_{m3}, where $\mu_{m3} = 1/3\ \mu_{m1}$.

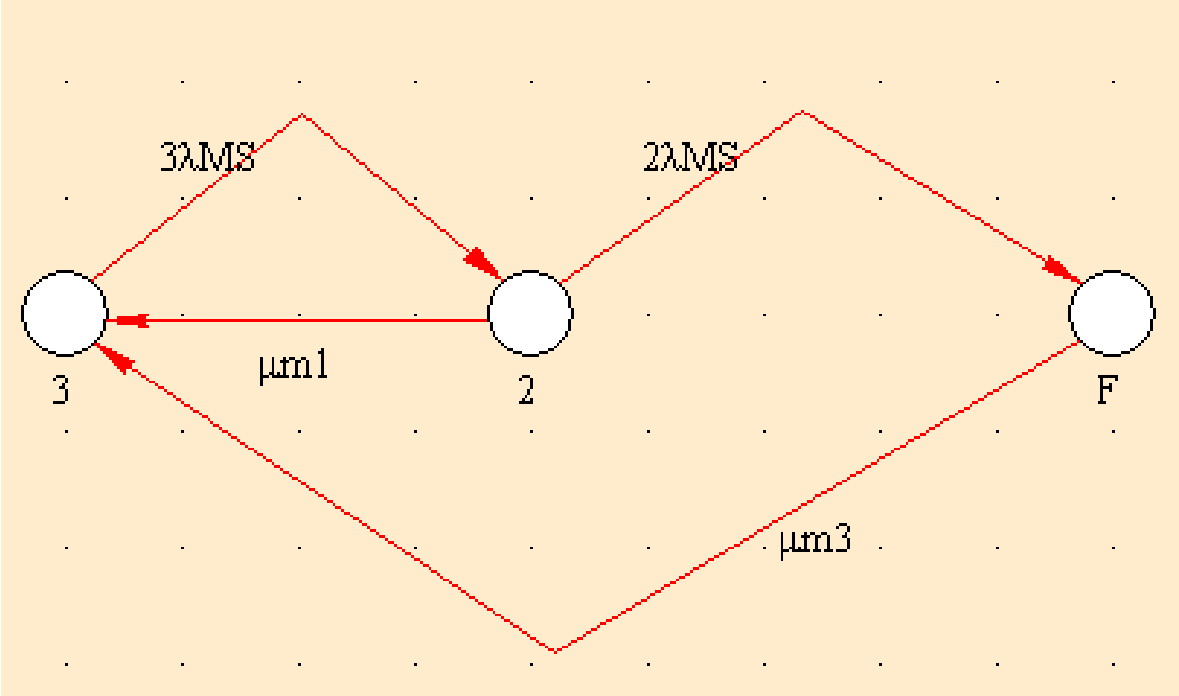

Figure 4.8: M Modules TMR Markov Model

4.3.3. M Modules for The Harsh Environment (5MR Model)

In the harsh environment, both SEUs and AdDEUs are considered. A worst case approach is taken where it is assumed that an AdDEU affects two M modules simultaneously. The Markov model of the 5MR is shown in figure 4.9. The digit number at each state denotes the number of operating modules. The system's failure state 'F' represents the system's inability to produce the correct decision or is giving an undesired output. As mentioned before, 5MR technique on the modules can properly function with a minimum of two operating modules. State '5' represents the whole five modules that are functioning. When a single failure occurs in any of the modules, the system moves to state '4' with a failure rate of $\binom{5}{1}\lambda_{MS}$ for all modules. On the other hand, if an AdDEU occurs in any combination of two modules, the system moves to state '3' where three modules are operating with a rate of $\binom{5}{2}\lambda_{MD}$.

In state '4' with four operational modules, if an SEU occurs in any of the modules, the system goes to state '3' with a failure rate of $\binom{4}{1}\lambda_{MS}$. It can also go directly to state 'F' with a failure rate of $\binom{4}{2}\lambda_{MD}$. Using DPR on the single faulty module, the system moves back to state '5' and the module is recovered with a repair rate μ_{m1}.

Moving to state '3', if a single module fails with a rate of $\binom{3}{1}\lambda_{MS}$, the system moves to state '2'. On the other hand, if AdDEU in any two of the three operational modules, this takes the system to the failure state 'F' with a failure rate of $\binom{3}{2}\lambda_{MD}$. In this same manner, in state '3', the non-operational modules are recovered using DPR with a repair rate of μ_{m2}, where $\mu_{m2} = 1/2\ \mu_{m1}$.

