STUDY AND DESIGN OF QUALITY OF SERVICE PARAMETERS FOR WIRELESS BODY AREA NETWORK

THESIS

submitted in fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

to

YMCA UNIVERSITY OF SCIENCE & TECHNOLOGY

by

MADHUMITA KATHURIA

Registration No: YMCAUST/Ph14/2010

Under the

Supervision of

Dr. SAPNA GAMBHIR

ASSISTANT PROFESSOR

Department of Computer Engineering

Faculty of Engineering and Technology

YMCA University of Science &Technology

Sector-6, Mathura Road, Faridabad, Haryana, INDIA

DECEMBER, 2017

DECLARATION

I hereby declare that this thesis entitled "**STUDY AND DESIGN OF QUALITY OF SERVICE PARAMETERS FOR WIRELESS BODY AREA NETWORK"** by **MADHUMITA KATHURIA**, being submitted in fulfillment of the requirements for the Degree of Doctor of Philosophy in the Department of Computer Engineering under Faculty of Engineering and Technology of YMCA University of Science and Technology, Faridabad, during the academic year May 2011 to December 2017, is a bonafide record of my original work carried out under the guidance and supervision of **DR. SAPNA GAMBHIR, ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTER ENGINEERING, YMCA UNIVERSITY OF SCIENCE AND TECHNOLOGY** and has not been presented elsewhere.

I further declare that the thesis does not contain any part of any work which has been submitted for the award of any degree either in this University or in any other University.

(MADHUMITA KATHURIA)

Registration No: YMCAUST/Ph14/2010

CERTIFICATE

This is to certify that this thesis entitled **"STUDY AND DESIGN OF QUALITY OF SERVICE PARAMETERS FOR WIRELESS BODY AREA NETWORK"** by **MADHUMITA KATHURIA,** submitted in fulfillment of the requirement for the Degree of Doctor of Philosophy in Department of Computer Engineering, under Faculty of Engineering and Technology of YMCA University of Science and Technology Faridabad, during the academic year May 2011 to December 2017, is a bonafide record of work carried out under our guidance and supervision.

I further declare that to the best of our knowledge, the thesis does not contain any part of any work which has been submitted for the award of any degree either in this University or in any other University.

DR. SAPNA GAMBHIR
Assistant Professor

Department of Computer Engineering,

Faculty of Engineering and Technology,

YMCA University of Science and Technology,
Faridabad

Dated:

ACKNOWLEDGEMENT

I thank my supervisor **Dr. Sapna Gambhir**, not only for her valuable guidance throughout my Ph.D tenure, but also for the care showed me during the hard times. In each and every meeting we had, with her immense research experience, she brought me encouragement and taught me how to the find solution for the various research issues in different ways, which induced me to instigate new ideas into my research. Her talks were not only focused towards research, but also on real life scenarios. This has helped me to complete my Ph.D in spite of the several hindrances, motivated me to handle difficult situations in real life and made me a better person. Without her help in terms of technicalities, resources and opportunity, I would not have reached this stage.

I wish to express my gratitude to **Dr. Komal Bhatia**, **Dr C. K. Nagpal**, **Dr. Atul Mishra**, and **Dr. Naresh Chauhan** for always motivating me and showing me the right way to pursue my Ph.D. I thank them for all their help and suggestions they showered me with a humble soul. I am indebted them for their constant encouragement and being readily available if I am in a need.

I owe much to my *Friend* and my *Husband*, **Mr. Amit Kathuria**, for his timely help during my ill health and his encouragement provided for finishing my PhD. I am wholeheartedly thankful to all my family members for their support they provided in the last few years of my tenure when I was going through a rough phase, both in my professional as well as in my personal life.

I wish to thank my *Daughter* **Havisha** for her unconditional love, affection and the tolerance she has showed all these years.

I owe God for everything!

(MADHUMITA KATHURIA)

ABSTRACT

The exponential growth in wireless communication and sensor technology gave birth to low power, low cost, multifunctional and small Wireless Sensor Network known as Wireless Body Area Networks (WBAN). WBANs have brought revolution in the area of networking and act as a promising technology in many application areas, particularly in healthcare; to enhance the quality of the fashionable healthcare services.

A recent study has exposed that due to heterogeneous and frequently changing environments, WBANs often provide poor Quality-of-Service (QoS). This research proposes novel QoS enhancement techniques, through which WBAN improve QoS by reducing factors those affect system's efforts. In this research work, a QoS model for heterogeneous traffic with constrained resources has been proposed. The model provides better QoS without over-provisioning of resources. A dynamic priority model has been adopted to handle assorted traffic in a dynamic environment in an efficient way.

Similar to other networks, WBAN follows a layered architecture which consists of five layers such as physical layer, MAC layer, network layer, transport layer, and application layer. Every layer does its own specific tasks and faces different issues. The main focus of this research is to handle QoS issues at the transport layer of WBAN, as it provides end-to-end reliable communication. QoS at transport layer includes various issues like packet loss, flooding due to uncontrolled flow rate, congestion, delay, starvation, heterogeneous traffic scheduling etc. QoS in WBAN heavily depends on on-time and accurate monitoring factors.

These limitations provide the motivation for the design of a new framework to deal with dynamic WBAN. In order to work proficiently in a dynamic environment, this framework is integrated with three protocols to fulfill the identified research concerns.

While improving QoS is the primary objective, this research majorly addresses the packet handling which has a great influence on achieving high QoS, especially in worst-case scenarios. For QoS provisioning, the heterogeneous packets are classified

and assigned to a dynamic prioritization strategy which helps during queuing and scheduling. The packet handling model proposes a mechanism to schedule with a percentage of service rates within a deadline to meet the requirement of low starvation and delay for emergency or critical traffic in the WBAN. An adaptive Bandwidth Sharing strategy is proposed so that required amount of bandwidth is distributed and assigned among all sensor nodes. This further maximizes the packet delivery rate and throughput. A scalable alert notification and request-response methods are integrated to make an effort to save a deteriorating health status because a false alert can cause a severe problem in patient monitoring.

It enhances QoS by focusing on the issues like packet loss, congestion, unnecessary retransmissions, duplicate packet, transmission delay, jitter, queuing delay, and flow flooding etc. in the network. It provides an efficient way to avoid unnecessary packet drop by dropping low priority packets and save the important packet. It controls and manages packet loss with selective retransmission of lost packet which avoids unnecessary retransmissions, reduces delay, and utilizes bandwidth. This technique allows important or high priority packets to use more resources as compared to others, and minimizes the queuing delay and starvation problem in the system. Transfer of important packets helps to reduce the loss of significant or critical data.

Because of the specific QoS requirements, WBAN requires an adaptive way which can adopt the changing behavior of the system quickly. Natured-inspired optimization algorithms provide dynamic, adaptive, real-time methods to this response. Therefore a nature-inspired optimization is used here to attain better QoS. This induces QoS performance metrics which are optimized using different fitness functions, contributing to the effective resource utilization.

The network simulator NS-2 takes the responsibility to perform the performance evaluation and demonstrates the virtues of the proposed mechanisms. The analyses of generated outcomes reveal that the proposed mechanisms are superior to existing methods.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ALGORITMS

ABBREVIATIONS

ACK	Acknowledgment
AIMD	Additive Increased and Multiplicative Decreased
AQM	Active Queue Management
ADMR	Adaptive Demand-Driven Multicast Routing
BW	Bandwidth
CCF	Congestion Control and Fairness
CAR	Circadian Activity Rhythm
CU	Controller Unit
CN	Congestion Notification
CD	Congestion Degree
CBR	Constant Bit Rate
DWBAN	Dynamic Wireless Body Area Network
DSR	Data Sending Rate
DPPH	Dynamic Priority based Packet Handling
DEPQ	Double-Ended Priority Queue
DUPACK	Duplicate Acknowledgment
DR	Drop Rate
EDR	Earliest Deadline Ratio
ECH	Extended Cuckoo Hashing
ERMDT	Energy Efficient Reliable Multi-path Data Transmission in Wireless Sensor Network for Healthcare Application
ESRT	Event-to-Sink Reliable Transport in Wireless Sensor Network
FIFD	Fractional Increase and Fractional Decrease
FF	Fitness Function
HP_DEPQ	High priority Double-Ended Priority Queue
HOCA	Healthcare Aware Optimized Congestion Avoidance and Control
ICA	Intelligent Congestion Alleviation
IoT	Internet of Things
LGH	Lion Group Hunting
LP_DEPQ	Low priority Double-Ended Priority Queue
LCCP	Learning based Congestion Control Protocol
LACAS	Learning Automata-Based Congestion Avoidance algorithm in Sensor Networks
MDPPH	Modified Dynamic Priority based Packet Handling
MSU	Medical Server Unit

MFCDN	Multi-factor based Congestion Detection and Notification
NACK	Negative Acknowledgment
NAM	Network AniMator
OMDPPH	Optimized Modified Dynamic Priority based Packet Handling
OBL	Opposition-Based Learning
OTcl	Object-oriented extension of Tcl
OCM	Optimized Congestion Management Protocol for Healthcare Wireless Sensor Networks
PSFQ	Pump Slowly Fetch Quickly
PCCP	Priority-based Congestion Control Protocol
PQ	Priority Queuing
PM	Physiological Monitors
PAN	Personal Area Network
PDA	Personal Digital Assistants
PDR	Packet Delivery Ratio
PLR	Packet Loss Ratio
QoS	Quality of Service
REDF	Ratio based Earliest Deadline First
RED	Random Early Drop
RTO	Retransmission Timeout
RP	Relay Points
RCRT	Rate Control Reliable Transport
SNACK	Selective Negative Acknowledgment
STCP	Sensor Transmission Control Protocol
TDMA	Time Division Multiple Access
Tcl	Tool Command Language
UWB	Ultra Wide Band
WSN	Wireless Sensor Network
WBAN	Wireless Body Area Network
WLAN	Wireless Local Area Network.
WPAN	Wireless Personal Area Network
WBANU	Wireless Body Area Network Unit
WFQ	Weighted Fair Queuing

CHAPTER 1

INTRODUCTION

1.1 Introduction

From last few decades, different wireless networks are governing all over the world, because of its advantages over the wired network i.e. low-cost, flexible communication, scalable, robust etc. Some improvised applications are having a huge demand for small, inexpensive, self-operating and uninterrupted monitoring devices which work intelligently and these requirements are fulfilled with the help of a new kind of network called Wireless Sensor Network (WSN). A WSN consists of tiny intelligent devices called sensors holding good capturing and processing capabilities. It is actually used in the physical environment for continuously and periodic monitoring. Due to its self-governing nature, it becomes the most useful technology in various applications of WSN, but it is unsuited to serve some of the more critical and crucial applications such as healthcare, physical rehabilitation, emergency services, ambient intelligence etc. because of its large communications range. The restrictions in WSN give birth to an extensive technology named Wireless Body Area Network (WBAN) for the next generation applications. The WBAN provides a hybridization of WSN [1-3] and Personal Area Network (PAN) [4, 28] where sensor devices are connected with a person by facilitating wireless communication with the help of various communication standards i.e. Bluetooth, WiFi, and ZigBee technologies among the sensor devices [13,15]. With the approach of limited-resources and low-cost wireless connectivity technologies, WBAN [5, 14] can be deployed with faultless communication.

WBAN [6, 8, 18] is small wireless network consisting of tiny sensors implanted inside or outside the human body, where these sensors sense and transmit the vital signal information data to a central device which is a computationally more intelligent powerful

device than these sensors. Important issues in WBAN include reliable data delivery, low transmission delay, low energy consumption, and also enabling patient mobility.

1.2 Wireless Body Area Network (WBAN)

The WBAN manifested as an intellectual and self-governing network for monitoring the vital signals or activities of a person to offer promising and significant services.

According to [7, 16, 31], the overall design of a WBAN contains four major agents. i) Wireless Body Area Network (WBAN); which equipped with sensors to measure the vital signals of a person and to send these measurements to a personal or local server. ii) The local server; which acts as a third party between the WBAN and the remote server. iii) Remote server; which securely stores, processes and manages the huge amount of data coming from local servers. iv)User; which observes and analyzes these data patterns, and takes the decision accordingly. User can be any medical representative i.e. doctor, nurse or any other. The architecture of a general WBAN system is given in Figure 1.1.

Basically, WBAN [12, 17] is envisioned to work innovatively in personalizing healthcare, medical, rehabilitation, drug delivery, swallowed camera pills, sleep analysis, high-risk pregnancy monitoring, gait analysis, motion detection services. Apart from the medical utility, it is relishing its marvelous contribution in other fields also such as sports, military, emergency services (like Firefighter, Disaster, Bomb disposal), entertainment applications (like gaming, videos, and music), Lifestyle, Consumer electronics etc.

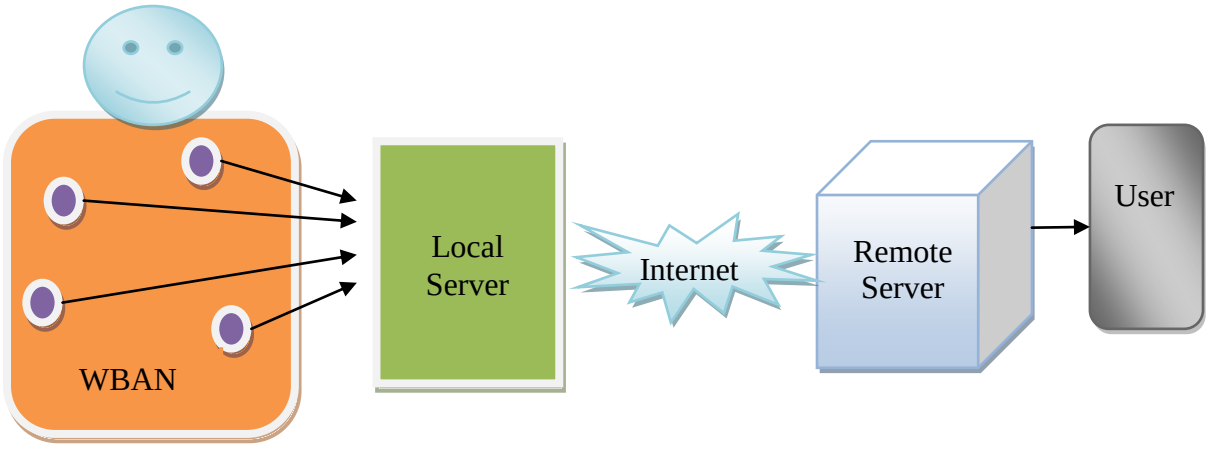

Figure 1.1 Structural Design of a Wireless Body Area Network

WBAN communications [11] require consistent communication with minimal delay within a short transmission range, less energy consumption. These specific needs of WBAN communication are not fulfilled by the conventional communication standards [23]. So a new communication standard, named IEEE Standard 802.15.6 [29] was designed by the IEEE task group to overcome this problem. Currently, different wireless technologies, such as IEEE 802.11 (Wi-Fi), IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (ZigBee), IEEE 802.15.6 (Body Area Network) and the 3G/GPRS, are used to achieve the various levels of communication and considered as perfect candidates for WBAN communications.

Particularly for patients in critical condition, needs highest reliability, shortest transmission delay and immediate response. The delivery of unreliable and delayed data to professionals could causes life threatening consequences. These special features distinguish WBAN from WSN and provoke many new issues [12]

1.2.1 Various Issues in WBAN (Layer Wise)

Like other networks, WBAN has five layers: Physical layer, MAC layer, Network layer, Transport layer, and Application layer. According to the survey [9, 23] most of the work has been done in physical and MAC layer and research on various communication techniques and technologies are still going.

The physical layer [9, 23, 37] of WBAN deals with the data transmission, modulation, and interference techniques and having issues like dynamic topology, frequent changes in data signaling, heterogeneous data rates, low power devices, interference, band selection, interoperability, scalability, fault tolerance, security, and Quality of Service (QoS).

The key role of the MAC layer [12, 30, 37] is to handle collision, and provide flow control, and reliability to the system. Various issues present in MAC layer include collision, control packets overhead; delay due to scheduling, dynamic channel assignment, idle listening, flooding due to over-emitting, energy consumption due to overhearing, random error, flow control, random noise, asynchronous duty cycles, multi-

radio and multi-channel design, energy consumption, security, and Quality of Service (QoS).

The responsibility of the network layer [9, 37] is to find an optimal route and to control traffic and congestion on the selected route. During transmission of data, the network layer faces various issues such as; optimum routing, real-time streaming, localization, network and node mobility in dynamic environment, traffic control, multi-path and multi-point routing, security, faults in network topologies, and Quality of Service (QoS).

The transport layer [37] helps in maintaining end-to-end reliability and controlling flow and congestion in the WBAN. Various issues related to transport layer are; bandwidth sharing, throughput, flow control, streaming data, drop packets due to queue overhead, packet re-ordering, delay, Jitter, traffic classification, queuing, scheduling, buffer management, error control, security, and Quality of Service (QoS).

The application layer [37] performs tasks like Reliability, Data novelty, Data security and integrity, Sensor management, Task, time and query management, Fault detection, fault-free data flow, consistent service, fair resource allocation with the help of application software. Various types of issues in the application layer includes System Lifetime, Request and response time control, Data integrity, Data freshness, Data discovery, Application Software faults, Service management, traffic management, encoding and compression, security, and Quality of Service (QoS).

Besides various open issues in WBAN like scalability, energy efficiency, load balancing, routing, fault tolerance, security, privacy, QoS issue gaining more attention.

1.3 QUALITY OF SERVICE (QoS) IN WBAN

As QoS is one of the key requirements of any application in WBAN, so it becomes a center of attention for all, and lots of research is going on around the world to improve QoS factors [20, 34] in Wireless Sensor Networks at different layers. Some WBAN applications are very sensitive to time and accuracy of data. The QoS issues in these kinds of applications require more attention.

QoS is all about to meet the service requirements of system in order lift system's performance. The traditional QoS [32, 36] metrics like delay, jitter, bandwidth, packet loss are not enough to fulfill performance requirements of a WBAN. Some of the features that challenge QoS provisioning in WBANs are resource constraints, traffic heterogeneity, real-time traffic, and frequently changes in network condition.

QoS for each layer is defined differently, like for application layer, QoS is all about system lifetime, system request and response time, resource allocation and processing time, data freshness, data resolution, data extraction, data discovery and data aggregation. At transport layer QoS directly linked to reliability, timeliness, and congestion. For network layer, QoS is termed as path latency, route destruction, routing robustness, energy consumption. At MAC layer, throughput, reliability and energy efficiency measures the QoS. For the physical layer, QoS defines in terms of physical medium and standards.

From communication point of view transport layer plays an important role and ensures end-to-end reliability in terms of packet delivery. The main requirement in a WBAN is timely delivery of packets with minimum loss. Compare to WSN, the employment of conventional reliability, timeliness, and congestion control at transport layer of WBAN may give better outcomes but fails to attain required QoS as it affected by various networking factors [35].

1.3.1 Factors affecting QoS in a WBAN

Despite the extensive use of WBAN in various applications, the variability in application-specific requirements demand different level of QoS [36]. The variation in performance metrics or factors reflects the QoS most. In addition to Loss and Delay, the factors those affecting the QoS in WBAN are explained below:

- *Limited Resources:* Limited resource is a big barrier for the WBAN as it restricts the proper utilization of resources, which drop down system performance.
- *Heterogeneous Traffic:* WBAN basically deals with heterogeneous and assorted traffic. This type traffic needs different kind of support like priority based queuing and scheduling and resource allocation. If traffic classification is not done

properly, then it creates a problem during scheduling which further degrades QoS performance in the system.

- *Bandwidth Sharing:* WBAN consists of various types of the heterogeneous nodes having different kinds of bandwidth requirement. So according to the requirement of bandwidth, a fair allocation of bandwidth should be done to achieve better QoS.
- *Criticality in node:* Depending upon the measured value the critical level of a sensor node is identified and according to this value, further decisions are taken. For a time-critical application, the critical value fluctuates frequently, and the QoS is influenced by this kind of changes in the system.
- *Dynamic nature of network:* Unlike other networks, WBAN are highly dynamic by nature. Sensed data from different sensor node may change their characteristics with time. These frequent changes in the WBAN must be handled properly in order to guarantee QoS in all circumstances.
- *Duplicate packet:* Generally in most of the systems, duplicate packet transmission may help in enhancing system reliability. However in WBAN, duplicate data transmission may cause wastage of resources like unnecessary bandwidth consumption and transmission delay, which further degrades QoS performance in WBAN.

1.4 PROBLEM STATEMENT

Most WBANs have heterogeneous traffic since they are dealing with multiple vital signals. It is often impractical or inconvenient to handle the sensors manually. Hence, it is necessary to employ an automatic, faultless, and pervasive system to improve the QoS over the period of time. All the available systems [53-54] tried to handle this requirement with their intelligent techniques but provide little benefit till today because of assorted traffic and dynamism in network. There are several challenges to be dealt in this domain, as QoS is tagged with several problems at each and every layer. The main objective of any WBAN is reliable and on-time transmission of data, and these factors and handled by the transport layer of the WBAN. Much research [70-71, 75] has been done to resolve reliability and congestion-related issues at transport layer to increase the QoS in the

WBAN. But these models have been silent towards other factors i.e. excessive or underutilization of Bandwidth, unnecessary retransmission of packets, transmission of duplicate data, jitter, waiting time, starvation and most importantly proper categorization, notification and early transmission of critical data. These factors also play a key role in QoS degradation in addition to reliability and congestion issues in WBAN. The above-stated limitations of WBAN need to be resolve for achieving improvised QoS in WBAN.

1.5 OBJECTIVES OF RESEARCH WORK

The main objectives of the research work are:

- To study various issues of WBAN i.e. Healthcare application in order to identify the factors which affect the QoS.
- To design a new architecture to resolve identified problems related to QoS at the transport layer of healthcare WBAN, which is capable to overcome QoS issues of supporting heterogeneous packet, data reliability, and congestion control as main features in a dynamic environment of WBAN.
- To design a heterogeneous packet handling protocol with dynamic prioritization policy in order to handle QoS in heterogeneous and frequently changing the environment of healthcare WBAN.
- To identify the critical condition as early as possible and notifies the same to the concerned person through alert messages.
- To detect and remove duplicate and retransmission overhead problems and to fairly share available resources among all sensor nodes according to their requirements.
- To improve the performance of QoS parameters in terms of Packet Loss, Delay, and Throughput.
- Compare the proposed system with existing systems with the help of some network simulator.

1.6 CONTRIBUTIONS OF RESEARCH WORK

The main contributions of this research work are presented as follows:

Design of a novel architecture for handling heterogeneous traffic in a dynamic environment of WBAN named DWBAN. This new architecture helps to serve a variety of applications including healthcare, military, sports and emergency services dealing assorted traffic in a frequently changing environment, which additionally adopt a dynamic priority policy for the enhancement of QoS in DWBAN. The proposed architecture put together the three solutions for enhancing QoS at transport layer; i) the Dynamic Priority based Packet Handling (DPPH) protocol, ii) the Modified DPPH (MDPPH) protocol and iii) the Optimized MDPPH (OMDPPH) protocol in order to offer improvised QoS while keeping packet loss, delay and throughput as key measurements in the dynamic WBAN system.

A Dynamic Priority based Packet Handling Protocol is designed for the DWBAN system to manage and prioritize incoming traffic properly. The main contribution of this protocol is to support system heterogeneity and deal with heterogeneous traffic efficiently with proper classification. It also offers a dynamic prioritization policy to assign specific priority to each sensor node as well as the packet, which further helps in Dynamic and Fair resource allocation, where sharing of resources done dynamically according to the requirement of the sensor node at that time span. Its scheduling approach decreases starvation issues at both queue level and packet level from the network. It also helps in detection actual condition of a patient as early as possible. All these features of DPPH protocols help in enhancing QoS by reducing important packet loss, transmission delay and jitter.

A Modified DPPH (MDPPH) protocol for the QoS management in the heterogeneous DWBAN is designed to overcome reliability and congestion related issues in DWBAN. The intended selective packet retransmission and recovery policy of the reliability module of MDPPH protocol retransmits only selected amount of high priority and high sequence numbered packets during loss recovery. By doing so, it reduces delay due to unnecessary retransmission of all lost packets. It also eliminates redundant packets transmission overhead issues with its duplicate packet mitigation approach. It follows a priority-based flow control or rate adjustment policy to utilize available resources properly so that large number of emergency and high priority packets

can be transmitted. Its intelligent queue management policy helps in reducing queuing delay and queue overhead problem by dropping selective amount of low priority packet during congestion.

An Optimized MDPPH (OMDPPH) protocol is proposed for further optimization of QoS performance metrics in the DWBAN system in order to achieve system specific QoS in a dynamic environment. It applies a Lion group hunting (LGH) optimization technique for the maximization or minimization of various performance metrics which are considered as the major QoS enhancement factors. The Lion group hunting technique is quite robust and gives satisfactory performance under the heterogeneous and dynamic environment with limited resources consumption. This optimization technique is scalable enough to find out the optimal solution that optimizes the solutions in a consistent manner despite the size of the solution space i.e. a number of sensor nodes. It helps in improving QoS performance by decreasing the packet loss and delay, and increasing the throughput of the DWBAN.

1.7 ORGANIZATION OF RESEARCH WORK

The structure of the research work is organized into eight chapters.

Chapter 1 brief outs a general overview of Wireless Body Area Network (WBAN) and introduce the main challenges faced by WBAN. This chapter explains the motivational factors which are helpful in carrying out the research. It also provides a background detail on QoS in WBAN and discusses the related issues present in each and every layer of WBAN. It also provides the motivation behind choosing the QoS issue present at the transport layer.

Chapter 2 presents intense survey related to research work. It covers research history and trends in evolution of WBAN. This chapter includes existing QoS related protocols. In each part of this chapter, a literature survey regarding different approaches used in this research work is been explained.

Chapter 3 discusses the overall design considerations for the proposed system. It begins with a brief description, motivation and long-term vision of the system. It contains the detail architecture and components of the proposed Dynamic WBAN system (DWBAN).

Chapter 4 presents first contributory work during research named Dynamic Priority based Packet Handling (DPPH) protocol. This chapter presents the introduction to DPPH protocol, its algorithm and its contribution with respect to various QoS parameters.

Chapter 5 explains second contributory work of research named Modified DPPH (MDPPH). MDPPH protocol is an extension solution to DPPH protocol. This chapter represents the ways to resolve issues at transport layer to enhance QoS in DWBAN.

Chapter 6 explains third contributory work of research named Optimized MDPPH (OMDPPH) protocol. This protocol uses a nature-inspired optimization technique called Lion Group Hunting (LGH), in order to improve more QoS performance metrics or factors. This protocol briefs optimization of various QoS factors.

Chapter 7 analyzes the performance of all proposed protocols in network simulator NS-2.35 and compares them with existing one as well.

Chapter 8 highlights the main contributions of the research work, concludes the proposed work and outlines the future research.

CHAPTER 2

RELATED WORK

2.1 INTRODUCTION

The Wireless Body Area Network (WBAN) is relatively advance and efficient network carrying slightly different feature as compared to Wireless Sensor Network (WSNs) [1, 3]. WBAN is always rewarded for its competence and skillful behavior in which it treats various applications like healthcare, disaster, sports, defense, and viable lifestyles etc. The objective of this chapter is to review and analyze various existing systems in WBAN. It provides a brief review of different QoS protocols at transport layer. Finally, a comparative analysis is done to looking at the ways that the involving mechanisms of existing protocols are alike or different.

2.2 WIRELESS BODY AREA NETWORK

Some unusual qualities of WBAN make it work differently to WSN. It has its own requirements, and limitations [12, 40, 124] which distinguish it from other networks and Table 2.1 shows all possible characteristics which differentiate WBAN from WSN.

Various WBAN systems [17, 22, 125] are following a general architecture as given in Figure 2.1. Where, the WBAN is equipped with sensors to measure several vital signals of a patient and send these measurements to a local server; Local server is a device acts as a gateway between the WBAN and the Remote server; Remote server is a device which securely stores, processes, and manages the huge amount of data coming from all of the local servers; User who observes and analyzes the incoming data, and forward appropriate instructions to the local server and patient; Database where data are stored for future use.

Table 2.1 Difference between WBAN and WSN

Features	Wireless Body Area Network	Wireless Sensor Network
Data Traffic	Heterogeneous	Homogeneous
Network size	Small (2-10 meter)	Large (100 m- km)
Communication	Singe or Next hop to Gateway node	Multi-hop
Redundancy	Does not deal with redundant nodes or data	Redundant nodes and data
Resources	Limited resources	Not limited
Scalability	On body nodes can be replaced and added easily	Nodes can be added with difficulties due to unreachable location
Loss	Loss of critical data is not bearable	Loss can be bearable
Latency	Cannot tolerate in case of emergency traffic	Can tolerate in some cases
Flexibility	High flexibility	Low flexibility
Battery life span	Life time/years/months/days	Years/months
Energy Scavenging	Done by body vibration, heat radiation	From solar/wind/vibration
Attenuation	In body tissues, temperature, and heat radiation, external factors	External environmental factors
Topology	Star and Dynamic when body move	Static
Mobility	Both Network and node Mobility	Mobility of individual nodes
Security	High level security, privacy data	Low level
Wireless standards	Low power i.e. Bluetooth, Zigbee, UWB	High power i.e. WiFi, Wimax, Gprs
Cost	Low	High

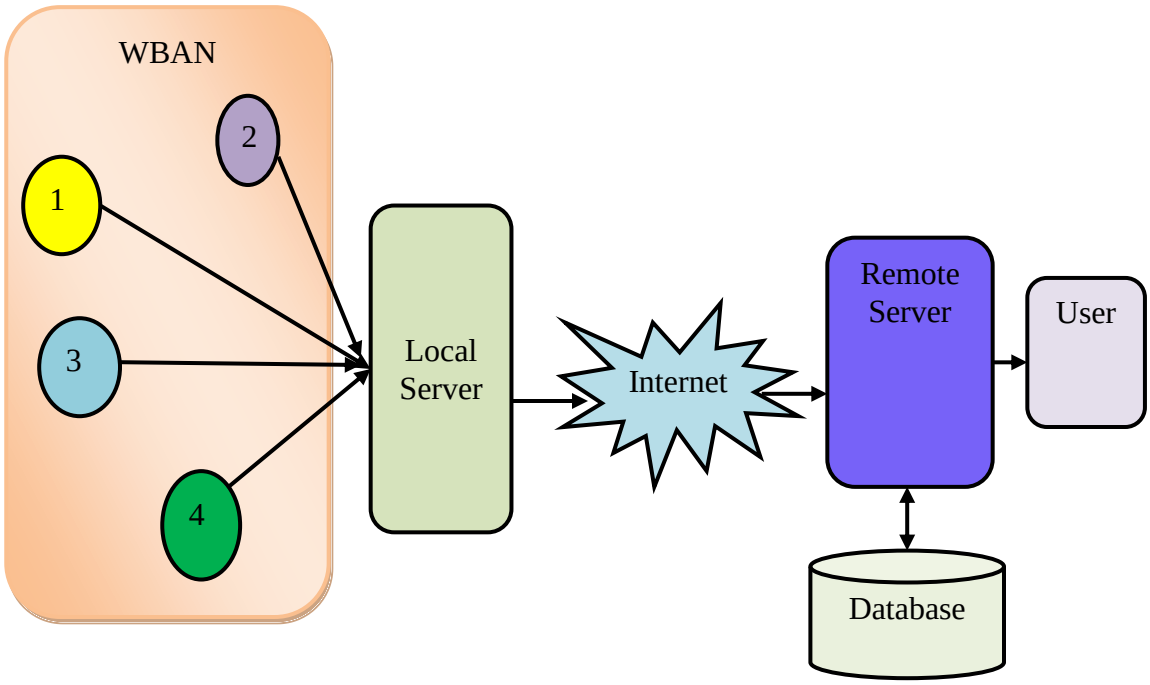

Figure 2.1 General Architecture of a WBAN

The integration of intelligent sensor devices in a specialized personal wireless network give birth to WBAN and its unique characteristics benefit variety of applications [24-25, 27, 41] including healthcare, physical rehabilitations, sports, emergency services, disasters, military, air force, fire fighters, terrorist trackers, bomb diffusers, astronaut monitoring, entertainment etc. The detailed application areas are explained in Figure 2.2.

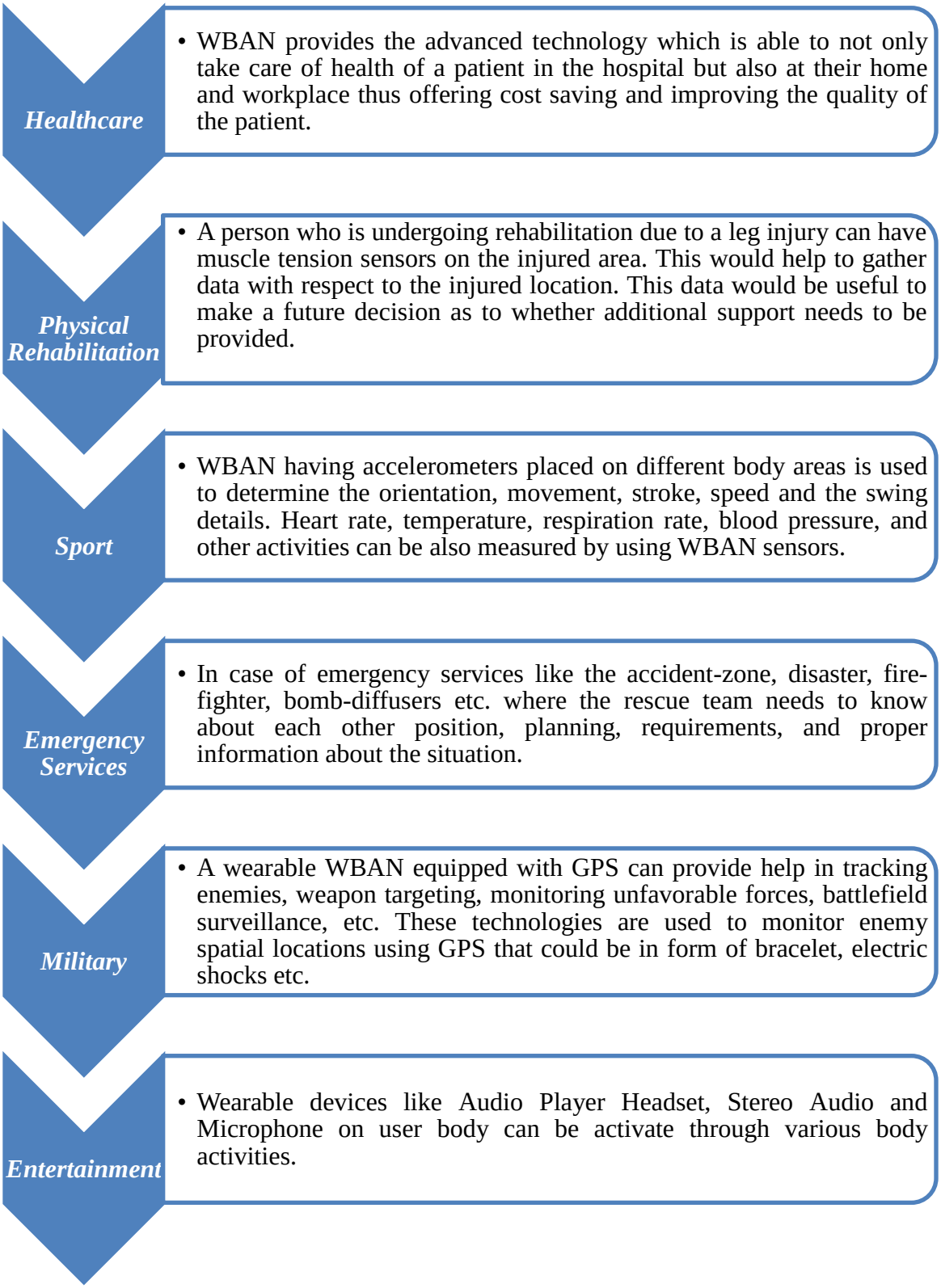

Figure 2.2 Various Application Areas of WBAN

A WBAN is a human centric network, where sensor nodes communicate with each other within a short-range communication area [20, 26, 32]. There are various communication standards which can be useful in WBAN. Descriptions of these standards are given below.

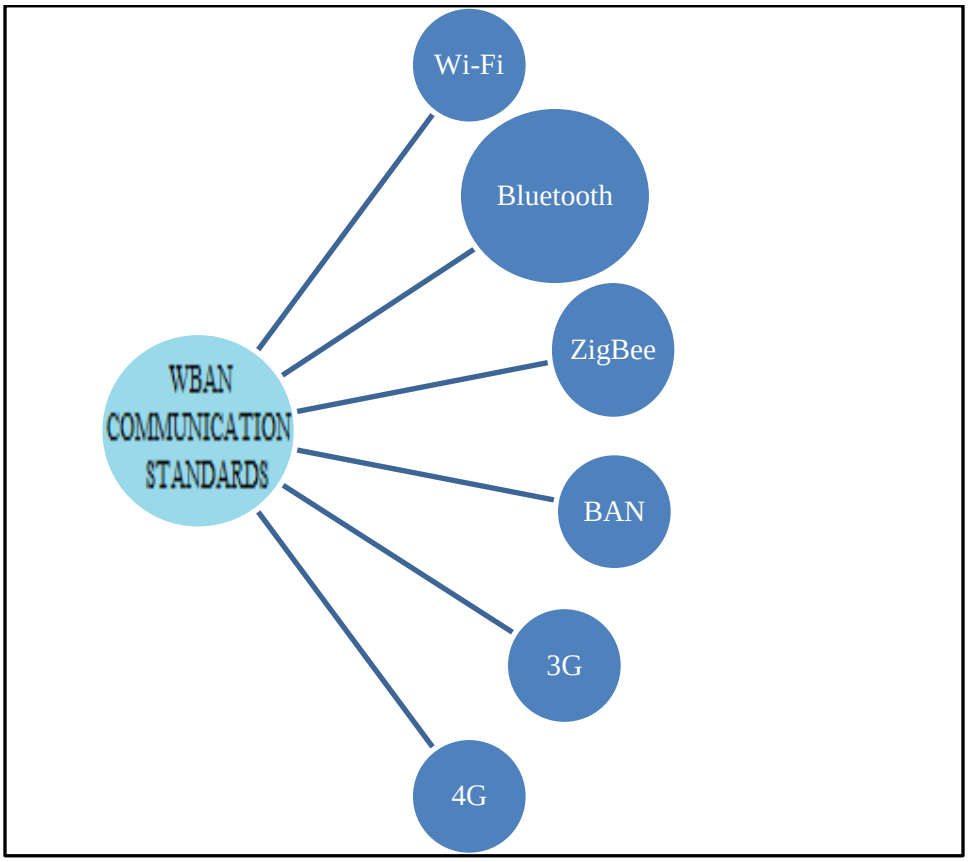

Figure 2.3 Various Communication Standards used in WBAN

- **Wi-Fi**: Wireless LAN, also known as Wi-Fi [13-14] is a set of low tier, terrestrial, network technologies for data communication. The WLAN standard operates on the 2.4 GHz and 5 GHz Industrial, Science and Medical (ISM) frequency bands [44]. The three most important versions of the WLAN standard are the 802.11a, 802.11b, and 802.11g. The most popular one is 802.11b, allowing 11 Mbps at a range of up to 100 meters, though the actual throughput of the user data is typically 6 Mbps. The application of the WLAN has been most visible in the consumer market, where most portable computers support at least one of the variations.

- **Bluetooth**: The IEEE 802.15.1 standard [13, 28, 33] is the basis for the Bluetooth wireless communication technology. Bluetooth is a low tier, ad-hoc, terrestrial, wireless standard for short-range communication. It is designed for small and low cost devices with low power consumptions. The technology operates with three different classes of devices, Class 1, Class 2 and Class 3, where the range is about 100 meters, 10 meters and 1 meter respectively. The Wireless LAN operates in the same 2.4 GHz frequency band as Bluetooth, but the two technologies use different signaling methods, which should prevent interference. Bluetooth can transmit at a speed of 1 Mbps, for the latest Bluetooth version 2 the transmit speed is 2.1 Mbps at ranges up to 10 meters.

- **ZigBee**: IEEE 802.15.4 is a low tier, adhoc, terrestrial, wireless standard in some ways similar to Bluetooth. The IEEE 802.15.4 standard [14, 39, 43] is commonly known as ZigBee, but ZigBee has some features in addition to those of the 802.15.4. The physical layer supports three frequency bands: a 2450 MHz band with maximum data rates of 250 Kbps, a 915 MHz band with 40 Kbps and an 868 MHz band with 20 Kbps, at ranges up to 10 meters. The ZigBee applications usually have lower data requirements, where Bluetooth is generally aimed at high data-rate applications.

- **BAN**: The IEEE 802.15 Task Group 6 (TG 6) is developing a new communication standard called the IEEE 802.15.6 [13, 29, 42] also known as the Body Area Network (BAN) standard, for low-power devices and operation on, in or around the human body to serve a variety of applications including medical, consumer electronics, entertainment and others. The BAN is still an ongoing standard whose first draft was released by the TG 6 in May 2010 with the latest draft of the new standard, the third version, being released in April 2011.

- **GPRS/3G**: The General Packet Radio Service (GPRS) [7, 13, 42] evolved from the Global System for Mobile Communication (GSM) to transport both voice and data in wireless cellular technology. The GPRS uses packet switching for sending

data. It enables connections to public and private data networks, such as TCP/IP and X.25 networks. The maximum data rate for the GPRS networks is 171 kbps. The Third Generation (3G) wireless devices use packet-switched networks for both voice and data. Theoretically, the 3G networks can offer a maximum data rate of 144 kbps in rural areas when a user is travelling at 500 km/h; 384 kbps in suburban areas at 120 km/h; and 2 Mbps at 10 km/h.

- **4G**: The 4G systems are being designed to support higher bit rates than 3G and full mobility. It is designed to deliver 5 to 10 times the rates of 3G that is, downlink above 100 Mbps and uplink above 50 Mbps [13-14]. The high data rates in 4G are achieved by using the technologies based on orthogonal frequency division multiplexing (OFDM) and Multi-Carrier Code Division Multiple Access (MC-CDMA). These technologies are also compatible with other enhancement technologies such as smart antennas and Multi Input Multi Output (MIMO) devices, together; 4G provides higher spectral efficiency and lower cost per bit than 3G.

A WBAN follows layered architecture and each layer performs differently from others. For managing risks in various healthcare applications in WBAN, it is essential to remove issues from each layer of WBAN [9, 23, 30, 37] in a suitable way. Issues directly affect the quality of data as well as service; on the other hand it can be disastrous when a critical condition was not detected timely and accurately.

Physical Layer

- *Topology:* In WBAN, with addition or removal of node the topology is changed, with change in sensor node's position the topology gets changed.
- *Data signaling*: Some applications of WBAN system requires constant signaling as they capture continuous and real-time data.
- *Data Rates:* It needs to handle different data rates due to heterogeneous kind of sensor nodes present in WBAN.
- *Device Design:* WBAN systems consist of tiny devices should be designed with low powered transceivers which radiate less heat.

- *Interference:* Sensor devices can tolerate heat or radiation emitted from human body. Interference should be minimized in between sensor devices implanted in, on human body, surrounding devices and external WBAN.
- *Band Selection:* Different WBAN applications require different kinds of Bandwidth, for example, ZigBee deals with health monitoring applications need low data rates needs low bandwidth, while Ultra Wide Band (UWB) expects more than ZigBee for real-time multimedia application.
- *Interoperability:* The integration of several sensing devices operating at different frequencies raises an interoperability problem.
- *Security:* Physical layer threat includes Jamming, Tampering, and Eavesdropping.
- *Fault tolerance:* WBAN system affected by many faults like environmental changes, hardware and communication medium problems.
- *Quality of Service (QoS):* As WBAN deals with real-time streaming of data, the capacity of data transmission medium and standards needs to be increased to enhance the QoS.

MAC Layer

- *Reliability:* Reliability is directly related to packet loss probability which is influenced by bit error rate of a channel and the packet transmission delay.
- *Control packets overhead:* Unnecessary transmission of control packets consume more resources and reduce the effective performance as they do not convey any data.
- *Scheduling:* Timely and guaranteed transmission of packet should be done with efficient scheduling.
- *Dynamic channel assignment:* Intelligent bandwidth assignment or dynamic channel sharing must be providing to avoid low throughput, high delay, high loss occurs due to noisy channel or interference.
- *Idle listening:* It arises when a node listens to an idle channel or when it is expected to receive packets and no packets are received. It consumes more power and time.

- *Over-emitting:* It takes place by long duration transmission of a message when the destination node is not ready to receive it. It may arises flooding at sink, channel busy, waste power and degrade performance.
- *Overhearing:* It is occurring when one sensor node receives a packet that is destined for other sensor nodes. Waste of energy take place due to acceptance of irrelevant packets.
- *Protocol overhead:* Some fields in the header like protocol-specific information (sequence number, sensor type, and packet type), connection identification (source, destination, and port address), and message specific information (checksum, timestamp, message length, priority) are increases significantly in some applications and needs to be handled otherwise causes problem.
- *Error Control:* WBAN require error resilience source, channel and network coding schema to control error and to increase network reliability.
- *Delay:* High transmission delay of packets occur due to low duty cycles. It needs be reduced.
- *Flow control:* Transmission delay and propagation delay occur due to flooding of packets at receiver side and should be controlled.
- *Synchronization:* Lack of synchronization in duty cycles of sensor nodes with variation in power and traffic distress the system throughput and energy.
- *Multi-radio and multi-channel design:* To avoid the collision, to improve performance and network capacity multiple channels can be used. Additional radios bands should be used in WBAN applications like disasters and live concert.
- *Energy maintenance:* Retransmission, collision, control packets overhead, over-emitting, overhearing, idle listening and traffic fluctuation are the main source of energy consumption.
- *Security:* Unfairness, Spoofing, Sinkhole, Sybil, Eavesdrop, Traffic analysis are the main attacks occur in this layer.
- *Fault Tolerance:* Faults in sensor node, and link, and scarcity in resources should be handled.

- *Quality of Service:* QoS in terms of flawless communication, throughput, reliability and energy efficiency can be achieved by adaptive channel coding, power scaling, and time slot division methods.

Network Layer

- *Optimum Routing:* To find an efficient path is a complex job because of limited bandwidth, fading, noise, and interference problem.
- *Delay:* On time delivery schema for real-time data must be enhanced to minimize delay.
- *Mobility:* Identification and maintenance of proper path in a dynamic or mobile environment of WBAN is tough task and should be done for performance improvement.
- *Traffic control:* Traffic control based routing protocol must be designed to control congestion and transmission rate.
- *Multi-Path Routing:* Multi-path and multi-point routing protocol must be applied for enhancement of performance and reliable data delivery.
- Control streaming: Streaming data over internet have significant problems like scalability, quality degradation in terms of high delay, high jitter, high loss rate and minimum throughput. Timely and reliable delivery of streaming data is more important in various applications.
- *Security:* Network layer of WBAN must be protected against Neglect, Homing, Misdirection, Black hole, Sybil, Sinkhole, and Selective forwarding attacks.
- *Fault tolerance:* Faults in network topologies and routing must be avoided.
- *Quality of Service:* QoS can be improved by handling path latency, route destruction, congestion, routing robustness, energy consumption, lost and damaged packets.

Transport Layer

- *Reliability:* Reliability is affected by high latency, bandwidth variation, short duration session, high bit error rates, and critical traffic.
- *Flow control:* Flooding in flow causes many problems like buffer overrun, transmission delay, propagation delay, congestion.

- *Congestion:* High data rates, low bandwidth, low buffer, and scheduling are the main sources of congestion. Congestion further causes to other problems like packet loss, limited throughput, packet drops and large buffer overhead.
- *Packet Loss or Drop:* Signal degradation over the network medium, channel congestion, faulty network is the main cause for packet loss. Buffer overflow, scheduling, queuing, duplicate retransmissions give arise to packet drop problem. Blindly dropping of packets may affect the quality of transmission, reliability, and increase latency, and jitter, and degrades the system performance.
- *Packet Re-ordering:* In-sequence delivery of packets is the most desirable feature of WBAN in order to handle reliability, packet loss and delay.
- *Jitter:* Introduced by congestion control mechanism and interference. This degrades the performance of the network, introduces unwanted noise in signals and increases the loss rate.
- *Traffic classification:* Applications of WBAN system monitor heterogeneous traffic which always influenced buffer strategy, delay, jitter, and bandwidth.
- *Scheduling:* Employment of an efficient scheduling mechanism to provide negligible starvation, stability and to do fair resource sharing is required.
- *Buffer management:* Mismanage buffer give rise to congestion, loss, and drop, delay, resource degradation problem.
- *Error control:* Corrupt or damage data may be dangerous for some WBAN application.
- *Security:* Protocol must be designed to protect from Replay, De-synchronization, Denial of service and Flooding attacks.
- *Fault tolerance:* Fault in link, path or session creation, should be resolved. Quality of Service: Transport layer QoS issues occurs due to Reliability, Congestion, Delay, Loss, and unfair bandwidth and buffer utilization.

