



A Secure and Efficient Communication Framework for Software-Defined Wireless Body Area Network

by

Khalid Hasan

B.Eng., M.Sc.

School of Information and Communication Technology

Griffith University, Gold Coast, Australia

Submitted in fulfilment of the requirements of the degree of

Doctor of Philosophy

March 2020

ABSTRACT

Due to the recent development and advancement of communication technologies, healthcare industries are becoming more attracted towards information and communication technology services. One of the interesting services is the remote monitoring of patients through the use of a wireless body area network (WBAN), which enables healthcare providers to monitor, diagnose and prescribe patients without being present physically. To develop reliable and flexible remote patient monitoring services, in this thesis, the current state-of-the art of WBAN and the limitations of current WBAN technologies are investigated in the healthcare domain. To this end, the relevant background, implementation challenges and limitations of WBAN are overviewed. The in-depth literature survey identifies the lack of a current WBAN architecture in terms of administrative control, static architecture, vendor dependency, traffic priority arrangements, resource utilization, secure data sharing etc. To find a solution to the limitations of WBAN, software-defined networking (SDN) is considered to be one of the promising solutions in this paradigm. However, the incorporation of SDN into WBAN has several challenges in terms of architectural framework, resource optimization and secure data sharing.

In this thesis, an SDN-based WBAN (SDWBAN) architecture is proposed to incorporate the functionalities and principles of SDN on top of the traditional WBAN architecture to overcome the existing barriers of WBAN. The proposed communication model of the SDWBAN framework utilizes the sector-based distance (SBD) routing protocol for data packet dissemination. Furthermore, an application classification algorithm is developed to prioritize emergency applications over normal applications. The proposed architecture and communication model have been simulated and experiments are conducted in Castalia 3.2. The simulation outcome demonstrates enhanced performance in terms of the packet delivery rate (PDR) and the latency of the emergency applications in comparison to normal applications.

For resource optimization, a mathematical model is developed to optimize the design of the control plane in the proposed SDWBAN framework. The purpose of the model is

to reduce the unnecessary wastage of resources and find an optimal relationship among the number of controllers, SDN-enabled switches (SDESWs) and body sensors (BSs) which can potentially maximize network performance. The key factors in the proposed mathematical model encompass the number of controllers, flow resolution time and number of SDESWs and BSs. The specific number of controllers returned by the model is used in the proposed SDWBAN and experiments are conducted in Castalia 3.2. The simulation results reveal that the optimal number of controllers returned by our model produces an acceptable range of PDR and latency.

Finally, a secure data-sharing platform is proposed for our SDWBAN framework. The platform is developed based on the cutting-edge blockchain technology and considers multiple entities such as healthcare professionals from various clinics, medical researchers and health insurers etc. The platform is implemented with a proof-of-concept (PoC) smart contract in Ethereum private blockchain using the Solidity programming language. The platform is validated in terms of time to execute functions in a data-sharing contract (DS-Contract) and hash-contract, the time to receive data packets from the gateway and the transaction time to run the smart contract. A low overhead is observed in the experiment which justifies the suitability of the platform to be used as a secure data-sharing platform for SDWBAN.

STATEMENT OF ORIGINALITY

This work has not previously been submitted for a degree or diploma in any university. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

A handwritten signature in black ink, appearing to read 'Khalid Hasan', with a stylized, sweeping flourish at the end.

Khalid Hasan

March, 2020

ACKNOWLEDGMENTS

All praise be to almighty Allah for giving me strength and patience to complete this thesis. I would like to express my sincere gratitude to my supervisor Dr Md. Saiful Islam, Dr Kamanashis Biswas and Dr Khandakar Ahmed for their constant support and guidance throughout this PhD. I am highly grateful to Dr Khandakar and Dr Kamanashis for their continual guidance and supervision that led to the completion of this thesis work. I would like to express my gratitude to my previous supervisor Dr Xin-Wen Wu for his encouragement and support.

I am grateful to Griffith University for providing a scholarship to cover my tuition fees and living expenses. I also must mention the support and motivation I received from my friends and colleagues throughout this PhD journey. I would like to especially thank Ujjwal, Mahamudul, Ismail, Shamol, Shikha, Nafi, Gul Zameen and Dr Javed for their continuous advice and motivation.

I would not have been able to focus on my PhD studies without the unconditional love and support from my parents, in-laws and all family members. Finally, I would like to express my heartfelt gratitude to my beloved wife, Tasnim Ferdousi Joti, for being tolerant and supportive during the tough times and motivating me to accomplish this work.

DEDICATION

To my beloved parents

Dr Mohammad Abul Qasem Gazi and Tayeba Sultana

Contents

Abstract	ii
Declaration of Authenticity	iv
Acknowledgments	v
Table of Contents	vii
List of Figures	xii
List of Tables	xiv
List of Abbreviations	xv
List of Publications	xvi
1 Introduction	1
1.1 Background	1
1.2 Motivation	4
1.3 Aims and Objectives	6
1.4 Original Contribution	7
1.5 Methodology	8
1.5.1 Investigation phase	8
1.5.2 Analysis and Design Phase	9
1.5.3 Testing and Evaluation Phase	11
1.6 Thesis Outline	12
2 Literature Review	15

2.1	Background	18
2.1.1	M2M Architecture	18
2.1.2	Wireless Body Area Network (WBAN)	20
2.1.3	Difference Between Wireless Sensor Network (WSN) and WBAN	22
2.2	WBAN Applications and Significance	23
2.2.1	Medical Applications	23
2.2.1.1	Wearable WBAN	24
2.2.1.2	Implant WBAN	25
2.2.1.3	Remote Monitoring	26
2.2.2	Non-Medical Applications of WBAN	26
2.2.2.1	Fitness, Performance and Wellness Monitoring	27
2.2.2.2	Entertainment Applications	27
2.2.2.3	Emergencies	27
2.2.2.4	Authentication	28
2.2.3	Significance of WBAN applications	29
2.2.3.1	WBAN in Aged Care Facilities	30
2.2.3.2	Cost Reduction	31
2.2.3.3	WBAN Bridging Social Network	31
2.3	Challenges in WBAN	31
2.3.1	Heterogeneous Devices and Traffic	32
2.3.2	Energy Efficiency	32
2.3.3	Environmental Challenges	34
2.3.4	Security, Authentication, and Privacy	35
2.3.5	Bio-Compatibility	35
2.3.6	Quality of Service (QoS)	36
2.3.7	Interference and Coexistence	37
2.3.8	Hardware Design	38
2.3.9	Rules of Engagement	39
2.3.10	Wireless Propagation Characteristics	39
2.3.11	Overheating	41
2.4	WBAN Communication Technologies	41

2.4.1	Bluetooth	44
2.4.2	Bluetooth Low Energy	44
2.4.3	ZigBee/IEEE 802.15.4	45
2.4.4	Ultra Wideband (UWB)	45
2.4.5	IEEE 802.15.6	46
2.4.6	Guidelines for WBAN Implementations	51
2.5	SDN in WBAN: Overview and Application Challenges	52
2.5.1	Definition of SDN	52
2.5.2	Significance of SDN	53
2.5.3	SDN Architecture	54
2.5.4	SDN Protocols and Standards	55
2.5.5	Applications of SDN	56
2.5.6	Research Challenges of SDN integration with WBAN	58
2.6	Blockchain Technology for SDWBAN	60
2.7	Summary	62
3	SDN-based Application-specific Traffic Management for WBAN	64
3.1	Introduction	65
3.2	Traditional WBAN vs SDWBAN Architecture	68
3.2.1	Traditional WBAN	68
3.2.2	SDN-based WBAN (SDWBAN)	69
3.3	SBD for SDWBAN	71
3.3.1	Learning Phase	71
3.3.2	Relaying Phase	74
3.4	The SDWBAN communication framework	76
3.4.1	Communication Model	76
3.4.2	Application Classification Module	78
3.5	Performance Analysis	79
3.5.1	Implementation Scenario	79
3.5.2	Results and Discussion	80
3.5.2.1	Scenario 1	82

3.5.2.2	Scenario2	84
3.6	Summary	90
4	Optimization of Control plane for SDWBAN framework	93
4.1	Introduction	94
4.2	Influential Factors of Optimization	99
4.3	Development of Optimization Model	101
4.4	Result and Analysis	108
4.4.1	Analytical Output	109
4.4.2	Simulation Output	111
4.5	Summary	115
5	Blockchain-based Secure Data Sharing Platform for SDWBAN	118
5.1	Introduction	119
5.2	Use Cases of SDWBAN	122
5.2.1	Data Collection and Monitoring for Medicare	122
5.2.2	Data Sharing for Medical Research	123
5.2.3	Health Insurance	123
5.2.4	Handling an Emergency Situation	123
5.3	Requirement Analysis	124
5.4	Data Sharing Barriers in SDWBAN	125
5.4.1	Blockchain Technology	125
5.4.2	Challenges	127
5.4.2.1	Interoperability	127
5.4.2.2	Data Management, Anonymity, and Privacy	127
5.4.2.3	Quality of Service (QoS)	128
5.4.2.4	Storage Capacity	128
5.4.2.5	Issues with Electronic Health Records (EHRs)	128
5.5	The Proposed Architectural Framework	129
5.5.1	Users in the System	130
5.5.2	Data Storage	132
5.5.3	Access Control	133

5.5.4	Data Hashing and Integrity Verification	136
5.6	Security and Privacy Analysis	137
5.6.1	The SDS protocol	138
5.6.2	The SDA protocol	138
5.6.3	Security Analysis of the Protocols	139
5.6.3.1	Protocol Formalization	141
5.7	Results and Analysis	142
5.7.1	Experiment Setup	142
5.7.2	Experiment Outcomes	143
5.7.3	Blockchain vs Cloud Implementation	146
5.8	Summary	148
6	Conclusions and Future Work	149
6.1	Conclusions	149
6.2	Practical Implication	151
6.3	Future Research Works	152
	References	155

List of Figures

Figure 1.1	The diagrammatic outline of the methodology	9
Figure 2.1	M2M architecture for wireless connectivity in mHealth scenarios (adapted from [35])	19
Figure 2.2	WBAN Architecture for medical and non-medical Applications .	20
Figure 2.3	Classification of WBAN	23
Figure 2.4	Real-time telemedicine monitoring system for patient rehabilitation	25
Figure 2.5	IEEE 802.15.6 standard NB PPDU structure	47
Figure 2.6	IEEE 802.15.6 UWB PPDU Structure	48
Figure 2.7	IEEE 802.15.6 HBC PPDU Structure	49
Figure 2.8	Beacon mode with Beacon Period superframe Boundaries	50
Figure 2.9	Non-Beacon Mode with Superframe Boundaries	50
Figure 2.10	Non-Beacon Mode without Superframe Boundaries	51
Figure 2.11	Traditional Network Vs SDN	53
Figure 2.12	Basic SDN Framework	54
Figure 2.13	Packet forwarding flow in OpenFlow	56
Figure 3.1	Traditional WBAN vs SDN based WBAN	69
Figure 3.2	SBD Route	76
Figure 3.3	Packet Flow	77
Figure 3.4	SDWBAN_gen_pkt	78
Figure 3.5	SDWBAN_app_pkt	79
Figure 3.6	SDWBAN_app_pkt with priority ID	79
Figure 3.7	SDWBAN_Ctrl_pkt with packet header	79
Figure 3.8	SDWBAN_Cntrl_pkt_cmd	79
Figure 3.9	Implementation Scenario	81

Figure 3.10	(a) PDR VS Simulation Time, (b) PDR VS Group of Application (95_AVG_5th Percentile graph), (c) CDF of PDR	84
Figure 3.11	(a) Latency VS Simulation Time, (b) Latency VS Group of Application (95_AVG_5th Percentile graph), (c) CDF of Latency	85
Figure 3.12	PDR VS Simulation Time (Group 1-5)	86
Figure 3.13	(a) PDR VS Group of Application (95th percentile, Average & 5th Percentile), (b) CDF of PDR for each group	87
Figure 3.14	Latency VS Simulation Time (Group 1-5)	89
Figure 3.15	(a) Latency VS Group of Application (95th percentile, Average & 5th Percentile), (b) CDF of PDR for each group	90
Figure 4.1	SDWBAN Framework	95
Figure 4.2	Hops in Building Grid	104
Figure 4.3	Intercept of quadratic equation	108
Figure 4.4	Number of SDESW per Controller	109
Figure 4.5	Average PDR with varying number of controllers	112
Figure 4.6	Average Latency with varying number of controllers	113
Figure 4.7	CDF Vs PDR	114
Figure 4.8	CDF Vs Latency	115
Figure 5.1	The structure of a block	126
Figure 5.2	Blockchain-enabled SDWBAN Data Sharing	130
Figure 5.3	Protocol Verification Using AVISPA	142
Figure 5.4	(a) Latency vs Simulation Time, (b) Latency vs Group of Application, (c) CDF of Latency	145
Figure 5.5	Computation time of contracts	146
Figure 5.6	(a) Verification, hash generation and updating time in blockchain, (b) Data retrieval time from cloud storage, (c) File creation, updating and deletion time in the cloud	147

List of Tables

Table 2.1	Wireless Technologies in Medical Monitoring	21
Table 2.2	Wireless technologies in medical monitoring	23
Table 2.3	Taxonomy of Medical Applications	29
Table 2.4	Taxonomy of Non-Medical Applications	30
Table 2.5	Taxonomy of WBAN challenges and related works	42
Table 2.6	Characteristics of Wireless Technologies Used in WBAN	43
Table 3.1	SDWBAN Components	70
Table 3.2	Simulation Parameters	82
Table 3.3	Scenario 1 Group	82
Table 3.4	Scenario 2 Group	85
Table 4.1	Notations and Meaning	102
Table 4.2	Numerical Co-efficient and root	107
Table 4.3	Optimal Controllers	110
Table 4.4	List of Parameters	110
Table 4.5	Group of Applications	111
Table 5.1	Simulation Parameters	143

LISTS OF Abbreviations

ACK	Acknowledgement
BAN	Body Area Network
B-ACK	Block Acknowledgement
CAP	Contention Access Phase
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CCA	Clear Channel Assessment
CW	Contention Window
CPP	Controller Placement Problem
EAP	Exclusive Access Phase
HBC	Human Body Communication
I-ACK	Immediate Acknowledgement
M2M	Machine to Machine
IoT	Internet of Things
LAN	Local Area Network
MAC	Medium Access Control
MICS	Medical Implant Communications and Services
NACK	Negative Acknowledgement
PDR	Packet Delivery Ratio
PHY	Physical
PHR	Physical Layer Header
PPDU	Physical Layer Protocol Data Unit
PLCP	Physical Layer Convergence Protocol
PSDU	Physical Layer Service Data Unit
PLR	Packet Loss Ratio
QoS	Quality of Service
RAP	Random Access Phase
RSSI	Received Signal Strength Indicator
SHR	Synchronization Header
SIFS	Short InterFrame Spacing
SNR	Signal-to-Noise Ratio
SDN	Software-Defined Networking
TDMA	Time Division Multiple Access

UWB	Ultra-Wide Band
WBAN	Wireless Body Area Network
WSN	Wireless Sensor Network
WLAN	Wireless Local Area Network
SDWBAN	SDN-based WBAN
SBD	Sector-Based Distance
SH	Sector Head
BS	Body Sensor
RTT	Round Trip Time
TOF	Time of Flight
LOS	Line of Sight
NLOS	Non-Line of Sight
SDESW	SDN-enabled Switch
SBI	South Bound Interface
NBI	North Bound Interface
EHR	Electronic Health Record
DHT	Distributed Hashtable
IPFS	InterPlanetary File System
ACL	Access Control List
DS-Contract	Data Sharing Contract
PoC	Proof of Concept

LIST OF PUBLICATIONS

Journal Articles

- **Khalid Hasan**, Khandakar Ahmed, Kamanashis Biswas, and Md. Saiful Islam, Omid Ameri Sianaki, “Software-Defined Application-Specific Traffic Management for Wireless Body Area Network,” *Future Generations Computer Systems*, Volume 107, 2020, Pages 274-285. [WoS Rank: Q1]
- **Khalid Hasan**, Kamanashis Biswas, Khandakar Ahmed, Nazmus S. Nafi, and Md. Saiful Islam, “A comprehensive review of wireless body area network,” *Journal of Network and Computer Applications*, Volume 143, 2019, Pages 178-198. [WoS Rank: Q1]

Submitted Journals

- **Khalid Hasan**, Khandakar Ahmed, Kamanashis Biswas, and Md Saiful Islam, “Control Plane Optimization for an SDN-based WBAN Framework to Support Healthcare Applications,” *MDPI Sensors*. **(Submitted)**
- **Khalid Hasan**, Mohammad Javed Morshed Chowdhury, Kamanashis Biswas, Khandakar Ahmed, and Md. Saiful Islam, “Blockchain based Secure Data Sharing Platform for Software-Defined Wireless Body Area Network”, *Wireless Networks*. **(To be submitted)**

Conference Articles

- **Khalid Hasan**, Khandakar Ahmed, and Kamanashis Biswas, “Performance Analysis of Polling Mechanism in WBAN,” 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW, 2018, pp. 1-4.

- **Khalid Hasan**, Xin-Wen Wu, Kamanashis Biswas, and Khandakar Ahmed, “A Novel Framework for Software Defined Wireless Body Area Network,” 2018 8th International Conference on Intelligent Systems, Modelling and Simulation (ISMS), Kuala Lumpur, Malaysia, 2018, pp. 114-119.

Symposium

- **Khalid Hasan**, Kamanashis Biswas, Khandakar Ahmed, and Md. Saiful Islam, “Challenges of Integrating Blockchain in Wireless Body Area Network,” in 2018 The 3rd Symposium on Distributed Ledger Technology, Gold Coast, Australia.

Chapter 1

Introduction

The recent growth in information and communication technology encompasses different aspects of life. Machine-to-machine (M2M) communication technology is such a technology that includes various kinds of applications such as automotive, health, energy, security and surveillance, smart metering, transportation etc. However, applications of M2M in the health sector are expected to be a major market driver with a predicted 774 million health-related devices being available by 2020, yielding a total revenue of 69 billion Euros [1]. In the paradigm of telemedicine and mobile health (mHealth), an emerging technology is the WBAN. The implementation of WBAN experiences various challenges in terms of architectural design, administrative control in overall application management, priority allocation for various kinds of data traffic, optimal network design, secure data-sharing process etc. This chapter encompasses an overview of the background and significance of the research, motivation, original contribution of the thesis, and thesis outline.

1.1 Background

With the proliferation of Information Technology (IT), healthcare services are hugely dependent on IT services. Electronic-health (e-health) is considered to be one of the

most important and promising aspects of IT services in healthcare. The advancements in WBANs are the key enablers of remote and in-hospital patient monitoring and are expected to revolutionize healthcare services and the real-time patient monitoring industry. Therefore, significant research opportunities persist in the field of WBAN applications in healthcare services and may bring significant improvements which could largely benefit our community.

In general, WBAN consists of different health-related sensors attached to the body or in some cases, sensors are implanted in the body. BSs are responsible for collecting physiological data from various application sensors such as ECGs, blood pressure, body temperature, heart rate etc. and sending the data to the gateway after which the gateway transmits the data to the remote server for processing. Different sensors based on the application are equipped with data acquiring functionality, a wireless data transmission module, energy supply module and micro-controller to coordinate the periphery module and execute the function of data processing. These sensors could be from multiple vendors that employ different sensor platforms with various wireless data transmission modules. Typically, devices from multiple vendors do not interoperate with one another [2] and therefore, it is complex to manage and the maintenance requires high investment when there is a change in the network.

The infrastructure and the application are closely coupled [3] in the existing application-based architecture of WBAN. Any changes required in the application intelligence require changes in the sensor platform, gateway and server. Ultimately, a secondary defined physical structure is required when each application needs to deploy its own sensor platform, gateway and remote server from scratch. Therefore, introducing a new application is not easy, rather it requires a lengthy deployment process. Hence, it creates a barrier to potential application innovation.

In the healthcare application of WBAN, patients usually have the freedom of mobility while the BSs are attached on their body. In such cases, sometimes they are in the vicinity or inside the neighboring WBAN. This mobility causes packet loss and increases error rate [4]. Therefore, a proper handover mechanism should be implemented in WBAN.

In a traditional WBAN, traffic priority is maintained through different access mechanisms defined by various standards. There is no administrative control on traffic flow. WBAN comprises low-priority traffic, emergency and on-demand traffic. Cases of multiple emergency events, where multiple sensors would like to transmit data, create congestion. As a result, the delay caused by congestion might have catastrophic outcomes. Above all, diverse traffic pattern needs to be handled carefully.

Inefficient resource utilization is another pitfall of the current architecture. According to [3], applied control logic which is embedded into hardware, cannot dynamically improve resource utilization. Specifically, when data collection cannot be controlled dynamically, sensors will continue to transmit data to a remote server even if the data are unwanted. This causes the unnecessary waste of energy and network bandwidth.

Although advancements in information technology has improved WBAN systems, dealing with sensitive information remains a challenge. Network architecture tends to be complex when dealing with massive data, and the management of a complex network with proper authentication and secure delivery becomes cumbersome. It makes the system vulnerable to unauthorized access, which is referred as cybercrime [5, 6]. Therefore, in terms of data confidentiality, authenticity, integrity and secure management, a strict and scalable security system is still a matter of concern for WBANs [7].

WBAN is heterogeneous in nature. There are various applications in WBAN which generate different types of traffic. To deal with the heterogeneous traffic in WBAN, a well-defined MAC protocol is necessary. However, priority should be always given to life-critical traffic or urgent data. The IEEE 802.15.4 standard employs a contention-free access phase to deal with emergency traffic by allocating a fixed number of guaranteed time slots (7 GTS) which fails to fulfil the requirements of WBAN, because a fixed number of slots fails to provide access to urgent data since the size of the data differs from application to application. The standard also does not address the provision of access to emergency data from multiple applications. It is quite possible that there could be a scenario in the network where multiple applications have emergency events to be reported at the same time. For the successful implementation of WBAN, it is important

to guarantee the timely delivery of all emergency data. In IEEE 802.15.6 standard, two Exclusive Access Phases (EAP) are defined to handle emergency traffic which is based on contended allocation. However, the problem with contended allocation is that it cannot guarantee the timely delivery of data although it reduces collisions. In healthcare system, if emergency data cannot be delivered within the required time frame, then necessity of the application becomes void. Moreover, when we have multiple emergency data arriving at EAP, there will be competition between the emergency data supplying nodes to get access within the contention window. This will cause every node with emergency data to be delayed, which may have serious consequences for the patient's health or even lead to death. The access mechanism CSMA/CA can ensure simultaneous access if multiple nodes have different priorities but if two or more nodes have the same priority, then there will be collision which will increase delay. Therefore, it is important to find a mechanism to allow access to multiple emergency data simultaneously to reduce delay. In addition, a heterogeneous WBAN network simulation is also required to analyze the individual sensor's performance and compare this with optimum service-level requirements.

1.2 Motivation

To solve the aforementioned problems, the concept of SDN could be useful to support WBAN applications in healthcare. The basic principle of SDN is that it divides and separates the network into two separate planes; the control plane which determines the traffic routes and the data plane which forwards the traffic packets. Implementing SDN in WBAN would allow a centralized network view which is preferred by network administrators. With SDN, the entire body area network can be controlled using a single secure monitoring and management platform. SDN would facilitate software updates, including network service updates, without directly intervening or physically configuring the network devices. The network can be configured, monitored and controlled using a hierarchy of SDN controllers regardless of vendor-specific network devices. It is expected that a well-defined SDN framework in WBAN will provide real-time communications, online dynamic configurations and flexible adaptations to

changes in the network. Some of the benefits of SDN for WBAN that are taken into consideration are discussed as follows.

- **Getting Rid of Complex Management-** SDN provides more administrative control by separating the control plane from the data plane. In the case of SDN implementation in WBAN, health service providers will have more flexibility and programmatic control over the network. It creates a simplified platform for apps and programs. Centrally controlled operations will allow health service providers to monitor multiple sites from one location. Therefore, individual network team administrators are not required for every site.
- **Independence of Vendor-** Open standards-based implementation of SDN simplifies network design and operations. This is because the instructions and commands are provided from the controller instead of vendor-specific instructions and protocols [8].
- **Data Prioritization-** More administrative control helps deal with heterogeneous traffic patterns. Priority can be given based on the situation. Life critical data can be given a higher priority over normal monitoring data. Therefore, from an infrastructural standpoint, SDN could be used to prioritize various types of data in WBAN. The SDN controller is capable of reserving bandwidth for delay-sensitive applications to ensure guaranteed transmission [3].
- **Patient Monitoring-** A patient monitoring system will be more flexible and reliable with the help of SDN. In WBAN, the free mobility of the patient requires monitoring as well, for example, people with dementia who have wandering behavior. In [9], a secure monitoring technique by tracking the location of patients and raising an alarm have been discussed. Therefore, whenever an endpoint joins the network, the SDN controller can identify the patient [10]. A patient monitoring controller can locate the endpoint and links the access interface to the virtual network.
- **Security-** Cybercrime is another serious threat to healthcare applications. Patients' data are confidential and private; therefore, ensuring secure and

authorized access only is essential. SDN can provide identification and authentication services to defend against several cyber-attacks in healthcare. For instance, Kanazawa Hospital [11], successfully deployed SDN to create four different virtual networks on an individual physical network for the purpose of security. A secure SDN-based WBAN architectural system has been proposed in [7] for efficient and secure data delivery.

- **Mobility and Accuracy of Location Tracking-** Patients have the freedom of mobility when body sensors are attached. During mobility, patients sometimes enter a neighboring WBAN. Therefore, the accurate tracking of a patient's position is important to support mobility. With SDN and a centralized routing algorithm, it is possible to obtain accurate location information [12]. Through a mobility management protocol, a centralized controller can update networking policies on the fly. Consequently, controllers update the flow tables with updated routing decisions to ensure optimal network performance [13].

1.3 Aims and Objectives

The primary aim of this research is to develop an SDN-based WBAN communication model, analyze the feasibility of the SDN-based WBAN model to maintain QoS, mobility, traffic priority and secure data sharing using blockchain technology.

Specific objectives can be encapsulated as follows:

- Propose an SDN-based WBAN communication model and validate the feasibility of the proposed model via simulation. In addition, model the packet dissemination mechanism to analyze traffic priority for normal and emergency events.
- Investigate the optimization mechanisms to maximize the performance of the SDN-enabled WBAN. A mathematical model for optimal control plane design is developed in the proposed SDWBAN framework.

- Propose a blockchain-based data-sharing model for the proposed SDWBAN framework. In addition, investigate and validate the secure data-sharing mechanism using blockchain technology via simulation.

1.4 Original Contribution

The original contributions of this study are highlighted as follows.

- **An SDWBAN Framework for Application-specific Traffic management:**

The first contribution is an SDWBAN framework to provide flexible and scalable dynamic control over the network with an increasing number of applications. To prioritize emergency traffic over normal traffic, an efficient application classification algorithm is incorporated. Furthermore, a modified SBD routing protocol is devised to support packet dissemination in the proposed SDWBAN communication framework. It is shown in the simulation output that the proposed SDWBAN framework ensures timely delivery of emergency data with an acceptable PDR and latency. It is also demonstrated that the proposed framework is capable of accommodating a various number of application groups.

- **Resource Optimization of SDWBAN Framework:** An optimal control plane design is proposed to determine the optimal number of controllers and SDESWS for the proposed SDWBAN framework. To achieve an optimal design, a mathematical model is developed based on three crucial factors, these being the number of controllers, latency and the number of SDESWS. In the resource optimization work, a relationship is established between the number of controllers, the SDESWS and BSs for a specific latency constraint. The optimized output is validated through simulation in Castalia 3.2. It is observed that the proposed mathematical model has a competitive outcome as the number of application groups increases.

- **Secure Data Sharing Platform for Healthcare Entities:** To ensure a secure data-sharing platform for various healthcare entities, blockchain technology is

incorporated in the proposed SDWBAN framework. In the implementation process, to ensure the privacy of the data, a fine-grained access control mechanism is designed by utilizing a smart contract. The aim is to ensure the users have full control over their own data. Moreover, the effectiveness of the proposed blockchain-based data-sharing system is evaluated via simulation for several application groups in different traffic conditions. Furthermore, the overhead of blockchain implementation is also carried out and the observed output demonstrates the feasibility of the blockchain-based secure data-sharing platform.

1.5 Methodology

To maintain the integrity of the research, a reliable and coherent methodology is imperative and hence, in this section the adopted methodology of this study is presented and discussed. The diagrammatic outline of the methodology undertaken in this research are manifested in Fig. 1.1. The complete research is split into three major phases. The first step is the investigation phase where the characteristics of WBAN applications, various technical requirements and standards, simulation platforms, various challenges etc. are reviewed. The research gaps are identified in this stage. The next stage is the analysis and design phase, where an architecture is designed incorporating the SDN principles into WBAN. The final stage includes the implementation and evaluation of the designed SDWBAN framework. The stages in each phase of the methodology are elaborated in the following sub-sections.

1.5.1 Investigation phase

The investigation phase serves as a statement of the problem to be solved. It also identifies the requirements and constraints limiting the designers' implementation options. The investigation phase includes two components: investigation of WBAN characteristics and its technical requirements and investigation on design constraints. In this phase,

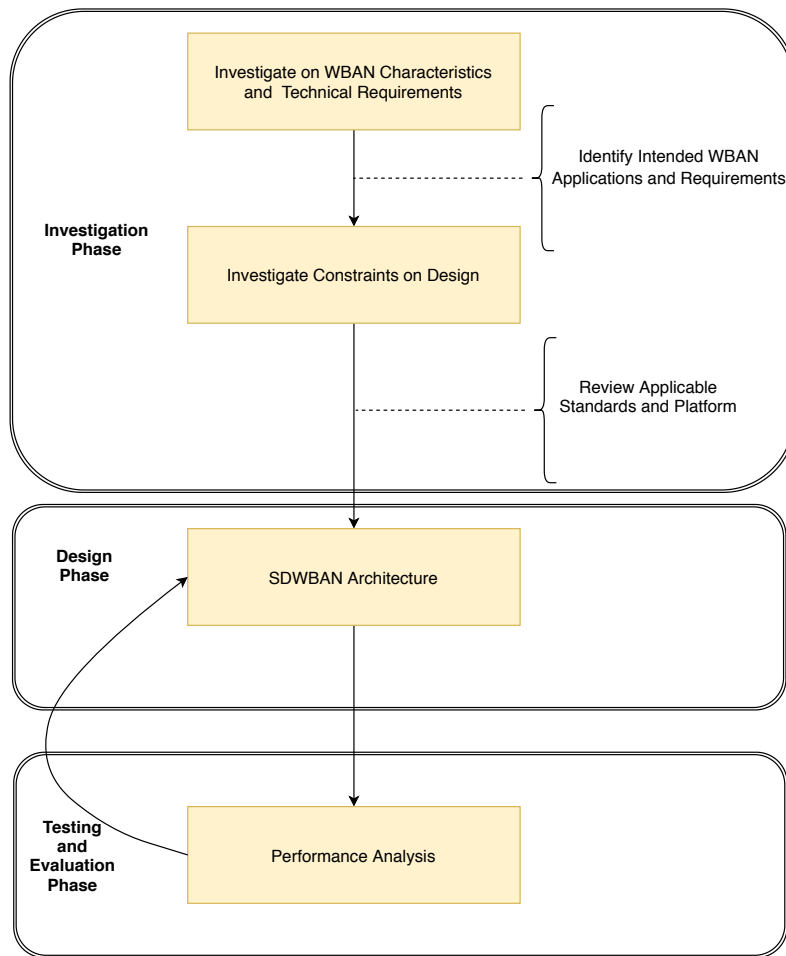


Fig. 1.1 The diagrammatic outline of the methodology

the existing literature on different applications of WBAN and requirement, candidate technologies and the applicable platforms and standards are investigated. In addition, based on the applicable platform and technical requirement characteristics, the design constraints are studied. The investigation phase aims to identify the research gaps of WBAN implementation in healthcare domain.

1.5.2 Analysis and Design Phase

In the analysis and design phase, a solution is developed that satisfies the specification of WBAN implementation. In this context, an SDWBAN architecture is established from the traditional WBAN architecture by analyzing the limitations of existing WBAN architecture. The analysis based on the literature survey reveals the shortcomings of

existing WBAN architecture in terms of complex management, vendor dependencies, traffic priority, administrative control, privacy and security in data sharing etc. To this end, the SDN incorporation with WBAN is designed so that the existing shortfall of traditional WBAN can be resolved.

The literature survey reveals few options regarding to a suitable platform for WBAN implementation. For instance, the Castalia and MiXiM [14] are among the mostly used simulators which are based on OMNet++. The module and structure of Castalia simulator offer scalability and flexibility for simulations that incorporates new and innovative distributed algorithms and protocols. In Castalia, National ICT Australia (NICTA) incorporated the channel measurements of test-bed implementation data and thus contributed to WBAN-specific wireless channels, mobility and radio models etc. [15]. Therefore, Castalia is based on a real-time measurement of channel models and the impact of body shadowing and fading. Whereas, the MiXiM offers mobility structures that includes posture variations and temporal correlation. However, considering new applications and the flexibility requirement of accommodating new algorithms and protocols, Castalia seems to be a more viable platform for this research. In previously established work, Castalia platform has been widely used such as SDN in industrial automation, smart-grid and WSNs which affirms the suitability and acceptance of Castalia simulator in this domain of research [16–18].

To facilitate the communication model of SDWBAN framework, a modified version of SBD routing protocol is devised. The design phase also incorporates a traffic priority classification algorithm based on SDN principle aiming to prioritize the emergency traffic over the normal traffic.

The analytical modelling of control plane design of SDWBAN framework focuses on flow resolution-related parameters. In the literature, the problems and solutions related to control plane optimization have been discussed from various perspectives depending on the nature of deployments. The analytical model and the simulation output are presented for a fixed flow resolution constraints. This enables a system designer to pay minute attention to the constraints and parameters for practical implications.

Nowadays, the significance of secure data sharing platform is in high demand. Preserving privacy and security in healthcare data demands a robust and reliable framework. To this aim, SDWBAN framework is further extended to incorporate the cutting-edge blockchain technology with SDWBAN. In order to retain the ownership of the personal healthcare data, a smart-contract has been designed and the security analysis has been carried out by AVISPA. This design offers a robust framework to share healthcare data with various entities such as doctors, insurer, research groups etc.

1.5.3 Testing and Evaluation Phase

The implementation translates the design into reality. Therefore, an implementation is carried out to demonstrate the validity of the proposed design. The designed SDWBAN framework is implemented in Castalia simulator for the purpose of validation. The implementation and the performance analysis of the designed SDWBAN framework is completed in two different scenarios. The first scenario evaluated the performance of the various number of applications. The output is analyzed in terms of PDR and latency with the growing number of applications. On the other hand, another implementation scenario is devised where emergency and normal application classification takes place. The performance analysis in both of the implementation scenario supports and validates the efficacy of the designed SDWBAN framework.

Initially, the implementation scenario involves arbitrary number of controllers and SDESWs. The analytical output establishes a relationship among the number of controllers, SDESWs and BSs. The analytical output is further validated through simulations in Castalia for optimum level of performance analysis in terms of PDR and latency.

In the final stage, the secure data sharing platform is implemented and evaluated. The analysis shows that the blockchain-based platform incurs very low overhead within the allowable range and thus suitable for SDWBAN framework. The fine-grained access control policy of smart contract ensures full control of data owners and hence, offers

secure data sharing platform with healthcare entities.

1.6 Thesis Outline

The chapters of this dissertation are organized as follows:

- **Chapter 1** provides a brief introduction to WBAN, the background and limitations of existing WBANs, the motivation and original contribution of the thesis, and a thesis outline.
- **Chapter 2** presents the relevant literature studies on WBAN, SDN and blockchain. Then, detailed applications of WBAN, the challenges, and communication technologies for WBAN are discussed. In addition, an overview of the SDN architecture and protocols and relevant standards are also presented. Furthermore, the prospect of blockchain technology for WBAN is also discussed.
- **Chapter 3** presents a SDWBAN framework for application traffic management in healthcare. The data communication model of the proposed framework, an application classification algorithm, SBD routing and the validation of the proposed SDWBAN via simulation are discussed.
- **Chapter 4** discusses the influential factors related to the design of the control plane for the proposed SDWBAN. In addition, a derivation of the mathematical model is also presented to determine the optimal number of controllers and SDESW for the SDWBAN framework.
- **Chapter 5** illustrates a secure data-sharing platform leveraging the principle of blockchain for the proposed SDWBAN framework. A smart contract- enabled fine-grained access control mechanism is also presented. Furthermore, the simulation work is discussed to validate the blockchain implementation for data sharing among various healthcare entities.

- *Chapter 6* summarizes the contribution of this thesis and outlines the future research prospects in the vicinity.

STATEMENT OF CONTRIBUTION TO CO-AUTHORED PUBLISHED
PAPER

The chapter 2 includes a co-authored journal paper, which has been published in Journal of Network and Computer Applications in 2019. The bibliographic details of the co-authored paper, including all authors, are:

- **Khalid Hasan**, Kamanashis Biswas, Khandakar Ahmed, Nazmus S. Nafi and Md. Saiful Islam, "A Comprehensive Review of Wireless Body Area Network", Journal of Networks and Computer Applications, Volume 143, 2019, Pages 178-198.

My contribution to the paper involved: Literature review of WBAN, challenges of WBAN, Applications, SDN in WBAN, blockchain for SDWBAN, writing and editing manuscript.

(Signed) _____ (Date) 10/03/2020

Khalid Hasan

(Countersigned) Saiful Islam (Date) 11/03/2020

Supervisor: Md. Saiful Islam

Chapter 2

Literature Review

Advancements in wireless communication technologies have impacted our day-to-day life in all aspects. In the era of the Internet of Things (IoT) and Big Data, it is inevitable to experience the effect of this advancement in the health sector. Electronic health monitoring [19], fitness monitoring [20], calorie measurement [21], online consultation with specialists, diagnosis and remote healthcare [22] are all possible these days by exploiting various communication technologies. Of the most promising communication technologies that enable applications to monitor human health data and post-processing, WBAN is considered the prime candidate.

Over the last five years, there have been many literature surveys that have attempted to highlight the key findings regarding the design, challenges and implementation issues of WBAN. Of these, some well cited survey papers [23–31] on WBAN cover a wide range of topics i.e., WBAN communication architecture, candidate technologies, applications in medical and non-medical fields, security issues of WBAN, propagation modelling, and implementation requirements etc. Movassaghi et al. [30] identified the application of WBAN in medical and non-medical sectors and gave a detailed view of PHY and MAC layers. In addition, the paper provided significant highlights on different routing protocols and security along with various technical challenges pertaining to implementation. Alam et al. [28] proposed one unique application of WBAN-wearable devices which is related

to safety and critical applications in severe environments, such as oil and gas industries, refineries and many petrochemical industries. In this work, an inter-WBAN interaction is presented where the WBAN coordinator works as a resourceful device that wirelessly interconnects the body sensors to an external network infrastructure utilizing WiFi or broadband cellular networks such as GSM, GPRS, 3G, and LTE.

A comparative analysis of various WBAN technologies and design challenges was provided in [29]. The paper concentrates on radio channel modelling, the minimization of energy consumption and coexistence issues in WBAN while providing a few case studies based on real implementation and experimentation in the field and in simulations. In [31], similar discussions based on a previous literature survey are presented, focusing on only a few medical applications and related technologies for WBAN. The analysis of coexistence issues and interference mitigation solutions in WBAN technologies is explained in [24]. Furthermore, the mathematical representation of coexistence issues in IEEE 802.15.6, IEEE 802.15.4 and low-power WiFi technologies and simulation results are compared. The paper also highlights interference mitigation solutions with a system model and definition. A link between WBAN and cognitive radio technologies is demonstrated in [32]. Context awareness at the MAC layer, application layer and challenges are analyzed in [25]. Specific challenges in relation to security and privacy in WBAN for healthcare applications are discussed in [27]. A survey of a WBAN-based electronic healthcare (e-healthcare) system in a residential environment is outlined in [23] which uses a smartphone-based healthcare application. The latest review paper [26] on WBAN introduces programming frameworks for WBAN and focuses significantly on energy efficient routing protocols. The paper also indicates the use of virtual reality (VR) as a futuristic vision of WBAN and the merging of WBAN with cognitive radio technology for energy efficiency.

Researchers have continually tried to find an optimal solution to the challenges of WBAN either by modifying the existing solutions or incorporating new technologies. Management related complexities, vendor dependencies, mobility, data privacy and security, energy efficiency, and traffic priority management are some of the most crucial constraints of WBAN. To deal with the challenges of WBAN, two recent and attractive

technologies, software-defined networking (SDN) and blockchain have been proposed. Both SDN and blockchain are making revolutionary changes by offering lucrative prospects in the domain of IoT applications, especially in WBAN. On one hand, an SDN centralized programmatic control system solves management-related complexities and vendor dependencies, whilst the decentralized distributed ledger of blockchain creates an effective and secure data sharing platform.

The aims of this chapter are to discuss the current architectures of WBAN in dealing with management complexities, security, reliability and so on. Moreover, it also aims to identify the significant future direction of research in improving communication architecture that deals with management complexity, reliability, security and privacy. The key highlights of this chapter can be put more concretely as follows:

- A taxonomy and the significance of WBAN are presented on the basis of various medical and non-medical applications of WBAN projects.
- A comprehensive overview of the important characteristics of the candidate technologies for WBAN is given with a special focus on the latest WBAN standard IEEE 802.15.6 has been presented to provide a deep technical overview of the state-of-the-art technologies in WBANs. In addition, an in-depth analysis on different implementation challenges and related works to address existing the challenges is critically examined.
- A discussion on the SDN technology is presented encompassing the significance of SDN in diverse fields such as SDN in cellular network, Wi-Fi, IoT, edge computing etc.
- The prospect of the proposed SDWBAN to deal with management complexities and security issues is presented.
- The security aspect of cutting-edge blockchain technology is discussed. In addition, the challenges of integrating blockchain in the proposed SDWBAN for data sharing is also analyzed.

2.1 Background

The number of patients affected by chronic diseases are increasing day by day. These patients are continually readmitted to hospital and healthcare centers and require significant medical attention. To treat patients efficiently, smart healthcare systems are continuously improving. With the fundamental characteristics of exchanging a huge amount of sensory data between participating nodes, this communication can also be classified as one of the candidates of M2M communication in the health sector [33]. A relatively new and emerging technology is WBAN under the paradigm of telemedicine and mHealth where different health-related applications are used. The primary requirement for developing smart health-related applications using WBAN is the need for interconnecting devices to have autonomous and self-organizing capabilities. A detailed overview of M2M and WBAN is presented in the next sub-sections.

2.1.1 M2M Architecture

As an emerging technology, M2M communication includes the autonomous and self-organizing capabilities of interconnecting devices. One of the best features of this technology is monitoring, while controlling the devices remotely [34]. The capability of remote monitoring has aided the expansion of M2M in diverse fields, including industrial automation, security and surveillance, smart metering, energy management, transportation, and healthcare. Of these, healthcare is expected to be a major M2M market driver. Fig. 2.1 [35] illustrates the simple architecture of the M2M system for healthcare applications.

The European Telecommunications Standards Institute (ETSI) proposed three important domains for M2M architecture; i) the M2M device domain where M2M devices communicate with a gateway through short-range area networks; ii) the network domain that connects the gateway to the applications through long-range access and core communication networks; iii) the application domain where various application services are defined based on different use cases.