There are two options to go from state '2' to the failure state 'F'. The first is through the failure of two modules with a rate of $\binom{2}{1}\lambda_{MS}$ while the second is through double failure in one module with a rate of $\binom{2}{2}\lambda_{MD}$. In this state, the three faulty modules are repaired with a rate of $\mu_{m3} = 1/3\ \mu_{m1}$. Finally, in state 'F', all of the five modules are recovered with a rate of $\mu_{m5} = 1/5\ \mu_{m1}$.

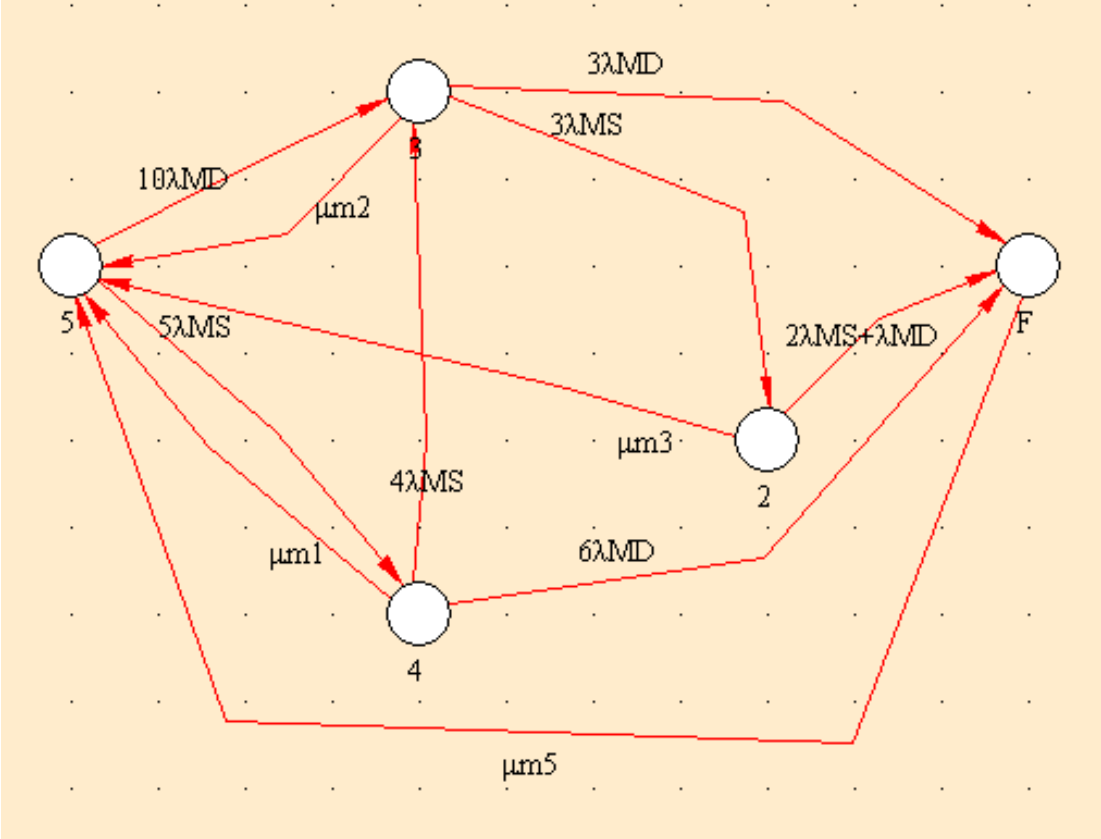

Figure 4.9: M Modules 5MR Markov Model

4.3.3. System Availability

By definition, availability is the probability that the system is working given a period of operation. System availability in Markov chains is calculated by finding the probabilities of the UP states, i.e. the system is functioning, and that of the DOWN states, where the system has failed. In TMR, states '3' and '2' are the UP states while state 'F' is the DOWN state. Similarly as in 5MR, the states '5', '4', '3', and '2' are the UP states while state 'F' is the DOWN state. At any instant of time, each state in the system has its unique probability as a function of time. For simplicity, the equations that govern the system's availability of PM Markov model are shown below [Bauer 2011]. The Failure rate (λ) is known as the reciprocal of the Mean Time Between Failures (MTBF), while the recovery rate (μ) represents the Mean Time To Repair [Bauer 2011]. For a system's steady state behavior over a long run, it is expected that the rates of entering and leaving states are equal; hence, this explains equation (2).