Application Layer

- *Manage services:* It needs to handle network transparency, resource allocation, data dissemination, data advertisement, task assignment, sensor query and problem partitioning.

- *Delay management:* Smart organization of time for transmission, retransmission, and processing data are required as some of WBAN applications can tolerate delay up to some extent.
- *Traffic management:* Its main task is to efficiently allocate network resources containing buffer, bandwidth and link capacity, to provide negotiated quality of service, to isolate one traffic class from the effect of other traffic class.
- *Encoding and compression:* Best encoding and better-quality lossless compression schemas with low complex and less computation are designed.
- *Interface with user:* It includes rich query language, quality of required data and how easily data should be served to the user.
- *Security:* It needs to fight against the threats like cloning, path-based Denial of Service, clock skewing, overwhelming nodes, aggregation distortions and selective forwarding.
- *Fault Tolerance:* It must handle network failure, operational failure, environment failure, operating system failure, and software failure.
- *Quality of Service:* QoS issues include system lifetime, system request and response time, resource allocation and processing time, data freshness, data resolution, data extraction, data discovery and data aggregation.

Quality of Service (QoS) is becoming the major concern in providing high performance in WBAN. There are numerous survey papers on WBANs and its technologies. In [38-39] the authors give a comprehensive survey on QoS issues in WBANs, protocols used, issues and research challenges [40, 45] discuss about the enabling technologies of WBANs and more about the issues related to healthcare applications. As WBAN is internally designed with a layered architecture, each layer has its own QoS requirements. So, QoS issues would be different and the methods to handle these would be different [32] for each layer. The Table 2.2 provides the layer wise QoS Requirements, issues and metrics in WBAN.

Table 2.2 QoS Requirements, Issues and Metrics of WBAN

Layers	QoS Requirements	QoS Issues	QoS Metrics
Application Layer	Reliability Data novelty Data Security Sensor Management Task Management Time Management Query Management Fault detection Fault-free data flow Consistent Service Fair Resource Allocation	System Lifetime Request time Response time Data integrity Data freshness Data Security Data Compression Privacy Faults in Application Software	System Lifetime Request time Response time Service time Fault calculation
Transport Layer	Packet level reliability Flow control Congestion control Packet loss recovery Fair bandwidth sharing Redundant packet elimination Fair resource allocation Minimum Delay Packet Re-ordering	Reliability Congestion Packet loss Packet drop Out-of-sequence packet Delay Jitter Bandwidth Duplicate packet	Packet Delivery Rate Packet Loss Rate Packet Drop Rate Transmission delay Jitter Queuing delay Retransmission Rate Buffer or Queue occupancy Throughput
Network Layer	Minimize path latency No congestion Fair scheduling Optimal and multi-path routing Node and network mobility Fault prevention	Path latency Route destruction Link or route congestion Network Mobility Energy consumption Link and node failures Faults in routing	Routing overhead Routing Delay Jitter Packet Transmission Rate Packet Loss Rate Energy
MAC Layer	Link-level reliability Channel Coding Power Scaling Error Control Time-slot control Minimize Collision Link Fault Tolerance	Error or damaged packet delivery Packet loss due to collision Transmission Delay Faults in Links	Packet Delivery Rate Packet Loss Rate Packet Error Rate Collision Probability In-order Delivery Throughput
Physical Layer	Maintenance of changes in topology and communication settings Controlled Data rate Fail channel allocation Fair load distribution Fault tolerance	Changes in topology Faults in Communication, Medium or Standards Bandwidth, Transmission range Interference Attenuation Noise in signal Faults in devices	Capacity of mediums Data Rate calculation Inspection of standards Signal-to-Noise Ratio

Before moving forward, it is worthwhile to discuss the existing work by providing a brief idea about the research systems or projects that had done numerous works to design and develop an efficient healthcare WBAN.

2.3 EXISTING WBAN SYSTEMS

A variety of research projects have been carried out on Healthcare WBAN application and many are still going on. Here, some of them have been explained, whose main contributions include Alerting, Reliable data transmission, Routing, Congestion, Delay and Quality of Service (QoS) [36, 48].

A project named CodeBlue [46] was designed to serve people in emergency cases, patient rehabilitation and disaster, along with real-time monitoring and location tracking. It provides the services like in-network packet filtering, data aggregation, and handoff during mobility etc. In addition to these, it also provides a query management policy, which allows the concerned medical person to request data in emergency cases along with a query filtering ability. Here the routing is handled by a new component named Adaptive Demand-Driven Multicast Routing (ADMR) protocol, which establishes multicast paths during congestion in a route. The forwarder component of CodeBlue simply rebroadcasts the coming messages. The duplicate suppression component is used for the tracking and avoidance of multiple transmissions of data. As it is designed for reliable transmission of data but it is not able to provide better reliability. The reason behind this is that it achieves reliability only because of duplicate retransmissions of data. It also faces resource limitation problems and unable to share available bandwidth according to the requirement among all links. Due to lack of prioritization concept it is unable to resolve resource assignment as well as face problem during data transmission.

Developers develop a persistent health monitoring with the help of GPRS and UMTS cellular networks in MobiHealth [47] project. Its main work is to sense and broadcast the patient's body medical statics in a specific time bound. The client then separate out the important data, and transmit these data to the central processing server. The main benefit of this is an integration of existing and experimental 2.5-3G capable

prototype hardware components in a generic WBAN platform. Further, it provides security and encryption mechanisms during the data transmission, so that only the authorized person is able to access the data. Here set of sensors are extended with wireless intra-WBAN communication standards ranging from Bluetooth to ZigBee and each sensor nodes transmits the sensed signal to a central device called MBU, basically a gateway. The MBU forwards the vital signals to the actuators. The MBU includes three modes. i) Store mode: it stores data for a specific time period and sends them at regular intervals to the hospital server. ii) Process mode: It processes the data and provides the patient with some initial stage information. iii) Stream mode: It set up a permanent connection with the hospital server and sends the data in a continuous stream. It helps in transmitting live vital signals to healthcare providers. The problem with MobiHealth is that it is able to monitor some vital signals than others as some measurements are severely interrupt by movement or other body motion activities. For ambulatory monitoring it consumes more power. It also suffers from limited bandwidth problem during simultaneous monitoring of different vital signals. It is unable to adjust bandwidth as well as rate properly during low or congestion, hence QoS degrades.

The aim of UbiMon [49] is to provide unobtrusive and distributed mobile monitoring capture each transient event. UbiMon illustrates a logical cross-disciplinary integration of different expertise of the fields, bringing together electronics, computing, medicine. It is designed for uninterrupted monitoring of patients. The system provides the architecture for collecting, processing and analyzing data from a number of sensors. In addition to the physiological parameters, it includes the concept of context awareness to enhance the capturing rate of unusual event. To deal with the high data rate, a lightweight protocol with special TDMA (Time Division Multiple Access) mechanism was applied here. To inform the clinician about patient condition, signals in high risk are listed first than others. For this, it also considers the previous sensor readings. It only work well in a static environment and consume more processing power. It is very difficult for UbiMon to handle assorted traffic.

ALARM-Net [50] is designed for a heterogeneous network which helps in monitoring environmental and physiological data efficiently. It consists of three

components. i) Circadian Activity Rhythm (CAR): Its main work is to study the daily life activities continuously, judge the patterns and take a decision about which sensors should be alive and which one should be sleep for a particular time interval, which helps to save power of the system. ii) AlarmGate: It has three useful sub-components: the Context Manager, the Request Authorizer, and the Auditor. The Context Manager aggregate and keeps a detailed record of the context objects related to both the users and the environment. All requested query is first transmitted to the Query Manager who processes and filters them and further forwards them towards the Request Authorizer. The job of the Request Authorizer is to check the system's privacy policies and take correct decisions regarding the access of context objects accordingly. The Auditor maintains a trace of the access request in an audit trace file, including the decision made for each request (i.e. allow or disallow). The last component is designed with a security and privacy enhancement feature which allows only the authorized person to use the information. Here the Privacy Manager can be comprised of the AlarmGate and the Security Manager's access can be limited to the legitimate users. It provides benefits like reliability, power management, data protection, and privacy policy to improve the system performance. It is not deal with emergency data transmission, congestion or delay issues.

A remote healthcare system named CareNet [51] is having a two-tier wireless network and an extensible software platform. It provides reliable and privacy-aware patient data collection, transmission and access. It is integrated with a backbone structure which helps scaling its performance. A privacy and data confidentiality policy is used in its secure communication components. It provides a web-based patient portal which can be accessed by authorized person only. Here same data may be forwarded through more than one base-station to enhance reliability. While on the other hand, a transmitted data packet is marked with a timestamp in its packet header to identify and eliminate duplicate data. When a duplicate data packet arrives late at the router will get dropped. This is not considering the concept of loss due to congestion or force loss. Duplicate packet transmissions consumes system resources and increase transmission delay.

A novel project named MEDiSN in [52] was designed for both patient monitoring and disasters management functionality. It is deployed with a different advanced

wireless backbone to transmit each incoming packet in same way. Its application layer is modeled with a priority mechanism. It is having multiple physiological monitors (PMs), which are mobile in nature helps in keeping sensed data temporary. It then encrypts and digital sign the sensed data and sends them to the relay points (RPs). So it is integrated with different stationary RPs which are self-organized into a bidirectional routing tree and allows gathered data from PMs to be transmitted towards gateways and vice versa. Here the RPs integrated with a collection-tree based routing mechanism to transfer their measurements. Gateways are associated with a database to keep the data. The authenticated GUI clients have the right to access this database. It handles the loss due to congestion, and reduces end-to-end delay by decreasing retransmissions rate. It further provides reliable communication, and routing. In addition to this, it provides an alert message passing concept where it piggybacks all types of alert messages. But this kind of piggybacking give rise to other problems as it increases the delivery rate of unnecessary alerts despite the normal faults in the system. It fails to utilize resources in a proper way.

A system or device works in real scenarios when numbers of well-organized instructions are processed perfectly at the back-end and these instructions are called protocols which are useful to design and develop an efficient system. The following section briefly illustrates the most popular protocols and their contributions to design and develop an enhanced WBAN.

2.4 EXISTING WBAN PROTOCOLS

Leveraging the versatile nature of WBAN, an extensive of research work has been done in this area. The main concentration of these research lies on QoS issues related like reliability [63, 69, 72], congestion [58, 66, 78, 80], delay [76], energy consumption [10, 73-74] and routing [45, 77, 79, 96].

Wan C. et al. [55-56] had proposed Congestion Detection and Avoidance protocols which detect the level of congestion after measuring queue occupancy and channel weight. When a node identifies a high congestion, it will inform about this congestion to its upstream neighbor nodes. Here during congestion avoidance phase,

nodes follow an Additive Increased and Multiplicative Decreased (AIMD) based rate adjustment policy using open-loop hop-by-hop backpressure. It adjusts multi-source rate using a closed-loop end-to-end approach. If the node's flow rate is flooded the network, a special indicator bit named "policy bit" is used to indicate about the congestion. When an event packet with a policy bit was received by a sink, the sink will transmit an ACK packet to all sensors to cut down their rate. CODA does not provide reliability and its response time of closed-loop multi-source is increased with congestion.

Ee C. et al. [57] provides a Congestion Control and Fairness (CCF) protocol with scalable algorithm for many-to-one routing in WSNs. Here a packet servicing time is used as a congestion detection factor and the transmission traffic was adjusted accordingly for purpose of congestion mitigation. Here, congestion control is performed on the hop-by-hop basis and each node uses exact rate of adjustment based on its available packet servicing rate. The data sending rate of each node is shared by N number of its child nodes. If the congestion level is reached at its threshold value, then the child nodes reduce their data transmission rate. Since a separate queue is maintained for every child node, a considerable amount of bandwidth is exhausted in this algorithm and it is not efficient for dense networks. The CCF was unsuccessful to effectively utilize the remaining bandwidth in the system, which further degrades the system's throughput. The rate adjustment in CCF relies only on packet service time which again acts as a major factor to exploit for bandwidth utilization. As a result, situations arise where some sensor nodes do not have enough traffic to transmit and bandwidth not in use or situations when there is a significant packet error rate arises.

Iyer Y. et al. [59] have given a Sensor Transmission Control Protocol (STCP) protocol which was designed with upstream reliability with fixed window size and congestion control mechanisms. Here the sink node uses a NACK packet for loss notification and a timeout-based retransmission policy as packet loss recovery mechanism. It always uses an ACK packet for unpredictable event-driven packets. In STCP, with an increase in network load, the latency gets increased due to congestion and channel contention. In order to handle this situation, it transmits more numbers of NACK packets which consumes more bandwidth.

Wan C. et al. [60] have designed a Pump Slowly Fetch Quickly (PSFQ) based reliability protocol. It consists of two operations; i) Pump Operation: This operation helps in injecting packets slowly into the network, which helps in providing time-controlled data forwarding. ii) Fetch Operation: A hop-by-hop recovery is done in case of packet losses in fetch operation. It takes the help of caching policy to store the out-of-order packets at the intermediate nodes. Here NACK packet is used to minimize the signal overhead problem. The main limitation with PSFQ is that it is unable to detect the loss of whole message and a loss of a single packet. The process of slow packet transmission may results large transmission delay and underutilization of bandwidth. Its hop-by-hop recovery with buffer caching concept needs more energy expenditures.

Akan O. et al. [61] have proposed an Event-to-Sink Transport (ESRT) protocol which maintains reliability for the whole application and not for a single data packet by regulating sensor frequency. If event-to-sink reliability is lower than that of required level, then the reporting frequency of source nodes started to get aggressive and began to increase in order to achieve the target reliability level; on the other hand, if event-to-sink reliability is higher than that of the required level, the reporting frequency of source nodes is conservatively reduced. This nature of ESRT protocol makes it robust even with the dynamic changing topologies. It conserves energy by dynamically controlling sensor reporting frequency. When congestion occurs in one region of the network, ESRT protocol reduces the data rate of nodes in other regions also which degrades the overall network's throughput.

Wang C. et al. [62] have proposed a Priority-based Congestion Control (PCCP) protocol. It is designed for a WSN, where congestion level was detected after analyzing both packet inter-arrival time and packet service time. This system provides a priority-based rate adjustment algorithm at each sensor node. The node with higher priority index or node with burst traffic gets more bandwidth than other nodes. PCCP had tried to achieve high link utilization, small buffer occupancy, low packet loss and low transmission delay. It follows only congestion control policy not the congestion avoidance policy, where it increases scheduling and data rate of all traffic sources in case of low congestion, and decreases the sending rate of all traffic sources in case of high

congestion. It performs poorly when the system faces frequently changes in a congestion level. PCCP considers the geographical priority and does not support assorted traffic or dynamic priority concept.

Misra S. et al. [64] has given Learning Automata-Based Congestion Avoidance algorithm in Sensor Networks (LACAS) which mitigates congestion problem by applying the automata theory at each node. It learns from the earlier period performance and calculates an enhanced flow rate that helps to avoid congestion. The intermediate nodes are having traffic flow characteristics so as to avoid congestion before it occurs. It reduces delay by having same packet arrival rate and service rate. This protocol is designed for the homogeneous environment, which treats each node equally. LACAS lacks to provide fairness in scheduling so faces resource constraint and starvation problems.

Paek J. et al. [65] have designed a Rate Control Reliable Transport (RCRT) protocol which focuses on the reliable delivery of data from source to sink while avoiding any intermediate congestion collapse. It works on transport layer at the sink. RCRT attempts to achieve best reliable data delivery in the network based on a NACK scheme. Here congestion is detected from round trip time, rate adaptation, and rate allocation. If the measured value is more than the expected value, it means congestion has occurred and it decreases the flow rate. The time to recover loss is also used as an indicator of congestion detection. Therefore, as long as the network is busy in repairing the packet losses within the Round Trip Time, the network is out of danger. In case of congestion, it controls congestion through rate adaptation mechanism. A specific transmission rate is allocated to each data flow using rate allocation mechanism. An improved RCRT uses a timer as congestion indicator and NACK for hop-by-hop loss recovery. It mainly provides reliability, control congestion, flexibility in capacity allocation, routing dynamics, and scalability. The major drawback with this protocol is to tackle the node with different nature or responsibility in a dynamic environment like healthcare. It also fails to manage the convergence time with highly varying Round Trip Times.

Yaghmaee M. et al. [67] have proposed Learning based Congestion Control Protocol (LCCP) for WBAN. A classification mechanism was applied for the classification of different traffic. This further helps in assigning different priorities to different traffic. This priority is used during the data transmission. In addition to this, it actively manages the buffer and controls the congestion of the system with a learning based rate adjustment approach. The performance of LCCP is not good for highly dense network in terms of throughput, delay and drop rate. It faces high starvation during scheduling.

Rezaee A. et al. [68] presented a Healthcare Aware Optimized Congestion Avoidance and control (HOCA) protocol for WSN, where a multipath routing technique is used by HOCA in order to avoid congestion in the network and an optimized congestion control algorithm is used for congestion mitigation. It also provides a better priority based queuing and scheduling technique which is hybrid of Class-Based Weighted Fair Queuing and Priority Queuing (PQ) policies. It achieves low latency and more reliability for sensitive traffics due to its PQ policy, as it allows sensitive traffic to be sent first than others. It provides fairness between high-class and other class traffic by assigning 20% of network bandwidth to the high-class traffic and distributing 80% bandwidth among other traffic. Here the bandwidth performance parameter is calculated based on the number of packets arrived at the sink node in a certain time unit. HOCA has better bandwidth performance and uses different paths to send a great amount of traffic (multipath routing). It also uses a time constraint parameter for data forwarding. Each request of patients has an expiry period, the request is not considered anymore after the end of the period. During active queue management, it calculates a drop probability and proactively drops incoming packet. Further, this drop probability consider for determining the sending rate and the degree of congestion in each node and as a result, it controls the congestion by decreasing sender's sending rate and multipath routing. These kind of proactive drop increases the retransmission rate in the system, which further increases the delay and resource consumption measures.

Manfredi [70] presented a congestion control algorithm for differentiated and heterogeneous healthcare WBAN system. It considers that packet loss happened only

because of collision and provides retransmission mechanism to recover them in the network. It had used a weighted based fair capacity sharing approach which helps in scheduling. It further works on timely delivery of packets and energy expenditure and packet loss reduction. It does not use any approach to avoid congestion from the network and even unable to handled criticality problem properly as its rate adjustment is not criticality based. It only handled loss during the collision, and has less guaranteed reliability which further degrades the system performance.

Rezaee A. et al. [71] have designed an Optimized Congestion Management Protocol for Healthcare Wireless Sensor Networks (OCMP) to resolve the problem of congestion in the system. It calculates the sending rate of each child node by considering available bandwidth as well as child node's priority. It tries to work on probability based congestion avoidance method. If the incoming packet is accepted, it controls the congestion with the help of proposed automata based congestion detection, implicit congestion notification, and optimized rate adjustment methods in the next phase. It's queuing policy is having a physical queue which is shared by N child node's traffic and one local traffic based on their priority. More space is assigned to higher priority nodes. The free space of any node can be used by other nodes. The biggest drawback of OCMP is its rate adjustment mechanism which increases transmission rate of all nodes when the network becomes underutilized; decreases transmission rate when the network becomes over utilized. It also not deals drop, queuing delay, jitter, starvation and duplicate related problems.

Mohanty P. et al. [75] have proposed an energy efficient multi-path data transmission (ERMDT) protocol for healthcare WSN. It allocates fair bandwidth to each zone based on the "sensing reliability" and the "number of patients" belongs to that zone. It uses alternate paths to transmit emergency and sensitive data during congestion. It computes the congestion probability for each class of traffic from its buffer status and control congestion by adjusting traffic load of the congested node. The buffer of the intermediate node is partitioned into n+1 different virtual sub-buffer to store n number of traffic flows and the last one is acting as the shared buffer. The emergency traffic is allocated to the shared buffer first. It uses its dedicated buffer when free spaces are not

available in the shared buffer. The emergency and feedback traffic are assigned lesser weight than the sensitive and regular traffic as they are expected to be less in number. It assigns the highest priority to the emergency and reduces the energy consumption. It follows a selected drop policy to avoid congestion, and a hop-by-hop retransmission and acknowledgment policy to achieve system reliability. Issues like duplicate packet transmission, delay due to retransmissions, jitter are not taken into consideration.

Some of the above-mentioned protocols have considered packet loss, congestion, transmission delay, and energy consumption as the main parameters for QoS performance degradation but they do not consider delay like the variation in transmission delay, queuing delay etc. Problems due to duplicate packet transmission and unnecessary retransmissions are not considered at all.

2.5 CONTRIBUTIONS AND FINDINGS OF EXISTING PROTOCOLS

This section explains how and in which way these entire protocols handle the QoS at the transport layer of a WBAN. A comparison analysis of existing protocols has been done keeping in mind their prime conduct of work for the achievement of required QoS metrics. The review further reveals the main findings from the related works. The main objectives, methodologies, contributions, and findings of the existing protocols are discussed in Table 2.3.

Table 2.3 Contributions and Findings of different Existing Protocols

S. N.	Protocols	Objectives	Methodologies	Contributions	Findings
1	**Misra (2009)**	First to avoid occurrence of congestion. If congestion occurs then it tries to reduce the packet loss and	Learning Automata based congestion avoidance.	Avoid Congestion, Reduce energy consumption, increase throughput.	Treat all nodes equally. Considered only packet loss due to congestion. Work for stationary nodes.

		to equalize packet arrival rate and packet service rate.			
2	**Rezaee (2014)**	To avoid and control congestion	Avoid congestion at routing phase with multi-path routing. Control congestion with rate controlled and active queue management (AQM) approaches.	Provides a priority based data forwarding. Reduce end-to-end delay and energy.	Not good for dynamic environment. Its AQM approach increases the packet drop, retransmission and delay rate.
3	**Manfredi (2014)**	Fair allocation of Bandwidth. Control congestion Reliable and time transmission of data.	Weight based scheduling. Fast Retransmission and Recovery. Random Drop	Assigns a fair share of bandwidth among all nodes using different weights. Retransmits all lost packets Reduces the waiting time or queuing delay by dropping packets. based congestion avoidance	Its random drop policy increases the retransmission rate which further increases the transmission delay due to increase in retransmission rate. It only considers the packet loss due to collision.
4	**Rezaee (2014)**	To avoid and control congestion	Traffic Prioritization. Weighted Fair Queueing and scheduling. Single and virtual queuing concept. Automata based Congestion	Offers fair bandwidth allocation. Buffer is assigned to different traffic according to their priority. Its optimized rate adjustment policy	Randomly drop packets during AQM. Increases transmission delay and scarcity of resources due to retransmission of all packets.

			Detection. Optimized Rate Adjustment.	decreases loss, delay, and energy consumption.	Queue occupancy based congestion detection and available bandwidth based rate adjustment is not efficiently reduce loss and delay. Face queue-level starvation problem.
5	**Mohanty (2016)**	To increase reliability. Save energy. Avoid congestion. Bandwidth utilization	Fair Bandwidth Allocation. Multi-path routing. Weight based scheduling. Selective dropping. Rate adjustment.	Efficient data forwarding. Reduce congestion and increase reliability with multi-path routing. Reduce congestion with selective dropping and rate adjustment.	Face queue-level starvation problem. Transmission delay and jitter increases due to retransmission of all lost packet. Queue occupancy based congestion detection. Retransmission Timer and ACK based loss detection.

2.6 EXISTING PROBLEMS IN WBAN

The quality of a WBAN protocol is not only about how it senses data but is how it analyzes it. If data is available timely but not in a readable format (with huge loss or error) or data received in a readable format but not in time, then this data become outdated and is of no use. However, in order to tune with these problems many researchers have developed many protocols, but still have many consequences like elimination of duplicate packets; minimization of unnecessary retransmissions; reduction

of force packets drops due to buffer overhead, scheduling and duplicate retransmissions;, proper distributions and utilization of resources; handling of transmission delay and jitter; minimization of waiting time of packets in a queue; starvation, rate flow and congestion control. In addition to these, No one has focus on how to manage and deal with an suddenly disorder in the health status means no one has developed a system or protocol which can detect the abnormal condition accurately as early as possible and commute the same to the concern medical person in time.

2.7 SUMMARY

This chapter provides a brief overview of various QoS improving protocols and their applicability in various area of WBAN. A large extent of work with regards to reliable, congestion, delay, and energy have already done in different areas of WBAN. The main objective of this survey is to introduce and evaluate the contributions of these works and reveals the existing problems in WBAN. From the survey, it is concluded that they have provided excellent techniques for handling QoS issues in terms of Reliability, Congestion, Delay, and Energy consumption etc. which are highly suitable for healthcare, medical, patient monitoring system but some issues including assorted packet handling, retransmission, and duplicate eliminations are still untouched which may act as prime factors for the improvement of QoS. This literature survey becomes the base for building a new framework for improving QoS.

CHAPTER 3

DWBAN: DESIGN OF A NOVEL QOS FRAMEWORK FOR WIRELESS BODY AREA NETWORK

3.1 INTRODUCTION

WBAN possess both an electrifying and dynamic behavior in many application areas, the healthcare system is one among them. A critical glance from literature survey indicates that all the existing systems tried their best to resolve and improve various QoS related issues with their highly expert knowledge but are not effective enough. Hence, still there is a need for improvement in many areas, and also a scope to explore and resolve new issues. From a QoS point of view, healthcare systems do have stringent delay and loss requirements. As healthcare WBAN system is all about dealing with human life, lost or delayed data can cause danger to the patient's life. Some authors in their work [34, 36, 39] have been highlighted these areas to support QoS but fails to bridge the gap properly, due to the dynamic environment of the healthcare system where the condition of a patient can fluctuate over the period of time. It is been observed, there are certainly other models [71, 75] targeted dynamic nature but fails to meet the application specific QoS requirements. Although reliability and congestion gain lots of attention in last few years, accurate classification and scheduling of heterogeneous traffic is a major factor for this kind of systems and very few proposals are available to explore their capabilities for enhancement of QoS. In addition to this, real-time monitoring of patient creates a further burden on QoS performance. Very few researchers have concentrated on these problems up to some extent however not focusing on unnecessary consumption of network resources due to redundant and retransmission of packets, which further distress the network with a heavy load in many circumstances.

An in-depth exploration indicates that researchers have put their efforts to meet the required QoS by tuning essential issues such as packet loss, congestion, energy consumption, routing, scheduling etc. But they keep remained silent in many areas like

the elimination of duplicate packets, delayed packets and unnecessary retransmission of all lost packets etc. These limitations reflect the inspiration behind the design of a framework for handling heterogeneous packets and conquer all the evaluated QoS issues in a dynamic environment of WBAN to improve the QoS performance of the WBAN system.

3.2 PROPOSED DWBAN FRAMEWORK

Keeping in mind the imperative requirements of QoS, a novel framework named Dynamic WBAN (DWBAN) is presented here. The idea behind this employment is to distinguish and serve heterogeneous traffic [19, 41, 66, 74] in a dynamic environment with a required share of resources to provide high-level QoS. In this framework, packet handling and QoS enhancement will be taken as the main area of exploration. The first protocol is carried out to add the benefits of packet handling in the enhancement of QoS. The second protocol is an extension to the first contributory work which provides QoS in terms of reliability, congestion, duplicate or redundant packet, retransmission packet, and delays. In respond to pressing need of application specific service in WBAN, the idea of optimization technique is being conceived to improve QoS performance metrics. Finally, the proposed work is evaluated through a comparison analysis to briefs the thinking of what DWBAN system will contribute. So it further helps in proving how these contributions are efficient as compared to other existing works for providing enhanced QoS in time-critical healthcare WBAN.

QoS refers to a mechanism for resource reservation and utilization rather than just achieving high-quality service. In healthcare system appropriate extent of resource allocation among all sensor nodes and its proper utilization is a challenging task but on the other site, it is compulsory for achieving better QoS. The requirement of each sensor nodes varies according to their heterogeneous nature and with time, so need node level classification and this can be done by assigning appropriate priority to each sensor node.

3.3 DETAILED ARCHITECTURE OF DWBAN

The proposed framework has three major units: i) WBAN Unit (WBANU), ii) Controller Unit (CU), and iii) Medical Server Unit (MSU). The WBANU is a unit of heterogeneous

sensor nodes which sense various vital signals generated by the different sensors implanted in, on or surrounding of a patient, and then transmits the same towards CU. Subsequently, the CU does its processing and reroutes them towards MSU. The MSU checks the received packet and sent an alert message to the healthcare person . The detailed architecture of the proposed framework is explained in Figure 3.1.

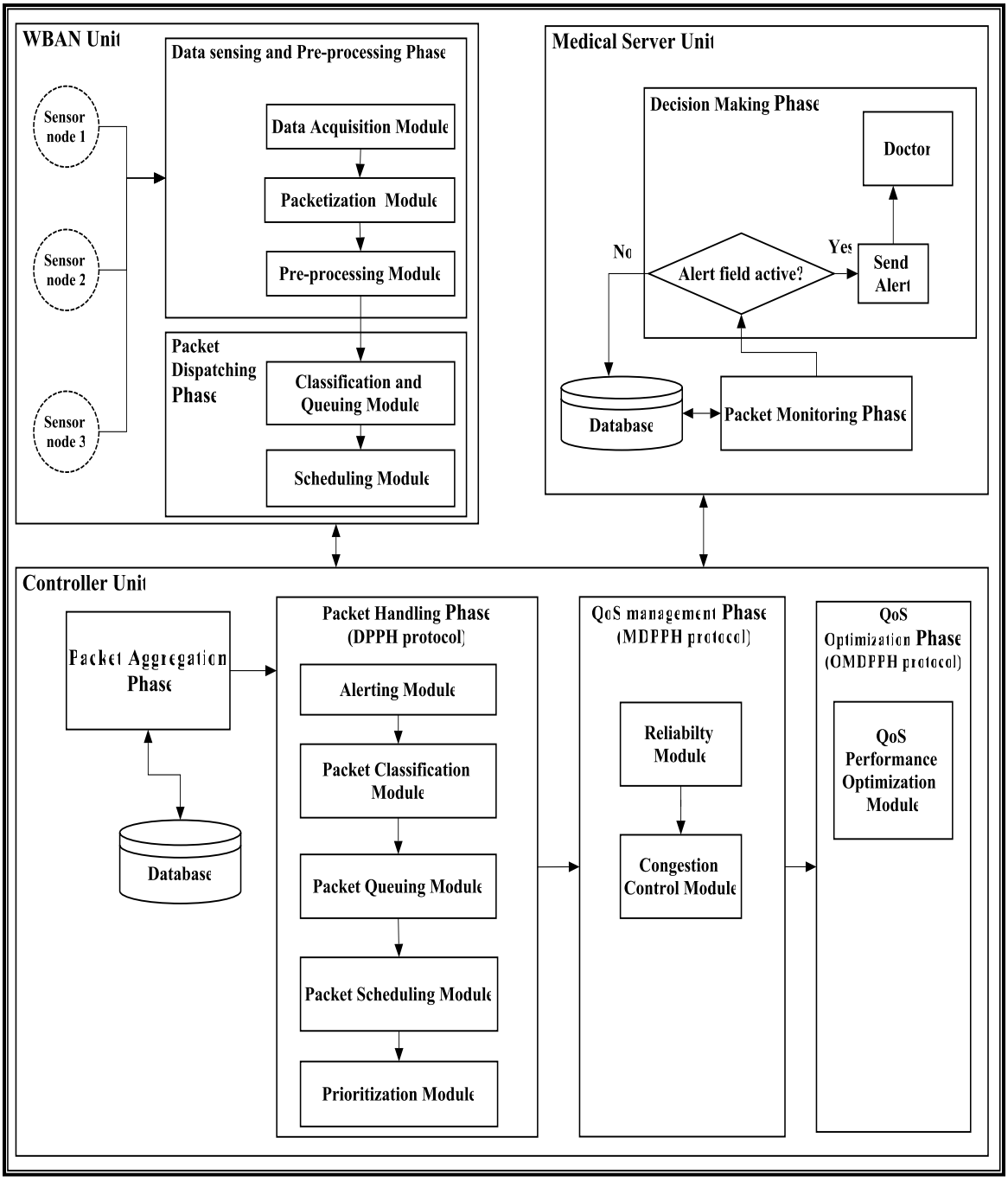

Figure 3.1 Proposed DWBAN Framework

3.3.1 WBAN Unit (WBANU)

WBAN Unit (WBANU) used to have a number of sensor nodes. Sensor nodes are tiny and intelligent devices which are having sensing, processing, and communication capabilities. Each and every sensor node captures vital signals from patient's body and then pre-processes them, and after that wirelessly transmits them to the CU. Each sensor node of WBAN allocated with a dynamic priority value assigned by the medical professional.

- Let's assume WBANU is having a different skill of sensor nodes $S_{i,}$ where i=1,2,..n denotes the priority of sensor S.
- T_M signifies the monitoring time, which can be furthered distribute into a series of time intervals T_k, where k= 1, 2,..n.
- For simplicity, it is assumed that every sensor node is having equal packet size (P_{Size}).
- A definite range r^{si} is set for each sensor node (i.e. $r^{si} = [r_{min} - r_{max}]$, where r_{min} represents the minimum value and r_{max} represents the maximum value for a particular vital signal).
- Critical threshold, Deadline, and Deadline threshold etc. are pre-estimated values for sensor node.

The modular architecture of WBANU is explained in Figure 3.2, where all the sensor nodes of WBANU consist of two phases: Data Sensing and Pre-processing phase and Packet Dispatching phase.

I. Data Sensing and Pre-processing Phase

The volume of data collection in healthcare WBAN systems is very high. So a more effective and efficient data sensing and processing techniques are required for accurate diagnosis of patient's actual condition. Various modules that come under this phase are:-

A. *Data acquisition Module:* After the establishment of the connection between a sensor node and the CU, each sensor node captures vital signal from the assigned body part through this module. This module is responsible for sampling the collective vital signals and converting them into digital formats for processing.

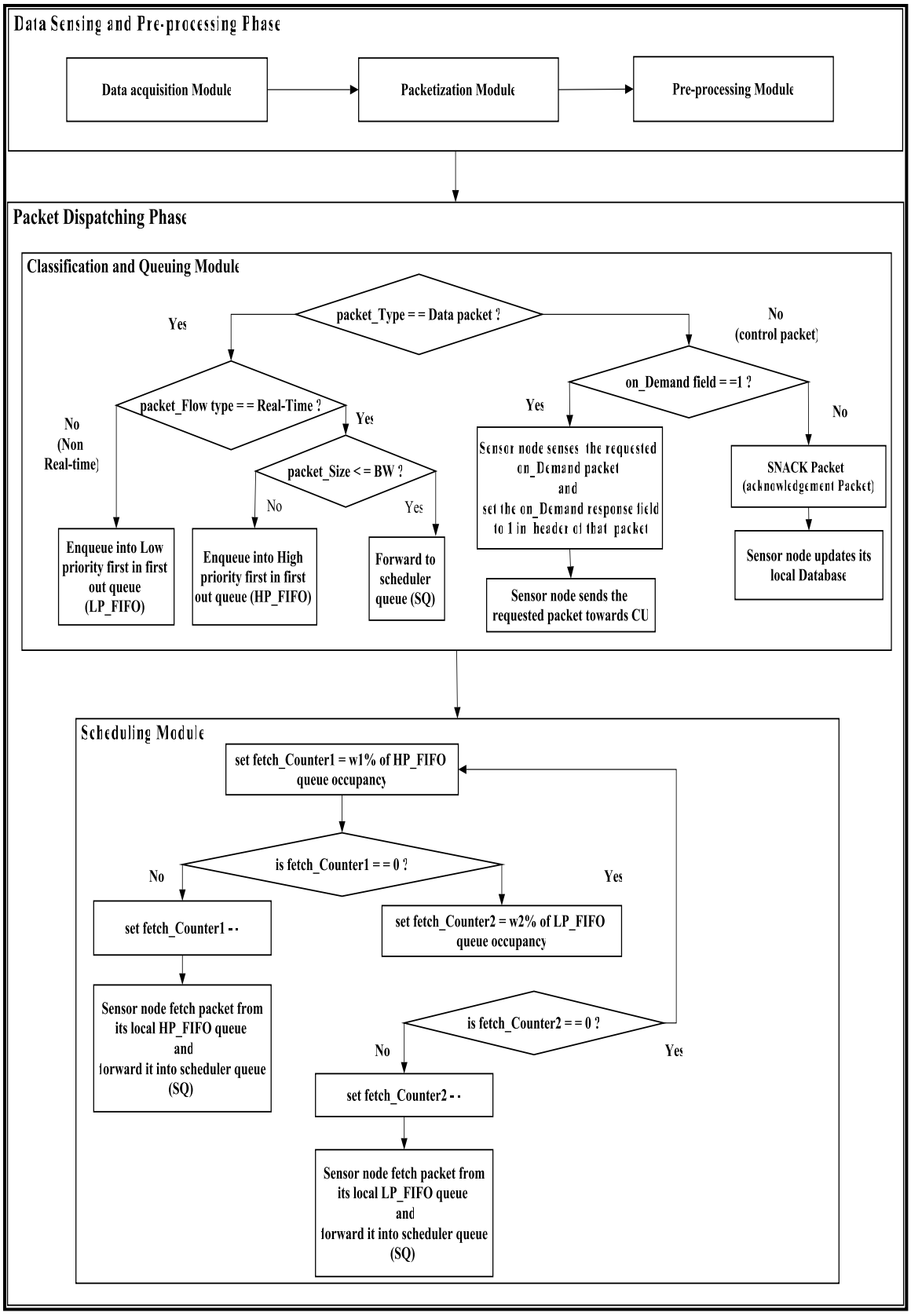

Figure 3.2 Workflow Diagram of WBAN Unit (WBANU)

B. ***Packetization Module:*** In Packetization Module, it splits the whole sensed vital signal sample into small fractions of a certain size (i.e. in bytes) called Packets. Each packet carries the actual data with additional information (payload) that will help for further processing i.e. IP address of sensor node, IP address of CU, sensor priority, packet size, bandwidth, transmission time, packet sequence number, no of packets sent in that time interval etc.

C. ***Pre-processing Module***: In Pre-processing Module, all pre-processing tasks are performed before a packet is being used for further processing. It allocates buffer and bandwidth to each sensor node. It also computes the sending rate and the transmission time for each packet in every sensor node. Therefore, computation of all these parameters depends on the priority of each sensor node to assure a certain level of required QoS.

- ***Allocation of Available Bandwidth (BW)***

  The available bandwidth [36, 39] for data transmission in WBAN is usually low. So a fair bandwidth sharing acts as an essential factor for the advancement of QoS. As every sensor node operates at different data rates in heterogeneous WBAN, equal bandwidth allocation might poses difficulties in many situations, like when nodes have to transmit images, audios, and videos data related to patient health. Another problem with WBAN is that what bandwidth allocated to all sensor nodes is not been utilized fully at all instances of times. Therefore a new bandwidth allocation technique is proposed here to distribute bandwidth among all sensor nodes as per their requirement. This further makes the correct use of bandwidth, as it calculates and assigns the bandwidth dynamically.

  In healthcare WBAN, some sensor nodes may be transmitted more data than other sensor nodes. The requirement of bandwidth can be changed with time, so need dynamic updating. The bandwidth allocation component should follow the following condition.

$$BW_k^{S_1} \geq BW_k^{S_2} \ldots\ldots\ldots \geq BW_k^{S_i} \quad (3.1)$$

where S_i denotes sensor node with priority i, and the sensor node with high priority assign more bandwidth than the low priority sensor node in the time interval k.

As depending on situation priority of any sensor node can be changed at any point of time, so a fair bandwidth allocation is done here in a dynamic way to handle all situations. Equation (3.2) helps to calculate the bandwidth ($BW_k^{S_i}$) allocated to each sensor node S_i at time interval t_k.

$$BW_k^{S_i} = Ceil\left(\left(\alpha * {BW_{av}}/{n}\right) + \left(\beta * {BW_{av}}/{i}\right)\right) \quad (3.2)$$

where BW_{av} is the whole available bandwidth between the WBANU and the CU, i denotes the priority of sensor node and n is the total number of sensor nodes. Here α and β *are the coefficient factors having values 0.6 and 0.2, and these values are chosen after an analysis as given in Appendix A.*

- ***Data Sending Rate (DSR)***

  Data Sending Rate can be expressed as the total number of packets which needed to be sent at a given time interval. With time, the data sending rate of any node can be changed, and they can need diverse reliability. In order to overcome from heterogeneity in reliability, the total available bandwidth should fairly share among all the nodes. The reliability can vary from sensor-to-sensor and data-to-data. For example, a heart patient with an ECG node required continuous monitoring of heartbeat signal, to generate more data as compared to the body temperature node which is been used for sporadic monitoring of body temperature. On the other hand alerts and on-Demand data that carry important information ought to be delivered without loss and within a reasonable deadline. The purpose of dynamic calculation and assignment of data sending rate to each sensor node in DWBAN is there to avoid congestion and huge delays; also it helps to prevent loss of critical or emergency data.

The calculation of DSR should be done in a manner which must be fair for all the sensor nodes, also which should not unnecessarily stuck packets when the network is lightly loaded. A *Quick Start* based DSR strategy is been proposed here for the proper utilization of bandwidth. Existing systems follow a standard slow start data rate [101], where data transmission is started with a fixed value i.e. one or two packets. Then it gradually increases its sending rate using additive increase method of Additive Increase and Multiplicative Decrease (AIMD) policy [102-103]. When congestion occurs, it cut down its DSR to either one packet or half of its current DSR using multiplicative decrease method of AIMD. The successor phase follows the same process by increasing one packet to its new DSR. The slow start process denotes the system performance by lowering packet delivery ratio and bandwidth consumption. The main focus of the quick start approach is to increase packet delivery ratio with the full and fair utilization of bandwidth. In the quick start, after the connection establishment phase, DSR for each sensor node is been calculated by the CU depending on each sensor node's priority so that they can send more numbers of packets and use bandwidth more effectively. Each sensor node follows the following inequality as the calculation of DSR totally depends on the priority of each sensor node.

$$DSR^{S1} \geq DSR^{S2} \ldots\ldots\ldots \geq DSR^{Si} \tag{3.3}$$

where i=1,2,….n are priority of sensor node.

The initial DSR for the time interval T_k is calculated exponentially in equation (3.4).

$$DSR_k^{S_i} = 2^{n-i} \tag{3.4}$$

where n denotes a total number of sensor nodes, and i denotes the priority of the sensor node.

In the subsequent time interval, DSR is increased or decreased according to the existing congestion level of the network.

- ***Transmission Time Gap (TTG)***

  In DWBAN, it is a basic requirement that the arrival of a packet at the destination should be within the specified time period. This arrival time can vary from sensor-to-sensor. For example, an ECG sensor node monitors data for every millisecond whereas; a body temperature sensor node senses data for every hour. By varying data transmission time for each and every sensor node, the packet transmission delay and congestion could be minimized. So a new approach called Transmission Time Gap (TTG) is introduced here. The proposed TTG is computed dynamically by the CU and notifies to all sensor nodes. The TTG helps in calculating the time gap after which a packet can be transmitted from a particular sensor node to the CU. TTG follows the sensor's priority for better result and the following inequalities.

$$TTG^{S1} \leq TTG^{S2} \ldots\ldots \leq TTG^{Si} \quad (3.5)$$

  As the TTG provides the gap between transmissions of two chronological packets for every sensor node in a particular time interval, so each sensor node considers its own TTG value for packet transmission. The TTG value for a particular sensor node can be calculated using equation (3.6).

$$TTG_k^{S_i} = 2^{i-1} \quad (3.6)$$

  where i denotes the priority of the sensor node and k denotes the time interval T_k.

  BW, DSR, and TTG are calculated individually and assigned to every sensor node dynamically for the utilization of bandwidth more effectively and minimization of packet loss.

II. Packet Dispatching Phase

The ultimate purpose of this phase is to categorize the generated data as per their traffic pattern, enqueue them, and schedule them in such a way that, appropriate dispatch of the packet will be done towards CU. This phase is having two modules.

A. Classification and Queuing Module

Classification is the process in which categorization of traffic is been done. On the basis of traffic flow type, data packets can be classified into two different categories under the proposed Classification Module. These are Real-Time (RT) and Non-Real-Time (NRT) traffic. This module is an important part of packet dispatching phase, which deals and maintains fairness in resource sharing by classifying and assigning priority to each flow. After having a practical or real-world scenario, RT and NRT data packets prioritize on the basis of their importance i.e. RT data packets ought to tend higher priority than NRT data packet. So that RT data packets are being processed prior to NRT data packets and can be successfully transmitted towards CU with least amount of delay.

On the other hand, a queue is a place where all the packets can be stored until there will be a proper availability of resources. The proposed Queuing Module differentiated between real-time and non-real-time traffic and interfaces with dual queues at the sensor node i.e. High Priority First in First out (HP_FIFO) queue and Low Priority First in First out (LP_FIFO) queue. On the basis of packet's priority, the queuing module inserts RT packets into HP_FIFO queue and NRT packets into a LP_FIFO queue. Each generated packet is forwarded to CU, instantly, on the availability of bandwidth. Otherwise, those RT packets will be saved into the HP_FIFO queue. Whereas, the NRT packets will store into the LP_FIFO queue unless and until they get a chance to transmit. The mechanism proposed in queuing module can maximize QoS while reducing queuing delay.

Algorithm 3.1 describes the working of classification and queuing module implemented at sensor node.

Algorithm: Classification and Queuing Module (at sensor node)

Input: *Packet*
Output: *Storing of packet in appropriate queue*

1. *Upon reception of packet*
   // Check packet type
2. ***If*** *(Packet Type==Real-Time),* ***Then***
   // Check availability of required bandwidth
   2.1. ***If*** *((Packet Size <= BW_k),****Then***
      2.1.1. Forward the packet towards scheduler queue
   2.2. ***Else***
      2.2.1. Enqueue packet into HP_FIFO
   2.3. ***End If***
3. ***Else If*** *(Packet Type==Non-Real-Time),* ***Then***
   3.1. Enqueue packet into LP_FIFO
4. ***End If***

Algorithm 3.1 Algorithm for Classification and Queuing Module at Sensor Node

B. Scheduling Module

Scheduling is the process which deals with decision making regarding the service sequence of data packets. A *Ratio Based Scheduling (RBS)* algorithm is proposed in Scheduling Module, where high priority queue gets a chance for its service prior to the low priority queue. This module follows a priority based servicing procedure, where the packets with high priority will get a chance first, whereas the packet with low priority will get a chance for their servicing afterward. According to above mentioned the data packets which are with the same priority will serve as First Come First Serve (FCFS) basis. The key job of RBS scheduling algorithm is to calculate the service rate (i.e. percentage) for both queues so that packets should be served from both HP_FIFO and LP_FIFO queues. Here the scheduling module of a sensor node checks HP_FIFO and LP_FIFO queue occupancy. After that, it extracts a 30% percentage of packets from HP_FIFO queue and 10% from LP_FIFO queue. The selection of 30% and 10% during percentile rate calculation is found in *Appendix B*. Finally, these packets queued into the scheduler queue for further service. Therefore, RBS scheduling method is a useful practical solution for the starvation problem at sensor node's local queues. It also ensures

a better level of fairness in scheduling among both queues. Algorithm run in scheduling module of sensor node is explained in Algorithm 3.2.

Algorithm: Scheduling Module (at sensor node)

Input: *Packet*
Output: *Serve packet or Drop packet*

1. ***While*** *(time interval is not expired),* ***Do***
   //Calculate the service ratio for both queues
   1.1. count1=30% of HP_FIFO queue occupancy
   1.2. count2=10% of LP_FIFO queue occupancy
   1.3. set fetch_Counter1=count1
   1.4. ***While*** *(fetch_Counter1! = 0),* ***Do***
      1.4.1. Fetch and delete packet from HP_FIFO
      1.4.2. Forward packet to scheduler queue
      1.4.3. set fetch_Counter1 - -
   1.5. ***End While***
   1.6. set fetch_Counter2=count2
      1.6.1. Fetch and delete packet from LP_FIFO
      1.6.2. Forward packet to scheduler queue
      1.6.3. set fetch_Counter2 - -
      1.6.4. ***End While***
2. ***End While***

Algorithm 3.2 Algorithm for Scheduling Module of Sensor Node

3.3.2 Controller Unit (CU)

This is been observed that in many cases in a healthcare system, a patient may be implanted with a group of sensor devices. The CU plays an important role and acts as the head for all those sensor nodes. Figure 3.3 explains the whole working principle of the CU.

The function of CU is to collect all physiological or vital data received from the sensor nodes. The collected data is further processed by the CU before transmitting to a Medical Server Unit (MSU) through wireless communications. The CU consists of following four phases.

