A Strict Quality of Service MAC Framework for Emergency Traffic in Wireless LANs

by

Shuaib Karim Memon

A thesis submitted to
School of Engineering, Computer and Mathematical Sciences,
Auckland University of Technology
in fulfilment of the requirements for the degree of
Doctor of Philosophy (PhD)

I dedicate this thesis to my parents, brothers
and lovely wife for their unconditional love
and support.

Abstract

The increasing usage of wireless local area networks (WLANs) in distributed emergency services (e.g., for natural or manmade disasters, telemedicine, and health care) and other time-critical applications requires an efficient medium access control (MAC) protocol. This MAC protocol would support emergency traffic and provide a strict quality of service (QoS) guarantee in saturated emergency applications where a high number of nodes report an emergency. The IEEE 802.11e working group enhanced the 802.11 MAC protocol to support QoS. However, recent studies have shown that the 802.11e standard has limitations since it neither supports emergency traffic nor provides a QoS guarantee under medium-to-high traffic loads.

In this thesis, a strict QoS MAC framework for emergency traffic in distributed WLANs under medium-to-high traffic loads is investigated. This framework is based on novel MAC protocols supporting emergency traffic in WLANs. This research first proposes a multiple preemptive MAC protocol (termed as multi-preemptive enhanced distributed channel access [MP-EDCA]), which was developed by modifying an enhanced 802.11e standard (EDCA) in which high priority emergency traffic is given the privilege to preempt the low priority traffic in accessing the medium. A significant network performance gain with respect to lower delays for lifesaving emergency traffic is obtained with MP-EDCA under medium-to-high traffic loads. The improved performance is achieved by modifying the slot time and short inter-frame space in the frame header.

One of the most crucial mechanisms for providing a strict QoS guarantee in WLANs is admission Control. The admission control estimates the state of the network's resources and thereby decide the emergency traffic flow that can be admitted without promising more resources than are available and therefore violating a previously made guarantee. Thus, a preemptive admission control MAC protocol is developed and reported in this thesis to support a strict QoS guarantee for emergency traffic in WLANs.

To serve more emergency nodes in WLANs, it is useful to be able to redesign frame aggregation and BlockAck method of MP-EDCA protocol mentioned earlier. The frame aggregation with a simple 2-bit BlockAck scheme (called FASBA) for MP-EDCA is investigated in this thesis. FASBA enhances the capabilities of MP-EDCA, provides assurance of service delivery and offers higher throughput performance by reducing MAC transmission overheads.

Table of Contents

Declaration of Originality

I certify that this thesis does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any university; and that to the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text. This thesis has been proofread by a professional editor who has made no contribution to the intellectual content of the thesis or been involved in rewriting text.

.

____

Shuaib Karim Memon
AUT, New Zealand
February, 2019

Acknowledgements

First and foremost, I thank my primary supervisor Associate Professor Nurul I. Sarkar for his patience, continuous support, supervision and guidance throughout this research work. His constant motivation and valuable mentoring helped me to complete this PhD research work. I feel the honour to be his PhD student.

I take this opportunity to express my deepest gratitude to my secondary supervisor, Professor. Adnan Al-Anbuky for his guidance, constructive discussions and encouragement during the various phases of this research.

I would like to convey my deepest gratitude to all the members of the Network and Security Research Group (NSRG), AUT. The NSRG has been a source of networking (friendship), good advice and collaboration. I would also like to thank especially Associate Prof. Jairo Gutierrez for his guidance and support.

I would like to acknowledge and express my warm gratitude to my friends and colleagues at AUT, Cornell Institute of Business & Technology, Auckland Institute of Studies and University of Sindh (Pakistan). In particularly, Dr Waseem Ahmad, Ms Fatina Aweidah, Mr. Kourosh Ahmadi, Dr Saghir Ahmad, Dr Imamuddin Khoso for sharing their experience, giving me advice and supporting me throughout my PhD research journey.

I would also like to thank the authorities of the University of Sindh for giving me a PhD scholarship.

I would like to thank the authorities of Auckland Institute of Studies, especially Dr Mike Watts (Academic Head of IT Programme) for his strong support.

Lastly and most importantly, I would like to express my love and gratitude to my wife Noureen Naz, my mother Naseem Akhtar and father Abdul Karim for their patience, love and encouragement helped me to undertake this doctoral journey and successfully prepare this thesis.

Shuaib Karim Memon
Auckland, New Zealand
February, 2019

List of Publications

Manuscripts relating to this research project have been published in the following Journal:

- S. K. Memon, N. I. Sarkar, and A. Al-Anbuky, "Multiple preemptive EDCA for emergency medium access control in distributed WLANs," *Wireless Networks*, vol. 23, pp. 1523-1534, 2017.

Manuscripts relating this research project are under review:

- S. K. Memon, N. I. Sarkar, and A. Al-Anbuky, "Preemptive admission control (PAC) for providing strict QoS guarantee in WLANs" – Journal Paper
- S. K. Memon, N. I. Sarkar, and A. Al-Anbuky, "A frame-aggregation with simple block acknowledgement (FASBA) for providing guarantee of service delivery in WLANs" – Journal Paper
- S. K. Memon, N. I. Sarkar, and A. Al-Anbuky, " Future of 802.11 MAC Protocols for Providing QoS Guarantee and Supporting Emergency Traffic: A Survey" – Journal Paper
- S. K. Memon, N. I. Sarkar, and A. Al-Anbuky, "Supporting emergency traffic in Wireless Networks" – Book Chapter

List of Figures

List of Tables

List of Abbreviations and Acronyms

802.11	IEEE 802.11
AC	Admission Control
AC_BE	Access Category Best Efforts
AC_BK	Access Category Background
AC_VI	Access Category Video
AC_VO	Access Category Voice
ACK	Acknowledgement
ACM	Access Category Mandatory
ADDTS	Add Traffic Stream
A-EDCF	Adaptive EDCF
AIFS	Arbitration Inter-frame Space
AIFSN	Arbitration Inter-frame Space Number
A-MPDU	Aggregated MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
AP	Access Point
ATA	Adaptive TXOP Allocation
ATIM	Announcement Traffic Indication Message
BE	Best Effort
BK	Background
BlockAck	Block Acknowledgement
BSS	Basic Service Set
BUMA	Buffer Unit Multiple Access
CA	Contention Adaptation
CAP	Controlled Access Phase
CCA	Clear Channel Assessment
CCPS	Centralised Channel Preemption Scheduling
CFP	Contention Free Period

CP	Contention Period
CP-EDCA	Channel Preemptive Enhanced Distributed Channel Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
CW	Contention Window
DCF	Distributed Coordination Function
DiffServ	Differentiated Services
DIFS	Distributed Coordination Function IFS
DSR	Design Science Research
DSSS	Direct Sequence Spread Spectrum
ECG	Electro Cardio Gram
EDCA	Enhanced Distributed Channel Access
EDCA-DRR	EDCA Distributed Resource Reservation
EDCA-LA	EDCA Link Adaption
EDCA-RR	EDCA Resource Reservation
EDCF	Enhanced Distributed Coordination Function
EP	Emergency Priority
FACU	Feedback-based Admission Control Unit
FASBA	Frame Aggregation with Simple Block Acknowledgement
FCR	Fast Collision Resolution
GHz	Giga Hertz
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
GUI	Graphical User Interface
HC	Hybrid Coordinator
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
HT	High Throughput
HTA	Holding Time Aggregation
IBSS	Independent Basic Service Set
I-EDCA	Improved EDCA
IEEE	Institute of Electrical Electronics Engineers

IFS	Inter-frame Space
IntServ	Integrated Services
IP	Internet Protocol
IPSD-EDCA	Improve Performance & provide Service Differentiation in EDCA
LASO	Latency Aware Service Opportunity
LPT	Low Priority Traffic
MAC	Medium Access Control
Max	Maximum
Mbps	Megabits per seconds
M-EDCF	Modified EDCF
MHz	Mega Hertz
MIMO	Multiple Input Multiple Output
Min	Minimum
MPDU	MAC Protocol Data Unit
MP-EDCA	Multi-Preemptive Enhanced Distributed Channel Access
MS	Milliseconds
MSDU	MAC Service Data Unit
NP	Normal Priority
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
PAC	Preemptive Admission Control
PC	Point Coordinator
PCF	Point Coordination Function
PDF	Probability Density Function
PHY	Physical
PIFS	Point Coordination Function IFS
PRED	Priority Random Early Detection
QAP	QoS Access Point
QBSS	QoS Basic Service Set
QHDCF	High-performance DCF with QoS support
QoS	Quality of Service
QSTA	QoS Station

RAM	Random Access Memory
RAMPS	Random Adaptive Method to adjust MAC Parameters
RED	Random Early Detection
RtoE	Risk to Environment
RtoH	Risk to Health
RtoL	Risk to Life
RtoP	Risk to Property
RTS	Request To Send
SIFS	Short Inter-frame Space
SPQAMP	Strict Priority base QoS Award MAC Protocols
STA	Station
SW-ARQ	Stop and Wait Automatic Repeating request
TC	Traffic Category
TCP	Transmission Control Protocol
TID	Traffic Identification
TS	Traffic Stream
TSPEC	Traffic Specification
TXOP	Transmission Opportunity
UDP	User Datagram Protocol
UP	User Priority
VI	Video
VO	Voice
VoD	Video on Demand
VoIP	Voice over Internet Protocol
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

Chapter 1

Introduction

In recent years, there has been a remarkable growth in the deployment of IEEE 802.11-based wireless local area networks (WLANs) under the brand name Wireless Fidelity (Wi-Fi) [1, 2]. This growth is due to the low cost, international standards (e.g., 802.11a, b, g, n, and ac) flexibility and mobility offered by the technology. The WLANs have been deployed almost everywhere, for example, in workplaces, homes, educational institutions, libraries, offices, shopping malls, stock markets, cafeterias, buses stops, airports, hospitals, health care centres, and disaster-affected areas [3]. Simultaneously, there has been significant growth in the use of time-sensitive applications, such as real-time video conferencing, voice over internet protocol (VoIP), internet protocol television (IPTV), video on demand (VoD) and in distributed emergency services (e.g. disaster surveillance, health monitoring system) over WLANs [4, 5]. The time-sensitive applications and emergency services are both not only characterised by their high bandwidth requirements but also impose strict restrictions on packet delays, jitter and packet losses and require a quality of service (QoS) guarantee. In addition to a QoS guarantee, emergency traffic requires in-channel preemption support (e.g., channel access priority on arrival).

The medium access control (MAC) protocol is a key factor influencing the performance of WLANs. The IEEE 802.11e working group enhanced the 802.11 MAC to provide QoS to time-sensitive applications in WLANs. IEEE 802.11e defines a mechanism termed hybrid coordination function (HCF), which includes two channel access mechanisms: (1) HCF controlled channel access (HCCA), and (2) enhanced distributed channel access (EDCA). HCCA is a centrally controlled reservation-based MAC protocol, which is rarely implemented on real systems because of its higher design complexity, inefficiency for normal data transmission and lack of robustness [6]. In contrast, EDCA is a distributed contention MAC protocol that provides QoS by adjusting inter-frame spaces (IFSs) and contention window (CW) sizes. EDCA is simple and easy to implement [7].

1.1 Motivation and Research Objectives

The increasing usage of distributed emergency services (for natural disaster or disaster caused by humans, telemedicine and health care) in WLANs requires the support of immediate channel access together with a strict QoS guarantee from MAC. The IEEE 802.11e (EDCA) standard is the MAC enhancement for QoS. However, the 802.11e (EDCA) has several performance limitations. The key limitations include no inherent support for emergency traffic [8, 9], neither provide QoS guarantee [10-14] nor works well under medium-to-high traffic load [15, 16].

Supporting emergency traffic by providing it with a strict QoS guarantee for WLAN under medium-to-high traffic loads is a challenging task. In the past 20 years, various QoS-aware MAC schemes have been proposed by many network researchers. Most of the schemes focus on either network capacity enhancement or service differentiation by adjusting the CW or IFS. While attempts have been made to develop methods for achieving a QoS guarantee, the problem of supporting emergency traffic as well as providing strict QoS guarantee under medium-to-high traffic conditions is yet to be fully solved [12, 17-24]. Therefore, the primary objective of this research was to develop a strict QoS-aware MAC framework to support emergency traffic by redesigning an enhanced IEEE 802.11e standard (EDCA). To achieve this aim, the following objectives have been set:

- To design and evaluate a novel QoS-aware MAC protocol to support emergency traffic in distributed WLANs.
- To design and evaluate a preemptive admission control (PAC) MAC protocol for strict QoS guarantee in WLANs.
- To redesign frame aggregation with a simple block acknowledgement MAC protocol to reduce the transmission overhead, enhance throughput performance and provide a guarantee of service delivery in WLANs.

1.2 Research Methodology for Investigation

The main objective of this thesis is to develop a strict QoS MAC framework for supporting emergency traffic with the provision of a strict QoS guarantee in WLANs. To achieve this research objective, extensive computer simulations were used as a primary tool for modelling the network and evaluating the performance of WLANs. In addition, the analytical modelling approach is also applied to some extend to study the system performance.

Figure 1.1 outlines the methodology adopted in this thesis. Both simulation and analysis were used to develop three MAC protocols: (1) multi-preemptive enhanced distributed channel access (MP-EDCA; Chapter 4) for supporting emergency traffic in the medium, (2) PAC-MP-EDCA (Chapter 5) for providing a QoS guarantee, (3) and frame aggregation with block acknowledgement (Chapter 6) for reducing the transmission overheads, enhancing throughput performance, lowering delay and increasing the number of high priority emergency nodes. These three MAC schemes constitute a framework. The advantages of the framework are accommodating an increased number of lifesaving emergency nodes in the network, giving privilege to high priority emergency traffic to preempt the low priority traffic and access the channel, and providing a QoS guarantee to lifesaving emergency services in terms of packet delays.

Considering the requirements of this research, testing the performance of the proposed MAC protocols in the real-world environment is highly expensive. Thus, this research adopts computer simulations to test and evaluate the performance of the proposed WLAN MAC protocols. Moreover, the simulation approach allows generalisation of the findings by testing various network scenarios. To choose the computer simulation tool, various simulations tools were analysed. The Riverbed Modeler (also known as OPNET Modeler) version 18.0 was chosen because it is a credible simulation tool used by network researchers worldwide [25, 26]. Certain authors in [27] have ranked Riverbed Modeler at the third position among various simulation tools used in network communication research published in the years 2007-2009. Moreover, Riverbed Modeler provides a development environment with many built-in tools to develop wireless technologies and protocols, and evaluate their performance before actual commercial production.

Moreover, the network, node, and process models of Riverbed Modeler were customised to implement the proposed MAC schemes (presented in Chapter 4 to 6). Extensive simulations were performed to evaluate the performance of the proposed MAC protocols. Simulations were also used for validation of the proposed models by comparing the simulation results with those of other MAC protocols in the related studies. Moreover, MATLAB was used in Chapter 6 to evaluate the performance of the mathematical concepts of the designed algorithms.

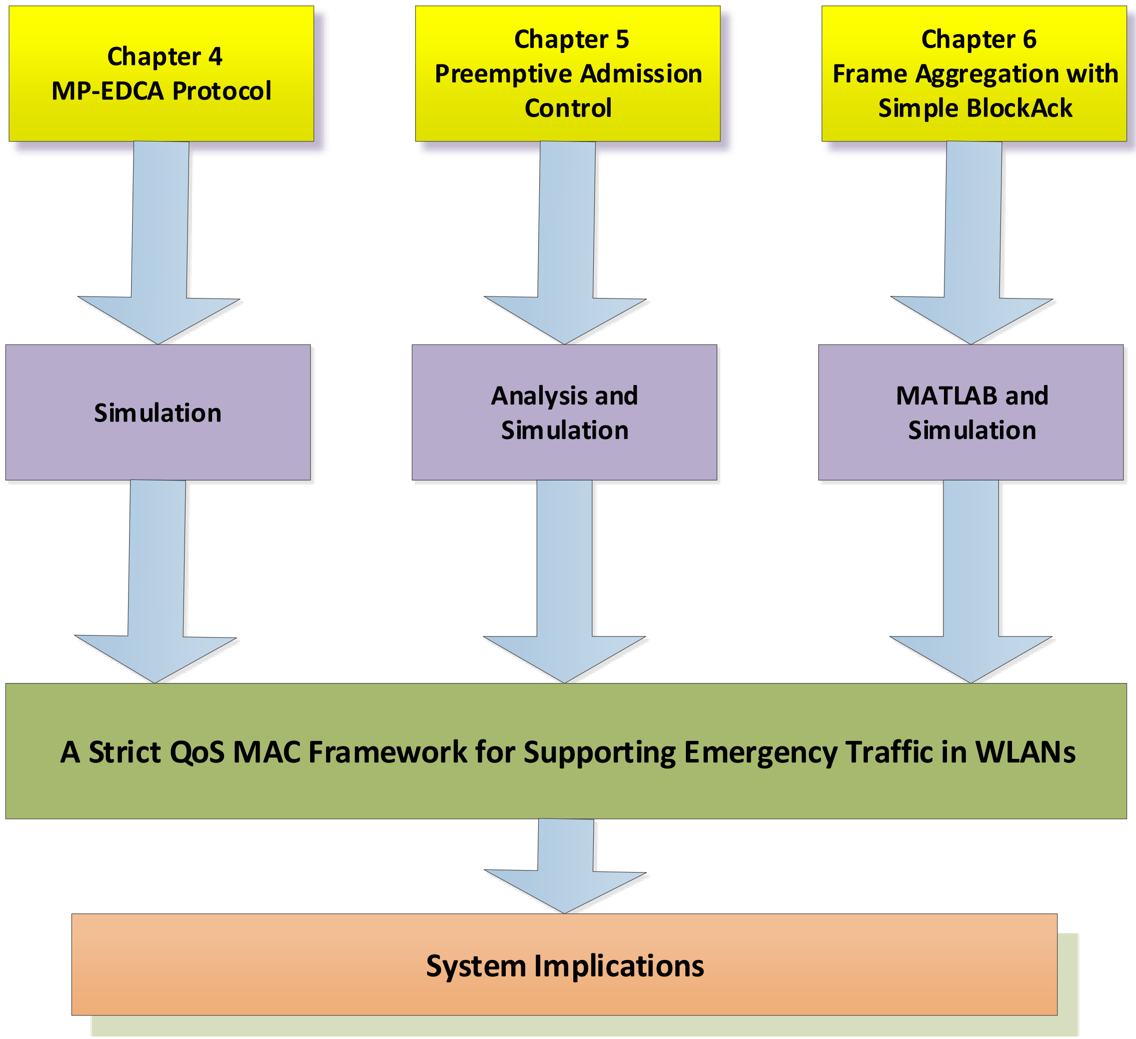

Figure 1.1: Block diagram of the adopted methodology.

1.3 Research Process Adopted

This thesis adopted a customised multi-methodological approach of the design science research (DSR) process, proposed by Nunamaker, Chen and Pudin [28] for developing the framework for supporting and providing a QoS guarantee in WLANs.

The multi-methodological approach serves as a commonly accepted framework for DSR. This methodology was suitable for this thesis since it is a fully connected model and incorporates the principles, practices and procedures required to conduct investigation during research. **Figure 1.2** shows the adapted customised multi-methodological approach to information science (IS) research.

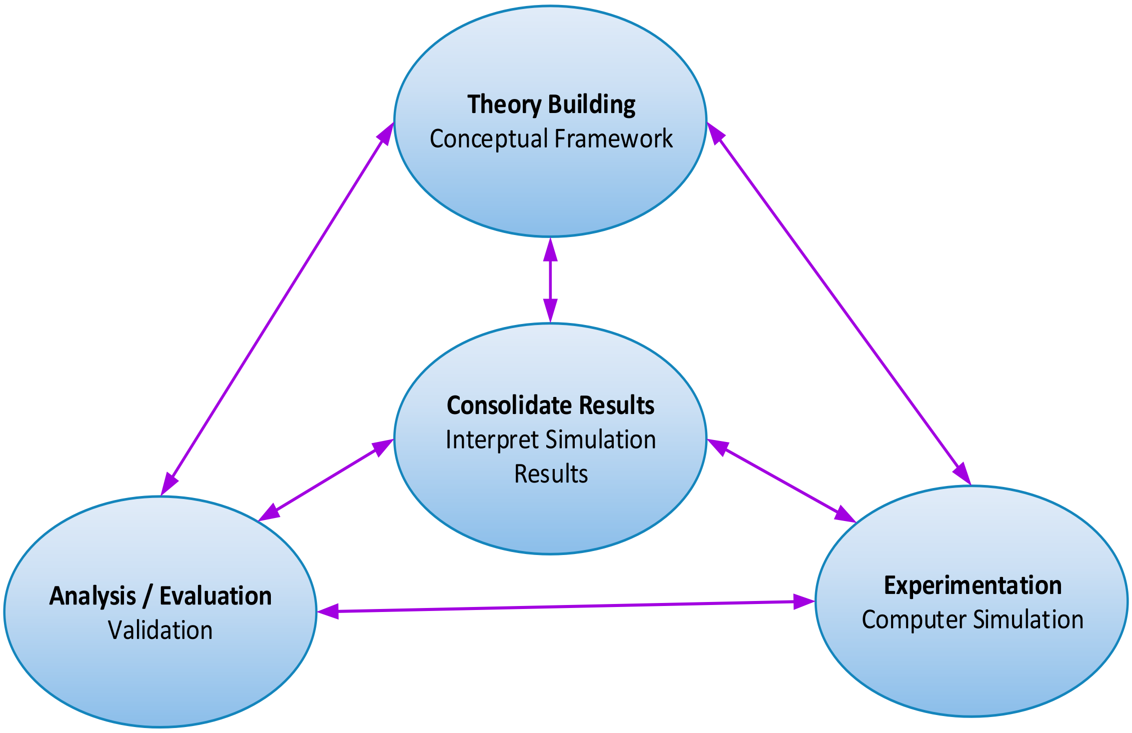

Figure 1.2: Customised multi-methodological approach used to perform this research.

The multi-methodological approach to IS of the DSR methodology includes four phases: theory building, experimentation, systems development and observation. Each phase contains a set of activities undertaken to achieve specific goals. The observation phase incorporates case studies, survey and field studies, which is for future work and is not included in the present research. Moreover, the systems development phase is customised to consolidate results. The entry point of the present research is theory building where the conceptual framework is constructed. System prototypes are set in the experimentation phase, and network simulations are performed in this phase. Analysis/Validation is very important for the undertaken research. A new phase, namely analysis/validation is created to assign due importance to these activities. This phase works as a bridge between the theory building phase and experimentation phase and may concern itself with either the validation of the underlying theories (looking backwards along the research life cycle) and contributing to theory building. Finally, the performance and usability of the proposed system is tested in the customised consolidate results phase. This phase also includes identification of strengths and weakness of the proposed system and interpretation of simulation results. Table 1.1 shows the four phases involved in the customised multi-methodological approach and their relationship to this research.

Table 1.1: Four phases of customised multi-methodological approach and its relationship to this research.

Phases	Relationship to this research
Phase 1 **Theory building**	This phase includes a review of the literature, identification of the problem, formulation of questions, development of ideas and concepts, construction of a strict QoS MAC conceptual framework, new methods and system models (e.g., analysis and simulation models).
Phase 2 **Experimentation**	This phase consists of research strategies such as simulations. This phase is guided by theory building. Results from network simulations may be used in the evaluation phase to refine theories and improve the system.
Phase 3 **Evaluation**	The observation phase is modified to the evaluation phase. This phase includes validation of simulation models and comparison of results.
Phase 4 **Consolidate results**	The system development phase is modified to the consolidate results phase. The performance and usability of the proposed system is tested and its strengths and weakness are identified. Finally, the simulation results are interpreted.

1.4 Contributions and the Structure of this Thesis

The overall structure of this thesis is shown in **Figure 1.3**. The figure presents three main sections, including the introductory part, main contributions and concluding remarks. It is important to develop a strong foundation for these areas before considering emergency support. The introductory chapter (Chapters 2 and 3) provide the foundation and background material for the thesis.

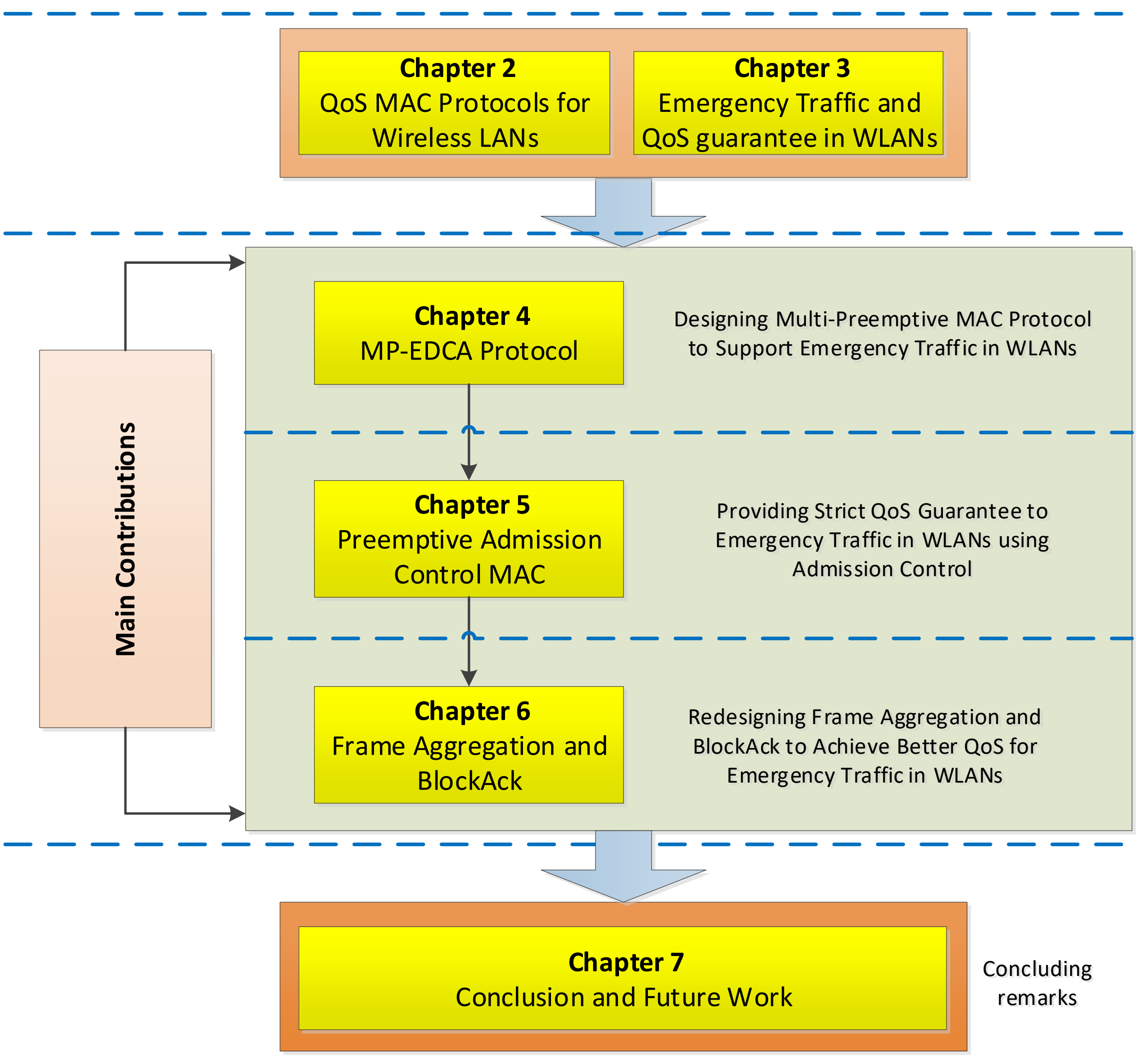

Figure 1.3: Structure of this thesis.

Chapter 2 provides an introduction to the QoS and WLANs. The QoS parameters are outlined. Applications from the QoS perspective are identified and described. The 802.11 MAC layer is described. In particular, the 802.11e MAC layer, including EDCA, and HCCA are described. The block acknowledgement and admission control scheme that affect the network performance are also discussed.

Chapter 3 describes emergency services and categories of emergency traffic. The performance of WLANs is highly influenced by MAC protocols. An in-depth review of literature in the areas of the QoS and emergency traffic support in wireless MAC protocols is provided. The chapter describes the previous research on providing service differentiation, and a QoS guarantee and supporting emergency traffic in WLANs.

The original contributions of this thesis are presented in Chapters 4 to 6, which are primarily concerned with supporting emergency traffic, providing strict QoS guarantee and enhancing throughput performance of WLAN performance.

Chapter 4 reports the design of a QoS-aware wireless MAC protocol termed the MP-EDCA protocol. The MP-EDCA protocol is developed by redesigning the 802.11e EDCA standard for supporting emergency traffic. For providing better emergency traffic support, organisations dealing with emergency services are studied. It is reported that organisations give priority to lifesaving emergency followed by health, property and environment.

MP-EDCA gives privileges to high priority lifesaving emergency traffic to preempt the ongoing traffic stream for immediate channel access and accommodate larger number of lifesaving emergency nodes. The Riverbed Modeler 18.0 evaluates the performance of MP-EDCA.

In Chapter 5, a PAC-MP-EDCA protocol is developed and reported. It protects existing high priority emergency traffic from other high priority or low priority emergency traffic. In this chapter, PAC-MP-EDCA is described and simulation results are presented to verify that the MP-EDCA performance can be enhanced with PAC.

Chapter 6 describes a method of frame aggregation with a simple block acknowledgement (termed FASBA) to achieve high throughput for emergency traffic in WLANs. FASBA enhances the throughput performance, increases the number of emergency nodes in the network, and provides a guarantee of service delivery in WLANs. FASBA is described and simulation results are presented to verify that the protocol’s performance is better than that of MP-EDCA protocol.

The thesis is summarised and concluded in Chapter 7.

Chapter 2

QoS MAC Protocols for WLANs

2.1 Introduction

In Chapter 1, the motivations for supporting emergency traffic and providing a strict QoS guarantee in WLANs were outlined. A primary objective of this thesis is to develop a framework for WLANs, which supports emergency traffic and provides a strict QoS guarantee for lifesaving emergency traffic in a dense emergency situation where a high number of nodes report the emergency. To achieve this objective, a general understanding of WLANs is required. This chapter aims to introduce various key concepts of WLANs that are necessary for designing, modelling and developing such a framework.

Section 2.2 describes QoS parameters used in this thesis for evaluating the performance of QoS WLAN MAC protocols. The applications from the QoS perspective are highlighted in Section 2.3. Factors which affect the QoS are summarised in Section 2.4. Section 2.5 has four subsections. The IEEE 802.11 standards are discussed in Subsection 2.5.1. In Subsection 2.5.2 the evolutionary path for adopting WLAN technology is outlined. The architecture of typical WLAN focusing on both ad hoc and infrastructure networks, is explained in Subsection 2.5.3. MAC is one of the important components of 802.11 WLANs that influence the QoS performance, and the IEEE 802.11 MAC protocol, including distributed coordination function (DCF) and point coordination function (PCF) are described in Subsection 2.5.4.

Section 2.6 describes IEEE 802.11e, which is an enhancement of the 802.11 MAC layer for the QoS. The 802.11 MAC protocols implemented in 802.11e namely EDCA and HCCA, are also outlined in this section. Section 2.7 highlights the transmit opportunity, frame aggregation, and block acknowledgement schemes introduced by IEEE 802.11e to enhance throughput performance. The WLAN admission control is described in Section 2.9. Finally, the chapter is summarised in Section 2.10.

2.2 Quality of Service (QoS)

Different communities perceive and interpret QoS in different ways. For example, the network communities refer to it as the "measure of service quality provided by the network to the users". Another side, the Internet Engineering Task Force considers QoS as "a set of service requirements to be met by the network while transporting a flow" [29]. The main objective is to provide the QoS while maximising network resource utilisation. The network user community refers to QoS as the quality perceived by applications/users. The International Telecommunication Union (ITU) defines QoS as "the ability of a network or network portion to provide the functions related to communications between users" [30].

In fact, the concept of QoS is very broad. Over IP networks, QoS is more technically oriented, focusing on monitoring and improving network performance metrics such as packet delay, jitter, packet loss, and throughput. Table 2.1 illustrates the commonly used network performance metrics [31].

Table 2.1: Commonly used network performance metrics.

Metric	Description
End-to-end packet delay (latency)	The time required to transfer a packet across a network
Jitter (delay variance)	Variability of packets delay within the same packet stream. For example, if delay of packet 1 is 8 ms and delay of packet 2 is 5 ms then jitter is 3ms.
Packet loss	Router or end devices will drop packets when buffer capacity is full, causing packet loss.
Throughput	The amount of data successfully delivered over the communication channel, usually measured in bits per second or packets per second.

MAC sub-layer is one of the key components, which influence the performance of the network. IEEE 802.11e working group enhances the capabilities of traditional 802.11 MAC by prioritising traffic in EDCA. However, EDCA has limitation as it neither support emergency traffic nor provide QoS guarantee. Therefore, this research enhances the capabilities of existing 802.11e MAC sub-layer for prioritising emergency traffic providing strict QoS guarantee.

2.3 Applications from the QoS Perspective

In recent years, the use of different applications over WLANs has grown significantly. From the QoS perspective, these applications can be categorised into three different groups [32]. Figure 2.1 illustrates various application from the QoS perspective. These applications from the QoS perspective are described as follows:

- Applications with quantitative QoS specifications: These applications require a strict QoS guarantee. These applications have specific requirements and impose strict restrictions on packet delay, jitter, packet loss and throughput. For example, the required one-way end-to-end delay for voice packet is 150 ms [33].
- Applications with qualitative specifications: These applications require QoS, but do not have any specific requirements to describe the desired treatment. For example, web browsing needs QoS but does not have any specific QoS requirement.
- Applications without qualitative specification: These applications do not require any QoS. For example, an application that runs in the background.

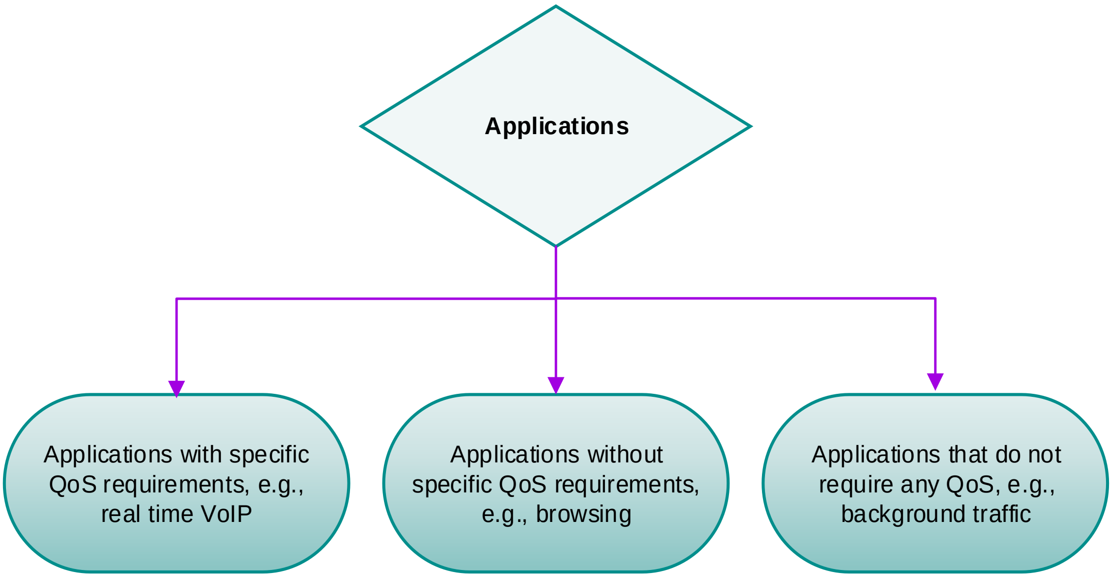

Figure 2.1: Applications from QoS perspective.