$$P(Up) + P(Down) = 1 \qquad (1)$$

$$P(Up) \times \lambda - P(Down) \times \mu = 0 \qquad (2)$$

$$P(Up) = \frac{\mu}{\lambda + \mu} \qquad (3)$$

$$\text{Availability} = \frac{MTBF}{MTTR + MTBF} \qquad (4)$$

In repairable systems, steady state availability is a better measure of the performance of the system [Sherwin 2000] which is very convenient measure in the proposed FPGA based smart band. It is worth mentioning that it irrelevant to compare the performance of TMR to that of 5MR because each technique targets different fault models in its corresponding environment. According to [Terada 2017], if TMR tech-

nique in FPGAs is applied in harsh environments as in nuclear power plants, the system's performance is going to be lower than that using 5MR.

4.4. Case Study

All of the presented Markov models have been simulated using modeling software named SHARPE [SHARPE 2017] with respect to the steady state availability. SHARPE stands for Symbolic Hierarchical Automated Reliability and Performance Evaluator, developed by Duke University. It is mainly used for modeling and analyzing stochastics models with respect to reliability, availability, performability and performance.

The probability of the fault being a single error is taken to be 0.7 as in [Alkady 2017]. Regarding the PM availability model, the failure rate of the softcore processor λ_{soft} is taken from the litrature to be 0.432/year while the failure rate of the memory λ_{mem_D} is equivalent to 0.0432/hour [Alkady 2017, Kastil 2012]. The recovery rate μ of the PM module is 6428/hour which includes the time of DPR of the PM module the network delay [Alkady 2017]. The steady state availability of this system is 99.99% as shown in the SHARPE results below figure 4.10.

```
********************************************************************************
********* Outputs asked for the model: Malak **************
Input parameters values: lam= 324.144, mu=4628571
Output:
Steady_State Availability for Malak
SS_Avail:   9.99929974e-001

----------------------------------------
```

Figure 4.10: PM Steady State Availability

Regarding the TMR, and according to the failure rate for the M modules shown in [Alkady 2017], $\lambda_M = \lambda_{mem\_S} = 0.1008$/hour while the repair rate for M module μ_{m1} is 53731/hour. This number is taken for a mean time to repair of 100ms. As shown in figure 4.11, the steady state availability of the M modules in TMR is 100%. When in-

creasing the failure rate to λ_M= 2/hour, the steady state availability decreased to 99.99999% as shown in figure 4.12.

```
********************************************************************************
********* Outputs asked for the model: Malak **************
Input parameters values: lam= 0.144, mu1=26865, mu=53731
Output:
Steady_State Availability for Malak
SS_Avail:   1.00000000e+000

----------------------------------------
```

Figure 4.11: TMR Case 1 with λ_M = 0.144

```
********************************************************************************
********* Outputs asked for the model: Malak **************
Input parameters values: lam= 2, mu1=26865, mu=53731
Output:
Steady_State Availability for Malak
SS_Avail:   9.99999983e-001

----------------------------------------
```

Figure 4.12: TMR Case 2 with λ_M = 2

Finally for the availability results of the 5MR model and using the values in TMR and $\lambda_{MS} = \lambda_M = \lambda_{mem\_S}$ and $\lambda_{MD} = \lambda_{mem\_D}$, the steady state availability is 100% as shown in figure 4.13. By increasing the M module failure rate λ_{MS} = 2/hour, the steady state availability becomes 99.9999% as shown in figure 4.14. This indicates the high performance of the system in their corresponding fault models.

```
********************************************************************************
********* Outputs asked for the model: Malak **************
Input parameters values: lam_D= 0.0432, mu2=26865, lam_S=0.1008, mu=53731, mu3=17910, mu5=10746
Output:
Steady_State Availability for Malak
SS_Avail:   1.00000000e+000

----------------------------------------
```

Figure 4.13: 5MR Case 1 with λ_{MD} = 0.0432

```
**************************************************************************
********* Outputs asked for the model: Malak **************
Input parameters values: lam_D= 0.857, mu2=26865, lam_S=2, mu=53731, mu3=17910, mu5=10746
Output:
Steady_State Availability for Malak
SS_Avail:   9.99999835e-001

-----------------------------------------
```

Figure 4.14: 5MR Case 2 with λ_{MD} = 0.875

Conclusion and Future Work

In conclusion, there is no doubt that WBANs could increase the efficiency of the healthcare systems. This thesis presented a novel fault tolerant WBAN architecture in the communication links. The system used two main protocols; low-power 802.11n and LTE. The choice of non-overlapping channel ensures no channel interference in such critical application. The system has been tested with in different scenarios depending on the availability of the functioning nodes and the severity of the sensory data. Simulation results from Riverbed 18.0.3 have shown acceptable results in terms of the packet loss ratio and the end-to-end delay calculated in four different network control loops; two closed loops are for actuation purposes while the other two open loops are for monitoring. Aiming to achieve IoT, the model was subjected to an IP cloud model.