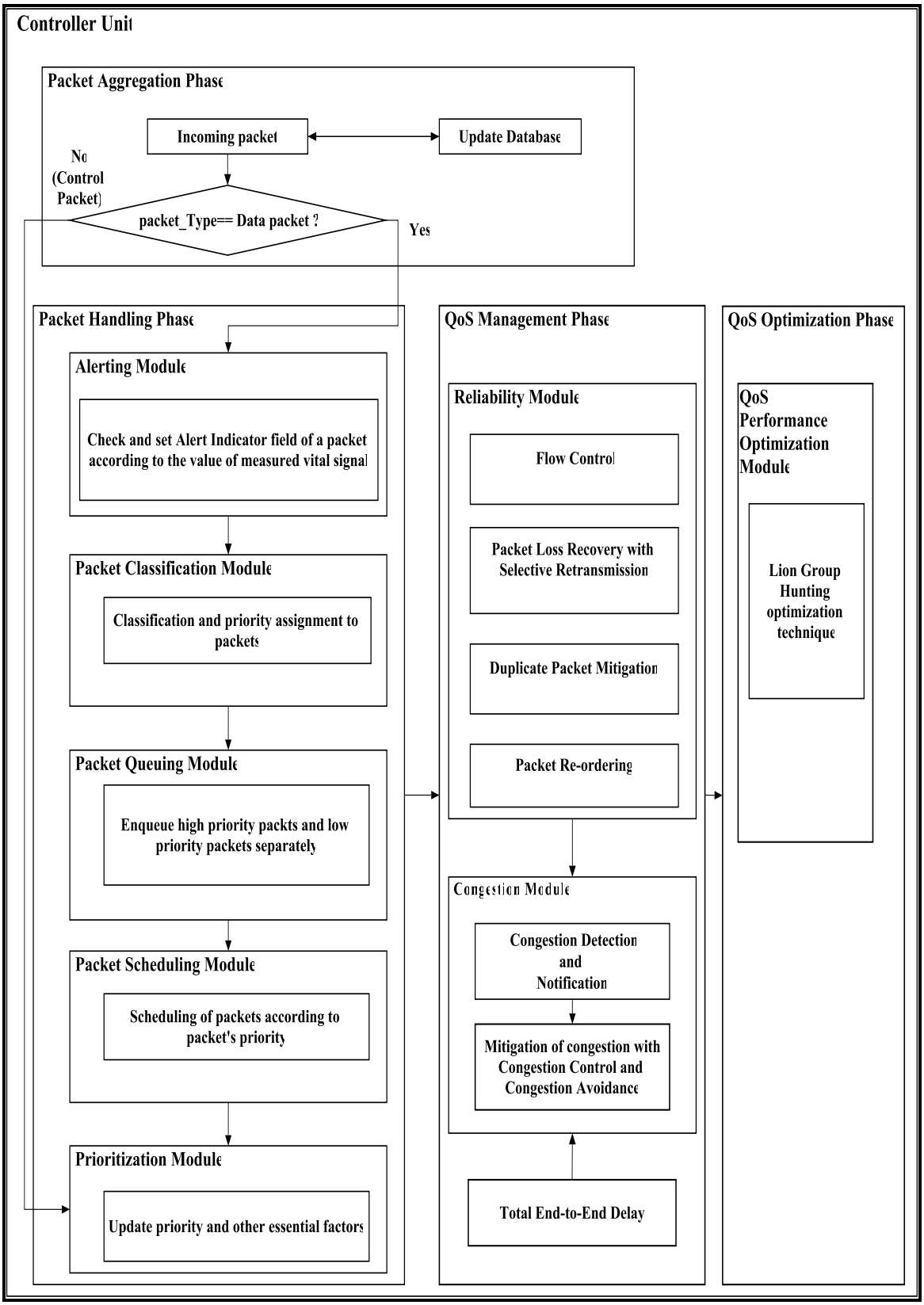

Figure 3.3 Workflow Diagram of Controller Unit (CU)

I. Packet Aggregation Phase

Aggregation [81] is the process of collecting data from various sources. In packet aggregation phase, the data obtained from all sensor nodes are aggregated based on certain criterion. It assists CU for further processing and updating of the database which further helps to supply essential information about the packet. In packet aggregation phase, aggregation is performed on packet level by combining and storing the payload and data of several packets into a central area. Its main objective is to get rid of duplicate and redundant packets and by this way it helps to save resources in terms of bandwidth, buffer, and energy. The packet aggregation phase will further help in accurate packet handling and QoS management in successor phases.

II. Packet Handling Phase (DPPH Protocol)

The important thing about this phase is that it handles and manages the incoming packet before it can use for further post-processing. This packet handling procedure provides a great help in achieving required QoS, because packets are the prime building block of any network. A protocol named Dynamic Priority based Packet Handling (DPPH) protocol is been designed so that handling of incoming packets can be done in a more accurate way for achieving better QoS in the DWBAN. It takes care of heterogeneous packets and limited resources. Moreover, to this, a healthcare system needs early identification and notifications in case of emergency situations. DPPH is able to come out of this problem by its in-time criticality detection and alerting approach. It also helps in reducing false alerts so that the valuable resources can be saved.

The most important job of DPPH includes packet level classification and prioritization for optimal resource utilization. It also provides both queue level and packet level scheduling for the recovery from the starvation problem. Further in a healthcare system, patient's health status fluctuates with time and any sensor node becomes vital at any point in time. Above mentioned situations can be some time complex, so to overpower this situation, the mechanism of dynamic prioritization is been developed in DPPH which is able to handle both packet and node priority.

III. QoS Management Phase (MDPPH Protocol)

The conduct of process in regards of QoS deals with an additional protocol called Modified DPPH (MDPPH), which is developed in the second phase of DWBAN to handle QoS issues in terms of reliability, congestion, redundant packet, retransmission packets, and delays.

The correct meaning of reliability is to successful delivery of packets at the destination node. A healthcare system requires deviation in reliability. So the Reliability Module of MDPPH uses selective retransmission approach for taking a careful decision in regards to retransmission rate calculation as well as packet loss recovery. This approach will further help in reducing transmission delays and also in saving bandwidth, as it minimizes retransmission rate by retransmitting only selected amount of important packets. It also ensures amplification in packet delivery ratio by proposing node based prioritization flow control and rate adjustment approach. This module is also very much useful in terms of mitigation of duplicate packet.

Congestion in DWAN needs to be mitigating in order to care network resources, improve fairness, reduce loss, and minimize packet delay. The congestion in a system is prolonged to data transmission or sending rate and take place when packet incoming rate surpasses packet outgoing rate in a queue. The proposed Congestion Control Module is designed to avoid congestion before it happens and control congestion after its occurrence. Inappropriate or obsolete information about the network congestion causes the system resources to be underutilized. Therefore to avoid such kind of problems, a multi-parameterized based congestion detection method has been proposed here. It also provides a very simple and smoothening process to mitigate congestion with dynamic rate adjustment and selective drop policies.

Hence, both reliability and congestion modules further help in minimizing the transmission and queuing delay problems along with packet loss.

IV. QoS Optimization Phase (OMDPPH Protocol)

The effectiveness of the proposed protocols do not necessarily reflect the required QoS performance under all circumstances and hence found, it still needs the best-suited techniques to meet required DWBAN specific QoS. These days various nature-inspired or bio-mimetic optimization algorithms are been applied in various fields to produce better outcomes. Therefore, in the third phase of DWBAN, a nature-inspired optimization algorithm is been applied to improve QoS in WBAN and is named as Optimized MDPPH (OMDPPH) protocol. The main objective of this optimization algorithm is to optimize the large number of diverse factors, which have been addressed as major performance parameters for the enhancement of QoS in DWBAN system. In the proposed OMDPPH protocol, a mathematical model of lion group hunting techniques is used. In order to get improved QoS in all situations, a novel fitness function has been formulated for all performance metrics. It has been cleared from the stated study that the lion group hunting algorithm is quite robust and provides satisfactory solutions. Hence the use of this technique can improve performance under all circumstances of DWBAN in its heterogeneous and dynamic environment with limited resources.

3.3.3 Medical Server Unit (MSU)

Medical Server Unit is the backbone of the proposed framework. It receives packets from the CU and intelligently takes the decision. It is the prime duty of MSU accepts health related data from CU and store it into corresponding medical server database. This further helps a medical person in analyzing the data patterns and also diagnosing the health status of the patient. The MSU is also responsible for the inspection and notification of an alert message to the healthcare professional in case of any emergency situation occurs. The medical person can update pre-defined health related parameters and can ask some extra information from CU through MSU. The whole working principle of the MSU is given in Figure 3.4.

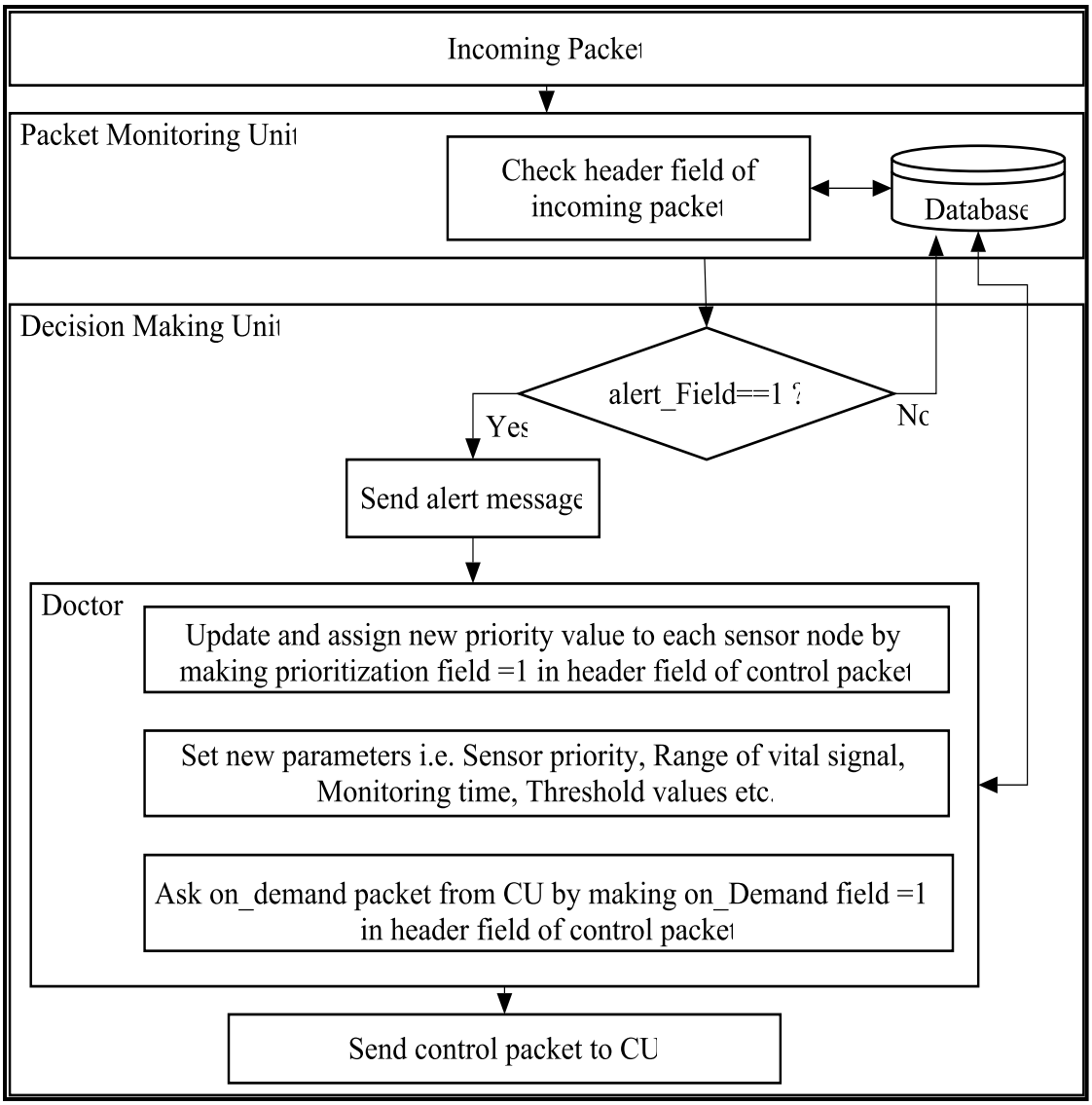

Figure 3.4 Workflow Diagram of Medical Server Unit (MSU)

I. Packet Monitoring Phase

In this phase, the MSU analysis the data provided by the CU, which can be demonstrated on the screen on the requirement basis. This data will be kept in the medical database so that it can be used in future. In this way, the stored data in the medical database can be helpful for identification and further diagnosis in patient's monitoring. This phase keenly observes every field of the each arrived packet and keeps updating its database accordingly.

II. Decision-Making Phase

The MSU checks alert_field of an incoming packet, if this field is in active mode, then it recognizes the serious health condition, the medical person can be immediately notified by issuing an alert message, which further helps the medical person to diagnose the health condition and take essential action.

Here a medical person can access patient's health related status from both local and remote place through the internet. The concerned medical person can take appropriate decision on the basis of receiving alerts as well data from the MSU. In this way, she/he can amend or demand more information regarding patient like;

- She/He can ask more detailed information from a specific sensor node. In regards to this, the MSU demand the same from CU by updating the On_Demand field in control packets.
- She/He can reprioritize all or most of the sensor nodes in case of emergency situation. On behalf of a medical person, the MSU will notify about these dynamic updation to the CU by activating the prioritization field in control packet.
- Similarly, she/he can make a request for modification in any parameter, which is being pragmatic for the patient's treatment. It is the duty of MSU to inform the same to the CU.

Apart from these, the MSU can also provide some feedback instructions to the patients prescribed by the medical person.

3.4 COMPARISON ANALYSIS

This section evaluates the behavior of proposed DWBAN framework against the existing ones. A research study [55-75] explores all the QoS related problems which can arise in WBAN along with their relevant solutions is been presented in the form of comparability. A deep comparison is made on the basis of a before-mentioned survey by considering various QoS measure parameters. The comparison table in Table 3.1 evidently prove that the incorporation of existing protocols is resilient to various other problems such as redundant packet elimination, retransmission of selected number of packets, starvation,

active queue management, and packet drop management, minimization of false alert notification, resource sharing and network dynamics.

Table 3.1 Comparison Analysis of DWBAN System with Existing Systems

Protocols---> Features	***OCMP (2014)***	***ERMDT (2016)***	***DWBAN***
Issues resolve	1.Congestion Control	1.Congestion Control 2. Reliability 3.Bandwidth allocation	1.Packet handling 2. Alerting 3. Reliability 4.Duplicate packets 5. Congestion 6. Delay 7. Retransmission 8. Packet Drop
End-to-End/ Hop-by-Hop	Hop-by-Hop	Hop-by-Hop	End-to-End
Dynamic priority	Patient and Node level	Weights	Both Node and Packet level
Bandwidth	Fair sharing	Zone and patient based	Sensor priority based
Rate adaptation	Slow start	Slow start	Quick start and Priority based
Packet Transmission Time Gap	Fixed	Fixed	Variable (priority based)
Classification	Service based	Flow based	Both flow and packet based
Scheduling	Weighted Fair Queue (WFQ)	Weighted Fair Queue (WFQ)	Ratio based Earliest Deadline First (REDF)
Starvation Handling	Queue level	Queue level	Queue and Packet level
Packet Loss Recovery	Retransmission of all lost packets	Retransmission of all lost packets	Retransmission of selected lost packets
Congestion Detection	Single Factor (Queue occupancy)	Single Factor (Queue occupancy)	Multiple Factors

Active Queue Management	Random Early Drop	Partial Drop	Selective Drop
Delay minimization	Waiting time delay	Queuing delay	Queuing and Transmission delay, and Jitter

OCMP [71] handle heterogeneous traffic perfectly, but deficient to control unnecessary packet retransmissions and packet drops during congestion. However, ERMDT [75] provides some methods to resolve retransmission overhead problems, but pays no attention towards packet drop and duplicate packet related problems. The DWBAN consider all the essential factors which are the prime concern for the enhancement of QoS.

3.5 SUMMARY

WBAN is attaining widespread attention in various healthcare applications since last few decades. It has been observed and analyzed from the recent literature study that, despite having potential ability, WBAN is lack to deliver data accurately and on time. Hence, experience worse quality of service (QoS) in the network. The demands of dynamic and heterogeneous factors in healthcare WBAN infuse the idea of developing an effective framework for the improvement of network performance in all situations. Thus to initiate this, a new architecture has been designed in this chapter. The main focus of this architecture is to handle heterogeneous constraint in the dynamic ambiance of WBAN. The proposed Dynamic WBAN (DWBAN) with its three protocols provides its best contribution to achieve enhanced QoS performance in terms of loss, delay, and throughput etc. At last, the influence and impact of proposed framework over existing ones are been done with the comparison analysis which further helps to brief the motivated thoughts behind the development of DWBAN.

CHAPTER 4

DPPH: DESIGN OF A DYNAMIC PRIORITY BASED PACKET HANDLING PROTOCOL FORDWBAN

4.1 INTRODUCTION

Exponential growth for improving QoS includes reliability and congestion as major factors, while it is evident from literature survey that QoS is primarily dependent on the proper packet management. Hence it is utmost importance to employ packet handling protocol as the primary task. However, very few researchers have thought of employing packet handling to enhance QoS. The QoS factors are highly influenced by increased network load, indiscriminate and heterogeneous traffic flows in WBAN. So for the attainment of improved QoS, an organization of packets should be done on a prior basis to resolve QoS issues from the healthcare WBAN system. This inadequateness encourages us to explore the feasibility of an effectual packet handling protocol named as Dynamic Priority based Packet Handling (DPPH) protocol in DWBAN, for managing heterogeneous packets in a frequently changing environment.

4.2 PACKET HANDLING WITH THE USAGE OF DPPH PROTOCOL

This is the first objective of our proposed research. Here we intended to develop a heterogeneous packet handling protocol for a dynamic environment as it is the fundamental building block of CU to make QoS provisioning in DWBAN as excellent as possible. As we know that, the improvement in QoS is not possible without dealing with following factors in any network i.e. heterogeneous traffic flows, packet loss, throughput, packet delay, jitter, and bandwidth utilization etc. Therefore the offered protocol with a variety of modules has been designed in such a way so that emergency and assorted packet handling can be done in an accurate way in DWBAN. It has taken alerting, prioritization and scheduling as the main area of exploration, whereas, the other two

baseline logics are there, which basically depends on classification and queuing of packets. Figure 4.1 shows the modular architecture of packet handling phase.

Figure 4.1 Modular Architecture of Packet Handling Phase (DPPH Protocol)

Here the packet handling phase deals with five different modules. The packet classification, packet queuing, and packet scheduling modules, are responsible for classification of packets according to their traffic type, assigning of priority to packets, and in-time queuing and scheduling of packets. In addition to these, the alerting module

is responsible for early identification of unusual condition and activation of alert field. Further, the prioritization module is designed in such a way that the MSU can handle an emergency situation by updating valuable factors regarding patient's vital signals with the help of CU. Prioritization module typically updates the priority of nodes, vital signal ranges, monitoring time and various threshold values etc. with the concern of medical person.

4.2.1 Alerting Module

Timely abnormality detection and notifications are two essential requirements [82-84] in healthcare WBAN for the correct treatment of patients. The mandate need of healthcare WBAN is to have an early warning system that can spot and vigilant the actual condition of all operative vital signals. However, from the literature study it is concluded that, most of the detection algorithms have limited capabilities such as that they could not be able to detect exact condition in a precise time interval. So be unsuccessful to fetch patient's actual health condition. Hence, there is a need to develop a process that can unfold in-time and accurate detection of an emergency situation in frequently changing environment of healthcare WBAN. Another key obstacle in healthcare WBAN, particularly in emergency situations is that sensor nodes may continue with their pre-set parameters and try to work despite soreness in the environment until they are ordered to change or immobilize the pre-mentioned parameters. In addition to these, issuing of alerts for any deviation in each incoming packet may increase the false alert rate and at the same time, false alerts can create a negative impact on the healthcare system, also further escorts to consume more network resources i.e. bandwidth, buffer, power or energy consumptions. At the same time false alerts may lead to undesirable consequences as the medical person can be busy in attending false alerts when real emergency data may be left unattended, which could cause fatigue to the system. Wrong measurements can also be another cause for the false alerts which may need unnecessary intervention for the healthcare personnel. So with this analysis, it is clear that the WBAN actually requires a proper alerting scheme with new improvisations, so that early and accurate detection can be done and false alert rate can be reduced. Wrong measurements can also be another cause for the false alerts which may need unnecessary intervention for the healthcare personnel. So with this analysis, it is clear that the WBAN actually requires a proper

alerting scheme with new improvisations, so that early and accurate detection can be done and false alert rate can be reduced.

Therefore, to avoid incorrect alert and wrong detection, a new alerting approach is being proposed in DPPH protocol. This approach has the potential to detect the emergency situation and will be able to reduce false alert rate. The proposed alerting module keeps a tally on received measurements so that the actual condition of a patient can be identified timely. It also quantifies the changes happens in activity or event levels, and at the same time can take specific actions. It works on the average frequency of variations in all measurements (e.g., vital signal variation value), as well as their median and deviations values, to account its alert detection. The alerting module monitors all the incoming packets at a particular time interval, and then an alert indicator got activated when the measured value exceeded the actual range of the vital signal. Unlike many other emergency protocols, it does not require user intervention and hence considered as much more effective than others. Here the alert indication field remained active until the packet reached the MSU. As the alerting module provides early detection with early warning, most of the time it acts as timely packet inspection module that analyzes packets for stimulating quick health interventions. It is basically designed to detect impending conditions, and will further help in sending accurate and clear notifications to the medical person or caregiver at the right time and in a definite way. An additional approach is then designed to differentiate between real health conditions and false alerts, so that the alerting process can further help to improve QoS in the system. The objective of this approach is to effectually separate false alerts from true alerts. Further, the packet classification and prioritization modules are directly reliant or subjected to alerting module.

Eventually, packets from various sensor nodes are received by the CU. Once when a packet is been received, in order to predict the fault, certain criteria must be specified. Hence, a threshold based alert mechanism is provided here as it is a suitable method for false alert detection. For accurate condition detection, data of the incoming packets were examined using statistical methods consist of weighted standard deviation (i.e. where

weight means the frequency of occurrence) along with mean and variance. Therefore differentiation between false alert and true alert totally depends on this threshold value. Here statistical analysis is applied to the previous data to determine an accurate deviation value, which is dynamically changed with time. Working principle of alerting module is mentioned below.

Step 1: Analysis of packet

The first and foremost job of the alerting module is to analyze the incoming packet and to check whether there is any abnormality present in the sensed vital signal or not. So, by choosing this method the incoming packet will compare with the pre-defined vital signal ranges. The calculation of variance is done with the difference between measured sensed value and the actual range. This difference provides actual information about the vital signal; whether it is critical or not.

Step 2: Variation Identification

The concept of Variation Identification works on Variation Indicator ($V_{Indicator}$), which provides the deviation between actual sensed value and the normal range of the vital signal. It calculates the absolute difference between these two. Then the value of $V_{Indicator}$ is used to identify the level of criticality. If the value of $V_{Indicator}$ is not equal to zero, then the alerting module stores this value into the CU database. Mathematically, $V_{Indicator}$ for a packet is calculated from equation (4.1).

$$V_{Indicator} = \begin{cases} M - r_{max}, if M > r_{max} \\ r_{min} - M, if M < r_{min} \\ 0, if r_{min} \leq M \leq r_{max} \end{cases} \quad (4.1)$$

where M is a measured or sensed vital signal value carried by a packet, and [r_{min} - r_{max}] indicates the minimum and maximum range value of the vital signal.

Step 3: Critical Counter

A concept of critical counter is added here in order to reduce false alerts from the system because false alerts add confusion and chaos, which further reduce the efficiency of overall network resources. The actual condition of a vital signal cannot be analyzed

accurately from a single packet. Therefore, the proposed alerting module uses the concept of critical counter by calculating a counter value for a particular time interval, so that several packets can be considered for criticality analysis. Detection of critical condition after analysis of multiple packets further helps in resolving the false alert problem. For a given time interval, a critical counter is calculated using equation (4.2).

$$C_{counter}^{S_i} = \frac{current\ DSR\ of\ sensor\ node\ S_i}{2^i} \quad (4.2)$$

where DSR is the data sending rate mentioned in previous chapter in equation (3.5) and i is the priority of the sensor node S_i.

Step 4: Criticality Indicator

The idea of activating critical indicator is to make aware a medical person aware about the expected criticality. When there was a reduction in the standard deviation variance of the collected data, the alerting module activates the alert indication field in the header part of the packet otherwise it activates the critical indicator field to provide pre-notification to the medical person about the chance of emergency occurrence. The alert indicator was activated after some time bound of monitoring, in order to perceive accurate condition and because of that quality of the monitored sample can become more imperative. These variations in packets are statistically report and revealed significant abnormalities in the system. Because of this, the alerting module can successfully detect and report the actual situation in all circumstances. The job of criticality indicator is to help the MSU to differentiate between the crucial and critical condition of a patient.

- If the MSU receives a packet with critical indicator field in active mode, then it will not send an alert message to the concerned medical person, but at the same time, this field helps the medical person to diagnose the pre-critical condition of a patient.
- The alerting module calculates the variation in each incoming packet using equation (4), unless until the critical counter value reach at zero level.

- Addition to this, if the calculated value of $V_{Indicator}$ is not equal to zero, then the alerting module activates the critical indicator ($C_{Indicator}$) field of packet $P_{i,j}$ of sensor S_i, by following the equation (4.3).

$$C_{Indicator}^{P_{i,j}} = \begin{cases} 1, if V_{Indicator} \; ! = 0 \\ 0, if V_{Indicator} = 0 \end{cases} \tag{4.3}$$

where $V_{Indicator}$ is the deviation between sensed vital signal and the normal range of a vital signal.

Step 5: Weighted Deviation Estimation

The main objective of estimation of Weighted Standard Deviation (W_{dev}) is to help in identifying the actual condition of a vital signal because it calculates the exact and accurate deviation value for a particular time interval. Further when the critical counter value reaches to zero; the alerting module starts fetching all $V_{Indicator}$ values from CU database. It then arranges them in the ascending order and finds their frequency of occurrences. After that, it selects their median value, calculates their difference from the median value and finds their W_{dev} as shown in equation (4.4).

$$W_{dev} = \sqrt{\frac{\sum_{l=1}^{C_{counter}} f_l * d^2}{\sum_{l=1}^{C_{counter}} f_l} - \left(\frac{\sum_{l=1}^{C_{counter}} f_l * d}{\sum_{l=1}^{C_{counter}} f_l}\right)^2} \tag{4.4}$$

where f_l denotes the frequency of variation in sensed values, d denotes the difference in deviation and median value, and $C_{counter}$ denotes the critical counter value.

Step 6: Alert Indicator field activation

Alert Indicator ($A_{Indicator}$) field of a packet plays an important role to assist the MSU to take the actual decision. The main purpose of this component is to check the W_{dev} value against the critical threshold value, which was set by the concerned medical person and can be updated with time. If the W_{dev} value is greater than the value of critical threshold, then alerting module activates the $A_{Indicator}$ field of the packet in packet header area.

- In the proposed DWBAN system, the status of a patient can be classified into Normal, Severe or Critical. This status will be decided based on the reception of alert messages from MSU.
- As soon as a packet with active alert indicator field is been received by the MSU, the MSU will immediately send an $A_{Indicator}$ to the concerned medical person.
- If the packet is having $A_{Indicator}$ field in inactive mode but having the critical indicator field in active mode, then it will be treated as low-level critical packet by the MSU and the MSU will not issue any alert message for this packet.
- The formula given in equation (4.5) helps in finding and activating the alert indicator ($A_{Indicator}$) field of a packet.

$$A_{Indicator} = \begin{cases} 1, & if W_{dev} > Critical\_TH \\ 0, & otherwise \end{cases} \quad (4.5)$$

where $A_{Indicator}$ is the alert indicator value, W_{dev} denotes the weighted standard deviation and Critical_TH denotes the critical threshold value.

The flow chart of the working of alerting module is given in Figure 4.2. To detect the variation in sensed vital signal, it uses Algorithm 4.1, which explains the working principle of proposed alerting module at CU node.

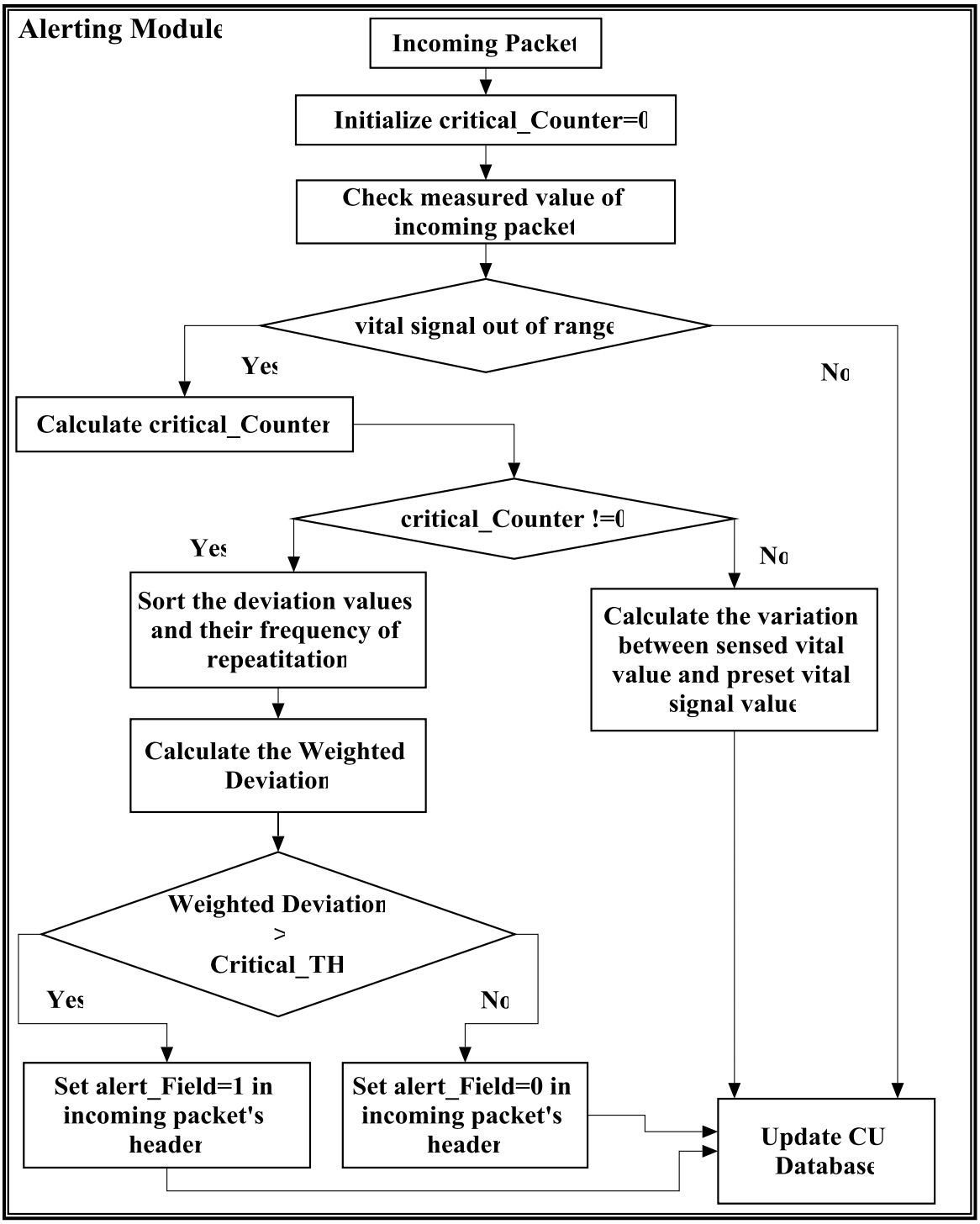

Figure 4.2 Flowchart of Alerting Module

Algorithm: Alerting Module

Input: *Measured vital signal value in incoming packet, and critical threshold value*
Output: *Alert Indicator field*

1. *Upon reception of data packet*
2. ***While*** *(time interval not expired),* ***Do***
   - 2.1. *Find variation index* $V_{Indicator}^{P_j}$ *using* ***Equation (4.1)***
   - 2.2. ***If*** ($V_{Indicator}^{P_j}$*! =0),* ***Then***
     - 2.2.1. *Find critical counter* $C_{counter}^{S_i}$ *value using* ***Equation (4.2)***
     - 2.2.2. ***While*** ($C_{counter}^{S_i}! = 0$), ***Do***
       - 2.2.2.1. *For each incoming packet*
       - 2.2.2.2. *Find variation index i.e.* $V_{Indicator}$
       - 2.2.2.3. *Store value of* $V_{Indicator}$ *into CU database*
       - 2.2.2.4. ***If*** ($V_{Indicator}$*!=0),* ***Then***
         Set critical indicator field to 1 as given in ***Equation (4.3)***
       - 2.2.2.5. ***Else***
         Set critical indicator field to 0 as given in ***Equation (4.3)***
       - 2.2.2.6. ***End if***
       - 2.2.2.7. *Set* $C_{counter}^{S_i}$--
     - 2.2.3. ***End While***
     - 2.2.4. *Find* W_{dev} *using* ***Equation (4.4)*** *when* $C_{counter}^{S_i}$ *becomes zero*
     - 2.2.5. ***If*** (W_{dev}*>Critical_TH),* ***Then***
       - 2.2.5.1. *Set alert indicator field to 1 as given in* ***Equation (4.5)***
     - 2.2.6. ***Else***
       - 2.2.6.1. *Set alert indicator field to 0 as given in* ***Equation (4.5)***
     - 2.2.7. ***End if***
   - 2.3. ***End if***
   - 2.4. *Update CU Database*
   - 2.5. *Send packet into packet classification module*
3. ***End While***

Algorithm 4.1 Algorithm of Alerting Module

The alerting module helps in early and accurate detection of actual condition of a patient. This module further helps during packet classification.

4.2.2 Packet Classification Module

Packet classification [85-87] can be defined as the process of categorizing incoming packets into a particular class which further affects the overall QoS performance of the system. An essential but challenging problem in DWABN is to design an efficient and effectual packet classification approach, as it is dealing with heterogeneous traffic. Basically, the DWBAN consists of multipoint-to-point communication, where the CU device receives different types of packets from different sensor nodes at the same time. Now it is the task of CU to take the decision which packet to forward prior to other, but the decision should be taken in such a way that packets carrying emergency and important data should be delivered in time and with less loss. This requires a proficient packet classification approach, in which emergency and requested packets should not face delay or loss problem. The packet classification can be further defined as the method of sorting out packets according to pre-defined rules. Once a packet is received by CU, the values in its header field are compared against these pre-defined rules. According to the matching rule, proper action will be applied to the packet, as specified in that rule. Packet classification also has a direct impact on differentiated services of WBAN like queuing, routing, scheduling, resource reservation, rate adjusting, load balancing and congestion control. These services need fair and accurate classification and prioritization of packets. Classification of packets considering multi-variant fields is not an easy as it seems.

The actual significance of packets cannot be perfectly characterized by the static prioritization approach, as the status of a sensor node keeps on fluctuating in DWBAN. Therefore a different kind of packet classification approach is designed for dynamic packet classification in DPPH protocol so that a better categorization of the packet can be done. The main action played by the CU is to categorize packets into distinct classes and assign them priorities according to their importance. So the proposed packet classification module is having dynamic classification and packet prioritization approaches which updates with time. The purpose of packet prioritization is to help CU for determining the correct order in which packets will be transmitted towards MSU during a specific time interval. During packet classification, classification is done by comparing the following fields of the incoming packet: packet traffic type, packet size, bandwidth, alert indicator

field and on_Demand indicator field. According to the match rule, the incoming packet can be classified into any one of the following four groups: Real-time packet; Alert packet; On_Demand packet and Normal packet.

- **Real-time packet:** As real-time packets carry delay-sensitive data i.e. audio, video etc., therefore they require bounded service latency or delay. This kind of packets will keep into a queue unless until sufficient amount of bandwidth is not available for their transmission.
- **Alert packet:** Alert packets are generated whenever the sensed value exceeds predefined critical threshold range. It is very clear that the alert traffic is not been generated on the regular basis and therefore it is completely unpredictable. The emergency data carried by an alert packet can be both loss and delay sensitive, so should be delivered within a reasonable time and with no loss.
- **On_Demand packet:**On-Demand packets are considered as the requested packets. These are mainly demanded by the medical person, to get more information about the particular vital node. It mostly demanded at the time of diagnosis and treatment. It can carry both delay and loss sensitive data so must be delivered with less loss and delay bounds.
- **Normal packet:** Normal packets are the packets which actually sensed continuously and transmitted in a regular and continual manner. This kind of packet mostly carries unobtrusive and routine health monitoring data, which is basically loss and delay insensitive data, so normal packet can bear both loss and delay.

Packet classifier

The packet classifier does two very important tasks, first it identifies the class of the packet and second, it sets the priority level of the packet.Then it forwards the packet with the defined priority. The first responsibility of packet classifier is to search and match header fields against the definite conditions. In this process, if the value of the field matched, then the incoming packet is grouped into one of these four classes i.e. Alert, Real-Time, On_Demand and Normal, if the value of fields does not match, then the packet will assign to an unknown class i.e. Null. When classifier identifies the class of the

packet, the second important task done by it is to set the priority field of each packet, so that packets can be stored or retrieved from the queue based on their priority value. Priority of the packet further helps in determining the order of scheduling.

Packet prioritization is a very revealing issue in a WBAN system because there are some packets which carry more important data or information than others. The packet prioritization policy helps in fast servicing of highest priority critical packets. Because of the dynamic nature of WBAN, each data packet from each sensor node can change its degree of importance with time. Therefore to overcome this problem, a dynamic packet classification and prioritization policy is designed here, so that the high priority packet can be delivered and survive with minimum loss and delays. By doing so, the proposed DPPH protocol reduces queuing and transmission delay and increases the packet delivery ratio for emergency packets. Working Principle of packet classification module is mentioned below.

Step 1: Classification of packets

In the proposed packet classification module, some fields of its header part i.e. packet traffic flow type, packet size, allocated bandwidth, alert indicator, on-Demand response indicator fields are taken into consideration for the generation of rule which further helps in the assignment of different priorities to different kinds of packets.

After reception of a packet, the analysis of packet is done by considering a set of five distinct header fields denoted by $Field = \{Field_1, Field_2, Field_3, Field_4, Field_5\}$ of each incoming packet and the classifier considers a set of state having five classes $State = \{Class_1, Class_2, Class_3, Class_4, Class_5\}$, where n=1, 2,…5. Each affixed with a unique priority.

Step 2: Assignment of priority

According to defined class, priority ‘1’ is assigned to an Alert packet, priority ‘2’ is assigned to a Real-Time packet, priority ‘3’ is assigned to an On_Demand packet and priority‘4’ is assigned to a Normal packet. These defined rules are given below.

Class$_1$:IF (Traffic type = Real-Time AND Packet size <=allocated bandwidth), then no priority will assigned to the incoming packet and it will transmitted immediately to the MSU.

Class$_2$:IF ((Traffic type = Non-Real-Time OR Traffic type = Real-Time) AND Alert indicator= 1), then the incoming packet will be assigned with a priority value '1'.

Class$_3$:IF (Traffic type = Real-Time AND Packet size >Allocated bandwidth), then the incoming packet will be assigned with a priority value '2'.

Class$_4$:IF (Traffic type = Non-Real-Time AND On_Demandindicator =1), then the incoming packet will be assigned with a priority value '3'.

Class$_5$:IF ((Traffic type = Non-Real-Time) AND (Alert Indicator!=1) AND (On_Demand Indicator !=1)), then the incoming packet will be assigned with a priority value '4'.

Figure 4.3 explains the flowchart for packet classification module, while Algorithm 4.2 summarizes the working principle of packet classification module.

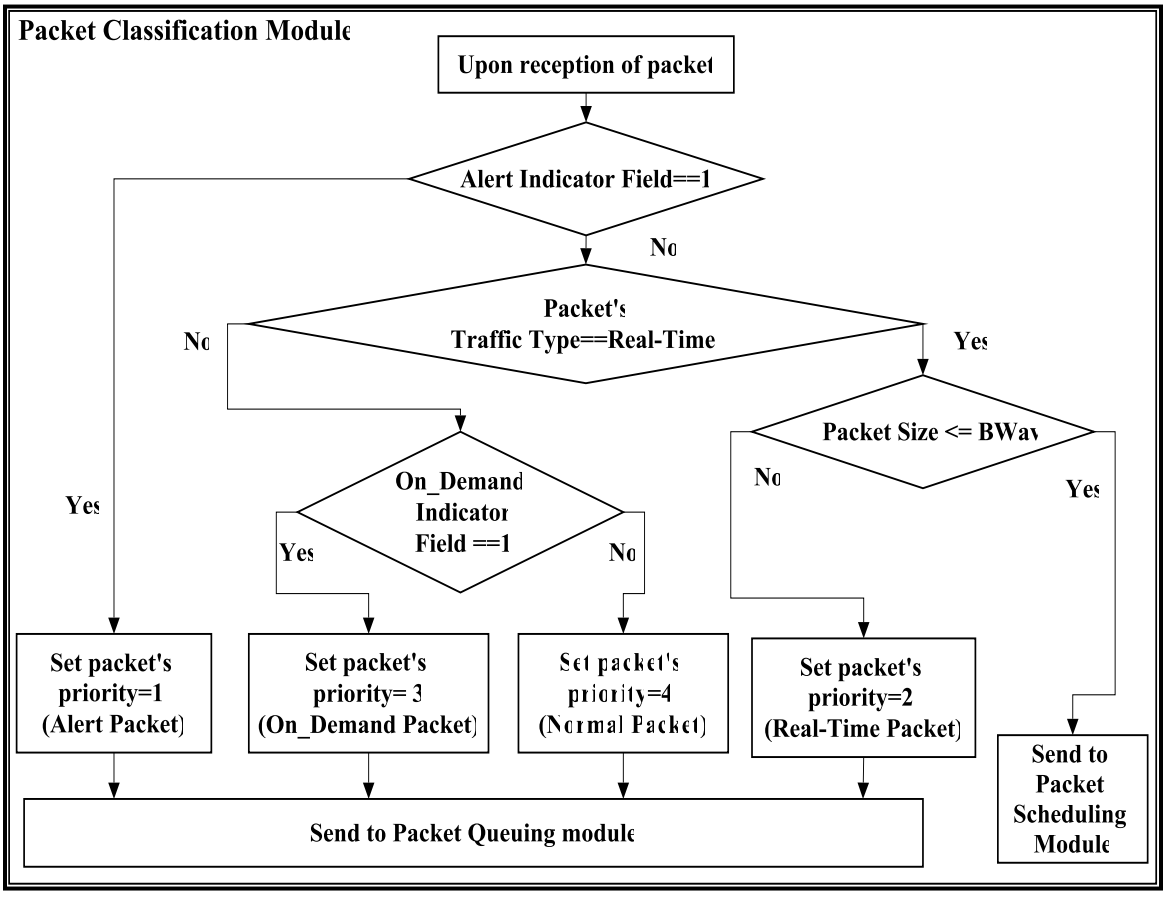

Figure 4.3 Flowchart of Packet Classification Module

Algorithm: Packet Classification Module

Input: *Incoming packet with various fields*
Output: *Assignment of priority to the packet*

1. *Upon reception of packet*
   //Check Alert indicator field
2. ***If*** *(Alert Indicator field = = 1),* ***Then***
   2.1. Assign priority i.e. priority = 1
   //Check packet's traffic type
3. ***Else***
   3.1. ***If*** *(Packet's Traffic type = = Real-Time),* ***Then***
   // Check available bandwidth
   3.1.1. ***If*** *(Packet Size <= BW_{av}),* ***Then***
   3.1.1.1. Assign priority i.e. priority = NULL
   3.1.1.2. Forward the packet towards packet scheduling module
   3.1.2. ***Else***
   3.1.2.1. Assign priority i.e. priority = 2
   3.1.3. ***End If***
   3.2. ***Else*** *//Packet_type is Non-Real-Time*
   3.2.1. ***If*** *(On_Demand field = = 1),* ***Then***
   3.2.1.1. Assign priority i.e. priority = 3
   3.2.2. ***Else***
   3.2.2.1. Assign priority i.e. priority = 4
   3.2.3. ***End If***
   3.3. Send packet into packet queuing module
   3.4. ***End If***
4. ***End If***

Algorithm 4.2: Algorithm for Packet Classification Module

It seems that, the packet classification module is success to achieve fast and accurate categorization of packets. Using dynamic priority assignment it extends the packet handling to support fast updation in the system which helps during queuing and scheduling.

4.2.3 Packet Queuing Module

From a scheduling point of view, the queue is illustrated as a place where packets are stored during service. These packets are waiting in their respective queues unless until appropriate amount of resources are not available or these are fetched out for further processing in the system. There is a high need to design a proficient queuing model for DWBAN, so that it could help in reducing the waiting or queuing delay [88] and starvation problem [81]. Queuing delay can be defined as the total time taken by a packet in a queue during waiting for its turn to schedule. Packets are stored temporarily in queues during the transmission or scheduling of other packets. An efficient packet queuing mechanism can reduce the effects of packet queuing delay and starvation in WBAN.

It is experienced that some of the existing protocols had adopted single queuing mechanism, where different types of packets can share the single place for their storing purpose. While single queuing mechanism had a problem of high starvation rate. Another study says that some authors had used the virtual queuing mechanism [71,75], where a single physical queue is divided into multiple numbers of virtual queues, and each virtual queue was assigned a particular weight so that each virtual queue gets a chance for scheduling and servicing. They had followed the concept of weighted fair queuing (WFQ) [68,71] where the physical queue is divided into different sub-queues according to the number of different traffic flows. The WFQ policy handles the starvation problem up to some extent but faces switching problem. The scheduler needs to switch in between these sub-queues for scheduling which is a very tedious process. In order to avoid such time-consuming task, some researchers have used multiple numbers of queues, where the number of queues at each node depends on the number of traffic flow present in the network. Here packets are stored into different queues according to their traffic flow type. The maximum utilization of memory is not done in this type of queuing, as with the number of traffic flow type the number of queues can be increased. If the packet arrival rate is not high for each flow, then most of the places in the queue keep remaining unused. Another problem with this type of queuing is switching problem.

The proposed packet queuing scheme considers only two Double Ended Priority Queues (High priority DEPQ (HP_DEPQ) and Low priority DEPQ (LP_DEPQ)). The packets are kept into these DEPQs according to their calculated priority value. It is implemented with a mechanism to store and schedule higher priority packets previous to lower priority packets. It also helps during congestion and drops low priority packets only. In addition to this, LP_DEPQ available space can be used by high priority packets if required. This proposal helps in reducing the waiting or queuing delay and starvation problem in the system. Working principle of packet queuing module is given as follows.

Step 1: Priority checking

Upon reception of a packet from the packet classification module, the priority of the packet is checked, and enqueue it into either HP_DEPQ or LP_DEPQ according to its priority.

Step 2: Enqueue of packet

- If the incoming packet is having priority either 1 or 2, then it will be inserted into HP_DEPQ. If the HP_DEPQ is full, then it fetches low priority packet from this queue and checks its priority against the incoming packet. If the priority of the incoming packet is less than the fetched packet, then it enqueues the incoming packet into LP_DEPQ, otherwise, it enqueues the fetched packet into LP_DEPQ and the incoming packet into the place of the fetched packet in the HP_DEPQ.

- If the incoming packet is having priority either 3 or 4, then this module checks whether the LP_DEPQ if full or not. If this is full, then it fetches a low priority packet from this queue and check its priority against the incoming packet, if the priority of the incoming packet is less than the fetch packet, then it drops the incoming packet, otherwise it drops the fetched packet and enqueue the incoming packet into the place of the fetched packet in LP_DEPQ. If the priority of the incoming packet is same as the fetch packet then it will apply the above rule for the sequence number of both the packets.

The flowchart of the proposed packet handling module is presented in Figure 4.4. The algorithm for this module is explained in Algorithm 4.3.