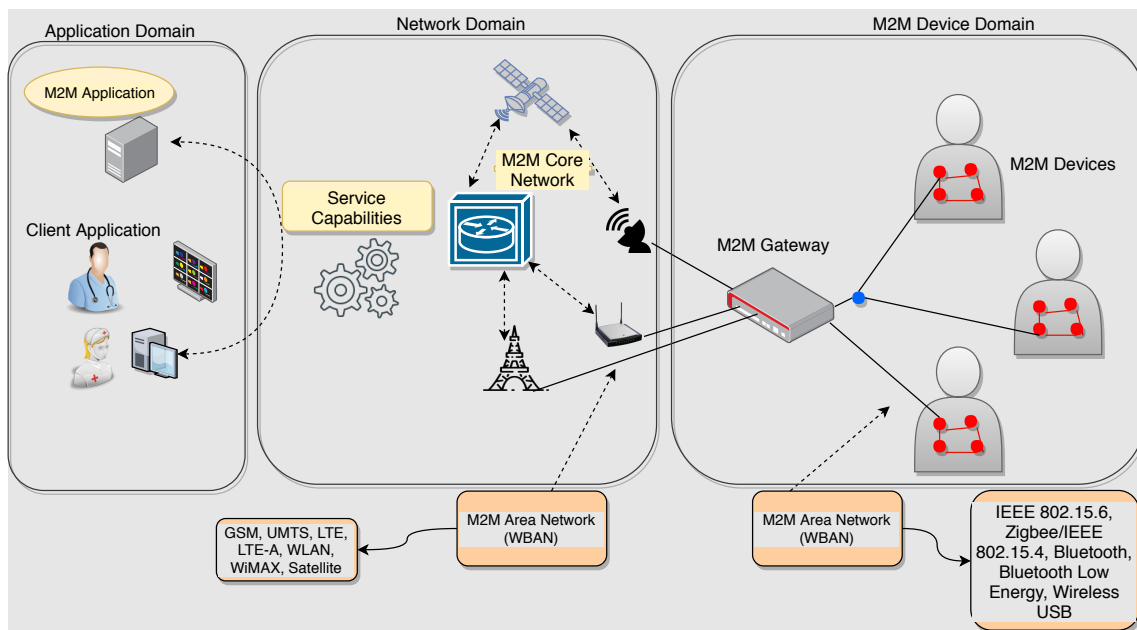


Fig. 2.1 M2M architecture for wireless connectivity in mHealth scenarios (adapted from [35])

M2M devices or WBAN sensors/actuators are installed in the vicinity of a patient's body or on the body (wearable) or implanted internally. The resource constrained sensors are capable of transmitting data autonomously or when data is requested. Each device is embedded with wireless communication functions, which enables them to connect to a short-range communication network. The M2M area network interconnects WBAN sensors to the M2M gateway. This M2M network employs different technologies such as ZigBee, IEEE 802.15.6, Bluetooth and Bluetooth Low energy. The M2M gateway works as a proxy between the M2M devices and the network domain. In reality, a gateway should be a portable device which has an interface of radio communication technology. Mobile phones, PDAs or smart watches can be used as a gateway. The M2M communication part connects the M2M gateway to the Internet, which then connects to the application server. This communication part utilizes traditional wireless communication technologies, for instance, Long-term Evolution (LTE), WiMAX and IEEE 802.11 WLAN. The application domain receives the data and processes these accordingly with the help of specific software [36].

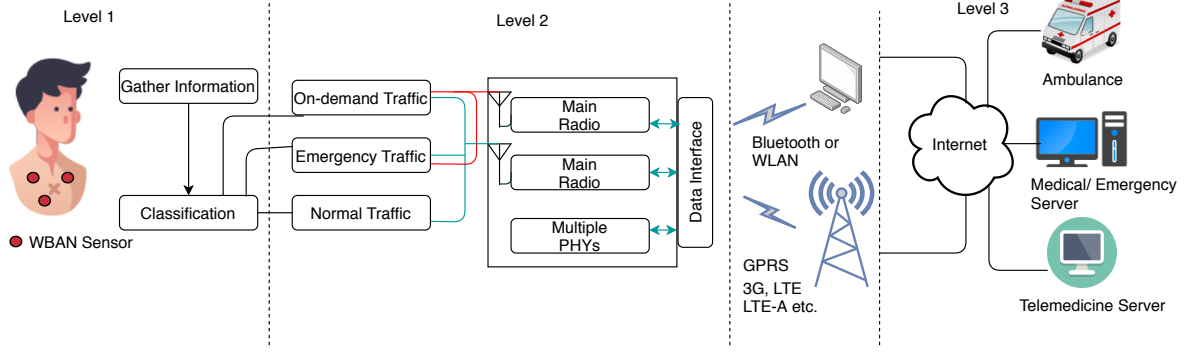


Fig. 2.2 WBAN Architecture for medical and non-medical Applications

2.1.2 Wireless Body Area Network (WBAN)

WBAN is a collection of multiple sensors attached to or in the body, which are used to receive different physical parameters, such as body temperature, blood sugar level, heart rate, pulse rate, respiratory measurement and even the amount of calories, burnt after exercise etc. WBAN is not only used in medical applications, it is also used in multimedia and gaming applications. Sensor nodes can be placed in different topologies such as a star, mesh or tree. However, it depends on the type of application and most of the time, it follows the star topology where the nodes are connected to a central coordinator. The detailed architecture of WBAN based on [37] is presented in Fig. 2.2 and consists of three levels. In level 1, different body sensors are attached to the human body which send data to an aggregator where the classification of traffic takes place. After the classification in level 2, a network coordinator communicates with the base-station. Level 3 comprises a few base-stations that keep the patients' physiological data and the healthcare service providers supply necessary diagnostic recommendations based on this data.

WBAN uses different technologies for data transmission such as Wireless Medical Telemetry Services (WMTS), unlicensed Industrial, Scientific and Medical (ISM) (2.4-2.4835 GHz), Ultra-wideband (UWB) and Medical Implant Communication Services (MICS). Depending on the type of service, these technologies are employed, due to the fact that some of the applications might require high data rates while some are satisfied with low data rates. For example, restricted WMTS (14 MHz) cannot support video or voice transmission. Instead, 2.4 GHz ISM band could be used. However, it

Table 2.1 Wireless Technologies in Medical Monitoring

	MICS	WMTS	IEEE 802.15.6 (UWB)	IEEE 802.15.4 (ZigBee)	IEEE 802.1 (Bluetooth)	WLANs (802.11b/g)
Frequency band	402-405 MHz	608-614, 1395-1400, 1429-1432 MHz	3-10 GHz	2.4 GHz (868/915 MHz Eur./US)	2.4 GHz	2.4 GHz
Bandwidth	3 MHz	6 MHz	>500 MHz	5 MHz	1 MHz	20 MHz
Data Rate	19 or 76 Kbps	76 Kbps	850 Kbps-20 Mbps	250 Kbps (2.4 GHz)	721 Kbps	>11 Mbps
Multiple Access	CSMA/CA, Polling	CSMA/CA, Polling	Not defined	CSMA/CA	FHSS /GFSK	OFDMA, CSMA/CA
Transmission Power	-16 dBm (25W)	10 dBm and <1.8 dBm	-41 dBm	0 dBm	4.20 dBm	24 dBm
Range	0-10 m	>100 m	1.2 m	0-10 m	10-100 m	0-100 m

causes adjacent channel interference since Bluetooth, ZigBee, and Wi-Fi also use this band. For implantable sensor application an allocated band is MICS (402-405MHz) [37]. Some of the wireless technologies used in medical monitoring are listed in Table 2.1.

WBAN traffic can be categorized into three types: on-demand traffic, emergency traffic, and normal traffic (as shown in Fig. 2.2). On-demand traffic is requested by physicians for diagnostic measurement. Emergency traffic is sent when a patient's condition surpasses a predefined threshold value. For instance, in the case of the blood pressure threshold (set by the physician), the monitoring device observes when a patient's blood pressure is below the threshold, the corresponding node triggers an emergency alarm informing the practitioner to take the necessary action. Even though this kind of traffic is not generally the case, it is rather unpredictable. Normal traffic refers to the regular monitoring of the patient's condition after a certain interval. Examples of normal traffic could be the diagnosis of the gastrointestinal tract, neurological disorder, cancer detection, handicap rehabilitation and the most serious, heart disease. The coordinator is in charge of processing and sending the data to the telemedicine and medical servers for further treatment or recommendations. If necessary, the coordinator might use a wake-up radio circuit to respond to the emergency.

2.1.3 Difference Between Wireless Sensor Network (WSN) and WBAN

Although the tasks of both wireless and body sensors are to sense and send data, the technical differences are in the implementation scenarios and use cases. It is important to realize the key differences between WSN and WBAN. Both WSN and WBAN applications have different requirements and challenges. Typically, WSN does not tackle the specific challenges related to the monitoring of health, where the prime focus of WBAN is to reliably monitor the patient's health activities. Therefore, the number of sensor nodes deployed for WBAN depends on different factors, such as the physiological parameters and it should be scalable when they are needed for an application. On the contrary, in WSN, nodes are typically deployed in a place where human access is limited or is challenging. Sometimes redundant nodes are deployed as a backup in case of some nodes are dysfunctional. The protocols supported by wireless sensor nodes and body sensor nodes are different in terms of the distance to be covered, mobility, and electromagnetic transmission etc. In particular, in WBAN, low power transmission is used since it is concerned with human health issues [38]. WBAN may occur in a more periodic manner with a stable data rate unless emergency event occurs. On the other hand, WSN is employed for event-based monitoring that takes place at an irregular intervals [39]. Strict security and privacy is maintained in terms of body sensor implementation while security and privacy in terms of wireless sensors could be a bit more relaxed in some applications. One of the important issues for both wireless and body sensors is energy efficiency. WBAN devices need to be very energy efficient as they have a very small form factor which is frequently less than 1 cm^3 [40]. Moreover, for implanted devices, changing the battery is a difficult job requiring expensive surgery. Therefore, it is expected that the battery should have a long lifetime, this being up to several years or even decades.

Table 2.2 Wireless technologies in medical monitoring

Application Type	Sensor Node	Data rate	Duty Cycle (per device)	Power Consumption	QoS (Sensitivity to Latency)	Privacy
In-body Applications	Glucose Sensor	Few Kbps	<1%	Extremely Low	Yes	High
	Pacemaker	Few Kbps	<1%	Low	Yes	High
	Endoscope					
	Capsule	>2Mbps	<50%	Low	Yes	Medium
On-body Medical Applications	ECG	3 Kbps	<10%	Low	Yes	High
	SpO ₂	32 bps	<1%	Low	Yes	High
	Blood pressure	<10bps	<1%	High	Yes	High
On-body non-Medical Applications	Music for Headset	1.4 Mbps	High	Relatively High	Yes	Low
	Forgotten Things	256 Kbps	Medium	Low	No	Low
	Monitor					
Off-body Applications	Social Networking	<200Kbps	<1%	Low	Low	High
	Motion Sensor	35 Kbps	-	-	-	Low

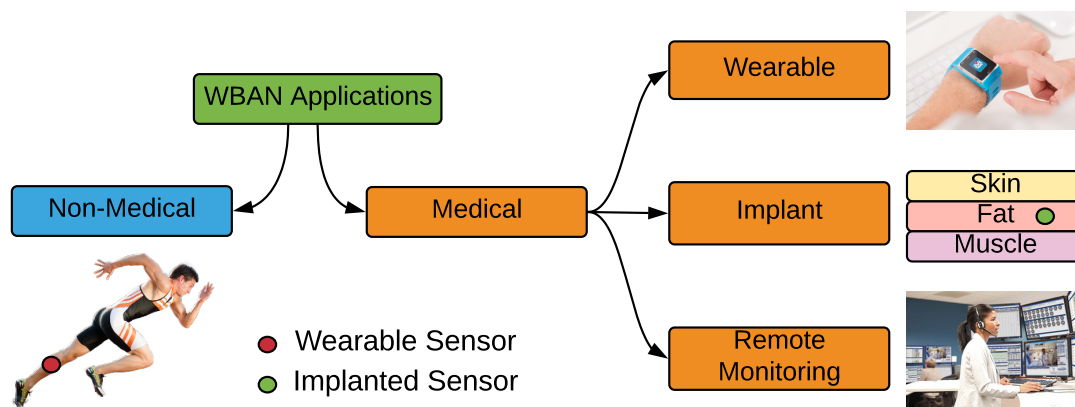


Fig. 2.3 Classification of WBAN

2.2 WBAN Applications and Significance

There are several applications of WBAN, both medical and non-medical applications. A summary of WBAN applications along with the required parameters is presented in Table 2.2 [41]. WBAN can further be classified into three categories as depicted in Fig. 2.3.

2.2.1 Medical Applications

The devices used in medical applications can be wearable, implantable or remote monitoring. These different types of medical applications are briefly explained in the

following sub-section.

2.2.1.1 Wearable WBAN

These WBAN devices are normally attached to the body surface by straps. Some examples of wearable WBAN applications are discussed as follows:

The activities of soldiers can be monitored using WBAN applications in the battlefield. Using GPS-enabled devices or a camera, it is possible to monitor these activities from a central station and maintain secure communication. To prevent an ambush, a secure communication should exist [37].

Athletic performance can be observed using WBAN. A personal trainer can follow up on the performance level of athletes by observing data sent from wearable devices attached to an athlete's body. In addition, real-time feedback through this application would lead to performance improvement and assist the athlete to avoid injury [42].

Sleep is an important activity in our daily life. Sleeping disorders eventually affect productivity in the workplace and can lead to cardiovascular diseases, dizziness while driving and even loss of appetite. Therefore, monitoring a patient's sleeping patterns has gained huge attention in recent days. A polysomnography test is used to diagnose a sleeping disorder through the analysis of a number of bio-potentials recorded overnight in a sleep laboratory. This kind of test requires the use of a lot of cables which makes the patient uncomfortable and causes even more disturbance during sleep. WBANs are capable of delocalizing and removing the need for cables [43].

Millions of people suffer from asthma. WBAN can be used to monitor allergic agents in the air and provide real-time feedback to physicians. A GPS-based device is proposed in [44] which monitors environmental factors and triggers an alarm in the case of detecting an environment to which the patient is allergic.

A real-time health monitoring service is available as a part of a WBAN application. For example, a patient rehabilitation (framework as shown in Fig. 2.4 [37]) center can be

monitored using a WBAN framework. As Fig. 2.4 depicts, patients can be monitored for a long time and physiological data can be forwarded to the cloud on a real-time basis. On the other hand, a panel of doctors or physicians can monitor patients' activity through video conferencing or through real-time database updates.

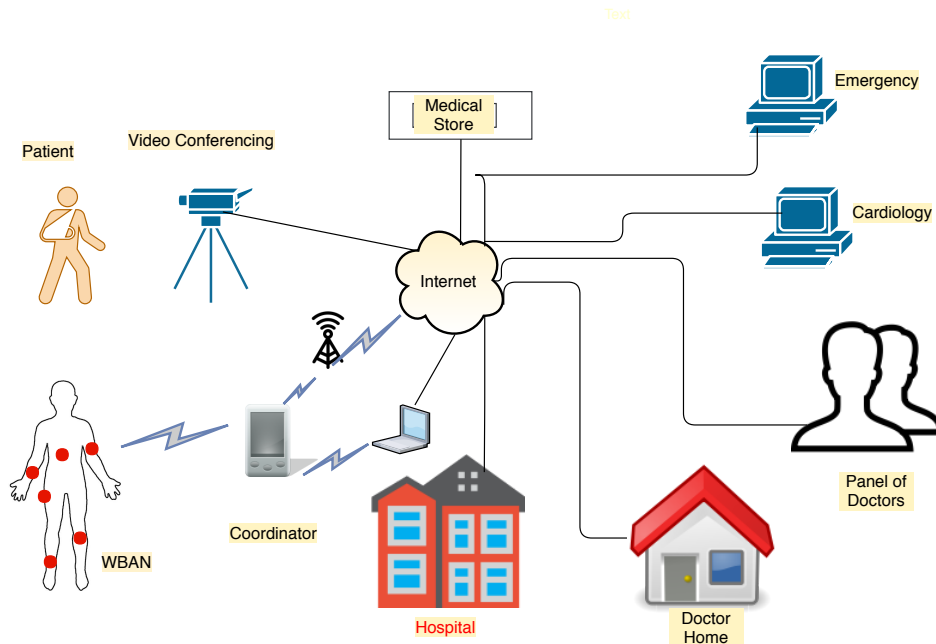


Fig. 2.4 Real-time telemedicine monitoring system for patient rehabilitation

2.2.1.2 Implant WBAN

These WBAN devices are normally implanted in the body. Some examples of implant WBAN applications are discussed below:

According to the global report on diabetes [45], the number of diabetes patients has increased to 422 million since 1980. In Australia, around 1.7 million people have diabetes and more than 100,000 Australians developed diabetes in the past year [46]. Various complications may arise due to this disease, such as heart attack, stroke, blindness, kidney failure and lower limb amputation. Regular monitoring by WBAN would lower the severity of diabetes and therefore keep it under control. Gluecocellphone technology, which is used with diabetes patients to provide glucose measurements which are forwarded to doctors for further analysis [42].

Cardiovascular diseases are one of the major causes of death, but this condition can be monitored through WBAN technology. Myocardial infraction (MI) can be monitored periodically and considerably lowers the risk. WBAN technology can be applied to monitor various abnormalities of physical health [30].

It is predicted that the rate of global cancer could increase by 50% to 15 million by 2020 [47]. By monitoring cancer cells through WBAN-based sensors, doctors can extract important data related to cancer detection and continue to diagnose tumors without biopsy, which would lead to the optimum analysis and treatment [30]. More about the implantable communication technologies of WBAN can be found in [48].

2.2.1.3 Remote Monitoring

The seamless Internet connectivity of WBAN allows a patient's vital signs to be tracked and provides real-time feedback on the healing process. To be specific, WBAN sensors are capable of sensing heart rate, body temperature, pulse rate, respiration rate, blood pressure, and other important physiological parameters. These sensors are continuously or periodically monitoring the patients' health condition and sending data to the doctors. Therefore, doctors find it easy to follow up and provide remote assistance either by video conferencing or a phone call.

2.2.2 Non-Medical Applications of WBAN

WBAN is not only used in medical applications, it is also used in various non-medical applications. A few examples of the non-medical application of WBAN are described in the following sub-sections.

2.2.2.1 Fitness, Performance and Wellness Monitoring

In recent days, many devices are being used for physical fitness and wellness. These devices keep a record of physical activities and performance. For example, the TomTom smart watch is capable of keeping track of how many calories have been burnt after a certain distance of jogging. Likewise, in a gym, a personal fitness trainer can keep records on a gym member's fitness level and follow up by planning activities at the next level. WBAN sensors attached to individuals send sensory data which can then be analysed. WBAN sensors can be deployed in corporate offices to monitor the performance of employees. For instance, Hitachi's Business microscope, which resembles a badge or an ID card worn by employees, monitors all the face-to-face communications between office workers, including how often and where; it collects information on how many times an employee leaves their chair, how far they walk and where they go; and it can also monitor the an employee's contribution in a group meeting. It also measures ambient lighting and air temperature. This information can be used by management to improve the work environment, which leads to better satisfaction and increased productivity [25].

2.2.2.2 Entertainment Applications

WBAN can be used in social networking, virtual reality and gaming applications Hand gestures or body movements, personal item tracking, and exchanging business card are some examples [30].

2.2.2.3 Emergencies

In the case of a household fire, smoke detectors can trigger a fire alarm. However, a hearing-impaired person will not be able to hear this alarm. A WBAN sensor can sense the seriousness of the situation and send a tactile alert to warn the person of the danger. This is useful also in industries which are vulnerable to fire or poisonous gas escape where WBAN sensors (off-body) can play an important role in saving lives in the workplace.

2.2.2.4 Authentication

A WBAN application can be used for secure authentication purposes by utilizing biometric parameters, such as fingerprints, face detection, palm prints, hand geometry, iris recognition, retina recognition and odor. Biometric signals, such as ECG, EEG and electrodermal activity (EDA) provide unique biometric signatures, which are difficult to steal, copy, forge or lose. This scheme is commonly known as “cognitive biometrics”. Future Attribute Screening Technology (FAST) is an example of such technology, which is used by the United States of America Department of Homeland Security. FAST uses bio-signals collected through off-body sensors, such as heart and respiration rate, facial skin temperature, voice pitch, pupil dilation and body movement [25].

A taxonomy of medical and non-medical applications is given in Table 2.3 and Table 2.4.

Table 2.3 Taxonomy of Medical Applications

Medical Applications	Focus	References
Cardiovascular Disease (CVD)(MyHeart)	Self-managed Monitoring System of CVD and Real-time Monitoring	[49], [50]
Heart Rate Monitoring	Electrocardiogram (ECG), Heart Rate (HR), Body Acceleration, Temperature Sensors	[51], [52]
Real-time Monitoring and Analysis of Human Health	Blood Pressure, Body Temperature, ECG, Blood Flow	[53], [54]
Health Face	Web-based Remote Health Monitoring	[55]
RehabSPOT	Stroke and Physical Dysfunction	[56]
Rehabilitation	Improve Rehabilitation and Assisting in Mobility	[57]
Comfortable Health Monitoring for New Born (Smart Jacket)	ECG	[58]
Kids Health Monitoring System (KiMS)	Temperature and Pulse Rate Sensor	[59]
Rehabilitation and Recovery Monitoring	Rehabilitation Exercise Monitoring	[60]
IMPAIRED	Low Back Pain	[61]
HipGuard	Leg and Hip Position Rotation	[62]
Real-time Activity Monitoring	Exercise Monitoring for patients with motor impairment	[63]
Fall Detection	Posture of Humans especially elderly people	[64], [65], [66]
Abnormal Condition Detection System	Monitors sitting, walking, lying and falling	[67]
Neurodegenerative	Parkinson	[68]
BASUMA	Health Monitoring (ECG, Reactive Oxygen Sensor, SpO ₂ sensor, Spirometer)	[69]
MobiHealth	Ambulatory Patient Monitoring (ECG)	[70]
AID-N	Emergency Response of Blood Pulse, ECG	[71]
MAHS	Spirometer, Pressure, Temperature, Pulse	[72]
Code Blue	Motion, Pulse , Oximeter	[73]
LifeMinder	ECG, Thermometer, SpO ₂ , Galvanic Skin Response	[74]
ASNET	Remote Monitoring (Temperature and Blood Pressure)	[75]
Ayushman	EKG, Blood Pressure, Oximeter, Gyroscopic Sensor	[76]
SMART	ECG, SpO ₂	[77]
Biofeedback	Controlling Emotion such as Stress	[78]
Assisted Living	Disable People	[79]

2.2.3 Significance of WBAN applications

An overview of the significance of WBAN applications is presented in the following sub-sections.

Table 2.4 Taxonomy of Non-Medical Applications

Non-Medical Applications	Focus	References
Golf Training	Wearable sensors to monitor quality of movements	[80]
Soccer Player Monitoring	Routing techniques to monitor soccer player's movement	[81]
THE-FAME	Muscle fatigue through sensing accumulation of lactic acid	[82]
Fitness Monitoring	Improvement in user's quality of life	[52]
Physical State Monitoring	Identifying exhausted player	[83]
Performance of Marathon Athlete	Real-time data collection in dense dynamic environment	[84]
Biometrics	User authentication	[85]
Sweat pH Analysis	Textile-based sensor	[86]
Indoor Positioning System	Assists visually impaired person to determine objects	[87]
DynaMo	Mobility pattern of players	[88]
Baseball Game	Calculates force, torque during baseball game	[89]
Precision Analysis of Dart Game	Measurement of speed, acceleration and timing.	[90]
Cyclist performance Analysis	Motion sensors used for monitoring lower limb kinematics	[91]
Project ProeTEX	Sensor based garments for activity monitoring of fire fighters	[92]
Soldiers Activity Monitoring	Estimates the impact of blast and effects on soldier	[93]
Management of Notification	Intelligent notification tool	[94]
Serious Gaming	Detects stress level and improve effectiveness of games	[95]

2.2.3.1 WBAN in Aged Care Facilities

The number of people in elderly home is increasing day by day due to the lifestyles like loneliness or to get a better healthcare services. A survey conducted in Asia, reveals that old age population is rising and it is estimated that in near future there will be one older person out of a group of four people [96]. Therefore, there is a need for healthcare services which can monitor the health status of an elderly person who is living in their own home and transmit medical data to doctors so that they can be diagnosed accordingly. WBANs has had a profound impact on healthcare services in terms of quality of care, healthcare management and safety. Many patients in aged care facilities need to be monitored continuously. It is expensive to involve medical staff in these types of duties and the work is cumbersome. With the aid of WBANs, the management of patient monitoring is more flexible and cost efficient.

2.2.3.2 Cost Reduction

Placing patients in hospital care is expensive, whether the cost is covered by a health insurance agency or through government funds. Hence, it is not always feasible to admit a patient in hospital simply to monitor their condition. However, the patient's physiological condition might deteriorate at any time when they are at home. In an emergency event, if the elderly person is by themselves, they will require expert medical assistance prior to being admitted to hospital. In cases such as this, WBAN can play a vital role in providing remote healthcare services.

2.2.3.3 WBAN Bridging Social Network

The most popular means of information sharing and communication among groups of people with similar interests is social networking. This huge popularity is due to several Web2.0 technologies [97]. In social networks, a common platform allows a group of people to create information while others consume it. In a similar fashion, a WBAN can capture physical events and even go beyond the capability of what these existing social media platforms offer by providing information without the need for any human intervention. For instance, an ECG sensor attached to an elderly person can capture an unusual heartbeat rate and send this information to a social network which might include his family members, the family physician, emergency services, friends, colleagues and so on.

2.3 Challenges in WBAN

WBAN is an emerging technology which is facing many challenges when it comes to the implementation phase. These include technical, ethical and non-technical challenges which are discussed in the following.

2.3.1 Heterogeneous Devices and Traffic

Networks comprise different kinds of sensors and actuators, thereby generating different measurements and data types. Some applications require real-time data while some only need periodic measurements. There are priority and non- priority data as well. Therefore, data types ranging from real-time audio to video content and continuous signals, such as ECG and EMG, should be supported by WBAN.

MAC protocols for WBAN play an important role in this context. Different activities, such as movement, body posture, and environment changes etc., lead to a sudden change in the data context. Thus, a dynamic resource allocation technique should be supported by the MAC protocol. The WBAN MAC protocol with a fixed slot allocation fails to meet the demand of heterogeneous and dynamic traffic of WBAN. Some attempts have been made to deal with context-aware WBAN. For an emergency response, an alarm is supported in [98] but it works only when no other node is scheduled to perform a data transfer. The use of a wake-up signal or wake-up radio is used in [99], to switch the node from a sleeping to an active state. However, the addition of a wake-up circuit makes hardware implementation complex and costly. In [100], another attempt to support a context-aware WBAN is made, which again lacks the computational ability to analyze the context. More recent work on the simulation-based WBAN MAC can be found in [101] where it is suggested that hybrid MAC protocols are used in cases of emergency data. However, this is challenging to implement in heterogeneous applications.

2.3.2 Energy Efficiency

One of the most important challenges in implementing WBAN is energy efficiency. Since WBAN sensors are supported by a small battery, the lifetime of the battery is essential to bear in mind. WBAN devices, which are wearable sensors, are easy to replace. However, in the case of implanted sensors, changing the battery might require costly major surgery. Implementing an energy efficient WBAN could be possible by improving the design of the PHY and MAC layers by developing an efficient hop system (single hop or multihop)

or having an adaptive duty cycle.

In [102], a TDMA-based MAC protocol for a multi-tier architecture for WBAN was proposed. This proposal includes sensor nodes in the first tier and a set of master nodes in the second tier and finally, an observation station in the third tier. Master nodes collect the data from the sensor nodes and forward them to the monitoring station. The limitation of this proposal is that it is based on a stationary network. One of the challenges is that when the patient moves, thereby the distance between the sensor nodes and master nodes varies. Consequently, the nodes adjust the transmission power, which makes the system less energy efficient. The authors of [103] discussed energy efficiency in terms of a derived path loss model on the human body. It is shown that single hop communication in WBAN is inefficient since nodes are located far away from the sink. Again, the issue of line of sight and non-line of sight exists as well. In the case of a transmitter residing at the back, while the receiver is at the front, more path loss incurs. In such cases, a multihop WBAN is more advantageous than a single hop.

Since different standards are used in WBAN, energy efficiency differs accordingly. IEEE 802.15.6 consumes more energy than IEEE 802.15.4. In the case of IEEE802.15.6, the carrier senses the channel and the back-off counter decreases its count based on sensing the channel. However, in IEEE 802.15.4, the back-off counter value decreases to zero after only two sensing phases. Despite this disadvantage of IEEE 802.15.6, its successful packet transmission is higher than IEEE 802.15.4. Ultimately, this leaves us with two choices, whether we want reliability or energy efficiency.

Sources of energy inefficiency are discussed in [104], which includes collisions, over hearing, idle listening, and resource allocation techniques etc. Energy efficiency by proper resource allocation was discussed in [105]. The proposed methodology employs the Global Energy Minimization (GEM) scheme in order to achieve optimization. By allocating the proper time and power, the energy efficiency problem is formulated. Network lifetime maximization and GEM schemes have been compared with uniform time allocation (UTA). However, in this proposal, the energy consumed while the nodes are asleep has been ignored due to the low consumption of energy.

A TDMA-based MAC protocol named BODYMAC is proposed in [106], where the main purpose is to reduce packet collision by switching the radio state. It uses flexible bandwidth management with the help of its superframe structure, where a synchronization beacon in the downlink part is allocated for transmission from the coordinator and the uplink part is used for packet transmission from the nodes to the coordinator. The uplink part is partitioned into two parts, the contention access part (CAP) and the contention free part (CFP). In CAP, the nodes inform the coordinator of the required bandwidth and CFP, the coordinator grants a time slot in which the nodes can transmit. In order to support BODYMAC, an efficient sleep mode scheme is also proposed. The sleep mode is initiated by turning the radio transmitter off, where the coordinator responds to the sleep request during the CAP period.

2.3.3 Environmental Challenges

WBANs experience path losses due to many reasons, such as postural body movement, node mobility, environmental obstacles, and absorption through body tissue. Many of these problems can be answered by creating multi-hop links by installing sensors at significant points. However, this will lead to a change in the operational condition of the network, which will cause interference and the consequences will be an error-prone and incomplete sensor data reception [30]. In addition, due to the strict health science regulations, designing WBAN is a crucial issue. Because, in implantable or wearable sensors, the antenna shape, size and material used should be in accordance with the constraints followed by healthcare facilities. More about the design restrictions in relation to size and shape according to organ and location can be found in [107–109]. To illustrate, the length of the urethra valve is restricted to a diameter of 4mm-6mm and it has to be replaced at a regular interval without surgery. This means that a path antenna, monopole or dipole antenna are difficult to use. In this situation, an alternative solution would be to use a helical antenna integrated into the shape of a valve implant [110].

2.3.4 Security, Authentication, and Privacy

It is imperative to make WBAN communication very secure to maintain data confidentiality, meaning the information transmitted from the WBAN can only be accessed by authorized entities and the authenticity of the incoming data is confirmed. Eavesdropping, false alarms or the injection of incorrect data may lead to serious consequences, such as a patient's death. Therefore, the security of WBAN should be dealt with at different layers e.g., physical, MAC, and network layers [37]. However, the implementation of security measures incurs extra overheads and also makes the system less energy efficient. Therefore, in [111], a lightweight security scheme is proposed for WBAN, where a lightweight biometric technique is used to authenticate messages in WBAN. In a lightweight biometric technique, a key agreement scheme permits key sharing between WBAN nodes with low overheads. This analysis is proved to be energy efficient. Different authentication methods, for instance, human faces, hand features, and EEG signals are being used in WBAN and continuous improvement is occurring in both in academia and industry. An ideal way to provide authentication is to use distinguishable human body characteristics. This is complex and challenging when patients connected to one WBAN reach the proximity of another WBAN. Therefore, it is important to identify to which network a patient belongs. In [112], the authors addressed the issue of node identification from the biometrics point of view. According to [113], the security in WBAN could be improved by establishing trust between nodes in the network. An attack resistant and lightweight trust management protocol is proposed in [114]. According to this proposal, the experiment outcomes of this paper prove that the network performance improves and protects the network from malicious behavior.

2.3.5 Bio-Compatibility

In the context of WSN applications, bio-compatibility is not a significant issue. However, for WBAN applications, especially in the case of implantable sensors,

bio-compatibility is an important issue to deal with. Due to implanted sensors underneath the skin or any other part of the body, body tissues show a reaction. This reaction is known as bio-fouling, which refers to the accumulation of proteins, cells and other unwanted bio-materials on the body surface. Bio-fouling could be the reason for the degradation of sensor current and thus may lead to sensor failure [115]. Alleviating the effect of bio-fouling using nine sensors was discussed in [116]. Further analysis related to bio-compatibility was discussed in [110], which identifies two factors for the body's reaction e.g., mechanical and chemical disruption. Mechanical disruption might cause tissue distortion and the occlusion of blood vessels. A blunt and rounded shape for the sensors could be used to lessen tissue distortion.

2.3.6 Quality of Service (QoS)

Quality of Service (QoS) is an important issue in WBAN and is different from WSN applications. QoS in WSN cannot be directly applied to WBAN since QoS depends on the sensitivity of the applications and the nature of the transported data. Hence, depending on the applications, QoS is different in WBAN. For critical patients, monitoring systems require the instant delivery of data, as a delay could cause a catastrophic situation [117]. According to the authors of [118], it is difficult to set the QoS for a distributed healthcare system due to the unpredictable nature of the WBAN environment. Traditionally, QoS includes latency, transmission power, reliability, and bandwidth reservation. According to [118], to support QoS in WBAN, the following factors need to be considered.

- **Resource Limitations:** Resources such as battery power, available bandwidth, transmission power, buffer size, and processing capacity are important constraints for any sensor node application. Traditional QoS of routing and MAC protocols are not appropriate for WBAN.
- **Unpredictable and Heterogeneous Traffic:** In WSN applications, generally there is periodic traffic and it is easy to define QoS for such applications. However, WBAN experiences different levels of traffic such as no traffic, data burst and

sometimes different loads of traffic due to different types of applications in WBAN. This heterogeneous traffic makes QoS support and requirement more complex and challenging.

- **Network Instability and Dynamics:** WBANs may comprise both stationary and mobile nodes. In addition, some nodes could be in an active state whereas others may stay in an inactive state for a certain period of time. In addition to these, link failures and power failures are very common in WBANs and therefore, a stable network may frequently become unstable. Routing and medium access become challenging in such unstable conditions.
- **Energy Balance:** The management of energy sources is very important and energy load should be distributed evenly among all sensor nodes and devices.
- **Data Redundancy and Criticality:** It is important to avoid redundant data and hence, save energy. One technique to avoid redundant data is data aggregation, but it complicates the network design. Again, not all data are of the same importance. Therefore, there should be a QoS mechanism to prioritize emergency data.

According to [119], three components can be used to satisfy QoS in WBAN. These are: i) an asymmetric architecture, in which most of the processing is done on the central node, ii) a virtual MAC that allows it to schedule wireless resources regardless of the MAC protocol used, and iii) an adaptive resource scheduler that schedules the remaining bandwidth to fulfill the QoS requirements in the case of channel failure due to RF interference because of patient movement.

2.3.7 Interference and Coexistence

Interference and coexistence are unavoidable issues that demand attention. According to standard IEEE 802.15.6 [120], up to 256 devices per body should be supported in WBAN and up to 10 WBANs in 6x6x6 meters should coexist, which is very challenging due to the proximity of nodes. Most importantly, there will be interference when WBAN

is surrounded by other technologies that operate at the same frequency as WBAN. For example, 2.4 GHz band ZigBee-based WBAN experiences interference from Bluetooth, IEEE 802.15.6, and WiFi networks. Some simulations which are based on studies to analyze interference and coexistence scenarios were performed in [121,122] with wearable sensors. The interference between nodes belonging to the same WBAN was investigated in [121] and the interference between nodes of different WBANs was investigated in [122]. The simulation results show that interference occurs due to the absence of synchronization between nodes, which creates collisions with nearby nodes. The coexistence experience with IEEE 802.11 b/g was investigated in [123,124]. In [123], two nodes were used to form a WBAN and were attached to a person's right arm and right shin. While conducting the experiment, the person was on the move. It was found that 16 channels of ZigBee were affected by the high transmission power of nearby WiFi access points. There was a high packet loss ratio (PLR) despite the ZigBee center frequency being far from the active WiFi stations. However, there are very few works on the implementation of the latest standard pertaining to the comparison of coexistence and interference issues with the existing technologies. In [125], a simulated environment, including five WBAN nodes on a human body, two WiFi nodes, and five ZigBee nodes was set in a room. The channel model used in the simulation included the effect of body propagation and movement. It was found that with the minimum shift keying (MSK) modulation technique, the MAC of IEEE 802.15.6 performs better than the MAC of the ZigBee network. The modified MSK and Gaussian MSK had a similar performance in terms of PLR despite the interference. In fact, it was found that IEEE 802.15.6 MAC shows better performance than the MAC of IEEE 802.15.4, but consumes more energy due to the longer sensing period.

2.3.8 Hardware Design

One of the important tasks is to design proper hardware for WBAN, or more specifically, to design the sensor node which is attached or implanted in the human body. Therefore, the design of the node has to be compliant with the nature of human body tissue. In addition, the design of the antenna is very crucial. Again, the design of

an implanted antenna depends on the location and the organ, which places a restriction on the designer. The size, material and shape of the antenna needs to be compatible with human tissue and the RF environment. The challenges of antenna design, such as antenna gain, polarization, sensitivity and ability to connect with the access point for non-line of sight position are very important. At present, UWB technologies have attracted the significant interest of researchers since they increase SNR levels at the receiver.

2.3.9 Rules of Engagement

Defining rules of engagement or, in other words, creating a WBAN which meets the requirement of patients is challenging. According to [126], three points should be taken into account when forming a WBAN: i) the environment within which WBAN nodes can function, ii) which devices are allowed to cooperate or which are not, and iii) how device information can be used. Once WBAN is formed, the devices should be able to interchange data, negotiate security parameters, perform data sampling, associate nodes, remove sensors, change a sensor's operational mode and so on. Any changes in the network should be recorded and shared among the other associated devices. In addition, local device registries should be updated once there is some sort of change.

2.3.10 Wireless Propagation Characteristics

Wireless propagation plays a vital role in communication between nodes. Since nodes are attached to the body, the mobility of the patients affects wave propagation and sometimes, devices attached to the back of a body experience a shadowing effect. In addition, nodes need to deal with dynamic environments such as twisting, running and multipath propagation. In the case of implanted devices, the position of the device has an effect on wave propagation. Therefore, it is necessary to have an accurate propagation model that will help the scientist predict the impact of realistic channels on network-level performance. This will help to design a more effective WBAN architecture and routing

algorithms.

Recently, the use of UWB channel models for body area networks has attracted increasing interest. Many simulations and experimental approaches are being studied in order to find a proper channel model. There is scant literature on the channel model for WBAN. However, there is no general channel model that can be used comprehensively irrespective of gender, age and application. In [127], the author conducted an experiment for in-body communications within the frequency range of 2.36-2.5 GHz. In this experiment, a phantom-based radio propagation study was performed, where the experimental set-up includes a vector network analyzer (VNA), a styrofoam container, a phantom aqueous solution and coaxial cable. An insulated dipole antenna and free space coax-fed helical antenna were used for in-body and off-body measurement, respectively. This is a practical approach to model a WBAN channel; however, authentic path loss data were not provided, and the results were presented only for human muscle tissue. Also, no latter work was done to validate the path loss model.

An attempt was made to develop a WBAN channel model for capsule endoscopy in [128]. An electromagnetic simulation software named SEMCAD was used to model path loss between implant nodes and coordinator. In this case, the operating frequency was 403.5 MHz, which is defined in the standard IEEE 802.15.6 for the Medical Implant Communication Service (MICS) band. However, the study lacks experimental validation. A frequency and distance dependent path loss model was investigated in [129]. In this case, a human body model was used in ANSYS HFSS (High Frequency Structural Simulator). An investigation was performed for a wide frequency range i.e., from 10 Hz to 100 GHz. The path loss model obtained from this experiment does not accurately represent the real WBAN case since the measurement was performed beyond the defined frequency standard of WBAN. Some other investigations [130, 131] were performed to find the path loss model for in-body communication in homogeneous human muscle tissue, brain, fat and skin. However, it is significant to validate the previous path loss model through simulation and experiment.

2.3.11 Overheating

Since WBAN sensors are sometimes attached directly to human skin, ensuring the sensors do not overheat is crucial. Usually, overheating is due to the radiation of the antenna during data transmission. This may cause damage to heat sensitive human body tissue [132, 133]. In addition, the routing protocols used in WBAN plays a prime role in the temperature rise of the sensors which ultimately causes discomfort and damage to tissues. Therefore, the issue of overheating should be kept in mind while designing routing protocols [134]. Electric and electromagnetic radiation causes a temperature rise in sensor devices which results in the tissue absorbing a part of the temperature. The effect of temperature rise and specific absorption ratio is discussed in [135].

There has been scant research on avoiding overheating problems due to routing protocols. To deal with the overheating issue of implanted nodes, the Temperature-Aware Routing Algorithm (TARA) was proposed which is based on a certain threshold temperature to find appropriate routes. However, this protocol suffers from high end-to-end delay and is also less energy efficient [136]. Least Temperature Rise (LTR) aims to rectify the problems encountered by TARA. LTR works by selecting the nodes with have the lowest temperature [137]. An improved version of LTR, Adaptive Least Temperature Rise (ALTR), utilizes a proactive delay technique to reduce the temperature of the nodes and follow this route [138]. Although these routing protocols try to avoid overheating nodes to route the packets, reliability is compromised in most cases. Therefore, temperature-aware routing protocols also need to adhere to the stringent constraints of WBAN.

2.4 WBAN Communication Technologies

WBAN supports a number of short-range technologies to communicate with the gateway, for instance, Bluetooth, Bluetooth Low Energy, ZigBee, and IEEE 802.15.6.

Table 2.5 Taxonomy of WBAN challenges and related works

Challenges References	Heterogeneous Devices and Traffic	Energy Efficiency	Environmental Challenges	Security, Authentication, and Privacy	Bio- Compatibility	QoS	Interference and Coexistence	Wireless Propagation Characteristics
[98, 99]	✓	✓						
[100]	✓							
[102, 104, 105]		✓						
[103]		✓						✓
[106]		✓				✓		
[30, 107, 108]			✓					
[107, 109]			✓					✓
[37, 112–114]				✓				
[111]		✓		✓				
[115, 116]					✓			
[117–119]						✓		
[120–125]							✓	
[110]			✓		✓			
[127–131]								✓

All of these short-range communication technologies possess a variety of characteristics and support different operating frequencies and networking topologies. A summary of the characteristics of the wireless technologies used in WBAN is provided in Table 2.6. Gateway to server communication utilizes long-range communication technologies such as, WiMax, LTE, and LTE-Advance. In this section, we focus on a number of short-range candidate technologies for WBAN only. In addition, we provide an implementation guideline for WBAN based on the latest IEEE 802.15.6 standard.