Finally, in order to study the effect of interference on the system, two inference models were introduced and tested. The first one is regarding the network congestion, where each link is congested with the maximum FTP data rate that a channel could support and the effect on the model's link was studied. This is done for the Wi-Fi and the LTE links. On the other hand, the second interference model applied to the proposed system is simply the addition of another patient with the same physical hardware attached in a close proximity to the main patient. Simulation results in the two interference models show expected acceptable output. This indicates that this model is a good working system for WBAN susceptible to interference due to interfering nodes on the same channels or simply with another nearby patient. In order to enhance this model, the study of cloud could be further investigated such that some pre-processing could be done on the gateways to avoid the overflow of data in the Internet, in addition to securing the patients sensors data.

Regarding the FPGA-based smart band design, it was intended to work on aggregator for wireless sensors data to be further sent to other nodes for processing. The use of FPGA in the smart band would allow changing the underlying architecture of the FPGA in case extra processing is needed during the smart band's operation. A very good example is simply the need to add sensors as EEG and ECG that would require extra DSP processing. Additionally, FPGA could be used if design errors were detected. Therefore, software/hardware reconfiguration could be done while the smart band is

operational. The FPGA-based smart band architecture consisted of a softcore processor and its memory block, along with some auxiliary modules. A novel scheme for wireless configuration network was presented in order to enable the FPGA based system to be reconfigured through the WLAN connection without increasing the off chip components.

When using FPGAs, transient faults could be eliminated using fault tolerant measures. Therefore, the processor was protected using a watchdog sent to the hardwired processor in the WCNI while the memory was protected with SEC-DED technique. DPR is performed on the same PM block, if a transient fault occurred in the processor or a double bit error in memory. This would lead to a loss of one sample; however, this could be tolerable. The system has been designed for two working environments. Accordingly, fault tolerant techniques on the M modules are done using TMR for the normal environment and 5MR for the harsh environment. Depending on the fault model of each environment, it followed that the normal environment is susceptible to SEUs while the harsh one is more prone to SEUs and MEUs.

The steady state availability of the system has been analyzed using Markov modeling. SHARPE has been used to model the Markov availability models for the watchdog protected processor, TMR and 5MR. From the results, the least available system had a steady state availability of 99.99%. Therefore, this showed the high availability of the whole FPGA based smart band system. For future enhancement of this FPGA-based smart band, more faults model could be taken into consideration as permanent faults.

References

[Abdel Reheem 2012] E.E. Abdel Reheem, Y.I. El Faramawy, H.H. Halawa, M.A. Ibrahimm A. Elhamy, T.K. Refaat, R.M. Daoud, H.H. Amer, "On the effect of interference on Wi-Fi-based Wireless Networked Control Systems," Proceedings of IEEE IET 8th International Symposium on Communication Systems, Networks and Digital Signal Processing CSNDSP, Poznan, Poland, July 2012, pp. 1-4.

[Adly 2016] M.A. Adly, A.A. Adly "Steady state analysis of a human motion electromechanical energy harvester," 28th International Conference on Microelectronics (ICM), Giza, Egypt, December 2016, pp. 281-284.

[Alkady 2015] G.I. Alkady, N.A. El-Araby, M.B. Abdelhalim, H.H. Amer and A.H. Madian, "Dynamic fault recovery using partial reconfiguration for highly reliable FPGAs," 4th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, August 2015, pp. 56-59.

[Alkady 2016] G.I. Alkady, A. AbdelKader, R.M. Daoud, H.H. Amer, N.A. El-Araby and M.B. Abdelhalim, "Integration of Multiple Fault-Tolerant techniques for FPGA-based NCS Nodes," 11th International Conference on Computer Engineering & Systems (ICCES), Cairo, Egypt, 2016, pp. 299-304.