Figure 4.4 Flowchart of Packet Queuing Module

Algorithm: Packet Queuing Module

Input: *Packet with priority value*
Output: *Enqueue packet into appropriate queue*

1. *Upon reception of a packet*
   // Check the priority of the incoming packet
2. ***If*** *(priority = =1* ***OR*** *priority = =2),* ***Then***
   // check high-priority queue
   2.1. ***If*** *(HP_DEPQ != Full),* ***Then***
      2.1.1. Enqueue the incoming packet into HP_DEPQ
   2.2. ***Else***
      2.2.1. Fetch low priority and low sequence numbered packet from HP_DEPQ
      2.2.2. ***If*** *(priority of incoming packet > priority of fetched packet),* ***Then***
         2.2.2.1. Delete the fetched packet from HP_DEPQ
         2.2.2.2. Enqueue this fetched packet into LP_DEPQ
         2.2.2.3. Enqueue incoming packet into HP_DEPQ
      2.2.3. ***Else***
         2.2.3.1. Enqueue the incoming packet into LP_DEPQ
      2.2.4. ***End If***
   2.3. ***End If***
3. ***Else If*** *(priority = =3* ***OR*** *priority = =4)*
   // check low-priority queue
   3.1. ***If*** *(LP_DEPQ != Full),* ***Then***
      3.1.1. Enqueue the incoming packet into LP_DEPQ
   3.2. ***Else***
      3.2.1. Fetch Low priority and low sequence no packet from LP_DEPQ
      3.2.2. ***If*** *(priority of incoming packet > priority of fetched packet),* ***Then***
         3.2.2.1. Delete fetched packet from LP_DEPQ
         3.2.2.2. Drop the fetched packet
         3.2.2.3. Enqueue incoming packet into LP_DEPQ
      3.2.3. ***Else***
         3.2.3.1. Drop the incoming packet
      3.2.4. ***End If***
   3.3. ***End If***
4. ***End If***

Algorithm 4.3 Algorithm of Packet Queuing Module

Basically, the queuing module is implemented with a dynamic reservation of buffer concept, where, when some portion of buffer of a low priority queue is not being in used; this unused buffer can be used by high priority packets or when space get deficient in high priority queue, buffers from the low priority queue are used by high priority queue.In addition, it leads to drop only low priority packets from the low priority queue in case of excessive data or queue overflow. It's fair resource sharing helps to allocate a fair share of buffer among both queues. The use of two DEPQs further helps in storing a packet in an orderly manner and helps to fetch packet from both ends during packet servicing and packet dropping. It also solves the problem of queuing delay which exists in the singular queue and switching delay which exists in multiple queues.

4.2.4 Packet Scheduling Module

Packet scheduling [90] is providing one of the most important processing in a network, as it deals with fair resource sharing and offers high packet service or delivery rates. Generally, packet scheduling implements a practice of making a decision either regarding packet servicing or packet dropping. Packet servicing can be defined as one of the methods of choosing and transmitting packets. Packet servicing policy can select a packet for transmission based on various factors of the packet such as flow type, priority of the packet, deadline etc. In some situations, scheduler may take a decision regarding dropping of selected packets. Dropping of a packet will depend on some of the traits of the packet such as packet size, bandwidth, packet arrival rate, deadline of the packet, waiting time of the packet, redundancy factor of the packet etc.

According to the research, a high-quality packet scheduling mechanism [93] can help in improving transmission rate and reducing transmission delays in WBAN. Results of literature survey say that various protocols [81,89] emphasize their work on priority based packet scheduling mechanisms, where they have focused on fair bandwidth sharing and weighted fair queuing based scheduling. But these algorithms follow a fixed priority scheduling policy, where it is observed that the entire system continues with a fixed priority which will not change during the complete execution of the system. On the other side, this kind of priority scheduling causes other difficulties like high drop rate, starvation, delay, and switching problem in the system. On the other hand, conventional

EDF [91] which is a kind of dynamic scheduling algorithm, generally used in real time systems for scheduling processes. EDF helps the system in those situations, where a large number of packets are present in the scheduler queue and each packet has a precise deadline, within which it must be served. In these situations, the job of the EDF scheduler is to check for the packet with the close deadline and served the packet accordingly.

WBAN needs to be scheduled intelligently all the incoming packets so that every packet can be transferred to the MSU earlier to its deadline. Therefore, in the packet scheduling module, a new approach, named Ratio based Earliest Deadline First (REDF) packet scheduling is proposed. The proposed approach pays attention towards dynamic priority and earliest deadline based packet servicing facet. REDF is also responsible to schedule more amounts of high priority packets and also allows packets to deliver within their deadline. If the deadline of a particular packet perishes, then that packet can be dropped according to its priority. In the proposed REDF scheduling, the priority based ratio control mechanism overcomes both queue-level starvation and queuing delay problem, while the EDF [92] with a predetermined deadline assists the scheduler to remove the packet-level starvation problem. So, the proposed scheduling module works very effectively to enhance QoS in terms of high packet delivery rate. Working of packet scheduling module is explained as follows:

Step 1: Calculation of Packet's waiting time

Here each sensor node is assigned with a pre-estimated (PE^d) deadline value, which was calculated during the connection establishment phase. It provides the information about the expected waiting time of a packet at the CU. Packets of different sensor nodes have different deadline values.

- The waiting time of a packet is defined as the time difference between current time and packet arrival time.
- The scheduler uses a set named as waiting time set (W) to keep the waiting time of each fetched packet.

Step 2: Ratio based scheduling

For a particular time period, the scheduler fetches and serves high priority packets from both queues.

- It first fetches 30% of high priority packets from the high priority queue and sends them to scheduler queue for service.
- It then fetches 10% of high priority packets from the low priority queue and sends them to the scheduler queue for service.
- The scheduler will continue this task unless deadline_watch timer will not get expire.

The selection of 30% and 10% during percentile of rate calculation is found in *Appendix B*.

Step 3: EDF based scheduling

Upon expiration of deadline_watch timer, the scheduler fetches and serves low priority packets from both queues.

- It fetches 30% of low priority packets from the high priority queue and findstheir Earliest Deadline Ratio (EDR). If EDR of a packet is less than the pre-set deadline threshold value, then it sends them into scheduler queue (i.e. ready queue or service queue), otherwise it is enqueued into the low priority queue.
- Then it fetches 10% of low priority packets from the low priority queue and findstheir EDR. If EDR of a packet is less than the pre-set deadline threshold value, then sends them into scheduler queue, otherwise, the packet is driven out from the low priority queue and gets dropped.

Procedure to calculate Earliest Deadline Ratio (EDR) is given below.

- In the initial phase, waiting time set is having no packets, i.e.

  $$W = \emptyset \tag{4.6}$$

  where W is the waiting time set which stores the waiting time of packets.
- The waiting time of a packet is calculated from equation (4.7).

  $$W_{i,j} = CR_{i,j} - AR_{i,j} \tag{4.7}$$

  where $CR_{i,j}$, $AR_{i,j}$ and $W_{i,j}$ denote the current time, arrival time and waiting time of a packet j belongs to sensor node i.

- The scheduler stores $W_{i,j}$into waiting set using the formula given in (4.8).

  $$W = W \cup W_{i,j} \tag{4.8}$$

  where $W_{i,j}$ denotes waiting time of a packet j belongs to sensor node i.

- Now the scheduler sorts the waiting set according to descending order of waiting time.

  $$W = Sort\{W \mid W_{i,j} > W_{i,j+1}\} \tag{4.9}$$

  where $W_{i,j+1}$ and $W_{i,j}$ denote the waiting time of a packet j and j+1 belongs to sensor node i.

- Scheduler fetches maximum value from W.

  $$W^{max} = Max(W) \tag{4.10}$$

  and

  $$W = W \cap W^{max} \tag{4.11}$$

  where W^{max} denotes the maximum waiting time.

- Scheduler calculates the Earliest Deadline Ratio using equation (4.12).

  $$EDR^d = W^{max}/PE^d \tag{4.12}$$

  where PE^d is the pre-estimated deadline, EDR^d denotes the earliest deadline ratio, W^{max} is the maximum waiting time.

- The packet was discarded by the scheduler, if its EDR is exceeded the pre-estimated deadline threshold value ($EDR^d > Th_{d,}$), otherwise it was forwarded to the scheduler queue for servicing.

  $$f(Pij) = \begin{cases} forward\ packet, & if EDR^d \le Th_d \\ Drop\ packet, & otherwise \end{cases} \tag{4.13}$$

  where EDR^d denotes the earliest deadline ratio, Th_d denotes the pre-estimated deadline threshold value, and $P_{i,j}$ denotes the packet j belongs to sensor node i.

The EDR provides fairness in resource utilization. It tries its best to save high priority packets and drops only low priority packets whose deadline expired. It is capable to handle both high and low priority packets and queue-level starvation, and successful to reducing the waiting time of packets.

The flowchart diagram of the REDF based packet scheduling module is specified in Figure 4.5, and the Algorithm 4.4 describes the complete working of this module.

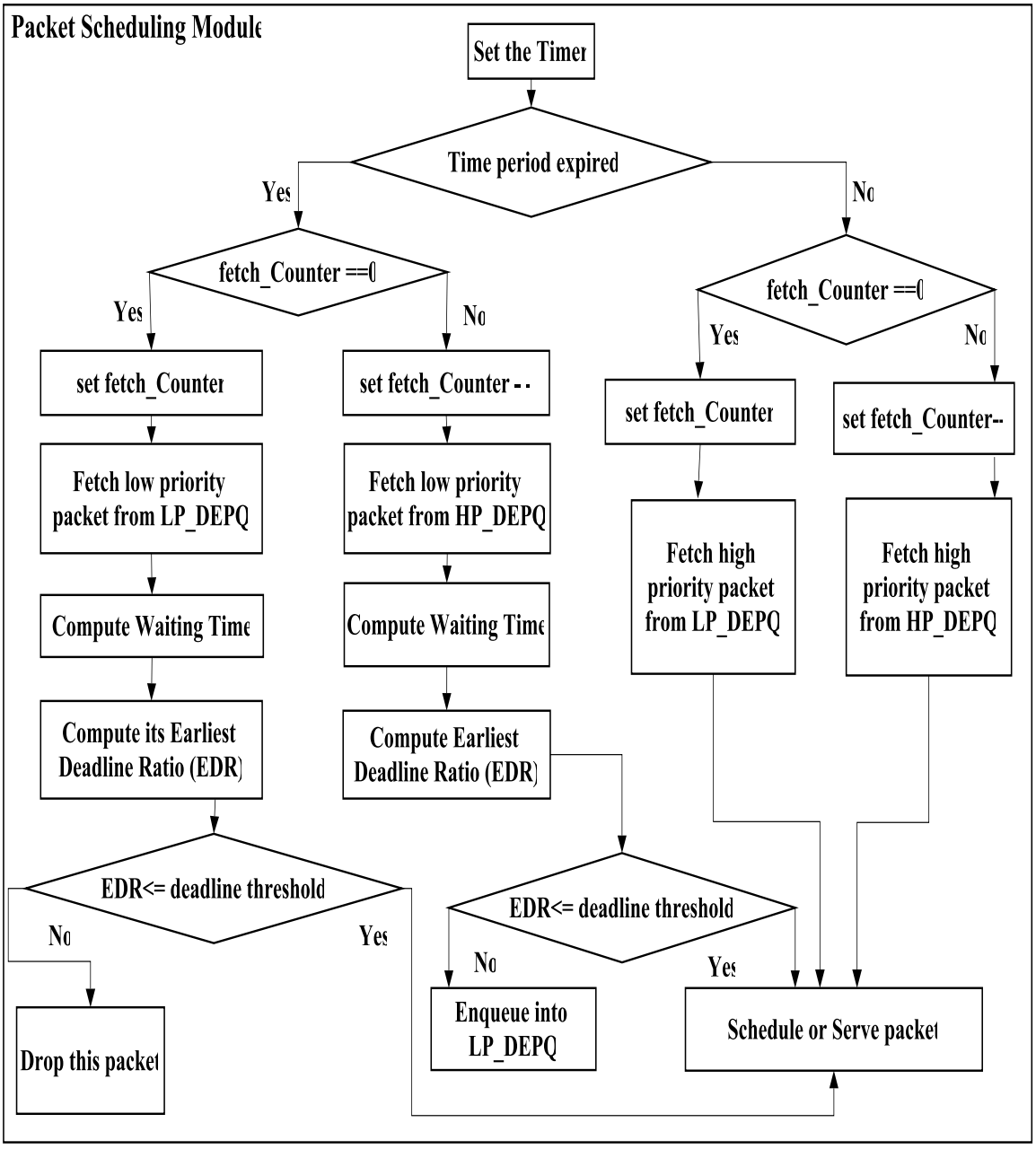

Figure 4.5 Flowchart of Packet Scheduling Module

Algorithm: Packet Scheduling Module

Input: *DEPQs, Deadline threshold value*
Output: *Schedule or serve packets from both HP_DEPQ and LP_DEPQ*

1. *Initialize and Set Timer (Deadline_watch timer)*
   - *1.1. Set count1 = 30 % of HP_DEPQ queue occupancy // Calculate Ratio*
   - *1.2. Set count2 = 10 % of LP_DEPQ queue occupancy // Calculate Ratio*
2. ***While*** *(Timer not expired),* ***Do*** *// fetch high priority packets from both DEPQs*
   - *2.1. Set fetch_Counter = count1*
   - *2.2.* ***While*** *(fetch_Counter! = 0),* ***Do***
     - *2.2.1. Fetch and Delete high-priority packet from HP_DEPQ and Serve it*
     - *2.2.2. Set fetch_Counter--*
   - *2.3.* ***End While***
   - *2.4. Set fetch_Counter = count2*
   - *2.5.* ***While*** *(fetch_Counter! = 0)*
     - *2.5.1. Fetch and Delete high-priority packet from LP_DEPQ and Serve it*
     - *2.5.2. Set fetch_Counter--*
   - *2.6.* ***End While***
3. ***End While***

// Fetch low priority packet from both DEPQs when timer expired

4. *Set fetch_Counter = count1*
5. ***While****(fetch_Counter!= 0),* ***Do***
   - *5.1. Fetch and Delete low-priority packet from HP_DEPQ*
   - *5.2. Compute wait-time and Calculate EDR using* ***Equations (4.6)*** *to* ***(4.12)***
     - *5.2.1.* ***If*** *(EDR <= Th_d),* ***Then***
       - *5.2.1.1. Serve or Forward packet*
     - *5.2.2.* ***Else***
       - ***5.2.2.1.*** *Delete this packet from HP_DEPQ and Enqueue into LP_DEPQ*
     - *5.2.3.* ***End If***
   - *5.3. Set fetch_Counter--*
6. ***End While***
7. *Set fetch_Counter = count2*
8. ***While*** *(fetch_Counter! = 0),* ***Do***
   - *8.1. Fetch and Delete low-priority packet from LP_DEPQ*
   - *8.2. Compute wait-time and Calculate EDR using* ***Equations (4.6)*** *to* ***(4.12)***
     - *8.2.1.* ***If*** *(EDR < =Th_d),* ***Then***
       - *8.2.1.1. Serve or Forward packet*
     - *8.2.2.* ***Else***
       - *8.2.2.1. Delete the packet from LP_DEPQ and drop it*
     - *8.2.3.* ***End If***
   - *8.3. Set fetch_Counter--*
9. ***End while***

Algorithm 4.4 Algorithm for Packet Scheduling Module

The REDF scheduling algorithm fairly schedules both low and high priority packets and drops only low priority deadline expire packets. It helps in reducing drop probability of important or emergency data. This algorithm also utilizes resources such as buffer and bandwidth for high priority packets, which carrying important data. It also reduces both queue-level and packet-level starvation from the system, which further lessens switching delay and packet dropping rate. Therefore in a provision to packet waiting and transmission delay, the REDF scheduling algorithm is considered as an efficient and optimal module.

4.2.5 Prioritization Module

Prioritization policy [94-95] can enhance the performance of a network. Due to this significant network parameters get more importance over than insignificant network parameters. In a healthcare WBAN, some interesting queries arise, such as which parameters should be prioritized? Who is responsible to set priorities? What are the causes to change the priority? etc.

Classification and prioritization of different types of packets are the important factor for reducing packet loss, starvation, transmission and queuing delay in a network. But at the same time, classification and prioritization [96-97] of sensor nodes are also essential requirement in WBAN in order to increase the resource utilization. On one side, automatic assignment of the priorities to the sensor node may reduce time in term of human intervention, but on the other side, rely on a device may become more tedious for accurate treatment, as it has no brain and works according to the instructions and inputs. As a healthcare WBAN system deals with life-threatening situations where a patient's condition can fluctuate at any moment of time. For this kind of system, accuracy is the main concern to have an accurate diagnosis.

The proposed prioritization module is able to updates priorities of all sensor nodes dynamically based on the current network status and requirements. After receiving a control packet from the MSU, the CU first checks its prioritization field value (i.e. active or inactive) and according to this value the actual status of the sensor node can be

recognized by the CU. If it is in active mode, then in response to this the priority as well as other parameters like Sensor node's priority, Vital ranges of sensor node, critical threshold value, sensor activation duration, monitoring time etc. will be reset by the CU after consulting the concern medical person and sends this control packet to the sensor node.

CU then checks another field named on_Demand request field which informs the CU about the request regarding additional information of a patient during a particular time interval. If it is in active mode, then the CU look for these requested packets in its local database and if found, then send them to the MSU. Otherwise it sends this control packet to the sensor node. Working principle of prioritization module is given below.

Step 1:When the Prioritization field is in active state

When a control packet is received by the CU, it first checks its prioritization field. If the prioritization field is having a value '1' or 'on', then CU updates its database with the new values provided in this control packet about each sensor node. CU then broadcasts same control packet to all sensor nodes.

Step 2: When the On_Demand request field is in active state

When a control packet is received by the CU, it checks the On_Demand request field of the control packet; if it is '1' or 'on', then CU searches these demand or requested packets in its local database, if these are found in its own database, then CU immediately sends them to MSU; otherwise, it sends this control packet to the particular sensor node.

Step 3: When the On_Demand indicator field is in active state

- Upon reception of the control packet, a sensor node checks this control packet's prioritization field first. If this field is in 'on' mode or '1', then it updates its own local database. Otherwise, it checks the On_Demand request field in the control packet; if it is in 'on' mode or '1', then sensor node fetches or sense these packets, activates the On_Demand indicator field in the header part of the sensed packet and sends it towards the CU.

- After the reception of an incoming packet, CU checks the On_Demand respond indicator field and assigns it with a priority index, and then forwards to the MSU for further processing.

The prioritization module is mainly concern about two things: dynamic updating of pre-set values and accomplishment of requested packets. Basically, the proposed prioritization module is worked in collaboration with the MSU. Figure 4.6 provides the flowchart diagram for the proposed prioritization module, while Algorithm 4.5 briefs the idea about its working.

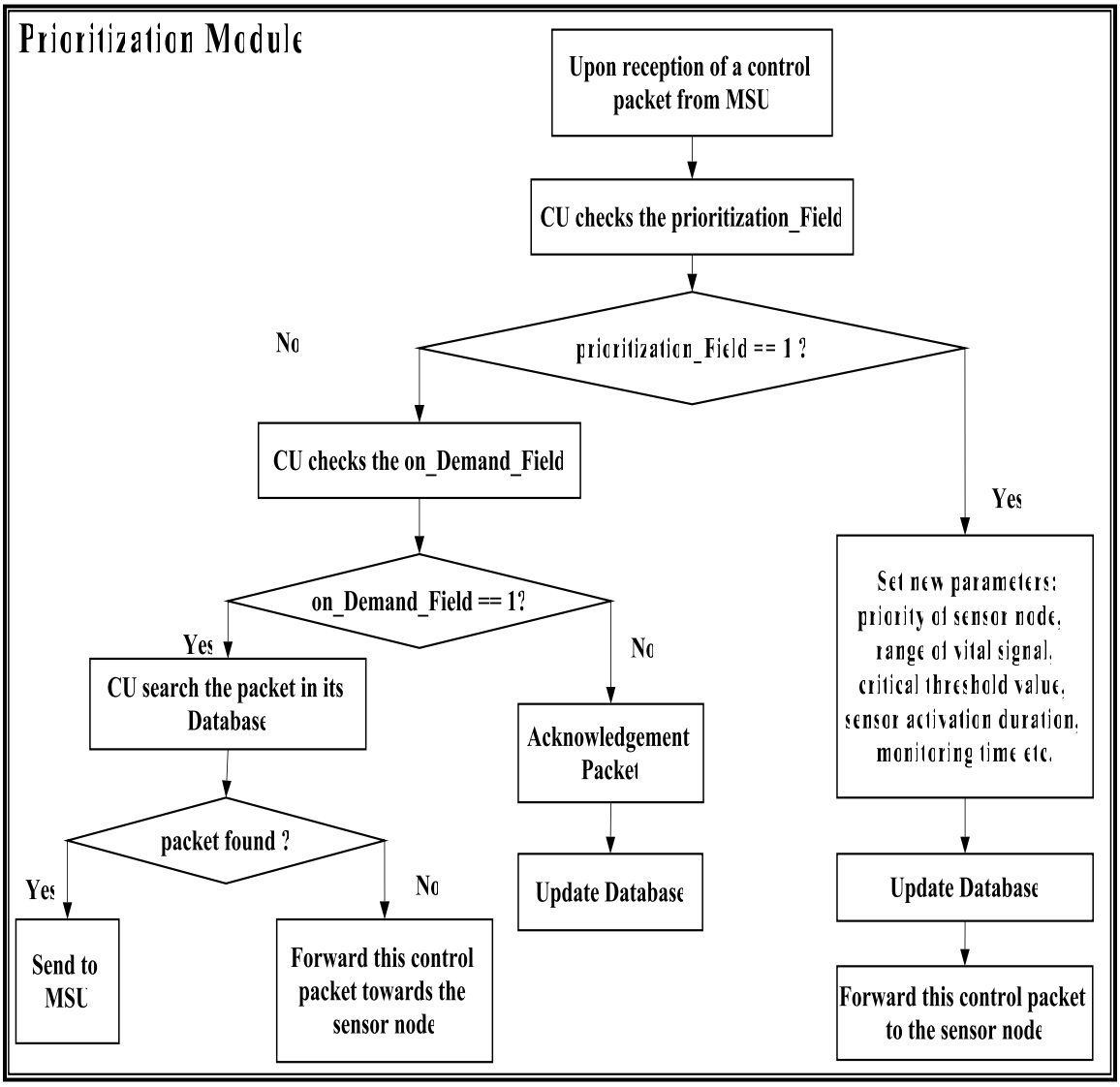

Figure 4.6 Flowchart Diagram of Prioritization Module

Algorithm: Prioritization Module

Input: *Control packet*
Output: *Reset parameters*

1. *Upon reception of control packet at CU*
   // Check prioritization field of control packet
2. ***If*** *(prioritization field = = 1),* ***Then***
   2.1. CU resets defined parameters and updates its database
   2.2. CU sends this control packet to the sensor node
   2.3. The sensor node updates it database and priority
3. ***Else If*** *(On_Demand request field = = 1),* ***Then***
   3.1. CU search the requested packets in its database
   3.2. ***If*** *(requested packets are found in its database),* ***Then***
      3.2.1. CU sends them to MSU
   3.3. ***Else***
      3.3.1. CU sends this control packet towards the sensor node
   3.4. ***End If***
4. ***End If***

Algorithm 4.5 Algorithm for Prioritization Module

The proposed prioritization module helps in updating the essential parameters related to a vital signal which further helps in accurate diagnosis of the patient's health status and in decision making by the concerned medical person.

4.3 SUMMARY

In this chapter, Dynamic Priority based Packet Handling (DPPH) protocol is proposed for WBAN. The proposed DPPH protocol is able to timely recognize the critical condition of a patient and also get notified the same through alerts to the medical person. This protocol focuses on developing a smart packet handling module for the improvement of QoS performance in the WBAN with its new and extended solutions. DPPH protocol helps in identification and organization of heterogeneous traffic in an aggressive environment of a healthcare system. It classifies all sensor nodes as well as packets and

assigns them a unique priority. This priority can be changed over the period of time according to the patient's condition. The switching and queuing delay problems are handled through its packet queuing module. Its REDF scheduling module helps in mitigating starvation, drop and delay related problems. It also resolves the false alerting problem in healthcare WBAN system. Apart from alert management, the information provided by this system is used to track the actual condition of a patient during the treatment.

CHAPTER 5

MDPPH: DESIGN OF A MODIFIED DPPH PROTOCOL FOR QOS MANAGEMENT IN DWBAN

5.1 INTRODUCTION

As it is known to all that, the entire performance of any network is been reckoning by a nucleus measurement termed Quality of Service (QoS). Therefore, different kinds of protocols have been designed in WBAN, but after all the amendments and improvisations, still, QoS issue didn't get a large amount of attention in WBANs like other issues actually till date. So there is a need to add some new creative and innovative ideas to provide assumptive QoS in WBAN applications. The study says that it is very difficult to manage proper QoS in time-critical WBANs like healthcare system because it deals with real-time and critical data. For eminence QoS measurement, various aspects of network metrics and services should be considered in a WBAN. Further, it is been observed that there are few researchers who actually had tried to improvise the QoS factors in various WBAN applications with their signifying conduct of work. But at the same time, QoS factors majorly relating to dynamic changes in healthcare WBAN still remains immaterial because of the limitations of WBAN, as a dynamic WBAN (DWBAN) needs assorted functionalities which are very sensitive by nature, hence it keenly demands more attention. QoS in DWBAN concerns with very serious factors like timely delivery of the packet, data accuracy, data availability, data loss, bandwidth utilization, throughput, and delay.

There are number of layers to count high performance in QoS in WBAN, which can be chosen with various issues and design of conducts for improvised QoS. The study says that most of the current researches focus only on MAC and Network layer QoS related problems, whereas there is a high need to develop a protocol actually can accord with QoS performance at transport layer along with lower layers to deal with packet reliability,

congestion, and delay. No transport layer protocol is designed till date for any kind of WBAN applications. But there are some researchers [75, 78, 80] who have conducted their work in the direction of healthcare Wireless Sensor Network to resolve congestion, reliability, routing, and energy-related problems. But so far their work have not concerned with on-time recovery of packet loss, and therefore face retransmission overhead problems which further hamper system reliability. It is seen that most of the approaches had used duplicate ACK/NACK based loss notification which again raises delay and congestion in the network due to control packet implosion problems. Further, from the analysis, it is found that no one had a concern about the duplicate packet transmission problem and due to this network resources get underutilized.

In particular, the above-mentioned factors which are affecting the performance of QoS are considered as main design issues for DWBAN. Therefore, the proposed QoS management protocol is designed for the transport layer of DWBAN, and is implemented with paying special attention in the way to handle congestion and reliability problems, while focusing packet loss, delay and resources as the main area of concern. In addition to this, it works out on packet retransmission and packet redundancy related characteristics, as these are the most unpleasant harms for these kinds of network.

5.2 QOS-AWARE MDPPH PROTOCOL

Two essential factors, packet loss, and delays which are provoked with congestion and reliability, deeply influence the effectiveness of QoS in DWBAN. But, it is different to resolve these issues due to the heterogeneous and dynamic nature of DWBAN. With such kind of obstacle, no dynamic QoS protocol has been proposed for healthcare WBAN system till date. A new and outstretched protocol named as Modified DPPH (MDPPH) protocol is been designed with these challenging limitations so that QoS issues can be managed in a better and improvised way in DWBAN. It is an extension to the previously specified DPPH protocol, designed to tackle QoS related issues in frequently changing atmosphere of healthcare WBAN. The primary goal of MDPPH protocol is to find out the ways by which congestion in the network could be avoided. It also deals with unnecessary transmission of the duplicate packet and retransmission overhead problems.

With the aforesaid observations, the proposed MDPPH protocol is designed with two modules; Congestion Module and Reliability Module to achieve its effectual objectives. Figure 5.1 illustrates the whole working principle of the MDPPH protocol.

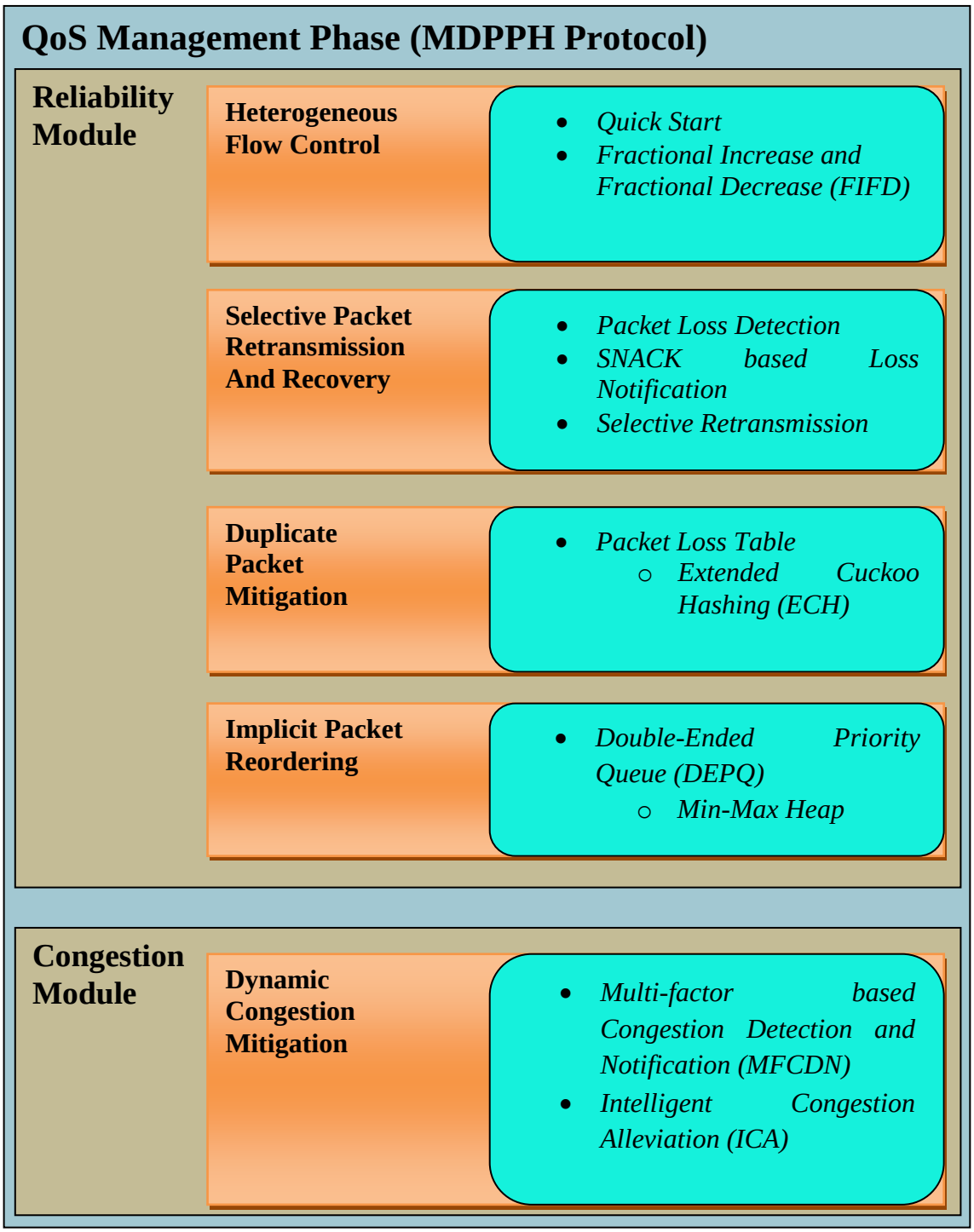

Figure 5.1 Modular Architecture of MDPPH protocol

5.2.1 Reliability Module

The reliability module deals with a foremost key aspect towards the sure short delivery of data in reasonable time [99-100]. The dynamic applications such as healthcare WBAN require that the important packets should reach to the concern medical person on correct time and without any loss, as the reliability of the healthcare system affects directly to the quality life of a patient and also become fatal when a life-threatening condition is not been detected within the specified time bound. Since reliability metric is often considered as reciprocal to packet loss rate varying over time. Hence, the success ratio of packet delivery imitates the level of reliability achieved by the network.

It is very important to fulfill the needs of ensuring data reliability within heterogeneous WBAN. Keeping in this observation, an entirely new approach is introduced. It is developed with a dynamic priority based reliability policy for time-critical healthcare systems so that the diagnosis and medication of the patient can be carried out on time.

The job of the reliability module in MDPPH protocol is to ensure the successful delivery of packets from the sensor node to the CU within the precise time interval to achieve guaranteed and timely delivery of packets. The concerned is about delivery of high priority packets, which are directly associated with patient's life. As a result, it offers splendid assistance during the critical health status diagnosis, and also handles the situation when actual conditions are unnoticed. At the same time, another purpose of this module is to get rid of packet retransmission overhead and redundant packet problems. In particular, it offers all these magnificent benefits with the help of its magnifying approaches: heterogeneous flow control; selective lost packet retransmission and recovery; duplicate or redundant packet mitigation and implicit packet re-ordering approaches. The work flow diagram of reliability module is given in Figure 5.2.

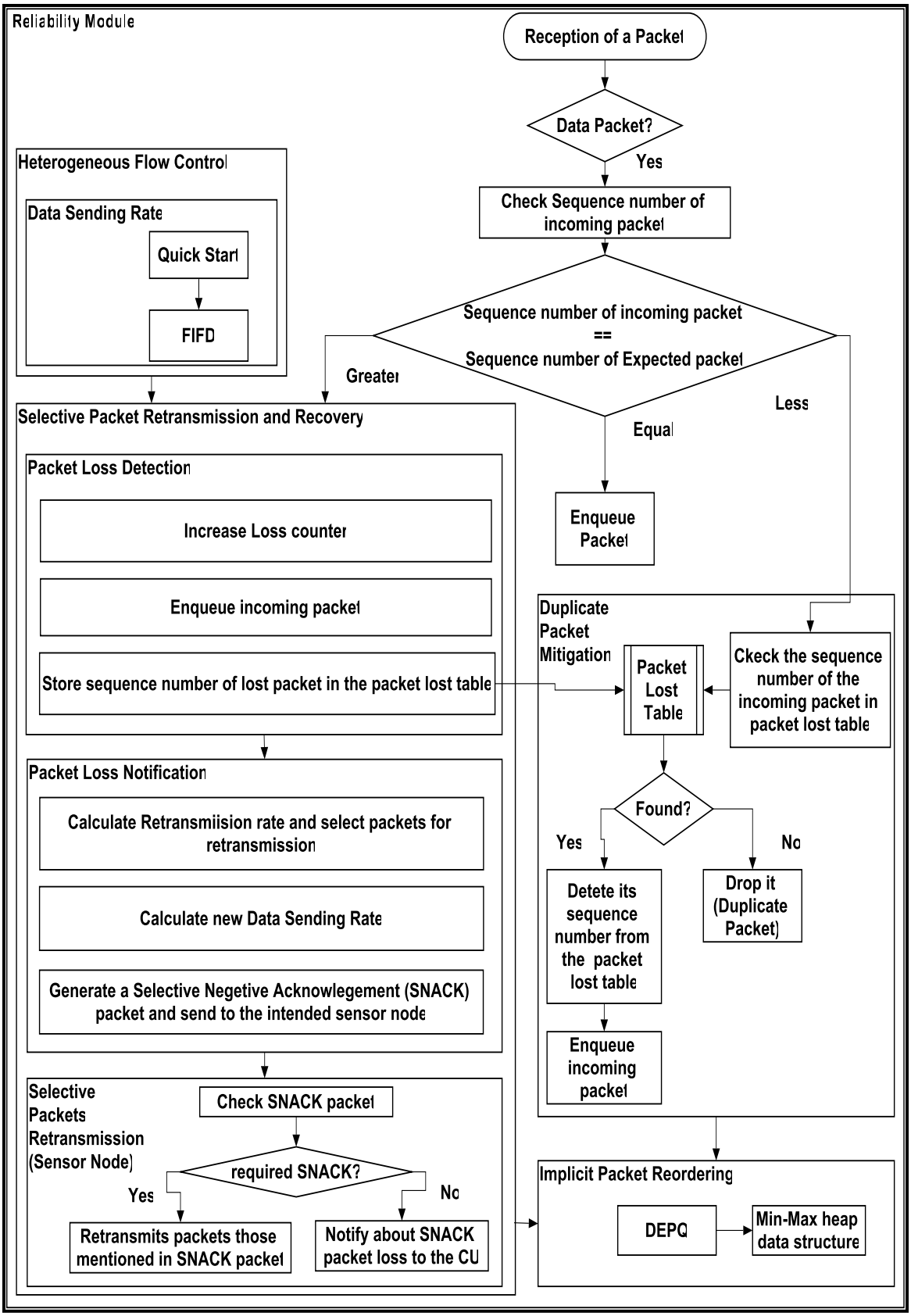

Figure 5.2 Workflow Diagram of Reliability Module

I. Heterogeneous Flow Control

The flow control [100] is considered as a more complex issue at the transport layer than at lower levels like the data link layer, as it became the real cause of transmission as well as queuing delay amongst all networks. A high or bursty flow rate can be a reason for the high loss, as queue fills up very quickly and further due to overflow it continuously drop data unless the rate of incoming data flow is been controlled properly. On the other hand, a low-rate flow control makes both bandwidth and buffer under-utilized or remain ideal. Such kind of problems can vary time to time and also remained for a longer span, so to overcome these kind of flow control issues a better approach is been required.

Heterogeneous flow control is the mechanism of controlling assorted traffic in between sensor node and the CU. By doing this, it prevents the CU from being overloaded at the time of bursty data transmission from all the sensor nodes.

In other words, flow control plays an important role in preventing the sensor node to overrunning the buffer of CU by deliberating the appropriate data sending rate to each sensor node. As it is observed that sensor nodes and the CU are often unrivaled in potentials and processing abilities, so the proposed heterogeneous flow control approach acts as an essential and useful component to get rid-off this instability. It is clear that the main target of the flow control mechanism is to prevent packets loss rate as well as retransmission rate, which actually is the need of DWBAN.

The proposed heterogeneous flow control approach is designed with *Quick Start* and *Fractional Increase and Fractional Decrease (FIFD)* strategies. Both Quick Start and FIFD asymptotically converge to the efficient and fair data sending rate adjustment during flow and congestion control, where quick start approach attains resource utilization and FIFD attains the congestion mitigation.

A. Quick Start

Different studies and analyses elaborate that, various existing protocols follow slow start approach [101] which starts their packet transmission with a small rate during the beginning phase as well as congestion control phase. In addition, to attain the intended target, the slow start phase increases its rate gradually one packet per round trip time with

every time interval, unless and until the data rate exceeding the slow start threshold value. This principle is characterized by the Additive Increase schema of Additive Increase Multiplicative Decrease (AIMD) [102-103] approach. The rate gets deceased during its Multiplicative Decrease phase when high congestion detected in the network. The limitation with this approach is that, in order to acquire the high throughput, it needs to wait longer during data transmission, which will increase the delay. On the other side bandwidth idealization crucially degrades throughput in the system.

In contrast to the slow start, a quick start based Data Sending Rate (DSR) strategy is proposed in this flow control approach to calculate and utilize the resources according to the requirement of sensor nodes with time. It begins its data transmission with a high sending rate. Though it is been observed that different kinds of sensor nodes deal with different kinds of services, therefore, it provides a variation in data sending or flow rate for each sensor node instead of the equal data rate.

The important thing about quick start is its maximum utilization of bandwidth capability. By determining flow rate dynamically, it can further help in reducing the packet loss and the retransmission rate. Quick Start can also contribute in minimizing the packet transmission time. Due to all these benefits, it can be considered as an important factor for controlling both flow and congestion in healthcare WBAN.

B. Fractional Increase and Fractional Decrease (FIFD)

Many authors used AIMD algorithm based rate adjustment policy during the congestion in order to handle the problem of packet drops. The AIMD algorithm is majorly known as the feedback control algorithm, which pursues a linear escalation and an exponential decline concept during congestion in the network. This technique helps in stabilizing the traffic flow, but at the same time, its attitude towards network resources is very wicked. It means AIMD follows the identical process to slow start i.e. a sender increases its rate by a regular amount (i.e. one or two packets) per round trip time or per response and decreases its rate by a fraction (i.e. half) of its current rate when congestion is happened in the network.

The heterogeneous flow control approach is employed with a new kind of rate increment and decrement principle called Fractional Increase and Fractional Decrease (FIFD) principle. According to the FIFD mechanism, the sending rate of a sensor node will increase with a particular fraction of amount during normal a scenario, while the rate will get decrease with a fraction amount when congestion occurs in the system. The expert methodology of FIFD is used to cope-up with the congestion phenomenon in a dynamic environment with its rate adjustment policy. The basic idea of this algorithm is to adjust the data sending rate of each sensor node after considering two main factors: previous DSR value and current priority of the sensor node.

Since the WBAN system is heterogeneous by its nature, FIFD attempts to control the data sending or flow rate dynamically by using a priority based increment or decrement in the flow rate. By doing so, it bequeaths with a fair resource allocation and managing process, as some sensor nodes might require more resources than others. This further satisfies the needs of both heterogeneous and dynamic environment of DWBAN efficiently. Working principle of Flow Control approach is explained below.

Step 1: Calculation of DSR

After connection set-up phase, the CU follows the quick start approach, which determines the DSR for each sensor node (i.e. how many numbers of packets a sensor node can send soon after its startup phase). Here the DSR directly depends on the priority of individual sensor node, though this value is not fixed, DSR can be updated time-to-time according to the system need. Actually, Quick start begins with a large value rather than with a single packet.

Step 2: Intitial DSR value calculation using Quick Start approach

The next step is related to notification of DSR, in which the CU and sends calculated DSR to the sensor node through control packet. The initial Data Sending Rate (DSR_0) is calculated using the formula given in equation (5.1) for a particular time period and is different for different sensor nodes.

$$DSR_0^{S_n} = 2^{N-n} \quad (5.1)$$

where n is the priority of the sensor node S_n and N denote the total number of priority values.

Step 3: Calculation of DSR value for next round applying FIFD approach

As the DSR of a sensor node is directly depends on its priority and the priority of a sensor node changes with time, the congestion notification (CN) value in the network is been checked by the CU for a particular time interval. According to this CN value, the new DSR_i is calculated for each sensor node by applying the FIFD policy as given in equation (5.2).This calculated new DSR added into the control packet and sends towards the intended sensor nodes by the CU.

$$DSR_i^{S_n} = \begin{cases} DSR_{i-1}^{S_n} + 2^{floor(k*(N-n))}, & CN = 0 \\ ceil\left(\frac{DSR_{i-1}^{S_n}}{2^{floor(k*n)}}\right), & CN = 1 \\ floor\left(\frac{DSR_{i-1}^{S_n}}{2^{n^2}}\right), & CN = 2 \end{cases} \quad (5.2)$$

where $DSRi^{Sn}$ is the current data sending rate, k is coefficient constant lies between [0, 1] and as analyzed in Appendix C can be 0.15, and CN is the congestion notification bit.

The proposed Quick Start and FIFD approaches are competently increases the data sensing rate and utilize bandwidth in an efficient manner.

II. Selective Packet Retransmission and Recovery

It is very clear from the literature review that, most of the WBAN applications require reliable delivery of packets so that the wastage of limited resources of WBAN can be prevented. Packet reliability is closely associated with loss considerations. Loss of packet occurs when there will be one or more packets which will not reach to the prescribed receiver or misplaced by the receiver itself. A proficient mechanism called selective packet retransmission and recovery is been proposed here for the skillful packet loss detection, notification and initiation of appropriate action for the recovery of loss. This approach performs the needful actions to achieve partial recovery using the following

three mechanisms; Packet loss detection, SNACK based packet loss notification and Selective packets retransmission.

A. Packet Loss Detection

The major aspect, which mostly affects the reliability in WABN, is a packet loss [130]. The reason of occurrence of this loss could be any one of the following factors; i.e. congestion in the network, bad channel conditions, link failure etc. Packet loss can be detected if there is a hole found in a series of the delivered the sequence number of packets. The order of the packet sent from each sensor node is identified by the sequence number of packets, and it further helps during reconstruction, regardless of any fragmentation, disordering, occurs during transmission. For better reliability, an acknowledgment and retransmission mechanism is been designed to compensate this.

Here the packet loss is been detected by the intended CU. It is done by analyzing the gap in the received packet's sequence number and can be mitigated through retransmission.

The percentage of loss rate can be calculated by finding out the ratio of the total number of lost packets in an interval with respect to the total number of packets transmitted in that interval. Algorithm 5.1 explains the working of packet loss detection technique.

B. Selective Negative Acknowledgment (SNACK) based Loss Notification

A general and very common problem with the reliable transmission is to deal with a large volume of feedback or control packets. Various restraint mechanisms are proposed in [59-60] to reduce the number of feedback packets. Following ways are followed to send notification to the sender when packet loss is experienced by the receiver.

Acknowledgment (ACK): After receiving a packet, a confirmation is sent back by the receiver to the sender issuing an ACK packet. An ACK can be used for individual or multiple receptions of packets.

Negative Acknowledgment (NACK): It provides the information about a lost packet. Through NACK, a notification about a lost packet was send to the sender by the receiver. A NACK can also issue for a single or multiple requested packets.

Algorithm: Packet Loss Detection

Input: *Packet Traffic type, Packet sequence number*
Output: *Sequence number of lost packet*

1. ***For*** *each reception of packet* P_i, ***Do***
   //Check Packet Type
   1.1. ***If*** *packet type= =1, then // data packet*
      1.1.1. *Set Recv_counter++*
      1.1.2. *Calculate* $Gap_i = (P_i).seq\_no - (P_{i-1}).seq\_no$
      1.1.3. ***If*** Gap_i*! =0, then*
         1.1.3.1. *Set Loss_counter+= Gap*$_i$
         1.1.3.2. ***For*** *k=1 to* Gap_i, ***Do***
            Call *insert (pkt_loss_table, loss packet* P_{Gapi}*)*
         1.1.3.3. ***End For***
         1.1.3.4. *Set* Gap_i*=0*
         1.1.3.5. ***Call*** *lossNotification (*P_i*)*
      1.1.4. ***Else***
         // Search the packet in DEPQ
         1.1.4.1. ***If*** P_i *is present in DEPQ,* ***Then***
            Drop P_i
            Set Drop_counter++
         1.1.4.2. ***Else***
            Insert packet P_i *into appropriate DEPQ*
         1.1.4.3. ***End If***
      1.1.5. ***End If***
   1.2. ***End If***
2. ***End For***

Algorithm 5.1 Algorithm for Packet Loss Detection

The aforesaid process recalls that an ACK is sent by a receiver when it receives the ordered packet. But sending notification for each delivered packet causes ACK implosion problem. Adaptation of NACK [60] came into the picture to achieve scalability and lessen implosion problem caused by ACK based feedback mechanism. Here a receiver publishes a NACK feedback packet as soon as it detects a missing sequence number in the sequence number of received packets. But in some cases like "single packet loss"

causes NACK implosion problem in the network. Without re-inventing the wheel, Selective ACK/NACK adopts the multiple packet notifications by issuing single notification about two or more received or lost packets to control the unnecessary transmission of feedback packets, but after all, it still faces the implosion problem. In all these cases, the overall performance and outcome is not only ruinous but also complicated. Another method called duplicate ACK (DUPACK) [65] was adopted by some of the protocols, but it increases the transmission delay for retransmitted packets and waiting time of out-of-order received packets.

In order to overcome this problem, an effort has been done with few amendments in already proposed methodologies, which is called as Dual-Selective NACK packet. The proposed loss notification adopts a twofold SNACK based loss notification and recovery policy, where the CU sends a SNACK packet signifying that it has not received the prescribed data packets during a specific duration. Algorithm 5.2 provides the pseudo-code for the packet loss notification approach.

In addition to SNACK sequence number, intended sensor's identification number and priority, DSR field, time of transmission. Every SNACK packet is having the following additional fields.

- *Packet_Type*: It provides the information about the type of packet i.e. data packet, control packet etc.
- *Retransmission Timer*: It gives information about retransmission time-out timer.
- *Retransmission Rate:* It provides the calculated retransmission cost as given in equation (5.3) which provides the information about how many packets needs to be retransmitted. It is totally based on priority of the sensor node. Lost packet's highest sensor node priority will retransmit more number of packets than others.

  $$Retx\_rate = ceil(\frac{Loss\_rate}{sensor\ priority}) \quad (5.3)$$

  where Retx_rate represents the retransmission rate, Loss_rate denotes the total lost packets.
- *Loss_List*: This field helps in providing information about the entire lost packet. It is further having two sub-fields.

- *Lost_seq_no*: It acts as the first field which provides the gap in the sequence number of the received packet.
- *Consecutive_loss_count*: The second field which keeps the count of a total number of consecutive packet loss information in the current series.

A different kind of problem is faced in this kind of notification approach. How to notify the sender about the successful reception of last packet, and how to handle problem when the sender is permitted to send only a single packet, and that packet get lost during transmission. To handle these problems, SNACK sequence number is to be filled with a unique marker '$'.

Algorithm: loss_Notification (Packet $P_{i,j}$)

Input: *Sequence number of lost packet*
Output: *Retransmission rate and new DSR*

1. *After detection of loss*
2. *CU generates a new SNACK packet and set its fields with new values*
   - *2.1. Set packet type = =2.*
   - *2.2. Increase the sequence number i.e. (SNACK).seq_no++*
   - *2.3. Calculate the new DSR using* ***Equation (5.2)***
   - *2.4. Calculate the new Retransmission rate using the* ***Equation (5.3)***
3. *CU prepares the loss list, where each cell is having two sub-fields*
   - *3.1. Set Lost_seq_no // provides the information of sequence no of first loss*
   - *3.2. Set Consecutive_loss_count // provides the information about all the consecutive lost packets with respect to the first lost packet*
4. *CU forwards this SNACK packet towards appropriate sensor node*

Algorithm 5.2 Algorithm for SNACK based Loss Notification

C. Selective Packets Retransmission

Packet retransmission mechanism acts as the final phase during packet loss recovery. Some of the existing protocols [60] highly accept the concept of retransmission timeout (RTO) mechanism to heal packet loss problem. While others [101,130] follow a fast retransmission approach is the recovery of packet loss. But both these approaches will cause large delay and low throughput. So a selective packet retransmission and recovery

approach is contributed here with an intellectual mechanism to deal with the above-mentioned issues. The main objective of it is to improvised the packet delivery rate efficiently and then reduce waiting time delay which occurs during packet loss recovery. To get rid of this problem, a method will be provided which offer a partial loss recovery by retransmitting selected amount of packets.