Table 2.6 Characteristics of Wireless Technologies Used in WBAN

<i>Technology</i>	<i>Operating Frequency</i>	<i>Data Rate</i>	<i>Coverage</i>	<i>Network Topology</i>
Bluetooth V.1 <i>802.15.1</i>	2.4 GHz ISM	780 Kbps	10-150 m (on-body only)	star
Bluetooth V.2 + Enhanced Data Rate (EDR)	2.4 GHz ISM	3 Mbps	10-100 m (on-body only)	star
Bluetooth V.3+ High Speed (HS)	2.4 GHz ISM & 5 GHz	3-24 Mbps	10 m (on-body only)	star
Bluetooth V.3+ Low End Extension (LEE)	2.4 GHz ISM	1 Mbps	10 m (on-body only)	star
RFID (ISO/IEC 18000-6)	860-960 MHz	10-100 Kbps	1-100m	Peer-to-Peer
Ultra Wideband (UWB)	3.1-10.6 GHz	110-480 Mbps	5-10 m (on-body only)	star
ZigBee (IEEE 802.15.4)	868 MHz, 915 MHz, 2.4 GHz ISM	20, 40, 250 Kbps	10-100 m (on-body only)	star, mesh, cluster tree
Near Field Communication (NFC)	13.56 MHz	106, 212, 424 Kbps	Up to 20 cm	Peer-to-Peer
ANT	2.4 GHz ISM	1 Mbps	30 m (on-body only)	star, mesh, peer-to-peer, tree
Sensium	868 MHz, 915 MHz	50 Kbps	1-5 m (on-body only)	star
Zarlink(ZL 70101)	402-405 MHz, 433-434 MHz	200-800 Kbps	2 m (in-body only)	Peer-to-Peer
RuBee (IEEE 1902.1)	131 KHz	9.6 Kbps	30 m	Peer-to-Peer
Z-wave	900 MHz ISM	9.6 Kbps	30 m	Mesh

2.4.1 Bluetooth

Bluetooth technology is designed for short-range communication with high data rates. It operates in 79 channels of each 1 MHz. As a short-range technology, Bluetooth is a good choice for implementation in WBAN. However, Bluetooth consumes a lot of energy and is therefore not suitable for WBAN applications. Bluetooth operates in a 2.4 GHz frequency band and the typical operating range is 10-100 m. This technology works like a star topology, where a master and seven slaves form the network. The master node provides clock and frequency hopping patterns. Nonetheless, the limitation is that it involves seven active slaves only, which puts a threshold on the maximum number of nodes to be used in the WBAN network. In the early 2000s, a WBAN project named MOBI Health used Bluetooth technology to transmit sensor data from a front-end device to a mobile phone or PDA [139].

2.4.2 Bluetooth Low Energy

Bluetooth Low Energy (BLE) is also known as Bluetooth 4.0. It was previously called Bluetooth Low-End Extension (LEE) and later Wibree. It is designed to operate with low power consumption, provide low latency, and operate in short-range and on small coin battery cells. It was first introduced by Nokia in 2004 to connect small devices wirelessly. After some development in LEE under a project named MIMOSA (for the use cases of WBAN and WPAN), LEE was announced publicly with the name Wibree in 2006. BLE supports a data rate of 1 Mbps. To provide better latency for crucial WBAN applications, BLE has the capability to employ few channels for pairing devices, and synchronization can be done in milliseconds. Similar to Bluetooth, the BLE technology forms a star network [140]. A continuous data mode operation of BLE consumes similar energy as classical Bluetooth. The star topology used in BLE offers mobility support for WBAN applications.

2.4.3 ZigBee/IEEE 802.15.4

ZigBee is another widely used technology for WBAN applications. ZigBee supports a variable data rate ranging from 20 Kbps to 250 Kbps. It operates in 16 channels over 2.4 GHz ISM band (250 Kbps), in 10 channels over 915 MHz bands (40 Kbps), and in one channel over 868 MHz bands (20 Kbps) [141].

ZigBee provides two modes for the multiple access procedure, namely beacon mode and non-beacon mode. In a beacon-enabled mode, a superframe structure uses two phases of operation namely, active and inactive phases. In the inactive phase, sensor nodes stay in low power mode to reduce energy consumption. The active phase consists of two parts: i) Contention Access Phase (CAP) and ii) Contention Free Phase (CFP) [142]. In CAP, nodes compete to gain access to data transmission using a slotted CSMA/CA mechanism and in CFP, Guaranteed Time Slots (GTS) are assigned to specific nodes to transmit data. This provides an opportunity to transmit emergency data during the GTS slots. However, a fixed number of GTS is not suitable for emergency data transfer in some WBAN applications. According to researchers, the performance of IEEE 802.15.4 is not satisfactory for WBANs. It has been pointed out that ZigBee can suffer from interference from other WLAN transmissions. Again, the maximum supported data rate is 250 Kbps, which is not sufficient for some real-time WBAN applications or the large-scale deployment of WBAN.

2.4.4 Ultra Wideband (UWB)

UWB technology is an attractive choice for use in WBAN because of the regulated low transmission power. The operating frequency band for UWB is 3.1-10.6 GHz, which is high. Although UWB is supposed to have low transmission power, its high operating frequency makes it consume high power. Therefore, designers experience difficulty in designing such UWB nodes. However, the possibility of avoiding high power consumption of an UWB receiver is to employ transmitter- only networks for low power networks like WBAN. In this case, only one transmitter is used to send data and monitor the

physiological parameters of a patient's body. A unique identification number of individual sensors assists in distinguishing individual patients [143]. According to [142], UWB is an attractive choice for several reasons. For example, for WBAN tracking in indoor environments, the UWB technology can provide precise localization. It is also concerned with power absorption by human tissue, therefore it regulates low transmission power and a low transmission duty cycle.

2.4.5 IEEE 802.15.6

The popularity, demand, and effectiveness of a real-time healthcare monitoring system will revolutionize future healthcare technology. IEEE 802 has established a task group named IEEE 802.15.6 for the purpose of standardizing WBAN. The aim of the standard is to support low power communication for in/on body nodes to forward physiological data to the access point. Based on the standard, WBAN is categorized in medical and non-medical applications. IEEE 802.15.6 defines physical layer specifications and MAC layer specifications as well. A description of the Physical and MAC layers is given below.

PHY Layer Specification: The IEEE 802.15.6 standard supports three PHYs, i) Narrowband (NB) PHY, ii) Ultra Wideband (UWB) PHY and iii) Human Body Communications (HBC) PHY. A description of each PHY layer is as follows.

- **NB PHY:** The responsibility of the NB PHY is to perform the following three tasks: i) activation and deactivation of the radio transceiver, ii) clear channel assessment (CCA) within the current channel, and iii) data transmission and reception. The Physical Layer Protocol Data Unit (PPDU) consists of three parts: i) Physical Layer Convergence Protocol (PLCP) ii) the PLCP header and iii) Physical Layer Service Data unit (PSDU). Fig. 2.5 illustrates IEEE 802.15.6 NB PPDU structure.

Packet transmission is carried out in an orderly manner. The first component to be transmitted is the PLCP preamble, then PLCP Header and finally PSDU. PSDU is pre-appended by PLCP Preamble and PLCP header. PLCP preamble is used

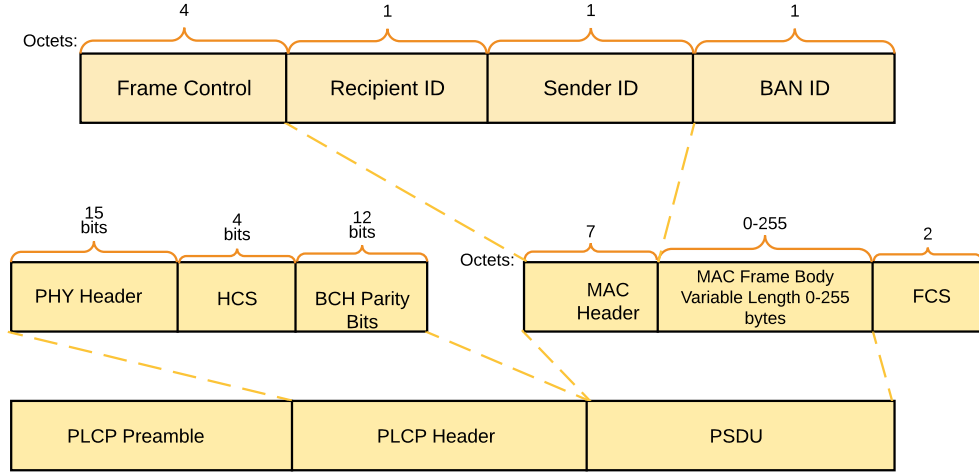


Fig. 2.5 IEEE 802.15.6 standard NB PPDU structure

at the receiver to synchronize time and offset recovery. The PLCP header is a transmitter with a given header data rate in the operating frequency. The PSDU unit consists of a MAC header, a variable MAC frame body length (0-256 bytes) and frame check sequence. A WBAN compliant device should be able to support transmission and reception in at least one of the following frequency bands: 402-405 MHz, 420-450 MHz, 863-870 MHz, 902-928 MHz, 2360-2400 MHz, and 2400-2483.5 MHz. Modulation parameters are different for different frequency bands of operation. According to the standard, modulation techniques such as, Differential Binary Phase-shift Keying (DBPSK), Differential Quadrature Phase Shift Keying (DQPSK) and Differential 8-Phase Shift Keying (D8PSK) are used in NB PHY. However, in 420-450 MHz, Gaussian Minimum Shift Keying (GMSK) technique is used [144].

- **UWB PHY:** High band and low band are the two frequency bands that are used in the UWB PHY. Each of the bands is divided into channels of bandwidth 499.3 MHz. The low band comprises three channels of which channel 2 is considered as mandatory with the central frequency of 3993.6 MHz. The high band consists of eight channels, where the seventh channel is considered to be mandatory with a central frequency of 7987.2 MHz. A WBAN device should be able to support at least one of the mandatory channels [144].

The UWB PHY is expected to be robust when performing in WBANs and thereby implementation is on a large-scales. In addition, in UWB PHY, signal power levels are in the order of those used in the MICS band, which provide a harmless power level for the human body and low interference for other devices. Some other functionalities of the UWB PHY include:

- Activation and deactivation of the radio transceivers.
- The PPDU is constructed by a Synchronization Header (SHR), Physical Layer Header (PHR) and Physical Layer Service Data Unit (PSDU), respectively (as shown in Fig. 2.6). The PPDU bits are converted into RF signals for transmission in the wireless medium.
- The UWB PHY may provide a CCA indication to the MAC in order to verify activity in the wireless medium.

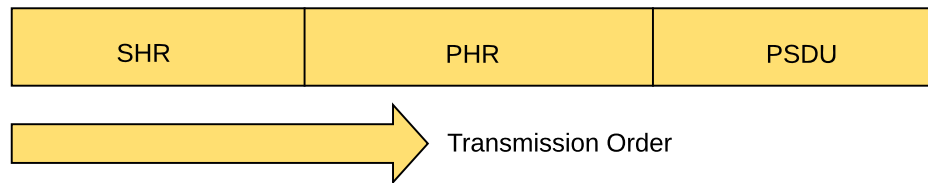


Fig. 2.6 IEEE 802.15.6 UWB PPDU Structure

- **HBC PHY:** Electric Field Communication (EFC) is used for human body communications for the PHY layer. It covers the entire communications for BANs, such as modulation, preamble/Start Frame Delimiter (SFD), and Packet structure. The structure of the PPDU includes PLCP preamble, Start Frame Delimiter (SFD), PLCP Header and PHY Payload as shown in Fig. 2.7.

The preamble and SFD are fixed in size. They are pre-generated and sent in advance of the packet header and payload. In order to ensure packet synchronization, the preamble sequence is transmitted four times while SFD is sent only once. Once the receiver receives the packet, it catches the beginning of the packet by identifying the preamble sequence and then it finds the start of the frame by detecting the SFD [144].

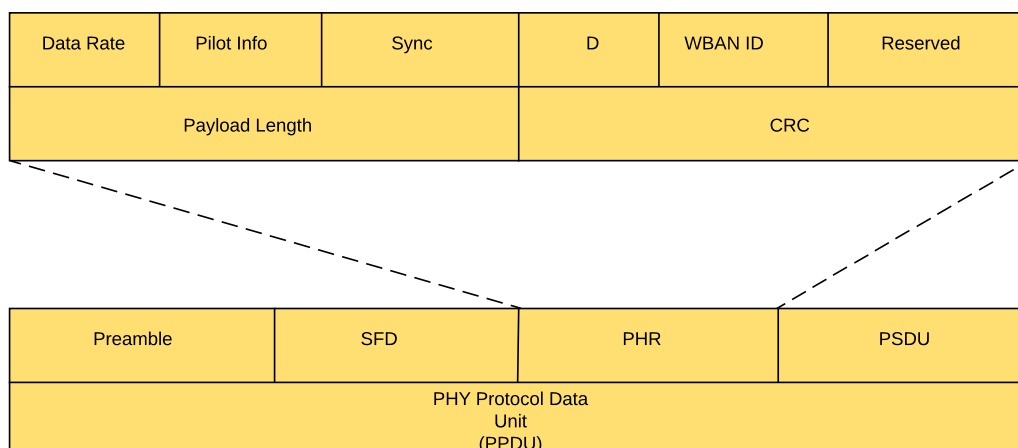


Fig. 2.7 IEEE 802.15.6 HBC PPDU Structure

MAC Layer Specification: To provide channel access, the IEEE 802.15.6 working group defines the MAC layer on top of the PHY layer. The coordinator or hub divides the entire channel in a superframe structure, where time-referenced resources are allocated. The hub chooses a beacon period of equal length to bound the superframes. The offset of the beacon period can be shifted by the hub. Beacons are transmitted in each beacon period of the active superframe unless prohibited by some MICS band regulations [144]. According to the standard IEEE 802.15.6, the hub has the responsibility to allow one of the following three access modes:

1. Beacon Mode with Beacon Period Superframe Boundaries.
2. Non-Beacon Mode with Superframe Boundaries.
3. Non-Beacon Mode without Superframe Boundaries.

Beacon Mode with Beacon Period Superframe Boundaries: In this mode, beacons are transmitted by the coordinator or hub in each beacon period except for inactive superframes. Hence, for inactive superframes the hub does not provide any access. Fig. 2.8 illustrates the structure of the superframe, which comprises two Exclusive Access Phases (EAP1 and EAP2), two Random Access Phases (RAP1 and RAP2), Type I/II access and a CAP.

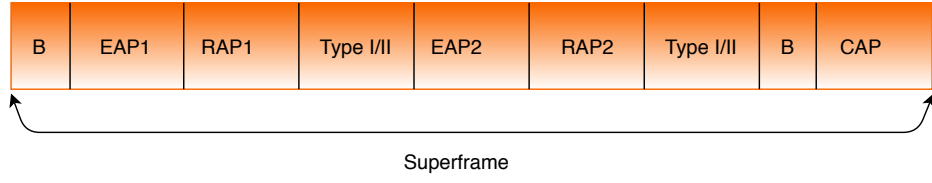


Fig. 2.8 Beacon mode with Beacon Period superframe Boundaries

In Fig. 2.8, B stands for beacon. The hub has the control to set any of the access phases to zero length. However, it allows RAP1 to end first when a guaranteed time is allocated for connected nodes. EAP1 and EAP2 phases are used for emergency traffic. RAP and CAP are used for normal traffic. In EAP, RAP and CAP phases, access is provided through CSMA/CA or slotted Aloha. Type I/II access phase is also called the Managed Access Phase (MAP). Type I/II access phases are used for both uplink and downlink allocation intervals. In Type I/II access polling mechanism is used for resource allocation.

Non-Beacon Mode with Superframe Boundaries: In this mode, beacon is not transmitted at all. The whole duration of the superframe boundary includes either Type I or Type II access phase as shown in Fig. 2.9. In the type I polling mechanism, the allocation length is specified in terms of the duration of the time granted for transmission, whereas in the type II polling mechanism, the allocation length is specified in terms of the number of frames granted for transmission.

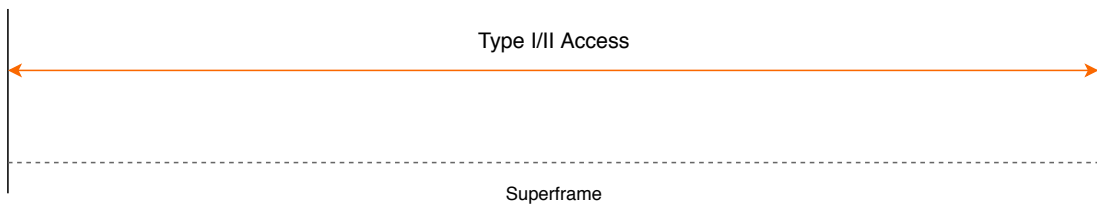


Fig. 2.9 Non-Beacon Mode with Superframe Boundaries

Non-Beacon Mode without Superframe Boundaries: This mode allows unscheduled Type II polling or posted allocations as shown in Fig. 2.10. It is a non-reoccurring time interval that a hub grants to itself using posting access to initiate a frame transaction.

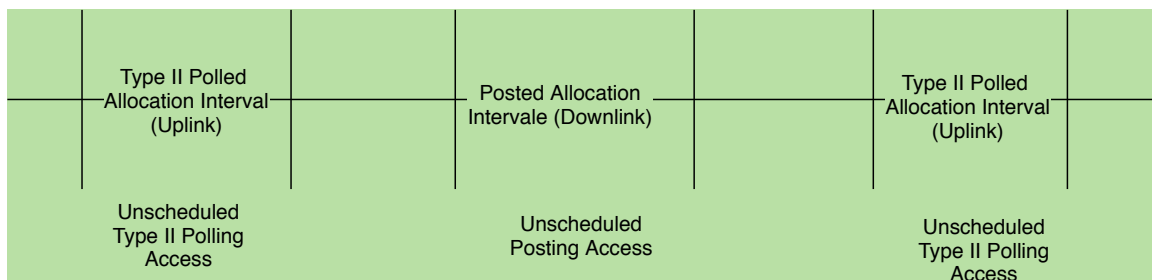


Fig. 2.10 Non-Beacon Mode without Superframe Boundaries

2.4.6 Guidelines for WBAN Implementations

IEEE 802.15.6 approved some key requirements in order to implement WBAN. The requirements are as follows [37, 42, 145] .

- The number of nodes in body area network should be scalable up to 256 nodes.
- WBAN link should be able to support data rate between 10 Kbps and 10 Mbps.
- Packet Error Rate (PER) should be less than 10% for a 256 octet payload (256x8 bits of data) for a majority (95%) of the best performing links based on PER (i.e., at a given signal-to-noise ratio 5% of channels that give the worst PER performance should not be used to determine whether this PER guideline is met).
- Nodes should be able to be added or removed to/from the network within 3 seconds.
- Nodes should be capable of reliably communicating with the network despite all sorts of movement due to sitting, turning, twisting arms, running, waving arms and dancing with others which may result in shadowing and channel fading.
- The maximum radiated transmission should not exceed 0 dBm or 1 mW. All devices should be capable of transmitting at 0.1 mW (-10 dBm). This complies with the specific absorption-rate (SAR) guideline of the Federal Communication Commission (FCC) of 1.6 W/kg in 1 g of body tissue [146].
- Jitter, latency, and reliability should be supported for WBAN applications that require them. Latency in medical applications should be less than 125 ms, and 250 ms in non-medical applications. Jitter should be less than 50 ms.

- Power saving mechanisms should be followed when WBAN operates in power-constrained environments.
- In-body and on-body area networks should be capable of coexisting in and around the body.
- Coexistence with heterogeneous environment should be supported where networks of different standards cooperate amongst each other to receive information.
- Some medical diagnoses might require a high data rate. For instance, ECG monitoring might require a UWB-based WBAN to support high data rates.
- WBAN must incorporate QoS management features to be self-healing and secure as well as allowing priority services.
- The physical layer should support collocated operation of up to 10 randomly distributed body area networks in a 6mx6mx6m volume.

2.5 SDN in WBAN: Overview and Application Challenges

In this section, an overview of SDN, SDN architecture, protocols and standards related to SDN and the challenges of integrating SDN in WBAN is discussed.

2.5.1 Definition of SDN

In recent years, SDN has attracted researchers from both academia and industry. SDN is a new networking paradigm which separates the control plane from the data plane platform. Decoupling the control plane from the data plane gives operators the opportunity to work in a centralized control program instead of numerous, multi-vendor, network devices to implement their favorite policies [147]. The control plane is a software based controller

and network devices become a simple packet forwarding device (the data plane) which can be programmed via an open interface i.e. ForCES [148], OpenFlow [149].

Fig. 2.11 [150] presents a contrasting architecture of traditional network and SDN. In SDN, a controller machine creates packet-forwarding rules for any changes in network topology, connection initiated by end hosts, shifts in traffic loads or messages from other controllers. A controller drives these rules towards programmable switches where necessary functionalities are implemented. This feature of SDN allows the easier deployment of new protocols and applications.

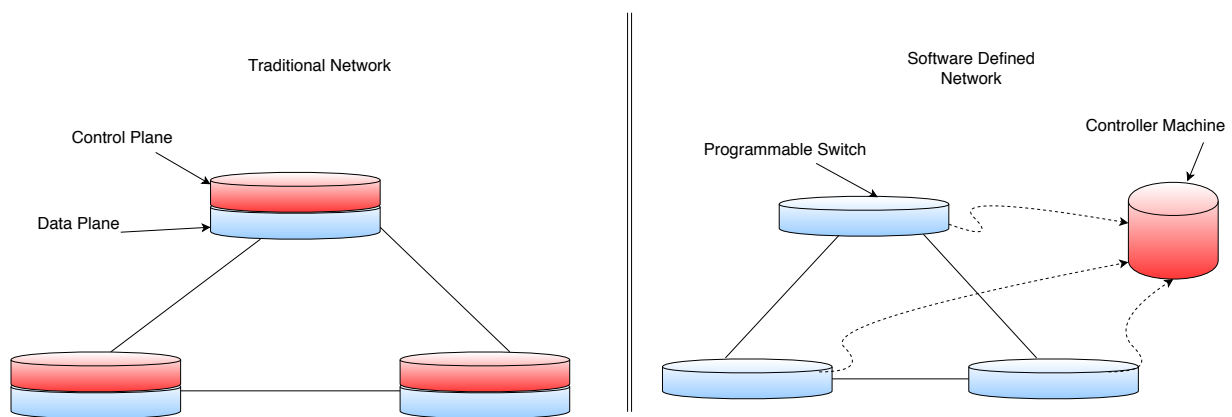


Fig. 2.11 Traditional Network Vs SDN

2.5.2 Significance of SDN

Traditional computer network consists of network devices such as routers, switches and many other middle boxes which are responsible for manipulating traffic other than packet forwarding. In such networks, the data plane and control plane are closely coupled. Many complex network protocols are implemented on them. When updating or configuring network policies, operators need to manually transform new policies to adapt to new changes. Ultimately, network management and performance turns out to be a complex and non-trivial task which tends to be error-prone [151].

In a network, the data plane is responsible for forwarding data based on the forwarding state. The control plane creates the forwarding state. When a packet comes to a router, it looks at its routing table before forwarding it to the appropriate

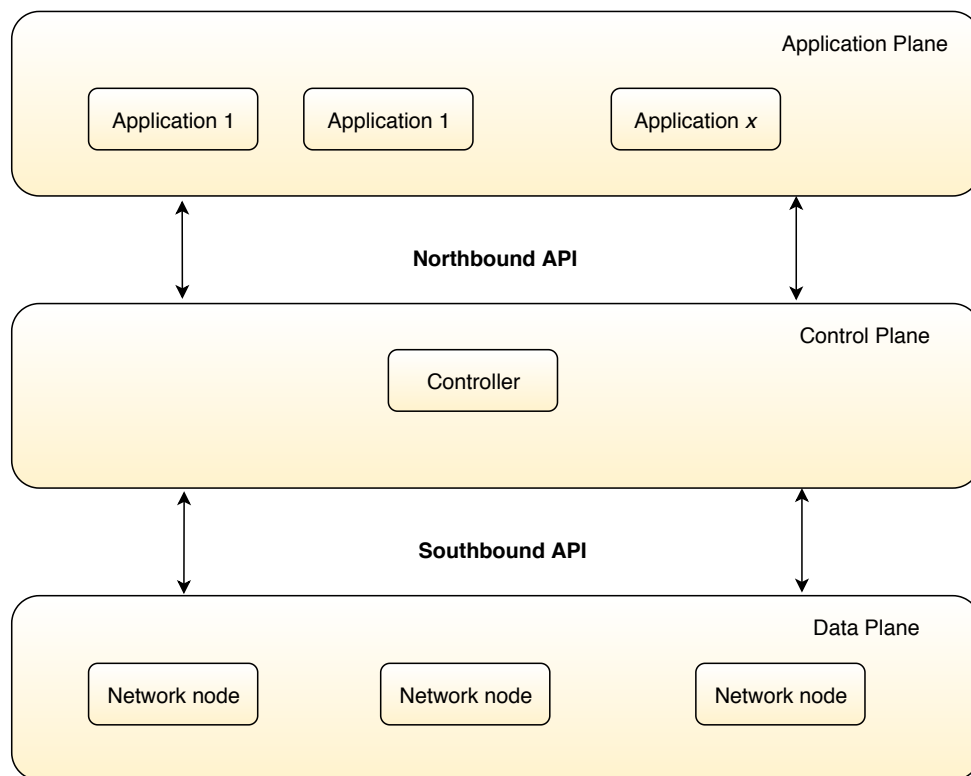


Fig. 2.12 Basic SDN Framework

destination. In a traditional network, since a data plane and control plane are combined, data flow decisions are made on board in each network element [152]. In such cases, new network deployment becomes troublesome since new network settings need to be directly implemented in the infrastructure. Therefore, it is very challenging to cope with the latest Internet applications and emerging technologies. Hence, the idea of SDN to facilitate network evolution [152]. SDN is expected to provide more programmatic control of the network data path. However, the primary objective of SDN is not to improve network performance, rather, it is to simplify network management and bring more flexibility.

2.5.3 SDN Architecture

SDN offers three layers of architecture. Fig. 2.12 [153] explains the basic SDN architecture where the three layers are: data plane, control plane and application plane.

The central controller translates the requirements from the SDN application plane to the data plane. It also provides the application plane an overview of the overall network topology including statistics and events. The communication interface between the application and control plane is referred to as the northbound API while the southbound API works as an interface between the control and data plane. The southbound API (SB API) provides programmatic control of all forwarding operations, advertisements, statistics and event notifications. On the other hand, the northbound API (NB API) provides an abstract view of the network, expression of network behavior and requirements. Applications from the application plane utilize the NB API to translate their network requirements and behavior to the SDN controller.

2.5.4 SDN Protocols and Standards

Currently, researchers are focusing improving of both NB and SB API. The standard development organizations are mentioned in [154]. Forwarding and control element separation (ForCes) and OpenFlow are the two most popular SB interface specifications. The Internet Engineering Task Force (IETF) developed ForCes. ForCes consists of two elements: the forwarding element (FE) and the control element (CE). FE handles packets while CE sends controls, signal functions and instructions regarding packet handling to FE. The logical function block (LFB) concept is used in ForCes, which has specific functions to process packets [155] and facilitate CE to control FE [151].

The OpenFlow protocol was developed by the Open Network Foundation (ONF). OpenFlow was the first protocol that allowed the direct manipulation of the data plane by the controller [155]. ONF proposed this protocol to develop and test a new control mechanism for a large network. The OpenFlow protocol defines a packet forwarding model, flow table generation and an update mechanism. This protocol institutes communication between an SDN controller and OpenFlow enabled switches. The flow table consists of flow rules that define the handling of packets. Flow entries or flow rules have three functions: match fields, counters and instructions/actions. Statistics on the packet headers, ingress port and metadata are the match identifiers [156]. The number

of packets received, the size of the packets and the duration of the flow are provided at the counters. And the instructions or actions tell what to do upon a packet match or mismatch. The flow chart (Fig. 2.13 [156]) presents a basic packet forwarding flow in OpenFlow. Whenever a packet comes to a switch, a header field is extracted and is matched against the flow table. If the flow matches, appropriate actions are taken. In the case of a flow miss, again appropriate actions are taken which are to either drop the packet or pass it to the next available controller or request a new rule for the particular packet.

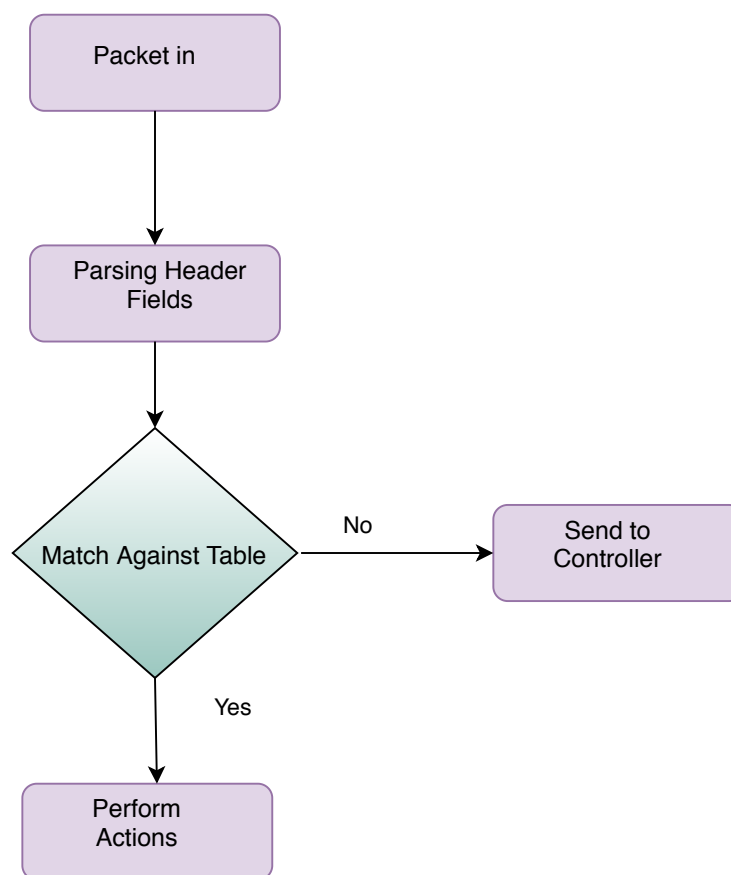


Fig. 2.13 Packet forwarding flow in OpenFlow

2.5.5 Applications of SDN

The applications of SDN are currently in existence and are also being further developed for a wide variety of fields. Some of the significant applications are briefly presented as follows.

- **SDN based Telecommunication Network-** The working principle of SDN in managing and simplifying the existing telecommunication network is of paramount importance. The addition and management of various services such as continuous subscribers' mobility, access control policy, inter-cell interference management, monitoring of network control and billing information, traffic management etc. could be backed through SDN implementation [157]. The OpenRoads project [158,159] demonstrated a backwards compatible and shareable SDN-based architecture for cellular networks which allows a seamless handover across a multiple wireless infrastructure. Some of the subsequent works related to the design of SDN-based cellular network requirements and challenges can be found in [157,160].
- **SDN-based IoT-** The significant capabilities and the opportunities of IoT applications in various sectors such as WSN, cloud computing, big data, industrial automation, healthcare etc. have augmented their rapid growth to provide diverse intelligent services. In heterogeneous IoT deployment, based on the nature of the application, QoS needs to be maintained in terms of packet loss or success, latency, jitter and bandwidth. In such cases, the SDN-based IoT implementation eases and lessens the complexity of managing heterogeneous IoT applications. A detailed discussion of SDN in IoT applications can be found in [161].
- **SDN in Edge Computing-** The technique of processing data in the proximity of users with a dense geographical distribution to support mobility to retain low latency and to provide improved QoS in heterogeneous environment is referred to as edge computing. The independently deployed heterogeneous IoT devices in the edge network come with various challenges such as unstructured data from various vendor deployed sensors and actuators, adaptation of the new technology, data collection system in a unified platform etc. [161]. One of the most appropriate solution to these challenges is to virtualize the network function and implement it in a SDN- based virtualization infrastructure [162].
- **SDN-based Data Center Networks-** The increasing demand for computing resources led to the development of data center networks. Data centers integrate

information technology and equipment to support data and the business development of organizations [163]. The common available resources such as CPUs, memory and storage are not capable or scalable to support increased network functionalities at some point [164]. Some of the important considerations in the underlying infrastructure of data centers are, energy consumption, latency and bandwidth. To deal with such issues, the integration of SDN with data center networks offers promising aspects. In early 2012, Google demonstrated a practical example by applying the SDN concept and architecture to connect data centers at the Open Network Summit [165]. Some other works related to the network productivity enhancement of data centers through SDN can be found in [166–168].

2.5.6 Research Challenges of SDN integration with WBAN

The theoretical concept of SDN is expected to reduce the complexity of network management whether it is wired or wireless. When it comes to the implementation in WBAN, it offers flexibility and programmatic control over the network. Open standards such as Openflow and ForCes simplify the network design and operations which diminishes the dependency on vendor-specific instructions and protocols as instructions and commands are provided from a controller [8]. Of the other benefits of SDN, reserving bandwidth for delay-sensitive applications [3], secure patient monitoring technique through tracking the patients locations [169], efficient and secured data delivery [7], the use of centralized routing algorithm to facilitate mobility [12], updating the routing table [170] and dynamically activating and deactivating of sensors [3] to support energy efficiency are the most significant. To leverage the potential benefits of SDN in WBAN, an SDWBAN architecture is proposed in [171]. However, incorporating SDN in WBAN experiences a few challenges. Some of the challenges are as follows:

- **WBAN Inherent Challenges:** Many of the WBAN challenges have not yet been adequately addressed,. although SDN suggests promising insights into resolving many of the current challenges of WBAN. Specially, the SDN paradigm promises a huge reduction in energy consumption by the node. However, the extent of this

claim needs to be evaluated and quantified. The amount of processing needed in proportion to energy usage should be determined. In addition, application-based energy usage must be calculated.

The aggregated sensed data is also paramount and needs closer research attention. In addition, WBAN deals with heterogeneous applications, hence, data aggregation from heterogeneous applications is also critical. This aggregation problem in heterogeneous WBAN needs to be explored.

The transmission of the data is also a major concern. It might not be pragmatic to have all sensors transmitting their raw data to the controller as this will result in excessive delay and congestion in the network. In the design, local controllers or some sink nodes could be used. However, this needs to be tested to evaluate its efficiency.

- **Implementation and Evaluation:** The idea of having SDN in WBAN is very recent. However, many researchers are proposing SDN for WBAN to provide security and authentication services. Still simulation and practical implementation need to be done. Some implementations have been successful in applying an OpenFlow standard in sensor nodes and serving it as SDN enabled switch for data plane and controller communication. However, practical implementation is needed to provide a clear indication of the progress made thus far. This would also usher in an opportunity to evaluate issues such as QoS, reliability, packet loss, bandwidth, stability, efficiency, and scalability.
- **Inter and Intra-Plane Communications:** Communication between the control plane and the application plane is important for the overall structural security of the network. Hence, any protocol considered needs to adequately address the security concerns. On the other hand, communication between the controller and the infrastructure devices, the southbound API, is also particularly important because it is the enabler of the transition from the high resourced control plane to the low resourced data plane. This transition presents an open research problem to be explored.

- **Standardization:** There is no standardized protocol available for the SDWBAN. Researchers from around the world have proposed many general frameworks. However, the lack of a standard could derail the development and further exacerbate the issue of dependent compatibility, which the SDN model seeks to avoid. Therefore, there is an urgent need for SDWBAN standardization. The lack of standardization will result in incoherent and incompatible architectures that may violate SDN's principal of heterogeneity.
- **Distributed Control System:** In order to provide scalability, reliability and performance in SDWBAN, an efficient distributed control system is needed. Distributed control solutions have been proposed for SDN enterprise networks and SDN based smart grid solutions. Hence, there is a need to investigate a novel distributed control system for SDWBAN without compromising any of the quality imperatives.

2.6 Blockchain Technology for SDWBAN

In this section, the importance and applications of blockchain technology in diverse fields of security measures with a specific focus on SDWBAN are presented.

Blockchain technology has the significance attention of researchers in the past few years. Although the technology was first used by Satoshi Nakamoto in a whitepaper [172] to explain the challenges of ownership pertaining to digital currencies, many other projects in IoTs, especially healthcare services started to use the concept of blockchain to maintain security and privacy [173]. WBAN in medical applications can benefit by employing the concept of blockchain. Specifically, a management system for various parties such as general practitioners, medical specialists, hospitals, and therapists can be supported when they need access to the same information [174]. A US-based startup, Gem Health Network [175], utilized the Ethereum Blockchain Technology [176], which offers a structural platform to allow businessmen, individuals and experts to access the latest treatment information and also enables experts to track the past history of the

patients. A real and proven example is the Estonian healthcare infrastructure which uses Guardtime Blockchain [177] to regain information on medical treatments performed in Estonia.

Wearable WBAN sensors generate a large volume of data that are important to the diagnostic process and are also a useful resource for medical research. Storing and sharing personal data is an important task. To facilitate secure data storage, a Swiss-based startup invented healthbank Blockchain which offers an individualized data trading platform to share personal data for research purposes and even shares data which can be tracked with a timestamp [178]. One of the latest studies [179] introduced BloCHIE, a blockchain based platform for health information exchange, to store a huge amount of data remotely that enhances collaborations between clinical research enterprises. Although the prospects of blockchain for WBAN seems to be attractive, it comes with a variety of challenges. Some of the crucial challenges of incorporating blockchain can be found in [180]. Some crucial aspects of integrating blockchain in WBAN are briefly discussed as follows.

- **Mutual Trust and Agreement:** It is vitally important to have trust between the participating entities such as patients, the health insurer, the medical research team and the healthcare providers. Permission to share and view the patient's private data is essential when it comes to further research into a specific disease.
- **Traffic Management:** The diverse nature of WBAN traffic demands an exclusive priority mechanism to process normal monitoring data and emergency data. Emergency data need to be addressed on a first-most priority basis so that emergency data experience a minimum amount of delay.
- **QoS:** As WBAN requires the delivery of data within a strict time frame in accordance with the specific applications, when block verification takes place by the miners, it constitutes some additional delays. As the number of patients increase, computational complexity and load increases, which ultimately effects the overall QoS of the network.

- **Data Controller:** One of the properties of blockchain is immutability, which means resistance to the modification of data. Device dysfunctions in WBAN might cause erroneous data recorded in Electronic Health Records (EHRs). Since the modification of data is not possible in blockchain, finding a data controller to deal with erroneous data is very challenging and is yet to be resolved.
- **Smart Contracts:** Generating self-executable clauses for smart contracts for different WBAN applications is very challenging because the smart contract model should be representable and quantifiable.

2.7 Summary

WBAN is an emerging field of research within the domain of healthcare. In this chapter, a review of the current research in WBANs and the recent literature on different research challenges are provided. Some of the key differences between WSN and WBAN are also discussed. Several limitations of traditional WBAN architecture are elaborated. In this context, it is essential to understand the existing architectures and limitations to address the challenges efficiently. This chapter highlights the applications of WBAN in both medical and non- medical fields. Furthermore, a taxonomy of medical and non-medical applications is provided with appropriate references. A comprehensive study on different candidate technologies for WBAN is also carried out, where the characteristics of candidate technologies are highlighted. The study emphasizes the implementation guidelines of WBAN based on the latest standard IEEE 802.15.6 which will aid future investigators, professionals and researchers. It is perceived that the successful implementation of WBAN will certainly improve quality of life, whether it is in the medical or non-medical aspect. It will reduce the costs associated with the hospitalization of patients and will assist the early detection of abnormalities. Finally, as new technologies like SDN and blockchain are emerging, incorporating these technologies with WBAN will bring revolutionary changes in the healthcare sector. It is expected that SDN and blockchain will be able to solve most of the crucial challenges of WBAN.

STATEMENT OF CONTRIBUTION TO CO-AUTHORED PUBLISHED
PAPER

The chapter 3 includes a co-authored journal paper, which has been published in Future Generation Computer Systems in 2020. The bibliographic details of the co-authored paper, including all authors, are:

- **Khalid Hasan, Khandakar Ahmed, Kamanashis Biswas, Md. Saiful Islam and Omid Ameri Sianaki**, “Software-Defined Application-Specific Traffic Management for Wireless Body Area Network”, Future Generations Computer Systems, Volume 107, 2020, Pages 274-285.

My contribution to the paper involved: Proposal of SDWBAN architecture, application classification algorithm, implementation, writing and editing manuscript.

(Signed) _____ (Date) 10/03/2020

Khalid Hasan

(Countersigned) _____ (Date) 11/03/2020

Supervisor: Md. Saiful Islam

Chapter 3

SDN-based Application-specific Traffic Management for WBAN

WBANs are usually used to collect and monitor health-related information for both critical and non-critical patients. However, the traditional WBAN communication framework is unable to guarantee the successful delivery of critical information due to a lack of administrative control and priority support for emergency data. To overcome these issues, this chapter proposes a novel SDWBAN framework for application-specific traffic management. An application classification algorithm and a packet flow mechanism are developed by incorporating SDN principles with WBAN to effectively manage complex and critical traffic in the network. Furthermore, a Sector-Based Distance (SBD) protocol is designed and utilized to facilitate the SDWBAN communication framework. Finally, the proposed SDWBAN framework is evaluated through the CASTALIA simulator in terms of Packet Delivery Ratio (PDR) and latency. The experimental outcomes show that the proposed system achieves high throughput and low latency for emergency traffic in SDWBANs.

3.1 Introduction

Health related data collected through WBAN sensors are paramount of importance in monitoring both critical and regular patients. To avoid undesirable circumstances of patients' health, it is imperative to have a system that guarantees successful transmission of emergency data to specialized healthcare entities such as doctors and emergency first aid team. However, the traditional communication frameworks of WBAN experience various challenges to maintain the QoS of patient monitoring, which intensifies with the increase of applications in the network.

One of the significant functions of WBAN is Patients data management that deals with three different types of data such as low-priority, high- priority, and data on-demand. Low priority data are regular monitoring data whereas high priority data refers to critical data when abnormalities are detected in a patient's health condition. Apart from these, health practitioners may also demand for medical data that belong to on-demand category. In traditional WBANs, there is no administrative control on data traffic as they are dependent on access mechanisms defined by different standards. Due to the lack of administrative control and static nature of WBAN sensor platforms, prioritizing emergency data over regular monitoring data in WBANs becomes a troublesome issue. It is also reflected in this chapter that how emergency applications retain low latency and high PDR in the presence of high volume of data traffic. In an emergency situation, life critical data pertaining to patient's health must have top most priority over normal data and should be sent to the healthcare providers with no or minimal delay. Therefore, it is highly important to have dynamic and flexible mechanisms and control over the devices to accommodate data linked to any undesired circumstances like death or injury. Moreover, for an optimum network lifetime, capability of dynamic resource allocation and scalable reconfiguration demand for an alternative solution with much more programmatic control over the network devices.

There has been extensive research on the development of WBAN in various aspects such as enhancement in MAC layer, traffic modelling, and energy efficiency. One of the important attributes of WBAN, reliability, is evaluated for two different body states i.e.,

standing, and running in [181]. The simulation results show that using Adaptive Transmit Power Mechanism, the PDR can be improved for a variety of body postures. However, the experimental setup was restricted to a limited number of WBAN nodes and the inclusion of emergency application was avoided. Similarly, a new transport layer protocol named Reliable Delay Sensitive Loss Recovery is developed in [182] to accommodate the real-time traffic and time-critical data. In inter-WBAN interference environment, a health criticality index has been proposed in [183] to prioritize WBAN traffic. Time slots with superior channel conditions are used in [184] to ensure transmission priority for critical traffic in WBAN. It is shown that the proposed technique achieves notable improvement in terms of QoS and energy efficiency.

In [185], a new approach to deal with emergency data has been presented which works based on a modified superframe structure of IEEE 802.15.4 MAC layer. In this paper, the average delay and throughput is improved by allocating dedicated channels for emergency and non-emergency data. However, the major limitation is that the issue of accommodating large number of applications is not considered in simulation and inefficiency could also be a big concern in utilizing resources. Similar to this paper, the authors in [186, 187] have proposed emergency data handling approaches through the modification of IEEE 802.15.4 MAC layer protocol whereas the concept of Emergency Contention Period (ECP) to transmit emergency alarm is introduced in [188]. In addition, several WBAN projects such as the CodeBlue project is designed to support emergency medical events with self-organising capability [189]. However, the project fails to ensure reliable communication since the system experiences notable packet loss due to lack of a reliable routing mechanism. Another limitation is that it works only with a limited number of applications.