2.4 Factors affecting QoS

There are various factors, which are present in the realistic environment and affect the QoS in terms of throughput, delay and packet loss. These factors are: network load, node mobility, noise, hidden nodes, channel fading, and security.

Network load: The network load is the key factor, which affects the QoS as all the nodes in one wireless network share the medium. Increasing the node in a network means increasing the channel access contention among the nodes. The increase network load increase the collision rate, decrease throughput performance, increase delay and cause of packet loss. [34].

The main objective of this research to support emergency traffic and provide strict QoS guarantee under medium to high traffic load. Therefore, we investigated performance of proposed MAC protocols considering the network load from low to high.

Node mobility: The node mobility affects the performance of the network. The increase distance between sender node and receiver node decrease the network performance due to weak signal strength and cause low throughput, higher delay and increase bit error rate (BER) [35].

Hidden nodes: A hidden node problem occurs when a node communicates with the AP but cannot communicate with the other node. Figure 2.2 illustrates the hidden node problem. Where node A and node C can communicate with AP but both are out of range (hidden) for each other.

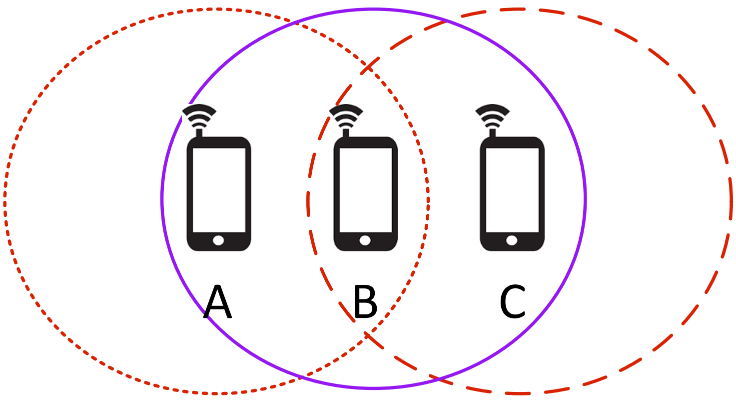

Figure 2.2: Hidden node problems in which Node A and C are hidden to each other.

Channel fading: In the wireless network, channel fading is the gradual loss of signal due to weather (e.g., rain) or obstacles (e.g., walls) and affect the performance of the network [36].

Noise: The noise is an unwanted energy in the signal and may affect the quality of signal. The QoS provided by the network is highly determined by the noise. The lower signal to noise ratio (SNR) may cause bursts of errors. In the wireless network, packets are corrupted due to bit errors cause by the noise. The SNR is measured in decibel (dB). The SNR higher than 40dB is considered excellent signal where a network provides excellent QoS by achieving higher throughput, lower delay and lower packet errors. Another side, SNR lower than 10dB means signal is not good enough for communication. The wireless network assures QoS guarantee wheen SNR is good (i.e., SNR > 25 dB0) [37].

Security: Security and QoS are commonly considered separate paradigms. However, both are linked together when we elaborate the network performance. For example, certain types of attacks on the network security affect the application performance and ensuring the application performance is the main mission of the QoS. In another example, taking the security measures such as encryption before sending the data and decryption when receiving it may increase the delay and overall affect the QoS [38].

2.5 IEEE 802.11 Standards, WLAN Architecture and MAC

2.5.1 IEEE 802.11 Standards

The IEEE 802.11-based WLANs have gained widespread popularity and have become ubiquitous networks [39]. The Physical (PHY) and MAC characteristics of 802.11 are specified in the legacy 802.11-1997 [40] and the latter 802.11a [41], 802.11b [42], 802.11g [43], 802.11n [39], 802.11ac [44] and 802.11ax. PHY and MAC specifications refer to amendments to achieve higher throughput by advancing the modulation and the channel coding. These all 802.11 based standards use the same carrier sense multiple access with collision avoidance (CSMA/CA) as a MAC protocol. They reduce their transmission rate for maximising the coverage area work in both ‘infrastructure’ and ‘ad hoc' modes. There are several MAC amendments to support QoS (802.11e) [45], security (802.11i) [3], and emergency and internetworking (802.11u) [16]. Table 2.2 summarises the main characteristics of 802.11 standards. The evolutionary path of these 802.11 standards is discussed in the next section.

Table 2.2: IEEE 802.11 standards and their technical specifications.

802.11 standards	Release	Freq. (GHz)	Data rate Mbps	MIMO stream	Modulation	Bandwidth MHz	Indoor range (m)	Outdoor range (m)
802.11	June 1997	2.4	1, 2	No	DSSS, FSSS	20	20	100
802.11a	Sep. 1999	5	6, 9, 12, 18, 24, 36, 48, 54	No	OFDM	20	30	120
802.11b	Sep. 1999	2.4	5.5, 11	No	DSSS	20	38	140
802.11g	June 2003	2.4	6, 9, 12, 18, 24, 36, 48, 54	No	OFDM, DSS	20	38	140
802.11n	Oct. 2009	2.4, 5	7.2 to 150 (per stream)	4	OFDM	20, 40	70	250
802.11ac	Dec. 2013	5	7.2 to 6933 (per stream)	8	MIMO-OFDM	20, 40, 80, 160	35	-
802.11ax	2019	2.4, 5	7.2 to 10530 (per stream)	4	Multi-User MIMO-OFDMA	20, 40, 80, 160	35	250
802.11i	Nov. 2004	Based on IEEE 802.11 PHY Characteristics						
802.11e	Nov. 2005	Based on IEEE 802.11 PHY Characteristics						
802.11u	Feb. 2011	Based on IEEE 802.11 PHY Characteristics						

2.5.2 An Evolutionary Path of Adopting WLAN Technology

Generally, IEEE throughput performance has increased over time from 1 Mbps (802.11b) to 7000 Mbps (802.11ac) [3, 16, 39-45] and the anticipated 802.11ax shall offer higher throughput of up to 10 Gbps. This shows that the key focus among all WLAN standards was associated with throughput enhancement. Based on performance, there are various IEEE WLAN standards.

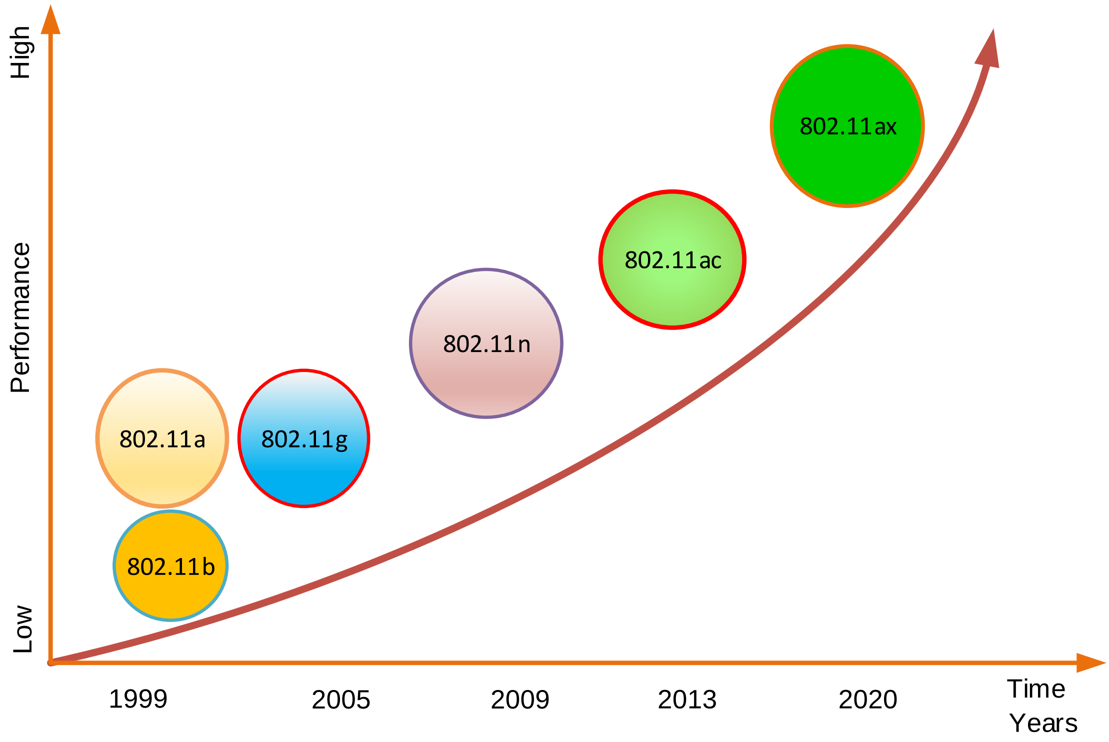

Figure 2.3: Evolutionary path for adopting 802.11 WLANs.

Figure 2.3 shows the evolutionary path for WLAN standards. At the bottom left of the figure, low performance, initially designed WLAN technologies (802.11a and 802.11b) are shown. Both were introduced in 1999. The key differences were in frequency bands and signal modulation techniques. The 802.11b uses the 2.4 GHz frequency band, which is suitable for long distance but has lower throughput (up to 11 Mbps), while the 802.11a uses the 5 GHz frequency band, which provides higher throughput (up to 54 Mbps) over a short distance. In terms of signal modulation, the 802.11a uses orthogonal frequency division multiplexing (OFDM), while the 802.11b uses direct sequence spread spectrum (DSSS).

At the top-right of the evolution path, is the 802.11ax, which is to be publicly released in 2019. In comparison to the 802.11a and 802.11b, the 802.11ax is designed to operate in the 2.4 and 5 GHz frequency bands. The 802.11ax applies orthogonal frequency division multiple access (OFDMA) to improve the overall spectrum efficiency, and thus, it is expected to offer higher user throughput compared with 802.11a and 802.11b. The throughput of 802.11ax is yet to be confirmed, but the predicted throughput is 10 Gbps.

While throughput enhancement has been the focus of the standards, the delay is another major factor that can affect communication systems. During the same period that is 1999 to date, there is significant growth in using different time-critical applications namely emergency services which require QoS support from standards. In 802.11a and 802.11b standards, QoS was not supported. All traffic namely voice, video and background traffic, was treated in the same way. IEEE 802.11e is the MAC enhancement in 802.11 for QoS. The 802.11e categorises the traffic into four categories: voice, video, best-effort and background traffic. However, there was no support for emergency services, which require immediate channel access (minimised delay).

2.5.3 IEEE 802.11 WLAN Architecture

IEEE 802.11 WLAN architecture is based on the basic service set (BSS). A BSS may have one or more wireless stations (STA – known as node) and a central base station termed an access point (AP). WLAN that deploys APs, often considered as infrastructure wireless LAN. In typical infrastructure-based BSS, nodes are connected with AP and the AP is connected with the Ethernet via the wire as illustrated, where Ethernet interconnects the AP with the router in **Figure 2.4**.

In IEEE 802.11 WLAN, STAs may group together (without the AP) to form an ad hoc network for internetworked communications. An ad hoc network without a central control and without connections to the outside world forms an independent BSS (IBSS). **Figure 2.5** is an illustration of an IBSS. An ad hoc network is suitable for dense emergency such as natural or manmade disasters, where relief works form a group and communicate with each other.

An ad hoc network may be categorised into two types, single-hop, and (2) multi-hop networks. In a single-hop network, a station (STA) communicates directly with another neighbouring STA within the transmission range. By contrast, in a multi-hop network, an STA communicates with another STA which may not be in the direct transmission range through intermediate STAs.

Further, in a multi-hop network, an STA communicate with designation STA through multiple intermediate STAs. A multi-hop network may consist of hundreds of STA and is unaffected if an intermediate STA leaves the network. However, many challenges remain in the design of multi-hop ad hoc networks, such as providing strict QoS guarantee, especially in term of end-to-end delay required by time-critical real-time applications, ensuring security or tackling route failure due to mobility of intermediate devices, unreliable wireless channels and lack of centralised control [46, 47].

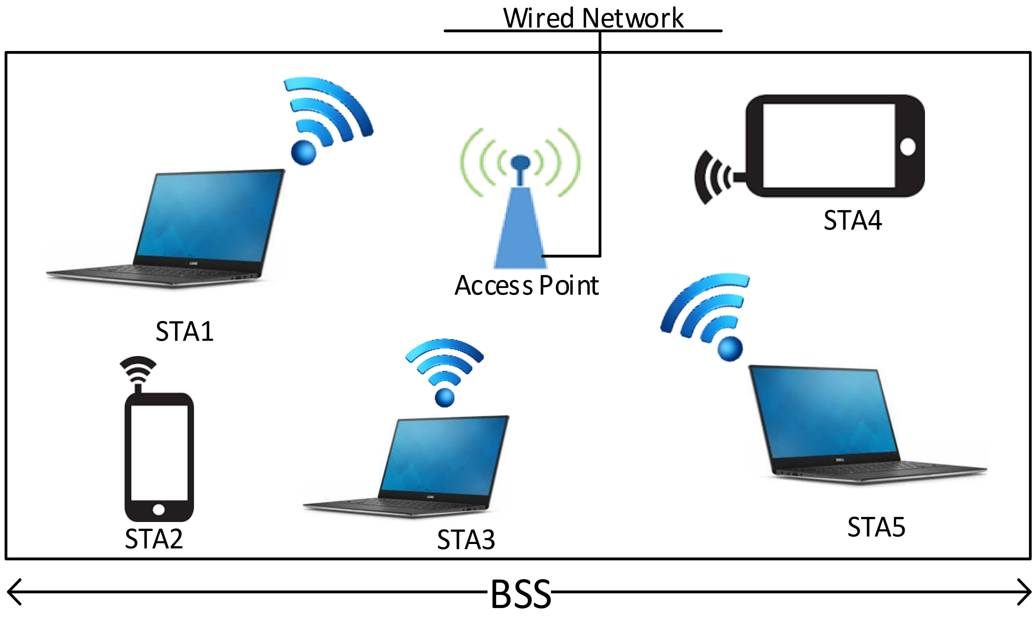

Figure 2.4: A 802.11-based wireless infrastructure network.

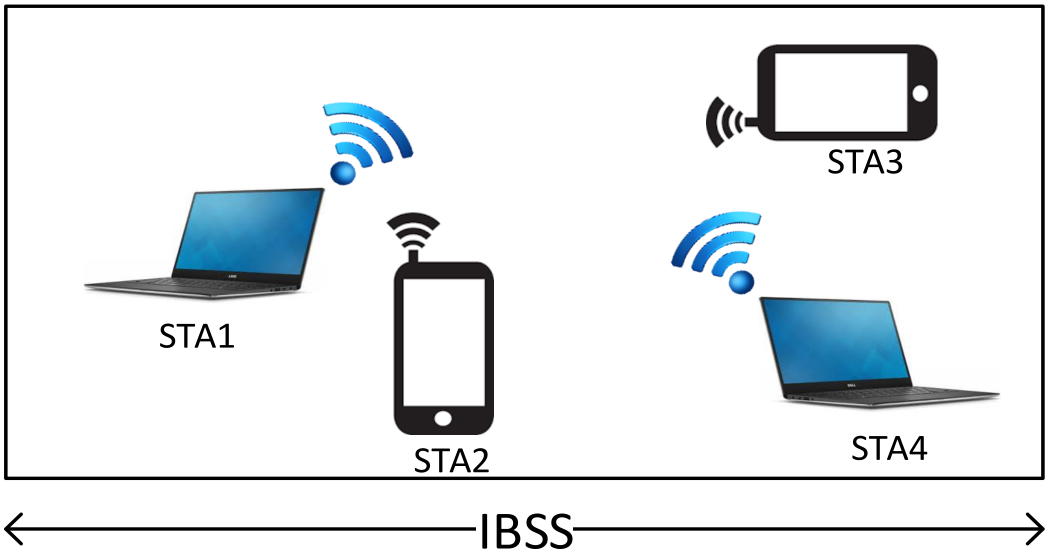

Figure 2.5: A 802.11-based wireless ad hoc network.

2.5.4 IEEE 802.11 MAC

An efficient QoS MAC protocol should provide a QoS guarantee to time-sensitive applications and support emergency traffic together with simplicity of operations and high bandwidth utilisation. Ideally, such a protocol should provide high throughput, and low end-to-end packet delay, jitter, and packet losses, as well as prioritise time-sensitive traffic.

The 802.11 MAC layer is among the most important components of a typical WLAN. The 802.11 MAC provides two access methods: (1) DCF as the core, and (2) PCF as optional. DCF is a contention-based protocol that can provide the best-effort service. The DCF is built on the CSMA/CA medium and optional request to send and clear to send (RTS/CTS) mechanism for sharing the medium among multiple STAs. In CSMA/CA, STA first sense the medium before initiating the transmission. Three IFS intervals are specified in the standard: short IFS (SIFS), point coordination function IFS (PIFS) and DCF-IFS (DIFS). The SIFS interval is the smallest IFS, followed by PIFS and DIFS, in that order. SIFS has highest priority use for acknowledgement, RTS and CTS frames. PCF has medium priority use for time-sensitive applications. DIFS has the lowest priority use for data. Many network researchers have proposed IFS-based schemes to support QoS for time-sensitive applications in the 802.11 MAC layer [48, 49].

In DCF mode, all STAs wait until the channel becomes idle for a DIFS period (see Equation 1). The DIFS period is calculated from DCF parameters. **Table 2.3** lists the DCF parameters of various IEEE 802.11 standards. STAs start the backoff process to avoid collisions. During the process, each STA chooses a random interval, termed backoff timer, calculated from CW: random [0, CW] × SlotTime, where CW = CW minimum (CWmin) $\leq$ CW $\leq$ CW maximum (CWmax); values of CWmin, CW, CWmax and SlotTime are based on the PHY layer. All STAs decrement their backoff timer until the medium becomes busy. If the time has not reached zero and the medium becomes busy, the STA freezes its timer. The STA transmits when its timer decrements to zero.

If two or more STAs' timers decrement 0, a collision will occur. Once an STA transmits the packets successfully, the receiving STA sends an ACK after a SIFS. If STA does not receive ACK packet within the timeout, the transmitting STA retransmits the frame (assuming that the frame has collided). To reduce the probability of collision, CW is doubled until it reaches CWmax.

The PCF provides contention-free (CF) frame transfer. This is available in infrastructure mode, where STAs are connected to the network through an AP. The PCF uses centralised polling approach based on the round robin algorithm. PCF would be suitable for time-sensitive traffic for QoS; however, its algorithm is complex and it is expensive to implement [50].

Table 2.3: DCF parameters of various IEEE 802.11 standards.

Standard	Slot Time	SIFS	DIFS	CWmin	CWmax
802.11a	9µs	16µs	34µs	15	1023
802.11b	20µs	10µs	50µs	31	1023
802.11g	Short = 9 µs Long = 20µs	10µs	Short = 28µs Long = 50µs	Short = 15 Long = 31	1023
802.11n (2.4 (GHz)	Short = 9µs Long =20µs	10µs	Short = 28µs Long = 50µs	Short = 15 Long = 31	1023
802.11n (5 GHz)	9µs	16µs	34µs	15	1023
802.11ac	9µs	16µs	34µs	15	1023
802.11ax	4.5µs	16µs	34µs	15	1023

2.6 IEEE 802.11e for QoS

The IEEE 802.11e [45] working group has developed a new standard, the IEEE 802.11e, to support time-sensitive applications i.e., real-time voice or video conferencing. IEEE 802.11e introduced a new coordination function termed HCF, which provides the combined advantages of DCF and PCF.

HCF uses the mandatory EDCA mechanism for contention-based transfer and an optional HCCA mechanism for contention-free services. Both EDCA and HCCA work on the top of DCF, as shown in **Figure 2.6**.

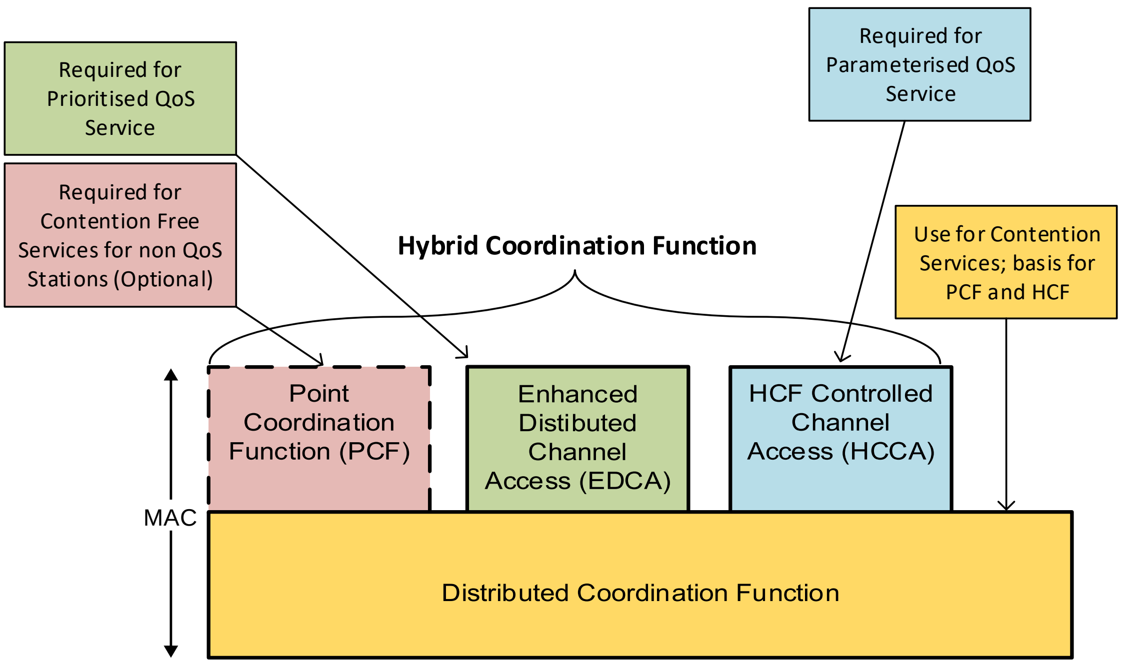

Figure 2.6: IEEE 802.11e MAC architecture.

2.6.1 Enhanced Distributed Channel Access (EDCA)

EDCA, previously termed enhanced distributed coordination function (EDCF) [45], is HCF's contention-based channel access; it provides service differentiation by using a prioritised QoS approach. EDCA defines the access category (AC) mechanism to prioritise the traffic at the STA. Each STA may have up to four access categories, that is, voice (AC_VO), video (AC_VI), best efforts (AC_BE) and background (AC_BK) to support eight user priorities (UPs) as defined in IEEE 802.1d [51]. The mapping from priorities to ACs is defined in **Table 2.4**.

The voice traffic has given a high priority, followed by vide, best-effort and background. An AC with the high priority is assigned a shorter CW to ensure that a higher priority traffic will be able to transmitted before the lower priority traffic. This is differentiation incorporated by setting the CW limits for each AC: CWmin[AC] and CWmax[AC], from which CW[AC] is computed, as shown in (2.1).

To provide further difference, a IFS is introduced for each AC. The arbitration IFS (AIFS) is used instead of DIFS. For each AC, AIFS is used that is larger from DFIS, as shown in (2.2).

$$CW[AC] = CWmin[AC] \leq CWmax[AC] \qquad (2.1)$$

$$AIFS\ [AC] = AIFSN[AC] \times SlotTime + SIFS \qquad (2.2)$$

$$Backoff\ Timer = Random[0, CW] \times SlotTime \qquad (2.3)$$

EDCA mechanism works similar to DCF i.e., any time, any STA can begin the transmission if the STA sense the medium idle. Otherwise, the STA defers until the end of current transmission on the wireless medium. After deferral, the STA waits for a period of AIFS [AC] to start a backoff procedure. The backoff is a random number interval calculated from the interval (1, CW [AC] + 1) as shown in (2.3). Each AC within STA contends for accessing the medium and starts the transmission independently if STA sense idle for at least AIFS. Collision among ACs within a single STA is resolved by granting the medium to the highest priority AC, after which the lower priority AC backoff. Table 2.5 lists the default DCF and EDCA parameters.

IEEE 802.11e introduced transmit opportunity (TXOP), a time interval for further prioritising the traffic. An 802.11e enabled STA with high priority traffic may hold the medium and send multiple frames during the TXOP interval. An STA can either content for obtaining the TXOP or can be allocated by the hybrid coordinator. An STA can only send one packet if TXOP value is set zero.

Table 2.4: User priority to access category mappings.

Priority	User priority (same as 802.1d priority)	802.1d designation	Access category (AC)	Designation (Information)
Lowest	1	Background	AC_BK	Background
↓	2	Not defined	AC_BK	Background
	0	Best effort	AC_BE	Best Effort
	3	Excellent effort	AC_BE	Best Effort
	4	Control load	AC_VI	Video
	5	Voice	AC_VI	Video
	6	Video	AC_VO	Voice
Highest	7	Network Control	AC_VO	Voice

Table 2.5: DCF and EDCF parameters for IEEE 802.11e.

Parameters	AC	CWmin	CWmax	AIFSN	TXOP Limit	
					FHSS	DSSS
DCF	-	aCW	aCWmax	2	0	0
EDCA	AC_BK	aCWmin	aCWmax	7	0	0
	AC_BE	aCWmin	aCWmax	3	0	0
	AC_VI	(aCWmin + 1)/2 - 1	aCWmin	2	6.016ms	3.008ms
	AC_VO	(aCWmin + 1)/4 - 1	(aCWmin + 1)/2 -1	2	3.264	1.504ms

2.6.2 HCF-Controlled Channel Access (HCCA)

The HCCA provides QoS by using a parameterised QoS approach. HCCA uses a QoS-aware centralised controller, termed an HC. The HC uses different operating approach than the PCF's point coordinator (PC). The HC is collocated with the QoS access point (QAP) of the QoS basic service set (QBSS). HCCA uses the HC's higher priority of access to the wireless medium to initiate frame exchange sequences. HCCA allocates TXOPs to HC and other QSTAs to provide a timer interval, called controlled access phase (CAP) for contention-free transfer of data. The HC traffic delivery and TXOP allocation may be scheduled during the contention period (CP) and any locally generated contention-free period (CFP) to meet the QoS requirements of a particular traffic category or traffic stream.

Centralised control MAC protocols manage QoS more easily but are rarely implemented in products currently owing to their higher complexity, inefficiency for normal data transmission and lack of robustness [6]. This research will be conducted based on the distributed wireless MAC protocol, that is, EDCA. The main advantage of the distributed function is that no centralised control mechanism (i.e., PCF or HCCA) is required and no infrastructure (i.e. access point) is necessary [52]. HCCA is beyond the scope of this research. However, further details about HCCA is available in [45].

2.7 Transmit Opportunity, Frame Aggregation, and Block Acknowledgement

In the legacy 802.11 [39], Stop and Wait Automatic Repeating reQuest (SW-ARQ) mechanism is used for packets transmission. In this mechanism, the sender transmits a single packet (frame) and then waits for an acknowledgement. This involves a lot of overheads owing to the time spent on sensing the channel before sending the packet and immediate transmission of ACKs after each receiving packet [53]. **Figure 2.7** shows the IEEE 802.11 MAC overheads and actual payload.

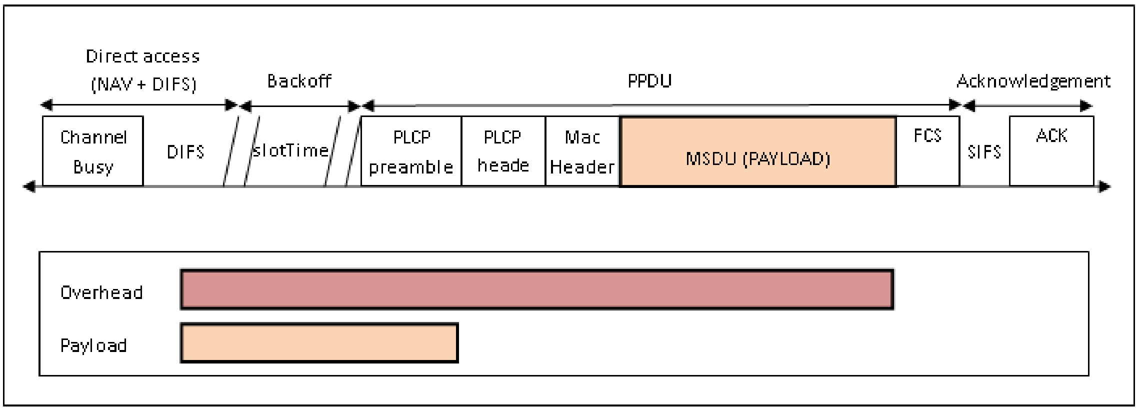

Figure 2.7: IEEE 802.11 MAC overheads and actual payload.

To eliminate the overheads and enhance the throughput performance, IEEE 802.11e introduced new mechanisms termed transmit opportunity (TXOP), frame aggregation and block acknowledgement (BlockAck). These mechanisms are briefly described in the next sections.

2.7.1 Transmit Opportunity (TXOP)

A TXOP is a time interval. In the EDCA mode, the STA may be allowed to access the channel for the period of a TXOP and send multiple frames during this period. An STA may not access the channel beyond this time. If the frame size is very large such that it cannot be transmitted in a single TXOP, the frame should be defragmented into smaller frames. If the TXOP value is zero (0), it means the STA can transmit only a single frame.

2.7.2 Frame Aggregation

During the TXOP period, an STA may combine multiple data packets received from the upper (transport) layer to make a large aggregated frame. Frame aggregation may be categorised into two types or levels: (1) aggregate MAC service data units (AMSDU), and (2) aggregated MAC protocol data units (AMPDU). The two-level frame aggregation is illustrated in **Figure 2.8**.

In A-MSDU, multiple MSDUs, also termed logical link control (LLC) packets, are combined together. Each A-MSDU has one MAC address followed by multiple MSDUs. For A-MSDUs, it is required that each MSDU should have same traffic identification (TID); that is, each MSDU in an A-MSDU belongs to same traffic flow, comes from one source and needs to be transmitted to one destination. Multiple A-MSDUs are aggregated to form a protocol data unit (PDU), in an A-MPDU, multiple PDUs are combined together. In contrast to MSDU, each PDU has its own TID.

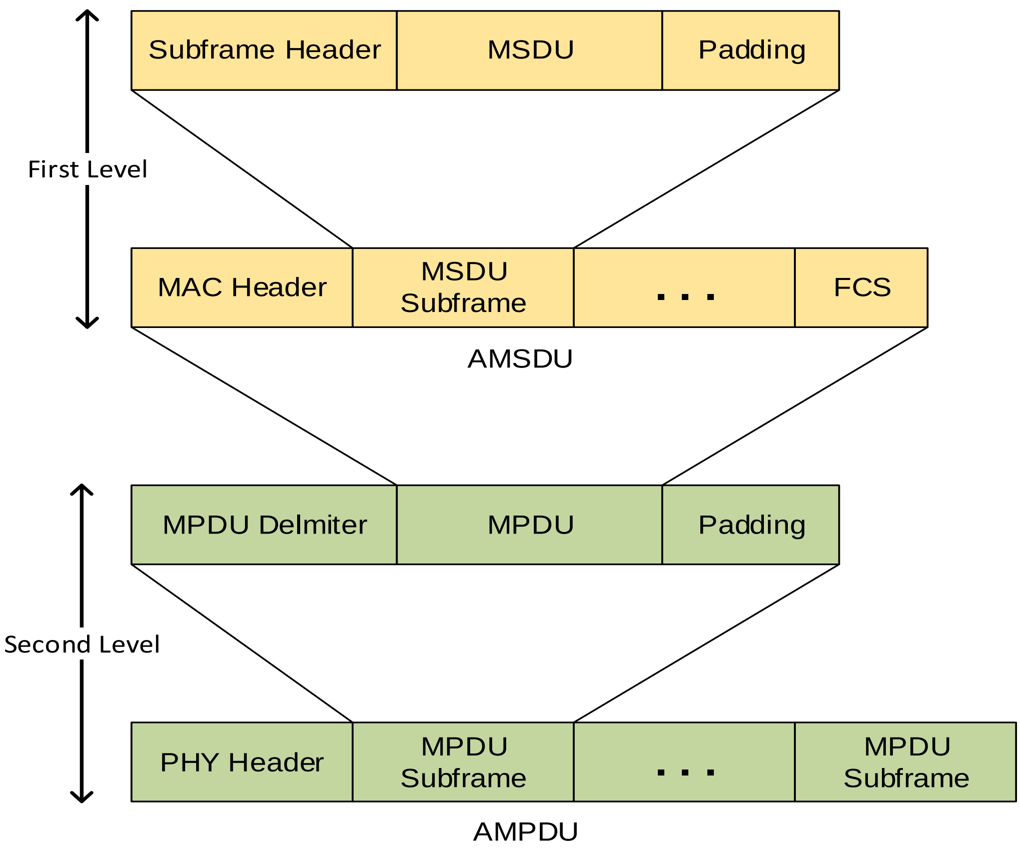

Figure 2.8: Two-level of frame aggregation.

2.7.3 Block Acknowledgement (BlockAck)

To eliminate protocol overhead, IEEE 802.11e [45] introduced an optional Selective Repeat ARQ (SR-ARQ) scheme, which is known as block acknowledgement (BlockAck or BA). The BlockAck (illustrated in **Figure 2.9**) is now a compulsory part of IEEE 802.11n high throughput (HT) devices [54]. This BlockAck mechanism (i.e., sending a single ACK instead of several ACKs) reduces protocol overhead, improves the channel efficiency and enhances the throughput performance [55]. The whole process of BlockAck is divided into three phases: (1) setup (2) transmitting and (3) tear-down phases. In the setup phase, both sender and receiver STAs negotiate the agreement on the successful transmission. The agreement may include the buffer size and BlockAck policy. After agreeing on the buffer size and BlockAck policy, the sender STA transmits a group of data frames (during a TXOP period) one by one without waiting for ACK in transmitting phase. All data frames are separated by a SIFS interval. Once all frames are transmitted, a single BlockAck frame is sent back to the sender STA to inform how many packets received without any error. Finally, the agreement between both (sender and receiver) STAs is terminated by sending the delba frame [45].