Here the loss recovery approach can be defined as the retransmission of lost packets within a definite time interval. So it is designed with two methodologies by keeping in mind benefits of both Rate-driven retransmission and Timer-driven retransmission approaches.

Rate-driven Retransmission approach: According to the rate-driven approach, when the CU discovers a packet loss in the incoming flow, it then calculates the retransmission rate for every sensor node. The decision about which packet needs to be retransmitted is taken by the CU after verifying the following information about a packet; the sequence number of a packet, its priority value, its parent node's priority value etc. According to this, the packet having high priority or important information is asked for retransmission; while for rest, it asks only selected number of lost packets, those having a highest sequence number for retransmission. By doing so, the purpose both loss recovery and retransmission delay get solved. On the basis of this selection, CU prepares the SNACK packets and sends it to the particular sensor node for providing information about the required lost packets. After the reception of a SNACK packet, the sensor node first verifies the sequence number of the SNACK packet, if there is a hole in the sequence number of SNACK packet, then it detects a SNACK loss and notifies about this loss to the CU. Otherwise, the sensor node checks that whether it is the required SNACK (i.e. second subsequent SNACK) packet or not, if it is the required one, then the sensor node retransmits all the asked packets.

Time-driven Retransmission approach: According to the time-driven recovery approach, if a sensor node does not receive any SNACK packet within a definite time interval from the CU, then it starts retransmitting all the packets by believing that all transmitted packets were lost.

Algorithm 5.3 outlines the working of the selective packet retransmission approach.

Algorithm: Selective Packets Retransmission (at sensor side)

Input: *Retransmission timer, Packet traffic type, SNACK packet*
Output: *Retransmission of packet*

1. *Set Retransmission timer*
2. ***While*** *(Retransmission timer!=0),* ***Do*** *// check incoming packet*
   - *2.1.* ***If*** *(packet_type = =2),* ***Then*** *// SNACK packet*
     - *2.1.1. Initialize SNACK_counter=0,* $D_{SNACK}=0$
     - *2.1.2. Set SNACK_counter++*
     - *2.1.3.* ***If*** *(SNACK_counter = =2),* ***Then***
       - *2.1.3.1.* ***If*** *(((*$SNACK_i$*).seq_no – 2) = =* D_{SNACK}*),* ***Then***
         - *2.1.3.1.1. Sensor* S_n *retransmits all the asked packets in the SNACK*
         - *2.1.3.1.2. Set SNACK_counter=0*
         - *2.1.3.1.3. Set* D_{SNACK}*=(*$SNACK_i$*).seq_no*
       - *2.1.3.2.* ***Else***
         - *2.1.3.2.1. Sensor node identifies the SNACK loss*
         - *2.1.3.2.2. Sensor node notifies the CU about this loss*
       - *2.1.3.3.* ***End If***
     - *2.1.4.* ***End If***
   - *2.2.* ***End If***
3. ***End While***
   // When Retransmission timer expires and there is no SNACK packet arrives
4. *Sensor node retransmits all packets for that interval by assuming that all packets are get loss during transmission*

Algorithm 5.3 Algorithm for the Selective Packets Retransmission

The working principle of Selective packet Retransmission and Recovery approach is illustrated below.

Step 1: Detection of missing packets

On reception of a packet, CU checks the sequence number of the received packet, if there is a gap found in the sequence number of the incoming packet, then it will detect packet

loss and updates the loss counter accordingly, otherwise, CU treats it as in-order packet and stores it into the queue.

Step 2: Packet loss notification by issuing SNACK packet

In case of packet loss, CU calculates the retransmission rate. After this, CU generates a new SNACK packet, and fills its fields with sequence number of packets which is to be retransmitted. It then sends this SNACK packet towards the sensor node.

Step 3: Retransmission of asked packets

After receiving the SNACK packet, all the requested are then retransmitted by the sensor node. In case Retransmission timer gets expired and sensor node does not receive any SNACK packet, then the sensor node will retransmit all the transmitted packets again.

A detailed explanation of the proposed selective packet retransmission and recovery approach is explained with an example in *Appendix D.*

The main objective of the selective packet retransmission and recovery approach is, not only to retransmits selected amount of recently lost packets upon the reception of the SNACK, but also to give more emphasis on the recovery of high priority lost packet. So, it retransmits high priority packets with a high degree of intensity than the low priority packets. By doing so, it is able to reduce retransmission overhead, delay, and congestion problems from the system.

III. Duplicate Packet Mitigation

The issue of resources expenditure for a network is rising up day by day. It is not only rising for the factors like congestion or delay but also due to some other factors like retransmission of duplicate or redundant packets. Packet duplication is a process of transmitting the same packet multiple times towards the receiver, and duplicate mitigation provides a way of suppressing transmission of same packets again and again from sender node to the receiver node. An embracing truth is that no work has been carried out in this regard; although duplicate packets are the main eradicator of network resources i.e. bandwidth, power or energy, and network like WBAN can’t afford these kinds of resource expenditures.

To maintain a consistent utilization of network resources, a duplicate packet detection and mitigation approach named *Duplicate Packet Detection* is been introduced here, which has the potential to identify and eliminate duplicate packets within the network and come out as a powerful technique to improve the efficiency of the network during the face of repeated packets.

A. Duplicate Packet Detection

It has been observed that in real-world the traffic of a network exhibits a large amount of duplicate packets during the process of transmission, and unfortunately network pays more resources for this. So that the proposed duplicate mitigation approach is being implemented to overcome the duplicate transmission of packets wisely and to save the bandwidth of the network effectively. For that, a technique is introduced which helps in keeping information regarding a lost packet. Here the sequence number of a packet plays an important role in the identification and elimination of a duplicate packet. So, in the proposed approach, the CU node maintains a lost table to store the information about the lost packet (i.e. the sequence number of the lost packet) which further helps in duplicity detection.

Packet Lost Table: When CU discovers a lost packet, it searches a place where it can keep the sequence number of a lost packet in the lost table. A new kind of technique called *Extended Cuckoo Hashing (ECH)* is been applied in order to find the actual place of the lost packet in the lost table. This ECH technique is an extension of cuckoo hashing technique [104]. The proposed lost table consists of a buffer, where information about a lost packet can be kept in any one of its three different prospect places. These places are determined by applying hash functions on the selected header fields of a lost packet, i.e. packet size, sequence number of the packet, priority of the packet and its parent sensor node. In the lookup process, it checks the first two prospect places. If it found any of the two places empty, it immediately inserts the lost packet's sequence number to any one of these two places. And if in case neither of these two places has been empty, then it finds out the third place, and if it is empty, then it stores the lost packet information in this place. When all of these three places are not empty, in that case, it selects any one place out of the two candidate places, throws out the existing sequence number (i.e. re-inserts

the victim packet' sequence number to its own alternative place) and then inserts the new lost packet's sequence number into this empty place. This process will then get repeatedly done until all lost packets found a specific place in the lost table. The Algorithm for the duplicate packet mitigation approach is given in Algorithm 5.4 ((a)-(d)).

Algorithm: Duplicate Packet Mitigation

Input: *Sequence number of lost packet*
Output: *Either detect a duplicate packet or find a place to store a lost packet*

1. *Upon reception of a packet P*
2. *Check its sequence number*
3. ***If*** *(sequence number of the incoming packet is greater than the expected packet's sequence number),* ***Then***
   - *3.1. Detection of a packet loss*
   - *3.2. Mark all lost packet*
   - *3.3.* ***For*** *each lost packet,* ***Do***
     - *3.3.1. Call search(pkt_loss_table, P) // search a place in loss table*
   - *3.4.* ***End For***
4. ***Else If*** *(sequence number of the incoming packet is less than the expected packet's sequence number),* ***Then***
   - *4.1. Check its sequence number in packet lost table*
   - *4.2.* ***If*** *(found),* ***Then***
     - *4.2.1. Set Retx_counter++*
     - *4.2.2. Delete this lost packet entry from pkt_loss_table.*
     - *4.2.3. Enqueue it into appropriate DEPQ*
   - *4.3.* ***Else***
     - *4.3.1. Drop packet// duplicate re-transmission packet*
     - *4.3.2. Set Drop_counter++*
   - *4.4.* ***End If***
5. ***Else if*** *(sequence number of the incoming packet is equals to the expected packet's sequence number),* ***Then***
   - *5.1.1. Enqueue the packet // in-order packet*
6. ***End If***

Algorithm 5.4 (a) Algorithm for Duplicate Packet Mitigation

Algorithm: search (pkt_loss_table, P)

Input: *Packet size, sequence number, priority, and parent node's priority of lost packet*
Output: *Candidate place in lost table*

1. *Initialize the size of Packet_loss_table=100*
2. *Select four fields from the packet P(Packet Size, Packet's Seq_no, Packet's Priority, Priority of sensor node)*
3. *Apply hash functions h1 and h2 on these above four fields to generate new places i.e. r_1 and r_2.*
4. ***Call*** *h1(Packet Size, Packet's Seq_no, Packet's Priority, Priority of sensor node)*
5. ***Call*** *h2(Packet Size, Packet's Seq_no, Packet's Priority, Priority of sensor node)*
   - 5.1. ***If*** *(r1 or r2 place in pkt_loss_table is empty),* ***Then***
     - 5.1.1. *Insert lost packet's Seq_no into the vacant place*
   - 5.2. ***Else***
     - 5.2.1. *Find the third new place $r_3=(r_1+r_2)/2$*
     - 5.2.2. ***If*** *(r3 is vacant),* ***Then***
       - 5.2.2.1. *Insert lost packet's Seq_no into the vacant place*
     - 5.2.3. ***Else***
       - 5.2.3.1. *Randomly choose a place from r_1 or r_2.*
       - 5.2.3.2. *Kicked out the already present packet's sequence no from that place and insert the lost packet's Seq_no into this vacant place*
       - 5.2.3.3. *Repeat step 5-6 until all the lost packet get separate place in loss table*
   - 5.3. ***End If***
6. ***End If***

Algorithm 5.4 (b) Algorithm for Searching a Packet in Lost Packet Table

Algorithm: h1 (Packet Size, Packet's Seq_no, Packet's Priority, Priority of sensor node)

Input: *Packet size, packet sequence number, packet priority, sensor priority*
Output: *First candidate vacant place in lost table*

1. *Concatenate these four values; Packet Size, Packet's Seq_no, Packet's Priority, and Priority of sensor node to generate a new value i.e.* V_1.
2. *Scan from right and Segregate* V_1 *into three subpart of equal length by filling the vacant place with 0's.*
3. *Length of each sub-group=ceil (*(V_1*. Length)/no of sub-group)*
4. *Add digits of each individual place of these groups to produce a new number* num_1.
5. *Divide this new number by size of loss table to find* r_1. *i.e.* r_1*=num1/Pkt_loss_table.Size.*
6. *Return* r_1

Algorithm 5.4 (c) Algorithm for Hash function (h1)

Algorithm: h1 (Packet Size, Packet's Seq_no, Packet's Priority, Priority of sensor node)

Input: *Packet size, packet sequence number, packet priority, sensor priority*
Output: *First candidate vacant place in lost table*

1. *Concatenate these four values; Packet Size, Packet's Seq_no, Packet's Priority, and Priority of sensor node to generate a new value i.e.* V_2.
2. *Add each individual digits of* V_2 *to produce a new number* num_2.
3. *Find the square of the* num_2 *to produce* $Snum_2$.
4. *Divide this new number by size of loss table to find* r_2. *i.e.* r_2*=*$Snum_2$*/Pkt_loss_table.Size.*
5. *Return* r_2

Algorithm 5.4 (d) Algorithm for Hash function (h2)

Working principle of duplicate packet mitigation approach is explained below.

Step 1: Verification of incoming packet's sequence number

Upon reception of a packet, the first job of the CU is to verify the packet's sequence number.

- If the arrival packet's sequence number is greater than the expected packet's sequence number, then it identifies packet loss, and marks all the lost or missed packets. After that, it searches the right place for all lost packets in its lost table using ECH technique and stores their information.
- On the other hand, if the incoming packet's sequence number is less than the expected packet's sequence number, then the CU first checks the existence of the incoming packet in its lost table.
    - If it finds the incoming packet's sequence number in its lost table, then it inserts this packet into an appropriate queue and erases packet's sequence number from the lost table.
    - If the incoming packet's sequence number is not found in the lost table, then CU drops this packet and increases the drop counter by one.
- If the arrival packet's sequence number is found out as equal to the expected packet's sequence number, then CU marks it as an in-order packet, hence enqueues this packet and increases the received counter by one.

Step 2: Storing of incoming packet's information

CU updates the loss table and its database with incoming packet's information.

The ECH based duplicate mitigation approach is endowed with an intelligent and time efficient duplicate packet elimination process. This approach very smartly identifies duplicate packets and is also helpful to segregate the true retransmission from the duplicate one. It also provides help during lost packet information storing or retrieving by providing multiple alternate places for a lost packet in the lost table. The main advantage of this is that it is much faster than other hashing techniques because it is the one which is able to provide a faster construction, searching, and deleting operation with less time complexity. It also eliminates collision problem during storing and searching.

IV. Implicit Packet Reordering

Packet reordering [105] can be defined as a process where the order of arrival of packets is not same as sending order. The concept of packet reordering is directly related to the performance analysis in many networks. That is why packet reordering is always been taken into account whenever the QoS performance of a system is been considering. Basically, it is counted as a phenomenon of organizing packets at receiver in accordance with their sending order. Packet loss or delays during packet transmission are the two key factors for such kind of issue in a network. A large scale of the study shows that most of the protocols [68, 70] have used an explicit packet reordering mechanisms, which are very complex as well as time-consuming.

To make the process very simple and to add the flavor of unfussiness, the proposed protocol conducts an implicit packet reordering mechanism, where two Double-Ended Priority Queue (DEPQ) are used to enqueue high priority and low priority packets in a totally different manner.

A. Double-Ended Priority Queue (DEPQ)

Existing systems of WBAN use Priority Queues (PQ) [106] for storing or retrieving of their packets, PQ is not able to use its both ends simultaneously for storing or retrieving of packets. To get rid of this the DEPQ [108] offers a way to store and extract both high as well as low priority packets from its both ends. DEPQ is more efficient than single-ended PQ because it is capable to utilize memory in a better way and also proven to be very helpful during deadline and starvation problems. Here, each DEPQ is made up of min-max heap-based [107] data structure.

Min-Max Heap: The min-max heap is a complete binary tree which is having alternative min and max levels used to store elements. It satisfies both min and max heap sorting or ordering property. The data structure of min-max heap supports various in-build functions like: - put(), getMin(), getMax(), removeMin(), removeMax(), size(), and isEmpty(), which are helpful for carrying out various operations in DWBAN. This section helps in briefing the benefits of min-max structure. During the enqueue operation, the min-max heap helps to discover an empty place and inserts the packet into the

appropriate place in the queue using both isEmpty() and put() functions. The high priority packet was searched from the DEPQ using getMin() function and delete from DEPQ using removeMin() function in the case when there is a need for scheduling. Problems like starvation or congestion can be handled by finding and deleting low priority packets from the DEPQ using getMax() and removeMax() functions. On the other hand, size() function helps in identifying the queue occupancy. The most important thing offered by min-max heap is its heap structure, which is very useful for a packet during insertion as well as deletion. During insertion, it adds the new element to its last place and sorts the list implicitly to store each element to their best place in the list. Likewise, during deletion process, after deleting an element from the heap it again sorts the heap implicitly so that every element can get its correct place. It is an effective technique as it performs smartly in both average as well as worst cases. So, as a result, the time-complexity of min-max heap structure is proven to be more effective than others. The time-complexity of min-max heap structure during put(),removeMin() and removeMax() operations is O(log n), and is O(1) while performing rest of the operations. Working principle of implicit packet reordering approach is given below.

Step 1: Check for out-of-order packets

After receiving a packet, the CU checks for its duplicity, if it is not a duplicate one, no matter it is been ordered or out-of-order packet, the CU enqueue the packet using isEmpty() operation. Afterwards, the place of the packet can be identified out implementing put() operation in the header fields of the packet such as sensor id, sensor priority, packet sequence number, packet priority etc.

Step 2: Insertion of packets during packet queuing

During retransmission, if a lost packet arrives at the CU, it inserts the packet using put(), where it will implicitly reorder the packet and store it in its right place.

Step 3: Deletion of packet from DEPQ during packet scheduling

During scheduling the CU identifies and deletes both the highest and the lowest packets from both end of the queue in a specific time interval. For this it takes help of getMax(),

removeMax(), getMin() and removeMin() functions according to its requirement, and rest of the packets in the queue is arranged implicitly.

Step 4: Calculation of DPEQ occupancy

During congestion, the basic job of the CU is to identify the queue occupancy and it can be done with the help of size() functions.

The basic objective of implicit reordering approach is to reorder the incoming packets without the intervention of any extra reordering technique which saves both time and efforts as explicit packet reordering task in a heterogeneous network can increase the delay in the network.

5.2.2 Congestion Module

Congestion [109] is one of the biggest and critical issues in any network because it increases packet drop rate and delay in the network. Such kind of problems occurs due to unnecessary retransmission of packets; as a result throughput of the overall network gets decreased. This is the main contributor in affecting the reliability during packet transmission and also the offender for degrading the link utilization in the system. There can be many reasons of occurrence of congestion, but the most crucial one is queue overflowing or over-jamming where packet arrival rate exceeds the packet service rate. The problem of congestion in WBAN is quite different from other networks. Most of the existing protocols [110-111] handle this situation by decreasing the packet flow rate at which a source node can be able to insert packets into the network. Such kind of protocols get decreased the throughput of the network. There are some other protocols which deal with congestion problems by their active queue management [113-114] or traffic redirection [112] policies. By doing this they are able to manage the overloaded queue.

After a deep study on the above protocols, it is been observed that congestion is still an obstacle due to aggressive nature which is treated as a perennial concern in healthcare WBAN. Avoidance of congestion in such kind of systems is an essential requirement, as these systems deal with critical data. In order to handle congestion in DWBAN, a new

approach named *Dynamic Congestion Mitigation* has been deployed by the congestion module.

I. Dynamic Congestion Mitigation

The dynamic congestion mitigation is been proposed with both congestion control and avoidance strategies, which are actually responsible for dynamic resource management. So it is composed of two key components: *Multi-factors based Congestion Detection and Notification (MFCDN)* component and an *Intelligent Congestion Alleviation (ICA)* component. These components consist of a new kind of rate control and packet dropping approaches which are important for the improvement of overall QoS performance. The modular architecture of the congestion module is explained in Figure 5.3.

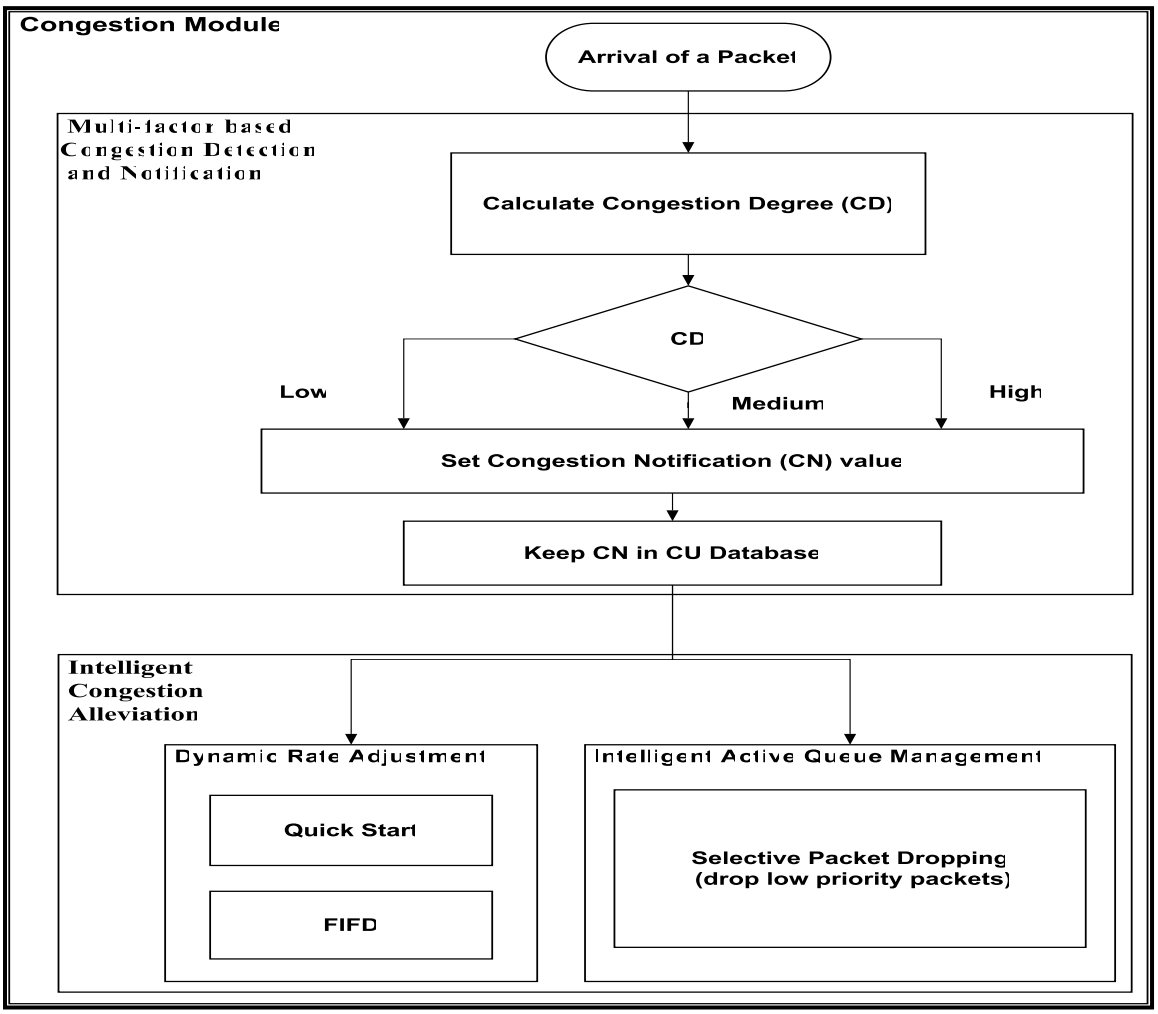

Figure 5.3 Workflow Diagram of Congestion Module

A. Multi-factors based Congestion Detection and Notification (MFCDN)

Congestion in a network can give birth to other serious problems like queuing delay, delay variation, retransmission etc. So, to overcome congestion, it is very important to detect the severity level of congestion. It was observed that queue occupancy is considered as one of the major factors for measuring congestion severity by many existing [71] protocols and their congestion control policies are exclusively based on this factor. Whereas the packet reception rate and packet service rate are considered into account as the congestion detection factors by some other protocols. But from the literature survey, it was very clear that consideration of all the mentioned factors is not sufficient to identify the actual status of the congestion and it makes congestion control a very fuzzy in critical networks.

The mechanism of MFCDN is very-very splendid, because of its capability for the accurate identification of the severity level of congestion. To implement multi-factor based congestion detection, it is very important to first evaluate the various factors which can be helpful in accurate detection of congestion. Thus MFCDN uses various parameters i.e. total loss, total delay, queue occupancy, and queue size for the detection of congestion.

Congestion Detection: Congestion detection identifies the level of congestion after measuring various parameters such as queue size, queue occupancy, total loss rate, and total delay present in the system. Queue size provides the information about how many packets can be kept in the queue. Queue occupancy is an effective measure of congestion detection which measures the total numbers of packets currently waiting in a queue during service. The total loss rate is defined as the total amount of packets get lost or dropped in the current interval. Total delay involves the transmission delay, delay variation and queuing delay featured by the network. In the proposed congestion detection method, the Congestion Degree (CD) is calculated after considering the above mentioned parameters. Here two threshold values i.e. maximum threshold (Th_{max}) and minimum threshold (Th_{min}) values are used to detect the category of congestion. The values of these thresholds are dynamic and can be adjusted with the changes in the environment for a particular time interval. Therefore two extra factors i.e. packet

incoming rate, and packet outgoing rate are considered to calculate Th_{max} and Th_{min} each time. The concept of the dynamic threshold can further influence the accuracy during congestion detection. Additionally, it also helps to control overflow and queueing delay.

Congestion Notification: Congestion notification is a process which provides the information related to congestion to the sensor node. The process of sending this information can be explicit or implicit, where the former one uses special packets for congestion notification, while the later one embeds congestion information in either data packets or control packets. MFCDN has considered the concept of implicit notification in its process. Here the congestion information is safely kept by the CU and also the information regarding the current status of congestion is indicated by the current data sending rate (DSR) field of the control packet, this will be calculated by the CU itself. Degree of Congestion (CD) is calculated after considering various parameters i.e. queue size, queue occupancy, total loss rate, and total delay. Here the congestion notification (CN) is identified from the calculated CD value and activated the CN in accordance with the level of congestion (i.e. No Congestion=0, Low Congestion=1, and High Congestion= 2).

The algorithm for MFCDN is given in Algorithm 5.5. The working principle of MFCDN approach is given below.

Step 1: Check for multiple factors in incoming packet

In this step, CU measures the values of multiple parameters like packet incoming rate, and packet outgoing rate, queue size, queue occupancy, total loss and total delay for a particular time interval.

Step 2: Calculation of minimum and maximum threshold values

CU computes the maximum threshold (Th_{max}) considering packet incoming rate, and packet outgoing rate as major factors using equation (5.3). The calculation of T_{min} is done from the equation (5.4).

$$Th_{max} = \begin{cases} 0.75, & if Packet_{outrate} \geq Packet_{inrate} \\ \frac{Packet_{outrate}}{Packet_{inrate}}, & Otherwise \end{cases} \quad (5.3)$$

$$Th_{min} = 0.5 * Th_{max} \quad (5.4)$$

where $Packet_{inrate}$ and $Packet_{outrate}$ define the packet incoming rate and packet outgoing rate and Th_{max} and Th_{min} denote the maximum and minimum threshold values.

Step 3.Calculation of degree of congestion

CU calculates the degree of congestion CD by applying equation (5.5) and taking into account the factors like queue size, queue occupancy, total loss and total delay.

$$CD = \frac{w_q * Q_{Occ} + w_l * Tot_{loss} + w_d * Tot_{delay}}{Q_{size}} \quad (5.5)$$

where w_q, w_l, w_d are three random weights generated from rand (0,1) function.

Step 4: Detection and notification of congestion level

The calculated CD is compared against the Th_{min} and Th_{max}, and generates the information about congestion notification (CN) by using the formula given in equation (5.6)

$$CN = \begin{cases} 0, & if CD \leq Thmin \\ 1, & if Thmin < CD < Thmax \\ 2, & if Thmax \geq CD \end{cases} \quad (5.6)$$

Step 5: Updation of CN bit and CU database

CU keeps the calculated CN value in its database and uses it for further mitigation of congestion in the system.

Algorithm: Multi-factors based Congestion Detection and Notification

Input: *Total loss, Total delay, Queue size Queue Occupancy, Packet incoming rate, packet service rate*
Output: *Congestion Degree, Congestion Notification*

1. *Set Time interval*
2. *Calculates the Th_{max} and Th_{min} using* ***Equation (5.3) and (5.4)***
3. ***For*** *each reception of packet*
   - *3.1. Calculates the congestion degree (CD) using* ***Equation (5.5)***
   - *3.2.* ***If*** *($CD < Th_{min}$), then*
     - *3.2.1. Set CN=0*
   - *3.3.* ***Else If*** *($Th_{min} <= CD <= Th_{max}$), then*
     - *3.3.1. Set CN=1*
   - *3.4.* ***Else If*** *($Th_{max} < CD$), then*
     - *3.4.1. Set CN=2*
   - *3.5.* ***End If***
4. ***End For***
5. *Store the CN value in CU database*

Algorithm 5.5 Algorithm for Multi-factors based Congestion Detection and Notification

The MFCDN technique helps in accurate congestion detection and early notification, as it tracks multiple factors.

B. Intelligent Congestion Alleviation (ICA)

The main limitation in some of the leading congestion avoidance and control protocols is that they only use "timeout" mechanism to detect and respond to network congestion, which further leads to an unnecessary long waiting time before some action will take place. Therefore to deal with such obstacles, authors [71, 75] had discovered a new mechanism called "fast retransmit", which is an enhancement to timeout mechanism as it helps in reducing the waiting time of the sender which a sender faces before retransmission of a lost packet, but at the same time increases the retransmission rate, because somehow they are responsible to retransmit all the lost packets. Thus the main focus of ICA should be on implementation of both the contents; i.e. *Congestion Control* and *Congestion Avoidance* algorithms so that the overall packet transmission can be

improved efficiently. The combination of these two strategies helps the system to improve the QoS in the aggressive and assorted environment of DWBAN.

Congestion Control: As the name suggests, the congestion control is a mechanism that should confidently handle the incoming traffic of the network. The congestion control mechanism is generally used to control packets loss and delay caused due to congestion in the network. So a new dynamic data sending rate adjustment based congestion control scheme is introduced in order to achieve dynamic rate allocation and maximum bandwidth utilization. Basically, it is very impractical to allocate a static rate to every node each time in WBANs, as both the available bandwidth and the severity level of sensor nodes are time-varying factors. Further, to achieve better results, it assures that the calculated data sending rate (DSR) of a sensor node must not exceed the allocated bandwidth at each time interval. So according to the need of each sensor node, the distribution of the available bandwidth among all active sensor nodes is done in such a way that maximum utilization of bandwidth can be achieved. To do so, it follows the *Quick Start* based DSR approach rather than slow start policy as discussed in heterogeneous flow control approach of reliability module (in section 5.2.1).

Congestion Avoidance: In DWBAN, the packet may come at CU in a burst from multiple sensor nodes, and the CU may receive more packets than it can serve for the time being. In that case, CU has to hold these packets until they get served until availability of resources and this situation give birth to buffer overflow problem and to overcome the same problem CU has to drop the incoming packets unwillingly. Complementary to existing Active Queue Management (AQM) strategies, proposed congestion avoidance strategy tries to mitigate the buffer or queue overflow problem very intelligently. Here the process of congestion avoidance strategy drops the selected amount of packets when congestion is likely to be happening in the network rather than just dropping all the incoming packets randomly. Some conventional AQMs affect the performance of the network by dropping approximately all incoming packets when outburst traffic arrives at the bottleneck buffer of the receiver, and this ultimately causes buffer overflows. This kind of packet dropping process is called Droptail [109] which in turn endows with performance degradation by stressing the source node for the

immediate adoption of the slow start approach. Due to which the utilization of bandwidth get reduced unless-until receiver buffer wins over the buffer overflow. A deep research says that Random Early Drop (RED) [115] is proven to be one step advanced than Droptail. Although RED is been widely adopted by all existing protocols, although it does have another crucial issue i.e. the average queuing delay of RED is sensitive to traffic load as well as other QoS performance parameters. The use of queue occupancy as major factor to measure the degree of congestion in RED gives a very little information about the severity of congestion. As a result, RED fails to take actual decision correctly under different congestion scenarios and is therefore not much suitable for a dynamic environment.

In a healthcare WBAN system, it is been observed that some packets are more important than others. So in order to improvise the quality of transmission or service, a smaller amount of important packets should be dropped during the congestion. To satisfy this requirement, the proposed congestion avoidance algorithm provides a *Selective Drop* policy during AQM. The job of this policy is to calculate the drop rate first and then drops the selected amount of low priority packets from the queue. By doing so, it saves high priority or more important packets. In addition to this, it also helps in reducing *Queuing Delay* during congestion. The queuing delay of a specific packet depends on various factors such as earlier arriving of packets and waiting for transmission; high queue occupancy; network congestion; queue management etc. These factors can vary significantly from packet-to-packet and from queue-to-queue.

The Algorithm for the Intelligent Congestion Alleviation approach is given in Algorithm 5. 6 and the working principle of ICA approach is illustrated below.

Step 1: Data Sending Rate calculation

For a particular time interval, CU checks its current CN field. According to the CN value, it computes the new Data Sending Rate (DSR) for each sensor node after applying the formula given in equation (5.2) and notifies the DSR in the current SNACK control packet.

Step 2: Estimate of Drop rate

Again according to the CN value, CU computes the new Drop Rate (DR), using equation (5.7) and then selects and discards that amount of low-priority newly arrived packets from the queue. If the incoming packet is having high priority, then the CU inserts it into the queue, instead dropping it. On the other hand, if the incoming packet is having low-priority then it will drop by the CU. In both cases, after dropping a packet the CU increases the drop counter.

$$DR_i^{S_n} = \begin{cases} 0, & ifCN = 0 \\ ceil\left(\frac{QO_i^{DEPQ}}{2*n}\right), & ifCN = 1 \\ ceil\left(\frac{QO_i^{DEPQ}}{n}\right), & ifCN = 2 \end{cases} \quad (5.7)$$

where QO^{DEPQ} denotes the queue occupancy in the current interval.

Algorithm: Intelligent Congestion Alleviation

Input: *Congestion Notification value*
Output: *Data Sending Rate, Drop Rate*

1. *Check the CN value*
2. ***If*** *(CN== 0),* ***Then***
   2.1. Set DR_i =0
   2.2. Set DSR_i= $DSR_{i-1}^{S_n} + 2^{floor(k*(N-n))}$
3. ***Else If*** *(Th_{min}<= CD <= Th_{max}),* ***Then***
   3.1. Set DR_i= $ceil\left(\frac{QO_i^{DEPQ}}{2*n}\right)$
   3.2. Set DSR_i= $ceil\left(\frac{DSR_{i-1}^{S_n}}{2^{floor(k*n)}}\right)$
4. ***Else If*** *(Th_{max} <=CD),* ***Then***
   4.1. Set DR_i = $ceil\left(\frac{QO_i^{DEPQ}}{n}\right)$
   4.2. Set DSR_i=$floor\left(\frac{DSR_{i-1}^{S_n}}{2^{n^2}}\right)$
5. ***End If***
6. *CU informs about the congestion through this calculated DSR value by adding it in the header field of a SNACK control packet*
7. *CU then sends this control packet to all sensor nodes*

Algorithm 5.6 Algorithm for Intelligent Congestion Alleviation Approach

The ICA includes both congestion control and avoidance concepts which help in reducing transmission and queuing delay as well as the unnecessary drop rate in the system. Its selective dropping approach further saves the high priority or urgent packets. Its data sending rate adjustment policy utilizes the bandwidth in a better way.

5.3 SUMMARY

In this chapter, MDPPH protocol for a delay-sensitive, time-critical healthcare WBAN is proposed. It provides the reason for improving QoS in DWBAN and thorough knowledge about the actual motivation behind MDPPH's design. The adaptation of fair sharing of bandwidth and data sending rate helps in reducing the loss and delay issues in the system. The reliability module facilitates heterogeneous flow and duplicate control, loss recovery, and possibly implicit reordering of packets. In radiance to above annotations, congestion module adopts multi-parametric congestion detection policy. Further, the outcomes with selective dropping and fair rate adjustment provide the bright side of the congestion control approach. Adding a bright and luminous factor called dynamic priority to the above modules highly enhance the performance beyond the expectation. Issues related to various delays are been resolved automatically with complement to both reliability and congestion improvising facilities. This chapter reveals the fact of the real behavior of MDPPH which affects the QoS performance in different scenarios.

CHAPTER 6

OMDPPH: DESIGN OF AN OPTIMIZED MDPPH PROTOCOL FOR OPTIMIZATION OF QOS IN DWBAN

6.1 INTRODUCTION

Day by day various advancements are taken place in WBAN, but achieving up to mark QoS in a heterogeneous and dynamic environment of DWBAN might be a difficult task due to various restrictions likewise high computational demands, low memory, low power, and limited resources. From the analysis, it was found that both DPPH and MDPPH protocols provide better QoS than the existing one, but they are not able to deliver high-level QoS. So there is a need for unification of a new mechanism which can magnify the level of QoS in the DWBAN.

An extensive research study digs out that Optimization is one of the best techniques which can help out to amplify the QoS in a better way? Basically, optimization provides a way of finding for the best optimal solution to any problem which is subject to specific constraints. Optimization gained popularity in various real-world engineering, mechanical, and networking areas [116-117] since last few years. For any problem, optimization selects the following three factors: i) Objective function which provides the problem to be optimized (minimized or maximized). ii) Variables provide the inputs for the objective function. iii) Constraints offer the restrictions to the variables. So that, it can allow possible values to the variables to obtain the optimal solution for the objective function, while entertaining all constraints.

A DWBAN carries dynamic nature where the performance of the system fluctuates with time so requires dynamic optimization. In a dynamic optimization, the search location may vary with time, the constraint conditions may not hold the search space, and the optimal solutions may be tangled with many neighboring candidates. So the dynamic optimization problems have objective functions that can change over time, thus potentially causing variations in the optimal solution and search space.

The proposed DWBAN is dealing with multiple QoS performance metrics so provided with multi-objective optimization functionality. Contrast to the single objective optimization whose main job is to minimize or maximize one objective under various constraints, whereas multiple objectives are optimized simultaneously in a multi-objective optimization problem.

A nature-inspired optimization technique represents an emerging computing paradigm that draws their motivation from different natural experts or species and is found to be a good choice for these kinds of systems as here the experts change their behaviors very frequently.

Therefore the proposed protocol in this chapter draws inspiration from nature, which has been very successful and has effectively solved similar types of complex problems for dynamic systems as they provide an optimal solution in a reasonable amount of time.

6.2. QOS OPTIMIZATION THROUGH OMDPPH PROTOCOL

Till date, various nature-inspired optimization algorithms [118-119] have been applied for various networking problems. But attaining a global-optimal solution is very tough for these algorithms especially for multi-dimensional, heterogeneous, and dynamic nature of DWBAN. Therefore, it demands a more powerful optimization approach to enhance its QoS performance. In addition, the above-mentioned optimization algorithms also require a large set of parameters to yield optimal solutions, which further increase the complications in the system. So an optimization technique with fewer number parameters needs to be applied to defeat the complexity problem in the system.

From the deep literature study, it observed that the lion optimization is a good match for the aforementioned provisions of QoS in DWBAN. According to [120], this approach mimics the hunting technique of lion and defeats other optimization algorithms for various mathematics and engineering related functions. During hunting, it accompanies an Opposition-Based Learning (OBL) [123] strategy. The fundamental idea of Opposition-Based Learning (OBL) has been illustrated as an adequate approach for

solving various problems in optimization. These features in lion optimization are the principal inspiration for the development of a novel protocol named Optimized MDPPH (OMDPPH) protocol to maximize QoS performance in the DWBAN.

In the proposed OMDPPH protocol, a Lion Group Hunting optimization algorithm is used to optimize the QoS performance metrics of the healthcare DWBAN. Due to the adoption of OBL policy and multi-dimensional encircling technique during hunting, this framework is able to optimize the QoS performance promptly. Lions are the most experienced and talented hunters among all of the cooperative hunters and possessing high success rate during the hunt. The Modular architecture of OMDPPH protocol is illustrated in Figure 6.1.

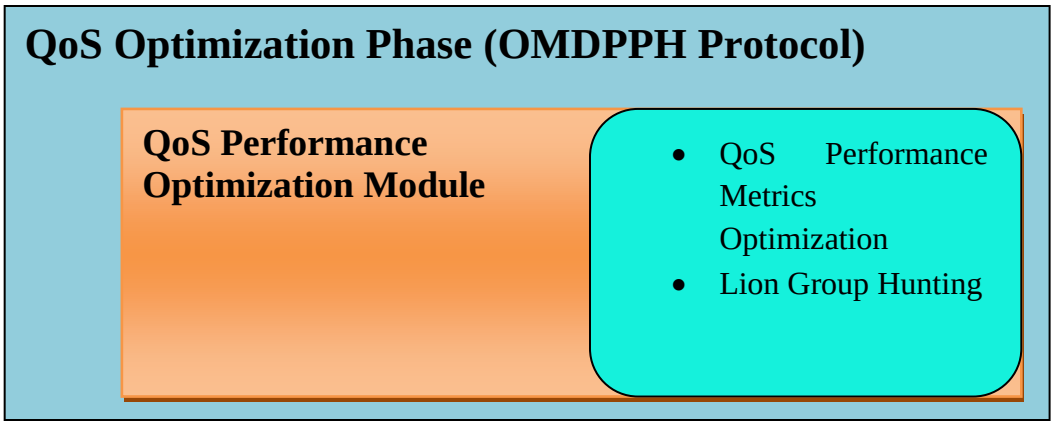

Figure 6.1 Modular Architecture of OMDPPH protocol

6.2.1 Lion Group Hunting Optimization Algorithm

Lions are the most social species of nature living in two kinds of groups i.e. Nomad and Pride. A pride is a social group consists of 1-18 related adult females along with their cubs and a coalition of 1-9 adult males. Lion is able to find enough food because they do their hunting cooperatively. From each pride, some figure of lionesses selected to hunt for a prey in a pack to supply food for their family members. These lionesses are trained to follow a clever stratagem or trick to encircle the prey and catch it. Male lions rarely take part in hunting and they are basically solo-hunters. One of the important characteristics of a lion is that they have a strict social hierarchy in order to maintain stability and to mutually assist each other during hunting. Hunters simulate an intelligent search strategy to encircle and capture the prey successfully.

Rajakumar [121] and Yazdani [122] illustrate the functionality of the lion group hunting technique to find best solutions for any kind of problem. According to their research, lion commonly obeys three strategies during hunting: i) Tracking, following and approaching the prey; ii) Harassing the prey; iii) Attacking the prey. During hunting, hunters are categorized into three sub-groups or packs named as Central pack, and Wing packs (i.e. Left and Right packs) according to their stalking roles and skill for chasing the prey. There are seven stalking roles which decide the group for a lioness. During practice phase of hunting, lionesses are selected one after another, and assigned different job and positions according to their pack, so that each individual lioness or hunter can encounter in its comfort zone with a preferred position in the pack.

Wing Pack: Hunters belongs to left and right wing packs are having fast running ability and have the capability to run faster than prey. The member belongs to left and right packs encircle or surround the prey from different direction (from opposite direction also). Then they will chase, follow and harass the prey for up-to some hours until prey becomes tired and finally then driven the prey towards the central pack members hiding in bushes.

Central Pack: The more powerful hunters are selected and put into this group during hunting. Normally group members of this group are hidden behind the bushes and tall grass. When members of wing pack driving the prey towards the central pack fellow members, they jump and attack the prey.

The Lion Group Hunting basically has scientific reasons how it outperforms than other group hunting. The first advantage is a categorization of hunter and position assignment accordingly, the second one is its multi-dimensional encircling technique along with opposition-based learning, and the third one is the attacking policy followed by the group members of the central pack. With these benefits, LGH is able to keep a physical equilibrium in between the exploitation and exploration in any solution space and thus able to achieve good performance on a wide spectrum of optimization problems. It further shows a high degree of flexibility, and robustness along with quick convergence. It has been proved that this technique is skilled enough for solving a wide variety of complicated and dynamic problems even with a small number of initial candidates.

The concept of group generation is shown in Figure 6.2, where seven hunters L = {L1, L2,….L7}are grouped into three different sub-groups or packs. The concept of opposition based encircling technique from n-directions is given in Figure 6.3.

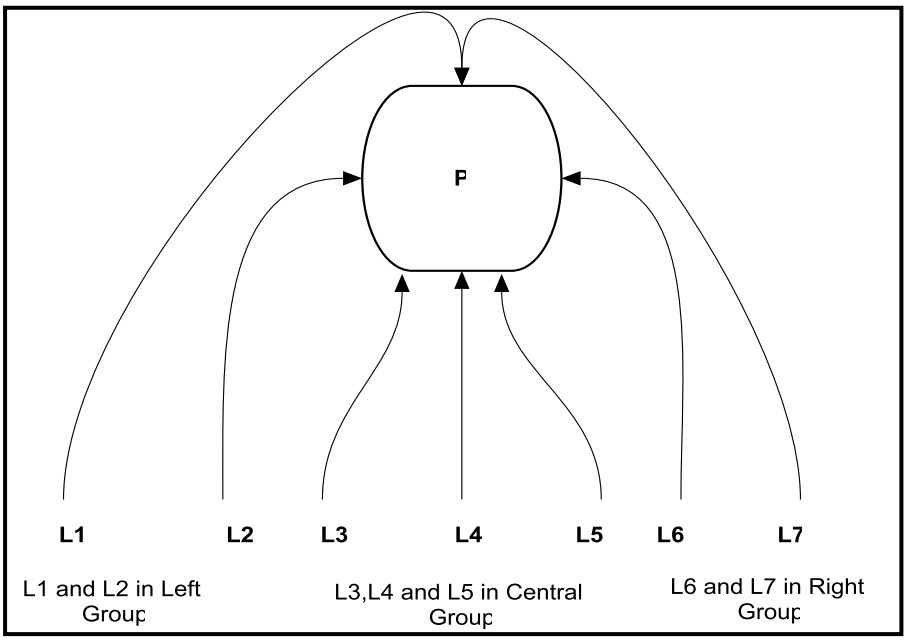

Figure 6.2 Formation of sub-packs in Lion Group Hunting

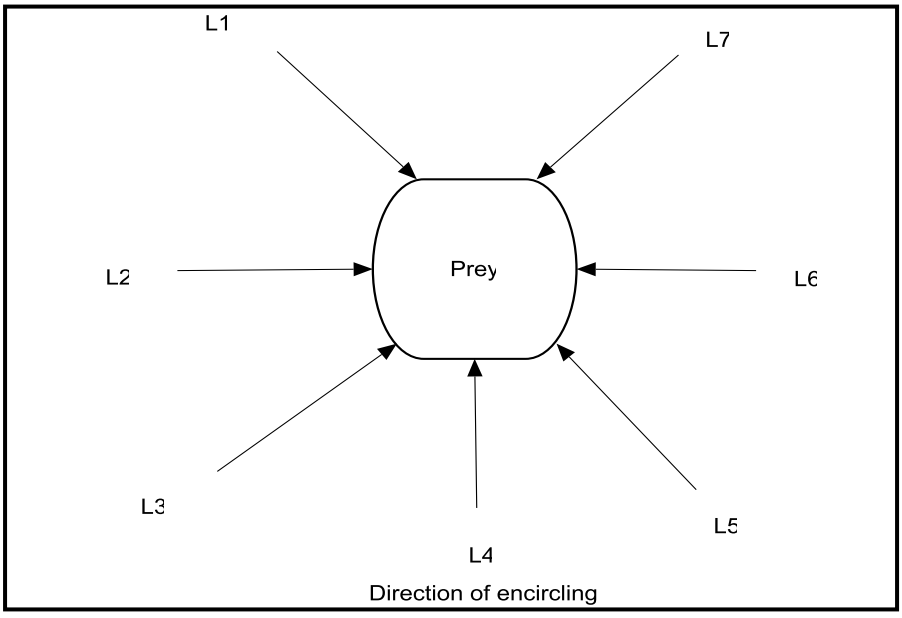

Figure 6.3 Multi-dimensional Encircling Strategies in Lion Group Hunting

During the practice phase of hunting, a dummy position of the prey is determined. Out of 'n' hunters, hunter with highest and intelligent attacking potential is chosen as the candidate for the central pack. Hunters with highest running capacity and lowest attacking ability put into the Left pack, and Right pack. Throughout hunting, the prey tries to escape and frequently changes its position. The position of the prey is considered as dynamic. In order to tackle the dynamic prey, each hunter corrects its position accordingly. If the new position of a hunter is better than its old position, then the success rate of capturing the prey is increased, otherwise, escaping rate will get increased. The position of each hunter is updated dynamically in this way.

Steps involved in LGH optimization technique

The proposed LGH technique depends mainly on two factors; the pack selection and re-positioning. The LGH optimization algorithm follows six basic steps to optimize the QoS performance.

Step 1: Initialization of population

In this step, the hunting group size is selected. On the basis of the number of hunters and their roles, hunters are randomly assigned to three sub-packs: central pack, the left pack, and right pack.

Step 2: Initial position of prey

The initial position of the prey is calculated using equation (6.1). Each selected hunter attacks the prey based on to their role and group they belong to.

$$P_0 = (\sum_{n=1}^{N} HL_n)/N \quad (6.1)$$

where P_0 is the initial position of the prey, HL_n is initial position of the n^{th} hunter, N denotes a total number of hunters participated in hunting.