In [190], the authors have proposed a cloud-assisted WBAN architecture that manages increased traffic load based on the Disease-centric Patient Group (DPG) formation process among the WBANs with specific disease type. In this paper, a pricing model and efficient mapping mechanisms are used to identify critical WBANs to optimize the expected packet delivery delay and network throughput. However, in real-life situation, the cluster formation of DPG is troublesome as the patients with

heterogeneous applications will have the liberty of mobility. Virtual queue based priority queueing has been used in [191] to support critical data of WBAN. It is shown in the study that using Load Balancing Priority Queuing mechanism is utilized to transmit critical traffic with minimum delay. The work lacks proper analysis of load balancing mechanism and the process of severity measurement for the data packets received from remote location.

To this end, the concept of SDN in IoT enabled devices especially for Body Sensors (BS) is expected to revolutionize healthcare services. An optimum level solution to many of the challenges of WBAN could be achieved by the emerging SDN paradigm [147]. One primary approach of incorporating SDN into healthcare is proposed in [192] that utilizes a centralised controller for health surveillance application with the help of Software-defined Robot. Nevertheless, the architecture lacks the detail description of SDN functionalities and priority based data traffic management i.e. emergency data. Another attempt of incorporating SDN into healthcare is described in [9] to securely monitor the patients of wandering behaviour. However, the study is limited to patient tracking and therefore overlooks the implementation of WBAN at large scale. An attempt to implement SDN based control system is introduced in [193] to manage emergency alerts in smart city environment. It is shown that by modifying the data routes of emergency and normal traffic, emergency resources could be made available in the locations of emergency event.

The aforementioned works come with the limitations of administrative control over emergency and normal data, DPG clustering technique, the elaboration of SDN functionalities, and the large number implementations of WBAN. To overcome these limitations, a robust communication framework named SDWBAN is designed that facilitates real-time patient monitoring in healthcare service. The proposed model utilizes cluster based SBD routing and prioritizes emergency data packets over normal traffic based on application classification algorithm.

In this chapter, a SDWBAN framework is proposed and implemented for heterogeneous WBAN applications by using both normal and emergency data. The SDWBAN framework implements a cluster based routing approach to route data

packets from sensor nodes to the destination. More precisely, a modified version of SBD routing protocol is devised to facilitate the packet communication mode at layer 3 [194]. In application layer, an application module named SDWBAN is developed, which adopts a packet dissemination model from the author's previous work [195] to accommodate emergency and normal data traffic. Finally, the proposed framework is implemented using CASTALIA simulator [196] and analysed the performance of the framework in terms of PDR and latency. The key points of this chapter include the followings:

- A flexible and scalable SDWBAN framework that provides dynamic control over the network with growing number of applications.
- An efficient application classification algorithm to support various applications in WBANs.
- A modified version of SBD routing protocol to facilitate the SDWBAN communication framework.
- Implementation and evaluation of the proposed framework using CASTALIA simulator.

3.2 Traditional WBAN vs SDWBAN Architecture

In this section, a short overview of the working principles of traditional WBAN architecture and SDWBAN architecture is presented. In addition, an architectural view of traditional WBAN vs SDWBAN is presented to demonstrate the transformation from the conventional system to the proposed system as illustrated in Fig.3.1.

3.2.1 Traditional WBAN

In general, WBAN architecture presents a three layer communication system where all BSs are located in the first layer. The BS senses physiological data according to predefined

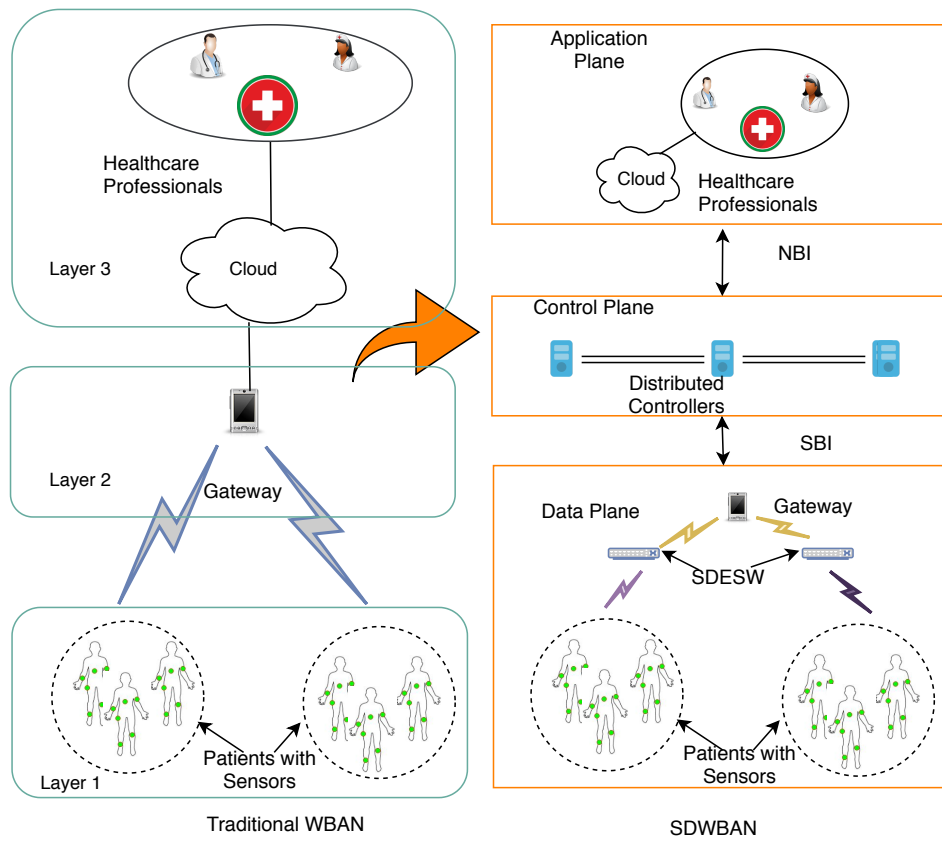


Fig. 3.1 Traditional WBAN vs SDN based WBAN

command and periodically transmits the information to a gateway. The gateway resides at the second layer of hierarchy and the communication interface between gateway and sensors utilizes short-range technologies such as Bluetooth, ZigBee, IEEE 802.15.6 etc to transmit and receive information. Any resourceful device such as Personal Digital Array (PDA), mobile phone may work as a gateway. After collecting physiological data from the BS, the gateway sends the data to the next layer using long-range technologies such as WiFi, WiMax, LTE, LTE-A etc. The cloud system works at layer three which enables the healthcare providers to access and monitor their concerned patients.

3.2.2 SDN-based WBAN (SDWBAN)

Although researchers have proposed a number of models to integrate SDN with WBANs, a standard architecture for SDWBAN is yet to be defined. A few conceptual works regarding the deployment of SDN in healthcare and particularly in WBAN can be

Table 3.1 SDWBAN Components

Components	Task	Layer
Body Sensor	Senses physiological data and sends to the SDESW	Data Plane
SDESW	SDN enabled switch communicates with controllers to retrieve flow information	Data Plane
Gateway	Receives data from SDESW and connects to cloud	Data Plane
SBI	Interface between control plane and data plane. Capable of all programmatic control of all forwarding operations, statistics and events notifications.	Between Control and Data Plane
Distributed Controllers	Multiple controllers reside in control plane. Maintain a communication with SDESW. Captures overall view of the network.	Control Plane
NBI	Interface between control and application plane. Applications from application plane use NBI to translate their network requirements and behaviour to the SDN controllers.	Between Control and Application Plane
Applications	Healthcare professionals can monitor their patients, define, install, operate and manage new WBAN application sets	Application Plane

found in [7, 11, 197]. In [195], a novel architecture for SDWBAN has been proposed that consists of three planes such as data plane, control plane and application plane. The data plane consists of BSs, gateways and SDN enabled switches (SDESW), where the switches receive control information from the control plane. In the data plane, a group of patients attached with sensors may form a cluster and share a common SDESW. The BSs transmit physiological data at a regular interval to the associated SDESW to reach to the destination. However the associated SDESW can directly transmit data to the destination gateway if the gateway is within the transmission range of the SDESW. Otherwise, packets are forwarded in a hop-by-hop fashion through multiple SDESWs until they reach to the destination. On the other hand, the control plane consists of multiple distributed controllers that can be in operation in a network. For east-west communication, these distributed controllers can be inter-connected so that in case of failure of any controller, another nearby controller can support the SDESWs. In the application plane, the management authority can define and install various WBAN applications to monitor patients. The communication interface between the application and the control plane is referred as Northbound Interface (NBI) while the Southbound Interface (SBI) works as an interface between control and data planes. A summary of the SDWBAN components is provided in Table 3.1.

The detailed explanation of SDWBAN communication architecture including packet dissemination model could be found in [195]. The proposed architecture presents multiple number of SDN-enabled Switches (SDESWs), gateways and controllers. In case of system

failure, the network can be supported by the neighbouring nodes. For instance, if a controller fails, another controller would require to cater for more number of SDEWSs. This might cause a little delay to re-establish the communication between controller and SDESWS. And if a SDESW fails while forwarding packet towards destination, next available SDESW can serve the purpose and forward to destination in multi-hop fashion. In case of failure of SDESW, WBAN sensors become orphaned and then they need to associate themselves with the next available SDESW based on the rank number.

3.3 SBD for SDWBAN

To support the proposed SDWBAN framework, a modified version of SBD routing protocol [194] is formed. The sector-based routing divides the network into multiple sectors where there is a sector head (SH) in each sector. The SH works as an SDESW where the SDN functionalities are implemented to retrieve control information from the controllers. Based on the control information, the SDESW routes the data packets to the appropriate destination. The SDESW is a static node which resides in the vicinity of patients' bed or in a room and multiple sensors from a sector can share a common SDESW. However, association with the SDESW is not fixed as it changes when the patients move around in the neighbourhood. This feature supports mobility issues of WBAN. The SBD routing function is split into rounds that consist of two phases: learning phase and relaying phase.

3.3.1 Learning Phase

In this phase, BSs associate themselves with the corresponding SDESW. The BSs periodically receive a beacon from the neighboring SDESWs. As they receive the beacon periodically, in the learning phase they can associate themselves with the appropriate SDESW. The BS-SDESW association begins with receiving beacons from nearby SDESWs as defined in Algorithm 3.1. Each BS assesses the received signal

Algorithm 3.1 Beacon Dissemination Process**Input:** Beacon frame**Output:** Null

-
- 1: *Network layer packet construction, beacon_ctr_pk*
 - 2: *// Assigning packet type and source id*
 - 3: *Packet_tp = 1 in network layer packet*
 - 4: *Source_id = Self_Net_Add and -1 as destination in beacon_ctr_pk*
 - 5: *Broadcast beacon_ctr_pk*
 - 6: *toMacLayer (beacon_ctr_pk, Broadcast_Net_Add)*
-

strength indicator (RSSI) and organises them into a vector $v(SDESW_i, RSSI_i)$, where $RSSI_i \geq RSSI_{i+1}$. However, RSSI does not guarantee to find the closest SDESW with which to be associated. Other environmental factors such as noise, fading, and attenuation are also important parameters to be taken into account. Therefore, we consider round trip time (RTT) to select the associated SDESW in the proposed model. To compute RTT, each BS sends a request packet to all nearby SDESWs and asks for immediate acknowledgement. Once the acknowledgement is received, the BS calculates the distance of the corresponding SDESW using the time of flight (TOF) principle. The BS then assigns a rank number for each nearby SDESW based on the RSSI and TOF values and associates itself with the appropriate SDESW. The TOF can be calculated by the following equation [198]:

$$T_{TOF} = \frac{T_{RTT} - T_{TPP}}{2} \quad (3.1)$$

Here, T_{TPP} denotes Time to Process Packet.

The distance between two nodes can be calculated as follows:

$$d_{RTT} = T_{TOF} \times c \quad (3.2)$$

Here, c is the speed of light. According to [199], equation 3.2 can be further extended by incorporating the faultiness factors involved in distance measurement as follows:

$$d_{RTT} = T_{TOF} \times c + \varepsilon_{RTT}^{LOS} + \varepsilon_{RTT}^{NLOS} \quad (3.3)$$

In real environments, particularly in the case of WBANs, sensors can be located on different parts of the body. Moreover, due to the various postures and movements of the body, signal propagation from sensors faces obstacles such as various objects located in the patient's surroundings and sometimes even patient body. Ultimately, the issue of line of Sight (LOS) and Non-line of Sight (NLOS) occurs. As can be seen, the above equation includes two fault components: ε_{RTT}^{LOS} and ε_{RTT}^{NLOS} . The ε_{RTT}^{LOS} refers to the LOS setting whereas ε_{RTT}^{NLOS} occurs due to a ranging in NLOS settings. The faultiness of the multipath effect (i.e. the obstruction of signals) of ε_{RTT}^{NLOS} can be reduced using the empirical approach described in [200] in order to calculate the accurate d_{RTT} . On the other hand, hardware related noise and uncertainties especially jitter contributes to the error component ε_{RTT}^{LOS} . Therefore, considering the jitter effect, T_{TOF} can be calculated as [201]:

$$T_{TOF} = \frac{T_{RTT} - (J_{t1} + J_{c1} + T_{TPP} + J_{c2} + J_{t2})}{2} \quad (3.4)$$

For the accurate calculation of the time between sending the initial packet and receiving the acknowledgement packet by the sender node, two timestamps are used. One contains the jitters J_{t0} , J_{c0} , J_{t3} , and J_{c3} . Similarly, on the other end, two timestamps are used to calculate the time between receiving a packet and sending the first bit of the acknowledgement where the jitter values are J_{t1} , J_{c1} , J_{t2} , and J_{c2} . The measured T_{RTT} is estimated as follows:

$$T_{RTT} = J_{t0} + J_{c0} + TOF_R + TOF_A + J_{t3} + J_{c3} + T_{TPP} \quad (3.5)$$

In equation 3.4 & 3.5,

- TOF_R = TOF for the request packet,
- TOF_A = TOF for the acknowledgement packet,
- J_{tK} = jitter caused by clock of transceiver, $[K=0,1,2,3]$
- J_{cK} = jitter caused by the clock of microcontroller

Algorithm 3.2 The SDESW Selection Procedure

Input: $rank, SDESW_IDs$ **Output:** Null

- 1: *Sort SDESW_IDs in descending order based on rank*
 - 2: *Create network layer packet assoc_ctr_pk*
 - 3: *Select dst_SDESW = top element from SDESW_IDs*
 - 4: *Set Self_Net_Add as source, dst_SDESW as destination and Packet_type = 2 to assoc_ctr_pk*
 - 5: *// Unicast association request to the closest SDESW_node*
 - 6: *toMacLayer(assoc_ctr_pk)*
-

On the basis of RSSI and TOF values, the BSs calculate the rank of the corresponding SDESWs using the following equation:

$$rank_i = \left(\frac{RSSI_i}{\max_{i=1}^M (RSSI_i)} \right) + \left(\frac{d_{RTTi}}{\max_{i=1}^M (d_{RTTi})} \right)^{-1} \quad (3.6)$$

Now, every BS sends an association request to the SDESW which has the highest rank in its list. Equation 3.6 finds the highest rank for the node with the maximum RSSI and minimum d_{RTT} between two nodes. The inverse operation of finding the maximum rank between two nodes occur because, the node with the minimum distance will receive the highest rank value. Algorithm 3.2 presents the steps involved in this process. Upon receiving the association request from the BSs, SDESW creates a list of BSs and assigns the conflict free time division multiple access (TDMA) frame slot to the BSs.

3.3.2 Relaying Phase

After receiving the data from the associated BS, the SDESW forwards the data packet to the destination in a multi-hop fashion. The associated SDESW knows the co-ordinate of the neighbouring SDESWs and selects a neighbouring node that is the minimum distance to the destination. However, if the destination node is within the communication range of the SDESW, it can transmit the data packet directly. The next hop selection process in relaying phase follows the steps presented in Algorithm 3.3.

According to Algorithm 3.3, all the neighbouring SDESWs (including the associated

Algorithm 3.3 Next Hop Selection Process

Input: Target switch $SDESW_i$ where $SDESW_i \in [1 \dots s]$
Output: Next hop $SDESW_k$, where $SDESW_k \in [1 \dots s]$

- 1: **procedure** FINDING(position of destination Gateway (GW) and current co-ordinate in the grid.)
- 2: $destCo \leftarrow$ Co-ordinate of $GW, (x, y, z)$
- 3: $CurCo \leftarrow$ Co-ordinate of associated $SDESW, (x_0, y_0, z_0)$
- 4: $Co_Neigh_i \leftarrow$ Co-ordinate of neighbouring $SDESW(x_i, y_i, z_i, \dots, x_n, y_n, z_n)$ where, $i = 1, 2, 3, \dots, n$
- 5: Calculate distance, t_dist from all neighbouring $SDESW$ to GW by Euclidean system
- 6: Sort t_dist in ascending order into a vector, $t_dist = [d_1, d_2, d_3, \dots, d_n]$
- 7: Select minimum distance from t_dist and corresponding $SDESW$
- 8: **if** $destCo \neq$ co-ordinate of selected $SDESW$ **then**
- 9: Return $SDESW_k$
- 10: Move the packet to $SDESW_k$
- 11: Repeat step 4 to 8
- 12: **else**
- 13: Move the packet to the GW
- 14: **end if**
- 15: **end procedure**

SDESW) calculate the Euclidean distance to the gateway. The associated SDESW sorts all the distances and then forwards the packet to its immediate neighbouring SDESW which is the minimum distance to the gateway. This process continues until the packet reaches its destination.

Fig. 3.2 illustrates the packet forwarding process from the associated SDESW to the gateway. As shown in the Fig. 3.2, sector (0) indicates the associated SDESW's location whereas the destination node is located in sector (15). There can be different routes to send the packet to the destination, as shown in the figure with the solid and dotted lines. It can be seen that, the possible routes for data transmission in the given scenario are as follows:

1. (0) \rightarrow (1) \rightarrow (2) \rightarrow (3) \rightarrow (9) \rightarrow (12) \rightarrow (15)
2. (0) \rightarrow (7) \rightarrow (8) \rightarrow (11) \rightarrow (15)
3. (0) \rightarrow (7) \rightarrow (8) \rightarrow (9) \rightarrow (12) \rightarrow (15)

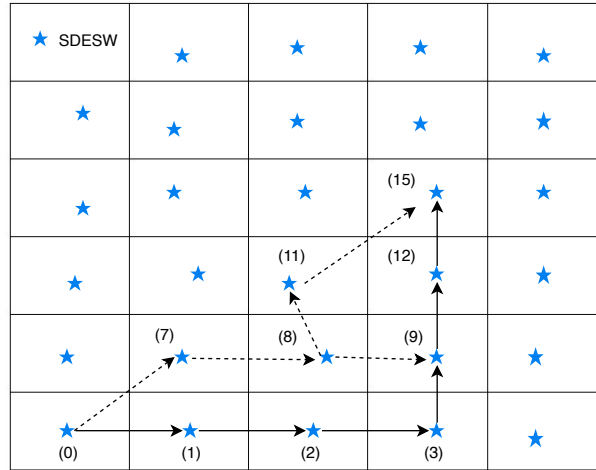


Fig. 3.2 SBD Route

However, according to Algorithm 3.3, the packet will be forwarded through the shortest possible route calculated on the basis of Euclidean distance. In this case, the shortest path is: $(0) \rightarrow (7) \rightarrow (8) \rightarrow (11) \rightarrow (15)$ and all packets will be forwarded through this path as long as the route is available.

3.4 The SDWBAN communication framework

In this section, the communication model of the proposed SDWBAN framework is presented, which includes an application classification algorithm and packet flow mechanism.

3.4.1 Communication Model

As clusters form in different sectors, the BSs located in every sector send data to their corresponding SDESWs. The SDESW then classifies the received data packet according to the predefined application IDs and checks if it is a normal data packet or an emergency application. Then the data packet is assigned an application and priority-based ID for processing. It should be noted that emergency data packets are given priority over normal data packets. In the case of an emergency data packets, all

SDESWs are also informed immediately regarding the emergency packets by the controller. After application classification and prioritization, the flow table look-up task is performed. If there is a match found at SDESW, packets are queued in the immediate buffer and then forwarded to the destination. However, if no match is found in the flow table, that particular packet is sent to the queue in the unresolved buffer. The SDESW then generates a packet.in request to the controller requesting for a flow command or asking instructions for the unmatched packet. The controller sends new flow commands or instructions in reply to the packet.in request. Note that the flow commands can be modelled in such a way that SDESW can unicast, multicast or broadcast the packet based on the WBAN applications. The flow chart shown in Fig. 3.3 demonstrates the packet flow process through the SDESW.

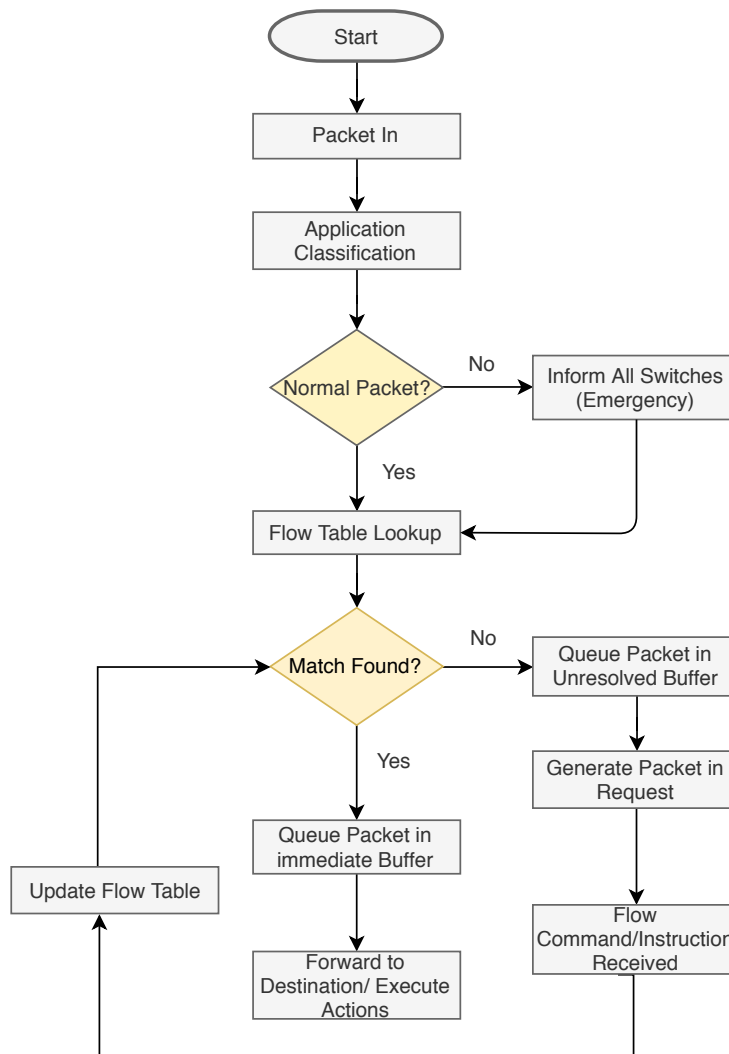


Fig. 3.3 Packet Flow

Algorithm 3.4 Application Classification Module**Input:** application_ID**Output:** Null

```

1: procedure APPCLASSIFICATION(
   SDWBAN_gen_pkt)
2:   classification_result ←
   classify_pkt(SDWBAN_gen_pkt)
3:   if classification_result ≠ normal then
4:     inform_emergency()
5:   end if
6:   lookup_result ← lookup_flow_table
   (classification_result)
7:   if match = True then
8:     queue_pkt_immediate_buffer()
9:     execute_actions()
10:  else
11:    queue_pkt_unresolved_buffer()
12:    pkt_in_req
13:    received_instruction()
14:    update_flow_table()
15:    Go To Step 7
16:  end if
17: end procedure

```

3.4.2 Application Classification Module

Usually, the BSs unicast data packets to their corresponding switches. Fig. 3.4 presents the format of a unicast packet at the application layer. Upon arrival of the SDWBAN_app_pkt, the switch identifies the corresponding application of the packet using the application classification module (Algorithm 3.4).

Packet ID	Source ID	Destination ID	Data Packet
-----------	-----------	----------------	-------------

Fig. 3.4 SDWBAN_gen_pkt

At this stage, the application name and ID are added to the incoming packet as shown in Fig. 3.5. After classifying the packet according to the application name and ID, the processing priority is checked, and a priority-ID is added to the packet as illustrated in Fig. 3.7 (a). Then, the switch performs flow table look-up task. When a flow is found, the related actions corresponding to this flow are performed. In the case of flow miss, the switch sends the packet to the queue of an unresolved buffer. After this, a control packet is generated, which is called the “packet_in_request” and is sent to the controller only with the packet header fields (see Fig. 3.7 (b)). The controller receives the packet and replies

with the “packet_out_response” which contains the flow command to be implemented by the switch. Fig. 3.7 (c) presents the SDWBAN_app_pkt including new flow command attached by the controller.

Packet ID	Source ID	Destination ID	Application ID	Application Name	Data Packet
-----------	-----------	----------------	----------------	------------------	-------------

Fig. 3.5 SDWBAN_app_pkt

Packet ID	Source ID	Destination ID	Application ID	Application Name	Priority ID	Data Packet
-----------	-----------	----------------	----------------	------------------	-------------	-------------

Fig. 3.6 SDWBAN_app_pkt with priority ID

Packet ID	Source ID	Destination ID	Application ID	Application Name	Priority ID	Source Switch ID	Destination Controller ID
-----------	-----------	----------------	----------------	------------------	-------------	------------------	---------------------------

Fig. 3.7 SDWBAN_Ctrl_pkt with packet header

Packet ID	Source ID	Destination ID	Application ID	Application Name	Source Switch ID	Destination Controller ID	Actions
							Forward/Drop/Unicast/Broadcast

Fig. 3.8 SDWBAN_Cntrl_pkt_cmd

3.5 Performance Analysis

This section provides the implementation scenario and discusses the experimental outcomes in terms of PDR and delay.

3.5.1 Implementation Scenario

The proposed SDWBAN architecture is simulated in a rectangular grid of 5x5 building blocks model where each block represents a sector. The network field size is $75 \times 75 \text{ m}^2$, where BSs are deployed randomly in the whole network area. These BSs associate themselves with an appropriate SDESW and thus form a number of clusters. We deploy the SDESWs in a static fashion in each sector of the 5x5 grid and the gateways are positioned in such a way that multiple SDESWs can share a single gateway. The distributed controller is statically deployed in a 2x2 grid, where a single distributed

controller supports multiple SDESWs from multiple sectors. Fig. 3.9 depicts the implementation scenario where, the dotted circle demonstrates the cluster under SDESW and the dotted arrow represents the destination gateway. The simulation parameters are given in Table 5.1. The path loss exponent has different values based on the environment. Typically, the value of the exponent ranges from 2 to 4. As we have considered an indoor wireless environment, the measured path loss exponent value in the indoor propagation environment is selected as 2.4. Anderson et al. further explained indoor wireless propagation characteristics in [202].

The potential application of this work could be in various sectors. In particularly healthcare sector, an elderly home where the different sensors are attached to patients' body for the purpose of measuring physiological parameter. Patients equipped with WBAN sensors in the same room could form a cluster and transmit data to the nearby SDESW. Various kinds of WBAN application sensors such as ECG, blood pressure, and temperature etc., generate valuable physiological data periodically. Depending on the physiological condition of the patients, the applications can be categorized as either normal or emergency applications. For instance, a particular application could be categorized as an emergency application, when the measured parameter seems to be abnormal based on a pre-defined threshold value.

3.5.2 Results and Discussion

The simulation is built on Castalia-3.2 version [203] on Ubuntu 16.04.4 where Castalia simulator is extended by adding two modules namely SDWBAN and SBD routing. The experiment is conducted for 100 iterations to realize the output in a number of ways such as average, median and 95% confidence interval. The PDR and latency are experimented and analysed against a varying number of applications. The PDR provides the percentage of successful packet delivery for the proposed SDWBAN framework for different number of applications. On the other hand, latency shows the time difference between the packet generation and resolution by an application. The PDR can be defined as follows:

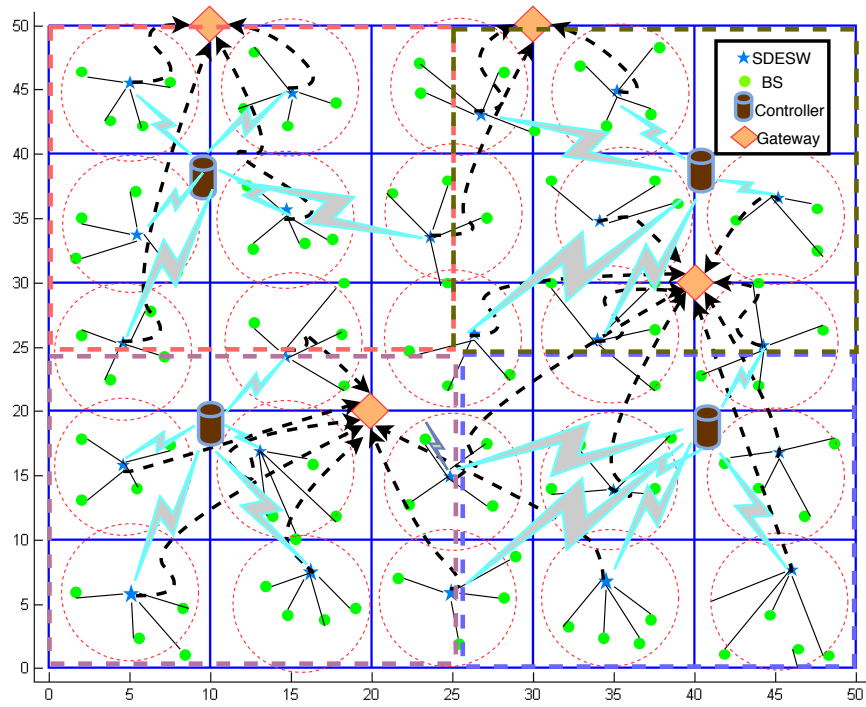


Fig. 3.9 Implementation Scenario

$$\text{PDR} = \frac{\text{No. of Packets Resolved}}{\text{No. of Packets Transmitted}} \quad (3.7)$$

In the simulation work, four different kinds of WBAN application such as blood flow, blood pressure, body temperature, and blood pH have been used. The physiological data transmission system of these applications have been cloned in the simulation. These sensors generate packets at different sampling interval. For instance, the sample inter-arrival time of body temperature is 5 sec whereas the sample inter-arrival time of blood pressure sensor is 0.01 sec [204]. Throughout group 1 to 5, different application IDs are assigned in each group so that the system treats all these different IDs as a new application. The simulation results are presented in two different scenarios. Both scenarios are presented in the following sub-sections.

Table 3.2 Simulation Parameters

Parameter	Value
Simulation Area	75x75 m ²
Number of BS, Gateway	100, 4
BS density	4 nodes/225 m ²
Total SDESW	25 (1 node per sector)
Total Controller	4 (2x2 grid)
Radio range (BS, SDESW, Controller)	~8 m, ~20 m, ~20 m
Transmission Power (SDESW, BS)	0 dBm, -10 dBm
Data Rate, Modulation Type, Bits Per Symbol, Bandwidth	250 Kbps, PSK, 4, 20 MHz,
Noise Bandwidth, Noise Floor, Sensitivity	194 MHz, -100 dBm, -95 dBm
Free Space Path Loss exponent	2.4
Initial Average Path Loss ($PL(d_0)$)	55 dB
Reference Distance (d_0)	1 m
Gaussian Zero-Mean Random Variable (X)	4.0
Number of Clusters	25

3.5.2.1 Scenario 1

In the first scenario, the traffics for different number of applications are generated and the PDR is observed against simulation time. The applications are grouped according to Table 3.3.

Table 3.3 Scenario 1 Group

Group	No of Applications
Group1	1
Group2	5
Group3	10
Group4	15
Group5	20

Scenario1_PDR: The simulation time was set to 60 minute in order to ensure a steady state result and as the output of the simulation follows a random distribution and the CDF is carried out, the 60 minute simulation time is considered to verify the standard deviation and variance in the result. The PDR is observed for different application groups at different time interval. During the simulation, the packet generation rate are

kept the same for each application group. As it can be seen from Fig. 3.10(a), the PDR decreases over the time as the number of applications increases. Significant differences can be observed from the PDR of group 4 and 5, as in group 4 the PDR is around 90% whereas for group 5 the PDR comes down to 84%. This is because, as the number of applications increases, SDESW to controller communication increases and thus the traffic load. Consequently, it results in more packets being dropped in the largest number of applications, i.e., group 5. For further analysis, the average PDR of each application group with 95th and 5th percentile are presented in Fig. 3.10 (b) and Cumulative Distribution Function (CDF) of PDR is presented in Fig. 3.10 (c). The both figures summarize the results of Fig. 3.10(a) and indicates that packet dropping rate increases as the network becomes more complex with more applications. For instance, at 90th percentile point of Fig. 3.10 (c), PDR of the group 1 is more than 95% and the PDR of group 5 is above 85%. The result demonstrates that any packet of group 1 at 90th percentile has 95% probability to be delivered successfully whereas, 5% probability to be dropped. Similarly, any packet of group 5 at 90th percentile, has 85% probability to be delivered successfully whereas, 15% probability to be dropped.

Scenario1_Latency: In this part, an analysis is carried out to measure the latency of each application group through the same experimental setup used in the PDR analysis. It can be seen that as the number of applications grows, the latency increases (Fig. 3.11). This is due to the increased number of control packets between SDESW and controller for different number of applications. In Fig. 3.11, latency of group 1, 2 and 3 ranges roughly from 20 ms to 60 ms while the latency group 4 and 5 results in between 60 to 120ms. More distinguishable points can be observed in Fig. 3.11(b)& Fig. 3.11 (c). The CDF of latency in Fig. 3.11 (c) at 90th percentile point exhibits latency of 30 ms for group 1 whereas 110 ms of latency occurs in case of group 5. This further demonstrates that any packet of group 1 has 90% probability to be delivered within 30 ms whereas, 10% of the time may not be delivered within 30 ms. Similarly, any packet of group 5 has 90% probability to be delivered within 110 ms whereas, 10% of the time, the packets may not reach within 110 ms.

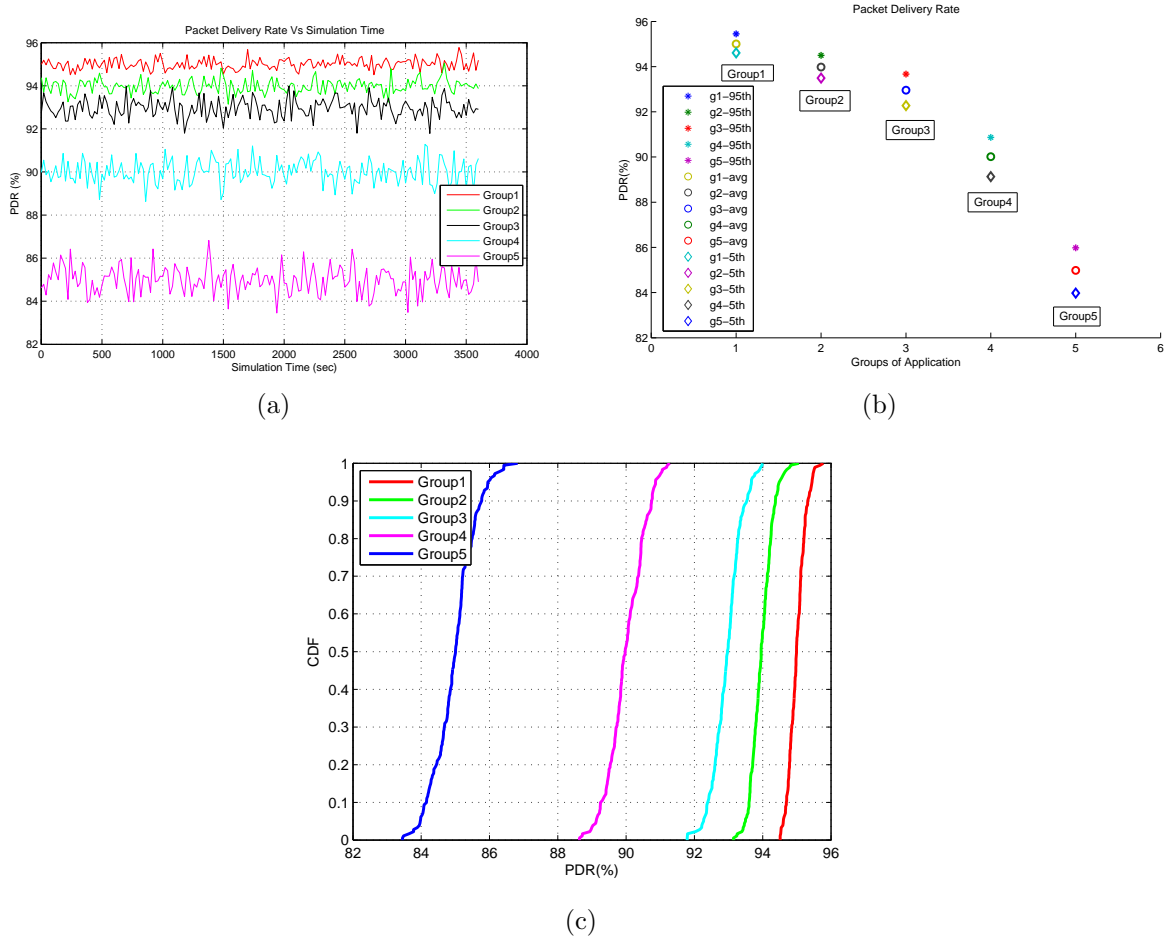


Fig. 3.10 (a) PDR VS Simulation Time, (b) PDR VS Group of Application (95_AVG_5th Percentile graph), (c) CDF of PDR

3.5.2.2 Scenario2

In this part of the experiment, emergency and normal applications are introduced. Therefore, the applications are grouped in a heterogeneous style where in each group, at least one normal and one emergency application are present. The number of applications is increased in various groups and more emergency applications are allocated to visualize the priority of emergency applications based on our proposed algorithm. The applications are grouped according to Table 3.4.

Scenario2_PDR: The simulation was run again for 60 minutes and the PDR for different group of applications are analysed and illustrated in Fig.3.12.