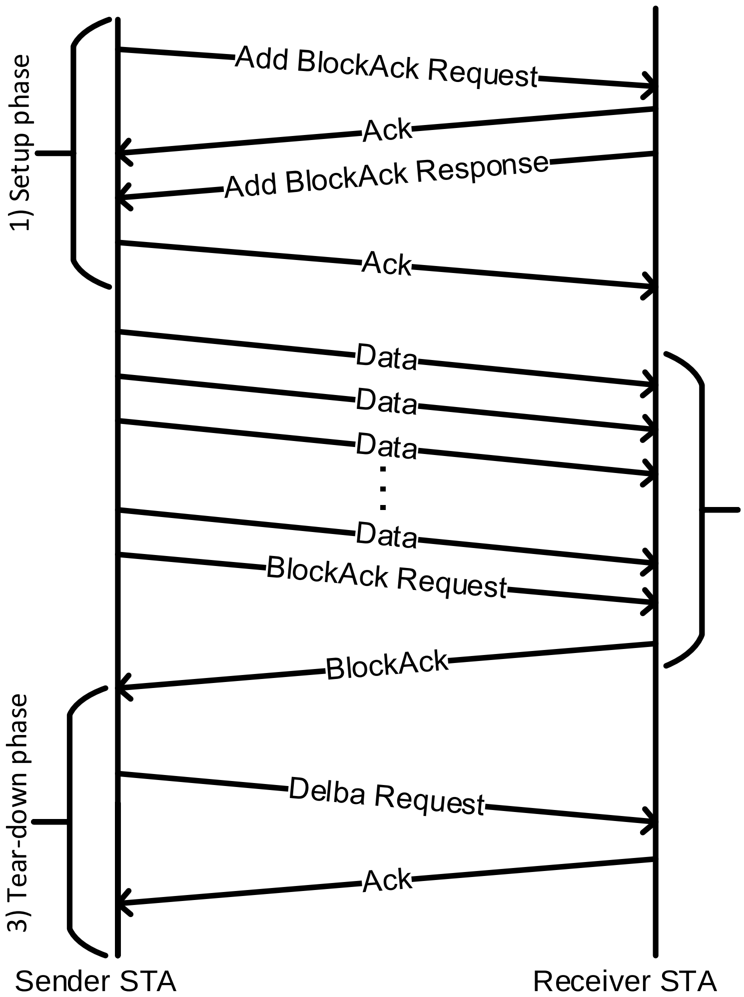

Figure 2.9: IEEE 802.11 (EDCA) BlockAck mechanism.

Two BlockAck schemes are used in IEEE 802.11e: delayed and immediate. Delayed BlockAck is useful for applications that can tolerate moderate latency. In this scheme, the sender sends a normal ACK frame first for an acknowledgement then the receiver sends back the BlockAck at any other time before BlockAck Timeout. The immediate BlockAck method is useful for applications requiring high bandwidth and low latency. In this scheme, receivers generate the BlockAck within the SIFS time interval.

2.8 Admission Control

The admission control is a useful technique to provide a QoS guarantee and handle network congestion [56]. An 802.11e [45] network may use admission control to administer policy, regulate the available bandwidth, or ensure that time-sensitive applications receive the required QoS guarantee. Admission control ensures that admittance of new traffic stream into a resource-constrained network does not affect the QoS required by existing traffic streams. There are two distinct admission control mechanisms: one for EDCA's contention-based access and another for HCCA' controlled access as illustrated in Figure 2.10. In general, admission control depends on vendors' specification such as available channel capacity, link conditions, retransmission limits, and the scheduling requirements of a given stream [39].

Admission control for EDCA is limited to AC_VO and ACVI. In EDCA based admission control, AP advertises ACM bit via a beacon if admission control is required for any particular AC. An STA with the particular AC sends an ADDTS request frame to AP with traffic specification (TSPEC). TSPECs allow an EDCA STA to send traffic requirements to the AP for admittance. After receiving the ADDTS request frame, AP executes the admission control algorithm and responds back to the STA using ADDTS response frame. The response frame contains the admission decision.

EDCA-based admission control mechanisms can be classified in different ways. For example, Gao, et al. [57] have categorised admission control into two types: (1) measurement-based admission control and (2) model-based admission control. The measurement-based admission control makes the decisions by continuously measuring the network conditions such as delay or throughput. There are various examples of measurement-based admission controls such as distributed admission control (DAC), two-level protection and guarantee, virtual MAC and virtual source algorithms, and threshold-based admission control. By contrast, model-based admission controls use certain models or performance metrics to estimate the network status. Markov chain or contention-based admission controls are examples of model-based admission control. **Figure 2.10** illustrates the classification of EDCA-based admission control mechanisms.

Khoukhi, et al. [58] categorised EDCA-based admission control for ad hoc networks as single hop and multi-hop (illustrated in **Figure 2.11**). The multi-hop admission controls may be further categorised into two types: (1) decouple and (2) couple. In couple admission controlled schemes, intermediate STAs have capabilities to make the routing decision to achieve admission decisions. Conversely, in decouple admission controls schemes, a traffic route is already discovered and the admission control know the route of traffic from source to destination [59].

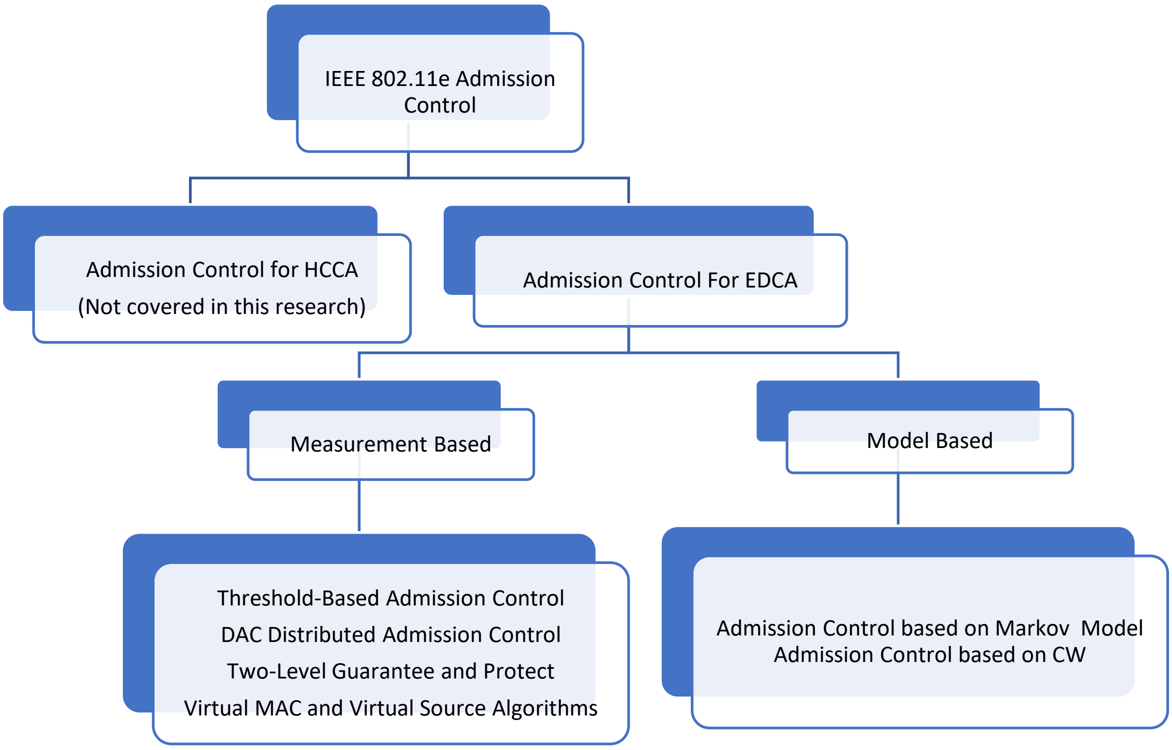

Figure 2.10: Classification of IEEE 802.11e-based admission control.

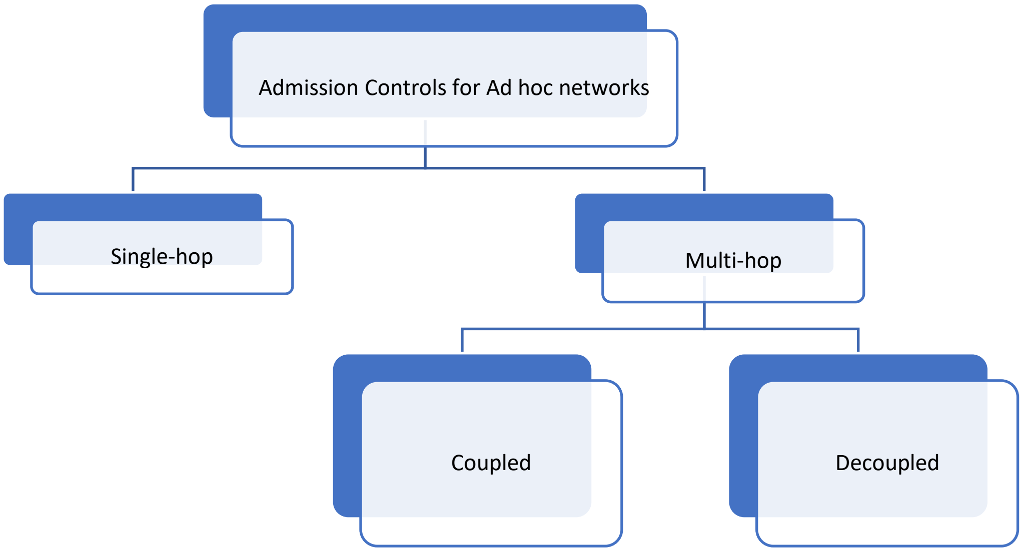

Figure 2.11: IEEE 802.11e wireless ad hoc network based admission control.

2.9 Adopted WLAN Performance Evaluation Approach

The primary objective of this thesis is to create a framework that supports emergency traffic and provides a QoS guarantee in WLANs under the high traffic load. The performance of a typical WLAN can be measured using QoS parameters, that is, network throughput, end-to-end MAC delay, and packet loss. This section depicts methods adopted for measuring QoS performance in this thesis.

It would be very costly to implement realistic dense network scenarios of proposed MAC protocols, IEEE 802.11 standards and other similar protocols for testing and evaluating the network performance. Thus, this research adopts computer simulation to test and evaluate the performance of the proposed MAC protocols. Moreover, simulation methods provide a means of varying different network metrics leading to a generalisation of the research findings.

For selecting the credible simulator, various simulators have been surveyed including Riverbed Modeler [25]. It is identified that Riverbed is one of the credible, widely used simulator tools for modelling WLAN [25], and MATLAB (matrix laboratory) [60] is one of the leading programming languages used for develop mathematical algorithms and analyse data. Both Riverbed and MATLAB are used to evaluate the WLAN performance. While Riverbed Modeler is used to develop, model, and simulate network scenarios for the purpose of testing and evaluating the network performance, MATLAB is used to evaluate the performance of the mathematical algorithms and produce the graphs based on the results produced by the Riverbed Modeler. The proposed methodology is appropriate for this thesis, a view that is supported by key network researchers [61-63].

In this thesis, the performance evaluation is presented for all proposed MAC protocols in Chapters 4, 5 and 6, while all WLAN MAC protocols are modelled and simulated in the same network environment (WLAN 802.11b, 802.11g and 802.11n). Further, the effectiveness of the proposed MAC protocols is evaluated in comparison with the IEEE 802.11standards and other similar existing MAC protocols.

2.10 Summary

In this chapter, the fundamentals of QoS, and WLANs were described and essential background information for designing QoS Wireless MAC protocols which support emergency traffic and provide a QoS guarantee was provided. In particular, IEEE 802.11 standards together with WLAN architecture were discussed. IEEE 802.11 MAC protocol including DCF and PCF were described. The 802.11e (enhanced of 802.11) with QoS MAC protocols implemented in 802.11 WLANs, including EDCA and HCCA were investigated. The schemes such as block acknowledgement and admission control, which may affect the performance of WLANs were also reported. A review of literature for supporting emergency traffic and providing QoS guarantee in wireless MAC protocols presented in Chapter 3.

Chapter 3

Emergency Traffic and QoS Guarantee in WLANs

3.1 Introduction

In Chapter 2, QoS and the fundamentals of IEEE 802.11 WLANs were discussed to gain a basic understanding. The primary objective of this thesis to develop a framework that supports emergency traffic and provides a QoS guarantee in WLANs. To achieve this objective, a clear understanding of the related challenges is required. The remainder of the chapter is organised as follow: First, Section 3.2 describes emergency services and emergency traffic. Next, Section 3.3 and its subsections 3.3.1 to 3.3.4 present an in-depth literature review on MAC protocols providing QoS guarantee and supporting emergency traffic. MAC protocols performance issues are highlighted in Section 3.4. Section 3.5 discusses the design challenges for MAC protocols. The approach adopted for validating simulation models is provided in Section 3.6. Finally, the chapter is summarised in Section 3.7.

3.2 Emergency Services and Emergency Traffic

3.2.1 Emergency Services

An emergency may be defined as a situation or an event that involves an immediate risk to human life, health, property or environment [64]. An emergency involving risk to life is prioritised since the general thinking is that nothing else is more important than human life.

In recent years, the use of emergency services (e.g. health monitoring, disaster surveillance) over WLANs has grown significantly [4, 5]. These applications require emergency traffic support from the medium (i.e., on-arrival channel access priority over normal traffic) together with a strict QoS guarantee especially in terms of delay under saturated network conditions.

3.2.2 Emergency Traffic

To provide better emergency traffic support in WLANs, organisations that deal with emergency services are studied. It is reported that most such organisations categorise emergency traffic into four different types: emergency to (1) life, (2) health, (3) property and (4) environment [65-67]. Not all emergencies require the same level of priority, and hence, these services can be linked to various service priorities. For example, emergency to life has the highest priority because nothing is more important than human lives. This is followed by prioritisation of health, property and environment (see Figure 3.1: Types of emergency traffic.

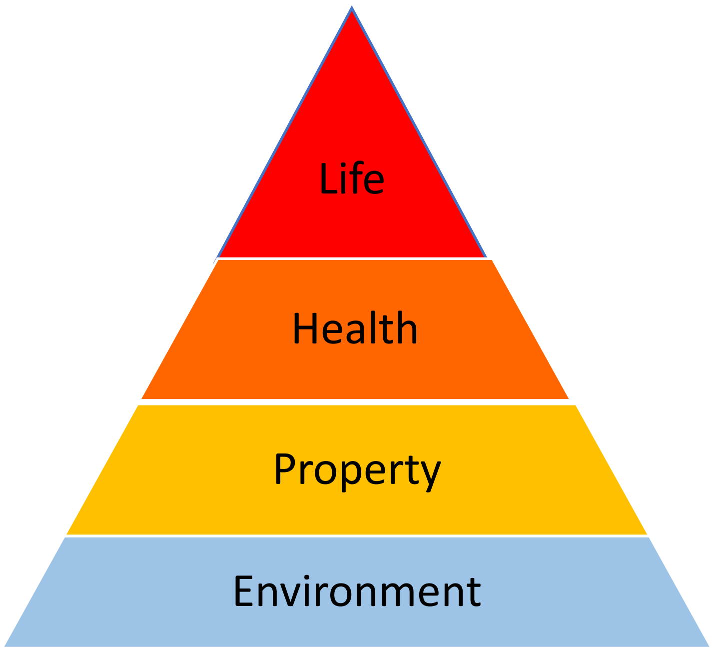

Figure 3.1: Types of emergency traffic.

3.3 Emergency Traffic and QoS Wireless MAC Protocols

The increasingly use of WLANs in public safety and emergency network services necessitates a strict QoS guarantee, especially since a large number of users report an emergency for immediate channel access. Unfortunately, the traditional IEEE 802.11e-based EDCA does not support a strict QoS guarantee for lifesaving emergency traffic under high loads. A key requirement of both type of traffic (i.e. real-time multimedia and emergency traffic) is certain QoS support (in terms of packet delay, throughput and jitter). In addition to QoS (in terms of delay, throughput and jitter), emergency traffic requires on arrival channel access priority than the routine (normal) traffic. The challenge is to design a MAC protocol that can satisfy these requirements owing to the probabilistic nature of the wireless medium.

An efficient QoS MAC protocol should provide a QoS guarantee to time-sensitive applications and support emergency traffic (through on-arrival channel preference and priority over normal traffic) together with the operational simplicity and high bandwidth utilisation. Ideally, such a protocol should provide high throughput, and low end-to-end packet delay, jitter, and packet losses, as well as channel access priority on arrival to emergency traffic. Many network researchers have attempted to investigate MAC protocols to enhance the performance of traditional IEEE 802.11 MAC protocols. These MAC protocols may be categorised into four different classes: (1) those providing service differentiation by adjusting MAC parameters, namely EDCA [45], (2) those providing a QoS guarantee in terms of delay by optimising admission control, that is, Xio’s two-level protection and guarantee mechanism [17], (3) those supporting emergency traffic by tunning physical parameters, that is, Balakrishnan’s CP-EDCA [8], and (4) those enhancing the throughput performance by reducing protocol overhead, that is, Sarkar’s buffer unit multiple access (BUMA) [68]. See Figure 3.2: Classification of IEEE 802.11 MAC protocols for QoS.

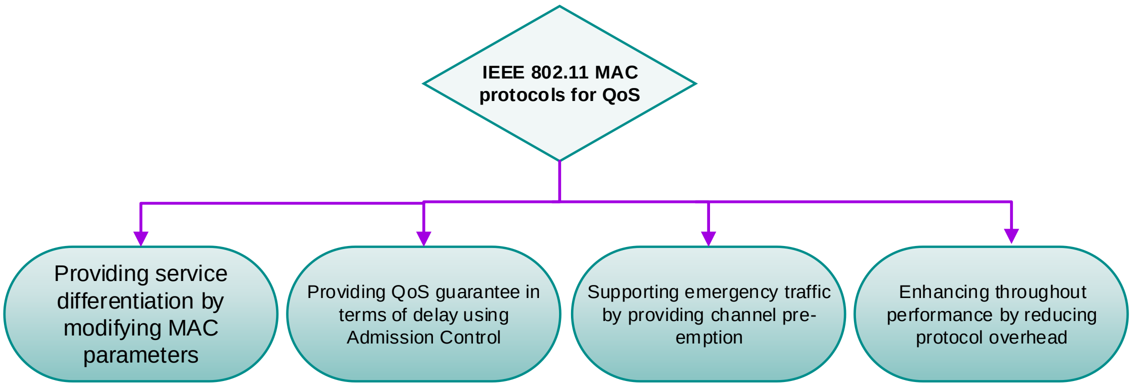

Figure 3.2: Classification of IEEE 802.11 MAC protocols for QoS.

The next subsection (i.e., 3.2.1, to 3.2.4) provide a brief review of the literature on these classifications of IEEE 802.11 MAC protocols for QoS.

3.3.1 Service Differentiation

The IEEE 802.11e working group introduced a new MAC protocol termed IEEE 802.11e [45] to support time-sensitive applications and provide a QoS guarantee. However, many network researchers [10-14, 69] reported that IEEE 802.11e (EDCA) does not perform well under medium-to-high traffic load because of its high collision rate, or because of many of slots are going free (idle slots) and there is MAC/PHY overhead. Over the past 20 years, many MAC schemes have been proposed by network researchers to improve the throughput performance and provide service differentiation by giving priority to time-sensitive applications. Most of the schemes are based on the backoff mechanism, CW, IFS or Hybrid schemes to improve the performance of EDCA under medium-to-high traffic loads.

Table 3.1 lists the key network researchers and their main contributions to the design of wireless MAC protocols. The column 2 of the table shows the main contributions done by the key researchers in wireless MAC protocols. The main approaches used to design or improve the performance of MAC protocols are highlighted in column 3 and limitations of MAC protocols are shown in column 4 (Table 3.1).

Table 3.1: Key researchers and their contributions to QoS-aware MAC protocols.

Researcher	Contribution	Key concept / description	Limitation
Younggoo, K. Y. et al. [70]	FCR	Adjusted contention window to achieve fast collision resolution.	Does not provide QoS under medium-to-high traffic loads.
Romdhani, L. et al. [71]	Adaptive EDCF	Dynamically adjusted the contention of each traffic class.	Reduces by more than 50% the collision rate but goodput obtained is up to 25%.
Lin, W. et al. [72]	M-EDCF	Avoided collisions by adjusting the contention window and backoff timer.	Limited for the inter-frame space.
Lai, Y. et al. [73]	EDCA-LA	Improved the performance by adjusting the backoff timer for each access category based on channel conditions.	Suitable for a cross-layer solution only that works in conjunction with a QoS-aware MAC layer.
Jian-Xin, W. et al. [74]	RAMP	Reduced collision by using adaptive random CW and AIFS values and assigning different values to same priority traffic at a time.	Limited error feedback in a complementary modular manner to achieve the output tracking & system robustness.
Moraes, R. et al. [75]	I-EDCA Improving EDCA	Achieved better performance by tuning CW based on channel condition.	Limited for default parameters of the EDCA standard, the number of high packet loss and packet delays under saturated network conditions
Li, M. et al. [76]	QoS for LPT	Achieved QoS for low priority traffic (LPT) with high throughput by adjusting the CW and persistence factor.	Optimal only for small problem and greatly outperforms some existing algorithms for large problem instances.
Liang, C. C et al. [77]	EDCA-CA Contention Adaptation	Improved EDCA performance by dynamically adjusting the CW of traffic classes based on applications requirements.	Limited as regards the numerical model and analysis to verify the adaptive CW scheme.
Shagdar, O. et al. [78]	TM-EDCA	Maximised channel capacity with better QoS (service differentiation) by adjusting CW of each AC is based on nodes and channel busyness ratio.	Limited to ACs, does not consider the traffic load and collision.
Chen, Y. et al. [10]	QHDCF	Obtained better performance for high priority traffic without affecting low priority traffic with high throughput.	Does not starve the low-priority traffic.
Kosek-Szott, K. et al. [79]	IPSD-EDCA	Introduced a new backoff mechanism to improve the performance of EDCA and provide service differentiation based on AIFS and CW.	Limited to AIFSN and CW, Provide differentiation service under the low-traffic loads.
Sanada, et al. [80]	IT-EDCA	Optimised the backoff to enhance the throughput performance. The proposed investigates the channel condition and optimise the CW and backoff mechanism.	Does not perform well when the traffic load increases.
Syed, et al. [81]	PI-EDCA	Enhanced throughput performance and reduced collision rate by optimising CW & adjust backoff time based on active STAs of each AC.	Increases the collision among STAs.

These DCF/EDCA schemes were grouped into three main categories (**Figure 3.3**). A brief description of each of the main contributions in the design of the wireless MAC protocols listed in **Table 3.1** is shown in Fig 3.3.

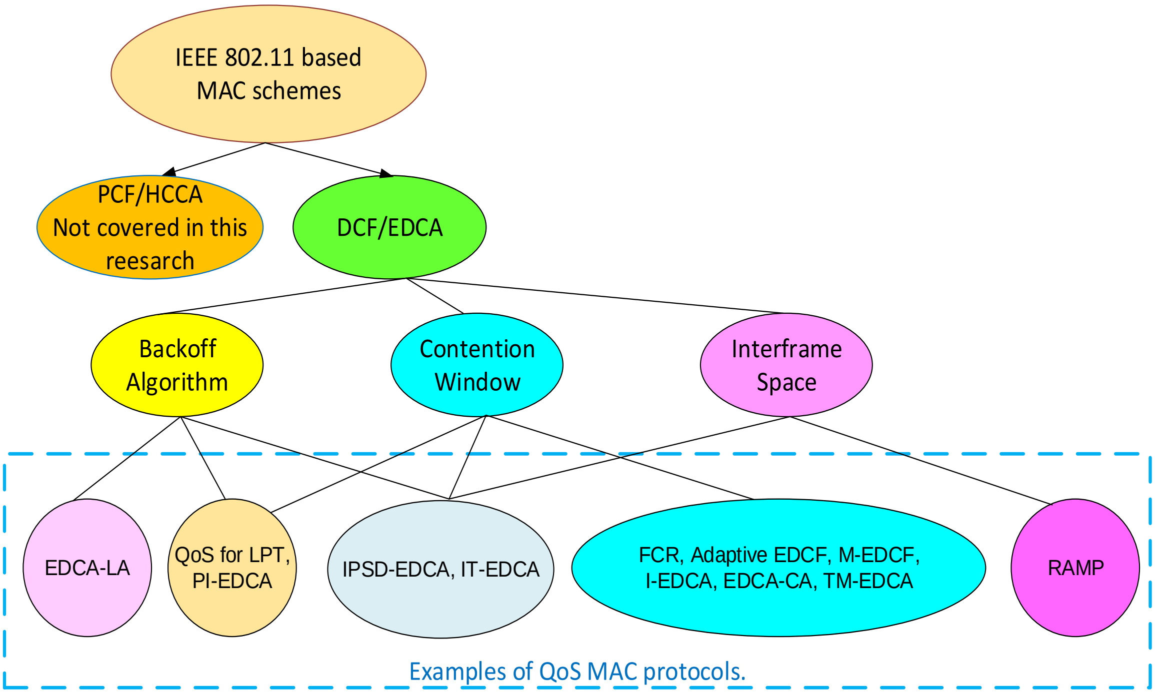

Figure 3.3: Approaches used in the design of wireless MAC protocols for providing service differentiation.

Younggoo, et al. [70] developed an efficient MAC scheme termed fast collision resolution (FCR) to resolve the collision quickly by increasing CW size for all STAs to reduce backoff in the contention resolution period. The FCR scheme assigns the smallest window size and idle backoff timer to the STA having successfully transmitted the packet to save idle time slots. Further, it decreases the backoff timer exponentially as compared with linearly as specified in EDCA when an STA detects a number of idle slots. Younggoo, et al [70] further proposed enhancement of FCR into a real-time-FCR scheme to improve the fairness and QoS support for time-sensitive applications. A similar scheme, the Adaptive EDCF (A-EDCF), was also proposed in [71]. The authors determined that the main reason of high collisions is resetting CW from CW[AC] to CW[min] after successful transmission in the existence of a number of STAs contending for the medium. Considering this fact, they proposed a step-by-step decrement in CW[AC] by a factor of 0.8 or lower after a successful transmission collision rate experienced by the AC; the factor value will be based on the collision rate experienced by the AC.

Lin et al. [72] developed the Modified EDCF (M-EDCF) to improve the performance of EDCA by increasing the CW size on the basis of the average collision rate and choosing the new backoff time. By contrast, Lai et al. [73] proposed an adaptive EDCA with a link adaption (EDCA-LA) scheme where each category adjusts its backoff timer based on channel conditions. Similarly, Jian-Xin [74] investigated a random adaptive mechanism to adjust MAC parameters (RAMPS). Author assigns different values to the same priority traffic streams in a given time. The authors in [75] and [77] enhanced the performance of EDCA by dynamically adjusting CW. In [75], CW was tuned according to the channel condition and average collision rate, while Liang et al. [77] adjusted the CW of each traffic class based on application requirements and network conditions.

While many network researchers have worked on either MAC enhancement or service differentiation independently, very little work has been carried out by considering the combined effect of MAC enhancement and service differentiation of EDCA. Li. et al. [76] proposed a dynamic priority reallocation mechanism, which distributes a number of active nodes over traffic streams and dynamically alters the CW and persistence factor to address the problem of high throughput with better service differentiation. Similarly, Shagdar et al. [78] also investigated the network throughput performance with service differentiation by adjusting the CW of each AC, taking the channel busyness ratio and considering the number of nodes within a network. Chen et al. [10] proposed a high performance distributed coordination function with QoS support (QHDC) scheme to enhance the performance of EDCA. QHDC works in two modes: active mode and contention mode. The active mode is used for data; the transmitting STA will select the next transmitting STA from active STAs based on the probability class having high priority. The contention mode follows the EDCA mechanism. Kosek-Szott et al. [79] reported a MAC scheme to provide service differentiation in EDCA (IPSD-EDCA). The scheme introduced a new backoff mechanism to achieve high throughput. Moreover, CWmin, CWmax and AIFS were used to provide better service differentiation.

Sanada, et al. [80] investigated the MAC protocol to enhance the throughput performance. The concept is to optimize the backoff mechanism. They investigated the channel condition and optimised the CW and backoff mechanism based on the traffic load. Syed, et al. [81] developed a MAC protocol for WLANs to enhance the throughput performance of EDCA. The proposed scheme estimates the active STAs for each AC, and based on that, optimises the CW and adjusts the backoff time.

Table 3.2: Key researchers and their contributions in providing QoS guarantee in WLANs.

Researcher	Contribution	Key concept / description	Limitation
Xiao, Y. et al. [17]	Providing QoS guarantee to voice and video	Introduced two-level approach; distributed admission control and tried-and-know mechanism to provide QoS guarantee to voice and video.	Change the connection window size for the deferring stations.
Chen, X. et al. [18]	Improving QoS guarantee to real-time traffic	Proposed two schemes; call admission control for high priority and rate control for low priority traffic.	Not improving QoS for other traffic.
Hamidian, A. et al. 2006 [12] and 2008 [19]	EDCA-RR EDCA-DRR	Improved QoS guarantee by investigating admission control and traffic scheduler. Real-time traffic reserved the channel. The problem of hidden STAs during reserved TXOP is also addressed.	All the traffic have same priority, not capable to prioritise traffic and have high collision rate.
Yang, C. et al. [20]	PRED	Enhanced in the previously proposed mechanism by Floyd, S. et al. [82] to provide better QoS guarantee.	Scheduling mechanism to give priority.
Sarma, N. et al. [21]	SPQAMP	Improved QoS guarantee by providing non-overlapping CW to time-sensitive traffic.	Static CW are assigned to time-sensitive traffic. May not perform well under medium to high traffic load.
Cetinkaya, C. [22]	Providing different QoS to different real-time traffic	Proposed three schemes, i.e., admission control, flow-based and class-based queuing to prioritise the traffic	Provide limited QoS for IP networks. Difficult to implement
Tadayon, N. et al. [23]	Improving QoS guarantee	Achieved better QoS guarantee by tuning CW on the basis of channel's load.	Limitation of Replacement for Uniform PDF with Gamma PDF.
Ferng, H. et al. [24]	FRRBC	Investigated QoS guarantee with fairness.	Using multiple mapping only functions from allowances to fixed-bit binary numbers to indicate different priorities.
Mansoor, et al. [82]	FACU	Proposed admission control and optimise TXOP	FACU exploits piggybacked information containing.

All these QoS Wireless Mac protocols provide service differentiation and enhance the performance of 802.11e (EDCA) using certain key parameters such as contention window, block acknowledgement, transmit opportunity. None of them works well under medium-to-high traffic load or provides any QoS guarantee.

3.3.2 Service Guarantee

Despite providing service differentiation, the EDCA cannot support strict QoS guarantee for time-sensitive applications [83]. Many efforts have been taken to provide QoS guarantee in EDCA. Table 3.2 lists the key network researchers and their main contributions in providing QoS guarantees to time critical applications. Column 2 of the table shows the main contributions in the wireless MAC protocols. The main approaches are used to design and improve the performance of QoS aware MAC protocols and the limitations of the corresponding method are highlighted in column 3 and column, respectively.

Many network researchers consider that a QoS guarantee cannot be provided without defining the proper network control mechanism and regulating new input traffic streams into the network. Xiao, Y. et al. [17] adopted a two-level protection approach to guarantee real-time traffic. They proposed distributed admission control and a tried-and-known approach. The distributed admission control measures the channel utilisation during each beacon interval, based on which available capacity is calculated. Traffic streams do not receive transmission time if their class capacity is zero. Further, STAs are not allowed to increase the transmission time allocated to them. Moreover, a tried-and-know mechanism, where a new STA flow is first temporarily accepted and then the throughput and delay performance is measured for some beacon interval. If it affects the performance (i.e., does not match the requirements) then flow is rejected.

Similarly, Chen et al. [18] proposed two schemes: call admission mechanism and rate control mechanism. The call admission control is for high priority traffic and the rate control for low priority traffic. The rate control utilises the remaining channel capacity without affecting high priority traffic; each STA monitors the channel busyness ratio and estimates the rate of the ongoing real-time traffic before adding new traffic. Hamidian, A. et al. [12] developed EDCA with resource reservation (EDCA-RR). They proposed traffic scheduler and admission control mechanism. Before admitting the new traffic stream, it calculates the schedule service interval; otherwise, it similar like the EDCA. In

[19], Hamidian, A. et enhanced EDCA-RR [12] and proposed the EDCA-distributed resource reservation (EDCA-DRR) scheme that uses a distributed approach for the same admission control, traffic scheduling and resource reservation.

Yang et al. [20] proposed the priority random early detection (PRED) mechanism by enhancing random early detection (RED) [84]. PRED alters the queue[AC] based on traffic loads, using a scheduling mechanism to prioritise each packet within the STA. Sarma et al. [21] investigated a strict priority based QoS aware MAC protocol, termed SPQAMP. The SQMAP gives priority to STAs those have real-time traffic to send the packet by assigning non-overlapping CW values for real-time and best-effort traffic, and resets the backoff counter instead of freezing for best-effort traffic.

Centikaya [22] investigated QoS for supporting time-sensitive applications. Author proposed admission control, class-based queuing and flow-based schemes. Further, each STA alters the backoff counter based on the priority of STA's own packet and of the previously transmitted packet to support QoS and provide protection to ongoing time-sensitive traffic from new traffic. Tadayon, N. et al [23] addressed the inefficiency of the uniform probability density function (PDF) used by EDCA while treading the new time-sensitive traffic. They replaced Uniform PDF with Gamma PDF to prioritise the time-sensitive traffic.

Mansoor, et al. [82] proposed a feedback based admission control unit (FACU) scheme and optimised the TXOP to improve the QoS of video transmission in WLANs. However, authors did not consider other real-time traffic such as voice or emergency. Moreover, the proposed scheme does not provide any QoS guarantee.

Most of these schemes only provide QoS guarantee under low traffic loads, and when the traffic load is increased, they provide service differentiation rather than QoS guarantee. Here, the question may arise about supporting a strict QoS guarantee, rather than service differentiation for time-sensitive applications operating under medium-to-high traffic load conditions.

3.3.3 Emergency Traffic Support in QoS MAC protocols

The 802.11e (EDCA) does not provide any mechanism to prioritise emergency traffic [39]. Recently, the 802.11u-2011 [16] working group introduced a new standard termed

802.11u for interworking with external networks that also supports emergency traffic over infrastructure-based WLANs but it may not provide emergency traffic support over ad hoc WLANs. The general packet radio service (GPRS) and global system for mobile communications (GSM), or any other infrastructure networks are highly affected by disasters. An ad hoc networking approach will allow the relief groups to enter the disaster area and communicate with each other quickly [85].

Previously, schemes to support emergency traffic over WLANs have been proposed. **Table 3.3** summarises the key network researchers and their main contributions in the support of emergency traffic over WLANs. Conte et al. [86] investigated centrally controlled admission control to support emergency calls. The admission control requires additional information to identify the emergency traffic. Further, two approaches are proposed to provide additional information: use of Emergency flag as a field in the traffic specification (TSPEC) element for the source message, and creation of high priority emergency traffic class and such class information is provided by using the Traffic Stream (TS) Information field of TSPEC with the source message. Authors in [87] investigated the performance traffic over EDCA under medium-to-high traffic loads. They introduced a new AC for emergency or any other time-critical traffic. However, emergency traffic requires immediate channel access and should be capable to preempt the ongoing traffic flow. To address this issue, many network researchers proposed channel preemption schemes [8, 88-91].

Sheu, T.L. et al. [90] proposed centralised channel preemption scheduling (CCPS) scheme. The proposed scheme can only be managed by a central controller but is not suitable for ad hoc or distributed networks. Eiager et al. [89] invented the latency-aware service opportunity (LASO) preemption channel scheme that curtails the ongoing traffic flow of the low priority traffic. However, ongoing low priority traffic flow can not be interrupted if the medium is assigned for a pre-allocated time duration. Balakrishnan et al. [92] proposed a channel preemptive EDCA (CP-EDCA) scheme to support emergency traffic in distributed networks. The new emergency traffic is capable to break an ongoing traffic flow and obtains the channel access. To provide pre-emption capability to emergency traffic, authors adjust the values SIFS and SlotTime. However, this scheme does provide priority to lifesaving emergency traffic may not works well in a dense emergency situation where a high number of emergency users want to access the channel.

Table 3.3: Key researchers and their contributions to support emergency traffic in WLANs.