Step 3: Re-Positioning of Prey

During hunting, the actual position or fitness of each hunter is changed according to the requirement; hence the prey also updates its position to escape from hunters according to the situation. If the current fitness of a hunter is better than its previous fitness, then

there is a chance of capturing the prey, otherwise, the prey will run away and the new position of the prey will be obtained by using equation (6.2).

$$P_i^{k+1} = P_i^k + C * r(0,1) * (P_i^k - HL_i^k) \quad (6.2)$$

where P^{k+1} denotes the new position of the prey, P^k is the current position of the prey, HL^k is the current position of hunter at k^{th} iteration, from i^{th} direction as hunter attacks from multiple or N-dimensional directions, r(Low, High) is defined the random number generation function which generates a random number in between low and high range. C defines the percentage of increment in the fitness of hunter.

Step 4: Re-Positioning of hunters belongs to the central pack

At the time of encircling the prey, the position of each hunter is updated. The new position of hunter belongs to the central pack is calculated using equation (6.3).

$$HL_i^{k+1} = \begin{cases} r\left(HL_i^k, P_i^k\right), if\ HL_i^k < P_i^k \\ r\left(P_i^k, HL_i^k\right), if\ HL_i^k > P_i^k \end{cases} \quad (6.3)$$

where P^k is the current position of the victim, HL^k is current position hunter and HL^{k+1} is the new position of hunter.

Step 5: Re-Positioning of the hunters belongs to Wing (i.e. Left and Right) packs

The new position of a hunter belongs to wing packs are calculated as given in equation (6.4).

$$HL_i^{k+1} = \begin{cases} r\left(\left(2 * P_i^k - HL_i^k\right), P_i^k\right), \ if\left(2 * P_i^k - HL_i^k\right) < P_i^k \\ r\left(P_i^k, \left(2 * P_i^k - HL_i^k\right)\right), \ if\left(2 * P_i^k - HL_i^k\right) > P_i^k \end{cases} \quad (6.4)$$

where $2*P^k$ is the current position of the victim from opposite direction, where $2*P_i^k$ is the position of the prey from an opposite direction of the hunter as the hunter belongs to wing pack, attacks from the opposite direction as hunters follow an Opposition Based Learning (OBL) technique during hunting as explained in Figure 6.4, while on the other hand, hunter belongs to central pack attack from front direction. The HL^k is the current position hunter and HL^{k+1} is the new position of hunter.

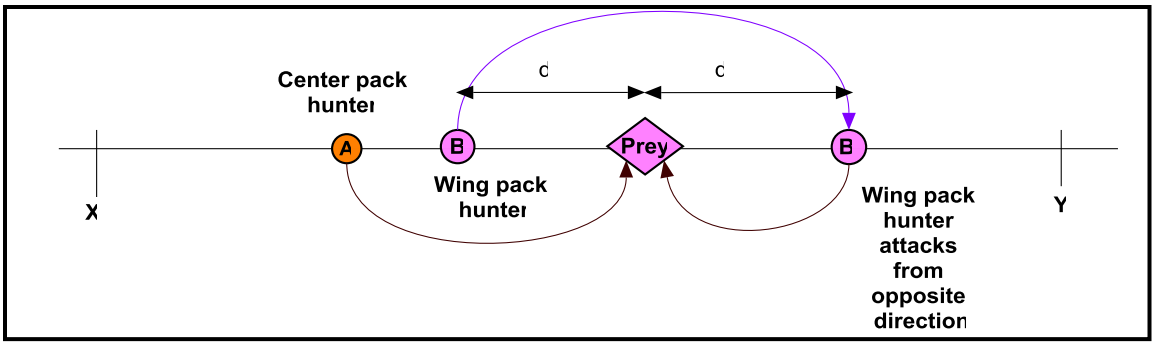

Figure 6.4 Opposition Based Learning (OBL) Encircling Technique in LGH

The OBL [123] made an important contribution to the LGH is to make use of opposite position to approach the solution in a more perfect way. According to OBL, an opposite position is probably closer than a random position and hence, helps to find the solution in less time. Thus, by attacking a prey from opposite direction provides a better search space and which is an essential factor to converge towards the right solution. Other advantage of this strategy is that it provides a circle-shaped neighborhood around the prey, and let hunters to close and attack to prey from different directions. Additionally, this strategy provides an opportunity for solutions to escape from local optima. In the Figure 6.4 the actual position of hunter 'B' belongs to wing pack is let 'd' distance from the prey, but it has to cover "d + d =2d" distance during hunting, as it attacks from the opposite direction.

Step 6: Termination

The changes in position of all hunters are continuing until either the obtained result of the objective function is not satisfied or the exit condition is not convinced. Hence, all the above steps are repeated until termination criteria is achieved.

6.2.2 QoS Optimization Module

The main objective of OMDPPH protocol is to develop a multi-objective QoS optimization approach based on LGH algorithm. So the QoS problem is formulated in the form of two basic functions; objective function and constraint violation functions. It filters out nine major objectives or fitness functions which are listed in Table 6.1. These fitness functions act as key measures for the improvement of QoS in the DWBAN. The main aim of these fitness functions is to find the optimal QoS in the specified time

interval. A mathematical formulation is developed to generate fitness functions which act as the real factors for the QoS performance improvement in the DWBAN.

Table 6.1 List of Fitness Functions

S. N.	**Performance Metrics**	**Fitness Functions**
1	Packet Loss Ratio (PLR)	$min \sum_i PLR(i), for\ all\ i \epsilon Set\ of\ sensor\ node$
2	Packet Drop Rate (DR)	$min \sum_i DR(i), for\ all\ i \epsilon Set\ of\ sensor\ node$
3	Elapsed Time Delay (D_{EL})	$min \sum_i D_{EL}(i), for\ all\ i \epsilon Set\ of\ sensor\ node$
4	Variation in Elapsed Time Delay (D_{VA})	$min \sum_i D_{VA}(i), for\ all\ i \epsilon Set\ of\ sensor\ node$
5	Queuing Delay (D_{QE})	$min \sum_i D_{QE}(i), for\ all\ i \epsilon Set\ of\ sensor\ node$
6	Queue Occupancy (Q_{Occp})	$min \sum_i Q_{Occp}(i), for\ all\ i \epsilon Set\ of\ sensor\ node$
7	Retransmission Rate (Retx)	$min \sum_i Retx(i), for\ all\ i \epsilon Set\ of\ sensor\ node$
8	Packet Delivery Ratio (PDR)	$max \sum_i PDR(i), for\ all\ i \epsilon Set\ of\ sensor\ node$
9	Throughput	$max \sum_i Throughput(i), for\ all\ i \epsilon Set\ of\ sensor\ node$

Here the fitness functions can be represented as minimize/maximize QoS(i),where i represent the n-dimensional decision vector which is belongs to a feasible region in the search space having domain size in the form of lower and upper bound. The upper and lower bound are explained as: 5<=number of nodes<=15.

All the listed fitness functions have the following additional constraints. The constraints are listed in Table 6.2.

Table 6.2 List of Constraints

S.N.	***Constraints***
1	$BW_k^{S_i} \leq BW_{av}$
2	$DSR_k^{S_i} \leq DSR_{max}$
3	$TTG_k^{S_i} \leq TTG_{max}$
4	$Th_{min} \leq CD_k \leq Th_{max}$

where BW denotes the bandwidth used by a sensor node, BW_{av} denotes the bandwidth allocated to a sensor node, DSR denotes the data sending rate, TTG denotes the packet transmission time gap, CD denotes the congestion detection, Thmin and Thmax denote the minimum and maximum threshold values, S_i denotes the sensor node where i belong to the set of sensor node, k denotes the time interval.

In order to optimize the QoS performance these nine fitness functions should not violate the above-mentioned constraints. These four constraints need to be controlled in order to improve the fitness functions. The fitness function of each performance metric is evaluated and checked against previous fitness function value in order to handle dynamic QoS in the DWBAN.

The performance of OMDPPPH algorithm in order to improve QoS performance metrics like loss, drop, delay, variation in delay, retransmission, throughput etc., clearly depends on the optimal mapping of performance metrics into LGH. For this the problem of QoS performance is formulated as an optimization problem and is explained in following steps.

Step 1: Selection of QoS performance affecting metrics

Here achieving the QoS performance is considered as the prey and the nine performance metrics or factors those affecting the QoS more are selected and considered as hunters. Each hunter is represented with a unique fitness function (FF). The metrics that affecting QoS more are placed into the central pack i.e. Throughput, and PDR. Out of the rest metrics, PLR and DR and Retx are categorized into left pack and $D_{EL,}$ D_{VD}, D_{QE}, Q_{Occp} are assigned to the right pack.

Step 2: Estimation of initial QoS

The initial QoS (QoS_0) is calculated using equation (6.5).

$$QoS_0 = (\sum_{n=1}^{N} FF_n)/N \tag{6.5}$$

where QoS_0 is the initial QoS, FF_n is the initial value of the n^{th} fitness function or metrics which affecting QoS, N denotes total number of metrics participated in achieving required QoS i.e. N=9.

Step 3: Updation of QoS

During monitoring time, the fitness function value of each metric is updated according to the changes in the system; hence the QoS is also changes with these. It means that QoS may deviate from system's requirement or the difference between actual and expected QoS may increase or vice versa. If the current fitness function value of the metric is better than the previous value, then there is a chance that QoS gets increased, otherwise, QoS may degrade. The actual difference between the expected and the actual QoS will be obtained by using equation (6.6).

$$QoS_i^{k+1} = QoS_i^k + C * r(0,1) * (QoS_i^k - FF_i^k) \tag{6.6}$$

where QoS_i^{k+1} denotes the new difference between actual and expected measure of QoS factor i, QoS_i^k is the old difference, FF_i^k is the new value of fitness function i at k^{th} iteration, r(Low, High) is defined the random number generation function which generates a random number in between Low and High range. C defines the percentage of improvement in the fitness function.

Step 4: Updation in highly affecting fitness function

At the time of achieving the QoS, the fitness function value of each metric is updated. The new fitness function value of a metric belongs to the central pack is calculated using equation (6.7).

$$FF_i^{k+1} = \begin{cases} r\left(FF_i^k, QoS_i^k\right), if\ FF_i^k < QoS_i^k \\ r\left(QoS_i^k, FF_i^k\right), if\ FF_i^k > QoS_i^k \end{cases} \quad (6.7)$$

where FF_i^k is current fitness function value of metric i and FF_i^{k+1} new fitness function value of metric i.

Step 5: Updation in other fitness function

The new fitness function value of a metric belongs to either the left or right pack, is calculated with the help of equation (6.8).

$$FF_i^{k+1} = \begin{cases} r\left(\left(2 * QoS_i^k - FF_i^k\right), P_i^k\right), \ if\left(2 * QoS_i^k - FF_i^k\right) < QoS_i^k \\ r\left(QoS_i^k, \left(2 * QoS_i^k - FF_i^k\right)\right), \ if\left(2 * QoS_i^k - FF_i^k\right) > QoS_i^k \end{cases} \quad (6.8)$$

where QoS_i^k is the required QoS, FF_i^k, FF_i^{k+1} are the old and new fitness function values for i^{th} metric.

Step 6: Termination

The steps from 1-5 are repeated until termination criteria is achieved. Here the monitoring time is considered as the stopping criteria of the iteration. When the termination criteria met, the desired QoS will be obtained.

The flowchart and algorithm for QoS optimization module of OMDPPH protocol is mentioned in Figure 6.5 and Algorithm 6.1.

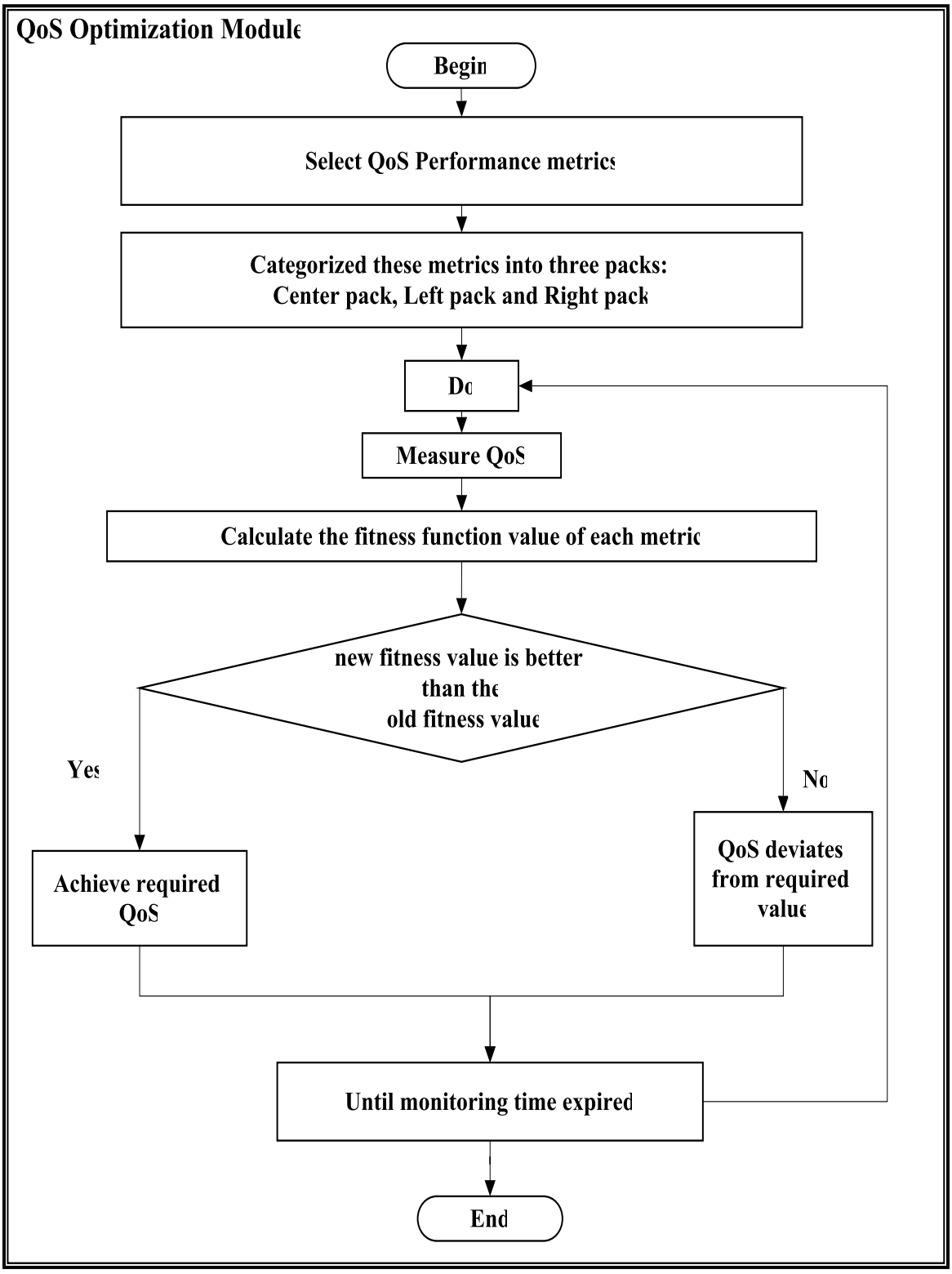

Figure 6.4 Workflow Diagram of the QoS Optimization Module

Algorithm: QoS Optimization

Input: *Formulas for fitness functions, Monitoring time, Constraints, Variables*
Output: *Optimal QoS performance measures*

1. *Initialize the monitoring time MT // for number of iterations*
2. *Select fitness functions FF_i, i = 1, 2 ...n // (i.e. n = 9, defines the number of metrics)*
3. *Initialize three sub-packs: Central pack =0, Left pack =0, Right pack=0*
4. *Divide and categorize fitness functions into above three packs*
5. *Find initialize QoS_0 using* ***Equation (6.5)***
6. *Set k=0*
7. ***While*** *(k<= MT),* ***Do*** *// Update the fitness function*
   - *7.1.* ***For*** *each FF_i,* ***Do***
     - *7.1.1. Calculate new fitness function value of metric i using* ***Equation (6.7-6.8)***
     - *7.1.2.* ***If*** *the new fitness value is better than the previous value,* ***Then***
       - *7.1.2.1. Update fitness value with new value*
       - *7.1.2.2. Change of achievement of required QoS gets increased*
     - *7.1.3.* ***Else***
       - *7.1.3.1. Change of deviation of required QoS gets increased*
       - *7.1.3.2. Find new QoS measures using* ***Equation (6.6)***
     - *7.1.4.* ***End If***
   - *7.2.* ***End For***
   - *7.3. k ++*
8. ***End While***

Algorithm 6.1 Algorithm for QoS Optimization using LGH Technique

The LGH algorithm restructures the QoS performance metrics and optimizes the QoS to an optimum point for a dynamic system where the QoS performance metrics fluctuate with respect to the change in system over time.

6.3 SUMMARY

In this chapter, a protocol for optimization of QoS performance in DWBAN is discussed. It first exhibited its interest towards high level of versatility and robustness when the WBAN system was very dynamic. Next, its focus is on tackling multi-objective QoS

problems in a dynamic WBAN. Nine objective functions were employed in order to benchmark the contributions of the proposed protocol in terms of exploration, exploitation, local optima avoidance, and convergence. The results show that the LGH is one of the ablest optimization techniques to provide highly ambitious results compared to others in terms of various performance metrics like the loss, delay, throughput etc. Finally, it concludes that LGH optimization algorithm is a reliable technique for improving QoS with multiple objectives of QoS in DWBAN. A large number of performance metrics further strengthen the capability of the DWBAN.

CHAPTER 7

SIMULATION AND PERFORMANCE EVALUATION

7.1 INTRODUCTION

Simulator tool provides the easiness to evaluate the functionality of required process. Instead of using real test beds, it helps in creating virtual networks, performing the test, optimizing and integrating new technologies. In enormous scenarios, new protocols can be established and verified easily with the use of simulator. To analyze the proposed DWBAN system, an experimental analysis is conducted in a network simulator NS-2, which helps to evaluate the various QoS performance parameters of DWBAN under various network conditions. This chapter briefly describes the simulation environment and various aspects considered to perform the simulation.

7.2 THE NETWORK SIMULATOR (NS-2)

NS-2 [126] is a kind of discrete event simulator that assists for analysis during dynamic communication in a network. It basically consists of two different languages; C++, and OTcl (an Object Oriented extension of Tcl (Tool Command Language)). The C++ language is used for detailed protocol implementation which runs faster but takes more time to change the code. On the other hand, the interpreter OTcl is act as a command and configuration interface, which can be easily modified or change but takes more time for execution. The whole simulation (i.e. topology of the network, modules and their associations, protocols, patterns of outputs etc.) is designed through OTcl coding which helps to execute users command. After the execution or run of the Tcl coding, it produces the output in the form of a trace file. These outputs can be representing graphically as well as interactively, using additional tools such as NAM (Network AniMator) [127], AWK [129], and Xgraph [128] as illustrated in Figure 7.1. The main job done by a trace file is to record the details of the flow pattern during the simulation, which can further illustrated as a text-based packet tracing or an animation-based packet tracing. The AWK

is a language used for text-based packet tracing. It is a file having sequence of statements which explains kind of action that should be performed at a specific time. The NAM is an animation tool provides graphical representation of simulation traces. It basically provides a visual interpretation of the network created and can be executed directly from a Tcl script. Finally, Xgraph is used to analyze trace files created during simulation.

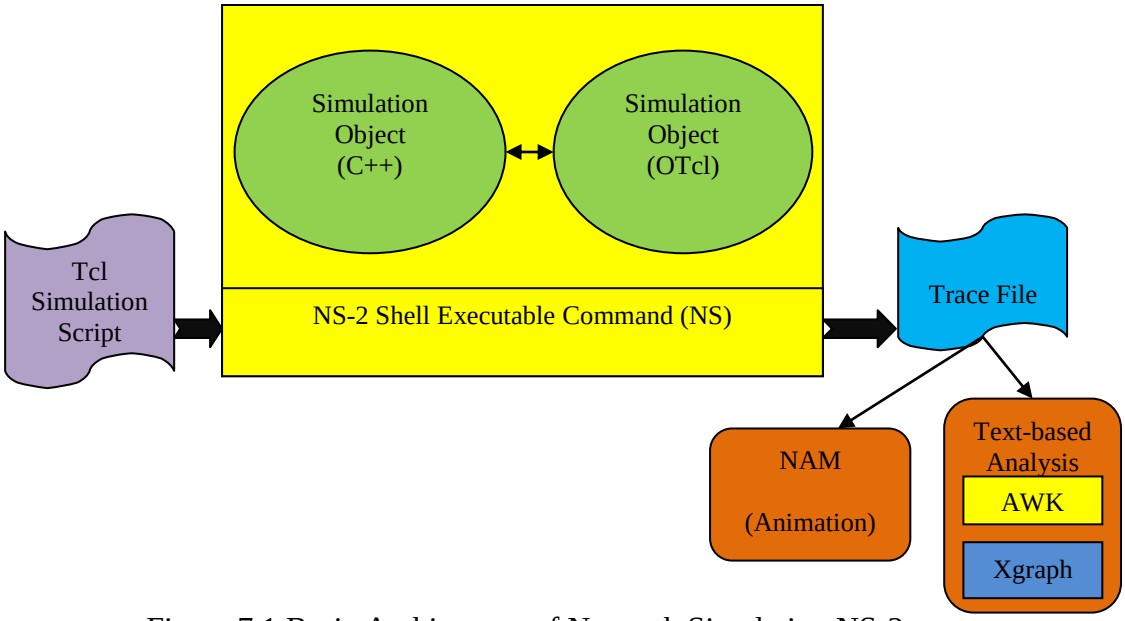

Figure 7.1 Basic Architecture of Network Simulation NS-2

7.2.1 QoS Performance Metrics

The simulation results are obtained under several experiments. The outcomes of the proposed protocols will be compared with the outcomes of the OCMP [71] and ERMDT [75] protocols using Xgraph. The performance of the proposed protocols is evaluated based on the following metrics.

I. Packet Delivery Ratio (PDR)

The total number of packets successfully received at the CU is called as packet delivery ratio. It represents the ratio between the number of packets received by the CU and the number of packets generated by the source sensor nodes. The packet delivery ratio can be illustrated by equations (7.1-7.5).

$$Generated_{Tx}^{S_n} = \sum_{i=1}^{I} Generate\_Counter_i \quad (7.1)$$

$$Generated_{Tx}^{Total} = \sum_{n=1}^{N} Generated_{Tx}^{S_n} \quad (7.2)$$

$$Received_{Tx}^{S_n} = \sum_{i=1}^{I} Receive\_Counter_i \quad (7.3)$$

$$Received_{Tx}^{Total} = \sum_{n=1}^{N} Received_{Tx}^{S_n} \quad (7.4)$$

$$PDR = \frac{Received_{Tx}^{Total}}{Generated_{Tx}^{Total}} * 100 \quad (7.5)$$

where $Generated_{Tx}^{Sn}$, and $Received_{Tx}^{Sn}$ define the of packets generated and received for a particular sensor node. $Generated_{Tx}^{Total}$, $Received_{Tx}^{Total}$ denote the total number of packets generated and successfully received, Receive_counter denotes the counter for packet reception, S_n denotes the sensor node, I denotes the total number of packets, N provides the total number of sensor nodes.

II. Packet Loss Ratio (PLR)

The packets get lost in transit due to various factors such as bad or weak radio signals, longer transmission distance, faulty links or channels. PLR is defined as the ratio between the numbers of packets lost to the number of packets generated by the source sensor nodes. Formulas given in equations (7.6-7.8) help during the calculation of packet loss rate.

$$Loss_{Tx}^{S_n} = \sum_{i=1}^{I} Loss\_Counter_i \quad (7.6)$$

$$Loss_{Tx}^{Total} = \sum_{n=1}^{N} Loss_{Tx}^{S_n} \quad (7.7)$$

$$PLR = \frac{Loss_{Tx}^{Total}}{Generated_{Tx}^{Total}} * 100 \quad (7.8)$$

where $Loss_{Tx}^{Sn}$, $Lost_{Tx}^{Total}$ is the packet loss of a sensor node and total packet loss during transmission, Loss_Counter denotes the counter for packet loss, S_n denotes the sensor node, I denote the counter for packets, N provides the total number of sensor nodes.

III. Drop Ratio (DR)

Packet drop occurs in various situations such as packet gets dropped during congestion due to queue overhead, packets drop during scheduling when deadline exceed, packet

drop during redundant packet elimination etc. Equations (7.9-7.11) provide the calculation process of total packet drop rate in the network.

$$Loss_{Drop}^{S_n} = \sum_{i=1}^{I} Drop\_Counter_i \quad (7.9)$$

$$Loss_{Drop}^{Total} = \sum_{n=1}^{N} Loss_{Drop}^{S_n} \quad (7.10)$$

$$DR = \frac{Loss_{Drop}^{Total}}{Generated_{Tx}^{Total}} * 100 \quad (7.11)$$

where $Loss_{Drop}^{Total}$, $Loss_{Drop}^{Sn}$ defines the total packet drop and packet drop of a sensor node, Drop_Counter denotes the counter for packet loss, S_n denotes the sensor node, I denote the counter for packets, N provides the total number of sensor nodes.

IV. Elapsed Time Delay (D_{EL})

Elapsed time delay represents the communication delays between two end-points and occurs if the packet is delivered after its expected time. This can be calculated by applying equations (7.12-7.14).

$$D_{EL}^{i} = \begin{cases} D_{AD}^{i} - D_{AD}^{i}, & if\ D_{AD}^{i} > D_{AD}^{i} \\ 0, & if\ D_{AD}^{i} \leq D_{AD}^{i} \end{cases} \quad (7.12)$$

$$D_{EL}^{S_n} = \sum_{i=1}^{I} D_{EL}^{i} \quad (7.13)$$

$$D_{EL}^{Total} = \sum_{n=1}^{N} D_{EL}^{S_n} \quad (7.14)$$

where D_{EL}^{i} defines the elapse time delay of the incoming packet i, D_{EL}^{Sn} denotes the total elapsed time for a particular sensor node or for one link, D_{EL}^{Total} denotes the total elapsed time for all sensors or all links, D_{AD} denotes the time when packet i actually arrived at the CU, D_{ED} denotes the expected delivery time of a packet i of sensor S_n.

V. Variation in the Elapsed Time Delay (D_{VA})

Variation in the elapsed time occurs when delay varies over time. The variation in elapsed time delay can be illustrated by the equations (7.15-7.17).

$$D_{VA}^{i} = D_{EL}^{i} - D_{EL}^{i-1} \quad (7.15)$$

$$D_{VA}^{S_n} = \sum_{i=1}^{I} D_{VA}^{i} \quad (7.16)$$

$$D_{VA}^{Total} = \sum_{n=1}^{N} D_{VA}^{S_n} \quad (7.17)$$

where D_{VA}^{i} defines the actual difference between two consecutive elapsed times, D_{VA}^{Sn} denotes the total variance in elapsed time for a particular sensor node; D_{VA}^{Total} denotes the total variance in elapsed time for all sensor node.

VI. Queuing Delay (D_{QE})

The queuing delay represents the waiting time of a packet in a queue during packet scheduling. It can be more elaborated by defining as the time gap between the packet arrival time and the packet servicing or scheduling time. The equations (7.18-7.20) are used for the calculation of total queuing delay.

$$D_{QE}^{i} = D_{AD}^{i} - D_{FD}^{i} \quad (7.18)$$

$$D_{QE}^{S_n} = \sum_{i=1}^{I} D_{QE}^{i} \quad (7.19)$$

$$D_{QE}^{Total} = \sum_{n=1}^{N} D_{QE}^{S_n} \quad (7.20)$$

where D_{QE}^{Sn} denotes the total Queuing time of a sensor node, and D_{QE}^{Total} denotes the total queuing time for all links, D_{QE}^{i}, D_{FD}^{i} and D_{AD}^{i} are the queuing delays, forwarding time and arrival time for packet i.

VII. Queue Occupancy (Q_{Occup})

Queue occupancy provides the actual status of the queue and is an essential factor to overcome packet drop issues occurs during congestion. The value of queue occupancy metric can be calculated using equation (7.21-7.22).

$$Queue_{Counter} = \begin{cases} Queue_{Counter} + 1, & when\ packet\ enqueue \\ Queue_{Counter} - 1, & when\ packet\ dequeue \end{cases} \quad (7.21)$$

$$Q_{Occp} = \frac{Queue_{Counter}}{Queue_{Size}} \quad (7.22)$$

where $Queue_{Occupancy}$ denotes the total number of packets present in the queue,$Queue_{Size}$ is the size of the queue provides the idea about how many packets can be stored in a queue, $Queue_{Counter}$ defines the total number of packets present in the queue.

VIII. Retransmission Ratio (Retx)

The retransmission rate is calculated by measuring the packets those are received more than once at the CU. The retransmission rate can be calculated from the formula given in equations (7.23-7.25).

$$Retx_{Tx}^{S_n} = \sum_{i=1}^{I} Retx\_counter_i \quad (7.23)$$

$$Retx_{Tx}^{Total} = \sum_{n=1}^{N} Retx_{Tx}^{S_n} \quad (7.24)$$

$$Retx = \frac{Retx_{Tx}^{Total}}{Received_{Tx}^{Total}} * 100 \quad (7.25)$$

where $Retx_{Tx}^{Sn}$, $Retx_{Tx}^{Total}$ defines the retransmission rate of a sensor node and total retransmission rate, Retx_Counter counts the number of packets transmitted repeatedly, S_n denotes the sensor node, i denotes the counter for packets, N provides the total number of sensor nodes.

IX. Throughput (Throughput)

The throughput of a network is measured in terms of successful delivery of packets within the threshold or simulation time. The equation (7.26) provides the formula for the calculation of the network throughput.

$$Throughput = \frac{(Received_{Tx}^{Total}) * Packet_{size} * 8}{Total_{Simulation\_Time}} \quad (7.26)$$

where $Total_{Simulation\_Time}$ denotes the total simulation time when packets are generated and transmitted from all sensor nodes to the CU, and $Packet_{Size}$ is the size of a packet.

7.2.2 Network Parameters

The QoS performance metrics have to be measured against some parameter that describes the characteristic behavior of the proposed system and can be varied in a controlled way.

i. Sensor Node: The number of sensor nodes takes part for data transmission during the simulation can be varied and the test will be performed on various sensor nodes.

ii. Simulation Time: The time for which the simulations will be run is called as simulation time. The simulation time can be varied according to the requirements.

iii. Data Rate: The Data Rate in a network defines how many packets can be transmitted per second. According to the load handling capacity of a network, its value can be changed.

iv. Packet size: Packet size can be changed with varying network load.

7.3 SIMULATION SETUP

The implementation of proposed protocols is carried out in the network simulator ns-2.35 [129] based on the precise scenarios given below. During simulation, the sensor node density is varied from 2 to 20 nodes within a fixed topological territory of dimension 5m x 5m, representing a single patient. The simulation takes place for a time period of 120 seconds with the 802.15.4 based MAC protocol, configured for wireless mode. In this simulation, parameters are configured for the performance evaluation of constant bit rate (CBR) traffic with a packet size of 70 bytes. The simulation setup for performance evaluation of the proposed systems with respect to variation in a number of nodes is given in Table 7.1.

Table 7.1Simulation Setup Parameters

Parameter	**Values**
No. of Nodes	5-15
Area Size	5 * 5 m^2
MAC	802.15.4
Transmission Range	1-7 m
Propagation	Two Ray Ground
Antenna	Omni
Queue length	150 packets
Packet Size	70 bytes
Bandwidth	250Kbps
Simulation Time	120 sec
Traffic Source	CBR

The QoS adopted here is modeled in such a simplified way so that it can provide an efficient simulation framework for the analysis of various performance metrics which may influence the QoS of the WBAN than the existing protocols. All of our simulations were run 120 seconds for each simulation. Each simulation configuration is run 5 times and results are averaged and presented in Xgraphs.

7.3.1 Snapshots of Simulation Process

Step-1:The simulation model of the proposed system will be written and save in a file with extension ".tcl" using TCL programming language as shown in Figure 7.2.

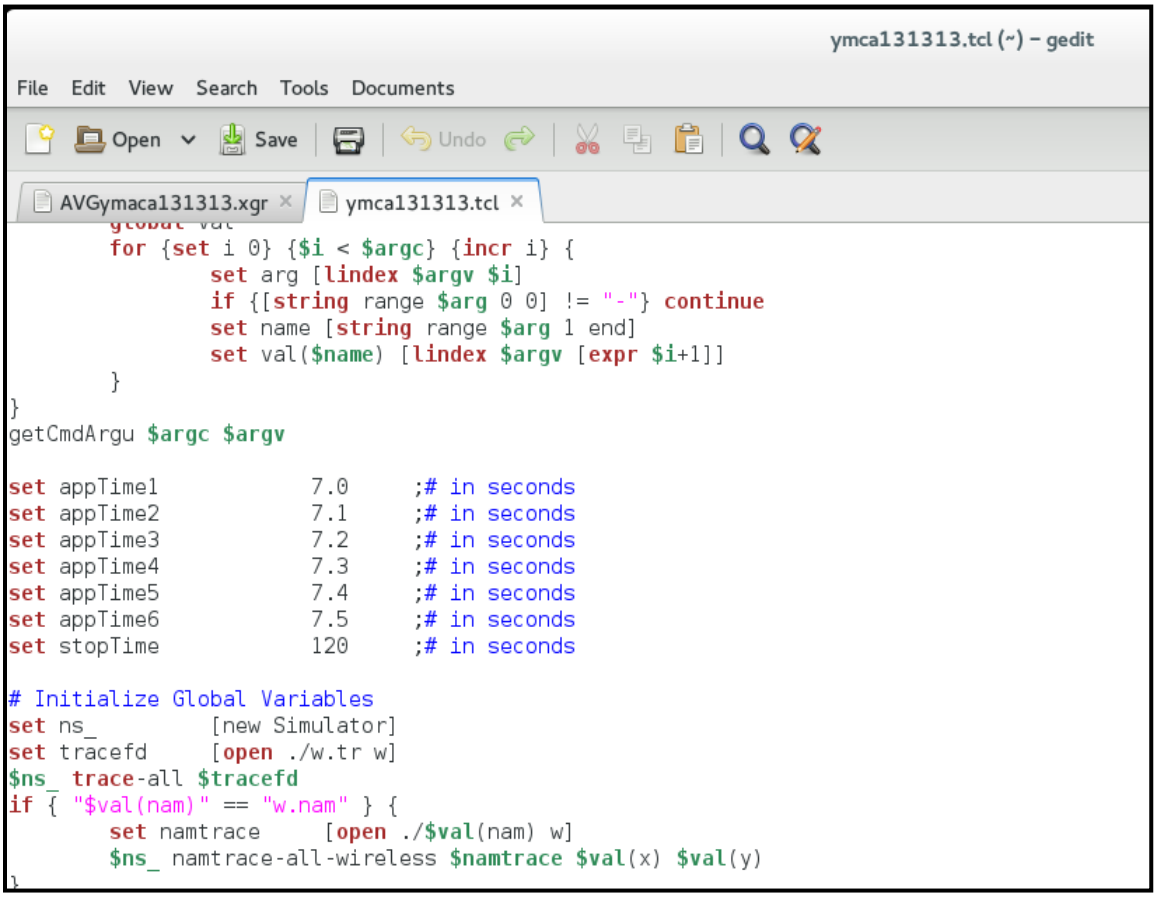

Figure 7.2 TCL Coding for Simulation Model

Step-2: After running the file, it will generate two files. A NAM file and a Trace file as shown in Figure 7.3 and Figure 7.4. Where the NAM file provides the animation for the network while the Trace file provides the details of the back-end post-process in a text format.

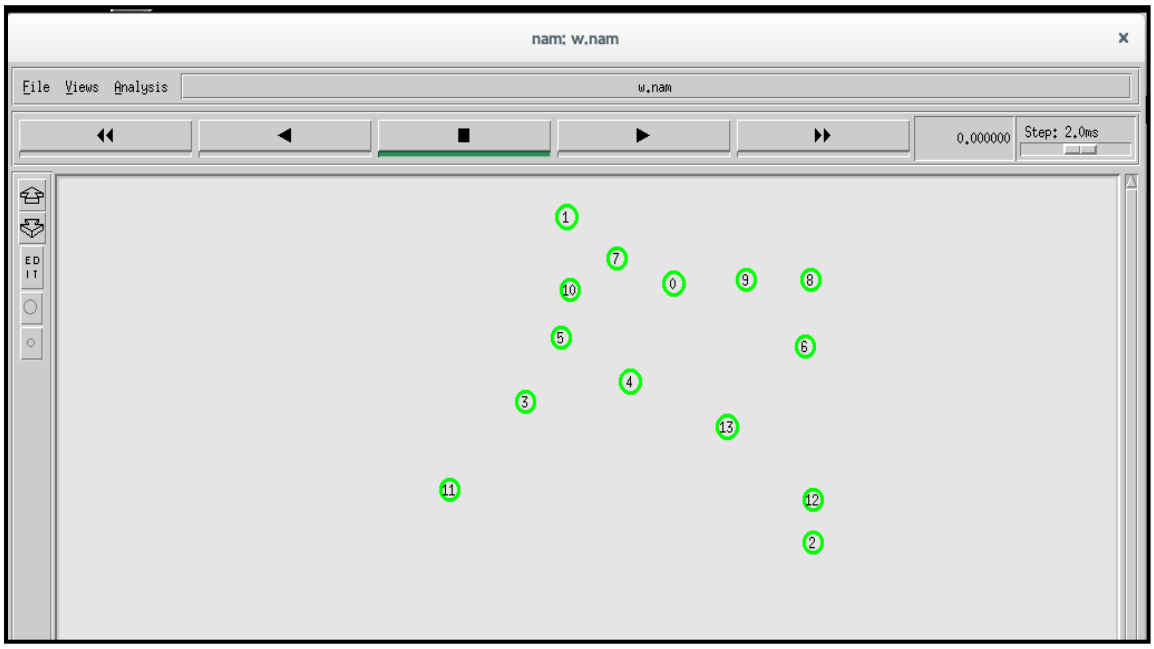

Figure 7.3 Topological graph of simulation model using NAM

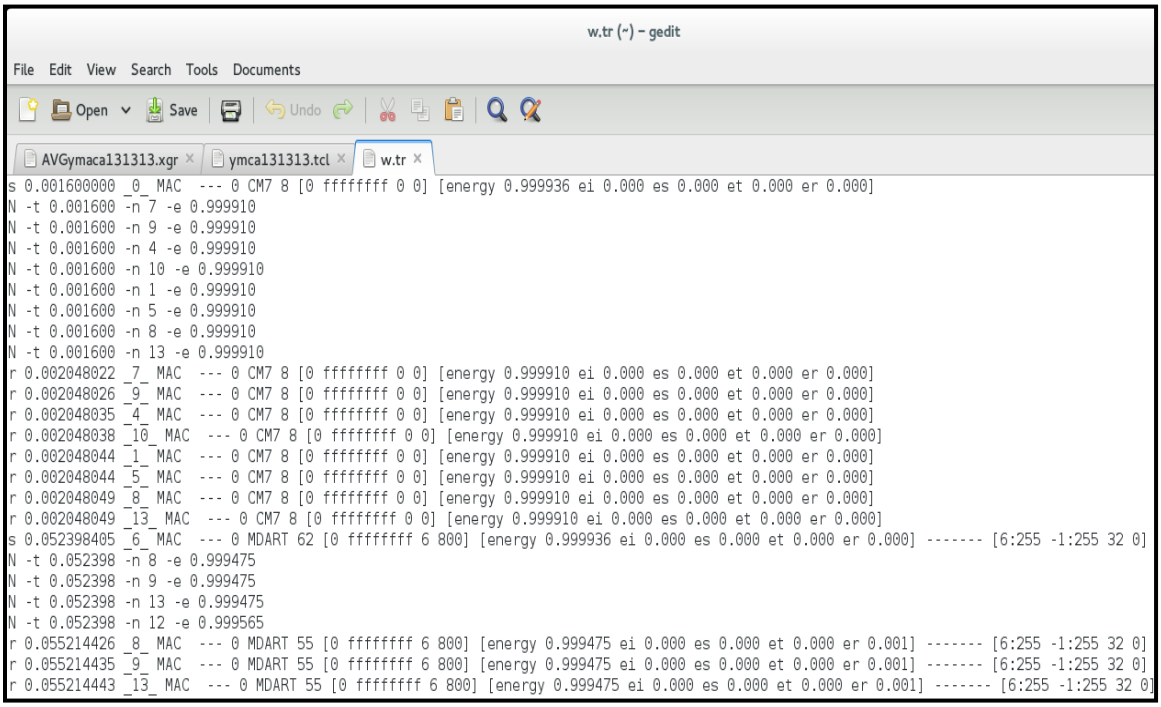

Figure 7.4 Trace file describes the output of Simulation

Step-3: The AWK file (".awk" extension) as given in Figure 7.5 while run, extracts data from the trace file, performs actions as given in this file, and finally, generates output results for all the performance metrics as illustrates in Figure 7.6.

```
BEGIN {
        recvdSize = 0
        startTime = 400
        stopTime = 0
status=0;
#*******************************
seqno = -1;

      droppedPackets = 0;

      receivedPackets = 0;

      count = 0;
status=1;
t1=0;
t2=0;
chk=0;
start=0;
end=0;
ret_coun=0;
end_c=0;
stop=0;
```

Figure 7.5 AWK Coding to generate output

```
set val(nam)
set val(traffic)

#read command line argume
proc getCmdArgu {argc ar
        global val
        for {set i 0} {$
                set arg
                if {[str
                set name
                set val(
        }
}
getCmdArgu $argc $argv

set appTime1
set appTime2
set appTime3
```

```
File  Edit  View  Search  Terminal  Help
 GeneratedPackets              = 2426
 ReceivedPackets               = 2125
 Packet Delivery Ratio         = 87.5927%
no of Packet drop               = 664
 no of Packet Loss ratio        = 301
 Packet Loss ratio              = 12.4073%
Packet Dropped ratio            = 14.9629%
 Average End-to-End Delay       = 1.43342ms
Average variation Delay         = 0.718319 ms
Queuing Delay                    =  0.0295035 ms
Queuing Occupancy                =  0.30466
retrarnsmission                   = 50.239%
 Throughput                     = 4.89 Kbps


[madhu@localhost ~]$
```

Figure 7.6 Generated results

Step-4: Now this output data can be considered for the generation of Xgraphs for further analysis of each performance metric.

7.3.2 Simulation Results and Analysis

Comparative analysis of performance comparisons between proposed protocols and existing protocols (OCMP, ERMDT) is done in this section. All the proposed protocols are compared with respect to number of nodes. If the number of nodes in a given area is increased, then node density increases, which further give rise to other problems like congestion, interference, delay etc. In this scenario, the simulation runs 5 times, and an average of these readings will consider for getting an estimation of the network performance for all the scenarios. The simulation will run with constant parameters like data rate, packet size, simulation time etc., and the performance metrics will be observed for the variations in the sensor node.

- **Packet Delivery Ratio:** The total number of packets received at the CU will help in calculation of packet delivery ratio.

Figure 7.7 Comparison analysis graph of Packet Delivery Ratio

It has been observed from Figure 7.7 that more numbers of packets are delivered from source to destination in the proposed protocols with increasing number of nodes. DPPH has offered 2% to 4% growth in PDR as compared to ERMDT and

OCMP protocols. The proposed dynamic priority based bandwidth sharing, data transmission rate, classification and scheduling policies help in increasing delivery rate in DPPH. In extension to DPPH, the MDPPH works on loss recovery, flow, and congestion control and provided 4% more delivery rate than the DPPH protocol. The quick start and fractional increased and decreased based rate adjustment policies of MDPPH perform efficiently in a dynamic environment than the OCMP and ERMDT and utilizes bandwidth in more efficient way. This further provides a growth of 6% to 10% in PDR over ERMDT and OCMP. The use of LGH optimization technique in OMDPPH protocol helps in maximizing the packet delivery rate with a rate of 14% more in comparison to ERMDT, 10% more than OCMP, 8% more than DPPH and 4% more than MDPPH.

- **Packet Loss Ratio:** When number of packets lost in the system during transmission increases, it becomes a critical factor for QoS.

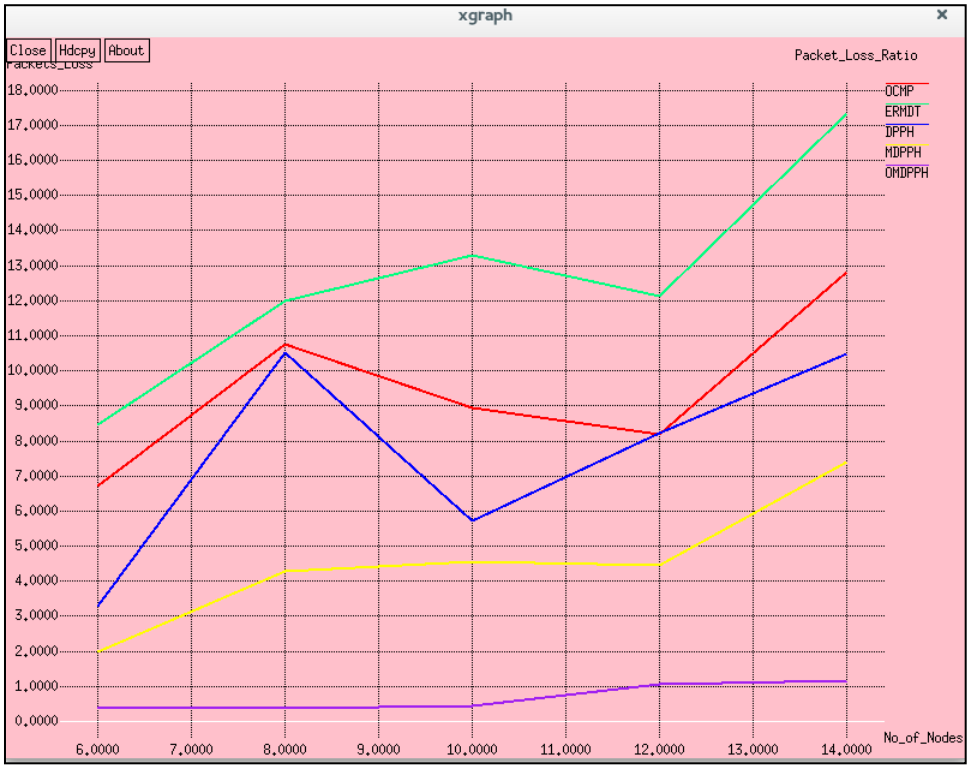

Figure 7.8 Comparison analysis graph of Packet Loss Ratio

The Figure 7.8 shows that the loss ratio of DPPH is comparatively lesser than in OCMP, and ERMDT. In OCMP large amount of packets drop due to buffer overflow with an increase in the number of nodes, as a result, the loss rate increases. ERMDT resolves this issue with an alternate path and rate adjustment policies during congestion, but does not consider the loss during transmission. The DPPH protocol improves the performance of the PLR with the same rate as specified during PDR. MDPPH improves the performance of the system by reducing the number of packet loss more than DPPH. The OMDPPH is also helpful in reducing drop at a better rate as compared to rest four protocols.

- **Packet Drop Rate:** Packet drop occurs in various situations such as congestion due to queue or buffer overhead, during scheduling when deadline exceeded, during redundant packet elimination.