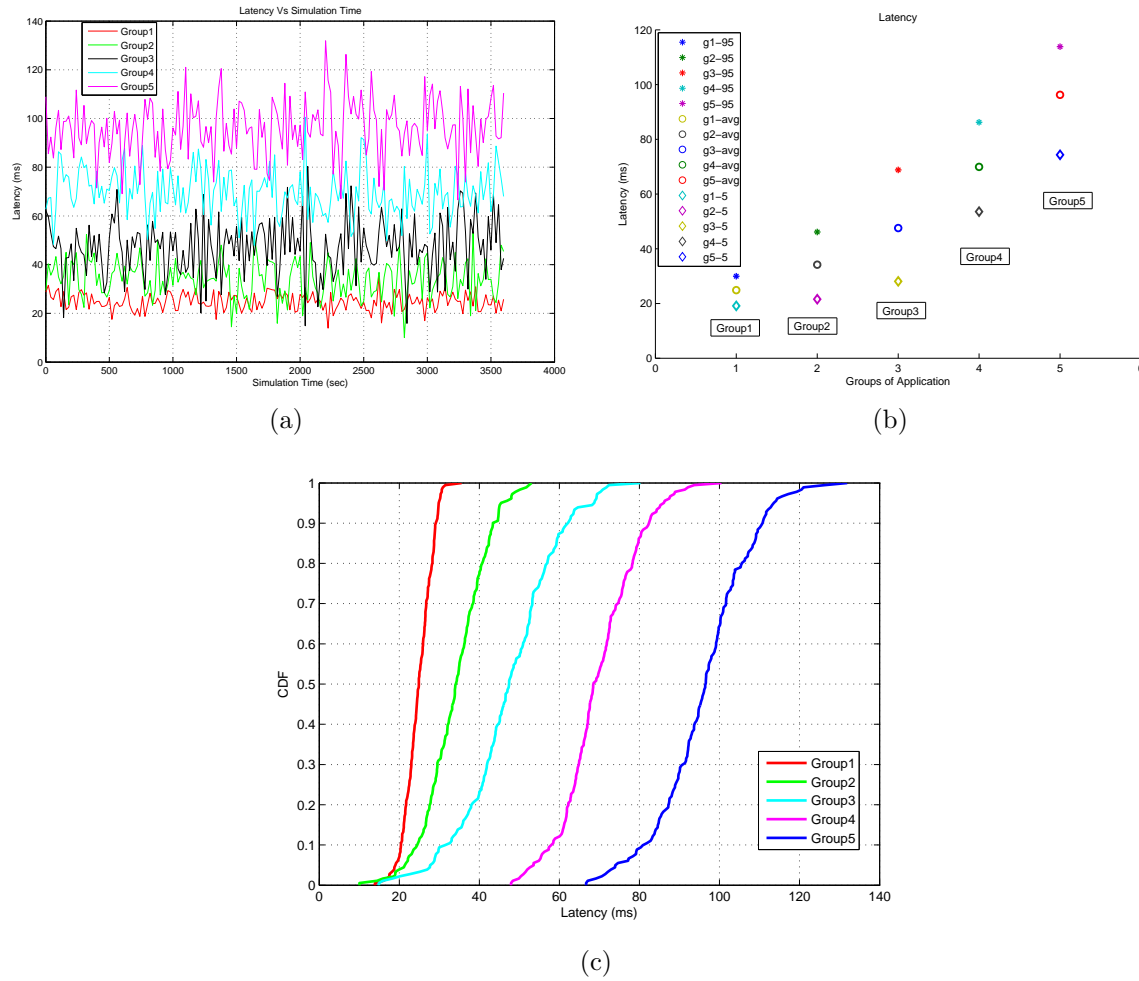
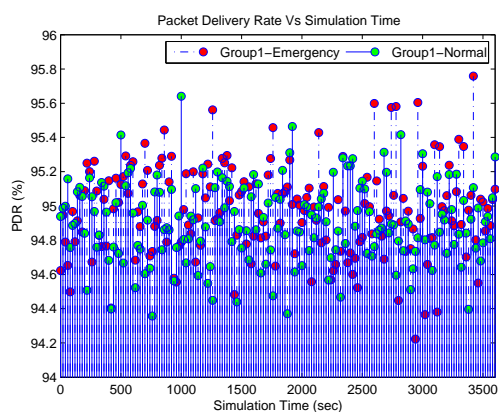


Fig. 3.11 (a) Latency VS Simulation Time, (b) Latency VS Group of Application (95_AVG.5th Percentile graph), (c) CDF of Latency

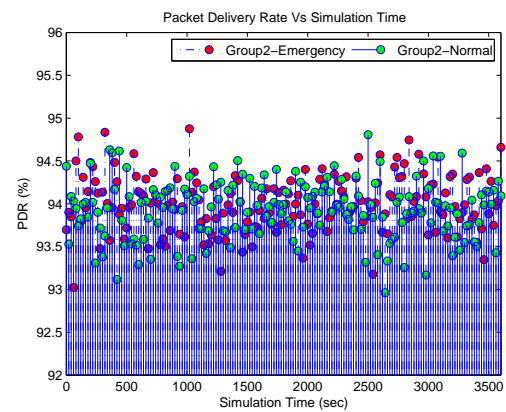
Table 3.4 Scenario 2 Group

Group	Normal Applications	Emergency Applications
Group1	1	1
Group2	2	3
Group3	4	6
Group4	7	8
Group5	10	10

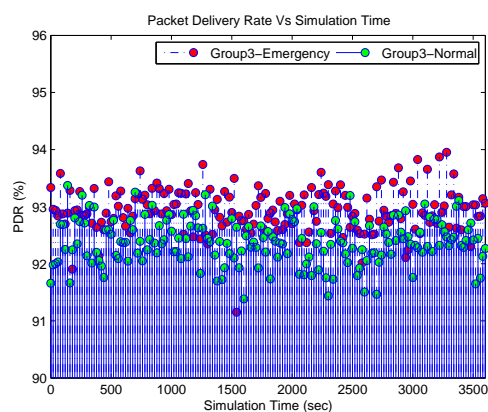
Fig. 3.12 depicts the PDR of various heterogeneous application groups over the simulation period. The Fig. 3.12(a) & (b) show the PDR versus simulation time results, where significant difference between emergency and normal applications cannot be interpreted clearly as the number of both emergency and normal application is low. This does not incur quantifiable amount of traffic between controller and SDN



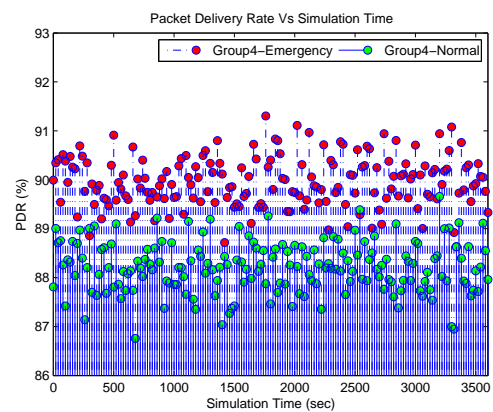
(a) Group1



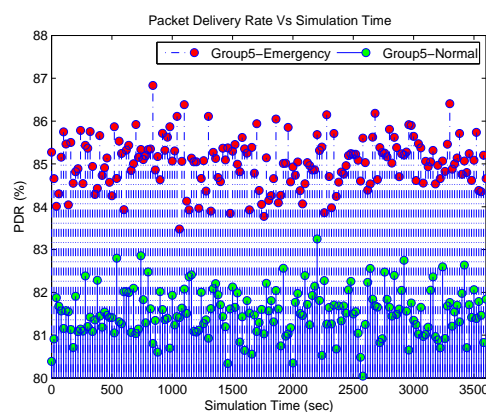
(b) Group2



(c) Group3



(d) Group4



(e) Group5

Fig. 3.12 PDR VS Simulation Time (Group 1-5)

communication. Therefore, the PDR in case of group 1 and group 2 output in similar percentage. However, it can be seen from Fig. 3.12(c-e) that the PDR of emergency

applications is always higher than the normal applications. This is because whenever emergency application is detected at the SDESW, emergency data packet is resolved immediately due to its priority. Although, the PDR decreases with the increase in the number of applications in each group, but the PDR of emergency applications is always higher than the normal applications. Further analysis of the results as shown in Fig. 3.13(a) & (b), where both of the graphs clearly present that the PDR of emergency applications exceeds the PDR of normal applications as the number of applications

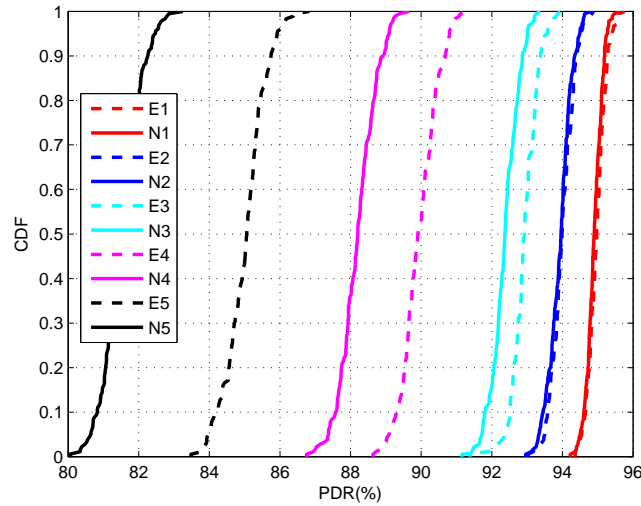
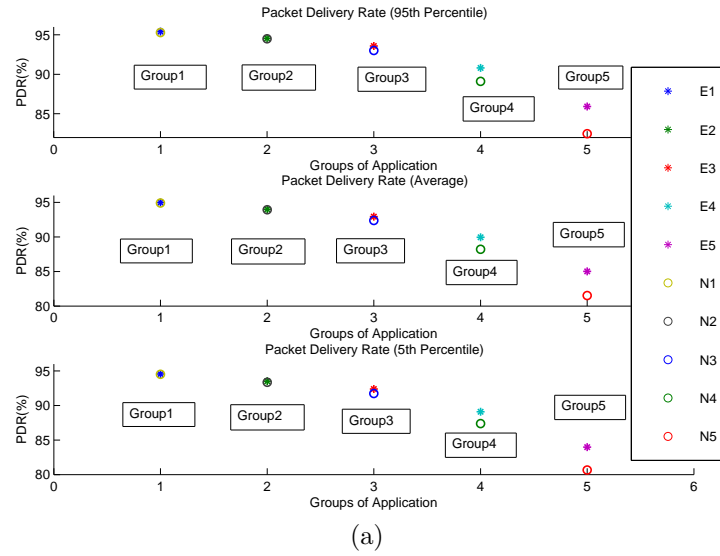
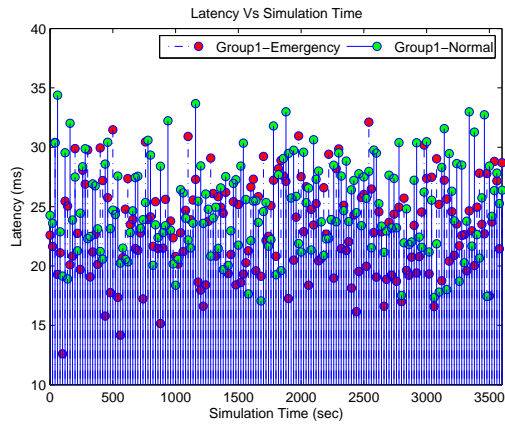


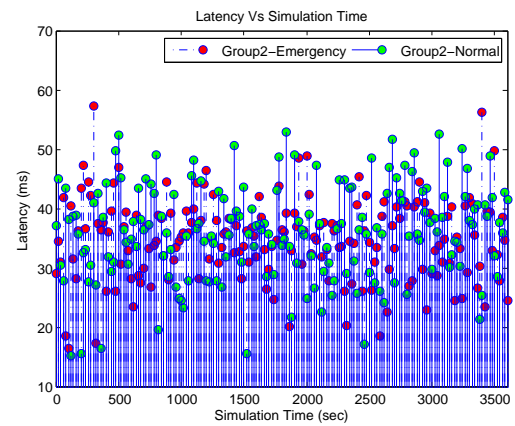
Fig. 3.13 (a) PDR VS Group of Application (95th percentile, Average & 5th Percentile), (b) CDF of PDR for each group

increases in different groups. The experimental outcomes prove that incorporating SDN into WBAN would make the network more flexible in terms of giving priority to life critical traffic even if the number of applications increases over the time.

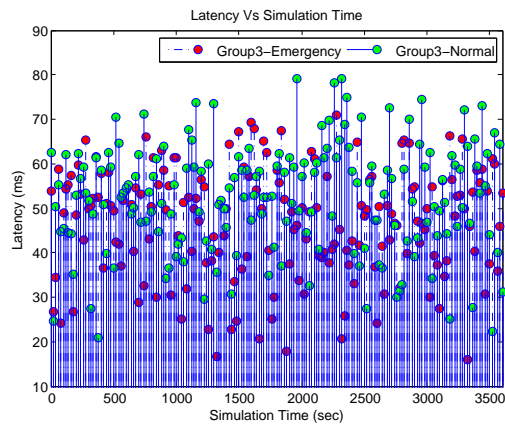
Scenario2_Latency: Here, the latency of all application groups are analysed like the previous experiment. First, the latency of emergency and normal applications are inspected over the simulation time. Fig.3.14 shows the latency incurred in over 60 minutes time. It can be seen that the latency of normal and emergency applications remain the same for group 1 and group 2 as shown in Fig. 3.14. However, for group 3 to 5, latency of normal applications started to rise whereas the latency of emergency applications shows a reduction. In order to have more clear analysis of our results, average latency is also plotted, 95th & 5th percentile as presented in Fig. 3.15(a) & (b). The application group 5 in Fig. 3.15(b) shows that at 90th percentile point emergency applications (E5) experiences around 98 ms latency while the normal applications (N5) experiences around 112 ms. This further determines that, 90% of the time, data packets of emergency application are delivered within 98 ms while 10% of the time packets may not be delivered within 98 ms. Similarly, 90% of the time data packets from normal applications has the probability to reach destination within 112 ms while, 10% of the time, packets may not reach within this time frame. The result obtained for scenario 2 supports the design goals of the proposed SDWBAN framework as it shows that the latency of emergency traffic is less than the normal traffic.



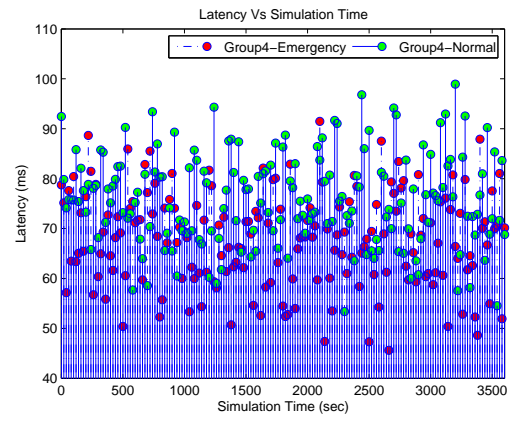
(a) Group1



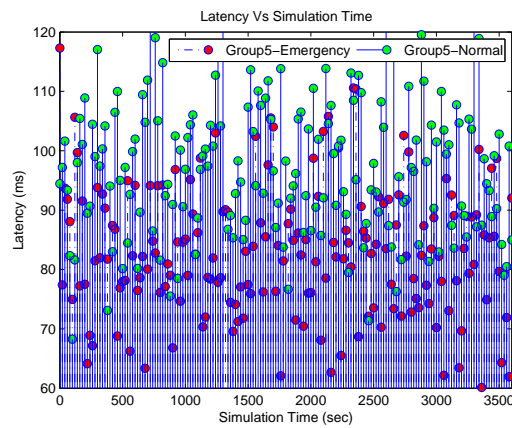
(b) Group2



(c) Group3

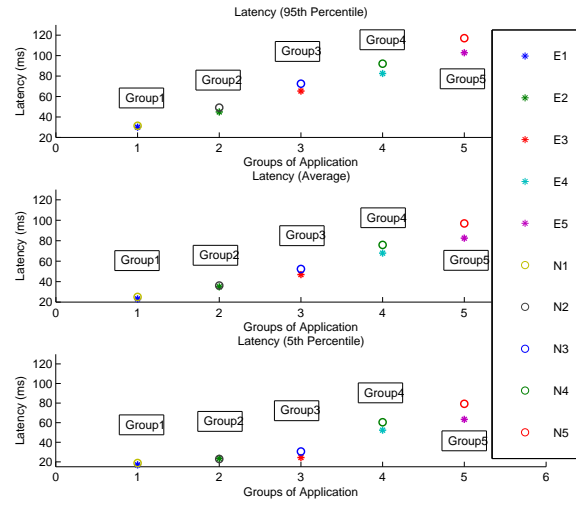


(d) Group4

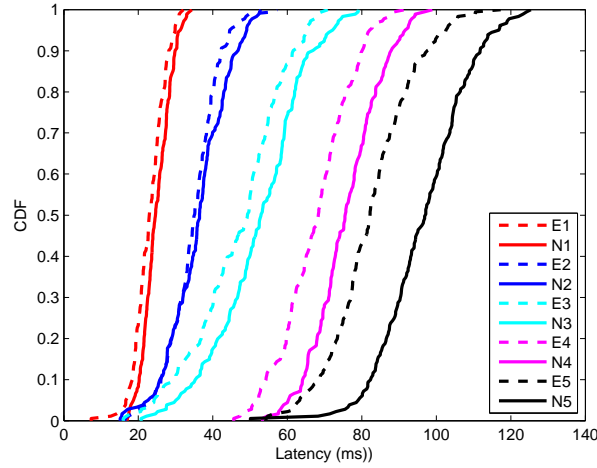


(e) Group5

Fig. 3.14 Latency VS Simulation Time (Group 1-5)



(a)



(b)

Fig. 3.15 (a) Latency VS Group of Application (95th percentile, Average & 5th Percentile), (b) CDF of PDR for each group

3.6 Summary

In this chapter, a SDWBAN framework is proposed that provides administrative controls on incoming packets in order to prioritize sensitive data over the normal data in healthcare applications. Further, an application classification algorithm and a modified version of SBD protocol are employed to implement data prioritization policy and to ensure efficient routing of data packets from source to destination nodes. Finally, the proposed framework is implemented in Castalia simulator and the impacts of SDN controller to resolve WBAN

traffic are analysed for a variety of applications group. From the simulation result, it can be seen that when the complexity in the network increases with large number of flow request from SDESW, the data packets from normal application are dropped by approximately 18.49% for group 5. On the contrary, the PDR of emergency application for the same group is reduced by 14.93% that illustrates 3.56% improvement in the PDR. A similar level of performance improvement in latency is observed for emergency applications as compared to normal applications. The improvement in the emergency application is due to the fact that the controller is still capable of processing the emergency data in the first-most priority basis. The outcomes of this implementation support the proposed framework of SDWBAN.

The performance of the proposed SDWBAN framework could be further investigated by varying number of controllers and SDESWs in the implementation. To do so, it is significant to design an optimization mechanism to determine specific number of controllers and SDESWs. The next chapter discusses the optimization mechanism for the proposed SDWBAN framework.

STATEMENT OF CONTRIBUTION TO CO-AUTHORED PUBLISHED
PAPER

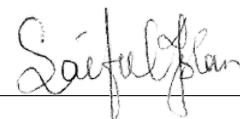
The chapter 4 includes a co-authored journal paper, which has been submitted in MDPI Sensors in 2020. The bibliographic details of the co-authored paper, including all authors, are:

- **Khalid Hasan**, Khandakar Ahmed, Kamanashis Biswas and Md. Saiful Islam, “Control Plane Optimization for an SDN-based WBAN Framework to Support Healthcare Applications”, MDPI Sensors. **(Submitted)**

My contribution to the paper involved: Proposal of mathematical model, analysis, implementation, writing and editing manuscript.

(Signed)  (Date) 8/06/2020

Khalid Hasan

(Countersigned)  (Date) 08/06/2020

Supervisor: Md. Saiful Islam

Chapter 4

Optimization of Control plane for SDWBAN framework

For the past few years, SDN has shown a lot of merits in diverse fields of applications, an important one being the WBAN for healthcare services. With the amalgamation of SDWBAN, the patient monitoring and management system has gained much more flexibility and scalability compared to the conventional WBAN. However, the performance of the SDWBAN framework largely depends on the controller which is a core element of the control plane. The reason is that an optimal number of controllers assures the satisfactory level of performance and control of the network traffic originating from the underlying data plane devices. This chapter proposes a mathematical model to determine the optimal number of controllers for the SDWBAN framework in healthcare applications. To achieve this goal, the proposed mathematical model adopts the convex optimization method and incorporates three critical SDWBAN factors in the design process: number of controllers, latency and number of SDES. The proposed analytical model is validated by means of simulations in Castalia 3.2 and the outcomes indicate that the network achieves high level of PDR and low latency for optimal number of controllers as derived in the mathematical model.

4.1 Introduction

The healthcare industry is advancing rapidly in providing remote healthcare services to patients with the assistance of information and communication technologies. The WBAN is regarded as one of the pioneers in delivering remote healthcare services. This is because the overall management and operations of WBAN has become much more flexible and independent with the incorporation of SDN technology. Since the working principles of SDN offers programmable features in installing new applications irrespective of the devices designed by numerous vendors, the combination of SDNs and WBANs is considered to enhance the remote healthcare services to an outstanding level.

The SDWBAN framework for patient monitoring applications simplifies the data packet forwarding functions from a source to a destination via SDESWs [195] as shown in Fig. 4.1. The SDWBAN framework consists of three planes that reflect the basic principles of the SDN architecture. The data plane of the SDWBAN framework holds the WBAN sensors, SDESWs and gateways. The distributed controllers reside in the control plane which maintains communication with the underlying SDESWs in order to provide instructions for packet_in requests. On top of that, the healthcare authorities manages various sorts of applications through the application plane. In a nutshell, the working procedure of SDWBAN is as follows: the WBAN sensors at the data plane form clusters and connect with SDESWs. These sensors forward data to the connected SDESWs in order to reach out to the gateway. Upon receiving the data from body sensors, the SDESW checks for a match with the flow table and initiates a packet_in request to the controller in the case of mismatch. The controller then processes the request and sends a packet_out response to the SDESW with appropriate action instructions. The SDESW then forwards/drops the data packet based on the retrieved instructions from the controller. The detailed functionalities of the SDWBAN framework can be found in [195].

The SDWBAN becomes more complex as the number of applications and patients increase in the deployed area. A successful implementation and assurance of optimal performance in a complex SDWBAN largely depends on the appropriate design of the

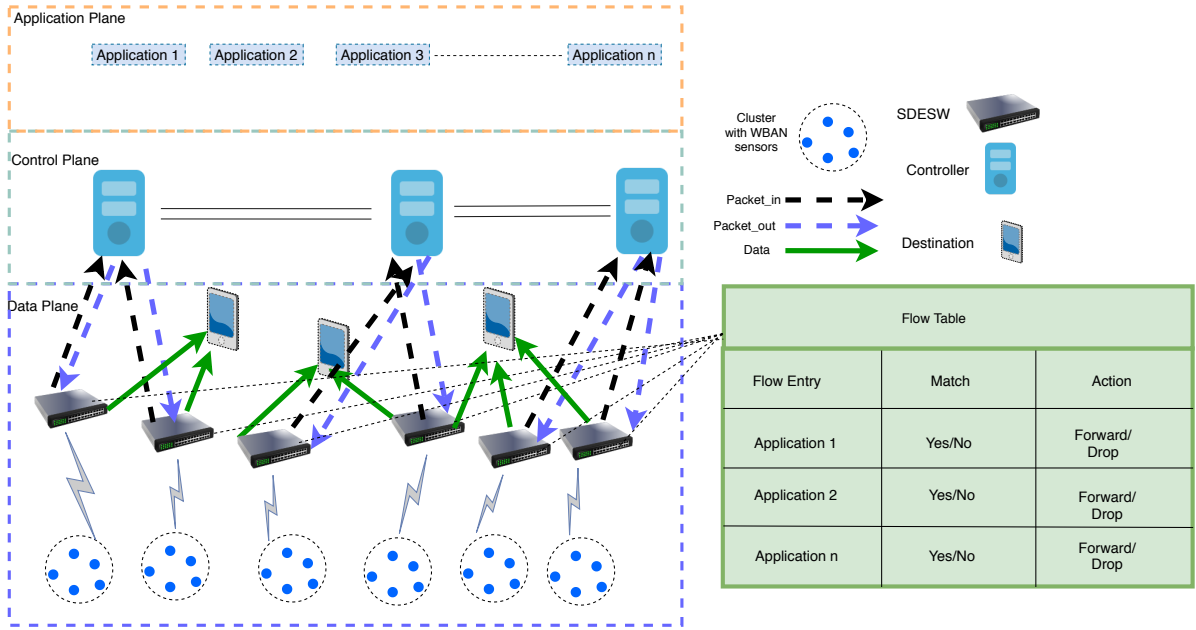


Fig. 4.1 SDWBAN Framework

control plane. In the design of the SDN control plane, the number of controllers plays a crucial role in maintaining QoS and network performance. For wired SDN deployment, multiple controllers can reside in the control plane as the controllers have own dedicated physical resources to maintain inter-controller communication. However, in the case of wireless deployment, the controllers share the same in-band frequency and this could ultimately cause congestion while supporting inter-controller communication. As bandwidth is one of the scarce resources in the wireless medium, utilizing multiple frequency bands for the control plane is very complex and hence, leads to further challenges such as interference, synchronization etc. Therefore, choosing the optimal number of controllers to maintain the QoS in SDWBANs is imperative.

Even though a logically centralized controller can provide a global view of the network, a large-scale deployment of a SDWBAN has several limitations in regard to performance and scalability [205]. This is obvious that having a multiple number of controllers in the control plane, can relax the bottleneck of excessive load on a single controller. However, in order to maintain an abstract view of the network, the controllers need regular state synchronization [206]. This synchronization enables the

controllers to support the underlying SDESWs with their queries for unknown applications or data forwarding instructions. Another issue is that the formation of the clusters is not fixed in a SDWBAN. Similarly, the number of supporting application groups under the SDESWs could also vary from scenario to scenario. As such, when the cluster size is bigger, the probability of receiving more packet in requests gets higher. Hence, it is vital to have a sufficient number of controllers in the control plane so that the originating *packet in* requests from the SDESWs respond within an acceptable time frame. Consequently, an optimum number of controllers is required so that the SDWBAN supported healthcare applications ensure reliability and the timely delivery of physiological data. On the other hand, the redundant use of controllers in the design of the control plane is an unnecessary waste of resources and thus, adds redundant complexity.

One of the first works related to the design of the control plane of SDN was done by Heller et. al. [207]. This work was motivated by three types of SDN users, namely, network operators, controller application writers and network management software writers. Being motivated by these instances, the authors analysed the controller placement problem (CPP) which addresses questions related to the number of controllers to use for a given topology and the placement of the controllers in the given topology. The authors defined a primary metric for the placement of the controllers and evaluated the average propagation latency of the control plane based on Euclidian distance. They also offered a solution based on the k -median and k -center algorithm. However, the solutions were stringently based on the average and worst case delay between the network elements. In the proposed method, decision to find the placement of the controllers was based on a brute force approach with the evaluation of possible locations. However, the approach did not consider traffic load variation and the dynamic adaptation with the number of controllers and position.

The flow setup delay in setting up paths between the controller and the switch is considered in [208] for wired SDNs. The functions of the proposed model are based on the activation and de-activation of the links throughout the network whenever required. The paper considers link cost, equipment cost, the capability of the controllers, path

setup delay and traffic patterns to determine the optimal number and location of the controllers. The prime focus of the work is to minimize the financial cost involved in the installation and removal of network elements.

Hock et al. [209] designed a trade-off mechanism among various placement of controllers that comprises different control latency and controller overheads. The authors used a mechanism named Pareto-based Optimal Controller (POCO) placement that enables a decision to be made by exploring the solution space and performing various analysis through a GUI. The weakness of this approach is that the controllers require a lot of link state information which affects inter-controller latency.

A network partitioned-based controller placement strategy is proposed in [210] that employs a k -center algorithm in order to assist load balancing and network stability. In this work, the authors considered heterogeneous data plane traffic for optimization. In contrast, Jimenez et al. [211] considered homogeneous type of traffic for optimal controller placement. However, both of these works are restricted to the initial observation of constant traffic load and neglect the issue of dynamic traffic load adaptation.

An optimization model for the deployment of controllers and sinks for wireless sensor networks (WSN) is proposed in [212]. The prime focus of the proposed model is to determine the optimal location of the controllers and sinks to maintain reliability and performance in a delay sensitive Internet of Things (IoT) system. Similarly, Wei et al. in [213] proposed a two-level hierarchy control framework for SDN-based IoT networks to relax the bottleneck with the growing number of IoT devices. The authors address the issue of a controller placement strategy based on the priority of the nodes and utilize a binary particle swarm optimization (BPSO) algorithm to optimize the control performance of the SDN-based IoT network. In addition, Kushan et al. in [214] discussed the optimization of controller placement for a hierarchical distributed software-defined vehicular network (SDVN). The prime focus of the work is to find the optimal placement of the controllers to reduce operational latency by locally distributing the top layer of the controllers while the bottom layer of the controllers is placed near the road side unit (RSU). Nevertheless, the studies in [212–214] do not

consider the optimal number of controllers in their proposed models and scenarios.

The aforementioned works are mostly related to the optimal location of controllers for the SDN-based network. The aim of optimization differs based on the nature of deployment and the requirements. Therefore, the problems and solutions related to the optimal control plane design have been discussed from various angles in the literature. However, this work is represented differently compared to the aforementioned studies. Since the timely delivery of data is of paramount significance in WBAN, the total flow resolution time sets a boundary limit for healthcare applications. Therefore, several flow resolution-related parameters are taken into account in developing a mathematical model to find the optimal number of controllers for the SDWBAN framework. The optimal design of the control plane should be able to respond the packet in request originating from all the SDESWs. This chapter focuses on the investigation for an optimal mathematical model that determines the number of controllers required for the SDWBAN framework. A mathematical model is developed based on three influential factors i.e. number of controller, latency and number of SDESW. The latency consists of important parameters involved in the controller to SDESW communication. The developed mathematical model institutes a relationship among the number of controllers, SDESWs and the body sensors. The analytical output is further validated through simulation in Castalia 3.2 simulator.

The key aspects of this chapter can be highlighted as follows:

- Development of a mathematical model that determines the optimal number of controllers for an SDWBAN framework. In addition, the mathematical model also establishes a relationship between the number of controllers and SDESWs.
- Implementation and validation of the mathematical model through the Castalia simulator.

4.2 Influential Factors of Optimization

There are several factors that play vital roles in the design of a control plane for SDWBAN implementation. These important factors are described as follows.

- **Number of Controllers:** The number of controllers plays a crucial role in the design and implementation of an optimal SDWBAN framework. The installation of a large number of controllers increases the complexity and cost of network management. The processing capacity of commercially available controllers typically varies, for instance, the processing speed of an industrial controller is usually very high and capable of maintaining millions of client devices simultaneously [215]. In such a case, the use of industrial controllers for SDWBAN deployment in an elderly home would be redundant. Since responding to the packet_in request initiated by the SDESW mostly depends on its processing speed, it is desirable to have an optimum number of controllers in SDWBAN deployment. The objective is to ensure well-maintained communication between the controller and the SDESW and thus, patient monitoring activities are not compromised at all.
- **Latency:** Latency is related to a number of factors such as flow request processing time, propagation delay, service rate etc. In SDWBAN deployment, if an inadequate number of controllers is deployed, the controllers might undergo a considerable amount of delay in route setup. Consequently, sending out the data forwarding instructions to the SDESW will be affected in terms of flow requesting resolving time. In addition, there could be an increased amount of traffic load in the control channel communication between SDESW and the controller as new applications are introduced in the system. Ultimately, the latency incurred by this will affect the overall network performance in terms of packet delivery which will hamper patient monitoring activities.
- **Geographical Location:** The geographical location of controllers and SDESWs is another important factor in designing the control plane. The issue of LOS and

NLOS exists in wireless network deployment between the transmitter and the receiver. The NLOS scenario could be due to the fact that the patients in SDWBAN are at liberty to roam around, and in addition, the placement of a particular application sensor might block the direct propagation from body sensors to the SDESW. Similarly, other objects such as the walls of buildings, deflections at sharp edges, and multipath propagation may affect the signal strength in an SDWBAN environment. Considering these factors, it is important to design a system that maintains a standard receiver sensitivity level. Furthermore, an arbitrary placement of network elements (controllers, SDESWs, gateway) would cause additional propagation delay between the network elements and ultimately increase overall latency.

- **Traffic Load distribution:** The number of SDESWs residing under a controller is an important issue in determining traffic load. If the number of SDESWs is high under a controller, the probability of receiving a packet.in request also increases. Consequently, the number of packet.out responses to the SDESW also increases. As a result, traffic load increases between the communication channel of the controller and the SDESW. Considering the processing capacity of a particular type of controller, SDN controllers can be programmed in such a way that the excess load can be distributed to the neighboring controllers.
- **Flow Setup Time:** The flow setup time is the amount of time a SDESW needs to send a query to the controller to install data forwarding rules in its flow table. If the number of flow requests originating from the underlying SDESW is larger than the processing capacity of the controller, the average flow setup time can increase significantly which will degrade the service performance [216].
- **Statistics Collection Time and Synchronization Cost:** In the case of multiple controllers residing in the control plane, inter-controller communication takes place to maintain an abstract view of the network and this assists the controllers to provide data forwarding decisions to the switches [205]. The controllers deployed in the network can be inter-connected so that upon failure of one controller, the next available controller can serve the orphaned SDESWs. Moreover, to maintain a

consistent view of the network, it is important to keep the synchronization between the controllers [206]. The controllers can have an overall view of the network by collecting various statistics such as port information, flows, flow table level etc. from the switches. This requires a number of messages to be exchanged between the controllers and switches. Consequently, a trade-off is necessary between the flow setup time and statistics collection time in order to avoid delay in flow resolution.

- **Number of SDESW:** The number of SDESWs in the deployed area could be a crucial point and may create a bottleneck in the network. With a higher number of SDESWs residing in the network, a higher number of flow requests are initiated to the controllers upon realizing an unknown flow. This will ultimately affect the PDR and latency of the network.

In a nutshell, in SDN deployment as well as in SDWBAN, various factors influence the performance of the network. The aim of the optimization of any network is to achieve the optimum level of performance that satisfies the purpose of the deployed application. When the network becomes increasingly complex, more factors will play critical roles in the performance of the network. In order to make the system robust and more secure, various influential factors and functionalities mentioned above can be incorporated in SDN deployment. However, not all the above-mentioned factors might be crucial for wireless deployment i.e. in SDWBAN deployment. Since patient monitoring in SDWBAN should maintain a strict delay boundary, out of all the influential factors related to the optimization of the control plane, we restrict our optimization constraints within three crucial factors: number of controller, latency and the number of SDESWs.

4.3 Development of Optimization Model

According to SDN principles, controllers are responsible for installing flow commands in a switch to route the data packets to appropriate destinations. As such, when an SDESW makes a query about an unknown traffic, the controller processes the query and replies back to the SDESW with appropriate flow commands. Thus, the time to process a flow is

Table 4.1 Notations and Meaning

Notations	Meaning
T_{FR}	Flow Request Delay
T_q	Queuing Delay
T_{proc}	Processing Delay
T_{prop1}	Propagation Delay- SDESW to Controller
T_{prop2}	Propagation Delay- Controller to SDESW
T_{RD}	Relaying Delay

a crucial factor in identifying the optimal point for the implementation of the SDWBAN framework.

Let us assume that T is the total flow resolution time of a controller to resolve an incoming flow request and to respond to the request to a SDESW. Therefore,

$$T = T_{FR} + T_q + T_{proc} + T_{prop1} + T_{prop2} + T_{RD}. \quad (4.1)$$

The notations used in the mathematical model are given in Table 4.1.

The Flow request delay (T_{FR}) is associated with a SDESW. This is the time it takes to realize there is a new flow which is not in the flow table and to send the query to the controller by sending a packet_in request. T_{FR} depends on the matching probability in the flow table and the speed of the flow look-up process.

The Queuing delay (T_q) is associated with the controller. This is the time experienced by each packet while waiting in the queue of a controller. Let us assume that each SDESW and controller maintains a single finite queue, which can be modelled by using the $M/M/1/K$ queuing model. The packet arrival rate from a SDESW to a controller due to the unmatched flow is assumed to be a Poisson distribution. Let us assume, the mean packet arrival rate from a SDESW is λ , a service rate at the controller is α , K is the maximum queue size at the controller, and utilization factor $\rho = \lambda/\alpha$. Therefore, according to [214], queuing delay T'_q due to a single SDESW can be represented by the following equation:

$$T'_q = \frac{\rho[1 - \rho^K - K \cdot \rho^{K-1} \cdot (1 - \rho)]}{\alpha(1 - \rho)(1 - \rho^{K+1})} \quad (4.2)$$

If there is θ number of SDESWS in the deployed area, queuing delay T_q can be expressed as,

$$T_q = \theta * T'_q \quad (4.3)$$

The Processing delay (T_{proc}), is associated with the controller and depends heavily on the processor's speed. This is the time taken by a controller to process a flow-request (packet_in) and reply to the SDESW with flow commands. The processing delay can be expressed as the inverse of service rate α . Therefore,

$$T_{proc} = \alpha^{-1} \quad (4.4)$$

Propagation delay (T_{prop1}, T_{prop2}) occurs when a flow request is sent from a SDESW to the controller and from the controller to a SDESW with an appropriate flow command (packet_out). By considering,

$$T_{prop1} \cong T_{prop2} \cong T_{prop} \quad (4.5)$$

where T_{prop} is the total propagation delay and from equations 4.1, 4.3, and 4.5,

$$T = T_{FR} + \theta * T'_q + T_{proc} + 2 * T_{prop} + T_{RD} \quad (4.6)$$

Relaying delay (T_{RD}) is associated with the SDESW. Let us assume, we have multi-hop communication between the SDESW and the controller. The flow request originating at the SDESW reaches out to the controller through multi-hop relay. Therefore, in each hop, the SDESW stores the request packet and forwards it to the next SDESW and so on until it reaches the controller. Let's say there are n number of hops between a SDESW

and a controller and T_{SF} is storing and forwarding delay which is a two-way computation associated with packet_in and packet_out responses. Therefore,

$$T_{RD} = 2 * n * T_{SF} \quad (4.7)$$

Since we are considering n number of hops between a SDESW and a controller, the propagation delay needs to be associated with the number of hops as well. Therefore, from equations 4.6 and 4.7,

$$T = T_{FR} + \theta * T'_q + T_{proc} + 2 * (T_{prop} + T_{SF}) * n \quad (4.8)$$

Lemma 4.3.1. Assume there are θ number of SDESWs uniformly distributed in a $(\sqrt{\theta} \times \sqrt{\theta})$ building grid with one SDESW in each cell as depicted in Fig. 4.2. A controller is deployed in the middle of the grid and all θ SDESWs are assigned to this controller. Then the average number of hops from a SDESW to controller is $\sqrt{\theta}/2$.

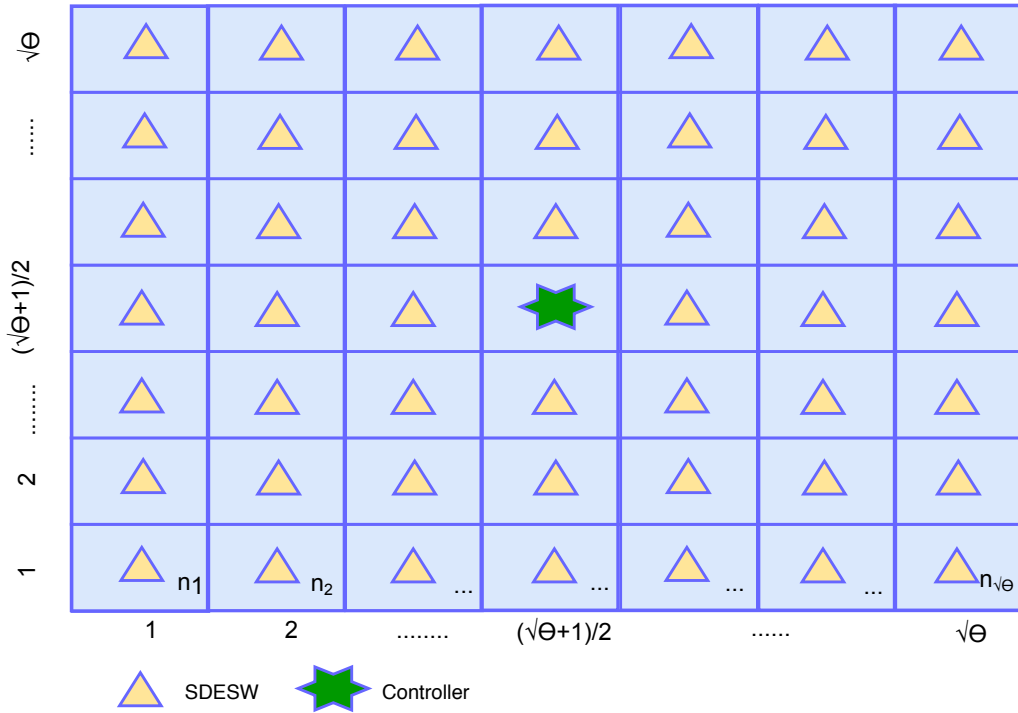


Fig. 4.2 Hops in Building Grid

Proof of Lemma: Let us assume the total number hop counts in building grid is N . The number of hops from the SDESWs are $SW_1, SW_2, SW_3, \dots, SW_{\sqrt{\theta}}$ to reach the controller located at the center are $n_1, n_2, n_3, \dots, n_{\theta}$.

Now, considering the hop counts row-wise from the SDESWs to the controller, total number number of hops would be,

$$N = (n_1 + n_2 + n_3 + \dots + n_{\sqrt{\theta}}) + (n_{\sqrt{\theta}+1} + n_{\sqrt{\theta}+2} + n_{\sqrt{\theta}+3} + \dots + n_{2\sqrt{\theta}}) \quad (4.9)$$

$$+ (n_{2\sqrt{\theta}+1} + n_{2\sqrt{\theta}+2} + n_{2\sqrt{\theta}+3} + \dots + n_{3\sqrt{\theta}}) + \dots$$

$$+ (n_{(\sqrt{\theta}-1)(\sqrt{\theta}+1)} + n_{(\sqrt{\theta}-1)(\sqrt{\theta}+2)} + n_{(\sqrt{\theta}-1)(\sqrt{\theta}+3)} + \dots + n_{\theta})$$

The hops are counted horizontally until it reaches to the intersection of the controller's column. Therefore,

$$N = \left\{ (\sqrt{\theta}-1) + (\sqrt{\theta}-2) + \dots + (\sqrt{\theta} - (\frac{\sqrt{\theta}+1}{2})) + \dots + (\sqrt{\theta}-2) + (\sqrt{\theta}-1) \right\}$$

$$+ \left\{ (\sqrt{\theta}-2) + (\sqrt{\theta}-3) + \dots + (\sqrt{\theta} - (\frac{\sqrt{\theta}+1}{2}) - 1) + \dots + (\sqrt{\theta}-3) + (\sqrt{\theta}-2) \right\}$$

$$+ \left\{ (\sqrt{\theta}-3) + (\sqrt{\theta}-4) + \dots + (\sqrt{\theta} - (\frac{\sqrt{\theta}+1}{2}) - 2) + \dots + (\sqrt{\theta}-4) + (\sqrt{\theta}-3) \right\} +$$

$$\dots + \left\{ (\sqrt{\theta}-1) + (\sqrt{\theta}-2) + \dots + (\sqrt{\theta} - (\frac{\sqrt{\theta}+1}{2})) + \dots + (\sqrt{\theta}-2) + (\sqrt{\theta}-1) \right\} \quad (4.10)$$

$$N = \left\{ \theta - \frac{(\sqrt{\theta}+1)^2}{4} \right\} + \left\{ \theta - \frac{(\sqrt{\theta}+1)^2}{4} - \sqrt{\theta} \right\} \quad (4.11)$$

$$+ \left\{ \theta - \frac{(\sqrt{\theta}+1)^2}{4} - 2\sqrt{\theta} \right\} + \dots + \left\{ \theta - \frac{(\sqrt{\theta}+1)^2}{4} \right\}$$

Finally, the average number of hops n from a SDESW to controller would be

$$n = \frac{N}{\theta} \cong \frac{\sqrt{\theta}}{2} \quad (4.12)$$

Then equation 4.8 can be rewritten as,

$$T = T_{FR} + \theta * T'_q + T_{proc} + 2 * (T_{prop} + T_{SF}) * \frac{\sqrt{\theta}}{2} \quad (4.13)$$

Hence,

$$\theta * T'_q + \sqrt{\theta}(T_{prop} + T_{SF}) + T_{FR} + T_{proc} - T = 0 \quad (4.14)$$

$$(\sqrt{\theta})^2 * T'_q + \sqrt{\theta}(T_{prop} + T_{SF}) + T_{FR} + T_{proc} - T = 0 \quad (4.15)$$

Let's assume that, $a = T'_q$, $b = (T_{prop} + T_{SF})$, and $c = T_{FR} + T_{proc} - T$. Therefore, from equation 4.15, it can be written,

$$a(\sqrt{\theta})^2 + b\sqrt{\theta} + c = 0 \quad (4.16)$$

The solution of the quadratic equation 4.16 would be,

$$\sqrt{\theta} = \left[\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \right] \quad (4.17)$$

The solution equation 4.17 will identify the minimum number of SDESWs (θ) under a single controller in a network. By substituting the coefficient values in equation 4.17 we find the number of SDESWs per controller,

$$\sqrt{\theta} = \left[\frac{-(T_{prop} + T_{SF}) \pm \sqrt{(T_{prop} + T_{SF})^2 - 4T'_q(T_{FR} + T_{proc} - T)}}{2T'_q} \right] \quad (4.18)$$

The solution of equation 4.18 will provide two different values of $\sqrt{\theta}$, that satisfy the quadratic equation. Based on the assumption, the numerical coefficient "c" contains the parameter "T", which is the total flow resolution time constraint, we therefore find "c" for a range of "T" and thus find the $\sqrt{\theta}$.

Table 4.2 Numerical Co-efficient and root

Flow Resolution Time (T ms)	Numerical Coefficient (C)	Root($\sqrt{\theta}$)
20	-0.0099	(0.4107,-2.4117)
30	-0.0199	(0.7292,-2.7302)
40	-0.0299	(0.9976,-2.9986)
50	-0.0399	(1.2340,-3.2349)
60	-0.0499	(1.4476,-3.4486)
70	-0.0599	(1.6441,-3.6451)
80	-0.0699	(1.8269,-3.8279)
90	-0.0799	(1.9986,-3.9996)
100	-0.0899	(2.1610,-4.1620)
110	-0.0999	(2.3155,-4.3165)
120	-0.1099	(2.4631,-4.4640)
130	-0.1199	(2.6046,-4.6056)
140	-0.1299	(2.7408,-4.7417)
150	-0.1399	(2.8722,-4.8731)
160	-0.1499	(2.9993,-5.002)

As it can be seen from the Table 4.2, for a fixed delay requirement, we get two different values for $\sqrt{\theta}$ that satisfy the derived quadratic equation. To illustrate, for flow resolution time of 110 ms, graph of the quadratic equation is given in Fig. 4.3.

Since, it is required to find the minimum number of SDESW per controller, the negative part of the solution is avoided and the valid solution of the quadratic equation would be $\sqrt{\theta}$, 2.3155.

Let us assume that packet arrival rate at the SDESW is δ , s is the number of WBAN sensors under each SDESW, and ϵ is the packet generation rate at each sensor, Therefore,

$$\delta = s * \epsilon \quad (4.19)$$

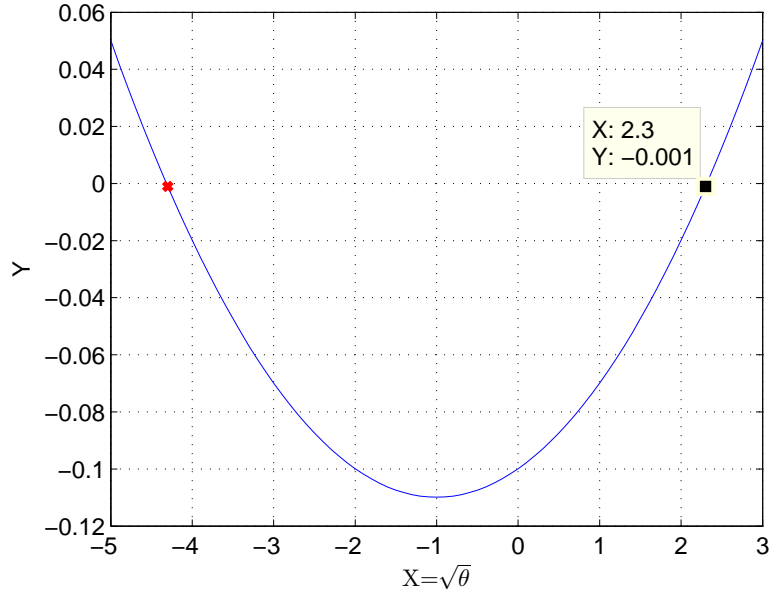


Fig. 4.3 Intercept of quadratic equation

If a SDES_W, SW can accommodate κ number of packets per second and the total number of body sensors in a WBAN is S , the outcome of the following convex optimization problem derives the optimal number of SDES_W required in the network [17].

$$\text{Minimize, } SW = \frac{S}{s}, \text{ subject to } s \leq \frac{\kappa}{\epsilon} \quad (4.20)$$

The optimal number of controllers C_{opt} would be,

$$C_{opt} = \frac{SW}{\theta} \quad (4.21)$$

4.4 Result and Analysis

This section provides results in two sub-sections. Firstly, the result of the optimization is discussed and secondly, performance analysis of a SDWBAN implementation is presented in relation of the optimized number of controllers.