[Alkady 2017] G.I. Alkady, R.M. Daoud, H.H. Amer, I. Adly, H.H. Halawa, M.B. Abdelhalim, "Highly Reliable Controller Implementation Using a Network-Based Fully Reconfigurable FPGA for Industrial Applications," Accepted for publication. IEEE 22nd International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus, September, 2017, 4 pages.

[Baig 2012] H. Baig and J.A. Lee, “An Island-style-routing compatible fault-tolerant FPGA architecture with self-repairing capabilities”, International Conference on Field-Programmable Technology (FPT), Seoul, South Korea, December 2012, pp. 301-304.

[Barakah 2012] D.M. Barakah and M. Ammad-uddin, "A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of a Virtual Doctor Server in Existing Architecture," Third International Conference on Intelligent Systems Modelling and Simulation, Kota Kinabalu, March 2012, pp. 214-219.

[Bauer 2011] E. Bauer, R. Adams, D. Eustace, Beyond Redundancy: How Geographic Redundancy Can Improve Service Availability and Reliability of Computer-Based Systems, Wiley Online Library, October 2011, pp. 292-295.

[Brown 1996] S. Brown and J. Rose, “FPGA and CPLD Architectures: A tutorial”,1996.

[Deylami 2014] M.N. Deylami and E. Jovanov, "A Distributed Scheme to Manage The Dynamic Coexistence of IEEE 802.15.4-Based Health-Monitoring WBANs," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 1, January 2014, pp. 327-334.

[ElSalamouny1 2017] M.Y. ElSalamouny, H.H. Halawa, R.M. Daoud, H.H. Amer, "Performance of Fault Tolerant WBAN for Healthcare," 3rd International Conference on Engineering & MIS (ICEMIS), Monastir, Tunisia, May 2017, 4 pages.

[ElSalamouny2 2017] M.Y. ElSalamouny, G.I. Alkady, I. Adly, R.M. Daoud, H.H. Amer, H. ElSayed, D.G. Mahmoud, H.A. Ismail, H.H. Halawa, "Highly Available FPGA-Based Smart Band for WBAN" 12th International Conference on Computer Engineering & Systems (ICCES), Cairo, Egypt, December 2017, 6 pages.

[Fong 2015] J. Fong and K. Takahata, "Implantable Drug Delivery Chips Enabled by Radio-Controlled Smart Microactuators". [Online] Recent Trends in Targeted Drug Delivery | www.smgebooks.com. [Accessed on 12 March 2017]

[Gauer 2010] C. Gauer, B.J. LaMeres, D. Racek, "Spatial avoidance of hardware faults using FPGA partial reconfiguration of tile-based soft processors," IEEE Aerospace Conference, Big Sky, MT, USA, April 2010, pp. 1-11.

[Gusev 2017] M. Gusev and A. Guseva, "State-of-the-art of cloud solutions based on ECG sensors," IEEE 17th International Conference on Smart Technologies (EUROCON), Ohrid, Macedonia, August 2017, pp. 501-506.

[Hughes 2012] L. Hughes, X. Wang, T. Chen, "A Review of Protocol Implementations and Energy Efficient Cross-Layer Design for Wireless Body Area Networks," Sensors, Basel, Switzerland, vol. 12, no. 11, November 2012, pp. 14730-14773.

[Huynh 2016] D.T. Huynh and M. Chen, "An energy efficiency solution for WBAN in healthcare monitoring system," 3rd International Conference on Systems and Informatics (ICSAI), Shanghai, China, November 2016, pp. 685-690.

[Kale 2016] V. Kale, "Using the MicroBlaze Processor to Accelerate Cost-Sensitive Embedded System Development," White Paper: MicroBlaze™ Embedded Processor, WP469 (v1.0.1) June 6, 2016.

[Kraemer 2017] F.A. Kraemer, A.E. Braten, N. Tamkittikhum, D. Palma, "Fog computing in healthcare: a review and discussion," IEEE Access, vol. 5, May 2017, pp. 9206-. 9222.

[Kastil 2012] J. Kastil, M. Straka, L. Miculka, Z. Kotasek, "Dependability Analysis of Fault Tolerant Systems Based on Partial Dynamic Reconfiguration Implemented into FPGA," Proceedings of the 15th Euromicro Conference on Digital System Design, Izmir, Turkey, September 2012, pp. 250-257.

[Khan 2008] J.Y. Khan, M.R. Yuce, F. Karami, "Performance evaluation of a Wireless Body Area sensor network for remote patient monitoring," 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Vancouver, BC, Canada. October 2008, pp. 1266-1269.