Researcher	Contribution	Key concept / description	Limitation
Conte, A. et al. [86]	Enabling emergency support to 802.11e	Proposed admission control (Central Controller) with additional information for 802.11e to enable emergency support.	Handles only a resource request for an emergency call in a well-adapted way.
Lu-ming, C. et al. [87]	Investigating emergency traffic performance	Investigated performance of emergency traffic under high traffic load. Proposed new access category for an emergency.	Supports only neural networks and synthetic model.
Sheu, T. L. et al. [90]	Centralised channel preemption	Defined centralised channel preemption mechanism that can only be coordinated through a central device.	Limited for the bandwidth resource of a web channel.
Eiger, M. et al. [89]	LASO	Proposed latency aware service opportunity channel preemption mechanism for emergency traffic.	Limited goal of the scheduling method is to meet delay requirements of HCCA traffic flows.
Balakrishnan, M. et al. [8]	CP-EDCA	Investigated in-channel preemption mechanism for emergency traffic.	Does not provide QoS guarantee to lifesaving emergency traffic under medium-to-high traffic load.
Selingnan, A. et al.	Terminal with Emergency Access	Proposed a terminal with an emergency access over WLAN to LAN and other communication systems.	Limited to a few terminals with emergency access.
Sunghwa, S. et al. [88]	Adaptive AIFS and admission control	Introducing a new Adapting AIFS and admission control to provide priority to medical application	Does not support lifesaving emergency traffic in the network.

Son, et al. [88] investigated three types of medical traffic: (1) medical alarm, (2) electro-cardiogram (ECG) and (3) non-real-time traffic. Medical alarm traffic was given the highest priority, followed by ECG and non-real-time traffic. They developed a MAC protocol for WLANs to provide priority to medical traffic. An adaptive AIFS scheme with admission control is proposed for 802.11e (EDCA). The key concept is to adjust AIFS values based on the QoS required by medical traffic. The AIFS values are increased for low priority traffic if high priority medical traffic is not receiving the required QoS. Moreover, an admission control is introduced for low priority traffic to provide a QoS guarantee to the highest priority medical alarm traffic. However, the highest priority traffic (medical alarm) is not protected by the same class of traffic. The strict QoS guarantee may not be achieved in saturated network conditions where a high number of nodes with medical alarm traffic need to access the medium.

Preemption schemes are also proposed in other wireless networks. Balakrishnan, M., et al. [93] investigated EDCA based channel preemption scheme for wireless sensor networks. The scheme achieves 50% lower delay while accessing the wireless medium for emergency traffic. In [91], authors investigated channel preemption mechanism for supporting emergency traffic cellular networks. They introduced two queues: one queue for emergency and another queue for the routine traffic; the emergency traffic is capable to preempt the routine traffic.

3.3.4 Frame Aggregation and BlockAck

The foundation background on the TXOP, frame aggregation and block acknowledgement was provided in Section 2.9. It was highlighted that IEEE 802.11 MAC does not perform well due to protocol overheads [39, 94]. To enhance the performance of 802.11 MAC and reduce the overhead, the IEEE 802.11e MAC introduced several mechanisms and parameters termed TXOP, block size and BlockAck. For performance optimisation, the 802.11e enhancement left these parameters open in the standard, for example, block size or BlockAck policies [95]. The use of a smaller block size increases the overheads since the STA needs to negotiation each time before transmitting the frame. Further, the larger block size may increase the error rate and results in delay for real-time applications [96, 97].

Over the past 10 years, many schemes have been proposed to enhance the throughput performance by reducing the protocol overhead. Most of the schemes are based on optimising TXOP, frame concatenation and BlockAck. **Table 3.4** lists the key network researchers and their main contributions to the design of wireless MAC protocols for enhancing the throughput performance in WLANs. Column 2 of the table shows the main contributions in wireless MAC protocols that other researchers have done. The main approaches these researchers used to design or improve the performance MAC protocol are highlighted in column 3.

Table 3.4: Key researchers and their main contributions in wireless MAC protocols.

Researcher	Contribution	Key concept / description	Limitation
Sarkar and Sowerby [68]	BUMA	Enhanced throughput performance by reducing transmission overhead.	Does not consider TCP applications. It is limited to UDP applications.
Cabral, et al. [98]	O-BlockAck	Optimised BlockAck to reduce delay and increase the number of users in the network.	Increases higher queue delay under medium-to-high traffic loads.
IEEE 802.11n [54]	A-MSDU A-MPDU Hybrid (two-level)	Enhanced throughput performance and achieved channel efficiency by using various frame-aggregation schemes	Aggregated only into a single MPDU
Hazra and De [99]	TXOP based frame concatenation and BlockAck (TFCB)	Investigated frame concatenation and BlockAck based on TXOP to enhance the performance and provide QoS	Based only frame-concatenation with block-acknowledgement scheme.
Saif, et al. [100]	mA-MSDU	Proposed aggregation scheme that aggregates frame header and implemented retransmission control over individual subframes	Headers are small compared with the legacy headers.
Azevêdo Filho, et al. [101]	HTA	Investigated packet aggregation scheme based on packet's journey (source node to destination) time and application's delay tolerance.	Compared with another prominent packet aggregation scheme.
Kim and Cho [102]	ATA for EDCA	Achieved performance enhancement and fairness by tuning TXOP and BlockAck.	Only for fairness among STAs with various multimedia applications.
Kowsar and Biswas [103]	Two-level aggregation	Optimised throughput performance by aggregating A-MSDU and A-MPDU.	Analyses its performance by using only simulation in multi-client mode.
Seytnazarov and Kim [104]	QAA-MPDU	Enhanced throughput performance by aggregation MPDU for voice traffic.	Has less nodes transmitting. It's only for A-MPDU aggregation.
Liu, et al. [105]	Adaptive A-MPDU	Investigated two-level frame aggregation scheme for retransmission for reducing transmission overheads.	Achieves only higher throughput. Increases queuing delay at the receiving end.

These 802.11 (DCF) or 802.11e (EDCA) based schemes were grouped into three main categories (Figure 3.4). A brief description of each of the main contribution to the design of the wireless MAC protocols listed in Table 3.4 is given below.

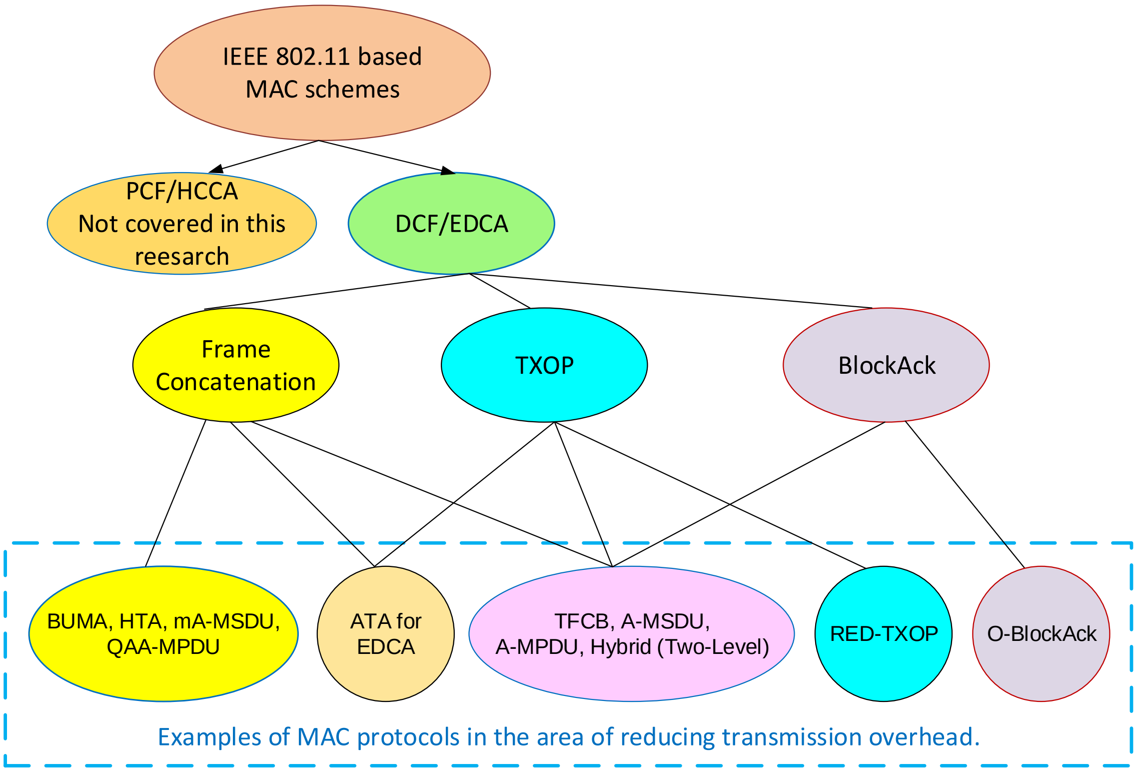

Figure 3.4: Approaches used in the design of wireless MAC protocols to reduce transmission overhead.

Recent studies [97] have shown that the 802.11e BlockAck scheme can enhance network throughput performance at the cost of resequencing delay at the receiving buffer.

Many MAC protocols have been proposed to reduce the transmission overhead, enhance the throughput performance and increase channel efficiency. These MAC schemes may be categorised as frames aggregation [54] [61] [97] , optimising TXOP [96] , BlockAck [91] or hybrid [92] [94] [95] [98]. Sarkar and Sowerby [68] proposed a new protocol termed BUMA that combines short packets in a flow to form large frames (with a single header and trailer) for reducing control and transmission overhead. However, BUMA is only suitable for UDP applications and may not provide assurance of delivery.

Azevêdo Filho, et al. [101] proposed a holding time aggregation (HTA) packet aggregation scheme for reducing the MAC transmission overload. In HTA, each station STA calculates the amount of time a packet takes for its journey and the time up to which an application may tolerate the delay. Moreover, STA considers the application requirement and dynamic wireless environment, that is, variable bandwidth for packet aggregation. However, the proposed HTA scheme is only suitable for UDP applications.

The IEEE 802.11n [54] standard defined two frame aggregation schemes for achieving higher throughput at the MAC layer, A-MSDU and A-MPDU. In the result of aggregation, the standard 802.11 introduced new frame headers. Although, these headers are smaller as size compared with those of the legacy 802.11, these still have negative performance especially when added with small payload. Moreover, the network performance is highly affected while transmitting the A-MSDUs because of lack of control of subsequence frames and retransmission. To address this issue, Saif, et al. [100] developed a MAC scheme termed minimised header MSDU aggregation scheme (mA-MSDU) for reducing the transmission overheads by aggregating MSDUs. The proposed scheme minimised headers' overheads by optimising the subframe aggregation headers. Moreover, the authors introduced implicit sequence control (ISC) as error controller for subframes. The advantage of using ISC is to retransmit only the corrupted subframes. By contrast, Kowsar and Biswas [103] proposed a two-level aggregation scheme by combining A-MSDU and A-MPDU schemes. This scheme enhances the throughput performance and decreases the MAC delay.

Implementation of IEEE 802.11n does not aggregate MPDU for voice traffic because of its specific end-to-end delay requirements. Seytnazarov and Kim [104] identified that the performance of the network is highly degraded in saturated traffic conditions when multiple nodes access the medium for transmitting voice traffic. They proposed a QoS-aware adaptive A-MPDU aggregation scheme (QAA-MPDU). The QAA-MPDU scheme optimises throughput performance by aggregating MPDU for voice traffic and reducing protocol overhead.

Liu, et al. [105] first reported that the adaptive MAC protocol data unit (A-MPDU) MAC scheme does not provide transmission efficiency under an error-prone environment. To overcome from this problem, they proposed an adaptive A-MPDU (AA-MPDU) frame aggregation scheme. The AA-MPDU uses three modules: (1) the bit error rate (BER), estimator to calculate the average error rate, (2) a retransmission A-MPDU Level (RAL) module to identify the position of lost subframe and (3) a theoretical throughput decision module that uses BER estimates and RAL modules for making decisions to use the frame aggregation scheme.

Hazra and De [99] proposed a frame concatenation with block acknowledgement scheme based on TXOP to enhance the throughput performance of EDCA and provide a QoS guarantee to time-sensitive applications. However, the proposed schemes are only suitable for client-server application, such as transferring files, or rich multimedia applications for sending multiple picture frames.

Cabral, et al. [98] optimised the block acknowledgement (O-BlockAck) scheme to reduce the delay and increase the number of users within the network. They investigated the performance of O-BlockAck scheme using a single service and a mixture of services used by the node. The empirical results showed that fragment size 12 is more appropriate for a mixture of services and supported users may be increased from 30 to 35within a network.

Azevêdo Filho, et al. [101] proposed holding time aggregation (HTA) packet aggregation scheme for reducing the MAC transmission overload. In HTA, each station STA calculates the amount of time a packet takes for its journey and the time up to which an application may tolerate the delay. Moreover, STA considers the application requirement and dynamic wireless environment, that is, the variable bandwidth for packet aggregation. However, the proposed HTA scheme is only suitable for UDP applications.

Many researchers investigated TXOP for enhancing throughput performance and reducing protocol overhead. Feng, et al. [106] proposed the random early detection transmit opportunity (RED-TXOP). They tuned the TXOP dynamically for optimising the throughput performance of multimedia traffic. Kim and Cho [102] investigated an adaptive TXOP allocation (ATA) scheme for EDCA to enhance the performance and provide fairness. In the proposed scheme, each station decides (to increase or decrease) the TXOP interval based on the traffic load and delay bound required by the application. An STA increases TXOP interval in two conditions. First, the STA increases its TXOP to satisfy the QoS guarantee required by its packet queue, and second, when the traffic load is low.

3.4 Wireless MAC Performance Issues

Previous research demonstrated that most of the proposed MAC schemes target throughput enhancement or service differentiation by adjusting IFS and CW. In addition to service differentiation, many MAC schemes have been proposed to provide the QoS guarantee. However, none of them provides a strict QoS guarantee. Further, little research has been conducted in the area of emergency traffic support over WLAN.

Moreover, there is a lack of a suitable framework to support emergency traffic in a dense emergency situation, such as a disaster where a high number of nodes report an emergency. The present thesis aims to develop a robust framework to provide a strict QoS guarantee for time-sensitive applications and to support emergency traffic by enhancing 802.11e.

A new MAC protocol termed MP-EDCA, developed as a minor modification of EDCA, can be used to overcome the limitation of the 802.11e (EDCA) as aforementioned. The MP-EDCA is described in Chapter 4. Moreover, the PAC protocol is used to enhance the performance of MP-EDCA and described in Chapter 5.

3.5 Design Challenges for Distributed Wireless MAC Protocols

The design principles of wireless MAC protocols are different from those of wired network protocols. Designing a wireless MAC protocol that supports emergency traffic and provides a QoS guarantee is a challenging task because of various factors, such as the shared medium at the local area network (LAN) level, probabilistic nature of the wireless medium, specific QoS required by time-sensitive traffic, preemptive support require by emergency traffic, node mobility and probabilistic nature of wireless medium.

Shared medium: At the LAN level, all the stations share the common channel. Without proper access control, two or more stations may transmit simultaneously resulting in packet collisions and delay. The main challenge is to control the shared wireless medium.

Specific QoS requirements: STAs with real-time multimedia or emergency traffic require a QoS guarantee. The increasing number of STAs on a particular channel (high traffic load) increases the chances of simultaneous packet transmission from multiple STAs and leads to a collision. In such scenarios, a specific QoS required by the real-time traffic may not be guaranteed without a proper admittance control mechanism.

Supporting emergency traffic: In addition to the QoS guarantee, emergency traffic needs special treatment as preemption. The preemption approach provides an immediate channel access ensuring the admission of emergency traffic. The IEEE 802.11u [16] is a new standard for interworking with external networks supporting emergency traffic and preemption over infrastructure-based WLANs. However, the proposed mechanism does not provide emergency traffic support over the distributed WLANs. Although various innovative MAC protocols have been developed by network researchers [8, 89] none of them supports emergency traffic under medium to high traffic load.

Node mobility: A wireless STA in the network may move independently and randomly which may increase the distance between the sender and receiver STAs. Variations in the distance may affect the QoS and overall network performance.

3.6 Validation of Simulation Models

For producing credible results, it is important to validate the simulation model and ensure that simulation parameters are configured correctly. One of the validating approaches is to compare the results of the simulation model with that of standards (e.g. IEEE 802.11e EDCA). Another approach is to compare the results with related work [107]. A credible network simulator may produce invalid results if the simulation parameters are not correctly configured. Therefore, simulation model verification becomes an important part of any simulation study. The validation of simulation results presented in Chapters 4, 5, and 6 are discussed next.

In this thesis, Riverbed Modeler commercial version 18.0 was used for designing models and evaluating the performance of the proposed protocols. In Chapter 4, the simulation results presented for the proposed MP-EDCA protocol was validated by comparing the results of Balakrishnan's CP-EDCA protocol [8]. We also compare our simulation results with the IEEE standards 802.11e EDCA [45]. Similarly, the simulation results for the proposed PAC-MP-EDCA (reported in Chapter 5) was against the IEEE standards 802.11e EDCA [45]. Finally, the results obtain for the proposed FASBA (presented in

Chapter 6) was validated by comparing the results with that of BUMA protocol [94] as well as the IEEE standards EDCA.

In addition to comparing the result of the proposed schemes with the state-of-the-art MAC protocols, simulation log files were thoroughly checked to ensure that there was no errors and the simulation models run smoothly. In addition to Riverbed simulations, programming algorithm was developed and implemented in MATLAB for further validating the FASBA's results (Chapter 6). For validating the programming algorithm, code review approach was used. In the code review approach, programming code was passed to other developers for code correctness.

3.7 Summary

In this chapter, a thorough review of the literature for providing a QoS guarantee and supporting emergency traffic in wireless QoS MAC protocols was presented. The literature review reveals that the IEEE 802.11e (EDCA) does not have inherent emergency traffic support. Moreover, it neither provides a QoS guarantee nor works well under medium-to-high traffic loads. Therefore, network researchers proposed many QoS MAC schemes to enhance the performance of 802.11e (EDCA). However, most of the QoS schemes have focused on either network throughput enhancement or service differentiation by adjusting CW or IFS. While many efforts have been made to provide a QoS guarantee in EDCA, but they do not provide a strict QoS guarantee especially under medium-to-high traffic loads. Additionally, there is not enough research published in the area of emergency traffic over WLANs. Therefore, research on developing techniques to provide a strict QoS guarantee as well as support for emergency traffic in such systems is required. Providing emergency traffic support in WLANs is further discussed in Chapter 4.

Chapter 4

Multiple Preemptive MAC Protocol for Emergency Traffic in WLANs

4.1 Introduction

In Chapter 3, a literature review on IEEE 802.11 for providing QoS and supporting emergency traffic in wireless MAC protocols was presented. The primary objective of this thesis is to support emergency traffic in WLAN. This is achieved by modifying the existing WLAN MAC protocol. This chapter presents a simple but effective Multiple Preemptive-EDCA (MP-EDCA) scheme that modifies physical parameters such as SIFS and slot time, in the IEEE 802.11e MAC protocol. MP-EDCA provides multiple levels of channel access preemption where high priority emergency traffic preempts the low priority emergency traffic for accessing the channel on arrival. The proposed scheme is also published in [108]. A method for supporting emergency traffic in a dense emergency situation where a high number of nodes report the emergency is described.

Although prior investigations [8, 86, 109, 110] have considered how to support emergency traffic by modifying WLAN MAC, the MP-EDCA scheme is simple and does not require any significant change in the existing protocols. Moreover, the same existing standard equipment may be used without a major redesign. The chapter starts by introducing the emergency traffic support and the choice of the network protocols in Section 4.2. The previous related studies are further reviewed in Section 4.3, while the proposed MP-EDCA protocol is described in Section 4.4. Section 4.5 illustrates the key concepts and design comparison of four channel access methods namely, the 802.11 DCF, 802.11e (EDCA), CP-EDCA and MP-EDCA. Section 4.6 presents the experimental setup and implementation details of MP-EDCA in Riverbed Modeler. Simulation results are presented and discussed in Section 4.7. Section 4.8 provides the strengths and weakness of the MP-EDCA protocol. The implementation aspects of MP-EDCA are discussed in Section 4.10. The chapter is summarised in Section 4.11.

4.2 Emergency Traffic Support and Choice of Network Protocols

As discussed in Section 2.2, an emergency requires immediate attention. Moreover, emergency traffic may be categorised into four types. Lifesaving emergency traffic has the highest priority because of the general view that nothing is more important than human life. To support the emergency traffic, we have the choice of a fixed backbone, centralised control infrastructure based or distributed networks.

Fixed backbone or infrastructure-based networks are highly affected by natural and manmade disasters, such as earthquakes, fires and floods. In fact, the traditional networks, such as GPRS, GSM and other infrastructure-based networks are not reliable for emergency communications (e.g., 9/11 disaster in the United States) since they quickly become overloaded in disaster-affected areas even in a small urban area. However, distributed wireless networks are becoming popular for emergency networking solutions [111, 112].

The distributed wireless networks use distributed wireless MAC protocols. The main advantage of such MAC protocols is that no centralised control infrastructure (i.e., access point) is necessary [52]. Conversely, supporting emergency traffic and providing a QoS guarantee under medium-to-high traffic loads is very challenging [15, 16].

In the IEEE 802.11 distributed wireless MAC protocols, including DCF and EDCA, each station or AC senses the medium for a certain amount of time (i.e., DIFS or AIFS time). If the medium is idle for the DIFS or AIFS time, the station transmits the frame. Otherwise, it postpones the transmission and waits for the idle time (interval). If the station senses the medium is busy after the interval, an STA or AC needs to delay its transmission further. This mechanism of existing wireless MAC protocols works well for normal traffic but is not helpful for emergency traffic that requires immediate channel access.

4.3 Previous Research on Enhancing of 802.11e

Many network researchers have proposed schemes to support emergency traffic and provide a QoS guarantee to enhance the performance of the 802.11e standard. This section only highlights the selected set of literature (discussed in Subsection 3.3.3) that has proposed approaches used to incorporate emergency traffic in WLANs. However, a centralized channel preemption technique was also investigated by Sheu, et al. [17] and Conte et al. [86]. While the preemption method in [17] seems to function for infrastructure-based WLANs, this centrally coordinated controller is not suitable for distributed WLANs. This was confirmed by the investigation in [86], and as a solution, the authors proposed two approaches: one, to include an emergency flag in the traffic specification field (TSpec) and the other, to introduce a class of high priority emergency traffic termed Traffic Stream Information (TSpec) with the source message.

The preemption approach provides immediate channel access, ensuring the admission of emergency traffic. The IEEE 802.11u-2011[16] working group was the first to introduce a new standard, 802.11u, for interworking with external networks supporting emergency traffic and preemption over infrastructure-based WLANs. However, the proposed mechanism does not provide emergency traffic support over ad hoc WLANs. This issue was addressed in [18], where the authors proposed another class of preemption termed a LASO, which prioritises the high-class traffic and limits the duration of lower-class traffic. However, it does not allow interruption once the channel is acquired for a pre-allocated duration.

The preemption approach was further improved in [8], whereby Balakrishnan et al. introduced a class of preemptive channel access method, the Channel Preemptive EDCA (CP-EDCA), to support emergency traffic. However, CP-EDCA does not support “multiple-emergency” traffic and is not suitable for applications requiring dense emergency networking. This is because CP-EDCA treats all emergency traffic in a similar way (i.e., no emergency service differentiation) and therefore lifesaving emergency traffic is highly affected. To overcome the limitations of CP-EDCA, the proposed class of EDCA protocol termed MP-EDCA is discussed in the next section.

4.4 Description of the Proposed MP-EDCA Protocol

The proposed MP-EDCA protocol described in this chapter differs from the earlier work described in Section 4.2. It has different goals and capabilities.

MP-EDCA overcomes the problem of CP-EDCA by providing multi-level emergency preemptions for quicker admission/access to the channel for lifesaving emergency traffic. This is achieved by breaking down the ongoing traffic stream and taking control of resources. MP-EDCA extends CP-EDCA by incorporating the idea of in-channel multiple preemptions to support dense emergency traffic in distributed networks. It provides high priority to a lifesaving emergency than to an emergency related to health, property and environment by adjusting SIFS and slot-time in the emergency frames. Moreover, MP-EDCA employs a prioritised queuing contention mechanism and contention-free bursting (CFB). The CFB allows continuous transmission of multiple high priority emergency frames without contending the transmit opportunity (TXOP) period.

The concept of in-channel multiple preemptions is shown in **Figure 4.1**. MP-EDCA supports both the normal traffic mode operation for priorities other than an emergency (**Figure 4.1a**) and emergency traffic mode of operation (**Figure 4.1b**). A high priority emergency queue has the privilege to interrupt the ongoing TXOP burst of lower priority emergency or non-emergency queue. The interrupted queue backs off and contends after the high priority emergency bursting. The IFS and slot time [14] are modified to support multiple preemptions for the transmission of emergency frames. The MP-EDCA algorithm, and timing sequences, are illustrated in Figure 4.1 for 802.11 radios.

.

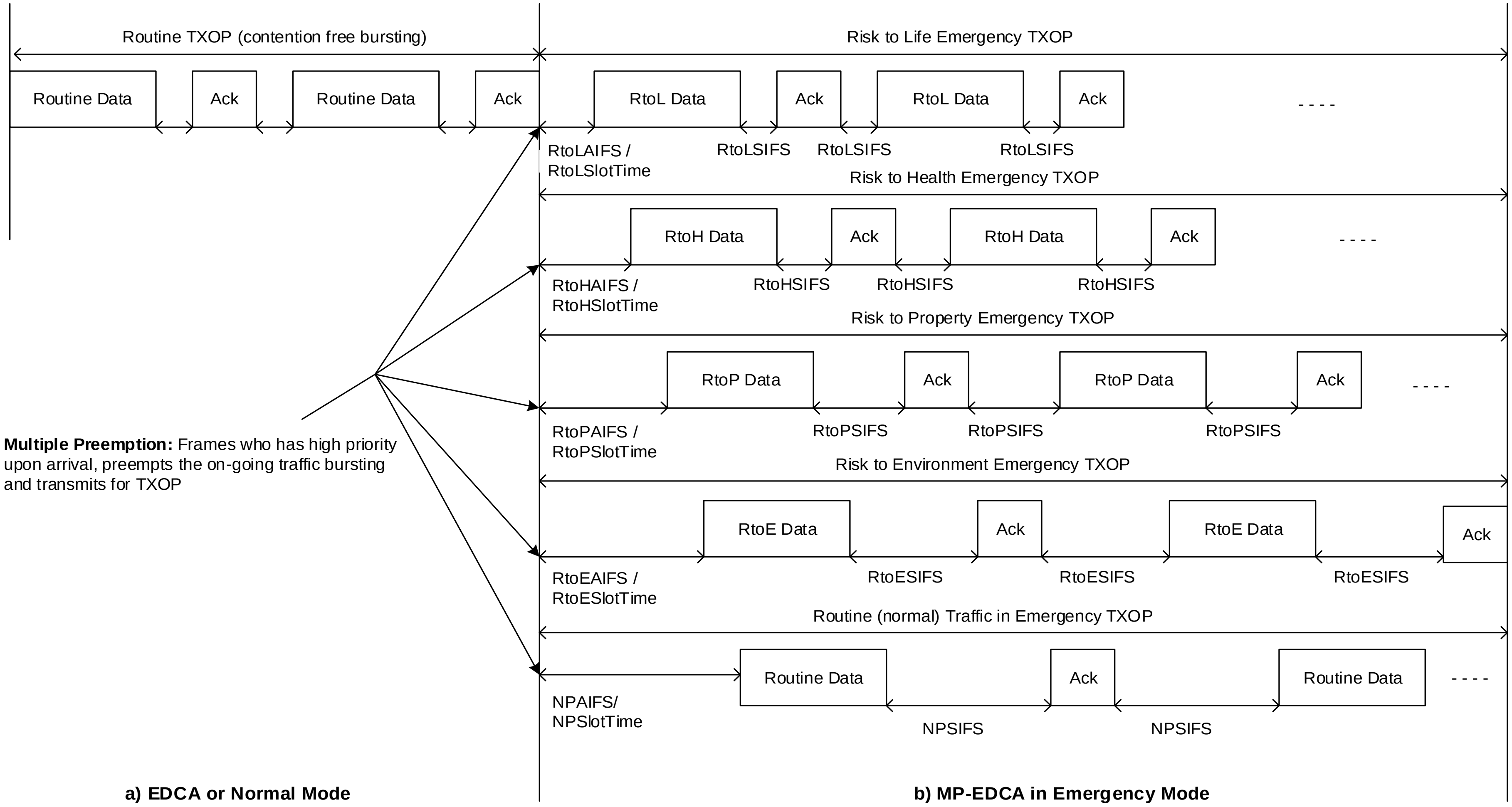

Figure 4.1: Channel TXOP multiple preemptions: (a) EDCA or normal operating mode; and (b) MP-EDCA emergency mode of operation.

The details of Channel TXOP multiple preemptions are as follows:

1. The risk to life SIFS (RtoLSIFS) is set to 10μs similar to SIFS. This minimum time is required for PHY/MAC processing and Rx/Tx turnaround time. In each RtoL frame burst, frames are separated by RtoLSIFS time. The RtoL frame burst is split by RtoLSlotTime that cannot be interrupted.

2. RtoLSlotTime: This slot time (25μs) is a combination of RtoLSIFS and Clear Channel Assessment (CCA). The slot time for R2L priority is different from the slot time for all other priorities. The CCA period is required to detect the frame in the wireless medium after the transmission initiation by another node. In MP-EDCA, the AIFS [13] duration for lifesaving emergency priority is one RtoLSlotTime.

3. The risk to Health SIFS (RtoHSIFS): This slot time (25 μs) is a combination of RtoLSIFS and CCA. In R2L TXOP frame burst, frames are separated by RtoHSIFS. Since RtoHSIFS slot time is equivalent to RtoLSIFS lifesaving emergency traffic is allowed to interrupt ongoing Risk to Health priority frame burst.

4. RtoHSlotTime: This slot time (40 μs) is a combined period of RtoHSIFS and CCA. The slot time for Risk to Health priority is different from RtoLSlotTime. The node with RtoH priority can sense the channel for RtoHSIFS as long as there is no ongoing transmission of R2L and the channel is idle for CCA to initiate the transmission. In MP-EDCA, the AIFS [13] duration for health saving emergency priority is one RtoHSlotTime.

5. The risk to Property SIFS (RtoPSIFS): This period (40 μs) is a combination of RtoPSIFS and CCA. The RtoHSIFS separates the frames in a TXOP frame burst of Risk to Property node. Since RtoPSIFS is identical to RtoHSlotTime, lifesaving and health-saving emergency traffic is allowed to interrupt ongoing transmission of Risk to Property nodes.

6. The risk to Property Slot Time (RtoPSlotTime): This slot time (55 μs) is the combined period of RtoPSIFS and CCA. RtoPSlotTime differs from RtoLSlotTime, RtoHSlotTime, and normal priority slot times. The node with

RtoP priority can sense the channel for RtoPSlotTime to initiate the transmission as long as there is no ongoing transmission from RtoL and RtoH, and the channel is idle for CCA.

7. The risk to Environment SIFS (RtoESIFS): This period 55 µs is a combination of RtoPSIFS and CCA. The RtoESIFS separates the frames in a TXOP frame burst of Risk to Environment node. The duration of RtoESIFS is identical to RtoPSlotTime, allowing RtoL, RtoH, and RtoP nodes to preempt the ongoing transmission of RtoE nodes.
8. The risk to Environment Slot Time (RtoESlotTime): This slot time (70 µs) is the combined period of RtoESIFS and CCA which is different from RtoLSlotTime, RtoHSlotTime, RtoPSlotTime, and normal slot time. The node with R2E priority can sense the channel for RtoESlotTime to initiate transmissions as long as there is no ongoing transmission from RtoL, RtoH, and RtoP, and the channel is idle for CCA.
9. Normal Priority SIFS (NPSIFS) during an emergency: The period (70µs) is the combined period of RtoESIFS and CCA. Basically, RtoESIFS separates the frames in a TXOP frame burst of normal priority node. The NPSIFS is identical to RtoESlotTime, allowing RtoL, RtoH, RtoP and RtoE nodes to interrupt the ongoing transmission of normal priority node.
10. Normal Priority Slot Time (NPSlotTime): This slot time (85 µs) is the combined period of NPSIFS and CCA. NPSlotTime differs from RtoLSlotTime, RtoHSlotTime, RtoPSlotTime, and RtoESlotTime. The node with no priority will sense the channel to initiate the transmission as long as the channel is not being used by any emergency nodes for the duration of CCA period. This allows nodes to transmit routine/normal traffic.

Figure 4.2 shows the MP-EDCA channel access timing diagram. The idea is similar to IFS of 802.11e (EDCA) that uses the waiting time to allow high priority traffic to access the channel. An ongoing frame burst sequence (Data-Ack-Data) is managed by SIFS. The smaller SIFS is set for high priority emergency traffic irrespective of the frame priority. However, in MP-EDCA, the highest priority emergency traffic controls the channel by interrupting the ongoing lower priority traffic burst.

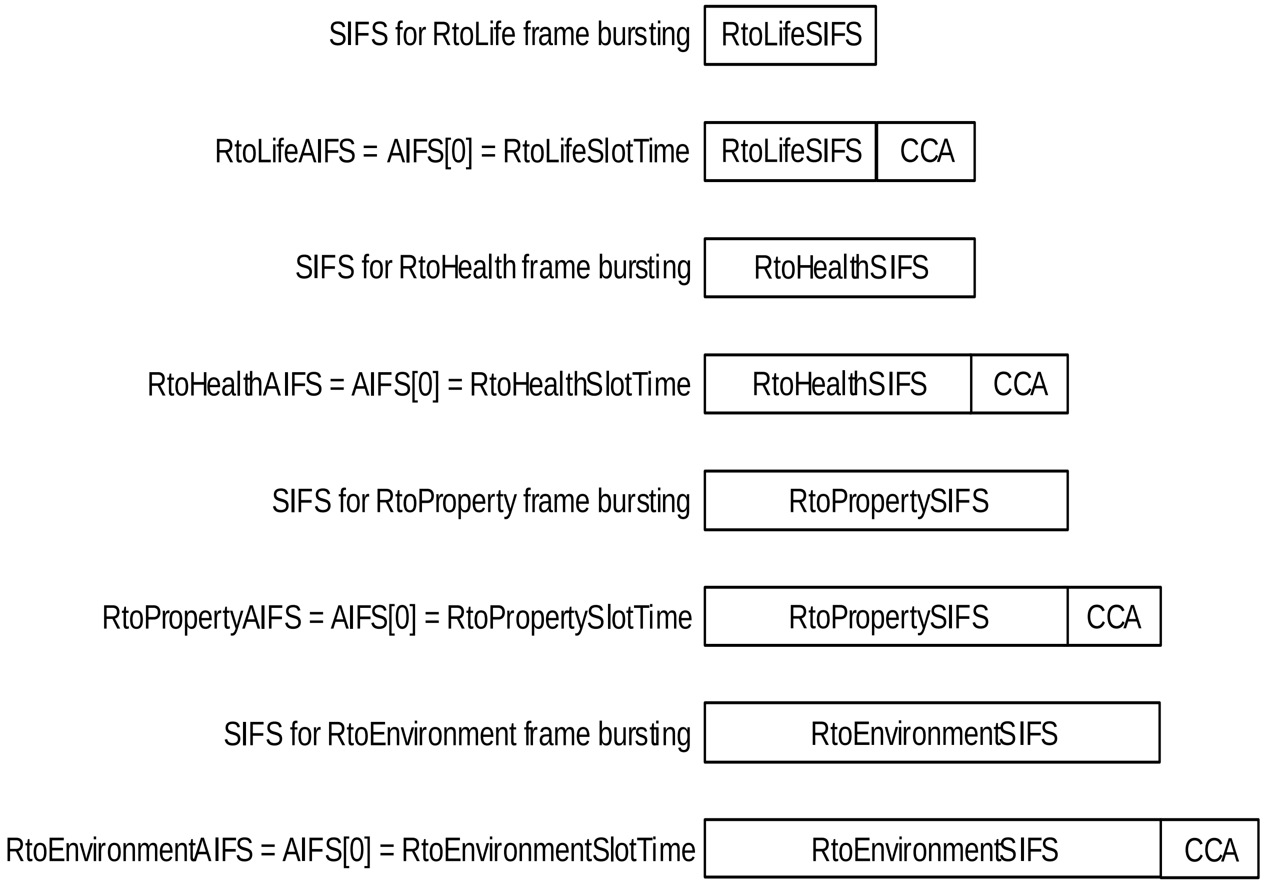

Figure 4.2: MP-EDCA SIFS and SlotTime modifications.