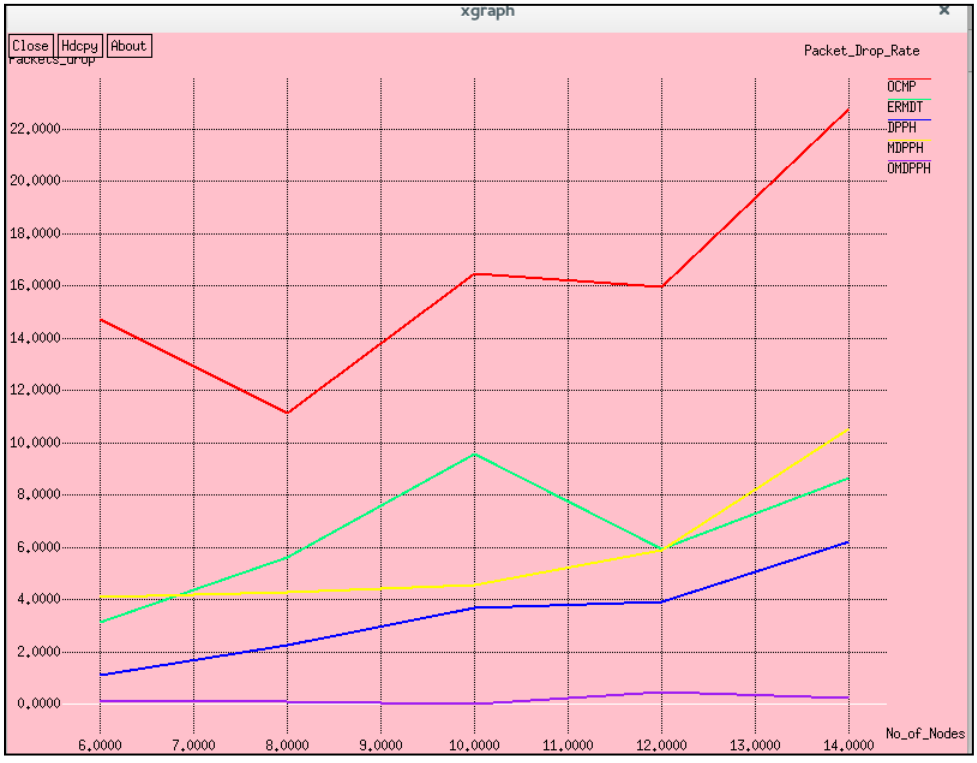

Figure 7.9 Comparison analysis graph of Packet Drop Rate

Figure 7.9 shows the comparison of packet drop rate with respect to increase in the number of sensor nodes. It has been observed that DPPH and MDPPH

experience minimum packet drop for high priority packets. In OCMP, flows are treated equally during packets dropped, which deteriorates the performance of OCMP. While ERMDT offers a controlled drop rate. During whole simulation, the OCMP drops 60% more packets than the ERMDT and the ERMDT have 10% more drop rate as compared to MDPPH. While the packet drop rate of MDDPH protocol has 42% more than the DPPH. The reason behind this is that DPPH considers the packets drop during queueing and scheduling while the MDPPH takes into account packets drop during scheduling, congestion, and duplicate packet mitigation, queuing and scheduling. In addition to this, MDPPH completely eliminates the drop of high priority or emergency packets. While the OMDPPH protocol reduces the packets drop rate up to 97% less than OMDPPH.

- **Elapsed Time Delay:** The Elapsed time delay in a network will take into account when the packet delivers to the receiver after its expected arrival time. It degrades the total end-to-end delay; make a packet delivered after its expected time.

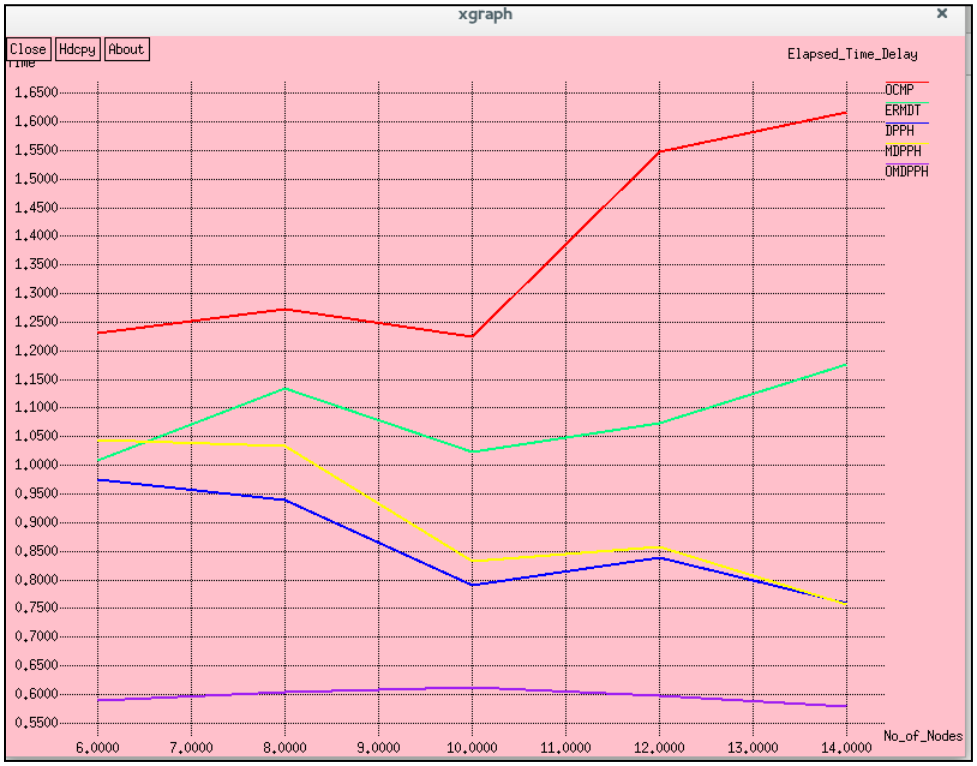

Figure 7.10 Comparison Analysis Graph of Elapsed Time Delay

The graph in Figure 7.10 shows that performance of DPPH increases in terms of delay reduction with an increase in number of sensor nodes than the OCMP, and ERMDT. Its REDF scheduling methods efficiently reduce more amount of delay as compared to others. The packet transmission time gap and transmission rate of DPPH protocol helps in decreasing elapsed time delay nearly 79% less than OCMP and 21% less than ERMDT. The drop rate in OCMP is relatively high which further increases the retransmission rate proactively. While ERMDT handles delay up to some extent with its retransmission policy, but still not perfect for the dynamic WBAN system. Due to high retransmission rate, these protocols face high congestion and delay. The MDPPH minimizes delay 5% less than DPPH by its selective packet retransmission and loss recovery policy. OMDPPH protocol dynamically adjusts this parameter and causes lesser packet transmission delay which is 35% less than MDPPH.

- **Variation in Elapsed Time Delay:** Variation in the elapsed time occurs when elapsed time delay varies over time.

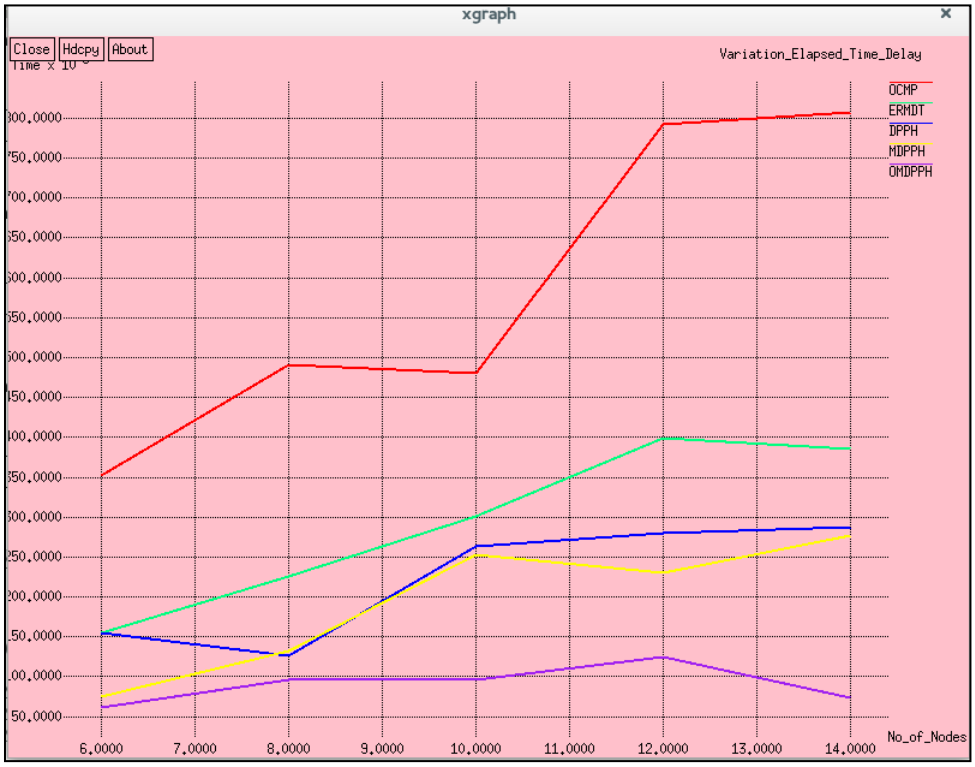

Figure 7.11 Comparison analysis graph of Variation in Elapsed Time Delay

As stated earlier, another factor which hampers the QoS is variation in elapsed time delay (VD). The variation in elapsed time delay, shown in Figure 7.11, directly depends on the elapsed time delay rate. The variation in elapsed time delay in DPPH is 62% less than OCMP and 24% less than ERMDT. As it was previously illustrated that the decrease in a delay in MDPPH is due to the fact of reduction in retransmission rate and congestion in it, which also reduces the variation in elapsed time delay with a percentage of 13% less than DPPH. Considering the optimization, the OMDPPH has attained 53% reduction in VD as compared to MDPPH.

- **Queuing Delay:** The large waiting time period during the scheduling of packet gives rise to queuing delay in a system.

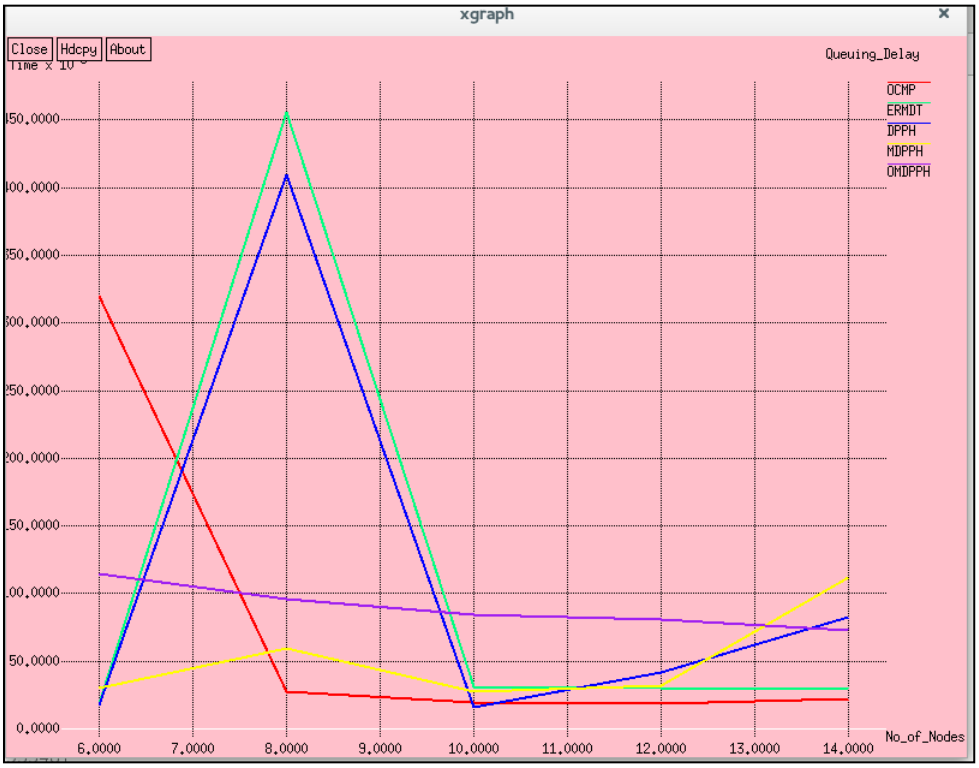

Figure 7.12 Comparison analysis graph of Queuing Delay

Figure 7.12 shows that the queuing delays with respect to number of nodes. The queuing delay experienced by DPPH and ERMDT protocols are almost same when node value is 8 and is more than the OCMP protocol. The queuing delay of

all the five protocols is nearly same when the node value varies from 10-14. In OCMP and ERMDT, the mean queuing delay is significantly reduced as compared to DPPH and MDPPH. The OCMP and ERMDT use single-queue discipline that does not differentiate between various types of flow. In a large size network, with increasing node, the single-queue scheduling approach faces a large starvation that causes queuing delay problem. The DPPH protocol having priority and rate based scheduling handles the queueing delay problem up to a large extent in a large network. The MDPPH and OMDPPH protocols are also able to minimize queueing delay as more as possible during the large network size and are remain stable throughout the whole simulation. While for others, this value is oscillated with number of nodes.

- **Queue Occupancy:** The amount of packets present in a queue provides the idea about queue occupancy.

Figure 7.13 Comparison analysis graph of Queue Occupancy

Comparison of queue occupancy as QoS performance is shown in Figure 7.13. It indicates that OCMP significantly has low queue occupancy than ERMDT, DPPH and MDPPH protocols. The OCMP is having an average of 24% less queue occupancy than these three. The MDPPH protocol provides 7% less queue occupancy than the DPPH and 5% less than ERMDT. The OMDPPH protocol is having 97% less queue occupancy than MDPPH.

- **Retransmission Rate:** The retransmission rate is calculated by measuring the packets that are received more than once at the CU.

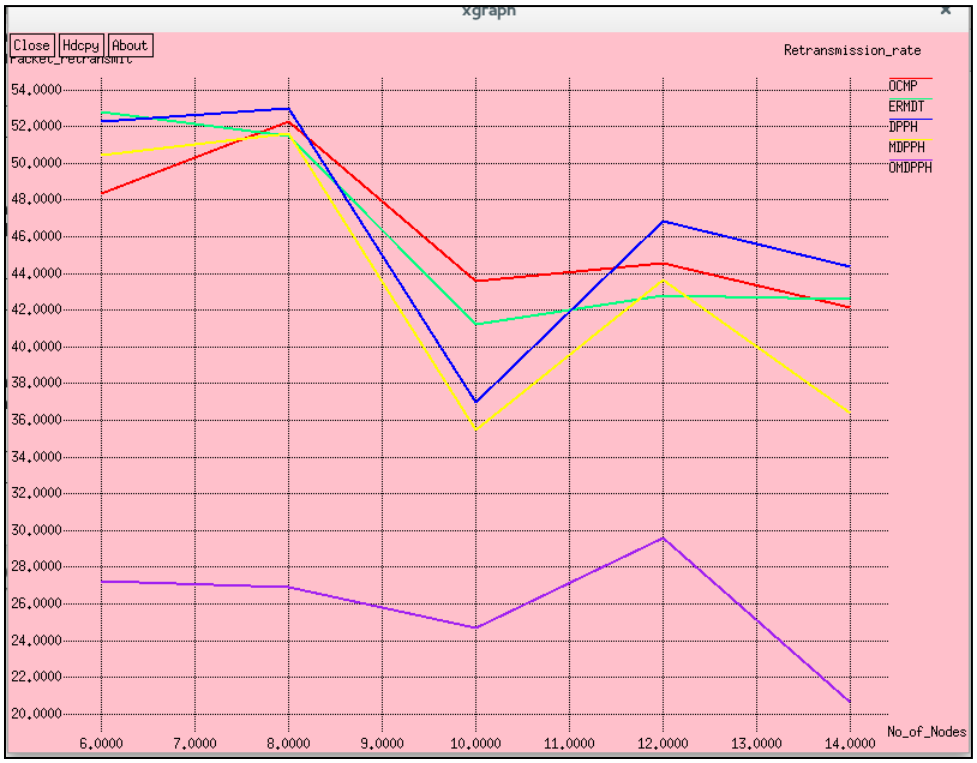

Figure 7.14 Comparison analysis graph of Retransmission Rate

Figure 7.14 illustrates the comparison analysis for the retransmission rate. As depicted from the graph, it is clear that the overall retransmission rate of all the proposed protocols have reduced a lot as compared to the existing ones. The variation in retransmission rate is not constant and oscillates rapidly during the simulation period. The reduction in the number of unnecessary retransmissions further reduces variations in elapsed time as well as queuing delay. For instance,

it would result in the reduction of end-to-end delays and lower resource consumption. The average retransmission rate of OCMP, ERMDT, DPPH are nearly same i.e. 46%. While the retransmission rate of the MDPPH protocol is about 8% less than these three protocols. This happened only because of selective retransmission approach and its rate adjustment policies. The OMDPPH protocol is providing 41% less retransmission rate as compared to MDPPH.

- **Throughput:** Throughput of a network is calculated by the total number of receiving packets per simulation time period. It can be also defined as the packet delivery rate over the total bandwidth.

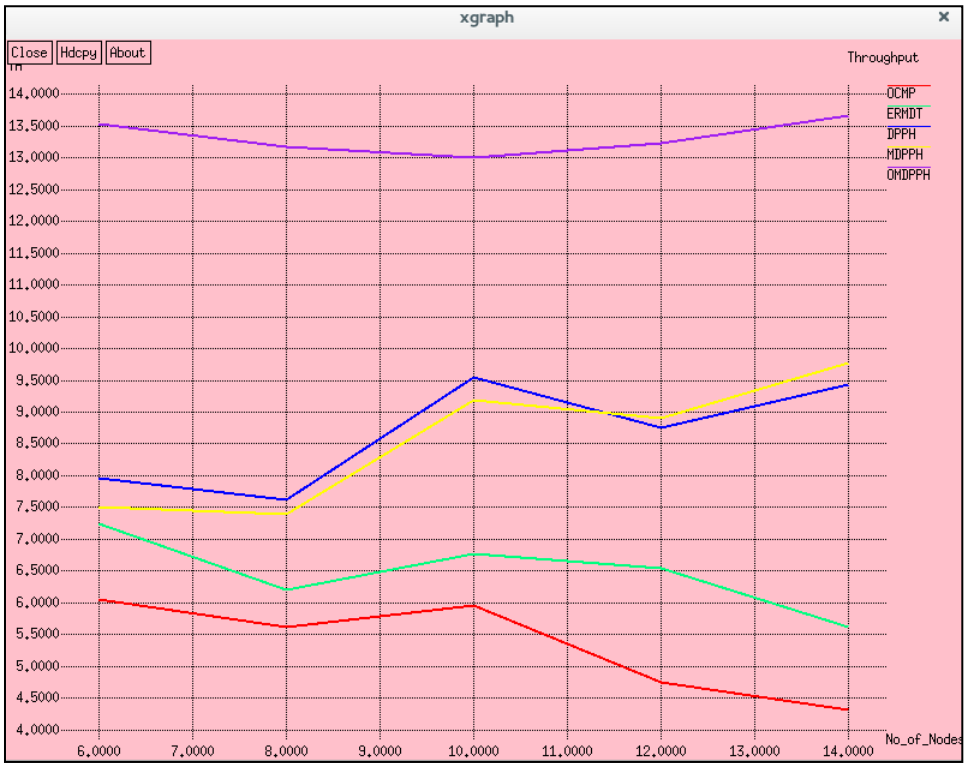

Figure 7.15 Comparison analysis graph of Throughput

Another significant factor of QoS is the throughput which defined as the total data packets received per monitoring time. The comparison results for the network throughput with respect to the variation in a number of nodes are shown in Figure 7.15. It has been observed that the OMDPPH protocol gives better results than others in terms of throughput during the whole simulation. It is also observed that the proposed protocol

amplifies the system throughput in an amazing way. The reason behind this is its packet reordering and redundant packet eliminations techniques. The throughput of OCMP and ERMDT are not constant during the complete simulation period. While the throughput of proposed DPPH and OMDPPH protocols are almost constant and they provide guaranteed throughput. In both light and dense scenarios, the proposed techniques show remarkable performance with notable improvements. This is mainly due to the resulting number of packet loss and the packet delivery ratio. The throughput of OCMP is 5Kbps which is 17% less than the throughput of ERMDT which is 6.5Kbps. Both DPPH and MDPPH achieves nearly equal amount of throughput on average i.e. 8-9Kbps which is 34 to 35% more than ERMDT. OMDPPH provides about 54 to 55% more throughput than the MDPPH and the DPPH i.e. 13.50Kbps.

7.3.3 Comparison Analysis of QoS Performance Metrics

The simulation results for all the QoS performance metrics are illustrated in Table 7.2. The results show the average value of total five simulation runs for node 6, 8, 10, 12, and 14 and it demonstrates that, proposed protocols show better performance than others. This table shows the step by step improvements in each protocol due to its contributions to the proposed system.

Table 7.2 Comparison Table for QoS Performance Metrics

Performance Metrics	OCMP	ERMDT	DPPH	MDPPH	OMDPPH
PDR	90.513	87.4	92.4	95.5	99.32
PLR	9.5	12.6	7.6	4.5	0.68
DR	16.233	6.6	3.49	5.9	0.2
ED	1.4	1.1	0.9	0.9	0.6
VD	0.6	0.3	0.23	0.2	0.1
QD	0.08	0.93	0.12	0.05	0.08
QOccp	0.33	0.42	0.43	0.41	0.01
Retx	46.18	46.19	46.7	43.5	25.8
Throughput	5.34	6.48	8.67	8.56	13.33

7.4 SUMMARY

This chapter has detailed performance evaluation of the operational properties of the proposed system with simulation results conducted using the network simulator NS-2. Firstly, the proposed protocols enhance the QoS by considering various performance metrics in comparison to existing protocols. The proposed DPPH algorithm reduces packet loss as it schedules the packets based on the available bandwidth and the data sending rate. The MDPPH reduces the number of retransmission and results in the reduction of elapsed time and queueing delay. The throughput analysis has also been made an excellence growth in all the three proposed protocols and output results show that OMDPPH maintains almost constant and better throughput. Additionally, the proposed system has been analyzed and passed for scalability against the variation in number of sensor nodes.

CHAPTER 8

CONCLUSION AND FUTURE SCOPE

8.1 CONCLUSION

This thesis provides the brief idea how QoS issues at transport layer affect the performance of a WBAN. Further, it surveys number of existing system and illustrates the key issues and open research problems related to QoS at the transport layer of WBANs. The main focus of this research lies in QoS enhancement in the WBAN.

Despite the best services provided by existing systems, they often provide poor QoS due to assorted traffic in a dynamic environment. These system models are designed to improve QoS in WBAN with respect to reliability and congestion as main affecting factors. But these systems are not sufficient to achieve better QoS in WBAN as they are silent towards other major factors like fair-resource sharing; handling of unnecessary retransmission of packets, and transmission of duplicate data; reduction of jitter, and waiting time; starvation; and early and accurate detection of critical data. So there is still a need for a new kind of system which can handle all these above-mentioned issues in a WBAN.

During research work, a new QoS model has been proposed to handle heterogeneous traffic in a dynamic environment of WBAN named as DWBAN. In order to work perfectly, the model is implemented with three protocols and simulated with a standard NS-2 network simulator. Finally, the model has been compared and analyzed against existing protocols in different scenarios. The generated outcomes confirm that the proposed protocols outperformed the existing protocol in all aspects.

8.2 CONTRIBUTIONS

The various contributions of the research work are listed below in order to achieve the target objectives.

- Design of a novel architecture for handling heterogeneous traffic in a dynamic environment of WBAN named DWBAN.
- Dynamic Priority based Packet Handling (DPPH) protocol
- Modified DPPH (MDPPH) protocol for QoS management
- Optimized MDPPH (OMDPPH) protocol for QoS optimization (sing Lion Group Hunting optimization technique)

In the first contributory work, a novel architecture is designed for the healthcare WBAN to deal assorted traffic in its frequently changing environment, which further applies dynamic priority policy to provide better QoS while considering packet loss, drop, delay, and throughput as key measurements in the WBAN system.

Secondly, a new packet handling protocol named DPPH has been proposed to handle packets as packets are the first building block for performance improvement in any network. DPPH is a dynamic packet handling protocol designed to manage heterogeneous or assorted packets. The other job of DPPH protocol is an early and accurate identification of the abnormal condition. In addition to this, it classifies heterogeneous packets and assigns them priority accordingly, which further helps in scheduling. In order to overcome the starvation and delay problem, it put forward a ratio-based earliest deadline first (REDF) scheduling. On the performance basis, the DPPH performs better than OCMP and ERMDT protocol; the reason of this betterment is its dynamic priority based packet classification and scheduling techniques.

The third significant contribution is the design of MDPPH protocol, which tackles QoS related issues with respect to reliability, congestion, and delay. It overcomes the delay due to unnecessary retransmission by retransmitting selected amount of packets. It also helps in elimination of duplicate packets. It applies a multi-factor congestion detection technique and overcomes the queuing delay and queue overhead problems by proper management of queue. It carries out both congestion control and congestion

avoidance policy by performing quick-start and fractional increased and decreased based rate adjustment, and Selective packet dropping policies. It has been shown from the performance results that the MDPPH perform better than DPPH, and the existing ERMDT and OCMP protocols due to its selective retransmission, selective drop and duplicate elimination strategies.

The fourth contribution of this research work is to make the WBAN more precise and more practical in terms of QoS, and this is done via introducing an optimization technique. Till date, no optimization algorithm has been developed for maximizing QoS performance at the transport layer of WBAN. With a totally new and efficient optimization technique named Lion Group Hunting (LGH), the QoS performances of the WBAN are optimized in the OMDPPH protocol. In this protocol, the QoS performance metric is mapped to the LGH algorithm. It has been demonstrated that the LGH optimizes the QoS in the WBAN with an Opposition-Based Learning (OBL) strategy which explores multi-dimensional search. The performance of OMDDP protocol is found better than MDPPH, DPPH, ERMDT and OCMP protocols. The simulation results of OMDPPH outperformed other protocols resulting in high QoS.

The proposed protocols are helpful in real scenarios because they handle QoS in the heterogeneous and dynamic environment. Proposed packet handling algorithm is more efficient to segregate critical data from rest of the data and informs for accurate conditions with true alerts. The extended work in second protocol helps in controlling and handling QoS related issues and also prevents the unequal distribution of resources. The application of optimization technique further provides stable and robust results under varying situations. All these above contributions help to enhance the efficiency of the proposed system with respect to various QoS performance metrics.

8.3 FUTURE SCOPE

Beyond what has been proposed during research work, there is more interesting research directions which can be further explored in future.

- Security and Privacy issues

For further enhancement of the system performance, privacy and security-related QoS issues (i.e. packet delay attack, packet drop attack, and duplicate packet attack) can be resolved. In the delayed attack, an attacker or a compromised node deliberately delays the transmission time of messages. In the packet drop attack, a compromised node drops packets maliciously while in the duplicate attack a compromised node relay duplicate packets instead drop them. The packet drop and duplicate attacks are very hard to detect because these kinds of problems occur in normal scenarios. Hence a better technique to identify and resolve these kinds of attacks can be designed in near future.

- Network Mobility

  WBAN supports both network and node mobility. The topology of a WBAN changes dynamically along with the movement of the body as it moves as a whole in an ambient network. Therefore, suitable network mobility along with a better multi-homing and handover strategy can be explored.

- Fault Tolerance

  The data transmission in WBAN must be accomplished without any failure as it carries critical data in some applications like healthcare. Achieving fault tolerance in such complicated and dynamic environment is not practically an easier task. Therefore a priority based fault tolerant technique can be developed for the dynamic nature of WBAN to save network resources.

- Big-Data

  The volume of data is getting increased day by day with the adoption of scalability in devices of WBAN, so there is a need to pay more attention to the data quality and quantity in such environments. The concept of Big-Data can be integrated into WBAN applications as these deals with high-volume and critical data sets which are hard to handle using traditional database management tools or data processing techniques.

- Internet of Things (IoT)

  For 24-hour autonomous monitoring and long-term continuous diagnosis purposes, the concept of Internet of Things (IoT) can be integrated to WBAN. IoT allows facilities like sensing, processing and communicating with different physical and biomedical parameters or things from various fields through the Internet. It helps in connecting the doctors, patients, and nurses through smart devices and provides a freedom to each of entity to roam without any restrictions. The functionality of IoT and its association with the sensing and wireless techniques can fulfill the requirements of healthcare applications more efficiently.

- Cloud Computing

  Cloud computing can be beneficial for a healthcare center by permitting it to use infrastructure, platforms, and software provided by the cloud providers, as it makes use of unlimited storage and computing resources with reasonable cost. In healthcare centers, the use of cloud computing has been advantageous for maintaining health records, observing patients, controlling diseases etc. effectively. The perfect implementation of cloud computing may contribute immense opportunities for pervasive healthcare systems for collaborating with peers and analyzing data.

REFERENCES

[1] C. Wang, K. Sohraby, B. Li, M. Daneshmand, and Y. Hu, "A survey of transport protocols for wireless sensor networks, "*IEEE network*, Vol. 20, No. 3, 2006, pp. 34-40.

[2] A. Sharif, V. M. Potdar, and A. J. D. Rathnayaka, "ERCTP: End-to-end reliable and congestion aware transport layer protocol for heterogeneous WSN, "*Scalable Computing: Practice and Experience*, Vol. 11, No. 4, 2010, pp. 359-371.

[3] B. Sharma and T. C. Aseri, "A comparative analysis of reliable and congestion-aware transport layer protocols for wireless sensor networks, "*ISRN sensor networks*, 2012, pp. 1-14.

[4] C. Ma, J. Sheu and C. Hsu, "A game theory based congestion control protocol for wireless personal area networks, "*Journal of Sensors*, 2016, pp. 1-13.

[5] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring, "*Journal of mobile multimedia*, Vol. 1, No. 4, 2006, pp. 307-326.

[6] Jovanov, C. Poon, G. Yang, and Y. Zhang, "Guest editorial body sensor networks: from theory to emerging applications, "*IEEE Transactions on Information Technology in Biomedicine*, Vol. 13, No. 6, 2009, pp.859-863.

[7] P. Khan, Md. A. Hussain, and K. S. Kwak, "Medical applications of wireless body area networks, "*International Journal of Digital Content Technology and its Applications*, Vol. 3, No. 3, 2009, pp.1-9.

[8] M. R. Yuce, "Implementation of wireless body area networks for healthcare systems, "*Sensors and Actuators A: Physical*, Vol. 162, No. 1, 2010, pp. 116-129.

[9] S. Ivanov, D. Botvich, and S. Balasubramaniam, "Cooperative wireless sensor environments supporting body area networks, "*IEEE transactions on Consumer Electronics*, Vol. 58, No. 2, 2012, pp. 284-292.

[10] Z. A. Khan, S. Sivakumar, W. Phillips, and N. Aslam, "A new patient monitoring framework and Energy-aware Peering Routing Protocol (EPR) for Body Area Network communication, "*Journal of Ambient Intelligence and Humanized Computing*, Vol. 5, No. 3, 2014, pp. 409-423.

[11] Y. Zhang, L. Sun, H. Song, and X. Cao, "Ubiquitous WSN for healthcare: Recent advances and future prospects, "*IEEE Internet of Things Journal*, Vol. 1, No. 4, 2014, pp. 311-318.

[12] 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 2014, pp. 1658-1686.

[13] J. Lee, Y. Su, and C. Shen, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi, "In *33rd Annual Conference of the IEEE Industrial Electronics Society*, 2007, pp. 46-51.

[14] B. Kumar, S. P. Singh, and A. Mohan, "Emerging mobile communication technologies for health, "In *IEEE International Conference on Computer and Communication Technology*, 2010, pp. 828-832.

[15] R. H. Jacobsen, F. O. Hansen, J. K. Madsen, H. Karstoft, P. H. Mikkelsen, T. A. Skogberg, E. S. Rasmussen, C. Andersen, M. Alrøe and T. S. Toftegaard, "A modular platform for wireless body area network research and real-life experiments, "*International Journal on Advances in Networks and Services*, Vol. 4, No. 3, 2011, pp. 257-277.

[16] J. Y. Khan and R. Y. Mehmet, "Wireless body area network (WBAN) for medical applications, "In *New developments in biomedical engineering*, InTech, 2010, pp. 591-627.

[17] D. M. Barakah and M. Ammad-uddin, "A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture, "In *Third International Conference Intelligent Systems, Modelling and Simulation*, 2012, pp. 214-219.

[18] S. Jeong, C. Youn, E. B. Shim, M. Kim, Y. M. Cho, and L. Peng, "An integrated healthcare system for personalized chronic disease care in home–hospital environments, "*IEEE Transactions on Information Technology in Biomedicine*, Vol. 16, No. 4, 2012, pp. 572-585.

[19] D. Zois, M. Levorato, and U. Mitra, "Energy-efficient, heterogeneous sensor selection for physical activity detection in wireless body area networks, "*IEEE Transactions on signal processing*, Vol. 61, No. 7, 2013, pp. 1581-1594.

[20] C. Chakraborty, B. Gupta, and S. K. Ghosh, "A review on telemedicine-based WBAN framework for patient monitoring, "*Telemedicine and e-Health*, Vol. 19, No. 8, 2013, pp. 619-626.

[21] S. Cheng, C. Y. Huang, and C. C. Tu, "RACOON: A multiuser QoS design for mobile wireless body area networks, "*Journal of medical systems*, Vol. 35, No. 5, 2011, pp. 1277-1287.

[22] J. Lewandowski, H. E. Arochena, R. N. G. Naguib, K. Chao, A. Garcia-Perez, "Logic-Centered Architecture for Ubiquitous Health Monitoring, "*IEEE Journal of Biomedical and Health Informatics*, Vol. 18, No. 5, 2014, pp. 1525-1532.

[23] 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, 2014, pp. 9153-9209.

[24] R. Negra, I. Jemili, and A. Belghith, "Wireless body area networks: Applications and technologies, "*Procedia Computer Science*, Vol. 83, 2016, pp. 1274-1281.

[25] E. Tóth-Laufer and A. R. Várkonyi-Kóczy, "A soft computing-based hierarchical sport activity risk level calculation model for supporting home exercises, "*IEEE Transactions on Instrumentation and Measurement*, Vol. 63, No. 6, 2014, pp. 1400-1411.

[26] 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, pp. 84-93.

[27] F. C. J. González, O. O. V. Villegas, D. E. T. Ramírez, V. G. C. Sánchez, and H. O. Domínguez, "Smart multi-level tool for remote patient monitoring based on a wireless sensor network and mobile augmented reality, "*Sensors*, 2014, pp.17212-17234.

[28] P. Johansson, M. Kazantzidis, R. Kapoor and M. Gerla, "Bluetooth: an enabler for personal area networking, "*IEEE Network*, Vol. 15, No. 5, 2001, pp. 28-37.

[29] K. Y. Kwak, S. Ullah, and N. Ullah, "An overview of IEEE 802.15. 6 standard, "In *IEEE 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies*, 2010, pp. 1-6.

[30] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao and V. C. M. Leung, "Body Area Networks: A Survey, "*Mobile Networks and Applications*, Vol. 16, No. 2, 2011, pp. 171-193.

[31] E. Jovanov and A. Milenkovic, "Body area networks for ubiquitous healthcare applications: opportunities and challenges, "*Journal of medical systems*, Vol. 35, No. 5, 2011, pp. 1245-1254.

[32] L. Hughes, X. Wang, and T. Chen, "A review of protocol implementations and energy efficient cross-layer design for wireless body area networks, "*Sensors*, Vol. 12, No. 11, 2012, pp. 14730-14773.

[33] O. Kasten and M. Langheinrich, "First experiences with bluetooth in the smart-its distributed sensor network," In *Workshop on Ubiquitous Computing and Communications*, Vol. 1, 2001, pp. 1-10.

[34] C. Abreu, F. Miranda, M. Ricardo, and P. M. Mendes, "QoS-based management of biomedical wireless sensor networks for patient monitoring, "*SpringerPlus*, Vol. 3, No. 1, 2014, pp.1- 13.

[35] M. A. Algaet, Z. A. B. M. Noh, A. S. Shibghatullah, A. A. Milad, and A. Mustapha, "A Review on Provisioning Quality of Service of Wireless Telemedicine for E-Health Services, "*Middle-East Journal of Science Research*, Vol. 19, No. 4, 2014, pp. 570-592.

[36] G. Zhou, Q. Li, J. Li, Y. Wu, S. Lin, J. Lu, C. Wan, M. D. Yarvis, and J. A. Stankovic, "Adaptive and Radio-Agnostic QoS for Body Sensor Network, "*ACM Transactions on Embedded Computing Systems*, Vol. 10, No. 4, 2011, pp. 1-34.

[37] H. Alemdar, and C. Ersoy, "Wireless sensor networks for healthcare: A survey, "*Computer Networks*, Vol. 54, No. 15, 2010, pp. 2688-2710.

[38] M. Patel and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies, "*IEEE Wireless communications*, Vol. 17, No. 1, 2010.

[39] K. Gill, S. Yang, F. Yao, and X. Lu, "A zigbee-based home automation system, "*IEEE Transactions on consumer Electronics*, Vol. 55, No. 2, 2009, pp. 422-430.

[40] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks, "*Wireless Networks*, Vol. 17, No. 1, 2011, pp. 1-18.

[41] J. M. Corchado, J. Bajo, D. I. Tapia, and A. Abraham, "Using heterogeneous wireless sensor networks in a telemonitoring system for healthcare, "*IEEE transactions on information technology in biomedicine*, Vol. 14, No. 2, 2010, pp. 234-240.

[42] F. Nasri and A. Mtibaa, "Smart Mobile Healthcare System based on WBSN and 5G, "*International Journal of Advanced Computer Science and Applications*, Vol. 8, No. 10, 2017.

[43] J. Hauer, V. Handziski, and A. Wolisz, "Experimental study of the impact of WLAN interference on IEEE 802.15. 4 body area networks, "*Wireless sensor networks*, 2009, pp. 17-32.

[44] J. Lansford, A. Stephens, and R. Nevo, "Wi-Fi (802.11 b) and Bluetooth: enabling coexistence, "*IEEE network*, Vol. 15, No. 5, 2001, pp. 20-27.

[45] Md A. Razzaque, C. S. Hong, and S. Lee, "Data-centric Multiobjective QoS-aware Routing Protocol for Body Sensor Networks, "*Sensors*, Vol. 11, No. 1, 2011, pp. 917-937.

[46] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "Codeblue: An ad hoc sensor network infrastructure for emergency medical care, "In *Workshop on Applications of Mobile Embedded Systems*, Vol. 5, 2004, pp. 6-9.

[47] A. Van Halteren, R. Bults, K. Wac, D. Konstantas, I. Widya, N. Dokovski, G. Koprinkov, V. Jones, and R. Herzog, "Mobile patient monitoring: The mobihealth system, "*Journal on Information Technology and Healthcare*, Vol. 2, 2004, pp. 365-373.

[48] U. Anliker, J.A. Ward, P. Lukowicz, G. Troster, F. Dolveck, M. Baer, F. Keita, E. Schenker, F. Catarsi, L. Coluccini, A. Belardinelli, D. Shklarski, M. Alon, E. Hirt, R. Schmid, and M. Vuskovic, "AMON: a wearable multi parameter medical monitoring and alert system, "*IEEE Transactions on information technology in Biomedicine*, Vol. 8, No. 4, 2004, pp. 415-427.

[49] J. W.P. Ng, B. P.L. Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou, and G. Yang, "Ubiquitous monitoring environment for wearable and implantable sensors (UbiMon), "In *International conference on ubiquitous computing*, 2004, pp.7-14.

[50] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, J. Stankovic, "ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring," *University of Virginia Computer Science Department Technical Report* 2, 2006, pp. 1-14.

[51] S. Jiang, Y. Cao, S. Iyengar, P. Kuryloski, R. Jafari, Y. Xue, R. Bajcsy, and S. Wicker, "CareNet: an integrated wireless sensor networking environment for remote healthcare, "In *Proceedings of the ICST 3rd international conference on Body area networks*, ICST, 2008. (https://dl.acm.org/citation.cfm?id=1460269)

[52] J. Ko, J. H. Lim, Y. Chen, R. A. M. Aloiu-e, Andreas, Terzis and G. M. Masson, T. Gao and W. Destler, L. Selavo, R. P. Dutton, "MEDiSN: Medical emergency detection in sensor networks, "*ACM Transactions on Embedded Computing Systems*, Vol. 10, No. 1, 2010, pp. 1-29.

[53] A Rodrigues, J. S. Silva, and F. Boavida. "iSenior-A support system for elderly citizens," *IEEE Transactions on Emerging Topics in Computing*, Vol. 1, No. 2, 2013, pp. 207-217.

[54] C. Cheng, N. Chanani, J. Venugopalan, K. Maher, and M. D. Wang, "icuARM-An ICU clinical decision support system using association rule mining, "*IEEE journal of translational engineering in health and medicine*, Vol. 1, 2013, pp. 1-10.

[55] C. Wan, S. B. Eisenman, and A.T. Campbell, "CODA: Congestion detection and avoidance in sensor networks, " In *Proceedings of the 1st international conference on Embedded networked sensor systems*, 2003, pp. 266-279.

[56] C. Wan, S. B. Eisenman, and A.T. Campbell, "Energy-efficient congestion detection and avoidance in sensor networks, "*ACM Transactions on Sensor Networks*, Vol. 7, No. 4, 2011, pp. 1-32.

[57] C. T. Ee and R. Bajcsy, "Congestion control and fairness for many-to-one routing in sensor networks," In *ACM 2nd international conference on Embedded networked sensor systems*, 2004, pp. 148-161.

[58] S. Brahma, M. Chatterjee, and K. Kwiat, "Congestion control and fairness in wireless sensor networks, "In *8th IEEE International Conference on Pervasive Computing and Communications Workshops*, 2010, pp. 413-418.

[59] Y. G. Iyer, S. Gandham, and S. Venkatesan, "STCP: a generic transport layer protocol for wireless sensor networks, "In *14th International Conference on Computer Communications and Networks*, 2005, pp. 449-454.

[60] C. Wan, A. T. Campbell, and L. Krishnamurthy, "Pump-slowly, fetch-quickly (PSFQ): a reliable transport protocol for sensor networks, "*IEEE Journal on selected areas in Communications*, Vol. 23, No. 4, 2005, pp.862-872.

[61] O. B. Akan and I. F. Akyildiz, "Event-to-sink reliable transport in wireless sensor networks, "*IEEE/ACM Transactions on Networking*, Vol. 13, No. 5, 2005, pp. 1003-1016.

[62] C. Wang, B. Li, K. Sohraby, M. Daneshmand, and Y. Hu, "Upstream congestion control in wireless sensor networks through cross-layer optimization, "*IEEE Journal on selected areas in Communications*, Vol. 25, No. 4, 2007.

[63] V. C. Gungor, Ö. B. Akan, and I. F. Akyildiz, "A Real-Time and Reliable Transport (RTRT) Protocol for Wireless Sensor and Actor Networks, "*IEEE/ACM transactions on networking*, Vol. 16, No. 2, 2008, pp. 359-370.

[64] S. Misra, V. Tiwari, and M. S. Obaidat, "LACAS: learning automata-based congestion avoidance scheme for healthcare wireless sensor networks, "*IEEE Journal on Selected Areas in Communications*, Vol. 27, No. 4, 2009, pp. 466-479.

[65] J. Paek and R. Govindan, "RCRT: Rate-controlled reliable transport protocol for wireless sensor networks, "*ACM Transactions on Sensor Networks*, Vol. 7, No. 3, 2010, pp. 305- 320.

[66] M. Monowar, O. Rahman, A. K. Pathan, and C. S. Hong, "Prioritized heterogeneous traffic-oriented congestion control protocol for WSNs, "*International Arab Journal of Information Technology*, Vol. 9, No. 1, 2012, pp. 39-48.

[67] M. H. Yaghmaee, N. F. Bahalgardi, and D. Adjeroh, "A prioritization based congestion control protocol for healthcare monitoring application in wireless sensor networks, "*Wireless personal communications*, Vol. 72, No. 4, 2013, pp. 2605-2631.

[68] A. A. Rezaee, M. H. Yaghmaee, A. H. Mohajerzadeh, and A. M. Rahmani, "HOCA: Healthcare Aware Optimized Congestion Avoidance and control protocol for wireless sensor networks, "*Journal of Network and Computer Applications*, Vol. 37, 2014, pp. 216-228.

[69] P. Mohanty and M. R. Kabat, "A hierarchical energy efficient reliable transport protocol for wireless sensor network, "*Ain Shams Engineering Journal*, Vol. 5, No. 4, 2014, pp. 1141-1155.

[70] S. Manfredi, "Congestion control for differentiated healthcare service delivery in emerging heterogeneous wireless body area networks, "*IEEE Wireless Communications*, Vol. 21, No. 2, 2014, pp. 81-90.

[71] A. A. Rezaee, M. H. Yaghmaee, and A. M. Rahmani, "Optimized congestion management protocol for healthcare wireless sensor networks, "*Wireless personal communications*, Vol. 75, No. 1, 2014, pp.11-34.

[72] D. Datta and S. Kundu, "Reliable and efficient data transfer in wireless sensor networks via out-of-sequence forwarding and delayed request for missing packets, "In *Fourth IEEE International Conference on Information Technology*, 2007, pp. 128-133.

[73] P. Mohanty, M. R. Kabat, and M. K. Patel, "Energy efficient reliable data delivery in wireless sensor networks for real time applications, "In *Computational Intelligence in Data Mining*, Vol. 3, 2015, pp. 281-290.

[74] D. Wu, B. Yang, H. Wang, D. Wu, and R. Wang, "An energy-efficient data forwarding strategy for heterogeneous WBANs, " *IEEE Access*, Vol. 4, 2016, pp. 7251-7261.

[75] P. Mohanty and M. R. Kabat, "Energy efficient reliable multi-path data transmission in WSN for healthcare application, "*International Journal of Wireless Information Networks*, Vol. 23, No. 2, 2016, pp. 162-172.

[76] M. Javaid, M. Yaqoob, M. Y. Khan, M. A. Khan, A. Javaid, and Z. A. Khan, "Analyzing Delay in Wireless Multi-hop Heterogeneous Body Area Networks, "*Research Journal of Applied Sciences, Engineering and Technology*, Vol. 7, No. 1, 2014, pp. 123-136.

[77] Z. A. Khan, S. Sivakumar, W. Phillips, and B. Robertson, "A QoS-aware routing protocol for reliability sensitive data in hospital body area Networks, "*Procedia Computer Science*, Vol. 19, 2013, pp.171-179.

[78] N. Yaakob, and I. Khalil, "A novel congestion avoidance technique for simultaneous real-time medical data transmission, "*IEEE journal of biomedical and health informatics*, Vol. 20, No. 2, 2016, pp. 669-681.

[79] Z. Khan, N. Aslam, S. Sivakumar, and W. Phillips, "Energy-aware peering routing protocol for indoor hospital body area network communication, "*Procedia Computer Science*, Vol. 10, 2012, pp. 188-196.

[80] N. Farzaneh, M. H. Yaghmaee, Moghaddam, and D. Adjeroh, "An adaptive congestion alleviating protocol for healthcare applications in wireless body sensor networks: Learning automata approach, "*Amirkabir/ Electrical and Electronics Engineering (Springer)*, Vol. 44, No. 1, 2012, pp. 31-41.

[81] N. Bradai, L. C. Fourati, and L. Kamoun, "WBAN data scheduling and aggregation under WBAN/WLAN healthcare network, "*Ad Hoc Networks*, Vol. 25, 2015, pp. 251-262.

[82] F. Javed, S. Farrugia, M. Colefax, and K. Schindhelm, "Early warning of acute decompensation in heart failure patients using a noncontact measure of stability index, "*IEEE Transactions on Biomedical Engineering*, Vol. 63, No. 2, 2016, pp. 438-448.

[83] J. Wang, Z. Zhang, B. Li, S. Lee, and R. S. Sherratt, "An enhanced fall detection system for elderly person monitoring using consumer home networks, "*IEEE transactions on consumer electronics*, Vol. 60, No. 1, 2014, pp. 23-29.

[84] V. Shiva, and T. Anuradha, "Patient Monitoring and Spontaneous alerting system using ADT, "*Indian Journal of Science and Technology*, Vol. 9, No. 30, 2016.

[85] D. E. Taylor, "Survey and taxonomy of packet classification techniques," *ACM Computing Surveys*, Vol. 37, No. 3, 2005, pp. 238-275.

[86] D. E. Taylor and J. S. Turner, "Classbench: A packet classification benchmark, " *IEEE/ACM Transactions on Networking*, Vol. 15, No. 3, 2007, pp. 499-511.

[87] S. Valenti, D. Rossi, A. Dainotti, A. Pescapè, A. Finamore, and M. Mellia, "Reviewing traffic classification, " In *Data Traffic Monitoring and Analysis*, 2013, pp. 123-147.

[88] M. Iftikhar, N. A. Elaiwi, and M. S. Aksoy, "Performance Analysis of Priority Queuing Model for Low Power Wireless Body Area Networks (WBANs), "*Procedia Computer Science*, Vol. 34, 2014, pp.518-525.

[89] Z. Xie, G. Huang, J. He, and Y. Zhang, "A clique-based WBAN scheduling for mobile wireless body area network, "*Procedia Computer Science*, Vol. 31, 2014, pp. 1092-1101.

[90] F. Dobslaw, T. Zhang, and M. Gidlund, "End-to-end reliability-aware scheduling for wireless sensor networks, "*IEEE Transactions on Industrial Informatics*, Vol. 12, No. 2, 2016, pp. 758-767.

[91] F. Zhang and A. Burns, "Schedulability analysis for real-time systems with EDF scheduling, "*IEEE Transactions on Computers*, Vol. 58, No. 9, 2009, pp.1250-1258.

[92] A. Ahmad, R. Arshad, S. A. Mahmud, G. M. Khan, and H. S. Al-Raweshidy, "Earliest-deadline-based scheduling to reduce urban traffic congestion, "*IEEE Transactions on Intelligent Transportation Systems*, Vol. 15, No. 4, 2014, pp. 1510-1526.

[93] L. Karim, N. Nasser, T. Taleb, and A. Alqallaf, "An efficient priority packet scheduling algorithm for wireless sensor network, "In *IEEE International Conference on Communications*, 2012, pp. 334-338.