[Khan 2016] A.U. Khan, A. Rahman, N. Khan , "Optimum placement of gateway node on human body for real-time healthcare monitoring using WBAN," Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, Ireland, August 2016, pp. 408-412.

[Lala 1985] P.K. Lala, "Fault Tolerant & Fault Testable Hardware Design", Prentice Hall, 1985.

[Latre´ 2011] B. Latre´, B. Braem, I. Moerman, C. Blondia, P. Demeester, "A survey on wireless body area networks," Springer Science+Business Media, LLC 2010, vol. 17, no. 1, Januray 2011, pp. 1-18.

[Maricau 2013] E. Maricau and G. Gielen, Analog IC Reliability in Nanometer CMOS, Analog Circuits and Signal Processing, Springer Science+Business Media New York 2013.

[Mills 2016] A. Mills, P.H. Jones, J. Zambreno, "Parameterizable FPGA-based Kalman Filter Coprocessor Using Piecewise Affine Modeling", IEEE International Parallel and Distributed Processing Symposium Workshops, Chicago, IL, USA, August 2016.

[Perez 2015] U.A. Perez. "Low Power WiFi: A study on power consumption for Internet of Things". Thesis by Facultat d'Informatca de Barcelone and Barcelona Tech., February 2015.

[Rotariu 2012] C. Rotariu, V. Manta, H. Costin, "Wireless remote monitoring system for patients with cardiac pacemakers," International Conference and Exposition on Electrical and Power Engineering, Iasi, Romania, October 2012, pp. 845-848.

[Riverbed 2017] 'Riverbed Official Website for Riverbed Modeler'. [Online]. Available: https://www.riverbed.com/ [Accessed 11 March 2017].

[Saleh 2015] A. Saleh, F. Negm, N. Said, Y. Sudan, H.H. Halawa, R.M. Daoud, H.H. Amer, H. ElSayed, T.K. Refaat, "A Wireless Body Area Network architecture for a prosthetic arm," 7th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Brno, Czech Republic, October 2015, pp. 275-280.

[Savani 2011] V.G Savani, A.I. Mecwan, N.P. Gajjar, "Dynamic Partial Reconfiguration of FPGA for SEU Mitigation and Area Efficiency," International Journal of Advancements in Technology, Vol 2, No 2. April 2011, pp 285-291.

[See 2012] T.S.P. See, C.W. Kim, T.M. Chiam, Y. Ge, A.A.P. Wai, Z.N. Chen, "Study of dynamic on-body link reliability for WBAN systems," IEEE Asia-Pacific Conference on Antennas and Propagation, Singapore, Singapore, October 2012, pp. 112-113.

[Sethi 2012] A.S. Sethi and V.Y. Hnatyshin, “The Practical OPNET User Guide for Computer Network Simulation,” Boca Raton: CRC Press, August 2013.

[SHARPE 2017] Official site for SHARPE: http://sharpe.pratt.duke.edu/[Accessed 28 August 2017]

[Shanehsazzadeh 2017] F. Shanehsazzadeh and M. S. Sadri, "Area and performance evaluation of central DMA controller in Xilinx embedded FPGA designs," Iranian Conference on Electrical Engineering (ICEE), Tehran, Iran, July 2017, pp. 546-550.

[Sherwin 2000] D. J. Sherwin, "Steady-state desires availability," IEEE Transactions on Reliability, vol. 49, no. 2, June, 2000, pp. 131-132.

[Terada 2017] R. Terada and M. Watanabe, "Error injection analysis for triple modular and penta-modular redundancies," 6th International Symposium on Next Generation Electronics (ISNE), Keelung, Taiwan, July 2017, pp. 1-4.

[Wi-Fi Alliance® 2016] ‘Wi-Fi Alliance® introduces low power, long range Wi-Fi HaLow’. [Online]. Available: http://www.wi-fi.org/. [Accessed: 11 March 2017]

[Xilinx Medical] Xilinx, “Smarter Vision: Intelligence for Smarter Medical Systems,” Available: https://www.xilinx.com/applications/medical.html/. [Accessed: 5 December 2017]

[Xilinx 2013] Xilinx, “Xilinx Partial Reconfiguration user guide”, UG702, April 2013.

[Xilinx 2015] Xilinx, “Virtex-6 FPGA Configuration,” UG360, November 2015.

[Youssef 2015] S.B.H. Youssef, S. Rekhis, N. Boudriga, "Design and analysis of a WBAN-based system for firefighters," International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Coratia, October 2015, pp. 526-531.