Figure 4.3 illustrates the principle of operation of the proposed MP-EDCA. Fig. 4.3(a) shows the burst of RtoL frames. Each frame is separated by RtoLSIFS. The bursts of risk to health, property, and environment frames are shown in Figures 4.3(b), 4.3(c) and 4.3(d), respectively. Each emergency frame is identified by its own SIFS. Figure 4.3(e) shows the burst of normal priority frames in the emergency period.

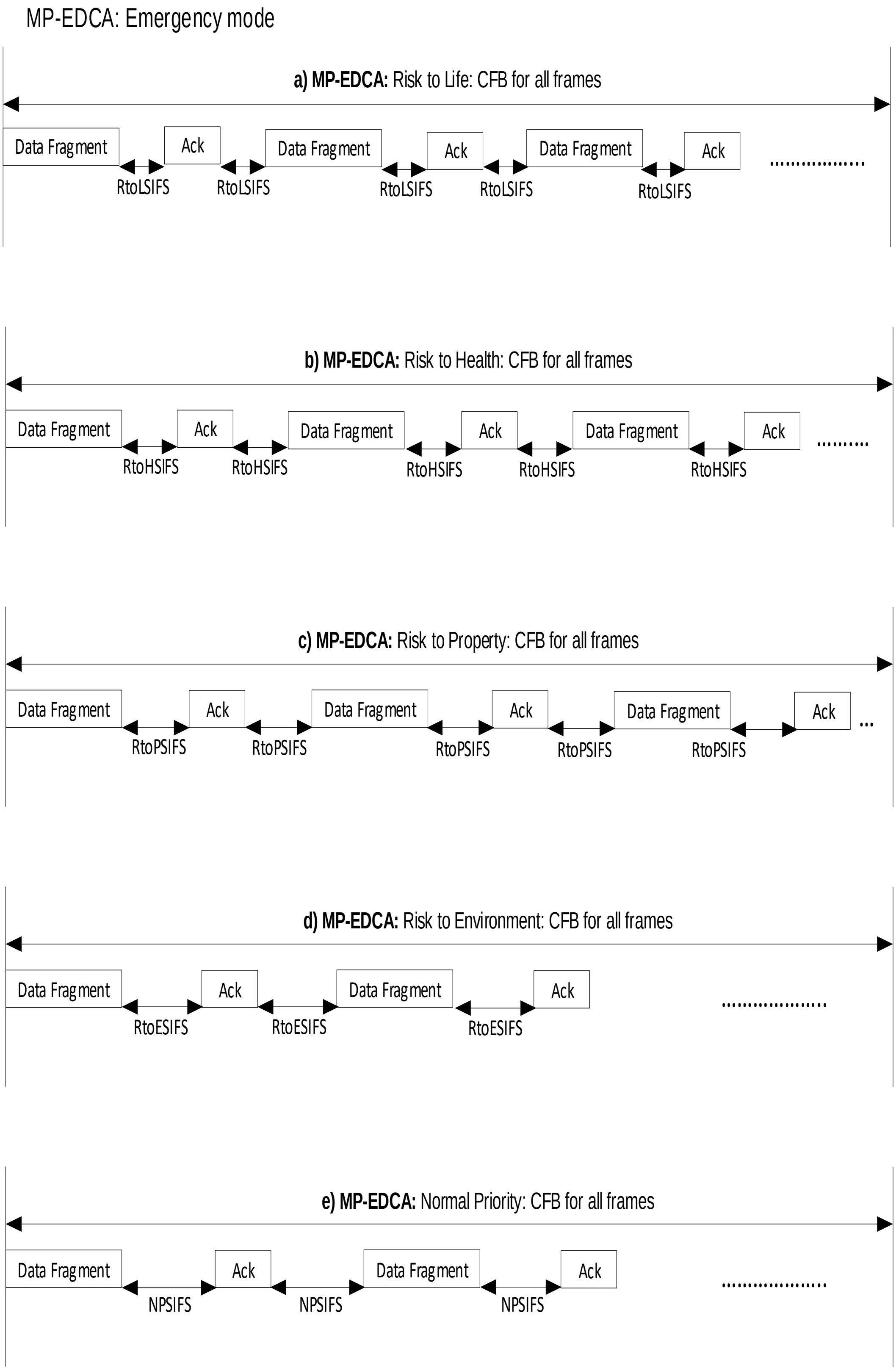

Figure 4.3: Frame bursting in MP-EDCA emergency mode.

The RtoL emergency TXOP bursting has the highest priority (RtoLifeAIFS) followed by Risk to Health emergency, Risk to Property, and Risk to Environment frame burst. Each IFS time is separated by CCA time, which is the minimum time required to detect a new transmission on the channel. The IFS and slot prioritisation mechanisms are exclusively used in providing multiple preemption privileges for various priority emergency traffic. Thus, all priorities other than an emergency will fall in the normal/routine category in the context of channel preemptions. However, prioritised channel access still exists between all traffic categories because MP-EDCA uses the same contention mechanism as standard EDCA.

A new RtoL emergency frame is transmitted if the channel is sensed idle for EPAIFS/RtoLSlotTime, which is the smallest period than that for all other priorities. Similarly, high priority emergency frames are transmitted if the channel is sensed idle for SlotTime/AIFS period since RtoLSlotTime < RtoHSlotTime < RtoPSlotTime < RtoESlotTime < NPSlotTime. A high priority emergency frame has a SlotTime ≤ Low priority emergency frame SIFS; therefore high priority emergency frames can break the ongoing lower-priority emergency transmissions on arrival, and on the next run wait for its smaller slot-time to access the channel. The low priority emergency frame backs off and contends after the high priority emergency burst to regain channel access.

A network allocation vector is used to protect the entire burst of frames subject to the TXOP limit [45] from the same or low priority emergency traffic. MP-EDCA complies with the 802.11e standard by allowing multiple preemptions even though the network allocation vector is set. However, the duration of the network allocation vector is set to protect only a single frame with immediate acknowledgement.

The above mechanism of MP-EDCA achieves multiple levels of preemption. A high priority emergency traffic preempts a low priority emergency traffic and receives channel access on arrival. To provide further service differentiation, the MP-EDCA node may use EDCA four (4) ACs (i.e. AC_VO, AC_VI, AC_BE and AC_BG) for different types of service. Table 4.1 illustrates EDCA's AC to MP-EDCA traffic mapping. Columns 1 and 2 show four types of applications together with associate ACs and Column 3 and 4 show emergency and normal traffic in MP-EDCA's emergency mode.

Table 4.1: EDCA's access category to MP-EDCA's traffic mappings.

Priority	EDCA applications type	Access category (AC)	Emergency traffic in MP-EDCA emergency mode	Normal traffic in MP-EDCA emergency mode
Lowest	Background	AC_BK	Risk to Environment	Background
	Best Effort	AC_BE	Risk to Property	Best Effort
	Video	AC_VI	Risk to Health	Video
Highest	Voice	AC_VO	Risk to Life	Voice

To provide further details on design difference, legacy 802.11 (DCF), 802.11e (EDCA), CP-EDCA, and MP-EDCA is described in the next section.

4.5 Design Comparison of DCF, EDCA, CP-EDCA and MP-EDCA

Figure 4.4 shows the key concepts and design comparison of four channel access methods namely, 802.11 DCF [18], 802.11e (EDCA) [45], CP-EDCA [8], and the proposed MP-EDCA. It is obvious that the IEEE 802.11 DCF does not provide any service differentiation (i.e., no QoS) at all. The 802.11e (EDCA) supports voice, video, best-effort, and background traffic through four queues as defined in the standard [45]. However, it has no provision for supporting emergency traffic. As shown in **Figure 4.4** CP-EDCA supports only one class of emergency traffic through a single queue in addition to serving routine traffic. The emergency traffic preempts the ongoing routine traffic to acquire the channel. In contrast, the proposed MP-EDCA supports four classes (Class 1 to Class 4) of emergency traffic (per node) through four emergency priority queues. The background traffic types are served through a separate queue. For instance, Class 1 (Risk to Life) emergency traffic stream may have the highest priority, followed by Class 2 (Risk to Health), Class 3 (Risk to Property) and Class 4 (Risk to Environment). Each high priority emergency traffic stream can preempt the low priority one to acquire the channel. A question may arise about four classes of emergency traffic in MP-EDCA: Why not implement three or five classes? We consider four classes of emergency traffic based on the published literature in which most organisations have categorised emergency into four classes, namely life, health, property and environment [9, 10]. These four classes are linked to services that have practical implications in real-life scenarios. For instance, the

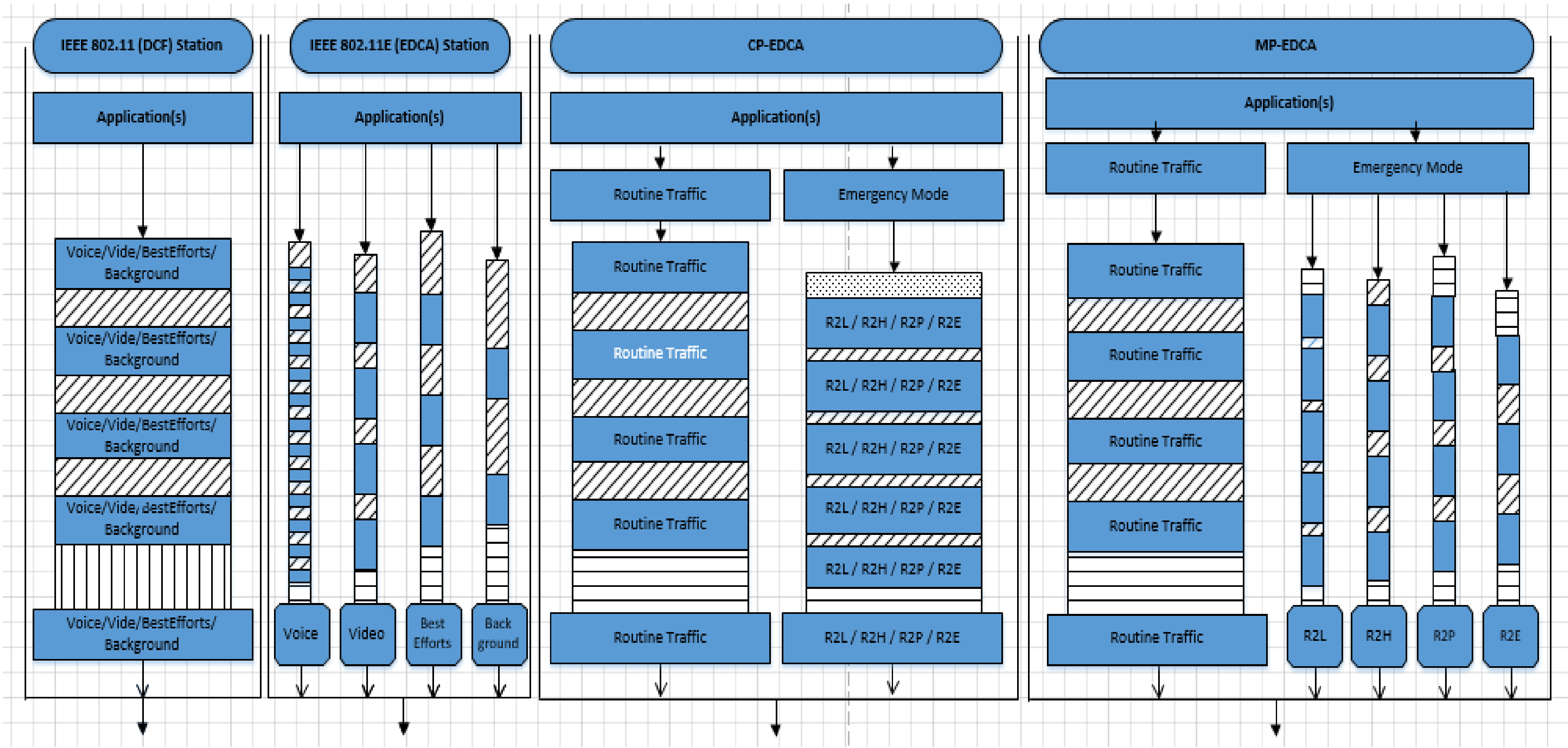

Figure 4.4: Principle of operation of 802.11, 802.11e, CP-EDCA and MP-EDCA.

lifesaving emergency has the highest priority because nothing is more important than human lives. This is followed by service prioritisation to health, property and environment. It should be noted that the proposed MP-EDCA cannot support unlimited priority classes owing to SIFS and slot-time constraints. The performance of these channel access is evaluated next.

4.6 Performance Evaluation

The concept of the proposed MP-EDCA scheme was presented in the previous section. This section presents the modelling and simulation setup. The proposed MP-EDCA protocol described in this chapter differs from the earlier work described in Section 4.3. It has different goals and capabilities.

In this section, the MP-EDCA and CP-EDCA protocols are implemented in the Riverbed Modeler. The performance of MP-EDCA is evaluated by extensive simulations. MP-EDCA's performance is compared with IEEE 802.11 (EDCA) [45] and Balakrishnan et al.'s CP-EDCA [8]. The MP-EDCA protocol was evaluated by measuring parameters such as average network MAC delay, average MAC delay node with lifesaving emergency traffic, data drop ratio, packet retransmission, and average throughput.

Note: The MAC protocols, namely, MP-EDCA, CP-EDCA, IEEE 802,11 (EDCA) for Chapter 4, MP-EDCA with PAC, MP-EDCA without PAC and EDCA for Chapter 5, FASBA for Chapter 6 were implemented in the Riverbed Modeler to model and evaluate the performance of the network.

4.6.1 Riverbed Modeler as a Simulation Environment

Various computer simulators are available to design and develop WLAN MAC protocols. To study the performance of the proposed MAC protocols and compare them with the state-of-the-art existing MAC schemes and IEEE standards, simulation models were developed by using Riverbed Modeler version 18.0 [25]. The Riverbed Modeler provides a development environment with many built-in tools to develop wireless technologies and protocols and evaluate their performance before actual commercial production. The

Riverbed Modeler was chosen because of its popularity [113] and availability at Auckland University of Technology during the duration of this research.

The Riverbed Modeler is available for the Microsoft Windows operating system. The C/C++ programming languages are used to develop Riverbed Modeler. Riverbed provides a graphical user interface (GUI) to create network scenarios. Moreover, Riverbed allows users to modify their C/C++ writing code and implement a customised model. The Riverbed code can be modified by using the Riverbed interface or Microsoft Visual C++ integrated development environment (IDE).

4.6.2 Riverbed Modelling Domains

The Riverbed Modeler comprises three hierarchal models: (1) network model, (2) node model and (3) process model. All codes are executed at the process model. As shown in Fig. 4.5, the process model deploys state machines to define various simulation events, which are presented as C++ programming. The Riverbed coding can be edited using Microsoft Visual Studio, which makes the debugging process easier than on the Riverbed interface. The proposed handover algorithm involved various modifications at both node and network access systems, particularly the MAC and network layers. The details of main modifications are explained in the following subsections. More details about Riverbed configurations are available in Appendix A.

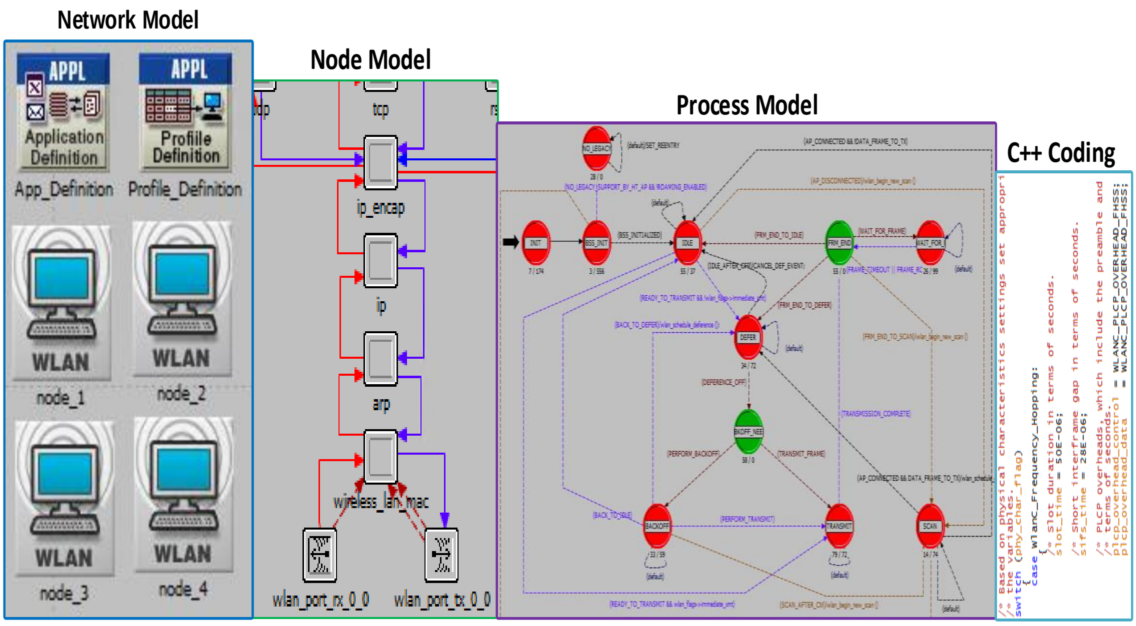

Figure 4.5: Riverbed Modeler hierarchical models.

4.6.3 Modelling Assumptions

To study the performance of the proposed MP-EDCA, the following assumptions are made:

- **Assumption 1:** Uniform distribution of emergency nodes. Each MP-EDCA scenario has the same number of risk to life, risk to property, risk to health and risk to environment nodes.
- **Assumption 2:** There is no hidden node.
- **Assumption 3:** The channel is noise free. Therefore, packet loss is because of the only collision.
- **Assumption 4:** All nodes are static.
- **Assumption 5:** All the nodes start (sending/receiving packet) at the same time.
- **Assumption 6:** Only the ad hoc (single-hop) networks are considered in the study.

4.6.4 Designing Node Model in Riverbed Modeler

The Riverbed Modeler provides comprehensive tools and built-model to design, and develop a communication network and evaluate the network performance. Riverbed has built-in functionality of IEEE 802.11 (EDCA). However, to implement MP-EDCA and CP-EDCA, Riverbed Modeler's node, process and state models were modified. This section briefly describes how the MP-EDCA scheme is modelled in the Riverbed Modeler. More details on using and configuring Riverbed Modeler are provided in Appendix A.

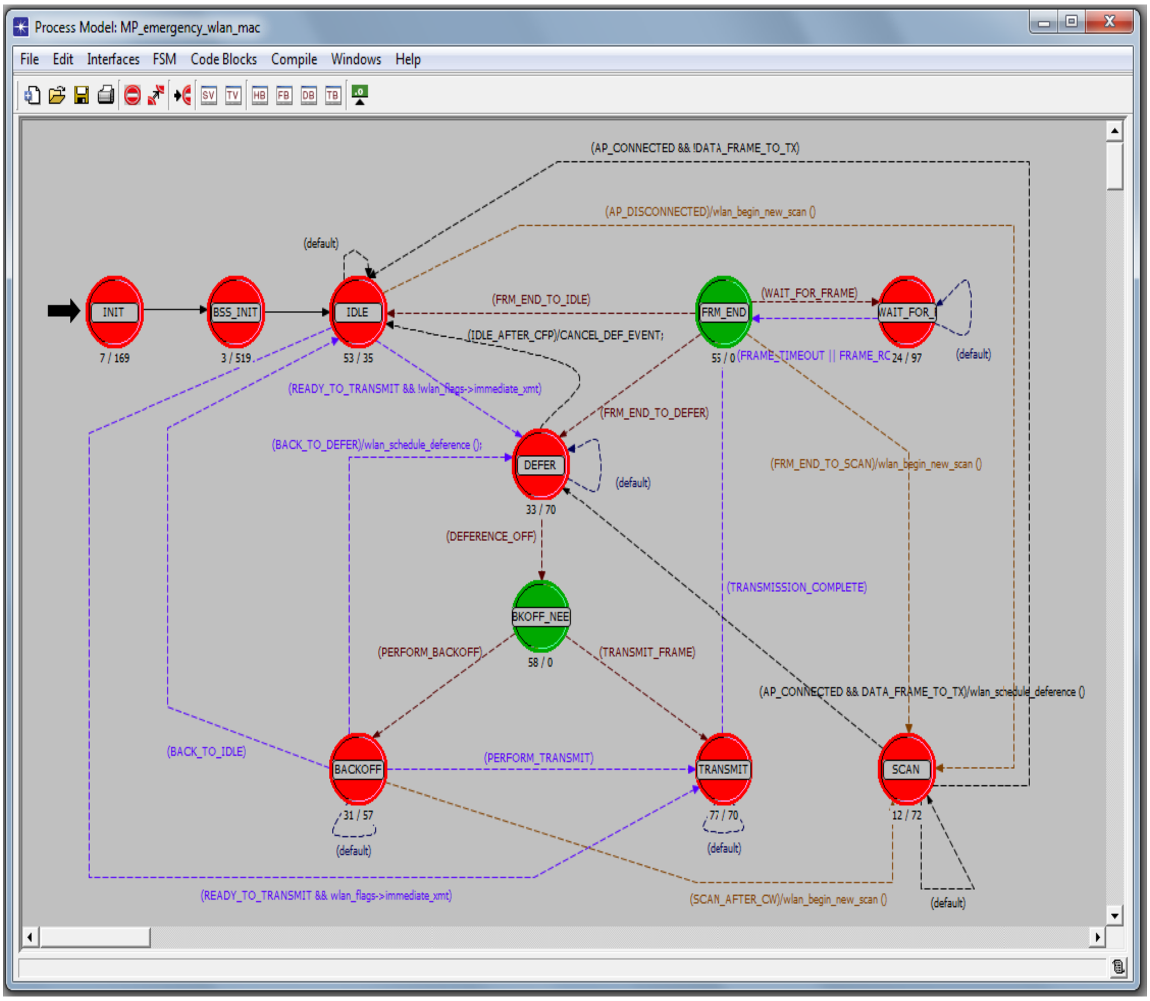

Figure 4.6: MP-EDCA customised process model.

Figure 4.6 shows the MP-EDCA process model developed by modifying the existing WLAN process model in Riverbed Modeler 18.0 (www.Riverbed.com). The timing modules (**Figure 4.2**) and the preemption algorithms (**Figure 4.3**) for both MP-EDCA and CP-EDCA are also implemented in Riverbed. The MP-EDCA emergency node model is depicted in **Figure 4.6**, enabling immediate channel access for Risk to Life emergency traffic throughout the TXOP period. No preemptions are allowed during the Risk to Life emergency TXOP period because it is prioritised by the shortest wait time.

Moreover, the WLAN node model was customised as shown in Fig. 4.7. The MAC and physical layers are enhanced to make it a better representation of an actual 802.11 WLAN. Further, several algorithms were developed and tested to support the four emergency priorities of MP-EDCA using Riverbed. A new MP-EDCA node was also created.

Figure 4.8 shows the WLAN attributes of the MP-EDCA node. A new attributed termed "Emergency" was created. The emergency attribute has values ranging from 1 to 5 to identify various priorities. For example, '1' is for risk to life priority, '2' for risk to health, '3' for risk to property, '4' for risk to the environment and '5' for normal priority in an emergency period.

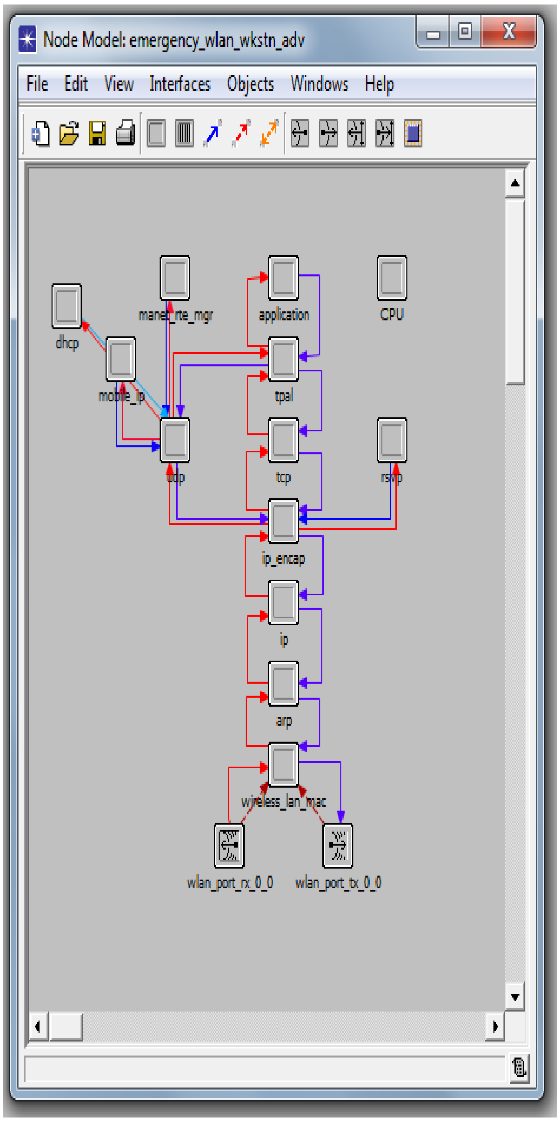

Figure 4.7: MP-EDCA node model.

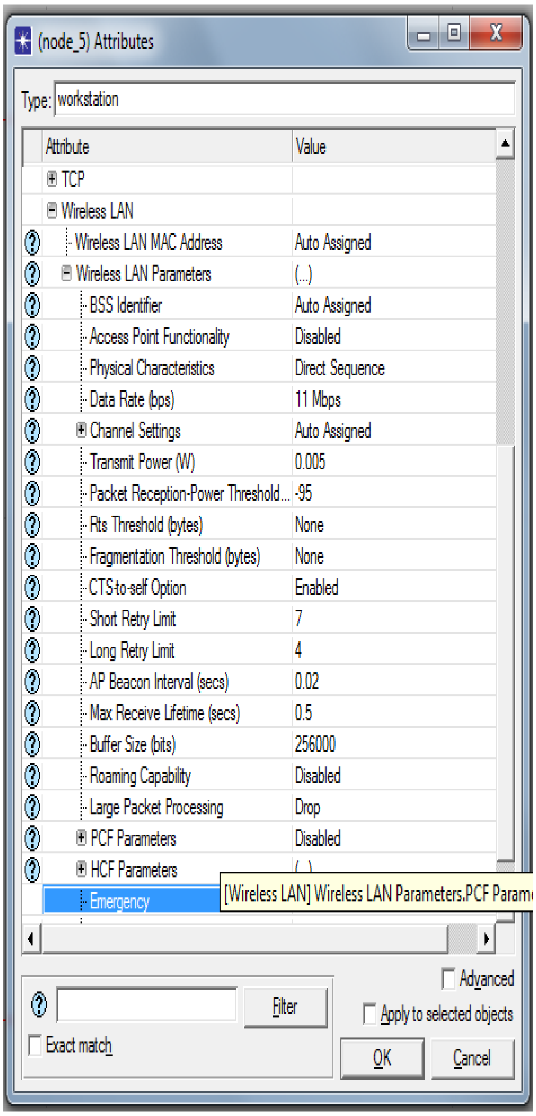

Figure 4.8: MP-EDCA emergency nodes attributes.

4.6.5 Code Contribution

The Riverbed Modeler has four models: (1) network, (2) node, (3) process and (4) state. The state model is based on C/C++ programming code. The state model consists of programming four blocks: (1) static variables, (2) temporary variables (3) head block, and (4) functional block. To implement MP-EDCA, the function block of Riverbed Modeler's WLAN_MAC module, which is written in C/C++ language was modified. Moreover, a new variable was created, the type_of_emergency_flag in the state variable block. The value of this variable, types_of_emergency_flag was set through the MP-EDCA node attribute. A code was added to set values SIFS and Slot as depicted in Fig. 4.9. Note: SIFS and slot_time values were set based on the type of emergency selected from the MP-EDCA's node.

```
/* MP-EDCA Code for Function Block of Emergency_WLan_Mac */
case WlanC_Direct_Sequence:
{
        if (type_of_emergency_flag == 1)        /* Emergency - risk to life */
        {
                sifs_time = 10E-06;
                slot_time = 25E-06;
        }
        else if (type_of_emergency_flag == 2)   /* Emergency - risk to health */
        {
                sifs_time = 25E-06;
                slot_time = 25E-06;
        }
        else if (type_of_emergency_flag == 3)   /* Emergency – risk to property */
        {
                sifs_time = 40E-06;
                slot_time = 55E-06;
        }
        else if (type_of_emergency_flag == 4)   /* Emergency – risk to environment */
                sifs_time = 55E-06;
                slot_time = 70-06;
        }
        else                    /* Normal data in MP-EDCA emergency */
        {
                sifs_time = 70E – 06;
                slot_time = 85E -06;
        }
}
/* End of MP-EDCA Code */
```

Figure 4.9: Code for setting SIFS and Slot Time based on the emergency type.

4.6.6 Modelling the Network

Figure 4.10 depicts the scenario used for the present study where mobile nodes are static and randomly distributed over the simulated area. Four types of emergency traffic are randomly attributed to mobile nodes, namely, lifesaving, health, property and environment applications. As discussed previously, lifesaving application is prioritised over remaining applications. The present scenario includes a high number of nodes reporting an emergency. Nodes with red colour are either node under the emergency situation or first responders have identified an emergency with a certain priority. Red nodes need more help from other first responders (green ones). Nodes with green colour are the first responders who are free and want to help in the disaster.

Figure 4.11 shows Riverbed representation of a fully connected network for simulating MP-EDCA emergency scenarios with N = 10 nodes. The risk to life, risk to health, risk to property, and risk to environment are shown in Figures 10(a) to 10(d), respectively. Each MP-EDCA scenario consists of an equal number of (Class 1 to Class 4) emergency nodes (identical configuration).

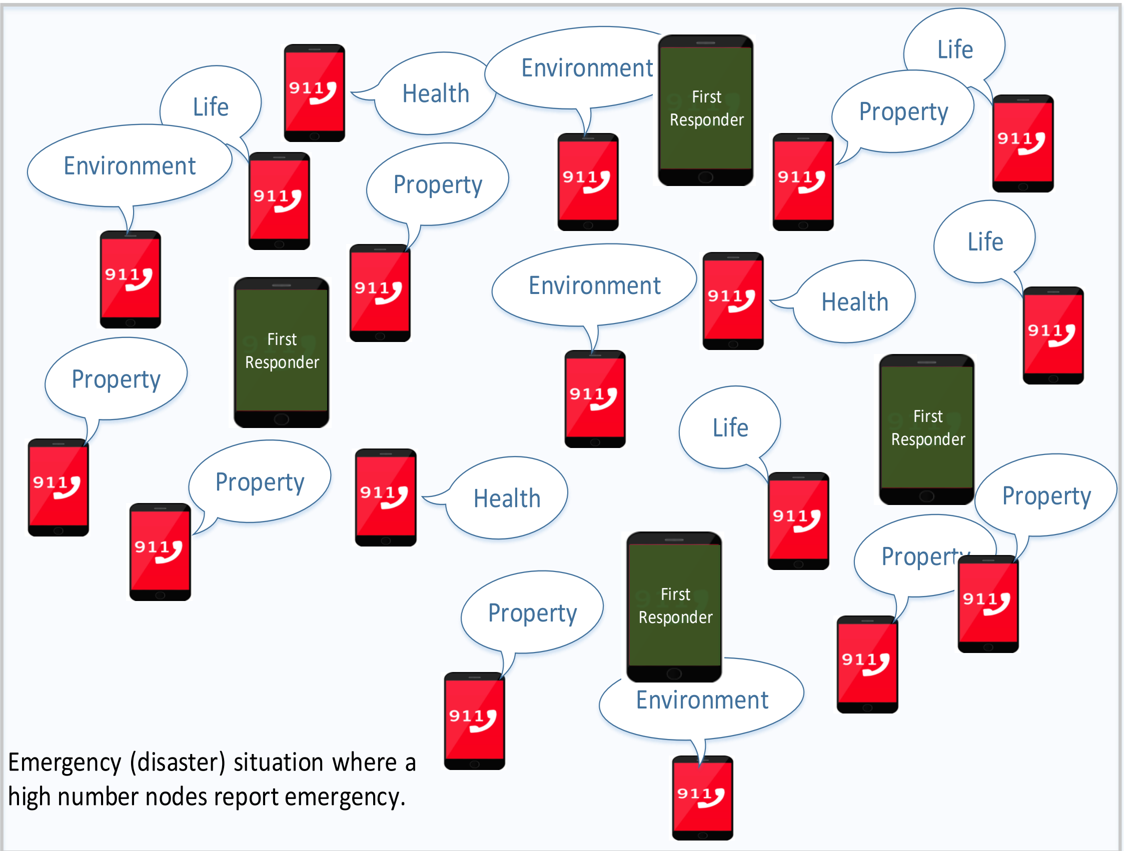

Figure 4.10: Simulation environment for MP-EDCA.

Figure 4.11 also shows (1) Application Definition, and (2) Profile Definition objects. Each scenario uses voice traffic generated by Application Definition. Further, application start time, simulation duration and number of repetitions are configured in Profile Definition. The number of nodes is increased up to 40 to observe the effect of system performance for various emergency priorities. MP-EDCA supports four types of emergencies with various priorities (uniform node distribution). Class 1 category nodes use RtoLSIFS and RtoLSlotTime, Class 2 category nodes use RtoHSIFS and RtoHSlotTime, Class 3 nodes use RtoPSIFS and RtoPSlotTime, and Class 4 nodes use RtoESIFS and RtoESlotTime. In CP-EDCA, all emergency nodes use a single emergency priority, therefore emergency priority RtoLSIFS and RtoLSlotTime are used in the present study as specified in CP-EDCA [8]. In EDCA [45], all nodes use default SIFS and SlotTime since EDCA does not support emergency traffic. Apart from SIFS and SlotTime, all other parameters are set to EDCA default values.

Figure 4.11: Riverbed representation of the fully connected network (MP-EDCA).

The performance of MP-EDCA is evaluated by extensive Riverbed-based simulation under high traffic loads. We simulated 30 scenarios, 10 for each of EDCA, CP-EDCA and MP-EDCA. **Table 4.2** shows the MAC parameters used in the simulation. The simulation results report the steady-state behaviour of the network and have been obtained with the relative error < 1%, at the 99% confidence level.

Table 4.2: MAC parameters used in simulation.