4.4.1 Analytical Output

Based on the derived mathematical model in equation 4.18, the relationship between the number of SDESWs per controller and the total flow resolution time is presented in Fig. 4.4.

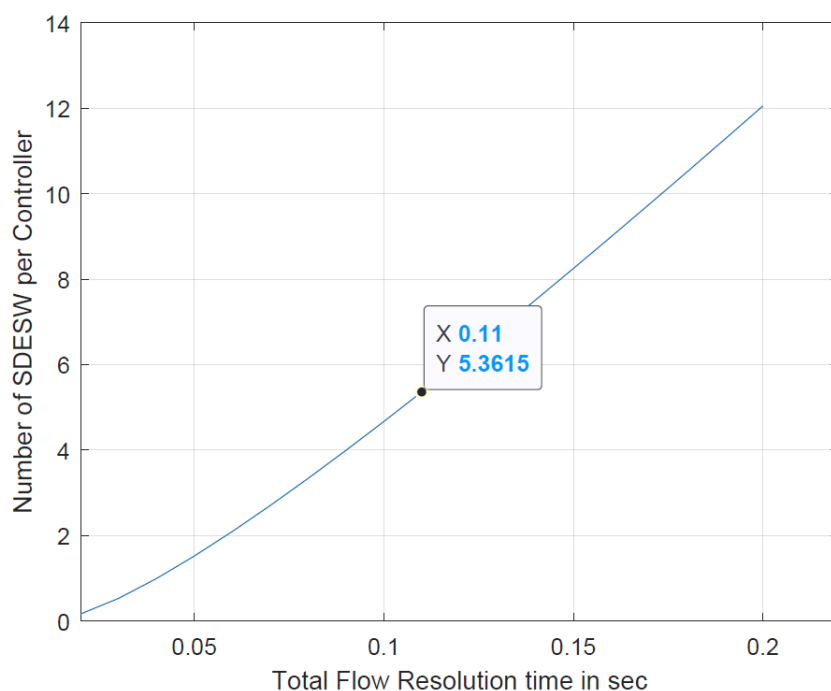


Fig. 4.4 Number of SDESW per Controller

The graph shows that for a total resolution time of 110 ms, the number of SDESWs under a controller is $5.3615 \approx 6$. Ultimately, the number of SDESWs per controller for a total resolution time of 110 ms leads to finding the optimal number of controllers for the implementation of SDWBAN. Therefore, based on the primary work of SDWBAN implementation 3, for a total number of 100 body sensor nodes and 4 nodes under one SDESW, the optimal number of controllers is 5. Similarly, based on the optimization model, the required number of controllers for a range of body sensors is provided in Table 4.3. The list of parameters assumed in the mathematical model is given in Table 4.4.

Some significant observations can be noted from the obtained mathematical model.

Table 4.3 Optimal Controllers

Number of Body Sensors (S)	Optimal Controllers
100	5
200	10
300	15
400	20
500	25

Table 4.4 List of Parameters

Parameters	Values
Flow Request Delay, T_{FR}	100 μs
Free space propagation speed, C	$3 * 10^8 m s^{-1}$
Average Distance from SDESW Controller, d_{avg}	32.30 m
Propagation Delay, T_{prop}	$T_{prop} = d_{avg}/C$
Storing and Forwarding delay, T_{SF}	20 ms
Packet Arrival Rate, λ	50 pkt/sec
Service Rate, α	100 pkt/sec
Maximum Queue Size, K	15

The observations are listed as follows:

- The optimal number of controllers required in an implementation scenario largely depends on the processing capacity of the controller. For instance, it is assumed that the service of the controller is 100 pkt/sec, which is based on simulation output. It is found from the simulation that the processing rate of a light-weight controller is 100 pkt/sec. However, industrially available controllers have higher processing capacity [217]. The controllers with higher processing capacity or service will result in a fast response to the incoming packet in request from a SDESW. The consequence will be low queuing delay due to the variable packet arrival rate from the underlying body sensors.
- The flow request delay is another important factor since it depends on the matching probability in the flow table and the speed of the look-up process.
- The packet arrival rate from the heterogeneous sensors affects the performance of the SDESW and the controller. Since the heterogeneous nature of WBAN sensors

generates data packets at various intervals, this could imbalance the traffic load in the communication channel between the SDESW and the controller.

- The number of controllers and the number of SDESWs affect the overall performance. If there are fewer controllers in the deployed area, this limited number of controllers might have to cater for all the SDESWs under the assigned controller. In such a case, packet forwarding might route in a multi-hop fashion to the controller if the distance between the SDESW and the controller is out of transmission range. Consequently, it degrades the performance in terms of success rate and latency.

4.4.2 Simulation Output

In this part of the analysis, simulation is conducted in Castalia 3.2 [203] on Ubuntu 16.04.4 platform. The experiment is conducted for 100 iterations and the performance of the a SDWBAN scenario is observed. In the initial work of chapter 3, the simulation includes a total number of four controllers in the simulation area. However, in this case, the number of controllers is varied while the number of SDESWs are kept fixed. The simulation is run for several groups of applications where the number of applications is incremented. The number of applications per group is listed in Table 4.5.

Table 4.5 Group of Applications

<i>Groups</i>	<i>Number of Applications</i>
Group 1	1
Group 2	5
Group 3	10
Group 4	15
Group 5	20

It should be noted that the simulation area and the other related parameters are kept similar to the initial work. For each group of applications, the simulation is conducted by varying the number of controllers from 1 to 10. Since the aim of this research is to find the optimal number of controllers for an SDWBAN framework, the simulation is

run for a different number of controllers to obtain the average PDR and latency for each application group.

In the first stage, the average PDR with a varying number of controllers is depicted in Fig. 4.5. It can be seen that when the number of controllers is low, the PDR for all groups (group 1-5) is also low and when the number of controllers starts to increase, the PDR increases as well. However, at some point, the PDR starts to decrease even the number of controllers increases. For instance, when the number of controllers ranges from 1 to 3, the average PDR increases. When the number of controllers ranges from 4 to 6, the average PDR still increases. However, after the 6th number of controllers, the average PDR decreases. The reasons of this are as follows:

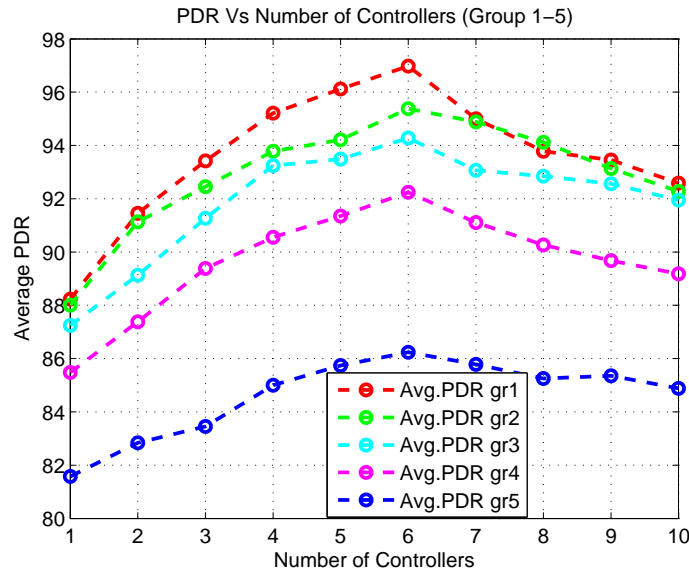


Fig. 4.5 Average PDR with varying number of controllers

- When the number of controllers is low (1, 2, or 3), less controllers are utilized to cater for a lot of flow resolve requests from a various number of application groups. This creates a bottleneck to respond to the incoming packet in requests coming from the SDESWs. Furthermore, a lot of multi-hop communication takes place since the destination controller is beyond the transmission range of SDESWs. This results in a delay in accessing the channel. In addition, the traffic load increases between the communication channel of SDESWs and the controllers. Thus, the PDR of all application groups decreases.

- When the controller number is between 4 to 6, the average PDR shows little variation in the output which actually shows the optimal range of controllers that are required for the SDWBAN framework.
- When the number of controllers is between 7 to 10, the PDR decreases due to the fact that a lot of controllers reside nearby and use in-band frequency. This also causes congestion and interference with the neighbouring nodes in the communication channel.

The simulation output is further observed by analyzing the average latency for a different number of application groups. The average latency depicted in Fig. 4.6 shows that initially with a low number of controllers, all application groups experience high latency. The average latency stays more or less stable when the number of controllers is between 4 and 6 but with an increase in the number of controllers, latency increases. This phenomena coincides with the facts of average PDR output. From the simulation

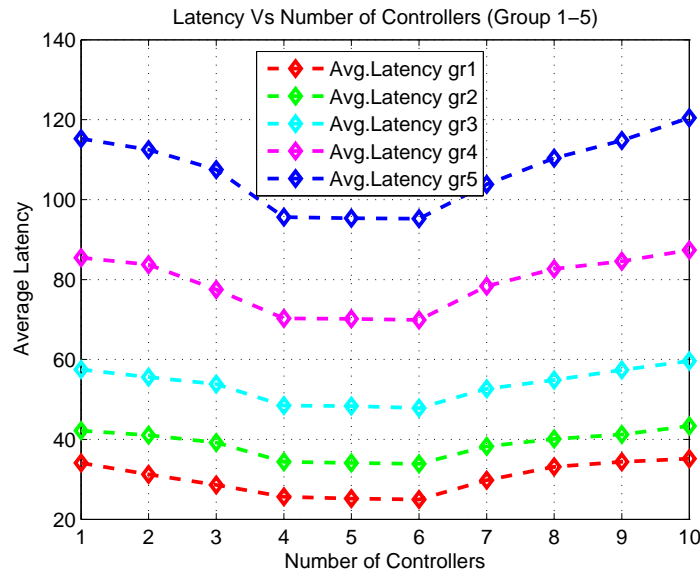


Fig. 4.6 Average Latency with varying number of controllers

outcomes of average PDR and latency, it can be seen that the best performance is received from the network when the number of controllers is set to 6. Although the PDR gain is high when using 6 controllers, no significant improvement in the latency is noticed in the outcomes. Even, the average latency remains almost same for 4, 5 and 6 controllers.

This outcomes indicate that the network would be able to achieve its peak performance for setting the number of controllers to 5. Since latency is one of the key elements in the proposed mathematical model, the experimental results validate the analytical outcome derived from the mathematical model for 100 body sensors.

The experimental output is further elaborated on for the CDF of PDR and latency for the optimal five controllers. Fig. 4.7 presents the output for a different group of applications in terms of PDR. According to Fig. 4.7, group1 has the highest PDR while group5 exhibits the lowest PDR. A similar type of variation can be noticed in the PDR of the other groups (2-4). The reason for this is due to the increased number of applications. As the number of applications increase, the SDESW initiates more packet_in requests for every unknown flow. Therefore, the traffic load between the control channel of SDESWs and the controller increases. Thus, more data packets are dropped due to congestion. As can be observed from the group1 graph, at the 90th percentile point, the PDR of group1 is 96.38% whereas the PDR of group5 is 86.78%. This performance demonstrates that any packet of group1 at the 90th percentile has a 96.38% probability of being delivered successfully and a 3.62% probability of being dropped. Similarly, any packet of group5 at 90th percentile point has a 86.78% probability of being delivered successfully whereas it has a 13.22% probability of being dropped.

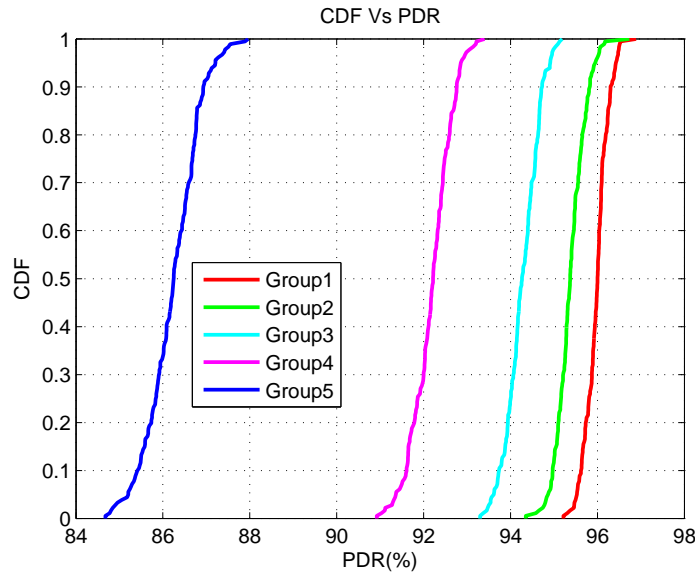


Fig. 4.7 CDF Vs PDR

An analysis is carried out to understand the performance of various groups of applications in terms of latency. Fig. 4.8 shows that at the 90th percentile point, the latency of the application group1 is the lowest whereas the latency of the group5 application is the highest. The group1 application experiences a latency of 29.34 ms whereas group5 experiences a latency of 110.5 ms at the 90th percentile point. This demonstrates that any packet of group1 has a probability of reaching the destination gateway within 29.34 ms and in 10% of the time, the packet may not reach the destination successfully. Similarly, for the data packet of application group5, any packet has a probability of being delivered successfully within a 110.5 ms time period while 10% of the time the packet may not be delivered. The result is obvious due to the fact that more time is required for the controller to resolve the packet_in request as the number of applications increases.

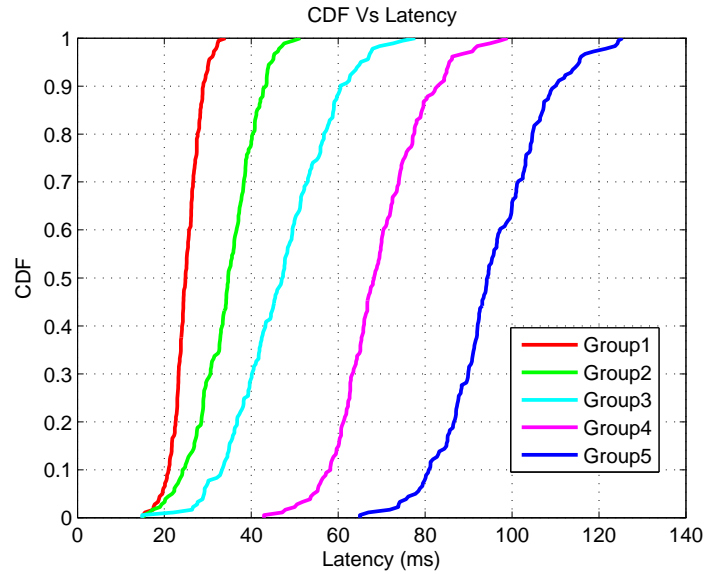


Fig. 4.8 CDF Vs Latency

4.5 Summary

In this chapter, an optimization model for the design of the control plane for SDWBAN framework has been developed. The derived mathematical model leads to a relationship between the number of controllers, SDESWs and WBAN sensors. Ultimately, from the

analytical output, the optimal number of controllers turns out to be 5 for the initial implementation of the SDWBAN framework. The analytical output is then validated by varying the number of controllers while other physical resources in the simulation remain similar to the initial one. The simulation output indicates the optimal point is 6 for both the average PDR and latency analysis of application groups 1 to 5. However, based on the simulation output, the average PDR and latency observed in the range of 4 to 6 controllers are quite acceptable. The outcome of the proposed mathematical model supports the control plane design of the SDWBAN framework.

STATEMENT OF CONTRIBUTION TO CO-AUTHORED PUBLISHED
PAPER

The chapter 5 includes a co-authored journal paper, which will be submitted in Wireless Networks in 2020. The bibliographic details of the co-authored paper, including all authors, are:

- **Khalid Hasan**, Mohammad Javed Morshed Chowdhury, Kamanashis Biswas, Khandakar Ahmed and Md. Saiful Islam, “Blockchain based Secure Data Sharing Platform for Software-Defined Wireless Body Area Network”, Wireless Networks. **(To be Submitted)**

My contribution to the paper involved: Data sharing barrier, Proposal of blockchain for SDWBAN framework, implementation, writing and editing manuscript.

(Signed)  (Date) 8/06/2020
Khalid Hasan

(Countersigned)  (Date) 08/06/2020
Supervisor: Md. Saiful Islam

Chapter 5

Blockchain-based Secure Data Sharing Platform for SDWBAN

In this era of digitization, there is an increasing need to securely share an ever-growing volume of data between multiple parties in near real-time. Of the modern data sharing technologies, blockchain has proven its necessity and unprecedented prospects in providing a secure environment for information exchange between two parties. In addition, the integration of IoT with blockchain has enabled a digital transformation in many areas such as healthcare, supply chains and financial services. Like blockchain, the programmable SDN concept is also achieving popularity due to its ability to reduce the complexity of managing networks. It is evident that incorporating SDNs with IoT based healthcare systems i.e., WBAN, can significantly improve the current healthcare management services. To leverage the maximum benefits of these two emerging technologies, this paper proposes an architectural framework that incorporates blockchain with SDWBAN to facilitate secure data sharing in a healthcare system. However, the successful integration of blockchain with SDWBAN is often hindered by a number of challenges, which are identified in this chapter. In addition, a smart-contract based fine-grained access control policy is designed to ensure that only data owners will have full control over their health data. The experiment outcomes show that the proposed model achieves good throughput and incurs a very low overhead in terms of

latency.

5.1 Introduction

The SDWBAN framework adopts the principles of SDN where the data plane and control plane functionalities are separated. The communication model of SDWBAN includes different parties such as patients, network providers, healthcare service providers, emergency medics, doctors, nurses and so on. Therefore, physiological data collected through wearable devices need to be shared among multiple sources. This information also sometimes needs to be shared with various parties such as medical research groups, insurance companies or with other medical centres for better treatment or for other purposes. This involves data sharing with different parties and traditionally, the method of sharing takes a long process of verification and therefore, the authenticity and integrity of data is sometimes lost. Moreover, an insurance claim after a particular diagnostic process involves a long systematical approach to process the payment. To overcome these issues, secure cutting-edge technologies such as blockchain are being adopted at various aspects to facilitate both consumers and the providers. In SDWBAN, data dissemination or access at different intervals of the diagnostic process can be regarded as *blocks of transactions* in the context of blockchain technology. However, incorporating blockchain technology with SDWBAN is non-trivial.

The idea of integrating blockchain with SDWBAN is fairly new. However, some discrete approaches to incorporate blockchain in healthcare have been proposed by several researchers. A startup, named the Gem Health Network [175], utilized Ethereum blockchain technology to create a structural platform to permit authorized parties, individuals, and experts to track the past history of patients. Similarly, an Estonian medical system started to use Guardtime blockchain [177] to retrieve information on medical treatments. Furthermore, an individual data trading platform Healthbank Blockchain [178] allows the owner of the data to access for research purposes. BlockHIE [179] is another blockchain based platform that proposes a health information

exchange mechanism to store data remotely in order to enhance collaboration between medical research industries. A recent study [218] proposed an integration of WBAN using smart contracts to securely automate patient monitoring. Integrating blockchain with healthcare covers a diverse area of healthcare services of which WBAN is an integral part from the perspective of IoT applications.

Ashraf et al. [219] proposed the idea of using a patient-centric agent that manages a blockchain component to preserve WBAN data securely. The proposed architecture is a two-tier model where data accumulation and blockchaining processes takes place in the first tier and key management for the healthcare provider is controlled by the healthcare control unit in second tier. The design requires a dedicated smartphone to connect with the patient-centric agent software that is in charge of miner selection and decision making to preserve eventful data into a blockchain through segregation. The top-to-bottom architecture constitutes multiple encryption processes at various levels of communication which could be a significant issue for patient monitoring as long as the delay is concerned.

A decentralized record management system named Medrec is proposed in [220] which uses blockchain technology for electronic medical records. TThe Medrec system facilitates data authentication, confidentiality and data sharing among multiple parties through the integration of a patient's database with the providers' database. Any changes or updates in the patient's record by the healthcare provider generates an auto-notification for verification purposes. The proposed system is lacking in terms of providing security for individual databases and does not address the issue of emergency patients who might be unable to give their consent for their data to be accessed given their condition. The process of sharing a patient's health-related document between various entities such as research and medical institutions is described in the Medshare [221] system. The process demonstrates a clinical data-sharing technique based on a smart contract and is capable of acting as an administrator to provide access to entities. However, Medshare contributes only to a sub-scheme of patient monitoring and skips the process of IoT-based patient monitoring.

A blockchain-based application named Healthcare Data Gateway (HDG) is proposed in [222] to enable the patient to control and share their personal data securely. The proposed system involves three-layer processing: i) the storage layer, ii) the data management layer and iii) the data usage layer. The storage layer employs a blockchain mechanism to protect the integrity of the data and the data management layer processes all kinds of incoming and outgoing requests. The healthcare-related entities reside in the data usage layer and the diagnostic center communicates with the patient and seeks authority to further process the data. Although the proposed system is a unified data storage system, it lacks detail on the consensus mechanism of cloud-based blockchain.

Roehrs et al. [223] developed a model named OmiPHR that aims to provide patients with a unified view of their personal health records and allows healthcare providers to view updated information pertaining to the patient even if the patient is under the supervision of another healthcare service provider. In this model, the PHR is encrypted and distributed in chained data blocks in the network and the blocks are available in multiple locations which incorporates with the blockchain technology. To ensure privacy and data integrity, the digital signature of each user is used in the data block. The OmniPHR model is lacking in terms of scalability as the data need to follow the standard used in the model. Otherwise data sharing between various entities is not possible.

This chapter investigates the crucial aspects of data sharing for the SDWBAN framework and proposes an architectural model to facilitate secure information exchange among healthcare entities. The key aspects of this chapter can be highlighted as follows:

- The challenges of SDWBAN in terms of data sharing have been investigated.
- An extensive security analysis has been carried out using the Automated Validation of Internet Security Protocols and Applications (AVISPA) to evaluate the security and privacy of the proposed system.

- A blockchain based secure data sharing platform for SDWBAN is designed with a smart contract-enabled fine-grained access control mechanism where users will have full control over their own data.
- Experiments are conducted on the proposed system for several applications-groups to evaluate its effectiveness in different traffic conditions. In addition, a number of experiments have been conducted to calculate the response time of blockchain and cloud-based healthcare systems to observe their performance in different scenarios.

5.2 Use Cases of SDWBAN

SDWBAN has several use cases in the healthcare domain. Each use case involves different types of requirements in terms of communication throughput, privacy, data quality and integrity. Here, four use cases are presented to understand the basic requirements of a data-sharing platform in SDWBAN.

5.2.1 Data Collection and Monitoring for Medicare

Data collection and monitoring is important to gain a comprehensive picture of patients' health and wellbeing. A number of intelligent physiological sensors have now been integrated into wearable devices and can be used for computer-assisted rehabilitation or the early detection of medical conditions. However, this area relies on the feasibility of implanting very small biosensors inside the human body that are comfortable and don't impair normal activities. The sensors implanted in the human body will collect data on various physiological changes in order to monitor patients' health status, irrespective of their location. Then, the information is transmitted wirelessly to an external computing unit and medical practitioners can use this data to provide healthcare services.

5.2.2 Data Sharing for Medical Research

Many novel devices such as chest straps, electronic garments, skin patches, smart glasses, and even smart jewellery have also started to emerge [224]. The range of parameters these devices can monitor is also expanding beyond heart rate and activity to include parameters such as blood pressure, blood glucose, respiratory rate, blood oxygen saturation, and body temperature [225]. In addition, the use of mobile monitoring devices is now common in hospital settings. Health professionals are increasingly using health monitoring devices for post hospital care.

This widespread adoption of wearable devices by consumers has raised the prospect of health researchers being able to conduct studies that were previously considered infeasible or too costly. For health researchers, there are a number of benefits of recruiting research study participants who own their own wearable devices. For example, research subjects located in a different city or even in a different country can share their data with the researchers. This vastly increases the potential number and diversity of research subjects.

5.2.3 Health Insurance

WBAN is considered as the primary source of WBAN is considered the primary source of real-time health data and the use of real-time health data is an important aspect in understanding the lifestyle of individuals. Health insurance companies around the world are interested in accessing this type of data. Many companies are also willing to offer incentives, such as low premiums if the individual lives a healthy life based on the data. However, it should be noted that insurance companies are not allowed to access individuals' health records without their consent.

5.2.4 Handling an Emergency Situation

SDWBAN can provide critical information at the time of an emergency with very minimal delay. Wearable and body implantable devices can deliver real-time data to emergency

services until healthcare facilities are available. In addition, modern wearable devices combined with smart phones are also capable of analyzing health data and generating an alarm in case of an emergency health condition.

5.3 Requirement Analysis

This section identifies a number of requirements based on the above-mentioned use-cases. Here, each of the requirements are explained.

- **Ability to Share:** WBAN continuously produces critical and sensitive health information. Individuals and health professionals often need to share this information for both medical and non-medical purposes. Therefore, there should be a *convenient* and *secure* data-sharing mechanism to facilitate this exchange.
- **Transparency in Data Sharing:** One of the major problems in sharing personal data is that there is a lack of trust between the data custodian and other individuals. In terms of WBAN, data custodians are health professionals and individuals often feel reluctant to allow others to collect and share their information. One real example is the failure of the Australian government's health initiative called "MyHealth", where the majority of Australians opted out of the service in the fear of that the data custodians may share their information with insurance companies [226]. Therefore, it is necessary that individuals should have access to *all access control* and the *data sharing policy* related to their personal data.
- **Quality of Service:** WBAN collects various types of data from the body. However, there are situations when specific data should be given priority over other types of data. For instance, when an irregularity is observed in the heart rate, the heart-rate data may be more important than the temperature data. Therefore, heart-rate data should get priority over temperature data during the data transmission phase.
- **Data Integrity:** Data accuracy is vital to provide financial incentives based on

data. For example, in a health insurance scenario, the premium rate or claim may be decided based on the data collected by the WBAN. In this particular scenario, it is important that nobody manipulates the data.

From requirement analysis, it is clear that SDWBAN can effectively solve some of the issues pertaining to healthcare systems, such as QoS. However, it is worth noting that there is a need for an emerging technology that will bridge the gap and tightly couple different entities in healthcare systems. Blockchain might be one such technology that can provide a fine-grained access control mechanism on top of SDWBAN to securely access sensitive information in a healthcare system.

5.4 Data Sharing Barriers in SDWBAN

As more technology floods into healthcare and adds more data from devices, the safe exchange of data among different entities in a healthcare system has become a major concern. To develop a blockchain-based data-sharing model for SDWBAN, first it is important to identify the challenges in SDWBAN. Furthermore, it is necessary to understand whether blockchain can be used as a potential solution to overcome these challenges. This section provides a brief overview of blockchain technology and then lists a number of challenges in SDWBAN that can be addressed through blockchain technology.

5.4.1 Blockchain Technology

A blockchain is a decentralized ledger or a continually updated list of transactions which records agreements, contracts, and sales [227]. Although initially developed to support cryptocurrency, this peer-to-peer system has been implemented for a wide variety of applications including finance, transport, education, governance and health sectors. The security of blockchain technology relies on strong cryptographic schemes which make it computationally impossible to tamper with transactions stored in a blockchain. This is

because an attacker would have to compromise 51% of the systems to surpass the hashing power of the target network.

Fig. 5.1 presents the structure of a block which contains a header and the contents of the block. The header consists of the following items

- A timestamp- serves as a secure proof of exact time.
- Merkle tree root- constructed by hashing paired data (the leaves), then pairing and hashing the results until a single hash (known as root hash) obtained
- Difficulty target- set by a consensus algorithm such as proof-of-work (PoW).
- Previous block header- a cryptographic link that creates a tamper-proof chain, and
- Nonce- required for solving the PoW and defending against replay attacks.

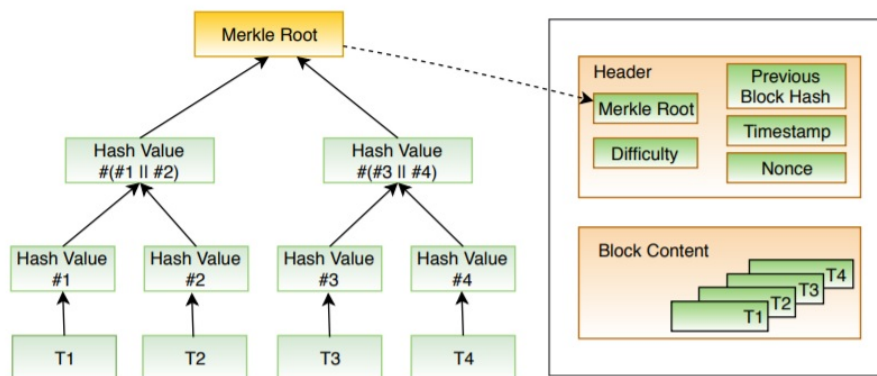


Fig. 5.1 The structure of a block

On the other hand, the block content contains the inputs and outputs of each transaction where the inputs contain the output of the previous transactions and a signature of the owner and the outputs include the asset to be sent as well as the address of the recipient. The signature acts as a proof of ownership of the asset which can only be verified by the public key of the owner. In a nutshell, every time a block (in other words, a group of transactions) is approved, the immutable stamp provides a guarantee that no one can tamper with the recorded data.

5.4.2 Challenges

Due to the inherent properties of SDWBAN, integrating blockchain technology with SDWBAN is not a trivial task. Although a sophisticated platform for a blockchain-based SDWBAN is yet to be developed, some obvious challenges including management and technical issues need to be taken into account as the first step. A discussion on several highlighted challenges is presented in this subsection.

5.4.2.1 Interoperability

To develop an effective and fast data-sharing platform, achieving agreement between different healthcare providers and patients is necessary. A lack of coordination and the unwillingness of collaborators poses a barrier to effective data sharing [228]. Patients and providers might experience serious problems in data retrieval and the sharing process. Most importantly, the consent of the patient is important when it comes to further research for a particular treatment. Therefore, patient-mediated and patient-driven interoperability introduces new challenges in terms of security, incentives and governance [229]. A blockchain-based data-sharing platform can mitigate these challenges by enforcing different policies in the form of automated smart contracts.

5.4.2.2 Data Management, Anonymity, and Privacy

Data handling, supplying and overall management is a critical task in SDWBAN. Trust is one of the key concerns in data management where the patient should be aware of the parties who can access to their physiological data. Furthermore, data should not be exposed to unauthorized entities where data can be used fraudulently by malicious users or attackers [230]. However, with the implementation of appropriate anonymization techniques, a consortium blockchain-based platform can overcome the issues related to data management and privacy.

5.4.2.3 Quality of Service (QoS)

One of the main concerns in SDWBAN is to ensure the delivery of data within the required time frame. Failure to do so might result in serious consequences in the diagnosis or treatment process. Since incorporating blockchain will increase the computational complexities, there is a chance of increasing computational delays. For example, when data transactions between various parties take place, block verification will contribute to some delay in accessing data and further analysis. A trade-off needs to be maintained between delay and security when selecting the number of miners and the blockchain platform to ensure QoS. For example, a consortium blockchain would provide better QoS compared to a public blockchain.

5.4.2.4 Storage Capacity

One of the potential bottlenecks could be the storage capacity of the devices in SDWBAN. Since the diagnostic process might consist of images, medical reports, and lab reports, all these require a large amount of storage space. In addition, each blockchain transaction creates copies of the transaction which are stored in all trusted entities. However, this issue can be resolved by using off-chain storage where only the hash of each block is included in the blockchain to provide data integrity. The original data blocks will be stored in off-chain storage.

5.4.2.5 Issues with Electronic Health Records (EHRs)

A significant part of patient data management involves managing EHRs. Maintaining correct EHRs and correcting erroneously recorded data is challenging. As such, there is a need for coordination between organizations to avoid data fragmentation. The smart contract support of blockchain technology can speed-up the data-sharing process and reduce operational errors.

5.5 The Proposed Architectural Framework

The proposed model combines both SDN and blockchain technology to improve the overall communication in the network and enables individuals to share their data with a third-party using access control policies written as smart contracts, which ensures transparency in the data sharing process. The SDN architecture improves network latency by decreasing end-to-end delay and increasing the throughput of a large WBAN network and it can also prioritize certain traffic if required. Fig. 5.2 shows a high-level overview of the proposed architectural framework where the functionalities of different modules have been separated into three logical layers. The main functionality of layer 1 is data collection where the wearable and/or implanted devices send the collected information to SDN enabled switches. Then, the switches forward the data traffic to the gateway on the basis of the priority schedule setup by the SDN controller. Finally, the gateway sends the information to the blockchain nodes at layer 2. The layer 2 devices are responsible for security and policy enforcement and data management. The raw data stored in the off-chain storage can be accessed by data consumers (e.g., health researchers, secondary health professionals, and insurance companies), if there is no violation of the access policy. It should be noted that the SDN controller can also work as a blockchain node although the proposed architecture keeps them separate to reduce the load. Layer 3 is also known as the blockchain access layer which implements data sharing and access control policies in the form of smart contracts.

The advantage of the proposed system is that both health professionals and individual patients can define their access and sharing policy in smart contracts respectively through a decentralized application (DApp) [231]. Thus, the system provides its users full control on their personal data and access rights. Health professionals can also update the priority setting of the controller for those applications handling emergency traffic. The following subsections provide a detailed explanation of the proposed data-sharing model.

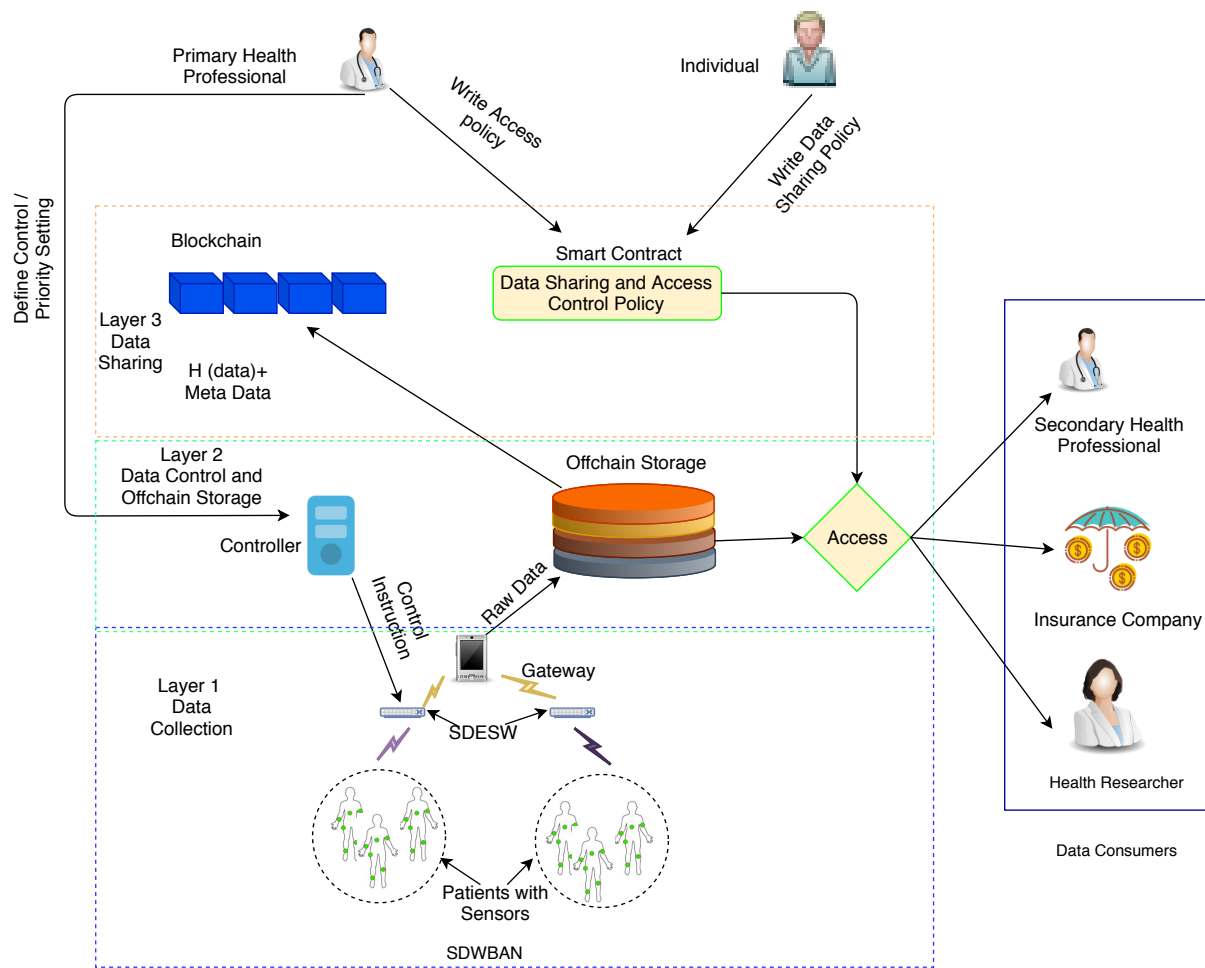


Fig. 5.2 Blockchain-enabled SDWBAN Data Sharing

5.5.1 Users in the System

In our current proposal, there are three types of users who have different capabilities in the system.

1. **Individual:** is a human being whose data is being collected using WBAN. Individuals may be referred to as patients who wear different kinds of devices/sensors both inside and outside their body. They can see their data collected by the devices using a web or mobile interface. However, they cannot control the collection of the data. They are also connected to the blockchain network via blockchain wallets. Using the blockchain wallet interface, they can define the data-sharing policies if they want to share their data with others (e.g.,

another health professional in another hospital or an insurance company). They also need to provide consent if the health professional wants to share their data with others. However, this requirement can be relaxed if the patient is in an emergency situation and unable to provide consent. An individual patient can be called a data subject.

2. **Primary Health Professional:** is a carer who provides medical services to a patient. A primary health professional can be a doctor, nurse, or diagnostic professional who directly communicates with the patient. Their access to health data is managed by the access control policies. Only certain types of health professionals have the right to share patients' data with others. They have to write their data access/sharing policy in the blockchain as a smart contract. An individual has access to this policy if the policy is related to their data. Therefore, the policy will be transparent to all involved parties. In addition to the access control policy, it is assumed that health professionals can configure the controller to manage the data flow.
3. **Data Consumers:** The data consumer is a person or a company who will be given access to the shared resources after evaluation of the data-sharing policy in the blockchain. For instance, a health insurance company, a secondary health professional and health researchers with whom the data subject (patient) wants to share their data are data consumers.

The detailed functionalities and operations of each role are specified by smart contracts between the parties, and its overall operation is demonstrated in the following subsections. The data transmission between the sensors and centralized devices around the patient is supported by WBAN based on the IEEE 802.15.6 standard, while the data transmission and storage applies to all the roles in the proposed system.

5.5.2 Data Storage

A WBAN continuously generates data and the amount of data becomes huge over a period of time. Blockchain is not typically a suitable technology for storing a large amount of data. Therefore, there is a need for a smart data management mechanism. As the most fundamental part of the healthcare system, the biomedical data collected from the sensors need to be transmitted to the storage devices for every period of time t which is specified by the stack of the controller. The controller gives the latest instructions to the switches and the wearable devices are configured to synchronize with the communication protocols. Afterward, the storage devices store the information structure which contains the patients' ID, name, corresponding medical doctor, time, and location, then they submit a transaction to the blockchain network in order to update the physical data of the patients.

1. **Off-chain Storage:** Patients' data will be collected using different kinds of sensors that are connected to the gateway via the SDESW. The gateway is the interface between the sensor network and the storage system. Due to the large volume of data, it is proposed the data is stored in the off-chain storage. However, access to data is controlled via blockchain. The off-blockchain key-value store is an implementation of Kademilia, a distributed hashtable (DHT), with added persistence using LevelDB2 and an interface to the blockchain [232]. The DHT is maintained by a network of nodes (possibly disjoint from the blockchain network), which fulfill the approved read/write transactions. Data are sufficiently randomized across the nodes and replicated to ensure high availability. It is instructive to note that alternative off-blockchain solutions could be considered for storage. For example, a centralized cloud might be used to store the data. While this requires some amount of trust in a third-party, it has some advantages in terms of scalability and ease of deployment. Another solution for off-chain storage could be the InterPlanetary File System (IPFS) [233] which is a protocol and peer-to-peer network for storing and sharing data in a distributed file system. IPFS uses content-addressing to uniquely identify each file in a global namespace

connecting all computing devices.

2. **On-chain Storage:** The hash [234] of the data is stored in the blockchain. This is sliced in time series. Each slice is hashed and then stored in the blockchain. The associated metadata is also stored in the blockchain for indexing and searching purposes.

5.5.3 Access Control

In terms of medical professionals, every individual physician only has access to the physical records of the patients who have been assigned to them. Doctors can also give instructions to the controller to prioritize certain types of data. The patients who are assigned to the specific doctor grant access to their own medical instructions.

An access control matrix [235] model is used to ensure the access control using smart contracts. The access control matrix maps the resources (objects) with their access rights. The access rights define who has what type (e.g., read, write, edit, delete) of access to any specific resource. The access control list mechanism has been employed, defined in [236], to implement the access control matrix model. The access control list (ACL) model is an object-centred approach [237] that defines for each object o , a list L that is the o 's access control rights. This list enumerates all the subjects that have o 's access rights. This list also specifies the access rights permissions (e.g., allow or deny) granted to the data consumers. To map the ACL to each object o in the off-chain, a list is defined which records the data consumers and the permissions granted to any specific object. This list is stored in the blockchain in the smart contract, which is deployed as a data-sharing contract (DS-Contract).

The DS-Contract is created/deployed on blockchain by the individual patient to specify the access rights granted to the data consumer. Hence, the owner of the contract is the individual patient. As mentioned, the used access control model is based on the ACL mechanism. Therefore, for each object (data resource), it is associated with a list that specifies the data consumer and the access rights granted to them. To

implement this mechanism, DS-Contract needs to maintain a list of the data consumers and the access rights granted to them. The access rights are granted to data consumers by the individual patient for the data which resides in the off-chain. Hence, for one data (object) one DS-Contract is deployed on the blockchain. An individual patient can create multiple DS-Contracts for multiple data that are stored in the off-chain storage, and multiple contracts for multiple data consumers for the same data resource. DS-Contract contains multiple functions that are called by an individual patient. The individual patient can add and delete data consumers, grant access and delete the policy. Off-chain storage will use the *getAccessRight()* function to verify the data consumer's access right. The functions (along with the code in Solidity) are described below. This contract is written using the Solidity language [238] in the RemixIDE [239].

addConsumer(): An individual patient calls this function when they want to grant access to a data consumer to the data residing in the off-chain storage. This function can only be executed by the individual patient as follows.

Algorithm 5.1 Pseudocode of addConsumer function

Input: consumerID, operationType, grantTime

Output: null

Steps:

- 1: **if** consumerID exists **then**
 - 2: revert; // consumer already has access rights
 - 3: **else**
 - 4: add operation type
 - 5: add permission
 - 6: add grantTime to the consumer's access list
-

deleteConsumer(): When a patient decides to revoke all access rights granted to a data consumer, they send a transaction to trigger this function. This is restricted so it can only be executed by the patient as follows.