[94] P. Phunchongharn, D. Niyato, E. Hossain, and S. Camorlinga, "An EMI-aware prioritized wireless access scheme for e-health applications in hospital environments, "*IEEE transactions on information technology in biomedicine*, Vol. 14, No. 5, 2010, pp. 1247-1258.

[95] S. Misra and S. Sarkar, "Priority-based time-slot allocation in wireless body area networks during medical emergency situations: An evolutionary game-theoretic perspective, "*IEEE Journal of Biomedical and Health Informatics*, Vol. 19, No. 2, 2015, pp. 541-548.

[96] H. B. Elhadj, J. Elias, L. Chaari, and L. Kamoun, "A priority based cross layer routing protocol for healthcare applications, "*Ad Hoc Networks*, Vol. 42, 2016, pp.1-18.

[97] R. H. Kim, J. G. Kim, and B. W. Seo, "Channel Access with Priority for Urgent Data in Medical Wireless Body Sensor Networks, "*International Journal of Applied Engineering Research*, Vol. 11, No. 2, 2016, pp.1162-1166.

[98] Y. Shao, K. Wang, L. Shu, S. Deng, and D. J. Deng, "Heuristic Optimization for Reliable Data Congestion Analytics in Crowdsourced eHealth Networks, "*IEEE Access*, Vol. 4, 2016, pp.9174-9183.

[99] R. Rejaie, M. Handley, and D. Estrin, "RAP: An end-to-end rate-based congestion control mechanism for realtime streams in the Internet, "In *Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, Vol. 3, 1999, pp. 1337-1345.

[100] O. B. Akan, "On the throughput analysis of rate-based and window-based congestion control schemes, "*Computer Networks*, Vol. 44, No. 5, 2004, pp. 701-711.

[101] C. Ho, Y. Chen, Y. Chan, and C. Ho, "Fast retransmit and fast recovery schemes of transport protocols: A survey and taxonomy, "*Computer Networks*, Vol. 52, No. 6, 2008, pp. 1308-1327.

[102] L. Cai, X. Shen, J. Pan, and Jon W. Mark, "Performance analysis of TCP-friendly AIMD algorithms for multimedia applications, "*IEEE Transactions on Multimedia*, Vol. 7, No. 2, 2005, pp. 339-355.

[103] D. Leith, R. N. Shorten, G. McCullagh, J. Heffner, L. Dunn, and F. Baker, "Delay-based AIMD congestion control," 2007, pp. 1-6, (http://eprints.maynoothuniversity.ie/1745/1/HamiltonDelayAIMD.pdf)

[104] R. Pagh, "Cuckoo hashing for undergraduates," *IT University of Copenhagen*, 2006, pp. 1-6.

[105] R. M. Narasiodeyar and A. P. Jayasumana, "Improvement in packet-reordering with limited re-sequencing buffers: an analysis, "In *IEEE 38th Conference on Local Computer Networks*, 2013, pp. 416-424.

[106] S. Moon, J. Rexford, and K. G. Shin, "Scalable hardware priority queue architectures for high-speed packet switch, "*IEEE Transactions on computers*, Vol. 49, No. 11, 2000, pp. 1215-1227.

[107] A. Arvind and C. P. Rangan, "Symmetric min-max heap: a simpler data structure for double-ended priority queue, "*Information Processing Letters*, Vol. 69, No. 4, 1999, pp. 197-199.

[108] M. Z. Rahman, R. A. Chowdhury, and M. Kaykobad, "Improvements in double ended priority queues, "*International journal of computer mathematics*, Vol. 80, No. 9, 2003, pp. 1121-1129.

[109] M. A. Kafi, D. Djenouri, J. Ben-Othman, and N. Badache, "Congestion control protocols in wireless sensor networks: a survey, "*IEEE communications surveys & tutorials*, Vol. 16, No. 3, 2014, pp.1369-1390.

[110] S. Misra, B. J. Oommen, S. Yanamandra, and M. S. Obaidat, "Random early detection for congestion avoidance in wired networks: a Discretized pursuit learning-automata-like solution, "*IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, Vol. 40, No. 1, 2010, pp. 66-76.

[111] N. Farzaneh and M. H. Yaghmaee, "Joint active queue management and congestion control protocol for healthcare applications in wireless body sensor networks,

"In *International Conference on Smart Homes and Health Telematics*, 2011, pp. 88-95.

[112] V. Ayatollahitafti, Md A. Ngadi, and J. B. M. Sharif, "A Traffic Redirection Based Congestion Control Scheme in Body Area Networks, "*Research Journal of Applied Sciences, Engineering and Technology*, Vol. 8, No. 17,2014, pp.1917-1922.

[113] O. A. Fdili, Y. Fakhri, and D Aboutajdine, "Impact of queue buffer size awareness on single and multi service real-time routing protocols for WSNs, "*International Journal of Communication Networks and Information Security*, Vol.4, No. 2, 2012, pp. 104.

[114] Md Samiullah, S. M. Abdullah, A. I. H. Bappi, and S. Anwar, "Queue management based congestion control in wireless body sensor network," In *International Conference on Informatics, Electronics & Vision*, 2012, pp. 493-496.

[115] S. Jamali, B. Alipasandi, and N. Alipasandi, "VRED: An improvement over RED algorithm by using queue length growth velocity, "*Journal of Advances in Computer Research*, Vol. 4, No. 1, 2013, pp. 31-38.

[116] S. Jamali and S. R. Zahedi, "An improvement over RED algorithm by using particle swarms optimization, "*IEICE Electronics Express*, Vol. 7, No. 17, 2010, pp. 1276-1282.

[117] R. Oftadeh, M. J. Mahjoob, and M. Shariatpanahi, "A novel meta-heuristic optimization algorithm inspired by group hunting of animals: Hunting search, " *Computers & Mathematics with Applications*, Vol. 60, No. 7, 2010, pp. 2087-2098.

[118] B. Singh and D. K. Lobiyal, "A novel energy-aware cluster head selection based on particle swarm optimization for wireless sensor networks, "*Human-Centric Computing and Information Sciences*, Vol. 2, No. 1, 2012, pp. 1-13.

[119] P. Kuila, and K. J. Prasanta, "Energy efficient clustering and routing algorithms for wireless sensor networks: Particle swarm optimization approach, "*Engineering Applications of Artificial Intelligence*, Vol. 33, 2014, pp. 127-140.

[120] B. Wang, X. Jin, and B. Cheng, "Lion pride optimizer: An optimization algorithm inspired by lion pride behavior, "*Science China Information Sciences*, Vol. 55, No. 10, 2012, pp. 2369-2389.

[121] B. R. Rajakumar, "The Lion's Algorithm: a new nature-inspired search algorithm," *Procedia Technology*, Vol. 6, 2012, pp. 126-135.

[122] M. Yazdani and J. Fariborz, "Lion optimization algorithm (LOA): a nature-inspired metaheuristic algorithm, "*Journal of computational design and engineering*, Vol. 3, No. 1, 2016, pp. 24-36.

[123] H. R. Tizhoosh, "Opposition-based learning: a new scheme for machine intelligence, "In *international conference on Computational intelligence for modelling, control and automation, and international conference on intelligent agents, web technologies and internet commerce,* Vol. 1, 2005, pp. 695-701.

[124] G. Yang, Ed., Body Sensor Network. LONDON: Springer-Verlag London Limited, 2006. (http://www.springer.com/in/book/9781447163732)

[125] M. R. Yuce, Jamil Khan, Ed., Wireless Body Area Network: Technology, Implementation, and Application, Australia, Pan Stanford, 2011. (https://www.crcpress.com/Wireless-Body-Area-Networks-Technology-Implementation-and-Applications/Yuce-Khan/p/book/9789814316712)

[126] T. Issariyakul, E. Hossain, Ed., Introduction to Network Simulator 2, Springer Science + Business Media, New York, 2009. (http://www.springer.com/in/book/9781461414056)

[127] K. Fall, and K. Varadhan, "The ns Manual (formerly ns Notes and Documentation), "*The VINT project*, Vol. 47, 2005.

[128] G. K. Wala, O. P. Gupta, and S. Kumar, "Congestion Avoidance in packet networks using network simulator-3 (NS-3), "2016, pp. 73-80.

[129] http://www.isi.edu/nsnam/ns/tutorial.

[130] https://tools.ietf.org/html/rfc2001

Appendix A

Appendix A provides the detail explanation why α is assigned with a value 0.6 and β is assigned with a value 0.2.

During analysis, let's the patient is having four sensor nodes and a total 250Kbps bandwidth is available to the DWBAN. As mentioned in Chapter 3, to fairly distribute the available bandwidth, three parameters have been taken into account, which are the priority of sensor node and values of α and β to estimate and assign the actual share of bandwidth from the total available bandwidth. From equation 3.2, it is clear that, both α and β play an important role during bandwidth sharing. Therefore, an appropriate value needs to be chosen for these two factors in order to fairly distribute the bandwidth among all sensor nodes so that the consumed bandwidth should not exceed beyond the total available bandwidth.

In order to calculate appropriate value for α and β, a MATLAB code is written for equation 3.2. It generates and assigns different priority values to each sensor node during specific interval of time to implement the dynamic prioritization. Total 81 iterations have been executed to generate all possible outcomes with respect to different values of α and β.

The following steps are performed to evaluate the value of α and β.

- The outer iteration run 9 times for the value of α ranging from 0.1 to 0.9 and for each value of α, the inner iteration run 9 times for the value of β ranging from 0.9 to 0.1.
- For all these 81 iterations, the bandwidth of each individual sensor nodes are noted down and summed to figure out the amount of total bandwidth actually assigned.

- Out of these iterations, only those values of α and β are selected for which the total bandwidth is nearly equal to the available bandwidth (i.e. 250Kbps) which is actually shared among all the four sensor nodes.
- Out of 81 cases, a total 9 possible cases are identified which give total bandwidth nearer to 250Kbps.
- For these 9 appropriate cases, a graph has drawn which demonstrates the bandwidth value for each pair of α and β according to node's priority.

value of α and β	Node with priority 1	Node with priority 2	Node with priority 3	Node with priority 4	Total utilization of BW
(α=0.1,β=0.5)	131	68	47	37	283
(α=0.2,β=0.4)	112	62	45	37	256
(α=0.3,β=0.4)	118	68	52	43	281
(α=0.4,β=0.3)	100	62	50	43	255
(α=0.5,β=0.3)	106	68	56	50	280
(α=0.6,β=0.2)	87	62	54	50	253
(α=0.7,β=0.2)	90	68	60	56	274
(α=0.8,β=0.1)	75	62	58	56	251
(α=0.9,β=0.1)	81	68	64	62	275

Figure A.1 Different values of α and β during Bandwidth Allocation

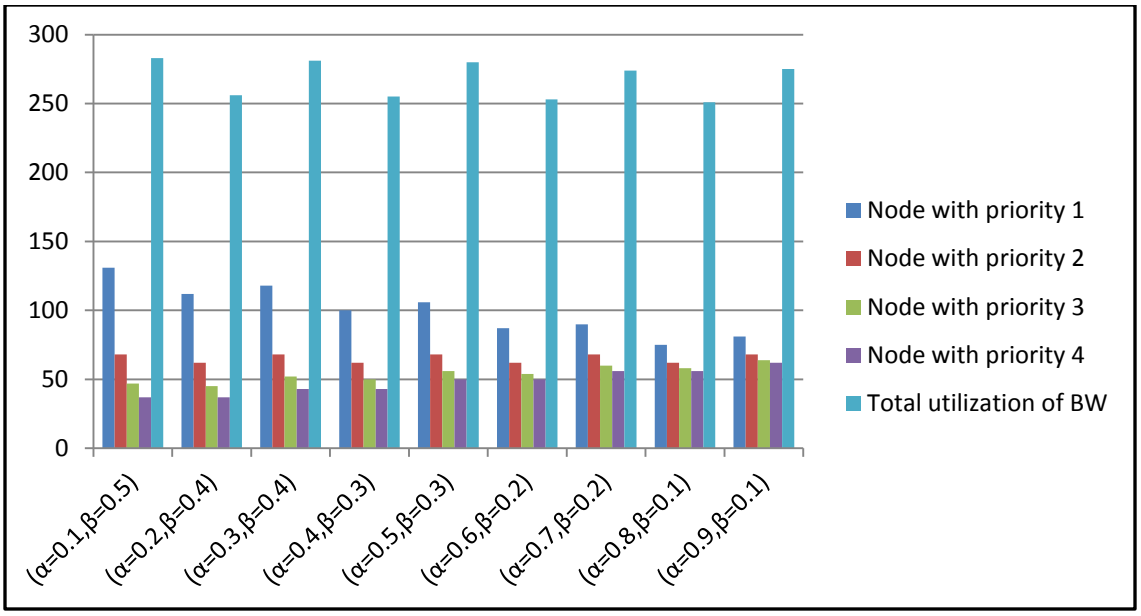

Figure A.2 Graphical representation of fair Bandwidth sharing

From the Figure A.1 and Figure A.2 it is quite clear that, the total assigned bandwidth is more close to total available bandwidth, in only two cases (i.e. (α= 0.6,β=0.2) and (α= 0.8 and β=0.1)). While out of these two cases, first case where α= 0.6 and β=0.2, the bandwidth has been allocated fairly among all sensor nodes according to their priority values. So, this is the reason behind the selection of values α= 0.6 and β=0.2.

Appendix B

Appendix B explains the reason why 30:10 percentage rates are considered during Rate Based Scheduling both in Chapter 3 and Chapter 4.

The purpose of the Rate Based scheduling is to schedule and serve more or nearly double number of packets from the high priority queue which is having high priority packets than the low priority queue having low priority packets.

To compute the rate, w1 and w2 have been taken as the percentage of high priority and low priority queue occupancies, which further help in the calculation of total number of packets, need to be schedule and serve in a time interval T_k.

For the estimation of w1 and w2, the current queue occupancy is taken into account, with the assumption that the queue is not empty.

- For the high priority queue, the queue occupancy is denoted as Q1 and the percentile of service rate is w1.
    - First the Q1 value is measured
    - Then w1% of Q1 is calculated and that amount of packets is served from the high priority queue.
- Similarly, for the low priority queue, the queue occupancy is denoted as Q2 and the percentile of service rate is w2.
    - First the Q2 value is measured
    - Then w2% of Q2 is calculated and that amount of packets is served from the low priority queue.
- The main challenge is to select a desire value for w1 and w2, which fulfill the requirements with less starvation and waiting time.
- For that a MATLAB code is written which generates the queue occupancy values randomly.

- Keeping in mind the concept of rate based scheduling (i.e. w1>w2), here different values for w1 and w2 are considered, where w1 is ranging from 10% to 50% with a 10 % lag, and w2 is ranging from 5% to 30% with a 5% lag.
- Total 21 iterations run for each possible value of w1 and w2 with the constraint w1>w2.
- For four different values of Q1 and Q2 (ranging from lower to higher value), the test is conducted and the generated outputs are represented in four different graphs as shown in Figure ((B.1)-(B.4)).

Percentage	Q1 (Occup=40)	Q2 (Occup=55)
(w1=10, w2=5)	4	3
(w1=20, w2=5)	8	3
(w1=20, w2=10)	8	6
(w1=20, w2=15)	8	9
(w1=30, w2=5)	12	3
(w1=30, w2=10)	***12***	***6***
(w1=30, w2=15)	12	9
(w1=30, w2=20)	12	11
(w1=30, w2=25)	12	14
(w1=40, w2=5)	16	3
(w1=40, w2=10)	16	6
(w1=40, w2=15)	***16***	***9***
(w1=40, w2=20)	16	11
(w1=40, w2=25)	16	14
(w1=40, w2=30)	16	17
(w1=50, w2=5)	20	3
(w1=50, w2=10)	20	6
(w1=50, w2=15)	20	9
(w1=50, w2=20)	20	11
(w1=50, w2=25)	20	14
(w1=50, w2=30)	20	17

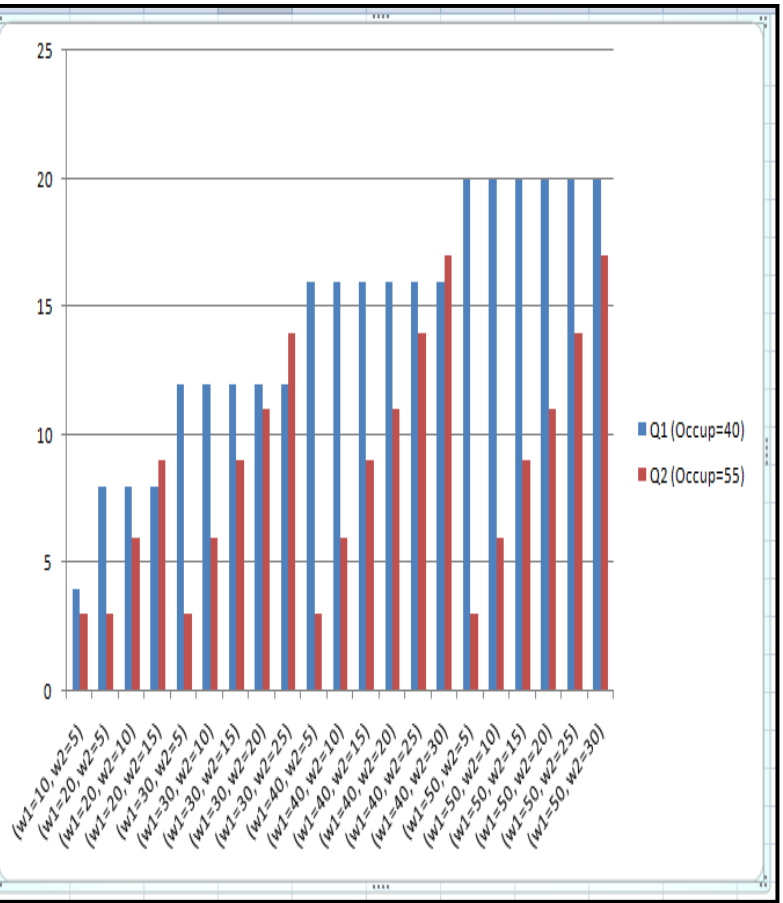

Figure B.1 Number of packet served when Q1=40, and Q2=55

Percentage	Q1 (Occup= 67)	Q2 (Occup= 94)
(w1=10, w2=5)	7	5
(w1=20, w2=5)	14	5
(w1=20, w2=10)	14	10
(w1=20, w2=15)	14	15
(w1=30, w2=5)	21	5
(w1=30, w2=10)	***21***	***10***
(w1=30, w2=15)	21	15
(w1=30, w2=20)	21	19
(w1=30, w2=25)	21	24
(w1=40, w2=5)	27	5
(w1=40, w2=10)	27	10
(w1=40, w2=15)	***27***	***15***
(w1=40, w2=20)	27	19
(w1=40, w2=25)	27	24
(w1=40, w2=30)	27	29
(w1=50, w2=5)	34	5
(w1=50, w2=10)	34	10
(w1=50, w2=15)	34	15
(w1=50, w2=20)	34	19
(w1=50, w2=25)	34	24
(w1=50, w2=30)	34	29

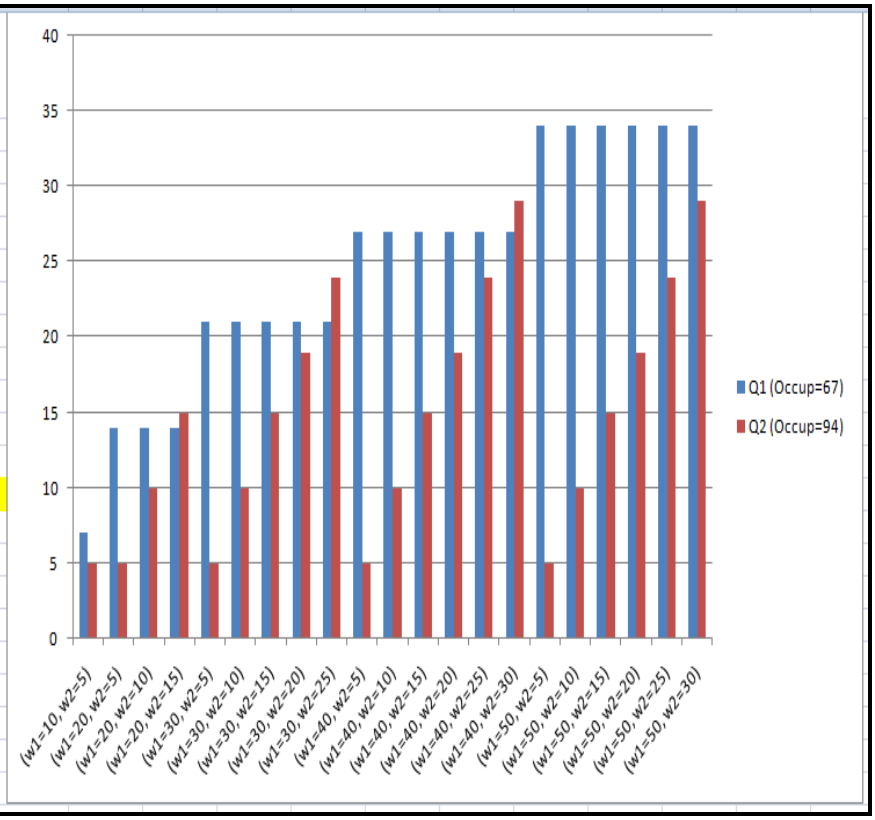

Figure B.2 Number of packet served when Q1=67, and Q2=94

percentage	Q1 (Occup=79)	Q2 (Occup=110)
(w1=10, w2=5)	8	6
(w1=20, w2=5)	16	6
(w1=20, w2=10)	16	12
(w1=20, w2=15)	16	17
(w1=30, w2=5)	24	6
(w1=30, w2=10)	***24***	***12***
(w1=30, w2=15)	24	17
(w1=30, w2=20)	24	23
(w1=30, w2=25)	24	28
(w1=40, w2=5)	32	6
(w1=40, w2=10)	32	12
(w1=40, w2=15)	***32***	***17***
(w1=40, w2=20)	32	23
(w1=40, w2=25)	32	28
(w1=40, w2=30)	32	34
(w1=50, w2=5)	40	6
(w1=50, w2=10)	40	12
(w1=50, w2=15)	40	17
(w1=50, w2=20)	40	23
(w1=50, w2=25)	40	28
(w1=50, w2=30)	40	34

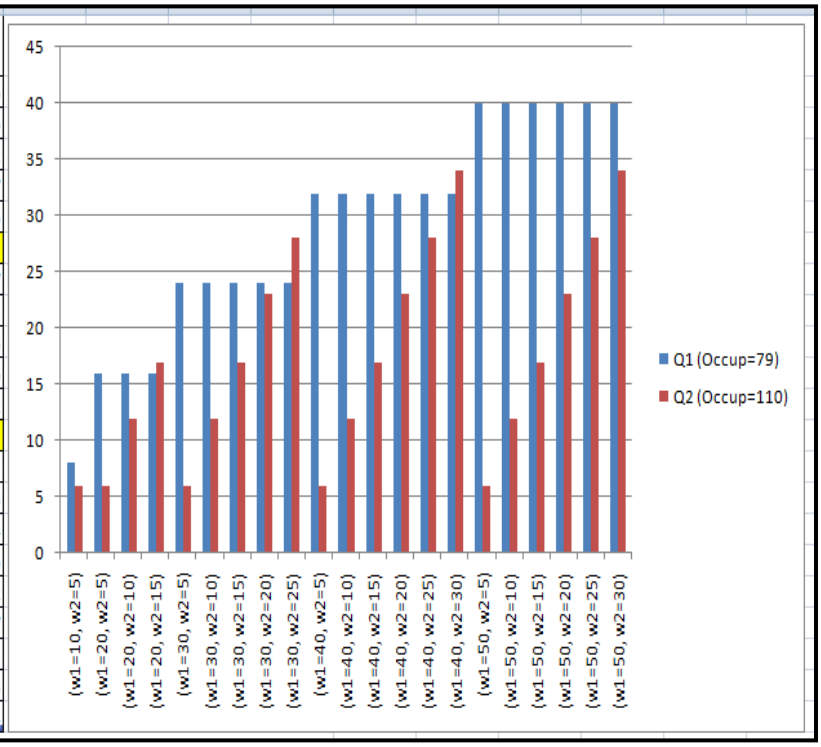

Figure B.3 Number of packet served when Q1=79, and Q2=110

Percentage	Q1 (Occup=97)	Q2 (Occup=133)
(w1=10, w2=5)	10	7
(w1=20, w2=5)	20	7
(w1=20, w2=10)	20	14
(w1=20, w2=15)	20	20
(w1=30, w2=5)	30	7
(w1=30, w2=10)	***30***	***14***
(w1=30, w2=15)	30	20
(w1=30, w2=20)	30	27
(w1=30, w2=25)	30	34
(w1=40, w2=5)	39	7
(w1=40, w2=10)	39	14
(w1=40, w2=15)	***39***	***20***
(w1=40, w2=20)	39	27
(w1=40, w2=25)	39	34
(w1=40, w2=30)	39	40
(w1=50, w2=5)	49	7
(w1=50, w2=10)	49	14
(w1=50, w2=15)	49	20
(w1=50, w2=20)	49	27
(w1=50, w2=25)	49	34
(w1=50, w2=30)	49	40

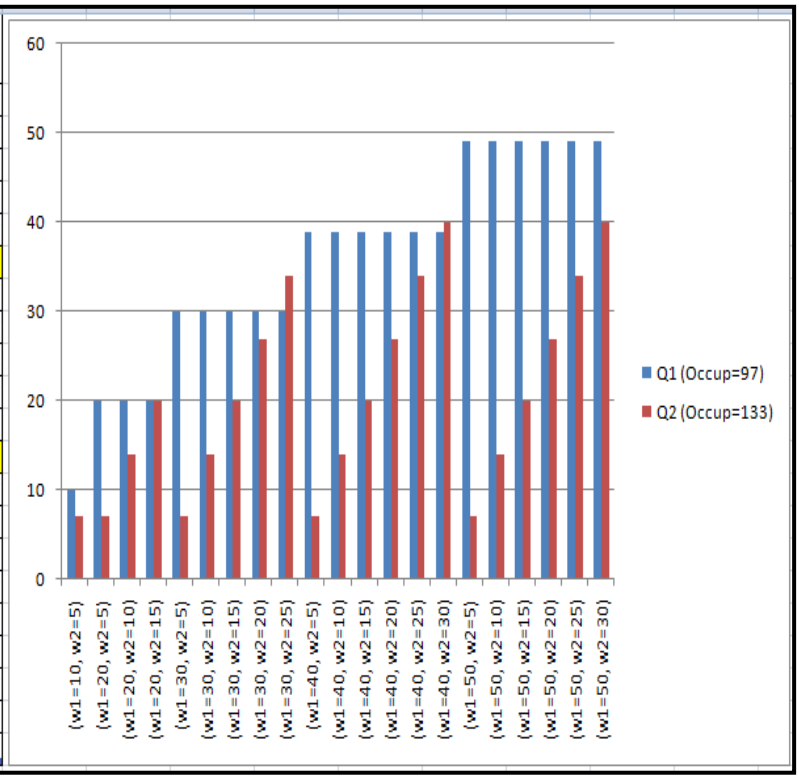

Figure B.4 Number of packet served when Q1=97, and Q2=133

- From the above four graphs it is noticed that out of 21 cases, only two cases (w1=30; w2=10 and w1=40; w2=15) provide good results.
- Out of these two cases, the first case (w1=30 and w2=10) is considered, although both cases generate nearly same ratio (i.e. number of packets chose from high priority queue for service is nearly double to the number of packets chose from the low priority queue). The reason is that, the starvation and waiting time during scheduling is considerably less as compared to the second case as in second case the number of packets ratio is more than the first case.
- So in the rate based scheduling, a ratio of 30% is considered for high priority queue and a ratio of 10% is considered for high priority queue in whole research work.

Appendix C

Appendix C shows how "Quick Start" approach along with FIFD work efficiently in during flow control and rate adjustment as compared to conventional Slow Start and AIMD.

As mentioned in equation 5.1, because of quick start approach the data transmission is begins with a high sending rate and according to the priority of sensor node, it assigns a diverse data sending rate for each sensor node instead of the equal data rate. In addition to this, the FIFD attempts to control the data sending or flow rate dynamically by using a priority based increment or decrement approach as given in equation 5.2.

A MATLAB coding is written for the execution of equation 5.1 and 5.2, and the outcomes for both slow start and quick start approaches are depicted in Figure C.1, where Figure C.1 illustrates the comparison with respect to number of received packets during 25 iterations. From the figure it is clear that due to Quick Start and FIFD, the DWBAN system receives more packets than Slow Start and AIMD.

In addition to Quick Start, proper selection of coefficient factor "k", which affects the data sending rate value during the rate adjustment also affects the data delivery or reception rate. From the equation 5.2, it is clear that the coefficient factor "k" plays a key role in enhancing data sending as well as data reception rate during the whole simulation. For different value of "k", a comparison graph is drawn for FIFD in Figure C.2 where Figure C.2 illustrates the total packet reception rate with respect to different coefficient values. It is clear from the Figure C.2 that for k=0.15 proposed flow control shows better results in terms of number of received packets.

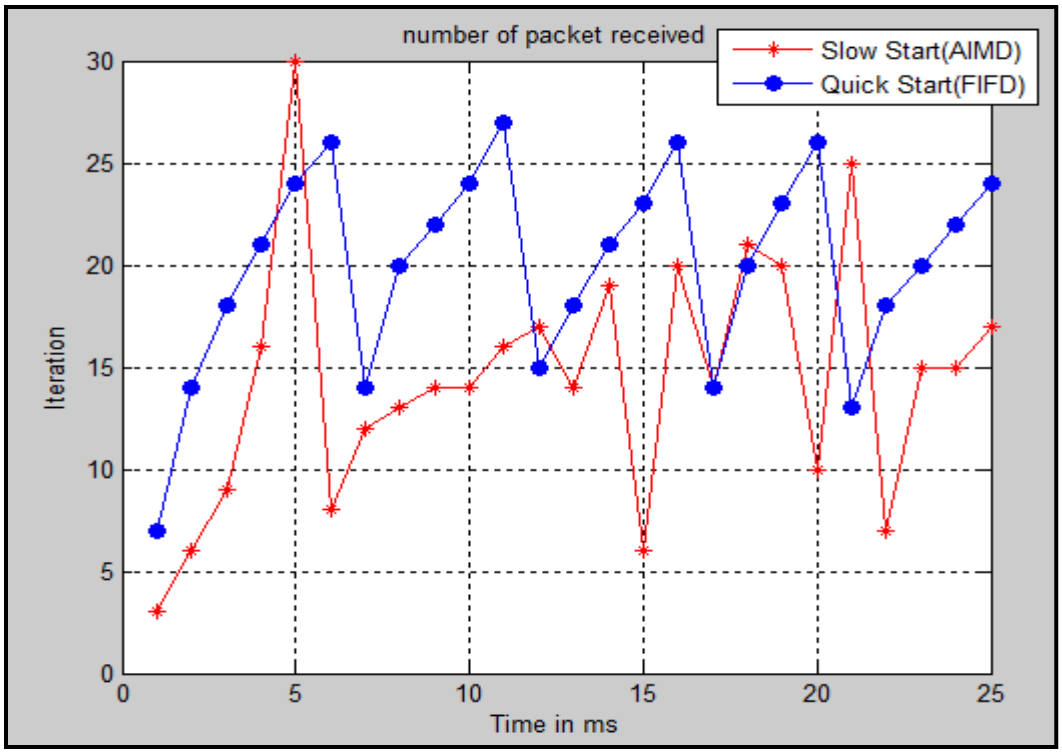

Figure C.1 Comparison results of Quick Start and Slow Start

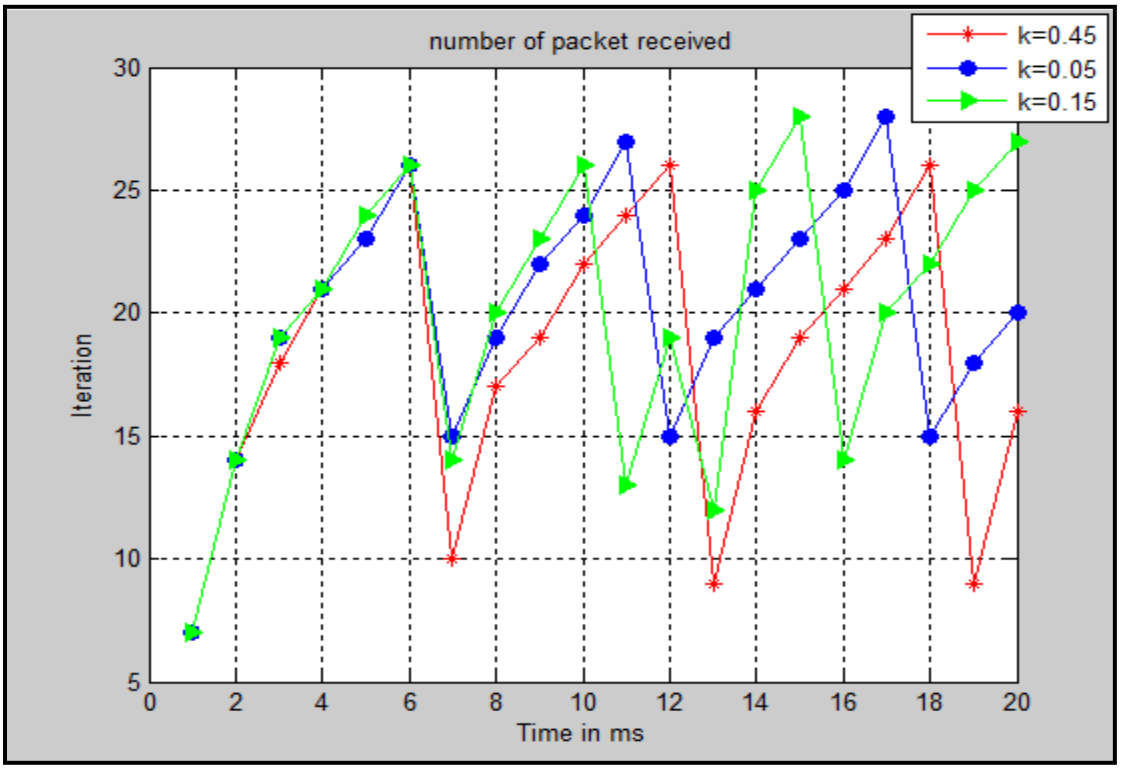

Figure C.2 Packet reception rate with respect to different values of coefficient k

Appendix D

Appendix D explains the working of whole Selective Packet Retransmission and Recovery approach with a suitable example.

As mentioned in Chapter 5, the proposed Selective Packet Retransmission and Recovery approach follows a rate-based retransmission mechanism and its working principle is explained in detail through Figure D.1.

Let's assume that the sender sensor node is S_2 having a priority value 2. As mentioned earlier, here the Data Sending Rate (DSR) value is calculated by the CU and informed to the sensor node through the SNACK control packet. The following parameters are taken into account during the whole process.

At sensor node:

- The current DSR=0 (Data sending rate)
- Generate_counter+=DSR (initial value is 0)
- SNACK=0 (SNACK counter)
- D_{SNACK}=0 (Last desire SNACK received)
- SQ=1,2,…12 (Scheduling Queue).

At CU node:

- The current DSR=0
- Gap= current packet sequence number–last in-order received sequence number +1 (i.e. initial value of Gap=0 and it finds the number of loss)
- Loss_rate+= gap (initial value is 0)
- Loss_Counter+=Loss_rate (loss counter and its initial value is 0)
- Receive_Counter=0(Receive counter)
- Retx_rate= ceil (Loss_rate/priority of sensor node, and its initial value is 0)
- Last_recv =0 (sequence number of last received packet)
- Last_loss=0 (sequence number of last lost packet)
- Loss_seq_no=0
- Consecutive_loss_count=0
- Loss_table is empty.

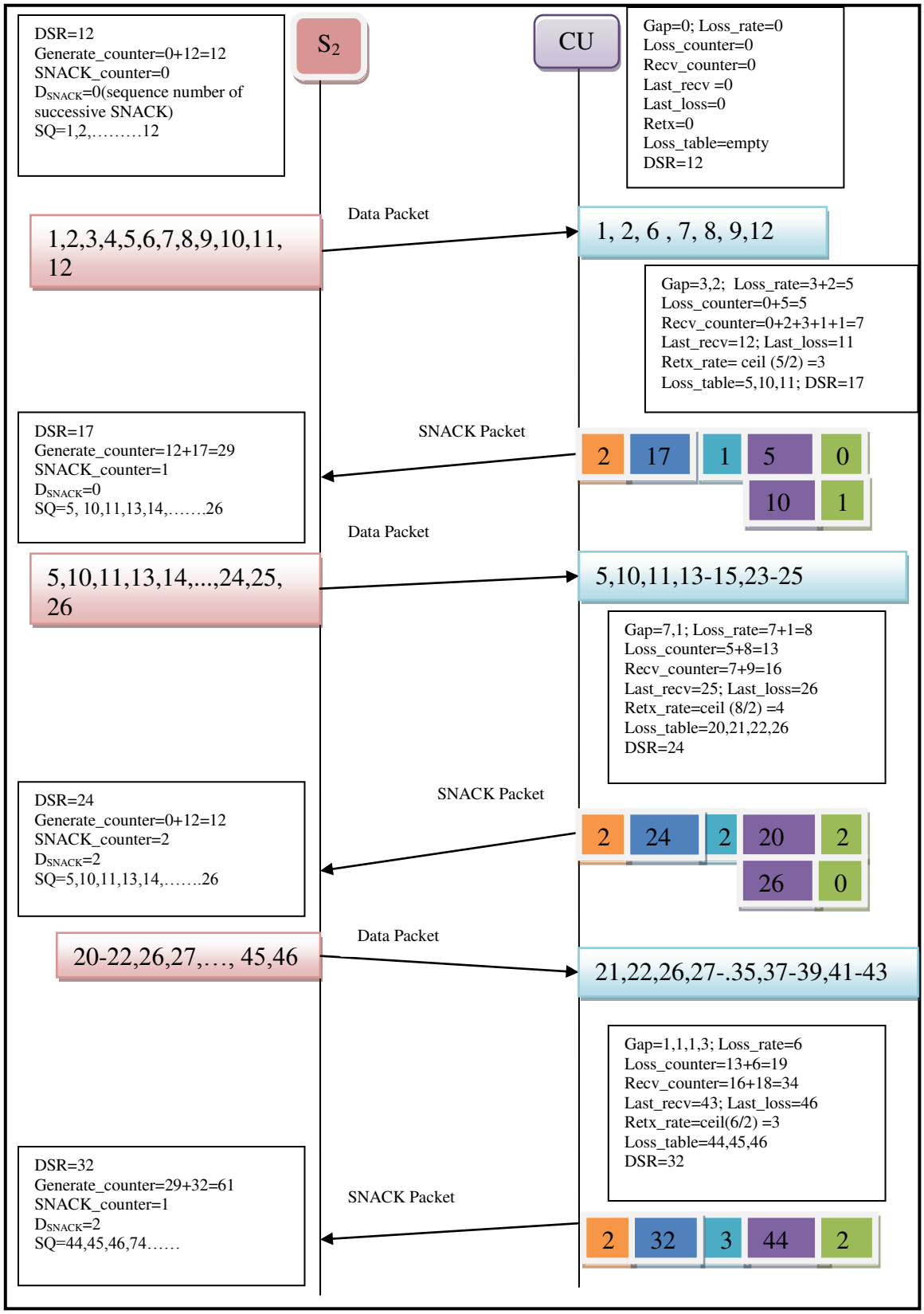

Figure D.1 Example of Selective packets Retransmission and Recovery

Figure D.1 Example of Selective packets Retransmission and Recovery

Here during a particular simulation time, the CU received packets from a sensor node and then identifies the lost packets and notifies the loss with by issuing SNACK packet, and the packet format for a SNACK packet is mentioned in Figure D.2.

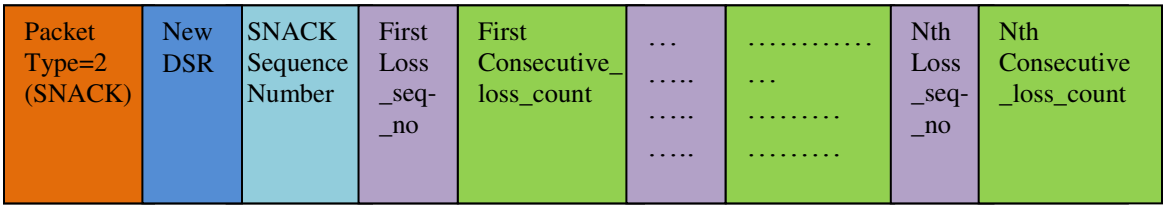

Figure D.2 SNACK Packet Format

The working of selective packet retransmissions and recovery is demonstrated in the following rounds.

Round 1

1. For time interval T_k, while the Retransmission timer is not expired and when connection is established,

   The CU calculates the new DSR=12 and informs to the sensor node with an initial SNACK packet.

   After reception of this packet, the Sensor Node identifies it as SNACK packet as packet type field =2, and get information about the DSR, so it sends 12 (i.e. packets with sequence numbers 1 to 12) packets towards CU. Then it updates the following parameter.

   - Generate_counter=0+12=12
   - SNACK=0, D_{SNACK}=0
   - SQ=1 to 12.

2. CU receives packets with sequence number 1, 2 and 6. CU calculates the following value.
    - Gap=6-2+1=3
    - Loss_rate=0+3=3
    - Receive_counter=0+3=3 (for packets 1, 2, 6)
    - Loss_counter=0+3=3

    Next, CU receives packets with sequence number 7, 8, 9 and 12.
    - Gap= 2
    - Loss_rate=3+2=5
    - Receive_counter=3+4=7 (for packets 7-9, 12)
    - Last_loss=11
    - Last_recv=12
    - Loss_counter=0+Loss_rate=0+5=5
    - Now the CU calculate the Retx_rate
        - Retx_rate=ceil (5/2) = ceil (2.5) =3 packets
        - CU chooses the highest sequence numbered three packets out of all the loss packets.
        - CU selects packets having sequence number 5, 10 and 11 for retransmission.
        - Then CU stores these three sequence numbers in its Loss_table.
3. The CU generates a new SNACK packet and fills its field with following values and sends it towards the sensor node.
    - packet type=2 i.e. SNACK packet
    - the new DSR=17 packets
    - the SNACK sequence number is 1
    - first Loss_seq_no=5 and its Consecutive_loss_count=0 (no consecutive loss) i.e. packet 5 only
    - second Loss_seq_no=10 and its Consecutive_loss_count=1 i.e. 10 and 11 (10+1=11)

2	17	1	5	0	10	1		

Round 2

1. After receiving the SNACK packet, the sensor node S_2 checks its fields.
    - Update the DSR=17
    - Generate_counter=12+17=29
    - SNACK=1
    - D_{SNACK}=0
    - SQ=5,10,11,13,14,……25,26

    Sensor node transmits these packets towards CU
2. CU receives 5,10,11,13,14,15, 23,24,25.
    - Gap=7 (packets 16-22)
    - Loss_rate=7
    - Receive_counter+=9=7+9=16
    - Next the Gap=1(for packet 26)
    - Loss_rate=7+1=8,
    - Last_loss=26
    - Last_recv=25
    - Loss_counter+=8=5+8=13
    - Retx=ceil (8/2) = 4
    - CU selects packets 20,21,22,26 for retransmission
3. CU generates a new SNACK packet, fills the following value and then sends the SNACK towards the sensor node.

4. Let's assume a case, when Retransmission timer expired and SNACK=0 (no SNACK packet received) at the sensor node, then the sensor node S_2 will retransmit all the packets from1-12.

Round 3

1. After receiving the SNACK packet, sensor node S_2 checks its fields.
   - Update the DSR=24
   - Generate_counter=29+24=53
   - SNACK=2
   - D_{SNACK}=2
   - SQ=20-22, 26, 27-46
   - Sensor node transmits these packets towards CU
2. CU receives packets 21, 22, 26, 27-35, 37-39, 41-43.
   - Gap=1, 1, 1, 3
   - Loss_rate=1+1+1+3=6
   - Receive_counter+=18=16+18=34
   - Last_loss=46
   - Last_recv=43
   - Loss_counter+=6=13+6=19
   - Retx=ceil (6/2) = 3
   - CU selects packets 44, 45, 46 for retransmission
3. CU generate a new SNACK packets and calculate the new DSR=32, fills the desire value and send it towards sensor node.

Note: The steps 1-3 are repeated until time interval T_k expires.

BRIEF BIODATA OF RESEARCH SCHOLAR

Madhumita Kathuria has completed her B.E (Computer Science and Engineering) from Biju Patnaik University of Technology, Odisha in 2000 and M. E. (Computer Science and Engineering) from Maharishi Dayanand University, Rohtak in 2007. She is pursuing her Ph. D in (Computer Engineering) from YMCA University of Science and Technology under the supervision of Dr. Sapna Gambhir (Assistant Professor in Department of Computer Engineering, YMCA University of Science and Technology). Presently she is working as Assistant Professor in Department of Computer Science and Engineering at Faculty of Engineering and Technology, Manav Rachna International Institute of Research and Studies from 2006. She is having 12 years of teaching experience. She has published more than 15 papers in various International and National journals and conferences. Her area of interests includes Wireless Body Area Network, Sensor Network, Network Security, Digital Image Processing, Learning and Computational Techniques.

List of Published papers

S. No	Title of Paper	Name of Journal where published	No.	Volume and Issue	Year	Pages
1.	A novel Optimization Model for Efficient Packet Classification in WBAN	International Journal of Energy, Information and Communications, SERSC publisher	ISSN: 2093-9655	Vol.7 Issue 4	2016	1-10
2.	Comparison Analysis of proposed DPPH protocol for Wireless Body Area Network	International Journal of Computer Applications (IJCA)	ISSN: 0975-8887	Vol. 144 Issue 10	2016	36-41
3.	Improvement of Quality of Service parameters in dynamic and heterogeneous WBAN	Indonesian Journal of Electrical Engineering and Informatics (IJEEI), Advanced Engineering and Science (IAES) publisher	ISSN: 2089-3272	Vol. 4 Issue 4	2016	299-306
4.	Performance Optimization in WBAN using Hybrid BDT and SVM Classifier	International Journal Information Technology and Computer Science (IJITCS), MECS PRESS	ISSN: 2074-9015	Vol. 8 Issue 12	2016	83-90

List of Accepted Papers

S.No	Title of Paper	Name of Journal where published	No.	Volume and Issue	Year
1	Dynamic Priority based Packet Handling protocol for Healthcare Wireless Body Area Network system	International Journal of Computational System and Engineering(IJCSYSE), Inderscience	ISSN:2046-3405	In Press	2017

List of Communicated Papers

S. No	Title of Paper	Name of Journal where published	Present Status	Year
1	A Novel Selective Retransmission approach for the guaranteed transmission of critical packets in a Medical WBAN (MWBAN)	Biomedical Signal Processing and Control, Elsevier, ISSN: 1746-8094	Under Review	Nov. 2017
2	Critical Condition Detection using Lion hunting optimizer and SVM classifier in a Healthcare WBAN	Journal of Organizational and End User Computing (JOEUC), IGI Global, ISSN:1546-2234	Under Review	Sept. 2017
3	Optimal Quality of Service for Healthcare WBAN based on cooperative hunting behavior of Lion	Internetworking Indonesia Journal (IIJ), ISSN: 1942-9703	Under Review	June 2017

List of Published papers in Conferences

S. N.	Title of Paper	Name of Conference	Indexing	Pages	Year
1.	DWBAN: Dynamic priority based WBAN architecture for healthcare system	3rd International conference on Computing for Sustainable Global Development	IEEE Xplore, Google Scholar	1-6	2016
2.	Priority based congestion control in WBAN	Eighth International conference on contemporary computing	Scopus, DBLP, IEEE Xplore, Google Scholar	428-433	2015
3.	Reliable delay sensitive loss recovery protocol for critical health data transmission	International Conference on Futuristic Trends on Computational Analysis and	IEEE Xplore, Google Scholar	333-339	2015
4.	Leveraging machine learning for optimize predictive classification and	International Conference on Recent Advances and Innovations in Engineering	IEEE Xplore, Google Scholar	1-7	2014
5.	Genetic Binary Decision Tree based Packet Handling schema for WBAN system	International conference on Recent Advances in Engineering and Computational	IEEE Xplore, Google Scholar	1-6	2014
6.	Quality of service provisioning transport layer protocol for WBAN system	International Conference on Optimization, Reliability and Information	IEEE Xplore, Google Scholar	222-228	2014

7.	Layer wise Issues of Wireless Body Area Network: A Review	International conference on Reliability, Infocom Technologies and	Google Scholar	330-336	2013
8.	Security and Privacy Assault of Wireless Body Area Network System	International conference on Reliability, Infocom Technologies and	Google Scholar	223-229	2013