<table>
<tr><td>General Parameters</td><td colspan="4">Data rate = 11 Mbps
Protocol = IEEE 802.11b
Number of nodes: 4, 8, 12, 16, 20, 24, 28, 32, 36 and 40
Application = Real-time voice
TXOP limit = 3 ms</td></tr>
<tr><td rowspan="9">Contention Parameters</td><td colspan="4">MP-EDCA</td></tr>
<tr><td>Risk to Life (RtoL) Priority Nodes</td><td>Risk to Health (RtoH) Priority Nodes</td><td>Risk to Property (RtoP) Priority Nodes</td><td>Risk to Environment (RtoE) Priority Nodes</td></tr>
<tr><td>RtoLSIFS = 10
RtoLSlotTime = 25
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td><td>RtoHSIFS = 25
RtoHSlotTime = 40
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td><td>RtoPSIFS = 40
RtoSIFS = 55
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td><td>RtoPSIFS = 55
RtoESlotTime = 70
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td></tr>
<tr><td colspan="4">CP-EDCA</td></tr>
<tr><td colspan="2">Class 0 (Emergency Priority)</td><td colspan="2">Class 1 (Normal Priority)</td></tr>
<tr><td colspan="2">EPSIFS = 10
EPSlotTime = 25
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td><td colspan="2">NPSIFS = 40
NPSlotTime = 55
AIFS[1] = 4 slots
WMin[1] = 8 slots
WMax [1] = 64 slots</td></tr>
<tr><td colspan="4">EDCA</td></tr>
<tr><td colspan="4">SIFS = 10 µs for all priorities
Slot Time = 20 µs (default) for all priorities
AIFS [2]
Wmin [0] = 2 slots
WMax = 8 slots</td></tr>
</table>

In this research, the MAC parameters used in simulation are for ideal environment. There are two reasons for choosing ideal environment: (1) generalise the results; and (2) it is always good to test evaluate the performance of proposed system under ideal environment.

For this chapter, we used the IEEE 802.11b standard, which has max throughput of 11Mbps [42]. While, 802.11n provides throughput up to 150Mbps (per stream) [39]. A network may accommodate more number of life-saving emergency nodes by using 802.11n [39] or 802.11ac [44]. Moreover, the stationary node model was used where node was static (no mobility). Another side, in real environment mobile nodes are keep moving. If a sender station moves near to the receiver station may be the cause of increased signal strength and increase the throughput performance. Another side, increased distance between sender and receiving node may be cause of weak signals and may be cause of packet loss, low throughput and higher end-to-end delay.

Emergency traffic is prioritised into four categorised. i.e., (1) risk-to-life, (2) risk-to-health, (3) risk-to-property and (4) risk-to-environment. Therefore, we use nodes multiple of four in the each simulation scenario. We use uniform node distribution. Therefore, each MP-EDCA scenario has equal number of emergency to life, health, property and environment saving nodes. This may not be the case in realistic scenario and number may vary of each emergency category. In such case, increasing high priority emergency nodes in the network increase the channel access contention and in the result strict QoS guarantee may be compromised. To address this limitation, a Preemptive Admission Control is investigated in Chapter 5.

Voice is preferred method of communication for first responders [114]. Therefore, real-time interactive voice is used for evaluating the network performance.

Testing the model under realistic environment is essential for the success of model [115]. Therefore, it is recommended for future work to test the performance of proposed MAC protocol under the realistic environment.

4.7 WLAN Performance Measurement Metrics

To evaluate the performance of MAC protocols proposed in chapter 4, 5, and 6, we used following WLAN performance metrics: MAC delay (Network and Class 1), packet retransmissions, throughput and packet drop ratio. These parameters of WLAN performance metrics are described below:

- **MAC Delay:** This is calculated from the duration when frame is inserted into the transmission queue of MAC layer, until the time frame is dispatched to the PHY layer. This includes time for generating (inserting the frame into the queue), total queuing time, contention delay, internal backoff and collision (in case of 802.11e) and dispatches time. The MAC delay is measured in milli seconds.
- **Network MAC Delay:** Average MAC delay of all the nodes in the network.
- **Average MAC Delay of Class 1 (risk to life) emergency traffic:** MP-EDCA categorises the emergency into four (4) classes as discussed in Subsection 4.4. The main motivation of this research is to provide a QoS guarantee for class (risk to life) saving emergency traffic. To evaluate the performance of class 1 (risk to life) traffic, each MP-EDCA scenario consists of an equal number of (Class 1 to Class 4) emergency nodes as shown in Fig. 4.11. Identical scenarios and configuration were used to compare the performance of MP-EDCA with state-of-the-art MAC protocols proposed in the literature, that is, CP-EDCA and EDCA. In each MP-EDCA-based scenario, the average MAC delay of class 1 (risk to life) emergency traffic was calculated and compared with average MAC delay of identical nodes of other schemes.
- **Packet Drop Ratio:** This ratio is also referred to as data dropped ratio. It is linked with the packet collision rate. A packet is usually dropped when one or more packets fail to reach the destination address. This is measured by the percentage (%) of data dropped to data sent [116].
- **Packet Retransmissions:** One of the most commonly used techniques used for recovering the packet errors and losses [117]. Sender resends the packet if the packet is damaged or lost. It is measured as the ratio or percentage of number of retransmission attempts with respect to number of packets sent

- **Average Throughput:** The most common parameter used to evaluate network performance, measured in Mbps. It is expressed in various ways, such as the amount of data successfully delivered within a timeframe. It can be explained as a fraction of the total channel capacity used for data transmission.

An efficient MAC protocol should satisfy the strict QoS needs of emergency traffic, in terms of lower MAC delay, higher throughput, lower data dropped and packet retransmission attempts.

4.8 Results and Discussion

The main motivation for designing MP-EDCA is to provide certain QoS guarantees (in terms of delay) for Class 1 emergency nodes in a dense emergency situation where a large number of nodes report an emergency. For performance evaluation, four parameters are considered: MAC delay, packet drop ratio, throughput and packet retransmission. The MAC packet delay (network-wide as well as an individual node) is a key performance metric considered in this chapter. The delay is measured from the moment an application frame is queued at the MAC-layer until the frame is successfully transmitted. This includes channel contention, queuing and frame transmission delays. Moreover, other QoS parameters such as throughput, packet drop ratio and packet retransmission attempted are used for testing the effectiveness of the proposed protocol for improving the overall network performance. MP-EDCA outperformed the other two MAC protocols, CP-EDCA and EDCA. The performance improvement is achieved by adjusting the values of SIFS and Slot Time. The tuning of SIFS and Slot Time allow the high priority traffic to preempt the low priority emergency traffic.

4.8.1 Network MAC Delay

Figure 4.12 shows the average network MAC delay of MP-EDCA, EDCA and CP-EDCA with varying node density from 4 to 40 nodes. The MAC delays of all three schemes (MP-EDCA, EDCA and CP-EDCA) are almost similar for N = 4 to 16 nodes. However, the average delays of both EDCA and CP-EDCA increase sharply for N = 16 to 40 nodes. One can observe that MP-EDCA offers lower packet delays than both EDCA and CP-EDCA for N > 16 nodes. For example, the network-wide MAC delays for MP-EDCA,

EDCA, and CP-EDCA are 3.4 sec, 8.7 sec and 8.5 sec, respectively. It is found that MP-EDCA can achieve about 60% lower delays than CP-EDCA. Considering 11 Mbps channel, about 5 sec reduction in one-hop MAC delay per emergency frame, when employing MP-EDCA, is significant.

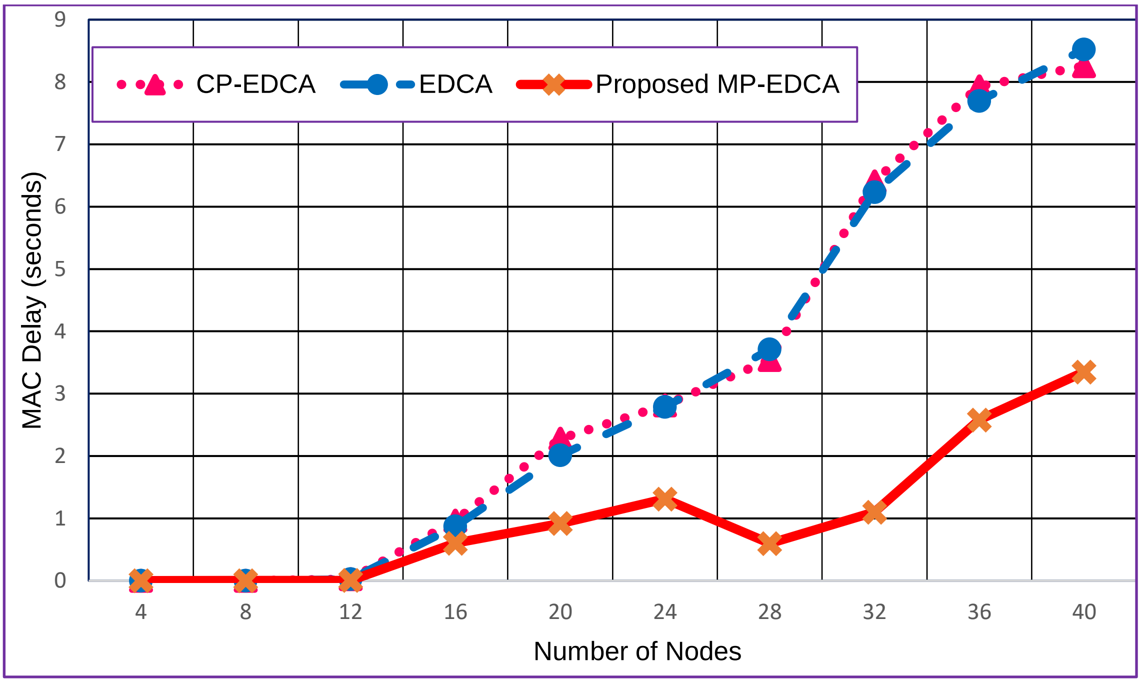

Figure 4.12: MAC delay comparison of EDCA, CP-EDCA, and MP-EDCA.

4.8.2 Average MAC Delay of Class 1 (risk-to-life) Emergency Traffic

One of the main objectives of this research is to support lifesaving emergency traffic in the network under high traffic loads. Figure 4.13 shows the average MAC delay of class 1 (Risk to Life) emergency node. The performance of the Class 1 node is compared with that of the CP-EDCA's emergency node (note: In CP-EDCA all types of emergency traffic have the same priority) and EDCA's node with voice priority. Notably, the proposed MP-EDCA offers about 70% and 80% lower MAC delays than EDCA and CP-EDCA protocols, respectively. Further, also noted that the MP-EDCA's MAC delays for Class 1 remain low when the nodes increased from 16 to 40. Figure 4.14 further illustrates the results. The average MAC delay for class 1 traffic (MP-EDCA) is within the limit of the required QoS by real-time voice traffic (i.e., one-way end-to-end delay) of accommodating increased number of lifesaving emergency nodes in the network and

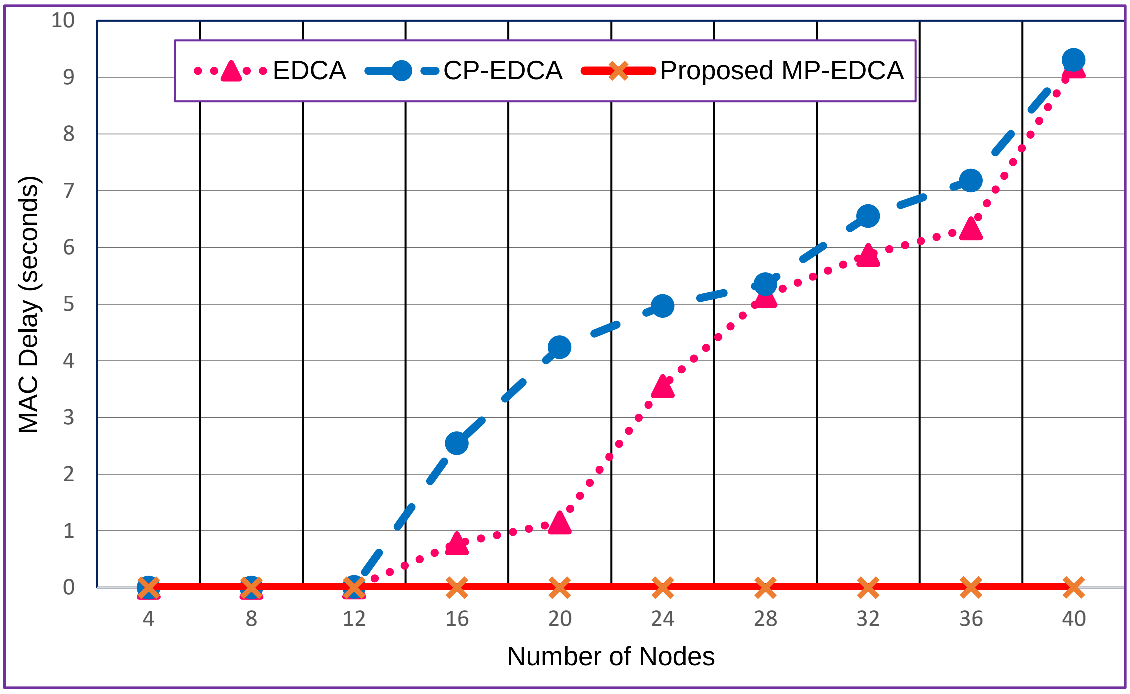

Figure 4.13: MAC delay for Class 1 (risk-to-life) emergency node. Comparison of EDCA, CP-EDCA, and the proposed MP-EDCA protocols.

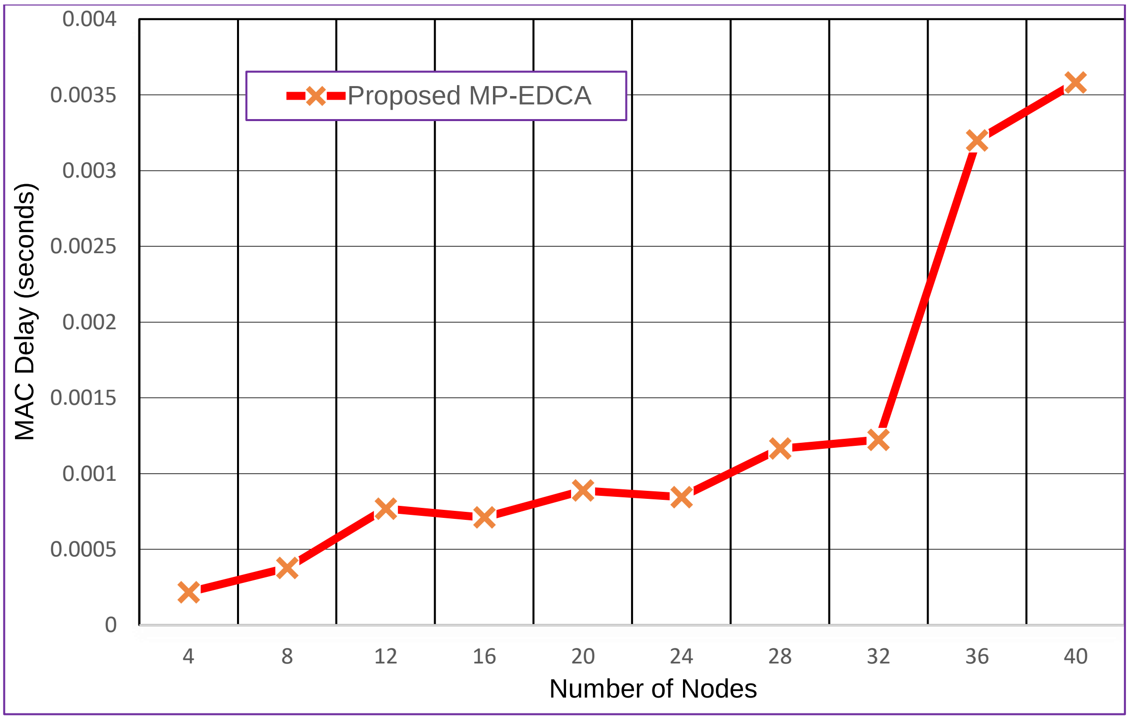

Figure 4.14: This diagram is redrawn by expanding Fig. 4.12 for clear illustration of MAC delay for MP-EDCA's class 1 (risk-to-life) emergency node.

providing the required QoS guarantee in terms of delay is achieved by providing on-arrival channel access and multiple preemptive mechanisms, and delaying low priority emergency traffic.

4.8.3 Packet Drop Ratio

The network-wide data (packets) drop ratio of MP-EDCA, EDCA and CP-EDCA protocols for N = 4 to 40 nodes for an ad hoc network is shown in Fig. 4.15. It is observed that fewer packets are dropped under the MP-EDCA protocol than EDCA, and CP-EDCA. For example, MP-EDCA offers about 75% lower data drop than EDCA for N = 12 nodes. This improvement is because of MP-EDCA protocol's channel access strategy where only high priority emergency (lifesaving) nodes compete for channel access (fewer instances of contention by nodes). Conversely, in EDCA and CP-EDCA, all the nodes (including low priority emergency nodes) compete for channel access. Consequently, MP-EDCA achieves higher throughput than EDCA and CP-EDCA.

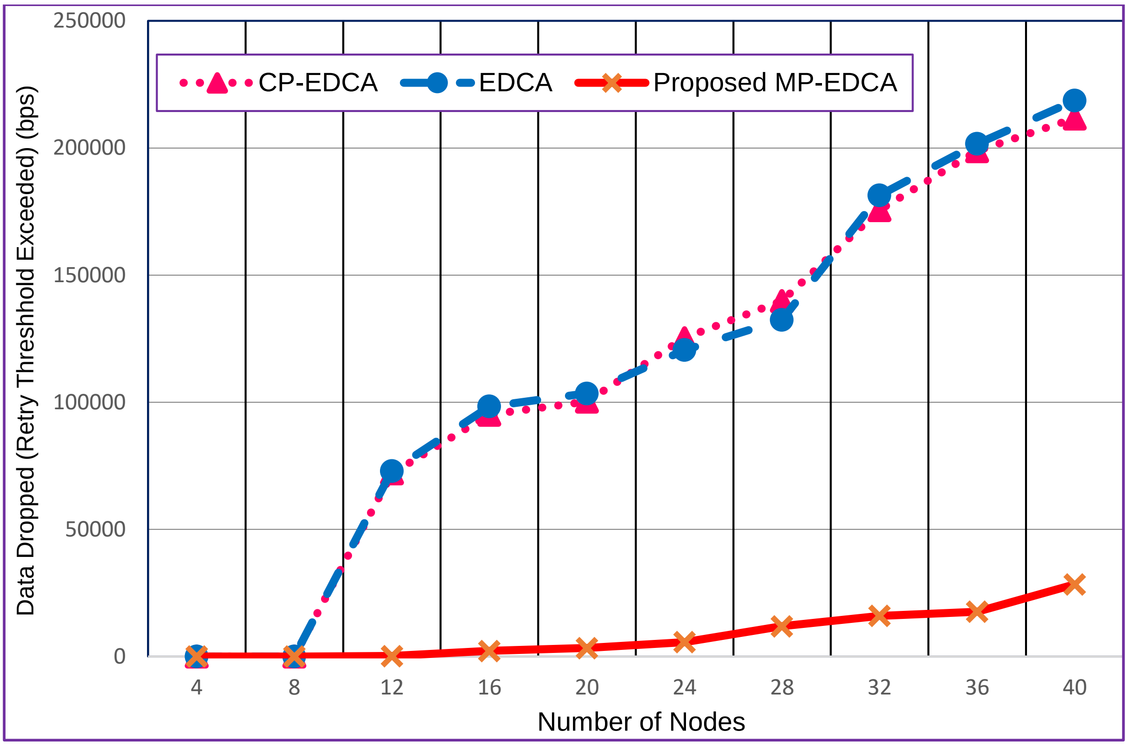

Figure 4.15: The packet drop ratio versus the number of active nodes of EDCA, CP-EDCA and the proposed MP-EDCA.

4.8.4 Packet Retransmission

The key idea of deploying MP-EDCA for WLAN is to provide the prioritised emergency traffic with the required QoS. This is achieved when the number of retransmitted packets is decreased and it improves the overall communication service. The simulation results shown in Fig. 4.16 present the average number of packet retransmissions for three protocols considered. For various number of nodes, the proposed MP-EDCA outperforms both CP-EDCA [8] and the standard ECDA. The MP-EDCA decreases the number of packets retransmitted up to 60% lower than both CP-EDCA and the standard EDCA. This was achieved by the optimisation of the slot time and SIFS.

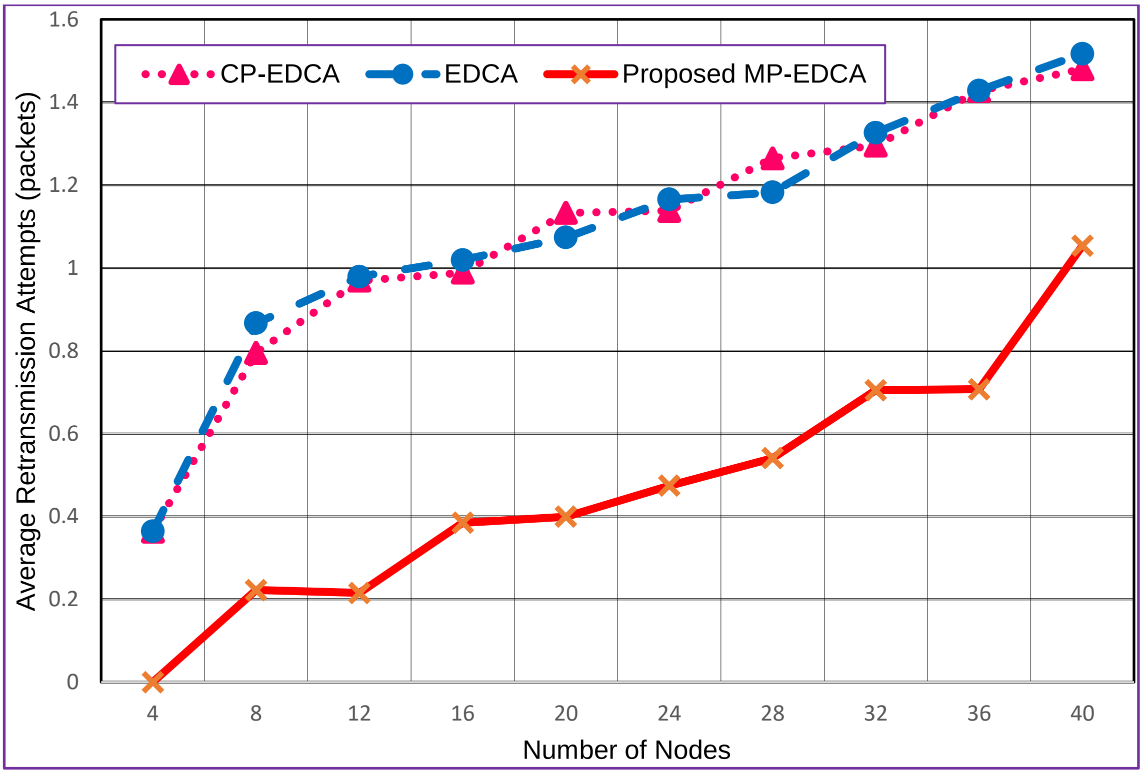

Figure 4.16: Average retransmission attempts versus the number of nodes of EDCA, CP-EDCA and the proposed MP-EDCA.

4.8.5 Average Throughput

Figure 4.17 exhibits the comparative average of the network throughput for various numbers of nodes. The obtained results show that the proposed MP-EDCA outperforms both EDCA and CP-EDCA QoS mechanisms in providing better throughput. MP-EDCA offers an improved network throughput up to 0.77 Mbps compared with 0.7Mbps of CP-EDCA and 0.64Mbps of EDCA. Generally, MP-EDCA achieves up to 20% and 10% higher network throughput over EDCA and CP-EDCA, respectively. On the examining the graphs in Fig. 4.17 closely, one can notice that the average network throughput constantly increases with the increase in the number of nodes.

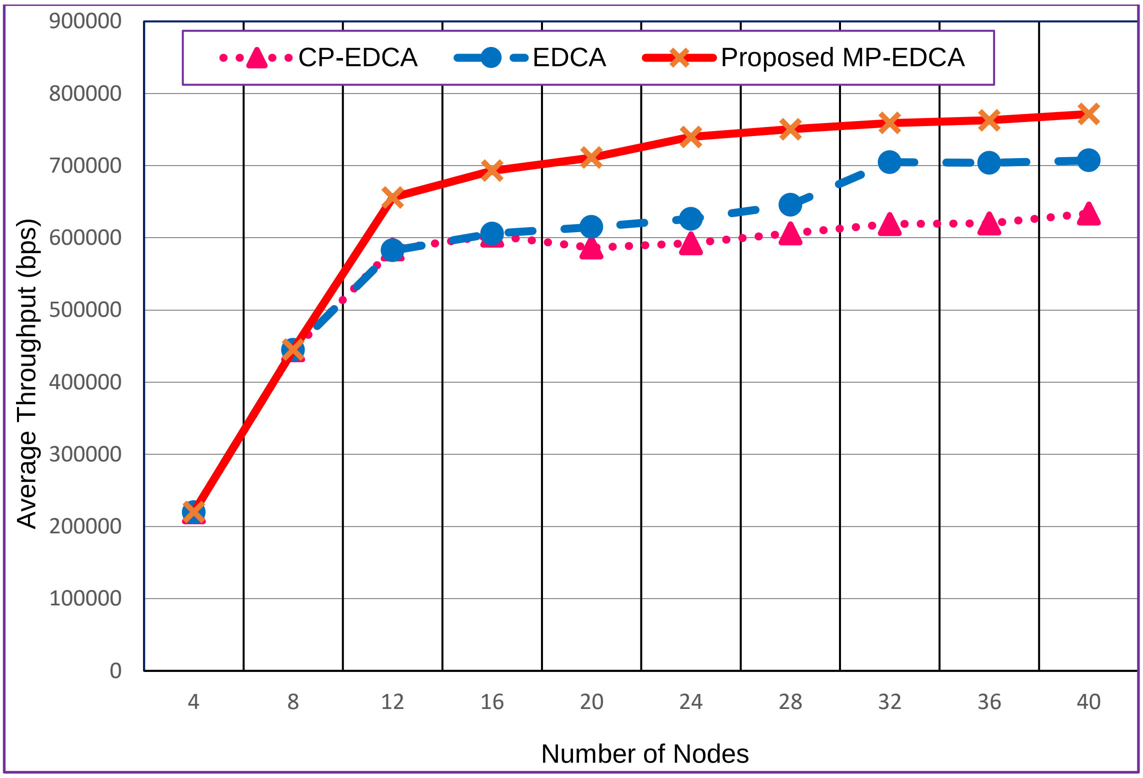

Figure 4.17: Average network throughput versus the number of nodes of EDCA, CP-EDCA and the proposed MP-EDCA.

4.9 Strengths and Weaknesses

4.9.1 Strengths of MP-EDCA

The MP-EDCA is a novel scheme that supports emergency traffic (provides immediate channel access as compared with the normal traffic), and accommodates increased number of emergency nodes in the network. Moreover, high priority emergency traffic is allowed to preempt the low priority emergency traffic. The proposed scheme is simple but effective and can be implemented with minor modification of EDCA. However, MP-EDCA does not provide a QoS guarantee in terms of delay when traffic loads increase.

MP-EDCA provides better emergency traffic support and accommodates more nodes with lifesaving emergency traffic in the network than EDCA and CP-EDCA because it prioritises the emergency traffic. In addition, a high priority emergency traffic may preempt the low priority emergency traffic and obtain immediate channel access. This improvement is due to MP-EDCA's multiple preemptive strategy. The MP-EDCA provides a certain QoS guarantee to class 1 emergency nodes in a dense emergency application where a large number of nodes report an emergency. Moreover, MP-EDCA is simple and can be easily implemented within EDCA. Further, the proposed scheme as energy efficient as EDCA because MP-EDCA uses the same contention mechanism as standard EDCA.

Although MP-EDCA provides a better emergency traffic support than EDCA and CP-EDCA, it does not provide a strict QoS guarantee and protection to ongoing emergency traffic burst from an upcoming same priority emergency traffic.

4.9.2 Limitations of MP-EDCA

To identify the limitations of MP-EDCA, extensive simulations performed in Riverbed Modeler [118] to study the performance of MP-EDCA and confirm the problem of a strict QoS guarantee. The nodes were increased further and five scenarios were created with the 44 nodes to 60 nodes of each EDCA, CP-EDCA, and MP-EDCA. Uniform node distribution was used since MP-EDCA incorporates the four different types of emergencies, related to life, health, property and environment.

Figures 4.12 to 4.17 illustrate that MP-EDCA performs better and accommodates more emergency nodes than EDCA and CP-EDCA. However, MAC delay for class 1 (risk to life) traffic of MP-EDCA is increases significantly for $N > 40$ nodes.

The MP-EDCA achieve its objective by providing on-arrival channel access priority and accommodating more lifesaving emergency nodes in the network. However, it does not provide a QoS guarantee when the network load is increased ($N > 40$ nodes) as shown in Fig. 4.18 and Fig. 4.19. The network overload may lead to performance degradation for lifesaving emergency traffic that should be strictly avoided.

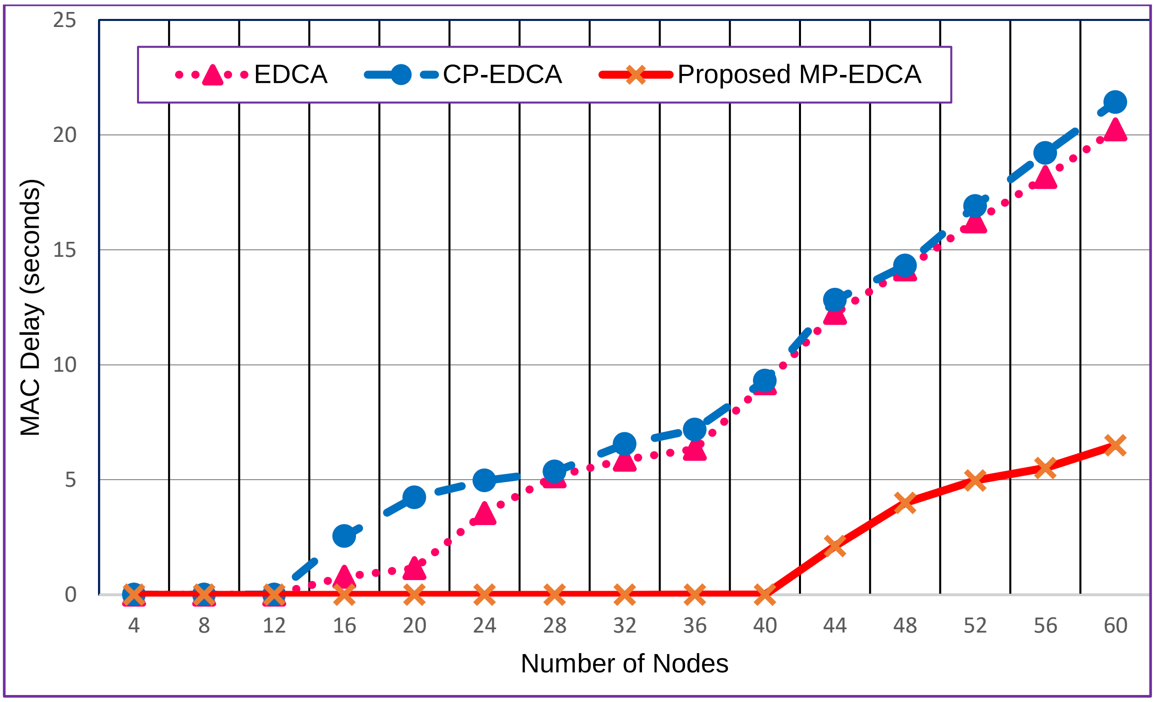

Figure 4.18: MAC delay performance for a Class 1 (Risk to Life) emergency node.

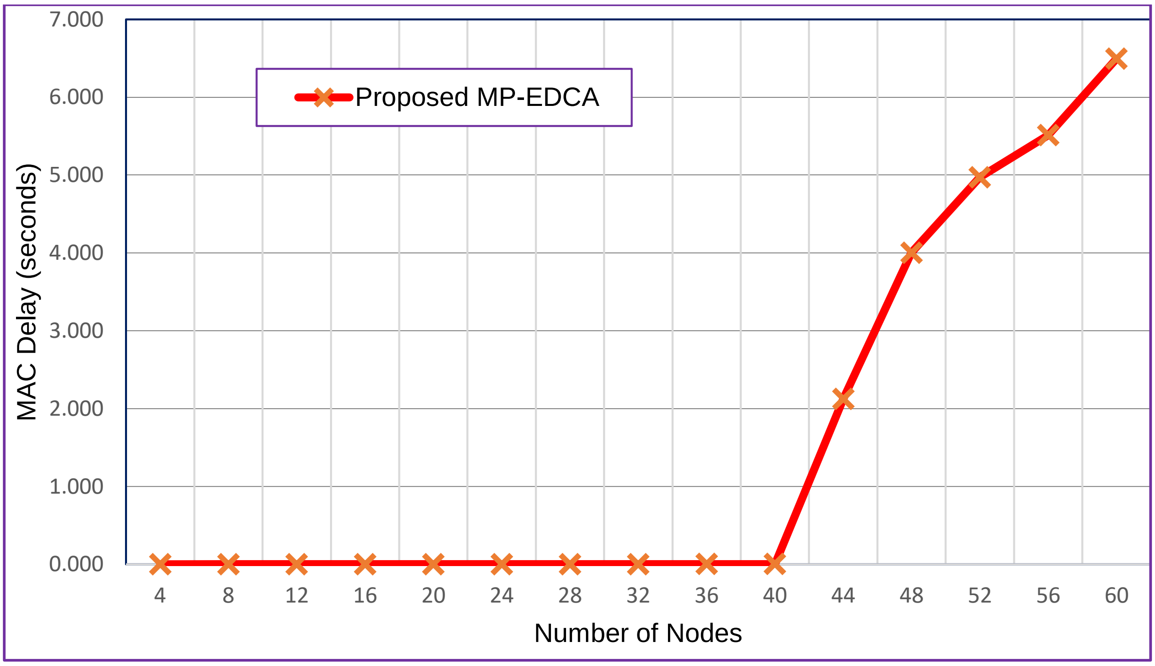

Figure 4.19: This diagram is drawn by expanding Fig. 4.17 for clear illustration of MAC delay for a Class 1 (Risk to Life) emergency node.

4.10 Implementation Aspects of MP-EDCA

A disaster is a dreadful dense emergency event, which may cause substantial loss of human life, property or environment [119]. Disasters can be categorised into two types, natural and manmade disasters. In recent years, the frequency of both disasters increased, which demands effective communication mechanisms for saving human life [120].

Cellular, fixed infrastructure or centrally controlled networks are highly affected by an emergency [121]. Moreover, cellular networks either become jammed (network congested) or shut down to avoid remote detonation of more explosives. For example, after the bombing attacks in Boston, the network load increased the number of times. Cellular networks were jammed because numerous people were trying to contact their loved ones or trying to gather information about the incident. To normalise the situation, people were warned through social media to text, rather than call to free some bandwidth. Moreover, people were requested to open their closed WLANs [121]. A news Article published in [121] also highlights the need for deployment of city-wide Wi-Fi (brand name of WLAN) with emergency traffic support.