Algorithm 5.2 Pseudocode of deleteConsumer function

Input: consumerID**Output:** null**Steps:**

- 1: **if** consumerID exists **then**
 - 2: delete consumer
 - 3: **else**
 - 4: revert; //if the data consumer doesn't exist, revert
-

getAccessRight(): This function is triggered for execution by the off-chain storage to verify the access rights of a data consumer who has requested to access/download data.

Algorithm 5.3 Pseudocode of getAccessRight function

Input: consumerID**Output:** permission**Steps:**

- 1: **if** consumerID exists **then**
 - 2: grant access permission
 - 3: **else**
 - 4: revert; //if the data consumer does not exist, revert
-

updateAccessRights(): When the patient wants to update the access rights for a given data consumer, this function is called. For example, if a data consumer is granted write and read permission, (i.e. write-permission = allowed, read-permission = allowed) and the owner wishes to revoke the write access (write-permission = denied), this function is called.

Algorithm 5.4 Pseudocode of updateAccessRight function

Input: consumerID**Output:** null**Steps:**

- 1: **if** consumerID exists **then**
 - 2: update access rights
 - 3: **else**
 - 4: revert; //if the data consumer does not exist, revert.
-

deleteDS(): A patient sends a transaction to execute this function when they want to delete the contract. A patient may call this function when they do not want to be part of the system anymore.

Algorithm 5.5 Pseudocode of deleteDS function

Input: PatientID, ContractID**Output:** null**Steps:**

- 1: **if** patientID exists **then**
 - 2: delete patient contract
 - 3: **else**
 - 4: revert; //if the patient id does not exist, revert.
-

5.5.4 Data Hashing and Integrity Verification

As previously described, only the hash of the data will be stored in the blockchain. The SHA-256 bit hash function will be used to generate a hash of the collected data. As the data is time series data, the hash will include the data point of a certain time-slot. In addition to this, the data will include metadata such as patient id, name, timestamp and time-slot. Both data and metadata are concatenated and then the hash is generated. Later, this hash value is used to verify the integrity of the data of that time-slot. The hash-contract is written to add and verify the hash of the data.

addHash(): allows the off-chain storage to add the hash of the original data and metadata into the blockchain.

Algorithm 5.6 Pseudocode of verifyHash function

Input: queryData, metaData

Output: boolean

Steps:

concatenate queryData and metaData and copy to storedData

- 1: **if** hash from blockchain matches hash of storedData **then**
 - 2: return success
 - 3: **else**
 - 4: return failure
-

verifyHash(): allows a patient or an insurance company to prove the integrity of the data which is vital for an insurance claim.

Algorithm 5.7 Pseudocode of addHash function

Input: data, metaData

Output: null

Steps:

- 1: **if** data exists **then**
 - 2: concatenate data and metaData and copy to storedData
 - 3: generate hash of storedData
 - 4: copy hash to the blockchain
 - 5: **else**
 - 6: revert;
-

5.6 Security and Privacy Analysis

In this section, the security of the proposed system is discussed in terms of confidentiality, integrity, privacy, and transparency. It is assumed that an adversary (or cooperative adversaries) can be a device in the SDWBAN, a node in the overlay

network, or the off-chain storage. Adversaries are able to sniff communications, discard transactions, create false transactions and blocks, change or delete data in storage, analyze multiple transactions in an attempt to de-anonymize a node, and sign fake transactions to legitimize colluding nodes. It is assumed that standard secure encryption methods are used in the SDWBAN and overlay tiers, which cannot be compromised by adversaries. In terms of security and privacy, two protocols are designed: the Secure Data Storage (SDS) protocol and the Secure Data Access (SDA) protocol, described as follows.

5.6.1 The SDS protocol

As discussed, data in the proposed system is stored in the off-chain storage to make sure that the SDESWs and the controllers used in the system are protected from cyber security attacks such as injection of malicious code. It is assumed that a secure trusted hardware will be used in the devices. Furthermore, to secure the generated data, a symmetric encryption mechanism like the Advanced Encryption System (AES) will be used in the proposed model. The reason is that even if someone obtains access to the off-chain storage, they won't be able to retrieve the original data. It is suggested that symmetric encryption is used because the encryption mechanism is faster and more suitable for a high volume of data generated by wireless sensors compared to asymmetric encryption mechanisms. For this encryption, the symmetric key has to be either pre-distributed or negotiated between the off-chain storage and the wireless sensors by a secure key exchange mechanism.

5.6.2 The SDA protocol

To access the data, the data consumer needs to satisfy the access control policy stored as smart contracts in the blockchain (explained in the previous section). After the data consumer's access is granted, the blockchain provides an access token and re-direct the data consumer to the off-chain storage. The off-chain storage allows the data consumer

based on the token. This token can be considered as something like the OAuth token [240] which has a specific scope and valid lifetime. The proposed token in this study also works for any particular data point (e.g., scope in OAuth) and remains valid for a specific time period. The data point encodes the identity of the data subject (e.g., whose data) as well as the data type (e.g., blood pressure vs heart-rate). To securely communicate the token between the blockchain module and the off-chain storage, the asymmetric encryption mechanism is used. That means the token is encrypted by the public key of the off-chain node and thus can only be decrypted by its private key. Since individuals are registered with the blockchain, all the access control policies related to their data are always visible to them. Blockchain ensures that no single entity/authority/malicious actor would be able to change the access control policies due to the “*immutability*” property of blockchain. In terms of privacy, since consortium-based blockchain is used, only the authorized person in the blockchain will have access to the personal data, unlike public blockchain, where everybody has access to all information stored in the blockchain. Therefore, the individual’s privacy will be ensured in the proposed system.

5.6.3 Security Analysis of the Protocols

Since SDWBANs deal with sensitive medical information, it is important to ensure that the proposed protocol is secure and cannot be compromised by malicious parties or individuals. This means that nobody other than the intended data consumer should obtain access to the shared data resource, and shared data should remain confidential during access time. Therefore, a vigorous security analysis is carried out using an automated security protocol verifier, namely, Automated Validation of Internet Security Protocols and Applications (AVISPA) [241] on both SDS and SDA protocols.

AVISPA is a popular security protocol verifier which uses mathematical logic to analyze the security properties of any given protocol. Researchers have used this tool to model and analyze popular security protocols such as SAML and OpenID [242], [243]. In AVISPA, the security protocols are specified using a special specification language

called the High-Level Protocol Specification Language (HLPSSL) [244]. Temporal Logic of Actions (TLA) is used in HLPSSL to allow the protocol verifier to specify their protocols in a more human readable way. Different entities are defined using the *Role* and the *actions* are associated with Roles. The parameters that are needed to communicate between different Roles are done using secure channels. These entities and their roles and interactions are specified using a special notation called the Alice-Bob notation as shown in listing 5.1, where two entities A and B are communicating a secret by using a secure Server S . The messages are encrypted by KAS , a symmetric key shared between A and S , when communicated between A and S . Similarly, messages exchanged between B and S are encrypted by KBS , a secret key only known to B and S .

```

1      1.  $A \rightarrow S : \{KAB\}_{KAS}$ 
2      2.  $B \rightarrow S : \{KAB\}_{KBS}$ 

```

Listing 5.1 Alice-Bob Notation

The security properties that need to be verified are set using the construct called *goal*. It supports two types of security goals: i) secrecy and ii) authentication. Here, secrecy refers to the goal which asserts that a certain value should be kept secret between only two entities. The format for specifying a secrecy goal is: *secrecy_of id*. The *id* represents a protocol *id*, variable in HLPSSL. The *id* is then embedded inside a *goal* fact which is written in HLPSSL as: *secret(value; id; A; B)*. This indicates that the goal represented using *id* asserts that the value should be kept secret between entities A and B . Then, the security fact is added as part of the transitions of the entity which generates the value. In contrast, the authentication goal checks if an entity is correct in believing that the other entity is the intended peer of a certain value upon reaching a certain state. The format for specifying an authentication goal is: *authentication_on id*, where *id* represents a protocol *id* variable in HLPSSL. The goal facts related to the authentication goal are witness and request.

The authentication of the data consumer during the data access and the data confidentiality are checked in two parts: i) between the wireless sensors and the off-chain storage and ii) between the data consumer and off-chain storage.

5.6.3.1 Protocol Formalization

All the entities of the proposed protocols are modelled using HLPsL by defining each role (e.g., wireless sensors (WS), off-chain storage (OCS), blockchain(BC), and data consumer (DC)) and then specifying their interactions. The modelling of a user in our protocols using HLPsL starts with dening some variables. The notations KDC, KOCS and KBC represent the public keys of the data consumer, off-chain and the blockchain respectively that are used in the encryption and decryption processes. It should be noted that symmetric encryption is used between WS and OCS and asymmetric encryption is used between OCS, BC and DC. As stated earlier, in this protocol verification, first, the secrecy of the *data* exchanged is checked between WSs and the OCS and *access token* communicated between the BC and the OCS. The authentication of the DC with the OCS is also verified.

The transitions in each role essentially denes the interactions among different entities. The role starts from an initial state (for the user this is θ) and upon receiving a message in a receiving channel, it switches to its next state. The receiving and sending of messages for the role are analogous to the respective interactions presented in the *A-B* notation. It is to be noted that HLPsL does not support a secure (HTTPS) channel. Therefore, to ensure security and simulate the behaviour of a secure channel, all messages are encrypted with the corresponding keys before they are sent over any (insecure) channel.

Finally, several secrecy (data and access token) and authentication (of data consumer) security goals are specied. During the testing of the SDA protocol, whether these goals are met or not is verified. The verification suggests that the designed protocols are secure as can be seen in Fig. 5.3.

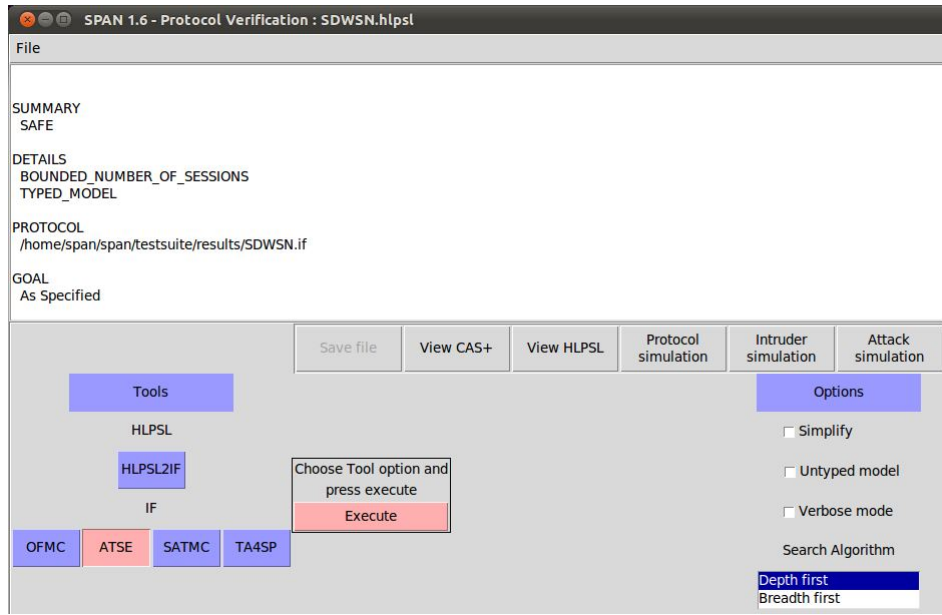


Fig. 5.3 Protocol Verification Using AVISPA

5.7 Results and Analysis

In this section, an overview of the implementation platforms, a list of the simulation parameters, and an analysis of the experiment outcomes are provided in detail.

5.7.1 Experiment Setup

The proposed model is simulated using Castalia-3.2 version [196] on Ubuntu 16.04.4. Since there is no simulation platform available for blockchain enabled SDWBAN implementation, the experiment is performed in two stages. First, using the Castalia simulator, the latency between sensors and the gateway node is calculated for different application-groups and then the total time required to execute smart contracts and store data in the blockchain is computed. Since, the proposed model implements blockchain on layer 2, layer 1 devices are not affected by any blockchain operations. The simulation parameters used in the first stage are listed in Table 5.1. The simulation is conducted for two application groups where group1 and group2 consist of 5 and 10 applications respectively to visualize the impact of an increased number of applications in the output. Different application IDs are assigned to each group, so that the SDES

treats the data packets from these IDs as a new application. Hence, upon the arrival of a new application, the SDESW makes a query to the controller and retrieves the packet forwarding instructions. The simulation has run for 100 iterations and the outputs are analyzed in terms of the latency experienced by each group of applications. The simulation results of this stage in combination with stage 2 outcomes would help to realize the trade-off between QoS and implementation cost. This would also be helpful in fine-tuning the implementation options such as consensus and block size.

Table 5.1 Simulation Parameters

Parameter	Value	Parameter	Value
Radio range (BS, SDESW, Controller)	~ 8 m, ~ 20 m, ~ 20 m	Reference Distance (d_0)	1 m
Transmission Power (SDESW, BS)	0 dBm, -10 dBm	Simulation Area	75x75 m ²
0.8Data Rate, Modulation Type, Bits Per Symbol, Bandwidth	250 Kbps, PSK, 4, 20 MHz,	Number of BS, Gateway	200, 4
Noise Bandwidth, Noise Floor, Sensitivity	194 MHz, -100 dBm, -95 dBm	BS density	8 nodes / 225 m ²
Free Space Path Loss exponent	2.4	Total SDESW	25 (1 node per sector)
Initial Average Path Loss ($PL(d_0)$)	55 dB	Total Controller	5
Gaussian Zero-Mean Random Variable (X_α)	4.0	Number of Clusters	25

In terms of blockchain implementation, proof-of-concept (PoC) smart contracts are implemented in Ethereum private blockchain using the solidity programming language and on the online Remix IDE. The time to execute each function in both DS-Contract and Hash-Contract using transaction time is calculated. Finally, the time needed to receive data packets from the gateway node and the transaction time is computed in blockchain to run the smart contracts. The experiment outcomes of both stages are presented below.

5.7.2 Experiment Outcomes

The first experiment outcomes exhibit the time required for each group of applications to be delivered successfully to the destination gateway. Fig. 5.4(a) shows latency over simulation time (3600sec) and it can be seen that application group1 experiences the

least amount of delay. When the number of applications increases as in group2, data packets take longer to reach the gateway. This is due to the increased amount of data traffic in the communication channel between the controller and SDESW. As the number of applications increases over the time, SDESW fails to find a match in the routing table. Therefore, whenever a new application sends a data packet to SDESW, the SDESW sends a packet in request to the controller and retrieves an appropriate instruction pertaining to the new application data packet. Thus, it creates traffic load and incurs more time to resolve an unknown application data. To further analyze the output of the simulation results, the average, 95th, 5th and Cumulative Distribution Function (CDF) graph is also analyzed. For instance, in Fig. 5.4(c), at the 90th percentile point, the group1 application experiences approximately 53.48 ms latency whereas the latency for group2 applications is approximately 76.81 ms.

For blockchain implementation, the time to execute each function in both DS-Contract and Hash-Contract using transaction time are calculated. Fig. 5.5(a) shows the computation time for adding and deleting a data consumer, getting and updating access right, and deleting the DS-contract with respect to an increase in the transaction number. The result depicts a linear growth in signing and validation times with an increase in the transaction number. Similarly, Fig. 5.5(b) shows the computation time for storing the hash of the data in the blockchain in terms of transaction time. It also presents the verification time for the queried data.

For blockchain implementation, the time to execute each function is calculated in both DS-Contract and Hash-Contract using transaction time. Fig. 5.5(a) shows the computation time for adding and deleting data consumer, getting and updating access right, and the deletion of the DS-contract with respect to an increase in the transaction number. The result depicts a linear growth in signing and validation times with an increase in the transaction number. Similarly, Fig. 5.5(b) shows the computation time for storing the hash of data in the blockchain in terms of transaction time. It also presents the verification time for the queried data.

From the experiment data, it is evident that the latency to send data from the sensors

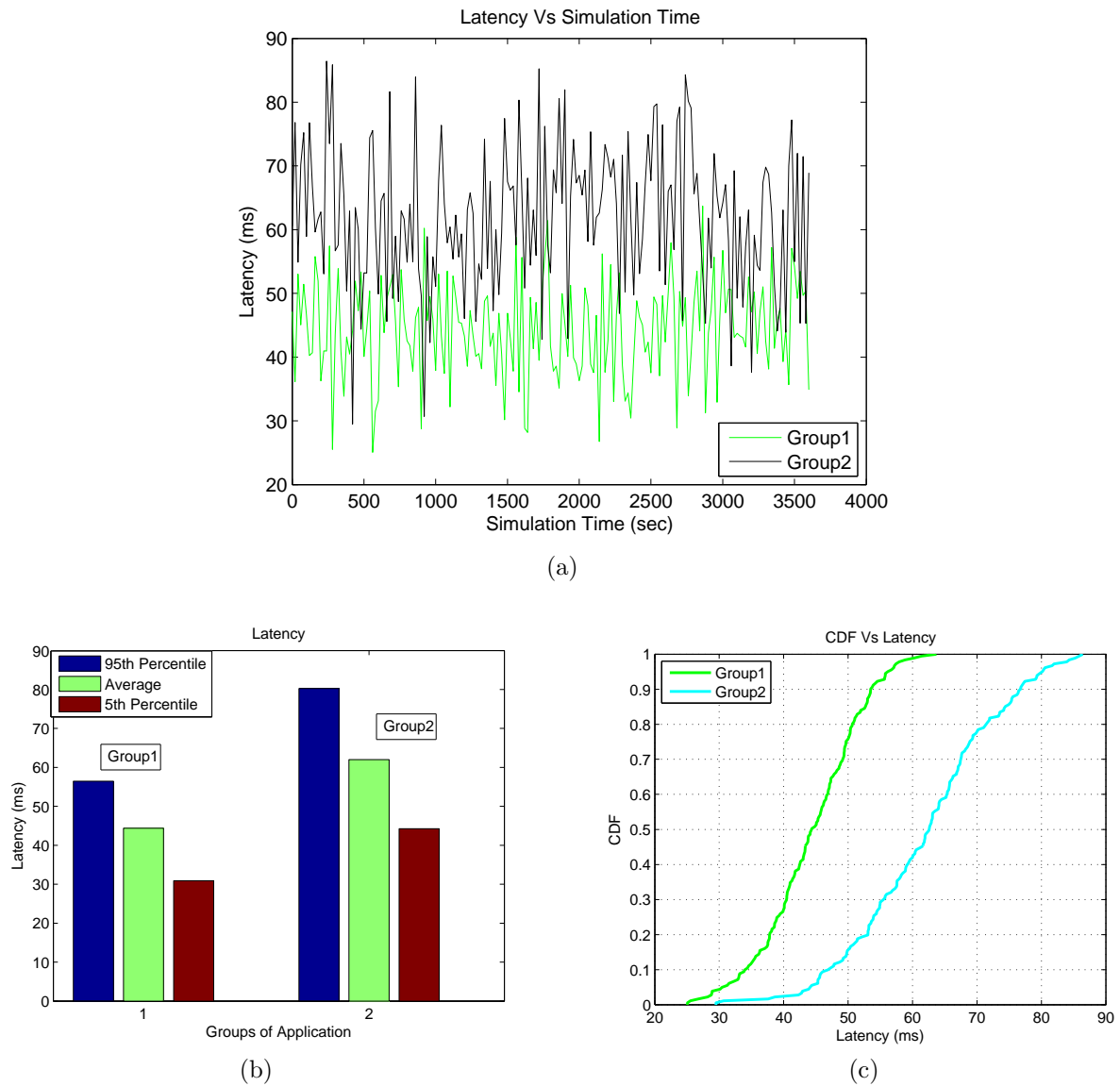
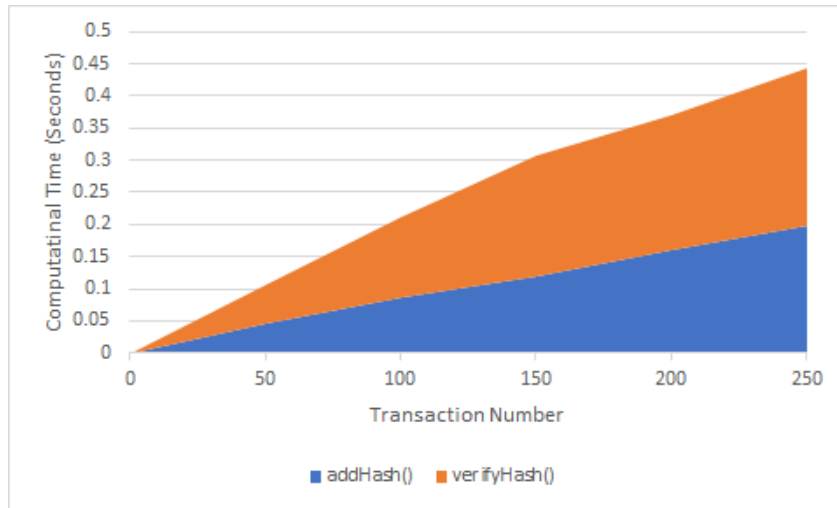


Fig. 5.4 (a) Latency vs Simulation Time, (b) Latency vs Group of Application, (c) CDF of Latency

to the gateway is very small and is almost in real-time. The overhead added by the smart contract is also reasonable for real-time systems. However, it needs to be mentioned that the smart contract execution time can vary based on the number of nodes and the setup of the environment. The performance can be improved in a consortium-based environment compared to our proof-of-concept implementation. Overall, the proposed solution can facilitate data sharing with greater transparency and integrity without adding significant overhead.



(a) Computation time for DS-Contract



(b) Computation time for Hash-Contract

Fig. 5.5 Computation time of contracts

5.7.3 Blockchain vs Cloud Implementation

Since there is no platform available for blockchain-based SDWBAN implementation, it is not possible to make a direct comparison between the performance of the proposed system and a cloud based system. However, implementations from the healthcare users' perspective and the experiment results obtained for these two platforms provide some critical insights that might be interesting for researchers. In this experiment, first, *verification* and *hash generation and uploading* time are computed for data of different size on the Ethereum platform using a local network. The aims of this experiment are:

i) to calculate the total time required to search for a data item in the blockchain and receive the response, and ii) to calculate the time required to generate the hash of the given data and store the hash in the blockchain. For cloud implementation, the time required to retrieve data of different sizes (i.e, response time) which is file creation, updating and deletion time from the AMAZON S3 cloud server (Sydney) are calculated using the NBN connection with 20Mbps uploading speed. The following graphs present the average outcomes of 100 trials conducted in this experiment.

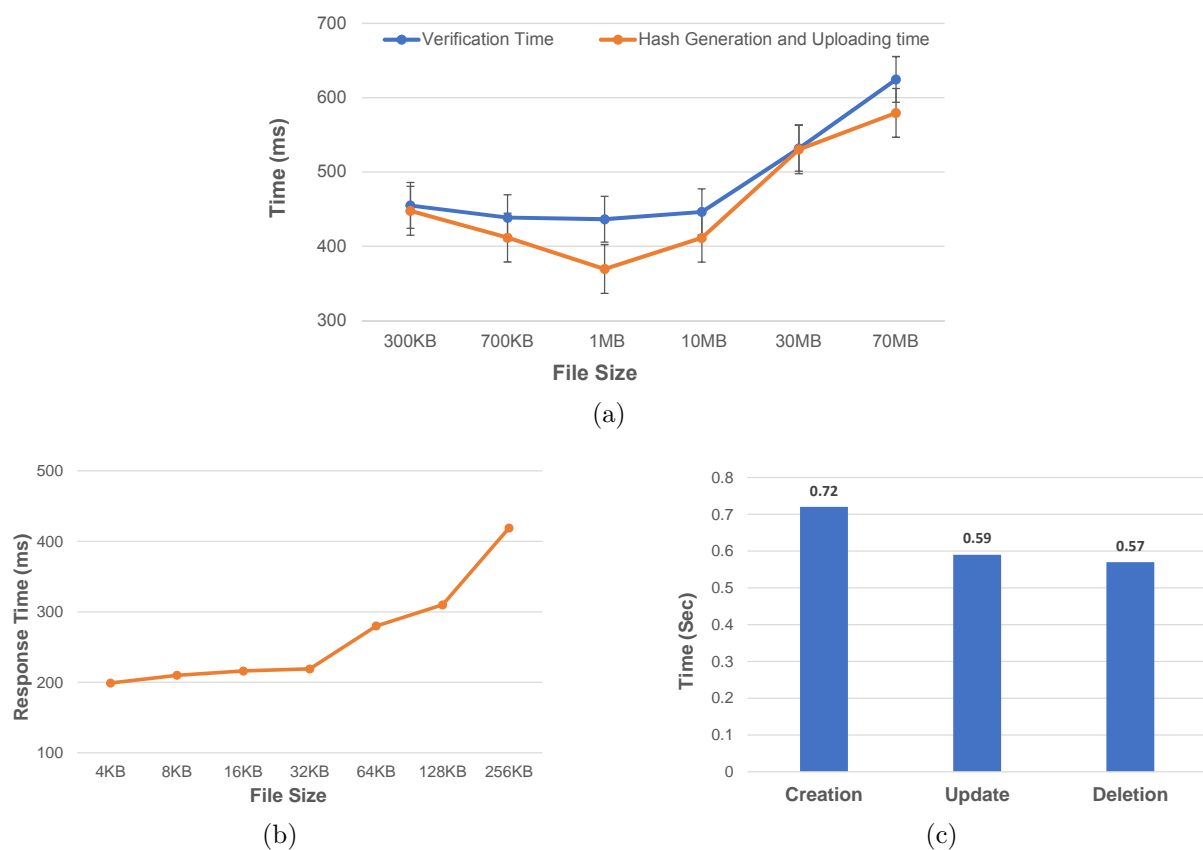


Fig. 5.6 (a) Verification, hash generation and updating time in blockchain, (b) Data retrieval time from cloud storage, (c) File creation, updating and deletion time in the cloud

Fig. 5.6(a) presents the data verification time, hash generation and uploading time on the blockchain for files of different sizes. It can be seen that data verification requires more time compared to hash generation and uploading in most of the cases. This is due to the need to search for the data item in the chain using the hash index, retrieving it and sending back the response. However, hash generation and uploading the hash of the data items into blockchain requires comparatively less time as the hash algorithm is

very fast and the blockchain is implemented in the local network. On the other hand, the response time for cloud-based systems is very high, as shown in Fig. 5.6(b). Since the cloud system relies on the Internet, it experiences a different level of latency every time. The average response time indicates that it requires a significant amount of time to retrieve information from the cloud. However, the response time can be reduced by using different techniques such as Amazon S3 Transfer Acceleration. Finally, Fig. 5.6(c) shows the file creation, updating and deletion time for an 8KB text file. It can be seen that the file creation operation takes more time than the update and deletion operations in the cloud.

From the outcomes, it is evident that the blockchain-based system is able to outperform traditional cloud-based systems in terms of performance. Since the consortium blockchain is implemented in a private environment with a small number of trusted nodes, the network will experience very low latency and low overhead. However, it would be interesting to see how the proposed system will perform in the public platforms although the consortium blockchain is the best choice to solve the data sharing problem in healthcare.

5.8 Summary

In this chapter, an architectural framework is proposed that incorporates blockchain with SDWBAN to facilitate information exchange in a healthcare system. In addition, a fine-grained access control policy is designed using a smart contract to ensure data owners have full control over their own data. The proposed architecture is also evaluated in a simulator and a test environment to measure its effectiveness. The experiment outcomes show that the proposed blockchain-based framework incurs very low overhead and thus is suitable for SDWBAN adoption as a data-sharing platform.

Chapter 6

Conclusions and Future Work

This chapter presents the concluding remarks of the thesis and the future research directions in the context of SDWBAN.

6.1 Conclusions

Developing a robust and flexible WBAN architecture is paramount in the area of remote patient monitoring. The architecture of WBAN should be able to provide seamless services while adopting new applications during its operation. A range of issues still need to be resolved to guarantee QoS in WBAN. At this stage, a comprehensive literature survey is conducted on WBAN which encompasses the architecture and operational functionalities of WBAN, the diverse range of applications in both medical and non-medical sectors, the supporting technologies of WBAN, and the challenges of WBAN implementation. Further investigation is carried out to identify the limitations of the existing architectural framework, application traffic priority arrangements, vendor dependencies, and the relevant security issues. Based on the literature survey, the assimilation of two cutting- edge technologies i.e. SDN and blockchain with WBAN may have huge potential in the healthcare domain. To this end, the primary focus of this thesis is to design a flexible WBAN architecture based on the SDN principle, called

SDWBAN. Then, to support the SDWBAN framework, a mathematical model is developed to observe the relationship between the number of controllers, SDESWs and BSs in an optimal manner. Finally, a secure data-sharing platform based on blockchain for SDWBAN is proposed which is implemented in an Ethereum private blockchain environment to visualize the performance of the proposed framework.

First, an SDWBAN framework is designed that adopts the SDN functionalities in order to support patient monitoring in healthcare. The SDWBAN utilizes cluster-based routing named SBD to traverse data packets from the source to the destination. An application classification algorithm is developed that classifies normal and emergency applications for the purpose of traffic priority arrangements. Emergency data traffic is given priority over normal data traffic to ensure that critical physiological data reach the healthcare professionals within the defined time constraints. The proposed framework is implemented in Castalia 3.2 software which is built on top of an OMNET++ simulator. The first simulation scenario includes various groups of applications where the number of applications increases gradually. The purpose is to observe the scalability and flexibility of the SDWBAN framework as the number of applications increases. The simulation output illustrates that the proposed SDWBAN framework is capable of accommodating a large number of applications within an acceptable PDR and latency. The second simulation scenario involves a various number of application groups where the groups are designed to have emergency and normal applications. The aim is to inspect the priority of the emergency application over normal application traffic which is based on the application classification algorithm. The results reveal that as the number of applications (normal and emergency) grow in different groups, emergency applications are always given priority over normal applications with satisfactory PDR and latency. The results from both scenarios of the simulation establish the fact that the proposed SDWBAN framework is valid.

In the next stage, the focus is on the design of the control plane for the proposed SDWBAN framework. The research investigates the various influential parameters pertaining to the design of the control plane for SDN incorporation in WBAN. A mathematical model is devised that includes three influential parameters i.e. controller number, the number of SDESW and total flow resolution time. The mathematical

model establishes a relationship between these three parameters and determines the optimal number of controllers that is required to cover the implementation area. The aim is to provide an optimal number of controllers that can support a fixed number of SDESWs and thus, BSs. The analysis of the mathematical model determines the optimum number of physical resources to support the proposed SDWBAN framework. Furthermore, the results from the analytical output and simulation support the optimization model for the control plane design of the proposed SDWBAN.

Finally, the focus is on developing a secure data-sharing platform in SDWBAN. The healthcare data received from the SDWBAN needs to be shared with multiple parties without compromising authenticity, integrity and confidentiality. Hence, the potential and the challenges of incorporating blockchain with SDWBAN in the healthcare domain have been established. A secure data-sharing platform is proposed by integrating blockchain features with SDWBAN. The blockchain-based secure data-sharing platform includes the design of a smart control to ensure the data owner retains control of their data. The blockchain implementation employs an Ethereum private blockchain using the Solidity language in RemixIDE. The experiment computes the time required for DS-Contract and Hash-Contract for a various number of transactions. The computational outcome from the experiment reveals that a low overhead is incurred by the smart contract. Furthermore, it also establishes the fact that the overhead added by the smart contract is acceptable for a real-time system.

6.2 Practical Implication

The practical implication of this research is in healthcare domains such as in elderly home, hospitals or clinics etc. The simulation outcome of this study beckons the practical implication to be a success with flexible management of various healthcare applications which would adopt multi-vendor WBAN application sensors. A system developer may consider the mentioned implementation scenarios as this study introduces a number of heterogeneous applications with normal and emergency data

traffic. Since numerous applications of WBAN displays various characteristics, the practical implementation might slightly deviate from the simulation-based result. However, the implementation of this framework in real-time heterogeneous WBAN applications monitoring is expected to be flexible with enhanced administrative control. With much more programmability and administrative control in the proposed SDWBAN framework, the adoption of multi-vendor WBAN sensors in the implementation area would ease the management complexity significantly. This will benefit real-time healthcare monitoring widely.

The optimization analysis of this study would also assist practical enactment to be effective in terms of designing the network with necessary resources. The analytical output related to the optimization of control plane would aid the system developer to maintain a strict delay requirement for the WBAN applications and thus, maintain optimum performance. Finally, the secure data-sharing platform would ensure secrecy of healthcare data while dealing with multiple entities.

6.3 Future Research Works

A number of research directions can be considered as future work to make the proposed SDWBAN framework more robust. These are outlined as follows.

- **Variable Payload Size:** Since various applications in WBAN capture data of various sizes, this can affect the overall network performance in terms of PDR and latency. Therefore, in future study, a variable payload size can be included to visualize a true heterogeneous WBAN environment in the existing SDWBAN framework.
- **Explore Routing Protocols:** Routing protocols play a crucial role in the successful delivery of data packets in the network. Hence, the performance of the proposed SDWBAN framework can be compared by implementing different cluster-based routing protocols.

- **Energy Efficiency:** Since the BSs are small and battery powered, undertaking an analysis of the energy efficiency of this work is also be a significant future aspect. An improvement to the energy efficiency of WBAN due to the incorporation of SDN can be explored. Furthermore, various energy harvesting (EH) techniques such as Photovoltaic Energy Harvesting (PVEH), Piezoelectric Energy Harvesting (PEH), Thermoelectric Energy Harvesting (TEH), RF Energy Harvesting (RFEH) etc. can be implemented in WBAN sensors.
- **Synchronization of Controllers:** To maintain an abstract view of the network, synchronization between controllers can be considered. Therefore, the east-west communication between the controllers can be taken into account in the control plane design.
- **Influential Factors of Control Plane:** The proposed optimization model can be explored by considering more influential parameters to observe the effect on network performance. As previously mentioned, east-west communication can be considered between controllers which may increase the overhead in the system. In addition, the proposed optimization model does not consider the delay incurred in gaining channel access. Hence, the back-off time or time to gain access in the channel can be included in the optimization model. The ultimate effect can be analyzed by observing the network performance and end-to-end delay.
- **Number of SDESWs and Processing Capacity of Controller:** It would be interesting to observe PDR and latency by varying the number of SDESWs while keeping the range of the number of controllers from 4 to 6. This will enable the effect of the flow request originating from a various number of SDESWs to be visualized. The service rate of the controller could be varied in the optimization model since with a higher service rate, the better the flow resolve rate. Therefore, a lower number of controllers would be able to support a higher number of SDESWs.
- **Health Insurance Claim:** Generally, health insurance claims take a significant amount of time to process. The secure data-sharing platform can be used to speed up the insurance claim process through verification. Therefore, one significant

research direction can be computing the time required for an insurance claim to be processed by the health insurer.

- **Comparison with Consortium-based Blockchain:** The current PoC smart contract is implemented using Ethereum private blockchain. In future study, the consortium-based blockchain environment can be utilized to compare the PoC implementation with the proposed one in terms of DS-contract and Hash-Contract computation. Moreover, various performance metrics such as reliability, scalability and throughput can be evaluated using a similar test environment to enhance accuracy and robustness.

References

- [1] “Research and markets: Machine-to-machine (m2m) communication in healthcare 2010-20: Reviews the major drivers and barriers for growth of m2m,” May 2011.
- [2] A. Drescher, “A survey of software-defined wireless networks,” *Dept. Comput. Sci. Eng., Washington Univ. St. Louis, St. Louis, MO, USA, Tech. Rep.*, pp. 1–15, 2014.
- [3] L. Hu, M. Qiu, J. Song, M. S. Hossain, and A. Ghoneim, “Software defined healthcare networks,” *IEEE Wireless Communications*, vol. 22, no. 6, pp. 67–75, 2015.
- [4] G. Cova, H. Xiong, Q. Gao, E. Guerrero, R. Ricardo, and J. Estevez, “A perspective of state-of-the-art wireless technologies for e-health applications,” in *2009 IEEE International Symposium on IT in Medicine & Education*, vol. 1, pp. 76–81, 2009.
- [5] G. B. Satrya, N. D. Cahyani, and R. F. Andreta, “The detection of 8 type malware botnet using hybrid malware analysis in executable file windows operating systems,” in *Proceedings of the 17th ACM International Conference on Electronic Commerce 2015*, p. 5, 2015.
- [6] G. B. Satrya and S. Y. Shin, “Optimizing rule on open source firewall using content and pcre combination,” *Journal of Advances in Computer Networks*, vol. 3, no. 3, pp. 308–314, 2015.
- [7] M. Al Shayokh, A. Abeshu, G. Satrya, and M. Nugroho, “Efficient and secure data delivery in software defined wban for virtual hospital,” in *2016 IEEE International*

- Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, pp. 12–16, 2016.
- [8] HITInfrastructure, “Benefits of Software-Defined Networking in Healthcare, [Available Online]:~<https://hitinfrastructure.com/features/benefits-of-software-defined-networking-in-healthcare>, [Accessed on: 2019-01-09].”
- [9] V. Varadharajan, U. Tupakula, and K. Karmakar, “Secure monitoring of patients with wandering behavior in hospital environments,” *IEEE Access*, vol. 6, pp. 11523–11533, 2018.
- [10] T. Slattery, G. Audin, D. Ward, C. Wilson, Z. Kerravala, J. Simmons, S. McGee-Smith, D. Michels, and B. Schultz, “Healthcare sdn: A good match?, [Available Online]:~<https://www.nojitter.com/healthcare-sdn-good-match>, [Accessed on: 2019-05-15].”
- [11] Artesyn, “How sdn can benefit healthcare, [Available Online]:~<https://www.rcrwireless.com/20170714/software/how-sdn-can-benefit-healthcare-tag99>, [Accessed on: 2019-05-17].”
- [12] B. T. De Oliveira, L. B. Gabriel, and C. B. Margi, “Tinysdn: Enabling multiple controllers for software-defined wireless sensor networks,” *IEEE Latin America Transactions*, vol. 13, no. 11, pp. 3690–3696, 2015.
- [13] M. A. Hassan, Q.-T. Vien, and M. Aiash, “Software defined networking for wireless sensor networks: a survey,” *Advances in Wireless Communications and Networks*, vol. 3, no. 2, pp. 10–22, 2017.
- [14] “MiXiM-Simu 2013, [Available Online]:~<https://sourceforge.net/projects/mixim/files/mixim/>, [Accessed on: 2020-05-31].”
- [15] D. Pediaditakis, Y. Tselishchev, and A. Boulis, “Performance and scalability evaluation of the castalia wireless sensor network simulator,” in *Proceedings of the 3rd International ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) Conference on Simulation Tools and Techniques, SIMUTools ’10*, (Brussels, BEL), 2010.

- [16] K. Ahmed, N. S. Nafi, J. O. Blech, M. A. Gregory, and H. Schmidt, "Software defined industry automation networks," in *2017 the 27th IEEE International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1–3, 2017.
- [17] N. S. Nafi, K. Ahmed, M. A. Gregory, and M. Datta, "Software defined neighborhood area network for smart grid applications," *Future Generation Computer Systems*, vol. 79, pp. 500 – 513, 2018.
- [18] N. S. Nafi, K. Ahmed, M. Datta, and M. A. Gregory, "A novel software defined wireless sensor network based grid to vehicle load management system," in *2016 the 10th IEEE International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1–6, 2016.
- [19] A. Bouazizi, G. Zaibi, M. Samet, and A. Kachouri, "Wireless body area network for e-health applications: Overview," in *2017 International Conference on Smart, Monitored and Controlled Cities (SM2C)*, pp. 64–68, 2017.
- [20] D. S. Gangwar, "Biomedical sensor network for cardiovascular fitness and activity monitoring," in *2013 IEEE Point-of-Care Healthcare Technologies (PHT)*, pp. 279–282, 2013.
- [21] S. V. B. Peddi, A. Yassine, and S. Shirmohammadi, "Cloud based virtualization for a calorie measurement e-health mobile application," in *2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*, pp. 1–6, 2015.
- [22] H.-y. Zhou and K.-m. Hou, "Pervasive cardiac monitoring system for remote continuous heart care," in *2010 the 4th IEEE International Conference on Bioinformatics and Biomedical Engineering*, pp. 1–4, 2010.
- [23] M. Ghamari, B. Janko, R. S. Sherratt, W. Harwin, R. Piechockic, and C. Soltanpur, "A survey on wireless body area networks for ehealthcare systems in residential environments," *Sensors*, vol. 16, no. 6, p. 831, 2016.
- [24] T. Hayajneh, G. Almashaqbeh, S. Ullah, and A. V. Vasilakos, "A survey of wireless technologies coexistence in wban: analysis and open research issues," *Wireless Networks*, vol. 20, no. 8, pp. 2165–2199, 2014.

- [25] D. P. Tobón, T. H. Falk, and M. Maier, “Context awareness in wbans: a survey on medical and non-medical applications,” *IEEE Wireless Communications*, vol. 20, no. 4, pp. 30–37, 2013.
- [26] R. A. Khan and A.-S. K. Pathan, “The state-of-the-art wireless body area sensor networks: A survey,” *International Journal of Distributed Sensor Networks*, vol. 14, no. 4, pp. 1–23, 2018.
- [27] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, “Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications,” *Egyptian Informatics Journal*, vol. 18, no. 2, pp. 113–122, 2017.
- [28] M. M. Alam and E. B. Hamida, “Surveying wearable human assistive technology for life and safety critical applications: Standards, challenges and opportunities,” *Sensors*, vol. 14, no. 5, pp. 9153–9209, 2014.
- [29] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, “A survey on wireless body area networks: Technologies and design challenges,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1635–1657, 2014.
- [30] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, “Wireless body area networks: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.
- [31] R. Negra, I. Jemili, and A. Belghith, “Wireless body area networks: Applications and technologies,” *Procedia Computer Science*, vol. 83, pp. 1274–1281, 2016.
- [32] B. Antonescu and S. Basagni, “Wireless body area networks: challenges, trends and emerging technologies,” in *ICST Proceedings of the 8th international conference on body area networks*, pp. 1–7, 2013.
- [33] S. H. Shin, R. Kamal, R. Haw, S. I. Moon, C. S. Hong, and M. J. Choi, “Intelligent m2m network using healthcare sensors,” in *2012 the 14th IEEE Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pp. 1–4, 2012.

- [34] D. Chandramouli, B. Covell, V. Held, H. Hietalahti, J. Hofmann, and R. Ratasuk, “Massive machine type communication and the internet of things,” *5G for the Connected World*, pp. 377–439, 2019.
- [35] E. Kartsakli, A. S. Lalos, A. Antonopoulos, S. Tennina, M. D. Renzo, L. Alonso, and C. Verikoukis, “A survey on m2m systems for mhealth: a wireless communications perspective,” *Sensors*, vol. 14, no. 10, pp. 18009–18052, 2014.
- [36] T. ETSI, “102 690, machine-to-machine communications (m2m), functional architecture,” *European Telecommunications Standards Institute (ETSI)*, vol. 20, p. 332, 2011.
- [37] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, “A comprehensive survey of wireless body area networks,” *Journal of medical systems*, vol. 36, no. 3, pp. 1065–1094, 2012.
- [38] IEEE Standards Coordinating Committee, “IEEE standard for safety levels with respect to human exposure to radio frequency electromagnetic fields, 3khz to 300ghz,” *IEEE C95. 1-1991*, 1992.
- [39] S. N. Ramli and R. Ahmad, “Surveying the wireless body area network in the realm of wireless communication,” in *2011 the 7th IEEE International Conference on Information Assurance and Security (IAS)*, pp. 58–61, 2011.
- [40] B. Gyselinckx, R. Borzi, and P. Mattelaer, “Human++: Emerging technology for body area networks,” in *Wireless Technologies*, pp. 227–246, CRC Press, 2007.
- [41] S. Ullah, P. Khan, N. Ullah, S. Saleem, H. Higgins, and K. S. Kwak, “A review of wireless body area networks for medical applications,” *International Journal of Communications, Network and System Sciences*, vol. 2, no. 8, pp. 797–803, 2010.
- [42] D. Lewis, “802.15. 6 call for applications in body area networks response summary,” *15-08-0407-05-0006*, 2008.
- [43] N. de Vicq, F. Robert, J. Penders, B. Gyselinckx, and T. Torfs, “Wireless body area network for sleep staging,” in *2007 IEEE Biomedical Circuits and Systems Conference*, pp. 163–166, 2007.