First responders (relief workers) need reliable communication during dense emergency situations to save human life. To provide reliable communication under such situation, a WLAN is the alternative. However, the WLAN in its current form does not support emergency traffic, especially in a dense emergency situation.

The deployment of MP-EDCA could address this issue by supporting emergency traffic and prioritising lifesaving emergency traffic. Moreover, the deployment shall take effect only when the existing WLAN upgrades the MAC protocol, such as the protocols proposed in this thesis. In addition to a disaster situation, the proposed protocol could be used in network-saturated conditions such as public events (e.g., soccer game) to prioritise emergency traffic.

WLANs use unlicensed radio frequencies. Therefore, other device protocols may take advantage of it. Consider the above emergency situations (e.g., 9/11 or Boston bombing), the deployment of MP-EDCA in an emergency is simple. Consequently, the system planners could use the ideas and results provided in this thesis for adequately handling a dense emergency in terms of communication.

4.11 Summary

In this chapter, an in-channel multiple service preemption scheme termed MP-EDCA was discussed. The MP-EDCA extends the original 802.11e capabilities by accommodating emergency traffic in 802.11 networks. The scheme provides immediate channel access privileges to high priority emergency traffic in distributed networks.

The performance of MP-EDCA, CP-EDCA and EDCA were compared by extensive simulation experiments. The simulation results showed that MP-EDCA achieved up to 60% lower MAC delays (network-wide), about 99% lower delays for risk-to-life emergency traffic, 75% lower packet drop ratio, up to 60 lower packets retransmitted and 20% higher throughput than CP-EDCA. The MP-EDCA can provide better QoS to emergency nodes under high traffic conditions more effectively. Moreover, immediate channel access for lifesaving emergency traffic is guaranteed even in a saturated emergency since nodes for an emergency provided. However, when all nodes are in "risk to life" (an unusual case), MP-EDCA performs as well as the CP-EDCA.

In MP-EDCA, physical parameters, such as SIFS and slot time are modified in such a way that high priority emergency (lifesaving) traffic receives the highest priority, immediate channel access and ability to preempt any low priority emergency (health, property and environment) traffic. Next, in Chapter 5, the provision of the QoS guarantee using admission control is investigated.

Chapter 5

Preemptive Admission Control MAC for Strict QoS Guarantee in WLANs

5.1 Introduction

In Chapter 4, a novel in-channel MP-EDCA was proposed for supporting emergency traffic. The primary objective of this thesis is to develop a MAC framework that supports emergency traffic (immediate channel access) and provide strict QoS guarantee in WLANs. The MP-EDCA protocol reported in Chapter 4 supports emergency traffic by giving privileges to high priority lifesaving emergency traffic to preempt the ongoing traffic stream for immediate channel access and accommodates more nodes with lifesaving emergency traffic. However, MP-EDCA may not be effective in providing a QoS guarantee under high traffic loads (see Fig. 4.18). Therefore, this chapter addresses the limitations of MP-EDCA by proposing a preemptive admission control (PAC) protocol, termed PAC-MP-EDCA.

Admission control is used to implement network management policies, manage the available bandwidth, or ensure that time-sensitive applications will receive the required QoS guarantee [45]. Admission control ensures that the admittance of new traffic streams into a resource-constrained network does not affect the QoS required by existing traffic streams. There are two distinct admission control mechanisms: contention-based for EDCA and controlled-based for HCCA. In general, admission control depends on vendors' specifications such as available channel capacity, link conditions, retransmission limits, and the scheduling requirements of a given stream [39]. The use of admission control in the proposed research will provide a strict QoS guarantee to time-sensitive applications.

The objective of PAC is to address the performance degradation issue of MP-EDCA and provide a strict QoS guarantee in dense emergency applications where a high number of nodes report the emergency. The PAC is simple and effective and uses admission control scheme based on the capacity analysis.

The remainder of the chapter is organised as follows. In Section 5.2, the previously reviewed research on providing QoS guarantee is reviewed further. The proposed PAC-MP-EDCA is described in Section 5.3. Section 5.4 presents the simulation setup and discusses implementation aspects of PAC. Simulation results are presented and discussed in Section 5.5. The strengths and limitations of PAC-MP-EDCA are discussed in Section 5.6, and the chapter is concluded in Section 5.7.

5.2 Previous Research on Providing QoS Guarantee using Admission Control

Emergency traffic requires a strict QoS guarantee and main limitation of IEEE 802.11e (EDCA) is that it does not provide any QoS guarantee to time-sensitive applications under medium-to-high traffic load [15]. Therefore, many network researchers believe that a QoS guarantee cannot be achieved without defining effective admission control. This section briefly reviews only a selected set of admission control schemes discussed in Subsection 3.3.2.

Despite providing service differentiation, the EDCA cannot support strict a QoS guarantee for time-sensitive applications [83]. Thus, numerous researchers proposed remarkable admission control methods for regulating incoming traffic into the network. Son, S. et al. [88] proposed admission control, which applies an adaptive arbitration inter-frame spacing AIF mechanism to address the QoS guarantee in EDCA. However, this admission control limits the traffic based on network capacity and adaptive AIFs to prioritise high priority traffic. The authors [88] only claim that the system provides differentiation of services near absolute priority for high priority traffic.

Xiao, Y. et al. [17] adopted a two-level protection approach to guarantee time-sensitive traffic. They proposed a distributed admission control and tried-and-known approach; The admission control measures the channel utilisation on each beacon interval, based on which available capacity is calculated. Traffic streams do not receive transmission time if their class capacity is zero. Further, STAs are not allowed to increase transmission time. In addition to the tried-and-known mechanism, a new STA flow is first temporarily accepted and throughput and delay performance are measured for some beacon interval. If it affects the performance and does not meet a specific requirement, then flow is rejected. Similarly, Hamidian et al. [19] proposed an EDCA-distributed resource reservation (EDCA-DRR) scheme that uses a distributed approach for same admission control, traffic scheduling and resource reservation. This EDCA-DRR is an enhancement of EDCA with resource reservation (EDCA-RR) [12], which calculates the schedule service interval and resource reservation before admitting the time sensitive traffic stream.

Time-sensitive applications need stringent QoS requirements and thus an efficient AC mechanism should always give them high priority. Chen et al. [18] proposed two schemes: call admission mechanism and rate control mechanism. Call admission control is for real-time traffic and rate control is for best-effort traffic. Rate control utilises remaining channel capacity without affecting the time-sensitive traffic; each STA monitors the channel busyness ratio and estimates the rate of the ongoing real-time traffic before adding the traffic. Similarly, Sarma et al. [21] investigated a strict priority based QoS-aware protocol (SPQAMP) that gives priority to time-sensitive STA to send the packet by assigning non-overlapping values to CW for high priority and low priority traffic and resets the backoff counter instead of freezing for low priority traffic. In addition, a similar approach that provides QoS to different time-sensitive applications based on the traffic flow and queuing schemes is proposed in [22]. In this AC method, each STA alters the backoff counter based on its own packet's priority and previously transmitted packet's priority to protect time-sensitive traffic.

Yang et al. [122] investigated the priority random early detection (PRED) mechanism by enhancing the random early detection (RED) proposed in [84]; PRED alters queue[AC] based on the traffic load used scheduling mechanism to give priority to each packet within the STA.

Finally, Pang et al. [123] investigated a Joint Measurement-based Admission and Bandwidth Control (JMABC). JMABC provides protection to ongoing traffic stream from the upcoming traffic stream through a measurement-based admission control scheme. Moreover, JMABC prioritises real-time traffic using the packet scheduling scheme. All incoming packets from other stations are first admitted by admission control and then forwarded to the adaptive class-based queue, which is monitored by a feedback monitoring module. The feedback monitoring module determines this queue's throughput and system's total throughput and provides the feedback back to admission control. JMABC may provide a QoS guarantee to real-time traffic, however, operations cost of JMABC may highly affect the system performance.

Most of the proposed schemes in literature only provide a QoS guarantee under low traffic load, and when the traffic load is increased they provide service differentiation rather than a QoS guarantee [124]. Unlike these approaches, the proposed PAC-MP-EDCA protocol provides a strict QoS guarantee, especially to lifesaving emergency traffic. The PAC-MP-EDCA is discussed next.

5.3 Description of Proposed Preemptive Admission Control Protocol

The proposed PAC-MP-EDCA scheme described in this chapter differs from the earlier work described in Section 5.2. It has different goals and capabilities.

The PAC mechanism in the proposed scheme can protect high priority traffic from low priority data. In most cases, it protects high priority data from being degraded by the other traffic of the same priority. In MP-EDCA, admission control is not required to protect high priority data from the low priority data owing to its preemptive nature. However, it may require protecting high priority lifesaving emergency traffic from other same priority traffic. In this section, a model-based admission control for EDCA is presented. The specifications of admission control are based on the IEEE 802.11e standard [2]. Moreover, PHY and MAC parameters use to tune the admission control were presented in Chapter 4. The PAC-MP-EDCA enhances the capabilities of 802.11e standard and defines the decision related to admission of new emergency flow starts/departs or the WLAN state changes. The PAC mechanism is assumed to be located at the central coordinator emergency node or AP (Fig. 5.1). In Fig. 5.1, the node in red colour represent the first responders in the disaster situation, and the node in green colour has all the resources. Green colour node works as a central coordinator node (AP). All other nodes look to the green node for resources.

The proposed PAC protocol addresses the performance degradation problem of MP-EDCA and provides a strict QoS guarantee to lifesaving emergency traffic. In the present study, an admission control is introduced based on the PAC algorithm and capacity analysis of emergency traffic. Among the four types of emergency traffic, admission control is applied to the Risk to life (lifesaving) emergency traffic.

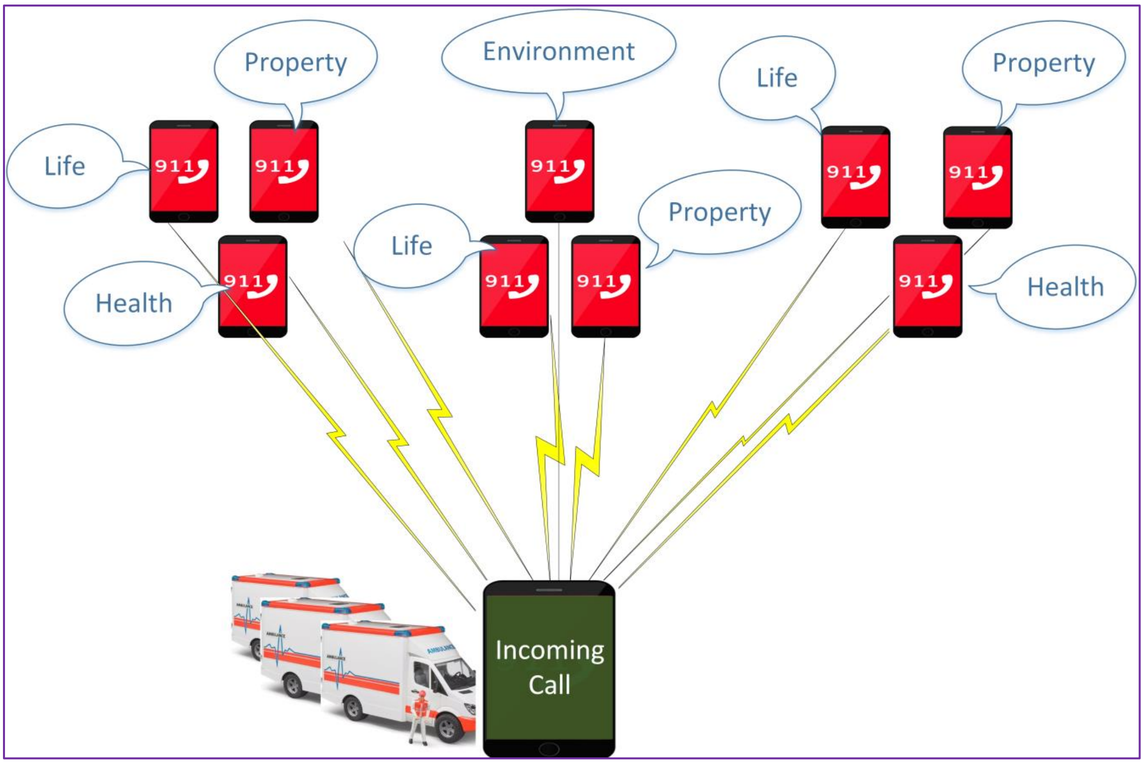

Figure 5.1: Emergency scenario of PAC-MP-EDCA.

Central coordinator node (green node in Fig. 5.1) advertises ACM bit for lifesaving emergency traffic category using the Beacon to indicate that admission control is mandatory for lifesaving emergency traffic. The node with lifesaving emergency traffic sends Add Traffic Stream (ADDTS) request action frame to AP that includes a Traffic Specification (TSPEC). The parameters for PAC includes a MAC Service Data Unit (MSDU) size, mean data rate, min Physical (PHY) rate, surplus bandwidth allowance (SBA). Once AP receive ADDTS request, AP runs the PAC mechanism (PAC algorithm and capacity analysis) and communicate back to the emergency node with the admittance decision using ADDTS response action frame.

5.3.1 The Proposed PAC-MP-EDCA algorithm

In the PAC protocol, a wireless station first specifies its traffic characteristics and QoS needs using the TSPEC. A new emergency traffic stream (node) can only join the network if either network has availability of required resources or the node has higher emergency priority than the priority with existing ongoing nodes. The PAC algorithm is implemented in each of the wireless nodes at the MAC layer. The implementation aspect of PAC-MP-EDCA is shown in **Figure 5.1**, and the corresponding pseudo-code is shown in **Figure 5.2**.

```
If required slots (bandwidth) is available for new traffic flow then
        Accept the new emergency traffic flow
Else
        If new traffic flow has higher priority than ENVIRONMENT (EMERGENCY) then
                find all existing lowest priority traffic flows than new traffic flow's priority
                Calculate the required number of slots for new traffic flow
                Find low priority traffic flow which is using the same number of slots //best
                match or random match
                Preempt the low priority of existing traffic flow
                Admit new high priority traffic flow
        Else (the new traffic flow has the lowest priority than all existing flows)
                Reject the admission of new traffic flow
        End
End
```

Figure 5.2: The pseudo code of the proposed PAC-MP-EDCA algorithm.

Suppose, there are Su-1 ongoing traffic streams. When the new emergency traffic stream Su^{th} arrives, the PAC will calculate the available resources. If enough resources are available to admit the new emergency traffic stream Su^{th} and satisfy the QoS required by the new stream without affecting the QoS required by ongoing traffic stream, admission will be granted to new traffic stream. Otherwise, the priority of new traffic stream is checked.

5.3.2 Capacity analysis of Risk to Life emergency

The PAC-MP-EDCA is based on the capacity analysis of emergency traffic. The capacity analysis approach presented in this Section is adopted from [86]. The main difference is that admission control reported by Sunghwa, S. et al. [86] is limited to low priority traffic, whereas admission control reported in this Chapter is only limited to the high priority lifesaving emergency traffic. Another difference is that the design of PAC-MP-EDCA is based on the MP-EDCA, described in Chapter 4.

In PAC-MP-EDCA, among the four categories of emergency traffic considered in this research, admission control is applied only to $RtoL$ (lifesaving) emergency traffic and will be activated dynamically when the load is reached at the network capacity. The high priority emergency traffic will be delivered timely because of MP-EDCA's preemptive nature. The problem occurs when the same priority traffic wants to access the medium in a saturated situation which increases the collision and degrade the performance. Therefore, proposed PAC-MP-EDCA analyse the network capacity and provide the protection to the existing (ongoing) flow of $RtoL$ emergency traffic from low or same priority emergency traffic specifically in saturated network condition. The admission control analyses the network capacity for emergency traffic before admitting the new traffic flow. To analyse the network capacity for emergency traffic, we followed the similar capacity analysis scheme conducted for saturated condition by [125].

For n $RtoL$ nodes within the BSS, let the probability of the network state as fraction of transmitting time of node k be denoted by ρ_k. The idle channel time is denoted by ρ_0. Furthermore, the ratio of the expected transmission time $\epsilon[\varphi_k]$ to the expected backoff time $\epsilon[\psi_k]$ for transmitting node k be denoted by $\mu_k = \epsilon[\varphi_k]/\epsilon[\psi_k]$.

The total number of transmissions by $RtoL$ node k are represented by $c_k(t)$. In the network scenario, if the channel is idle and all the $RtoL$ nodes waiting for the channel would decrease the backoff counters. Thus, the ratio of ρ_k to ρ_0 can be represented as:

$$\frac{\rho_k}{\rho_0} = \lim_{t\to\infty} \frac{\frac{1}{t}\sum_{j=1}^{c_k(t)} \varphi_k(j)}{\frac{1}{t}\sum_{j=1}^{c_k(t)} \psi_k(j)} = \lim_{t\to\infty} \frac{\frac{1}{c_k(t)}\sum_{j=1}^{c_k(t)} \varphi_k(j)}{\frac{1}{c_k(t)}\sum_{j=1}^{c_k(t)} \psi_k(j)} = \frac{\epsilon[\varphi_k]}{\epsilon[\psi_k]} = \mu_k \tag{5.1}$$

Where $\psi_k(j)$ represents the length of the j-th backoff interval of $RtoL$ node k and $\varphi_k(j)$ is the length of jth transmission of $RtoL$ node k. From the equation (5.1), a system of the linear equations may be defined as below:

$$\rho_\emptyset = \frac{\rho_1}{\mu_1} = \frac{\rho_2}{\mu_2} = \cdots = \frac{\rho_n}{\mu_n} \tag{5.2}$$

As $\sum_{k=0}^{n} \rho_k = 1$, the above equation can be solved as follows:

$$\rho_\emptyset = \frac{1}{1+\mu_1+\mu_2+\cdots+\mu_n}, \quad \rho_k = \rho_\emptyset \mu_k \tag{5.3}$$

We consider that MPDU of $RtoL$ node k consists of a MAC header (where MAC header includes frame check sequence). Let, the payload be transmitted at the rate of δ_k, the PHY header consist of preamble and acknowledgement frame; and are transmitted at the ratio of $\delta_{min}(\leq \delta_k)$, which does not depend on δ_k, in case of reliable transmission. Moreover, T_{PH}, T_{MH}, T_{PL}, and T_{ACK} is the time period for transmitting the complete frame i.e., PHY header, MAC header, payload and ACK. The transmission rate of node k to transmit a packet, denoted as $\overline{\delta_k}$, can be expressed as:

$$\overline{\delta_k} = \omega_k \delta_k + (1 - \omega_k)\delta_{min}, \tag{5.4}$$

where $\omega_k = \frac{(T_{MH}+T_{PL})}{(T_{PH}+T_{MH}+T_{PL}+T_{ACK})}$.

As, T_{SIFS} is negligible as compare to T_{PL}, thus is not considered in the calculation of $\overline{\delta_k}$. herefore, x_k, the achievable throughput of saturated node k, is given as:

$$x_k = \rho_k \overline{\delta_k} = \left(\frac{\mu_k}{1+\mu_1+\mu_2+\cdots+\mu_n}\right) \overline{\delta_k}, \tag{5.5}$$

Based on the pseudo code (Fig. 5.2) and above capacity analysis, a simple admission control for $RtoL$ emergency services is designed. We consider that a node with $RtoL$ emergency traffic first sends a request for admission to the central coordinator node. After receiving the request, central coordinator node may send the admission response with acceptance or rejection.

Discussion:

Let n_{RtoL} and ν_{RtoL} be the total number of ongoing $RtoL$ nodes, the maximum number of allowable $RtoL$ nodes is based on the capacity analysis e.g., 40. The central coordinator node receives the admission request, the central coordinator node accepts the request as long as $n_{RtoL} < \nu_{RtoL} - \Delta\nu_{RtoL}$, where $\Delta\nu_{RtoL}$ is a positive integer number. Here, $\Delta\nu_{RtoL}$ is used for modelling error of capacity analysis into consideration. Once the $RtoL$ emergency traffic stream is admitted, the central coordinator node updates n_{RtoL} . In case, central coordinator node does not receives any traffic from connected $RtoL$ node for a given time, that is, generally more than the packet generation interval of the $RtoL$ application. Then, the central coordinator node shall consider the connection is lost, therefore, decrease the n_{RtoL} by 1. In this process, central coordinator node will not calculate the probability or rates in Eqs. (5.1) to (5.5) to estimate the ν_{RtoL}, that can be estimated by the traffic model of $RtoL$ node. Therefore, there is not computation cost of this admission control.

Consider, the throughput achievable in Eq (5.5) is taken without estimating the collision, the assumption is that the central coordinator node will not admit new $RtoL$ nodes over the capacity. The central coordinator node will maintain the number of $RtoL$ connection at the given time for managing the network capacity. Since, multiple $RtoL$ nodes simultaneously access the medium and be cause of collision. Therefore, to minimise the probability of the collision, the admission delaying techniques may incorporated in central coordinator node. For example, υ_{int} as the interval for generating packet of $RtoL$ node, and τ_k is a time when the $RtoL$ connection i is admitted. The $\Delta\tau_k(> 0)$ as the offset timing of $RtoL$ connection k within υ_{int} $\Delta\tau_k = mod(\tau_k, \upsilon_{int})$ where $mod(x, y)$ is a modulus function that divides x by y and returns modulo. If the central coordinator node receives a new admittance request for $RtoL$ node at the time of τ_k, it calculates the difference between $\Delta\tau_m$ and $\Delta\tau_k(\forall k \neq m)$. If the calculated difference is lower than $CW_{RTOL} \cdot \varphi_{slot}$ for any $k \neq m$, the central coordinator node may not respond to the admission request and may delay the admission by certain time while $d(> 0)$, where:

$$\Delta\tau'_m = mod(\tau_m + d, \varphi_{int})$$

$$\underset{\{k \neq m\}}{\text{Min}} |\Delta\tau'_m - \Delta\tau_k| > CW_{RTOL} \cdot \varphi_{slot} \qquad (5.6)$$

Then, the central coordinator node updates the offset timing of $RtoL$ connection m as the updated value of $\Delta\tau'_m$. Moreover, the central coordinator node accepts the $RtoL$ node admission request if no any $RtoL$ node satisfying Eq (5.6). The admission request from $RtoL$ nodes may come at random time. Therefore, the probability is negligible.

The ν_{RtoL} is a few tens, φ_{int} is a hundred milliseconds and $CW_{RTOL}. \varphi_{slot}$ is less than 1 milisecond. Therefore, the delay from central coordinator node while admitting the new $RtoL$ node is according to the Eq (5.6).

5.4 Performance Evaluation

The objective of PAC-MP-EDCA is to address the performance degradation issue, and provide a QoS guarantee to the lifesaving emergency traffic of MP-EDCA. Therefore, this section evaluates the performance of the proposed PAC and compares it with the MP-EDCA [108] and EDCA [126]. Three simulation models, (1) MP-EDCA with PAC (PAC-MP-EDCA), (2) MP-EDCA without PAC and (3) EDCA models were developed in Riverbed Modeler [25]. While the main objective is to evaluate the performance of MP-EDCA with and without PAC, the performance of PAC-MP-EDCA is compared with that of the already implemented EDCA for the validating simulation results. For developing the models, the code, existing process models and node models of Riverbed Modeler were modified. The performance of PAC-MP-EDCA is evaluated by using extensive simulations.

5.4.1 Simulation Environment and Parameters

Figure 5.3 shows the Riverbed representation of a fully connected network of PAC-MP-EDCA. For simulating (1) PAC-MP-EDCA, (2) MP-EDCA and (3) EDCA, a total of 45 scenarios (15 scenarios in each case) were created. For each scenario, nodes vary from N = 4 to 60, which communicated with the central coordinator node. AP functionality of a central coordinator node was enabled.

Uniform node distribution was used in the MP-EDCA and PAC-MP-EDCA scenarios where each scenario consists of an equal number of (Class 1 to Class 4) emergency nodes (identical configuration). The number of nodes was increased up to 60 to observe the effect of system performance for various emergency priorities. MP-EDCA supports four types of emergencies with various priorities (uniform node distribution).

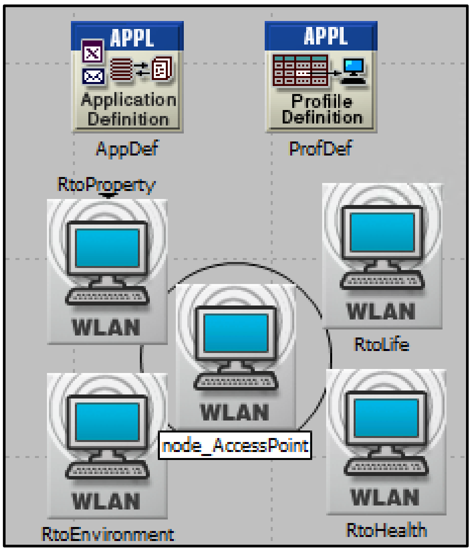

Figure 5.3: Riverbed representation of the fully connected network PAC-MP-EDCA.

Class 1 category nodes use RtoLSIFS and RtoLSlotTime, Class 2 category nodes use RtoHSIFS and RtoHSlotTime, Class 3 nodes use RtoPSIFS and RtoPSlotTime, and Class 4 nodes use RtoESIFS and RtoESlotTime. In EDCA [45], all nodes use default SIFS and Slot Time as EDCA does not support emergency traffic. Apart from SIFS and Slot Time, all other parameters are set to EDCA default values. Table 5.1 shows the parameter values used in the simulation of MP-EDCA with PAC (PAC-MP-EDCA) and without PAC (MP-EDCA). Each simulation run lasted 300 seconds. The real-time voice traffic was used to evaluate the performance.

Table 5.1: MAC parameters used in simulation.

<table>
<tr><td>General Parameters</td><td colspan="4">Data rate = 65Mbps (base)/600 Mbps (max)
Protocol = IEEE 802.11n
Number of MP-EDCA without PAC nodes without 4 - 60 nodes
Number of MP-EDCA with PAC: 4 – 60 nodes
Application: Interactive voice (G.723.1.5.3K Encoder Scheme)
TXOP limit = 3 ms</td></tr>
<tr><td rowspan="5">Contention Parameters</td><td colspan="4">MP-EDCA and PAC-MP-EDCA</td></tr>
<tr><td>Risk to Life (RtoL) Priority Nodes</td><td>Risk to Health (RtoH) Priority Nodes</td><td>Risk to Property (RtoP) Priority Nodes</td><td>Risk to Environment (RtoE) Priority Nodes</td></tr>
<tr><td>RtoLSIFS = 10
RtoLSlotTime = 25
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td><td>RtoHSIFS = 25
RtoHSlotTime = 40
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td><td>RtoPSIFS = 40
RtoSIFS = 55
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td><td>RtoPSIFS = 55
RtoESlotTime = 70
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td></tr>
<tr><td colspan="4">EDCA</td></tr>
<tr><td colspan="4">SIFS = 9 µs for all priorities
Slot Time = 20 µs (default) for all priorities
AIFS [2]
Wmin [0] = 2 slots
WMax = 8 slots
Short = 9µs
Long =20µs 10µs Short = 28µs
Long = 50µs Short = 15
Long = 31 1023</td></tr>
</table>

5.5 Results and Discussion

The main motivation for designing PAC is to provide certain QoS guarantees for Class 1 (lifesaving) emergency nodes of MP-EDCA in a dense emergency where numerous nodes report an emergency. To study the performance of PAC, QoS parameters, such as average network MAC delay, average MAC delay of class 1 (risk to life) traffic, data drop ratio, packet retransmission and average throughput were measured. The WLAN performance measurement metrics are defined in Chapter 4 (Section 4.7).

5.5.1 Network MAC Delay

Figure 5.4 exhibits the average network MAC delay for the proposed PAC-MP-EDCA compared with MP_EDCA and the standard EDCA. As shown in the figures, the MAC delay remains the same and very low for all three considered schemes up to 25 nodes. When the number of nodes increases from 25 to 60, the MAC delay for EDCA sharply increases up to 0.067 seconds (4.02 ms), while it remains low for both PAC-MP-EDCA and MP-EDCA schemes. EDCA delay increases due to the increased collision since all nodes have the same priority and thus the contention is high. The effectiveness of the proposed PAC-MP-EDCA is shown in **Figure 5.5**. On examing Fig. 5.5 closely, it can be observed that both schemes offer the same MAC delay up to 44 nodes. However, when the number of nodes keeps increases (from 45 nodes onwards), MP-EDCA delay increases accordingly, since it does not provide prioritisation of lifesaving emergency nodes. The effectiveness of PAC is remarkable for an increased number of nodes (from 45 nodes onwards) where the MAC delay is not affected by the increased network load/number of nodes for lifesaving emergency nodes. Thus, based on the simulation results, it can be confirmed that WLAN technologies could be used for emergency traffic provided that the existing MAC protocol admission control implements the proposed PAC scheme.

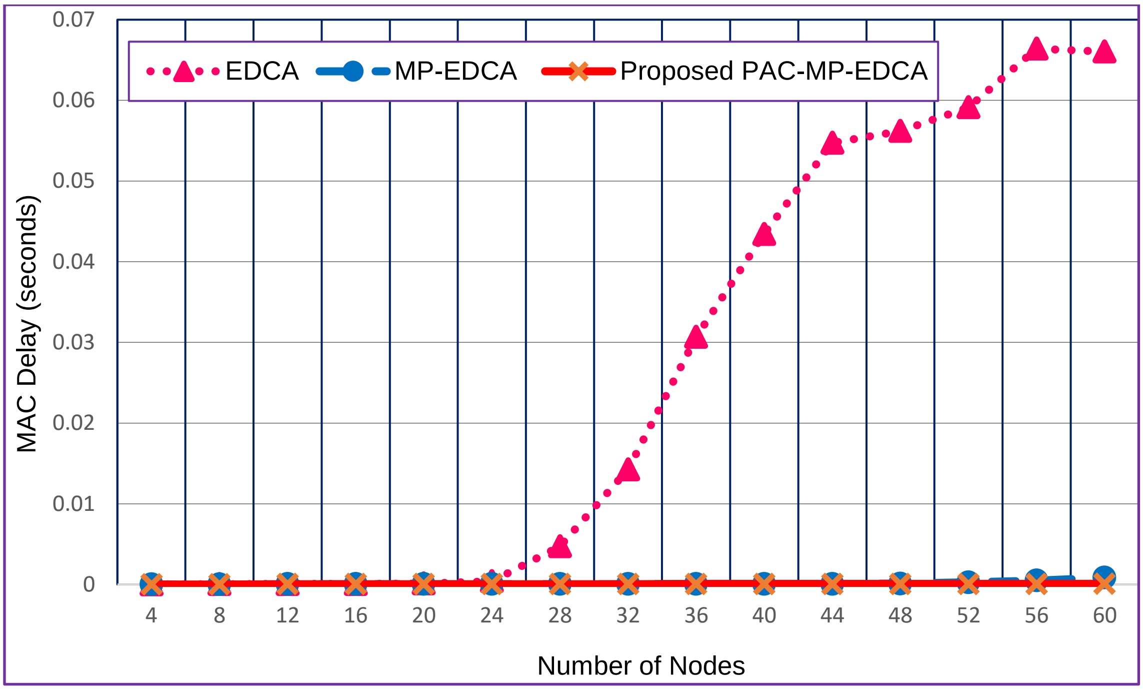

Figure 5.4: Network MAC delay. Comparison of EDCA, MP-EDCA, and the proposed PAC-MP-EDCA protocols.

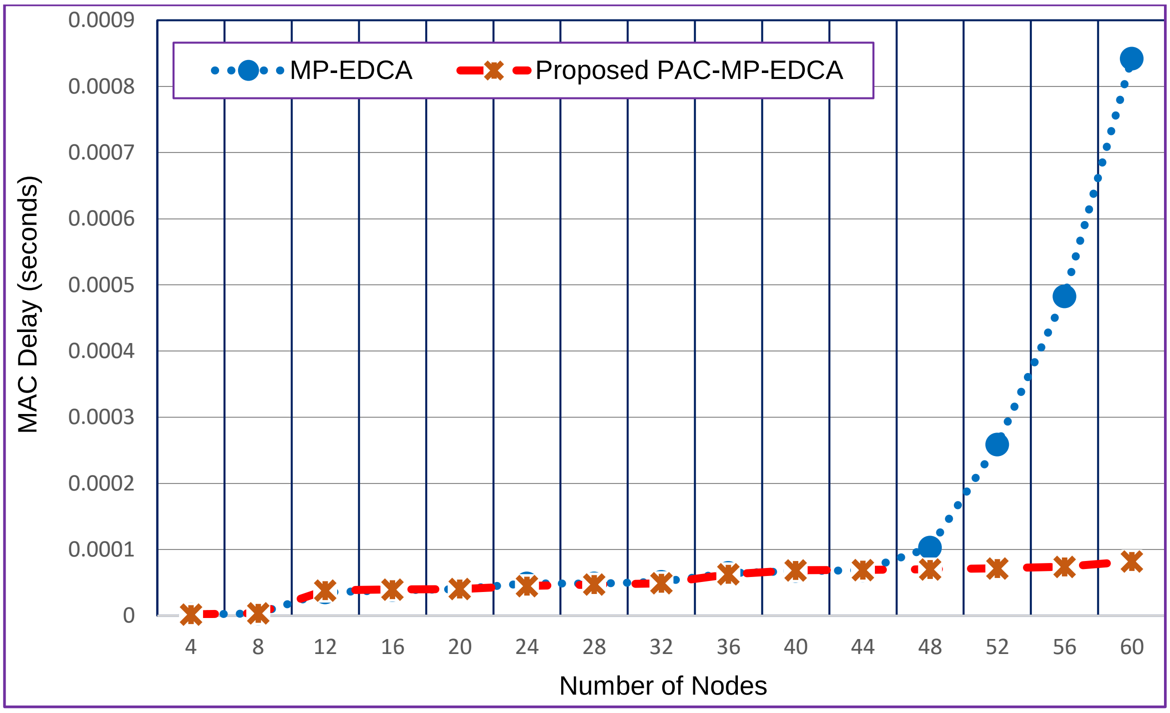

Figure 5.5: This diagram is redrawn by expanding Fig. 5.4 for clear illustration of MAC delay of PAC-MP-EDCA and MP-EDCA

5.5.2 Average MAC Delay of Risk to Life Emergency Traffic

Figure 5.6 depicts the simulation results of the MAC delay performance of the average risk to life nodes for the considered MAC protocols at the various number of nodes. The delay remains very low and the same for three schemes up to 20 nodes. Similar to network MAC delay, the delay for EDCA increases exponentially up to 0.04 sec (2.4 ms) from 20 nodes up to the end of the simulation. Delays for both MP-EDCA and PAC-MP-EDCA remain constant and the same from 20 nodes to 40 nodes. The key contribution of the proposed PAC-MP-EDCA is well identified with an increased number of nodes, from 40 nodes to 60 nodes where the delay for PAC remains very low and constant compared with MP-EDCA delay which increases from 0.1 ms at node 40 nodes up to 1.1 ms at 60 nodes. **Figure 5.7** compares the node MAC delay achieved for both MP-EDCA and PAC-MP-EDCA. The proposed PAC achieved up to 98 % and 10% lower MAC delay over the standard EDCA and MP-EDCA schemes, respectively. Generally, PAC offers very low and constant node MAC delay regardless of the increase in the number of nodes.