-
- [44] H.-T. Chu, C.-C. Huang, Z.-H. Lian, and J. J. Tsai, “A ubiquitous warning system for asthma-inducement,” in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC’06)*, vol. 2, pp. 186–191, 2006.
- [45] World Health Organization, “Global report on diabetes, [Available Online]: <http://www.who.int/news-room/fact-sheets/detail/diabetes>, [Accessed on: 2019-03-29].”
- [46] Diabetes Australia, “Diabetes in Australia, [Available Online]: <https://www.diabetesaustralia.com.au/diabetes-in-australia>, [Accessed on: 2019-04-02].”
- [47] World Health Organization, “Global cancer rates could increase by 50% to 15 million by 2020, [Available Online]: <http://www.who.int/mediacentre/news/releases/2003/pr27/en/>, [Accessed on: 2019-02-02].”
- [48] A. K. Teshome, B. Kibret, and D. T. Lai, “A review of implant communication technology in wban: Progress and challenges,” *IEEE reviews in biomedical engineering*, vol. 12, pp. 88–99, 2019.
- [49] J. Habetha, “The myheart project-fighting cardiovascular diseases by prevention and early diagnosis,” in *the 28th IEEE Annual International Conference of the Engineering in Medicine and Biology Society, 2006. EMBS’06*, pp. 6746–6749, 2006.
- [50] J. Luprano, J. Sola, S. Dasen, J. M. Koller, and O. Chetelat, “Combination of body sensor networks and on-body signal processing algorithms: the practical case of myheart project,” in *International Workshop on Wearable and Implantable Body Sensor Networks (BSN’06)*, pp. 79–82, April 2006.
- [51] T. Tanaka, T. Fujita, K. Sonoda, M. Nii, K. Kanda, K. Maenaka, A. C. C. Kit, S. Okochi, and K. Higuchi, “Wearable health monitoring system by using fuzzy logic heart-rate extraction,” in *IEEE World Automation Congress 2012*, pp. 1–4, 2012.
- [52] S. Khan, A.-S. K. Pathan, and N. A. Alrajeh, *Wireless sensor networks: Current status and future trends*. Boca Raton, FL: CRC press, 2012.

-
- [53] D. H. Lee, A. Rabbi, J. Choi, and R. Fazel-Rezai, "Development of a mobile phone based e-health monitoring application," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 3, no. 3, pp. 38–43, 2012.
- [54] S. Kannan, "Wheats: a wearable personal healthcare and emergency alert and tracking system," *Eur. J. Sci. Res*, vol. 1, pp. 382–393, 2012.
- [55] İ. Kirbaş and C. Bayılmış, "Healthface: A web-based remote monitoring interface for medical healthcare systems based on a wireless body area sensor network," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 20, no. 4, pp. 629–638, 2012.
- [56] M. Zhang and A. Sawchuk, "A customizable framework of body area sensor network for rehabilitation," in *International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL)*, pp. 1–6, 2009.
- [57] A. Hadjidj, M. Souil, A. Bouabdallah, Y. Challal, and H. Owen, "Wireless sensor networks for rehabilitation applications: Challenges and opportunities," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 1–15, 2013.
- [58] S. Bouwstra, W. Chen, L. Feijs, and S. B. Oetomo, "Smart jacket design for neonatal monitoring with wearable sensors," in *2009 the Sixth IEEE International Workshop on Wearable and Implantable Body Sensor Networks*, pp. 162–167, 2009.
- [59] A. Basak, S. Narasimhan, and S. Bhunia, "Kims: Kids' health monitoring system at day-care centers using wearable sensors and vocabulary-based acoustic signal processing," in *2011 the 13th IEEE International Conference on e-Health Networking, Applications and Services*, pp. 1–8, 2011.
- [60] A. Guraliuc, A. Serra, P. Nepa, G. Manara, and F. Potorti, "Detection and classification of human arm movements for physical rehabilitation," in *2010 IEEE Antennas and Propagation Society International Symposium*, pp. 1–4, 2010.
- [61] A. Chhikara, A. Rice, A. H. McGregor, and F. Bello, "Wearable device for monitoring disability associated with low back pain," *World*, vol. 10, p. 13, 2008.

- [62] P. Iso-Ketola, T. Karinsalo, and J. Vanhala, "Hipguard: A wearable measurement system for patients recovering from a hip operation," in *2008 the Second IEEE International Conference on Pervasive Computing Technologies for Healthcare*, pp. 196–199, 2008.
- [63] T. Watanabe and H. Saito, "Tests of wireless wearable sensor system in joint angle measurement of lower limbs," in *2011 IEEE Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5469–5472, 2011.
- [64] G. Anania, A. Tognetti, N. Carbonaro, M. Tesconi, F. Cutolo, G. Zupone, and D. De Rossi, "Development of a novel algorithm for human fall detection using wearable sensors," in *2008 IEEE SENSORS*, pp. 1336–1339, 2008.
- [65] W.-S. Baek, D.-M. Kim, F. Bashir, and J.-Y. Pyun, "Real life applicable fall detection system based on wireless body area network," in *2013 IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 62–67, 2013.
- [66] F. Felisberto, F. Fdez-Riverola, and A. Pereira, "A ubiquitous and low-cost solution for movement monitoring and accident detection based on sensor fusion," *Sensors*, vol. 14, no. 5, pp. 8961–8983, 2014.
- [67] S. Yazaki and T. Matsunaga, "A proposal of abnormal condition detection system for elderly people using wireless wearable biosensor," in *2008 IEEE SICE Annual Conference*, pp. 2234–2238, 2008.
- [68] S. Patel, K. Lorincz, R. Hughes, N. Huggins, J. H. Growdon, M. Welsh, and P. Bonato, "Analysis of feature space for monitoring persons with parkinson's disease with application to a wireless wearable sensor system," in *2007 the 29th IEEE Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 6290–6293, 2007.
- [69] T. Falck, J. Espina, J. . Ebert, and D. Dietterle, "Basuma - the sixth sense for chronically ill patients," in *International Workshop on Wearable and Implantable Body Sensor Networks (BSN'06)*, pp. 60–63, April 2006.

- [70] K. Wac, R. Bults, B. van Beijnum, I. Widya, V. Jones, D. Konstantas, M. Vollenbroek-Hutten, and H. Hermens, “Mobile patient monitoring: The mobihealth system,” in *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 1238–1241, Sep. 2009.
- [71] T. Gao, T. Massey, L. Selavo, D. Crawford, B.-r. Chen, K. Lorincz, V. Shnayder, L. Hauenstein, F. Dabiri, J. Jeng, *et al.*, “The advanced health and disaster aid network: A light-weight wireless medical system for triage,” *IEEE Transactions on biomedical circuits and systems*, vol. 1, no. 3, pp. 203–216, 2007.
- [72] E. Kang, Y. Im, and U. Kim, “Remote control multi-agent system for u-healthcare service,” in *KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications*, pp. 636–644, Springer, 2007.
- [73] V. Shnayder, B.-r. Chen, K. Lorincz, T. R. F. F. Jones, and M. Welsh, “Sensor networks for medical care,” in *Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems*, SenSys ’05, pp. 314–314, 2005.
- [74] K. Ouchi, T. Suzuki, and M. Doi, “Lifeminder: a wearable healthcare support system using user’s context,” in *Proceedings 22nd International Conference on Distributed Computing Systems Workshops*, pp. 791–792, July 2002.
- [75] T. Sheltami, A. Mahmoud, and M. Abu-Amara, “Warning and monitoring medical system using sensor networks,” in *The Saudi 18th national computer conference (NCC18)*, pp. 63–68, 2006.
- [76] K. Venkatasubramanian, G. Deng, T. Mukherjee, J. Quintero, V. Annamalai, and S. K. Gupta, “Ayushman: A wireless sensor network based health monitoring infrastructure and testbed,” in *Proceedings of the First IEEE international conference on Distributed Computing in Sensor Systems*, pp. 406–407, Springer-Verlag, 2005.
- [77] D. Curtis, E. Shih, J. Waterman, J. Gutttag, J. Bailey, T. Stair, R. A. Greenes, and L. Ohno-Machado, “Physiological signal monitoring in the waiting areas of an

- emergency room,” in *Proceedings of the 3rd ICST international conference on Body area networks*, p. 5, 2008.
- [78] E. L. van den Broek and J. H. D. M. Westerink, “Biofeedback systems for stress reduction - towards a bright future for a revitalized field,” in *2012 Proceedings of international conference on Health Informatics (HEALTHINF)*, 2012.
- [79] A. D. Wood, J. A. Stankovic, G. Virone, L. Selavo, Z. He, Q. Cao, T. Doan, Y. Wu, L. Fang, and R. Stoleru, “Context-aware wireless sensor networks for assisted living and residential monitoring,” *IEEE Network*, vol. 22, pp. 26–33, July 2008.
- [80] H. Ghasemzadeh, V. Loseu, E. Guenterberg, and R. Jafari, “Sport training using body sensor networks: A statistical approach to measure wrist rotation for golf swing,” in *Proceedings of the Fourth ICST International Conference on Body Area Networks*, p. 2, 2009.
- [81] V. Sivaraman, S. Grover, A. Kurusingal, A. Dhamdhare, and A. Burdett, “Experimental study of mobility in the soccer field with application to real-time athlete monitoring,” in *2010 the 6th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 337–345, 2010.
- [82] S. Akram, N. Javaid, A. Tauqir, A. Rao, and S. N. Mohammad, “The-fame: Threshold based energy-efficient fatigue measurement for wireless body area sensor networks using multiple sinks,” in *2013 the 8th IEEE International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, pp. 214–220, 2013.
- [83] M. Garcia, A. Catalá, J. Lloret, and J. J. Rodrigues, “A wireless sensor network for soccer team monitoring,” in *2011 IEEE International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, pp. 1–6, 2011.
- [84] M. Lauzier, P. Ferrand, H. Parvery, A. Fraboulet, and J.-M. Gorce, “Wbans for live sport monitoring: an experimental approach, early results and perspectives,”

- in *EURO-COST IC1004-European Cooperation in the Field Of Scientific and Technical Research*, 2012.
- [85] K. Revett and S. T. de Magalhães, “Cognitive biometrics: Challenges for the future,” in *Springer International Conference on Global Security, Safety, and Sustainability*, pp. 79–86, 2010.
- [86] S. Coyle, D. Morris, K. Lau, D. Diamond, N. Taccini, D. Costanzo, P. Salvo, F. Di Francesco, M. G. Trivella, J. Porchet, and J. Luprano, “Textile sensors to measure sweat pH and sweat-rate during exercise,” in *2009 3rd International Conference on Pervasive Computing Technologies for Healthcare*, pp. 1–6, April 2009.
- [87] D. Morris, B. Schazmann, Y. Wu, S. Coyle, S. Brady, J. Hayes, C. Slater, C. Fay, K. T. Lau, G. Wallace, and D. Diamond, “Wearable sensors for monitoring sports performance and training,” in *2008 5th International Summer School and Symposium on Medical Devices and Biosensors*, pp. 121–124, June 2008.
- [88] L. De Nardis, D. Domenicali, and M. G. Di Benedetto, “Mobility model for body area networks of soccer players,” in *The 3rd European Wireless Technology Conference*, pp. 65–68, Sep. 2010.
- [89] M. Lapinski, E. Berkson, T. Gill, M. Reinold, and J. A. Paradiso, “A distributed wearable, wireless sensor system for evaluating professional baseball pitchers and batters,” in *2009 International Symposium on Wearable Computers*, pp. 131–138, Sep. 2009.
- [90] M. Walsh, J. Barton, B. O’Flynn, C. O’Mathuna, and M. Tyndyk, “Capturing the overarm throw in darts employing wireless inertial measurement,” in *2011 IEEE SENSORS*, pp. 1441–1444, Oct 2011.
- [91] R. Marin-Perianu, M. Marin-Perianu, D. Rouffet, S. Taylor, P. Havinga, R. Begg, and M. Palaniswami, “Body area wireless sensor networks for the analysis of cycling performance,” in *Proceedings of the Fifth ACM International Conference on Body Area Networks*, pp. 1–7, 2010.

-
- [92] G. Magenes, D. Curone, L. Caldani, and E. L. Secco, "Fire fighters and rescuers monitoring through wearable sensors: The proetex project," in *2010 Annual International Conference of the IEEE Engineering in Medicine and Biology*, pp. 3594–3597, Aug 2010.
- [93] H. B. Lim, D. Ma, B. Wang, Z. Kalbarczyk, R. K. Iyer, and K. L. Watkin, "A soldier health monitoring system for military applications," in *2010 IEEE International Conference on Body Sensor Networks (BSN)*, pp. 246–249, 2010.
- [94] D. Chen, J. Hart, and R. Vertegaal, "Towards a physiological model of user interruptability," in *Springer IFIP Conference on Human-Computer Interaction*, pp. 439–451, 2007.
- [95] T. M. Connolly, E. A. Boyle, E. MacArthur, T. Hainey, and J. M. Boyle, "A systematic literature review of empirical evidence on computer games and serious games," *Computers & Education*, vol. 59, no. 2, pp. 661–686, 2012.
- [96] V. Sukkird and K. Shirahada, "Technology challenges to healthcare service innovation in aging asia: Case of value co-creation in emergency medical support system," *Technology in Society*, vol. 43, pp. 122 – 128, 2015.
- [97] M. A. Rahman, M. F. Alhamid, A. E. Saddik, and W. Gueaieb, "A framework to bridge social network and body sensor network: An e-health perspective," in *2009 IEEE International Conference on Multimedia and Expo*, pp. 1724–1727, June 2009.
- [98] O. Omeni, A. C. W. Wong, A. J. Burdett, and C. Toumazou, "Energy efficient medium access protocol for wireless medical body area sensor networks," *IEEE Transactions on biomedical circuits and systems*, vol. 2, no. 4, pp. 251–259, 2008.
- [99] M. Al Ameen, J. Liu, S. Ullah, and K. S. Kwak, "A power efficient mac protocol for implant device communication in wireless body area networks," in *2011 IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 1155–1160, 2011.
- [100] T. O'Donovan, J. O'Donoghue, C. Sreenan, D. Sammon, P. O'Reilly, and K. A. O'Connor, "A context aware wireless body area network (ban)," in *2009 3rd*

- International Conference on Pervasive Computing Technologies for Healthcare*, pp. 1–8, April 2009.
- [101] G. Pradhan, R. Gupta, and S. Biswasz, “Study and simulation of wban mac protocols for emergency data traffic in healthcare,” in *2018 the Fifth IEEE International Conference on Emerging Applications of Information Technology (EAIT)*, pp. 1–4, 2018.
- [102] S. Marinkovic, C. Spagnol, and E. Popovici, “Energy-efficient tdma-based mac protocol for wireless body area networks,” in *2009 the Third IEEE International Conference on Sensor Technologies and Applications*, pp. 604–609, 2009.
- [103] B. Braem, B. Latrej, I. Moerman, C. Blondia, E. Reusens, W. Joseph, L. Martens, and P. Demeester, “The need for cooperation and relaying in short-range high path loss sensor networks,” in *2007 International Conference on Sensor Technologies and Applications (SENSORCOMM 2007)*, pp. 566–571, Oct 2007.
- [104] S. Ullah, B. Shen, S. Riazul Islam, P. Khan, S. Saleem, and K. Sup Kwak, “A study of mac protocols for wbans,” *Sensors*, vol. 10, no. 1, pp. 128–145, 2009.
- [105] X. Zhou, T. Zhang, L. Song, and Q. Zhang, “Energy efficiency optimization by resource allocation in wireless body area networks,” in *2014 the 79th IEEE Vehicular Technology Conference (VTC Spring)*, pp. 1–6, 2014.
- [106] G. Fang and E. Dutkiewicz, “Bodymac: Energy efficient tdma-based mac protocol for wireless body area networks,” in *2009 9th International Symposium on Communications and Information Technology*, pp. 1455–1459, Sep. 2009.
- [107] W. Scanlon, G. Conway, and S. Cotton, “Antennas and propagation considerations for robust wireless communications in medical body area networks,” in *IET Seminar on Antennas and Propagation for Body-Centric Wireless Communications*, vol. 11803, 2007.
- [108] M. Patel and J. Wang, “Applications, challenges, and prospective in emerging body area networking technologies,” *IEEE Wireless Communications*, vol. 17, pp. 80–88, February 2010.

- [109] A. Kiourti and K. S. Nikita, "A review of implantable patch antennas for biomedical telemetry: Challenges and solutions [wireless corner]," *IEEE Antennas and Propagation Magazine*, vol. 54, no. 3, pp. 210–228, 2012.
- [110] G.-Z. Yang and G. Yang, *Body Sensor Networks*. London: Springer-Verlag, 2006.
- [111] G. Selimis, L. Huang, F. Massé, I. Tsekoura, M. Ashouei, F. Catthoor, J. Huisken, J. Stuyt, G. Dolmans, J. Penders, *et al.*, "A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design," *Journal of medical systems*, vol. 35, no. 5, pp. 1289–1298, 2011.
- [112] C. C. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73–81, 2006.
- [113] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "A distributed trust evaluation model and its application scenarios for medical sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1164–1175, 2012.
- [114] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "Retrust: Attack-resistant and lightweight trust management for medical sensor networks," *IEEE transactions on information technology in biomedicine*, vol. 16, no. 4, pp. 623–632, 2012.
- [115] C. A. Chin, G. V. Crosby, T. Ghosh, and R. Murimi, "Advances and challenges of wireless body area networks for healthcare applications," in *2012 IEEE International Conference on Computing, Networking and Communications (ICNC)*, pp. 99–103, 2012.
- [116] N. Wisniewski and M. Reichert, "Methods for reducing biosensor membrane biofouling," *Colloids and Surfaces B: Biointerfaces*, vol. 18, no. 3-4, pp. 197–219, 2000.
- [117] S. Ullah and K. S. Kwak, "Throughput and delay limits of ieee 802.15. 6," in *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 174–178, 2011.

- [118] N. Xiong, A. V. Vasilakos, L. T. Yang, L. Song, Y. Pan, R. Kannan, and Y. Li, “Comparative analysis of quality of service and memory usage for adaptive failure detectors in healthcare systems,” *IEEE Journal on Selected Areas in Communications*, vol. 27, pp. 495–509, May 2009.
- [119] G. Zhou, J. Lu, C. . Wan, M. D. Yarvis, and J. A. Stankovic, “Bodyqos: Adaptive and radio-agnostic qos for body sensor networks,” in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, pp. 565–573, April 2008.
- [120] I. S. Association *et al.*, “Ieee standard for local and metropolitan area networks—part 15.6: Wireless body area networks,” *IEEE Standard for Information Technology*, vol. 802, no. 6, pp. 1–271, 2012.
- [121] D. Domenicali and M. Di Benedetto, “Performance analysis for a body area network composed of ieee 802.15.4a devices,” in *2007 4th Workshop on Positioning, Navigation and Communication*, pp. 273–276, March 2007.
- [122] D. Domenicali, L. De Nardis, and M. Di Benedetto, “Uwb body area network coexistence by interference mitigation,” in *2009 IEEE International Conference on Ultra-Wideband*, pp. 713–717, Sep. 2009.
- [123] J.-H. Hauer, V. Handziski, and A. Wolisz, “Experimental study of the impact of wlan interference on ieee 802.15. 4 body area networks,” in *Springer European Conference on Wireless Sensor Networks*, pp. 17–32, 2009.
- [124] J. Hou, B. Chang, D.-K. Cho, and M. Gerla, “Minimizing 802.11 interference on zigbee medical sensors,” in *Proceedings of the Fourth ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) International Conference on Body Area Networks*, p. 5, 2009.
- [125] F. Martelli and R. Verdone, “Coexistence issues for wireless body area networks at 2.45 ghz,” in *European Wireless 2012; 18th European Wireless Conference 2012*, pp. 1–6, April 2012.

- [126] S. Warren and E. Jovanov, “The need for rules of engagement applied to wireless body area networks,” in *Proceedings of the IEEE consumer communications and networking conference (CCNC)*, 2006.
- [127] R. Chávez-Santiago, C. Garcia-Pardo, A. Fornes-Leal, A. Vallés-Lluch, G. Vermeeren, W. Joseph, I. Balasingham, and N. Cardona, “Experimental path loss models for in-body communications within 2.36-2.5 ghz,” *IEEE J. Biomedical and Health Informatics*, vol. 19, no. 3, pp. 930–937, 2015.
- [128] T. Aoyagi, K. Takizawa, T. Kobayashi, J.-i. Takada, and R. Kohno, “Development of a wban channel model for capsule endoscopy,” in *IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting*, pp. 1–4, 2009.
- [129] Y. Liu and R. D. Gitlin, “A phenomenological path loss model of the in vivo wireless channel,” in *IEEE 16th Wireless and Microwave Technology Conference*, 2015.
- [130] D. Kurup, W. Joseph, G. Vermeeren, and L. Martens, “In-body path loss model for homogeneous human tissues,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 54, no. 3, pp. 556–564, 2012.
- [131] D. Kurup, G. Vermeeren, E. Tanghe, W. Joseph, and L. Martens, “In-to-out body antenna-independent path loss model for multilayered tissues and heterogeneous medium,” *Sensors*, vol. 15, no. 1, pp. 408–421, 2014.
- [132] D. Takahashi, Y. Xiao, and F. Hu, “Ltrt: Least total-route temperature routing for embedded biomedical sensor networks,” in *IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference*, pp. 641–645, 2007.
- [133] A. Bag and M. A. Bassiouni, “Hotspot preventing routing algorithm for delay-sensitive applications of in vivo biomedical sensor networks,” *Information Fusion*, vol. 9, no. 3, pp. 389–398, 2008.
- [134] F. T. Zuhra, K. A. Bakar, A. Ahmed, and M. A. Tunio, “Routing protocols in wireless body sensor networks: A comprehensive survey,” *Journal of Network and Computer Applications*, vol. 99, pp. 73–97, 2017.

-
- [135] K. Awan, K. N. Qureshi, and M. Mehwish, "Wireless body area networks routing protocols: a review," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 4, 2016.
- [136] Q. Tang, N. Tummala, S. K. Gupta, and L. Schwiebert, "Tara: thermal-aware routing algorithm for implanted sensor networks," in *Springer International Conference on Distributed Computing in Sensor Systems*, pp. 206–217, 2005.
- [137] A. Bag and M. A. Bassiouni, "Energy efficient thermal aware routing algorithms for embedded biomedical sensor networks," in *2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 604–609, 2006.
- [138] C. Oey and S. Moh, "A survey on temperature-aware routing protocols in wireless body sensor networks," *Sensors*, vol. 13, no. 8, pp. 9860–9877, 2013.
- [139] R. Istepanian, S. Laxminarayan, and C. S. Pattichis, *M-health*. Boston, MA: Springer, 2006.
- [140] H. Cao, V. Leung, C. Chow, and H. Chan, "Enabling technologies for wireless body area networks: A survey and outlook," *IEEE Communications Magazine*, vol. 47, no. 12, 2009.
- [141] F. Touati and R. Tabish, "U-healthcare system: State-of-the-art review and challenges," *Journal of medical systems*, vol. 37, no. 3, p. 9949, 2013.
- [142] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, "Body area networks: A survey," *Mobile networks and applications*, vol. 16, no. 2, pp. 171–193, 2011.
- [143] H. C. Keong and M. R. Yuce, "Analysis of a multi-access scheme and asynchronous transmit-only uwb for wireless body area networks," in *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 6906–6909, Sep. 2009.
- [144] K. S. Kwak, S. Ullah, and N. Ullah, "An overview of ieee 802.15. 6 standard," in *2010 the 3rd IEEE International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL)*, pp. 1–6, 2010.

- [145] D. B. Smith, D. Miniutti, T. A. Lamahewa, and L. W. Hanlen, "Propagation models for body-area networks: A survey and new outlook," *IEEE Antennas and Propagation Magazine*, vol. 55, no. 5, pp. 97–117, 2013.
- [146] Federal Communications Commission , "Cell Phones and Specific Absorption Rate, [Available Online]:~<https://www.fcc.gov/general/cell-phones-and-specific-absorption-rate>, [Accessed on: 2018-11-09]."
- [147] J. H. Cox, J. Chung, S. Donovan, J. Ivey, R. J. Clark, G. Riley, and H. L. Owen, "Advancing software-defined networks: A survey," *IEEE Access*, vol. 5, pp. 25487–25526, 2017.
- [148] A. Doria, J. H. Salim, R. Haas, H. Khosravi, W. Wang, L. Dong, R. Gopal, and J. Halpern, "Forwarding and Control Element Separation (ForCES) Protocol Specification, RFC 5810," tech. rep., 2010.
- [149] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.
- [150] M. Casado, N. Foster, and A. Guha, "Abstractions for software-defined networks," *Communications of the ACM*, vol. 57, no. 10, pp. 86–95, 2014.
- [151] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1617–1634, 2014.
- [152] M. Uddin, *Toward open and programmable wireless network edge*. PhD thesis, Old Dominion University, 2016.
- [153] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements.," *IEEE Access*, vol. 5, no. 1, pp. 1872–1899, 2017.

- [154] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-defined networking: A comprehensive survey,” *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.
- [155] O. N. Foundation, “Software-defined networking: The new norm for networks,” *ONF White Paper*, vol. 2, pp. 2–6, 2012.
- [156] W. Braun and M. Menth, “Software-defined networking using openflow: Protocols, applications and architectural design choices,” *Future Internet*, vol. 6, no. 2, pp. 302–336, 2014.
- [157] L. E. Li, Z. M. Mao, and J. Rexford, “Toward software-defined cellular networks,” in *2012 European Workshop on Software Defined Networking*, pp. 7–12, Oct 2012.
- [158] K.-K. Yap, M. Kobayashi, R. Sherwood, T.-Y. Huang, M. Chan, N. Handigol, and N. McKeown, “Openroads: Empowering research in mobile networks,” *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 1, pp. 125–126, 2010.
- [159] K.-K. Yap, R. Sherwood, M. Kobayashi, T.-Y. Huang, M. Chan, N. Handigol, N. McKeown, and G. Parulkar, “Blueprint for introducing innovation into wireless mobile networks,” in *Proceedings of the Second ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architectures, VISA '10*, (New York, NY, USA), pp. 25–32, 2010.
- [160] M. Bansal, J. Mehlman, S. Katti, and P. Levis, “Openradio: a programmable wireless dataplane,” in *Proceedings of the first ACM workshop on Hot topics in software defined networks*, pp. 109–114, 2012.
- [161] S. Bera, S. Misra, and A. V. Vasilakos, “Software-defined networking for internet of things: A survey,” *IEEE Internet of Things Journal*, vol. 4, pp. 1994–2008, Dec 2017.
- [162] L. M. Vaquero and L. Roderio-Merino, “Finding your way in the fog: Towards a comprehensive definition of fog computing,” *SIGCOMM Comput. Commun. Rev.*, vol. 44, pp. 27–32, Oct. 2014.

- [163] J. Pang, G. Xu, and X. Fu, “Sdn-based data center networking with collaboration of multipath tcp and segment routing,” *IEEE Access*, vol. 5, pp. 9764–9773, 2017.
- [164] A. A. Pranata, T. S. Jun, and D. S. Kim, “Overhead reduction scheme for sdn-based data center networks,” *Computer Standards Interfaces*, vol. 63, pp. 1 – 15, 2019.
- [165] C.-Y. Hong, S. Kandula, R. Mahajan, M. Zhang, V. Gill, M. Nanduri, and R. Wattenhofer, “Achieving high utilization with software-driven wan,” *SIGCOMM Comput. Commun. Rev.*, vol. 43, pp. 15–26, Aug. 2013.
- [166] N. Medhi and D. K. Saikia, “Openflow-based scalable routing with hybrid addressing in data center networks,” *IEEE Communications Letters*, vol. 21, pp. 1047–1050, May 2017.
- [167] N. T. Hai and D. Kim, “Efficient load balancing for multi-controller in sdn-based mission-critical networks,” in *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*, pp. 420–425, July 2016.
- [168] H. Zhang, X. Guo, J. Yan, B. Liu, and Q. Shuai, “Sdn-based ecmp algorithm for data center networks,” in *2014 IEEE Computers, Communications and IT Applications Conference*, pp. 13–18, Oct 2014.
- [169] V. Varadharajan, U. Tupakula, and K. Karmakar, “Secure monitoring of patients with wandering behavior in hospital environments,” *IEEE Access*, vol. 6, pp. 11523–11533, 2018.
- [170] Y. Choi, Y. Choi, and Y.-G. Hong, “Study on coupling of software-defined networking and wireless sensor networks,” in *International Conference on Ubiquitous and Future Networks*, pp. 900–902, 2016.
- [171] K. Hasan, X.-W. Wu, K. Biswas, and K. Ahmed, “A novel framework for software defined wireless body area network,” in *2018 the 8th IEEE International Conference on Intelligent Systems, Modelling and Simulations (ISMS)*, pp. 114–119, 2018.
- [172] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” tech. rep., 2008.

- [173] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199 – 221, 2018.
- [174] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 the 18th IEEE International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–3, 2016.
- [175] G. Prisco, "The Blockchain for healthcare: Gem launches Gem Health Network with Philips Blockchain Lab, [Available Online]:~<https://bitcoinmagazine.com/articles/the-blockchain-for-healthcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938/>, [Accessed on: 2018-11-09]."
- [176] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *2017 the 19th IEEE International Conference on Advanced Communication Technology (ICACT)*, pp. 464–467, 2017.
- [177] O. Williams-Grut, "Estonia is using the technology behind bitcoin to secure 1 million health records, [Available Online]:~<https://www.businessinsider.com.au/guardtime-estonian-health-records-industrial-blockchain-bitcoin-2016-3?r=usir=t>, [Accessed on: 2018-11-09]."
- [178] P. Nichol, "Blockchain applications for healthcare," *Najdeno*, vol. 4, no. 9, p. 2017, 2016.
- [179] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "Blochie: a blockchain-based platform for healthcare information exchange," in *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, pp. 49–56, 2018.
- [180] K. Hasan, K. Biswas, K. Ahmed, and M. S. Islam, "Challenges of integrating blockchain in wireless body area network," *The 3rd Symposium on Distributed Ledger Technology, 2018 Griffith University, Australia*, 2018.
- [181] E. Sarra and T. Ezzedine, "Performance improvement of the wireless body area network (wban)," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–6, Sep. 2016.

- [182] M. Kathuria and S. Gambhir, “Reliable delay sensitive loss recovery protocol for critical health data transmission system,” in *2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE)*, pp. 333–339, Feb 2015.
- [183] X. Yuan, C. Li, Q. Ye, K. Zhang, N. Cheng, N. Zhang, and X. Shen, “Performance analysis of ieee 802.15. 6-based coexisting mobile wbans with prioritized traffic and dynamic interference,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 5637–5652, 2018.
- [184] G. Sun, K. Wang, H. Yu, X. Du, and M. Guizani, “Priority-based medium access control for wireless body area networks with high-performance design,” *IEEE Internet of Things Journal*, 2019.
- [185] F. Ullah, A. H. Abdullah, M. M. Arshad, and A. Aliyu, “Emergency data handling medium access control protocol for wireless body area network,” in *2017 6th ICT International Student Project Conference (ICT-ISPC)*, pp. 1–4, May 2017.
- [186] B. KIM, J. CHO, and D.-Y. KIM, “An emergency handling scheme for superframe-structured mac protocols in wbans,” *IEICE Transactions on Communications*, vol. E94.B, no. 9, pp. 2484–2487, 2011.
- [187] C. Lee, H. Lee, and S. Choi, “An enhanced mac protocol of ieee 802.15.4 for wireless body area networks,” in *the 5th International Conference on Computer Sciences and Convergence Information Technology*, pp. 916–919, 2010.
- [188] S. Nepal, A. Pudasaini, Jae-young Pyun, Suk-seung Hwang, C. G. Lee, and Seokjoo Shin, “A new mac protocol for emergency handling in wireless body area networks,” in *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 588–590, July 2016.
- [189] V. Shnayder, B.-r. Chen, K. Lorincz, T. R. F. F. Jones, and M. Welsh, “Sensor networks for medical care,” in *Proceedings of the 3rd ACM International Conference on Embedded Networked Sensor Systems*, SenSys ’05, (New York, NY, USA), pp. 314–314, 2005.

-
- [190] S. Misra and A. Samanta, "Traffic-aware efficient mapping of wireless body area networks to health cloud service providers in critical emergency situations," *IEEE Transactions on Mobile Computing*, vol. 17, pp. 2968–2981, Dec 2018.
- [191] M. Ambigavathi and D. Sridharan, "Energy efficient and load balanced priority queue algorithm for wireless body area network," *Future Generation Computer Systems*, vol. 88, pp. 586–593, 2018.
- [192] L. Hu, M. Qiu, J. Song, M. S. Hossain, and A. Ghoneim, "Software defined healthcare networks," *IEEE Wireless Communications*, vol. 22, pp. 67–75, December 2015.
- [193] A. Rego, L. Garcia, S. Sendra, and J. Lloret, "Software defined network-based control system for an efficient traffic management for emergency situations in smart cities," *Future Generation Computer Systems*, vol. 88, pp. 243–253, 2018.
- [194] K. Ahmed and M. A. Gregory, "Optimized tdma based distance routing for data centric storage," in *2012 the 3rd IEEE International Conference on Networked Embedded Systems for Every Application (NESEA)*, pp. 1–7, 2012.
- [195] K. Hasan, X. Wu, K. Biswas, and K. Ahmed, "A novel framework for software defined wireless body area network," in *2018 the 8th IEEE International Conference on Intelligent Systems, Modelling and Simulation (ISMS)*, pp. 114–119, May 2018.
- [196] A. Boulis, "Castalia, a simulator for wireless sensor networks and body area networks, version 2.2," *User's Manual*, 2009.
- [197] NEC, "Software-Defined Networking (SDN) Solution Nagoya City University Hospital, [Available Online]:~<http://au.nec.com/en/au/media/docs/case-studies/nec-sdn-case-study-nagoyai-city-university-hospital.pdf>, [Accessed on: 2019-01-09]."
- [198] S. Adler, S. Pfeiffer, H. Will, T. Hillebrandt, and J. Schiller, "Measuring the distance between wireless sensor nodes with standard hardware," in *2012 9th Workshop on Positioning, Navigation and Communication*, pp. 114–119, March 2012.

-
- [199] A. Bahillo, S. Mazuelas, R. M. Lorenzo, P. Fernandez, J. Prieto, R. J. Duran, and E. J. Abril, “Hybrid rss-rtt localization scheme for indoor wireless networks,” *EURASIP Journal on Advances in Signal Processing*, vol. 2010, no. 1, p. 126082, 2010.
- [200] H. Hashemi, “The indoor radio propagation channel,” *Proceedings of the IEEE*, vol. 81, pp. 943–968, July 1993.
- [201] S. Adler, S. Pfeiffer, H. Will, T. Hillebrandt, and J. Schiller, “Measuring the distance between wireless sensor nodes with standard hardware,” in *2012 9th Workshop on Positioning, Navigation and Communication*, pp. 114–119, March 2012.
- [202] J. B. Andersen, T. S. Rappaport, and S. Yoshida, “Propagation measurements and models for wireless communications channels,” *IEEE Communications Magazine*, vol. 33, pp. 42–49, Jan 1995.
- [203] A. Boulis *et al.*, “Castalia: A simulator for wireless sensor networks and body area networks,” *NICTA: National ICT Australia*, vol. 83, 2011.
- [204] J. Y. Khan, M. R. Yuce, G. Bulger, and B. Harding, “Wireless body area network (wban) design techniques and performance evaluation,” *Journal of Medical Systems*, vol. 36, pp. 1441–1457, Jun 2012.
- [205] M. F. Bari, A. R. Roy, S. R. Chowdhury, Q. Zhang, M. F. Zhani, R. Ahmed, and R. Boutaba, “Dynamic controller provisioning in software defined networks,” in *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, pp. 18–25, Oct 2013.
- [206] D. Levin, A. Wundsam, B. Heller, N. Handigol, and A. Feldmann, “Logically centralized?: State distribution trade-offs in software defined networks,” in *Proceedings of the First ACM Workshop on Hot Topics in Software Defined Networks*, HotSDN ’12, (New York, NY, USA), pp. 1–6, 2012.

- [207] B. Heller, R. Sherwood, and N. McKeown, “The controller placement problem,” in *Proceedings of the First ACM Workshop on Hot Topics in Software Defined Networks*, HotSDN ’12, (New York, NY, USA), pp. 7–12, 2012.
- [208] A. Sallahi and M. St-Hilaire, “Optimal model for the controller placement problem in software defined networks,” *IEEE Communications Letters*, vol. 19, pp. 30–33, Jan 2015.
- [209] D. Hock, M. Hartmann, S. Gebert, M. Jarschel, T. Zinner, and P. Tran-Gia, “Pareto-optimal resilient controller placement in sdn-based core networks,” in *Proceedings of the 2013 25th International Teletraffic Congress (ITC)*, pp. 1–9, Sep. 2013.
- [210] G. Yao, J. Bi, Y. Li, and L. Guo, “On the capacitated controller placement problem in software defined networks,” *IEEE Communications Letters*, vol. 18, pp. 1339–1342, Aug 2014.
- [211] Y. Jiménez, C. Cervelló-Pastor, and A. J. García, “On the controller placement for designing a distributed sdn control layer,” in *2014 IFIP Networking Conference*, pp. 1–9, June 2014.
- [212] H. R. Faragardi, M. Vahabi, H. Fotouhi, T. Nolte, and T. Fahringer, “An efficient placement of sinks and sdn controller nodes for optimizing the design cost of industrial iot systems,” *Software: Practice and Experience*.
- [213] W. Ren, Y. Sun, H. Luo, and M. Guizani, “A novel control plane optimization strategy for important nodes in sdn-iot networks,” *IEEE Internet of Things Journal*, vol. 6, pp. 3558–3571, April 2019.
- [214] K. S. K. Liyanage, M. Ma, and P. H. J. Chong, “Controller placement optimization in hierarchical distributed software defined vehicular networks,” *Computer Networks*, vol. 135, pp. 226 – 239, 2018.
- [215] F. D. Roadmap, “Cisco Application Policy Infrastructure Controller, Release 1.0 (1e), Release Notes, [Available

- Online]:~https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/release/notes/apic_rn_101.html, [Accessed on: 2020-05-06].”
- [216] A. Tootoonchian, S. Gorbunov, Y. Ganjali, M. Casado, and R. Sherwood, “On controller performance in software-defined networks,” in *Proceedings of the 2Nd USENIX Conference on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services*, Hot-ICE’12, (Berkeley, CA, USA), pp. 10–10, 2012.
- [217] L. Zhu, M. M. Karim, K. Sharif, F. Li, X. Du, and M. Guizani, “Sdn controllers: Benchmarking performance evaluation,” 2019.
- [218] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, “Healthcare blockchain system using smart contracts for secure automated remote patient monitoring,” *Journal of medical systems*, vol. 42, no. 7, p. 130, 2018.
- [219] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, “Continuous patient monitoring with a patient centric agent: A block architecture,” *IEEE Access*, vol. 6, pp. 32700–32726, 2018.
- [220] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “Medrec: Using blockchain for medical data access and permission management,” in *2016 2nd International Conference on Open and Big Data (OBD)*, pp. 25–30, Aug 2016.
- [221] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, “Medshare: Trust-less medical data sharing among cloud service providers via blockchain,” *IEEE Access*, vol. 5, pp. 14757–14767, 2017.
- [222] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control,” *Journal of Medical Systems*, vol. 40, p. 218, Aug 2016.
- [223] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, “Omniphr: A distributed architecture model to integrate personal health records,” *Journal of biomedical informatics*, vol. 71, pp. 70–81, 2017.

- [224] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, "Continuous authorization in subject-driven data sharing using wearable devices," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 327–333, 2019.
- [225] Y. Gao, H. Li, and Y. Luo, "An empirical study of wearable technology acceptance in healthcare," *Industrial Management & Data Systems*, vol. 115, no. 9, pp. 1704–1723, 2015.
- [226] A. Government, "My health record, [Available Online]:~<https://www.myhealthrecord.gov.au/>, [accessed on: 2018-01-08]."
- [227] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *2016 the 18th IEEE International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp. 1392–1393, Dec 2016.
- [228] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *IEEE International Conference on Open and Big Data (OBD)*, pp. 25–30, 2016.
- [229] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability," *Computational and structural biotechnology journal*, vol. 16, pp. 224–230, 2018.
- [230] B. A. Tama, B. J. Kweka, Y. Park, and K.-H. Rhee, "A critical review of blockchain and its current applications," in *2017 IEEE International Conference on Electrical Engineering and Computer Science (ICECOS)*, pp. 109–113, 2017.
- [231] K. Wu, Y. Ma, G. Huang, and X. Liu, "A first look at blockchain-based decentralized applications," *Software: Practice and Experience*, 2019.

- [232] G. Zyskind, O. Nathan, *et al.*, “Decentralizing privacy: Using blockchain to protect personal data,” in *2015 IEEE Security and Privacy Workshops*, pp. 180–184, 2015.
- [233] Y. Chen, H. Li, K. Li, and J. Zhang, “An improved p2p file system scheme based on ipfs and blockchain,” in *2017 IEEE International Conference on Big Data (Big Data)*, pp. 2652–2657, 2017.
- [234] N. Ferguson, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, and J. Walker, “The skein hash function family,” *Submission to NIST (round 3)*, vol. 7, no. 7.5, p. 3, 2010.
- [235] R. S. Sandhu, “The typed access matrix model,” in *Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy*, p. 122, 1992.
- [236] J. Daly, A. X. Liu, and E. Torng, “A difference resolution approach to compressing access control lists,” *IEEE/ACM Transactions on Networking*, vol. 24, no. 1, pp. 610–623, 2015.
- [237] J. Qian, S. Hinrichs, and K. Nahrstedt, “Acla: A framework for access control list (acl) analysis and optimization,” in *Springer Communications and Multimedia Security Issues of the New Century*, pp. 197–211, 2001.
- [238] C. Dannen, “Solidity programming,” in *Introducing Ethereum and Solidity*, pp. 69–88, Springer, 2017.
- [239] “RemixIDE, howpublished = <https://remix.ethereum.org/>, note = Accessed: 2019-11-10.”
- [240] D. Hardt *et al.*, “The oauth 2.0 authorization framework,” tech. rep., RFC 6749, October, 2012.
- [241] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, *et al.*, “The avispa tool for the automated validation of internet security protocols and applications,” in *Springer International conference on computer aided verification*, pp. 281–285, 2005.

-
- [242] A. Armando, R. Carbone, L. Compagna, J. Cuellar, and L. Tobarra, “Formal analysis of saml 2.0 web browser single sign-on: breaking the saml-based single sign-on for google apps,” in *Proceedings of the 6th ACM workshop on Formal methods in security engineering*, pp. 1–10, 2008.
- [243] M. S. Ferdous and R. Poet, “Formalising identity management protocols,” in *2016 The 14th IEEE Annual Conference on Privacy, Security and Trust (PST)*, pp. 137–146, 2016.
- [244] D. Von Oheimb, “The high-level protocol specification language hlpsl developed in the eu project avispa,” in *Proceedings of APPSEM 2005 workshop*, pp. 1–17, 2005.