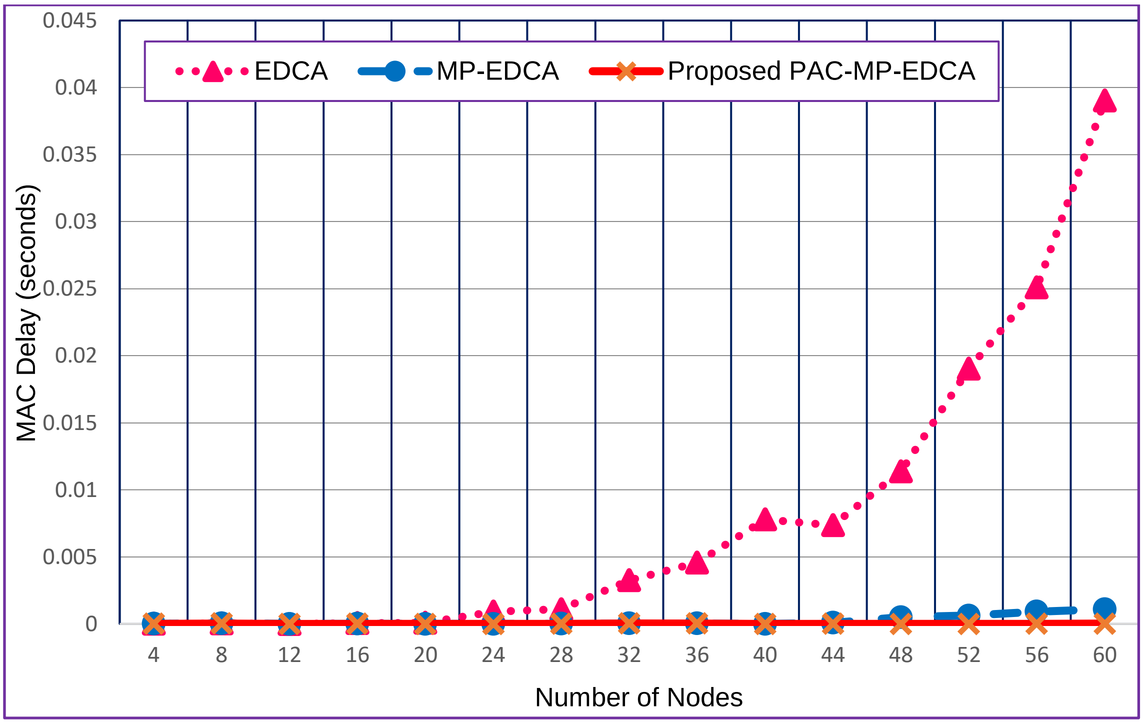

Figure 5.6: Average MAC delay of class 1 (risk-to-life) emergency nodes. Comparison of the EDCA, MP-EDCA, and proposed PAC-MP-EDCA.

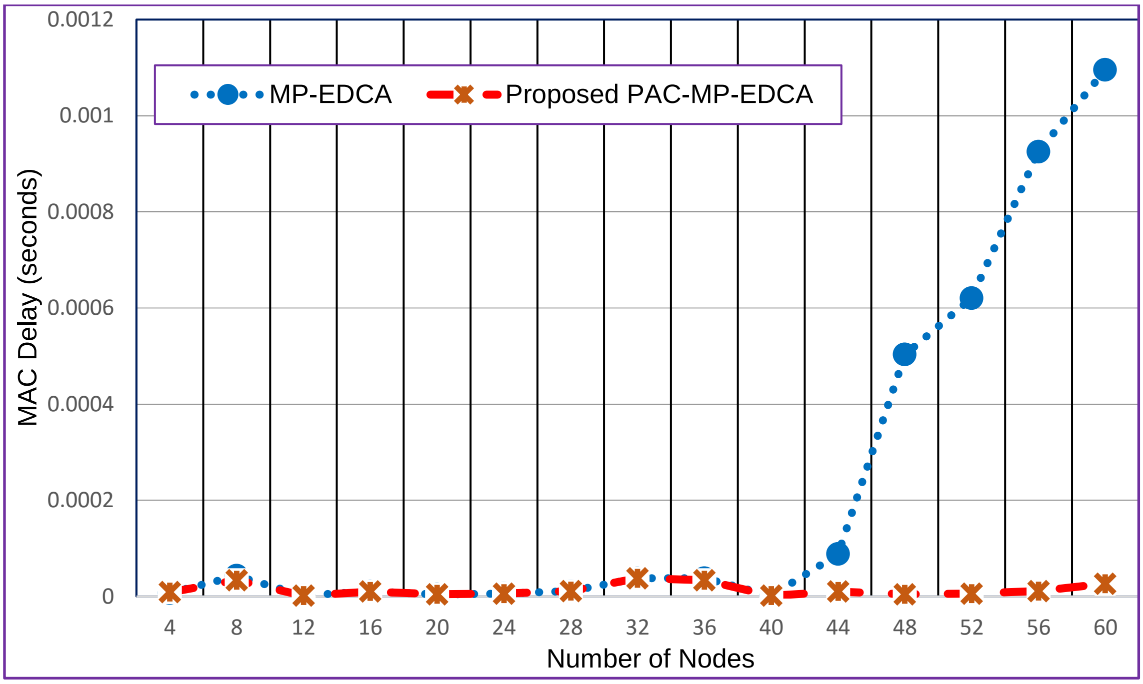

Figure 5.7: This diagram is redrawn by expanding Fig. 5.6 for clear illustration of MAC delay of PAC-MP-EDCA (class 1) risk-to-life emergency nodes.

5.5.3 Packet Retransmission

Figure 5.8 shows the number of retransmitted packets for the three MAC protocols considered in the simulation. The proposed PAC-MP-EDCA improves the MAC packet retransmission efficiency by reducing the number of retransmissions attempts required in packet recover the losses. It can be observed that the number of retransmitted packets increases with the increase in the number of nodes for all schemes. The PAC-MP-EDCA achieved 80% and 20% lower retransmitted packets over the standard EDCA and MP-EDCA schemes, respectively. Therefore, the proposed PAC-MP-EDCA scheme can be used in wireless networks to achieve efficient retransmission.

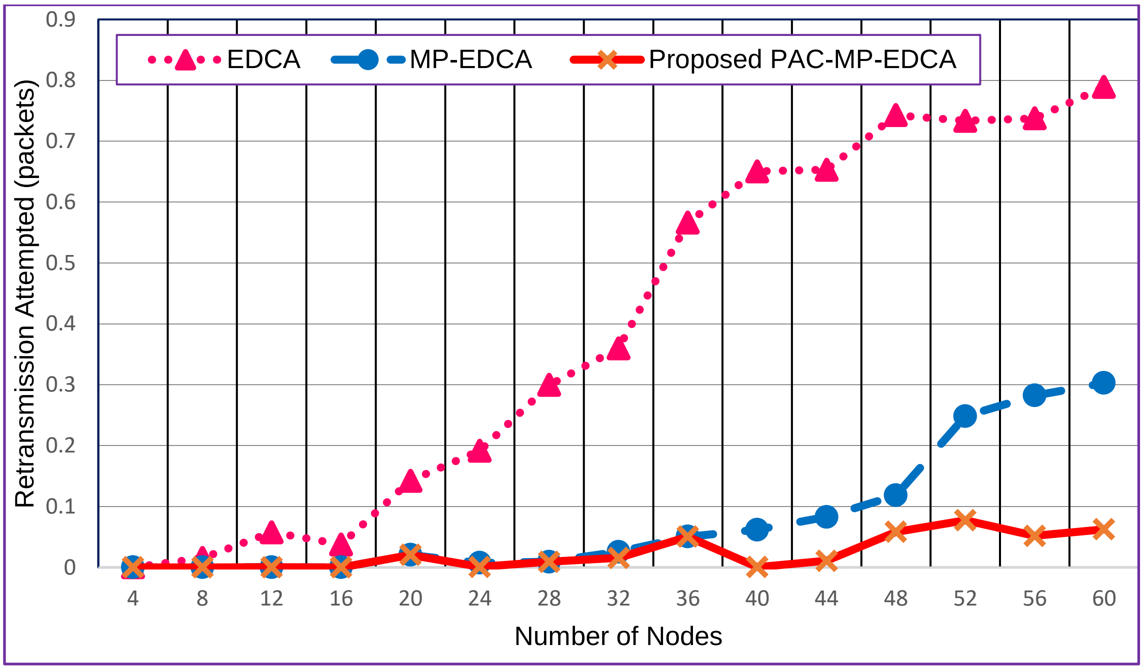

Figure 5.8: Packets retransmission attempts. Comparison of EDCA, MP-EDCA and the proposed PAC-MP-EDCA.

5.5.4 Average Throughput

Figure 5.9 exhibits the comparative average of the average user throughput for a variable number of nodes. The graphs in Fig. 5.9 shows that the proposed PAC-MP-EDCA offers improved throughput up to 9 Mbps, while the lowest value is attributed to the standard EDCA that provides up to 7 Mbps for 60 nodes. Generally, all three protocols provide equal throughput for small number of nodes (up to 25 nodes). This is because with fewer nodes, there is no network congestion. The main contribution of the proposed PAC-MP-EDCA scheme is that it can support a larger number of nodes with traffic generated by lifesaving nodes prioritised. The proposed PAC achieved up to 22% and 12% higher throughput than the standard EDCA and MP-EDCA, respectively. Significantly, the key difference between these protocols is noticed for an increased number of nodes. Thus, the proposed PAC is needed for improving the user throughput for prioritised traffic in real-world applications.

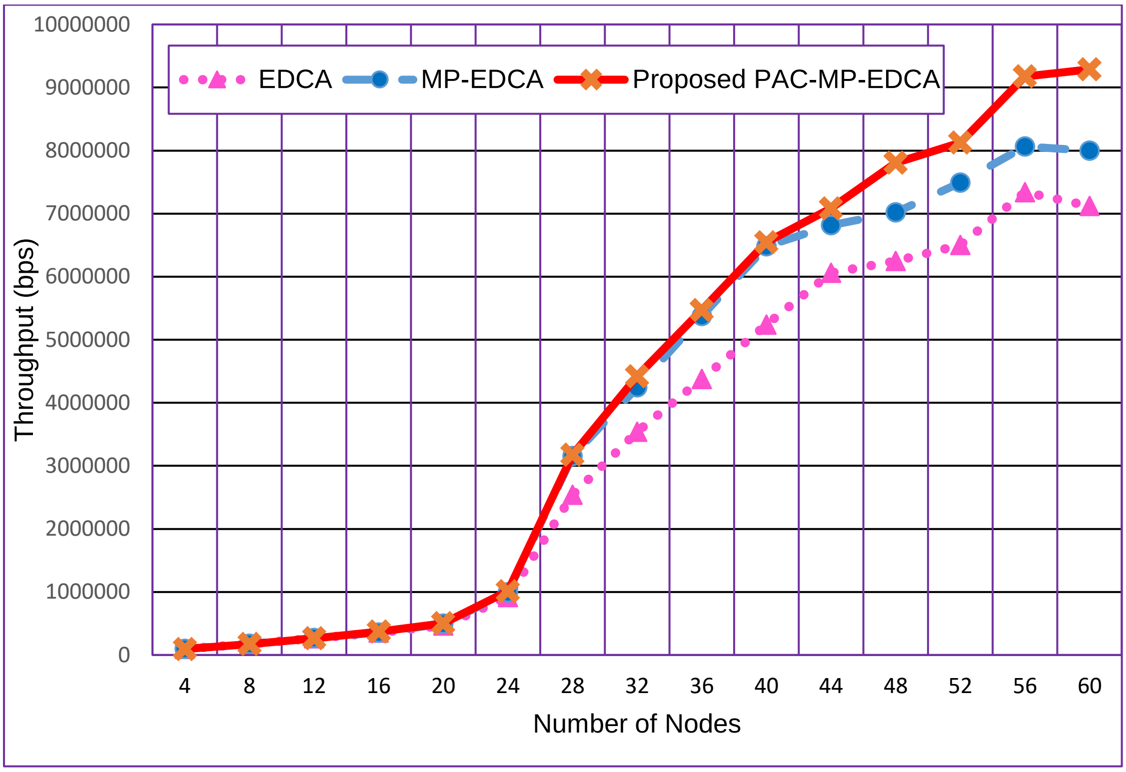

Figure 5.9: Average throughput Comparison of EDCA, MP-EDCA and the proposed PAC-MP-EDCA.

5.6 Strengths and Weaknesses

The main contribution and strength of PAC are to address the performance degradation issue and assure a strict QoS guarantee for emergency traffic specifically lifesaving emergency in the dense emergency where a high number of nodes report the emergency. Therefore, this chapter proposes a PAC protocol. PAC enhances the capabilities of the MP-EDCA protocol and addresses the performance degradation issue when the network traffic load increases from low to high. Moreover, PAC protects the high priority lifesaving emergency ongoing traffic flow from the upcoming same high priority or low priority flows. Further, PAC assures the QoS guarantee to lifesaving emergency traffic in a saturated emergency situation where a high number of nodes report an emergency. The proposed admission control scheme is based on the preemptive approach and network capacity analysis mechanism. Therefore, maximum number of lifesaving emergency are admitted in the network. Moreover, the proposed scheme is simple, energency efficient and can easily be implemented by modifying the existing 802.11 (EDCA).

EDCA, MP-EDCA and PAC-MP-EDCA were implemented and tested in the Riverbed simulation environment. We contributed code (written in C++) to Riverbed Modeler by creating new node and process models.

There is a trade-off between exiting lifesaving traffic streams and upcoming lifesaving traffic streams. To provide the QoS guarantee to existing lifesaving traffic streams, admittance is limited to other upcoming lifesaving traffic streams. Moreover, the process of enabling admission control may provide the QoS guarantee but increase the overhead.

5.7 Implementation Aspects of PAC-MP-EDCA

Recall the disaster situation and implementation aspects of MP-EDCA discussed in Section 4.10. In the disaster situation, first responders protect human life, save property and protect the environment [127]. First responders (relief workers) need reliable communication during dense emergency situations to save human life. For saving human life, first responders need resources, which are with the central coordinator node as shown in Fig. 5.1. Therefore, they need effective communication with central coordinator node. In certain scenarios, a high number of nodes (first responders) might have lifesaving emergency traffic and would want to communicate with a central coordinator node for resources. In such a scenario, the performance of a network may be degraded when a high number of nodes with lifesaving emergency traffic communicate with a central coordinator node.

In such a situation, the deployment of PAC-MP-EDCA could address this issue. The PAC may be dynamically activated at the central coordinator node in the dense emergency situation, such as a disaster. The PAC-MP-EDCA enabled central coordinator will admit the nodes with risk to life traffic based on the available network capacity. Moreover, all the nodes with risk to life priority by default preempt the low priority emergency traffic owing to the inherent MP-EDCA support.

When planning for deployment of WLANs, system planners can consider PAC-MP-EDCA to support emergency traffic where lifesaving emergency traffic has the highest channel access priority. PAC-MP-EDCA is most useful in a situation where there is at least one central node that can handle admission control.

5.8 Summary

In this chapter, a PAC-MP-EDCA protocol is proposed and reported. The PAC extends the capabilities of the original 802.11e and MP-EDCA. The PAC provides a strict QoS guarantee to MP-EDCA's class 1 (lifesaving) emergency traffic under saturated network conditions. The PAC provides a strict QoS guarantee together with immediate channel access privilege to high priority emergency traffic in a saturated emergency without much starvation in the network, which is significant QoS improvement over 802.11e (EDCA) and its variants, CP-EDCA and MP-EDCA.

The performance of PAC-MP-EDCA, MP-EDCA, and EDCA were compared in extensive simulation experiments. The simulation results showed that PAC-MP-EDCA achieved up to 88% lower MAC delays (network-wide), about 99% lower MAC delays for risk-to-life emergency, 73% lower packet retransmitted and 15% higher throughput than MP-EDCA for N >= 60 nodes. The PAC-MP-EDCA provides significant performance improvement over EDCA and MP-EDCA. PAC-MP-EDCA assures a strict QoS guarantee to lifesaving emergency traffic under high network traffic loads where a high number of nodes report an emergency. However, nodes with risk to lifesaving emergency traffic may not be admitted if the network has no capacity.

In PAC-MP-EDCA, admission control based on the network capacity analysis introduced. The PAC-MP-EDCA also incorporates the MP-EDCA's capability, that is, gives highest priority to lifesaving emergency traffic and allow high priority emergency traffic to preempt any low priority emergency (health, property and environment) traffic. Next, in Chapter 6, achieving a better QoS for emergency traffic by redesigning frame aggregation with a simple block acknowledgement (FASBA) scheme is reported.

Chapter 6

Redesigning Frame Aggregation and BlockAck to Enhance QoS Guarantee for Emergency Traffic in WLANs

6.1 Introduction

In Chapter 5, a novel preemptive admission control protocol was proposed to provide a QoS guarantee in WLANs. The primary objective of this thesis is to develop a framework that supports emergency traffic and provide strict QoS for emergency traffic in WLANs. To achieve the objectives, frame aggregation with simple BlockAck schemes are redesigned and termed, FASBA. The FASBA enhances the capabilities of MP-EDCA protocol (Chapter 5), provides assurances of service delivery, enhance the throughput, reduce MAC transmission overheads and ultimately larger number of emergency nodes supported in the network.

Many researchers [94, 96, 101, 103] investigated frame aggregation to enhance throughput performance and reduce MAC transmission overheads. However, these schemes work on UDP traffic and may not provide a guarantee of service delivery. Moreover, these schemes use either smaller block size which increases the transmission overheads or larger block size which may increase the error rate and results in a delay for time-sensitive applications [96, 97]. Furthermore, IEEE 802.11e introduced BlockAck scheme, which is now a compulsory part of IEEE 802.11n high throughput devices [25]. However, recent results show that BlockAck enhances the throughput performance at the cost of resequencing delay at the receiving buffer [44].

Many network researchers investigated frame aggregating and BA schemes to enhance throughput performance. Most of the frame aggregation methods and BlockAck schemes are complex, or they only use an ideal environment (error-free channel) and work under low traffic load. To overcome these performance problems, this chapter proposes an extension to MP-EDCA (Chapter 4) called frame aggregation with simple block acknowledgement (FASBA) which was developed through minor modifications of EDCA [126]. The proposed scheme is suitable for traffic (such as emergency traffic) which required service delivery guarantee under medium to high traffic load.

The key network researchers and their main contributions in the area of wireless MAC protocol design and performance improvement by tuning TXOP, frame aggregation and BlockAck were identified and discussed in Chapter 2. In Section 6.2, previously related research on frame aggregation and block acknowledgement schemes are further reviewed. The proposed FASBA protocol's frame redesign strategy is discussed in Section 6.3. Section 6.4 evaluates FASBA and simulation results are presented in Section 6.5. The implementation aspect is discussed in Section 6.8 and the summary of the main findings in Section 6.9.

6.2 Previous Work on the Frame Aggregation and Block Acknowledgement

Many MAC schemes have been proposed by network researchers to enhance the throughput performance of the 802.11 MAC protocol by reducing protocol overhead. However, these schemes are based on aggregating frames, optimising block acknowledgement or adjusting transmit opportunity (TXOP). This section only recaps a selected set of literature (discussed in Subsection 3.3.4) that is indicative of the range of approaches used to incorporate emergency traffic in WLANs.

IEEE 802.11 does not perform well due to protocol overheads [39, 94]. For the performance optimization, 802.11e enhancement left these parameters open in the standard, for example, block size or BlockAck policies [95]. Network researchers have developed various techniques for enhancing the performance of 802.11 by reducing the overhead. Most of the proposed mechanisms modified TXOP, block size and BlockAck for improving the performance of IEEE 802.11e protocol. The small size of the block increases the communication overheads since each time STA needs to negotiation before transmitting the frame. To overcome the issue of the small size of the block, one can form a large frame by combining short packets in a flow. However, the larger block size may increase the error rate and results in a delay for real-time applications [96, 97]. Thus, Sarkar and Sowerby [68] proposed a new MAC protocol called buffer unit multiple access (BUMA). The proposed BUMA protocol reduces transmission overheads by applying the frame aggregation approach and achieves higher throughput. However, BUMA is only suitable for UDP applications and may not provide a guarantee of service delivery. Similarly, Saif, et al. [100] developed a MAC scheme called minimised header MAC service data unit (MSDU) aggregation scheme (mA-MSDU) for reducing the transmission overheads by aggregating MSDUs. This scheme optimized the subframe by minimizing the headers overhead. Furthermore, researchers in [93] proposed an Implicit Sequence Control (ISC) as subframes error controller that retransmits only the corrupted subframes. On the other hand, a two-level frame aggregation mechanism is suggested by combining A-MSDU and aggregate MAC protocol data unit (A-MPDU) schemes [96]. This scheme enhanced the performance of throughput and offered a reduced MAC delay. Both A-MSDU and A-MPDU are defined by IEEE 802.11n [54] standard for achieving higher throughput at the MAC layer. Although the new frames are smaller in size compared with legacy 802.11, they still have negative performance, especially when added with the small payload. Moreover, network performance is highly affected while transmitting the A-MSDUs due to lack of control subsequence frames and retransmission. Implementation of IEEE 802.11n do not aggregate MPDU for voice traffic due to its specific end-to-end delay requirements. Seytnazarov and Kim [104] identified that the performance of the network is highly degraded in saturated traffic condition when multiple nodes access the medium for transmitting voice traffic. Authors proposed a QoS aware adaptive A-MPDU aggregation scheme (QAA-MPDU). The QAA-MPDU scheme optimizes throughput performance by aggregating MPDU for voice traffic and reducing protocol overhead. Liu, et al. [105] developed adaptive A-MPDU MAC scheme.

Hazra and De [99] developed a frame concatenation with block acknowledgement for providing QoS guarantee for time-sensitive applications. However, the proposed scheme is only suitable for the client-server application. To provide fairness and enhancing the performance of EDCA, Kim and Cho [102] proposed an Adaptive TXOP Allocation (ATA) scheme. In ATA scheme, stations adjust the TXOP interval based on traffic load and delay bound required by the application. The TXOP interval is increased in two steps: First, STA increases its TXOP to satisfy the QoS guarantee required by its packet queue. Second, when the traffic load is low.

For reliable communication, the receiving station acknowledges each and every received packet. However, this mechanism decreased the overall network performance due to an increasing number of acknowledgement packets. As the solution, researchers proposed various approaches utilizing and optimizing block acknowledgement Cabral, et al. [98]. The Optimized block acknowledgement (O-BlockAck) developed in Cabral, et al. [98]] reduces the delay and increase the number of users within the network. O-BlockAck scheme uses single service and a mixture of services used by the node. The empirical results have shown that fragment size 12 is more appropriate for a mixture of services and supported users may be increased from 30 to 35within a network. One more mechanism for improving the EDCA scheme is called holding time aggregation (HTA) developed by Azevêdo Filho, et al. [101]. In HTA, each STA calculates the amount of time a packet takes for its journey and the time an application may tolerate the delay. However, the proposed HTA scheme is only suitable for UDP Applications.

6.3 Redesigning Frame Aggregation and Block Acknowledgement Schemes

The proposed FASBA scheme described in this chapter differs from the earlier work described in Section 6.2. It has different goals and capabilities. First, the main objective of the proposed FASBA scheme to accommodate more number of emergency nodes. This objective is achieved by enhancing the WLAN throughput performance under medium to high traffic load and reducing transmission overhead. Secondly, provide QoS guarantee in terms of message delivery. These objectives of FASBA are achieved by aggregating frames and implementing Simple BlockAck mechanism. The FASBA extends BUMA[94] by incorporating the idea of frame-aggregation for reducing protocol's transmission overhead. Moreover, FASBA employs a simple 2-bit BlockAck strategy which will increase the number of nodes in the network and provides QoS message delivery.

In each FASBA enabled STA, a buffer (temporary memory) is used to combines and hold three (3) packets with single packet header and trailer at the MAC layer before transmission for reducing transmission overheads and optimizing the performance. **Figure 6.1** illustrates the FASBA's frame aggregation mechanism. The figure also shows the acknowledgement mechanism followed by SIFS.

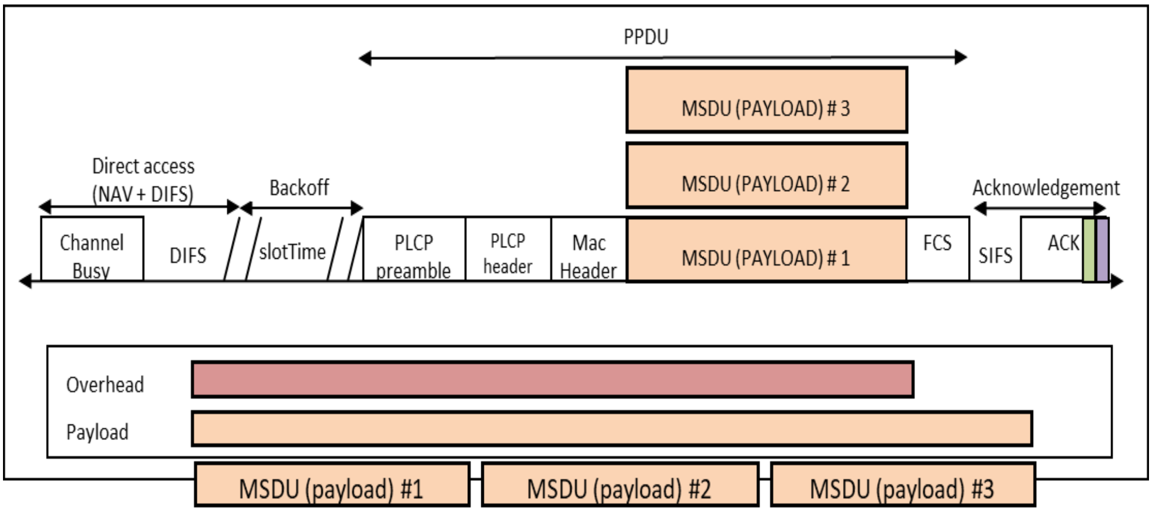

Figure 6.1: FASBA frame aggregation of three packets with two-bit acknowledgement.

The FASBA's simple block acknowledgement mechanism is illustrated in Table 6.1. The first column shows the two bits of acknowledgement, followed by purpose and next possible bits which will be sent by the STA. If both Ack bits are 11, means all three packets (i.e. packet 1, packet 2, and packet 3) are successfully delivered. The transmitting STA will send next three packets (i.e. packet 4, packet 5, and packet 6). If Ack bits are 01, means packet 2 and packet 3 are transmitted successfully. The transmitting STA will send packet 1, 4, and 5. Similarly, if Ack bits are 10, means packets 1, and packet 2 are delivered successfully and STA will send packet 3, 4, and 5. In all other cases, all three packets will be resent.

Table 6.1: Proposed FASBA's simple 2-bit BlockAck mechanism.

Two bits	Purpose	Next Packets)
11	All frame/packet received successfully. Transmit another one.	4, 5, and 6
01	Only resend packet 1, (packet # 2 and #3 received successfully).	1, 4, and 5
10	Only resend packet 3, (packet # 1 and #2 received successfully)	3, 4, and 5
00 / None	Resend (all three packets).	1, 2, and 3

6.4 Performance evaluating of the proposed FASBA Scheme

In this section, the performance of FASBA is evaluated by quantitative stochastic simulation. FASBA's performance is compared with that of EDCA. The FASBA protocol was evaluated by measuring parameters such as throughput, packet delay, packet drop ratio and retransmission attempts.

6.4.1 Simulation Environment and Parameters

To evaluate the performance of FASBA, network simulator Riverbed Modeler and MATLAB were used for the simulation study. In Riverbed Modeler, total 30 scenarios were created, 15 of each FASBA, and MP-EDCA. Table 6.2 shows the MAC parameters used in the simulations. To implement the frame concatenation as shown in Fig. 6.1, a new data frame is developed with the reserve type field of 11 and subtype value of 1000 of the frame control field of MAC frame structure.

A new simple 2-bit BlockAck request and response frames are created by customising the 802.11 EDCA frames in Riverbed Modeler. The node, network and process models of Riverbed Modeler were customised. The 802.11 WLAN MAC packet formats may be categorized into three types i.e. (1) Management, (2) Control, and (3) Data packets. For implementing FABA in Riverbed Modeler, Type of MAC data (shown in Fig. 6.2) and BlockAck of control packets (shown in Fig. 6.3) are modified. The type bits of WLAN data packet are used for identifying the packet sequence. And only four bits out of 32 bits of BlockAck field of control packs were used for sending the acknowledgement.

Moreover, EDCA's MAC model was also customised to implement the BlockAck request and BlockAck frames. The activation of FASBA is through the same activation process used in the EDCA, that is adding block acknowledgement (ADDBA) frame.

The FASBA's implementation mechanism frame-aggregation with block-acknowledgement maintain the backward compatibility with the existing DCF and EDCA MAC protocols.

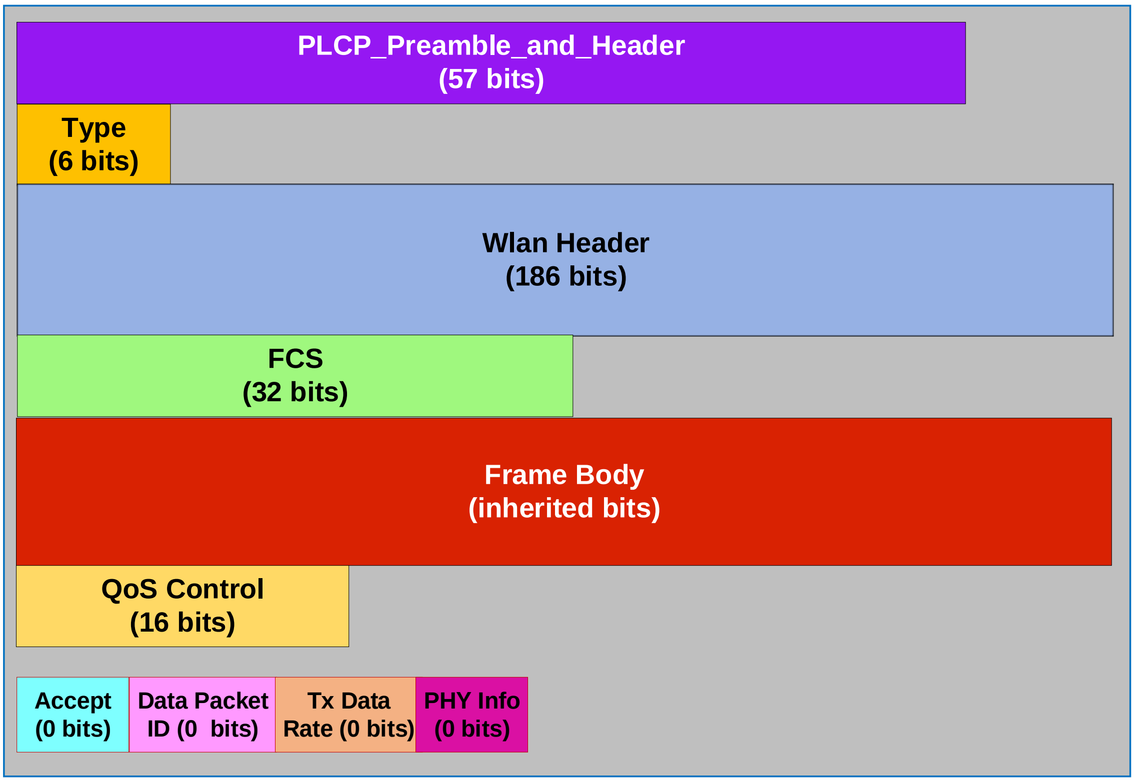

Figure 6.2: FASBA's data packet format.

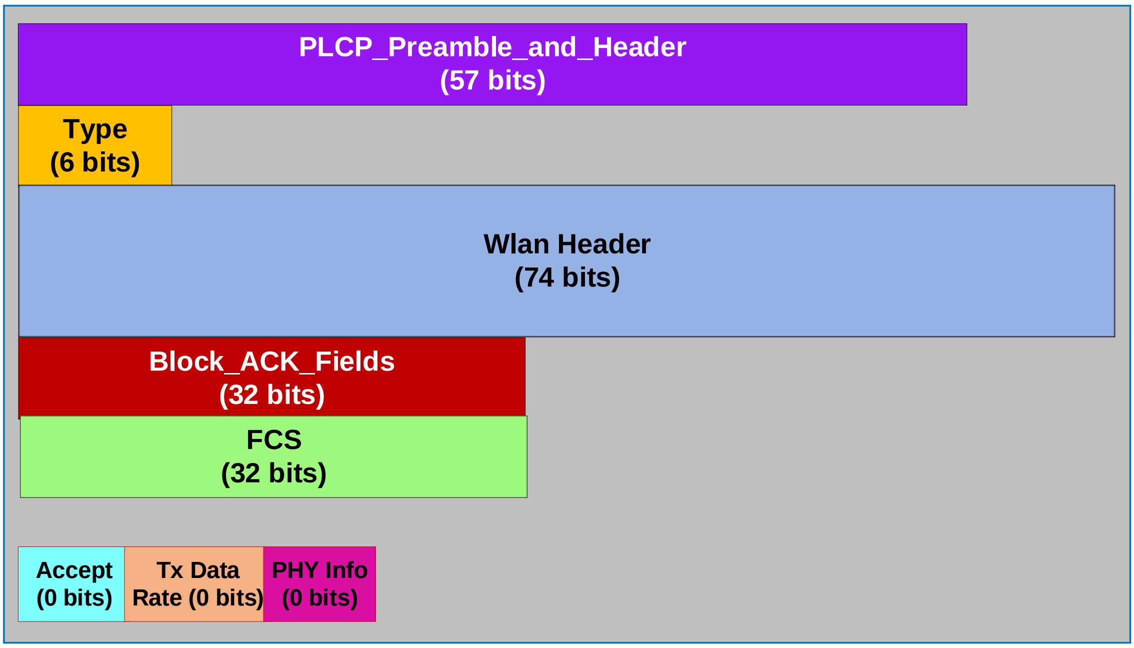

Figure 6.3: FASBA's control packet format.

Table 6.2: MAC parameters used in simulation.

<table>
<tr><td>General Parameters</td><td colspan="4">Data rate = 65Mbps (base)/600 Mbps (max)
Protocol = IEEE 802.11n
Number of MP-EDCA nodes: 4 - 60
Number of FASBA nodes: 4 – 60
Application: data (text message of 150 characters).
TXOP limit = 0 ms</td></tr>
<tr><td rowspan="3">Contention Parameters</td><td colspan="4">MP-EDCA and FASBA</td></tr>
<tr><td>Risk to Life (RtoL) Priority Nodes</td><td>Risk to Health (RtoH) Priority Nodes</td><td>Risk to Property (RtoP) Priority Nodes</td><td>Risk to Environment (RtoE) Priority Nodes</td></tr>
<tr><td>RtoLSIFS = 10
RtoLSlotTime = 25
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td><td>RtoHSIFS = 25
RtoHSlotTime = 40
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td><td>RtoPSIFS = 40
RtoSIFS = 55
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td><td>RtoPSIFS = 55
RtoESlotTime = 70
AIFS [0] = 1 slot
WMin[0] = 2 slots
WMax[8] = 8 slots</td></tr>
</table>

6.5 Simulation Results and Discussion

For both individual stations and the overall network, three important network performance metrics are used i.e. (1) throughput, (2) packet delay, (3) packet drop ratio (packet loss). These performance metrics were defined in the Chapter 4 (section 4.7).

6.5.1 Throughput Performance

The network throughput versus active nodes of FASBA and MP-EDCA for an ad hoc and infrastructure network is exhibit in Fig. 6.4 and Fig. 6.5 respectively. One can observe that FASBA provides higher throughput than EDCA irrespective of network architecture, especially under medium to high traffic. For example, Fig. 6.4 compares average network throughput (ad hoc network) for N = 4 to 60 nodes. It is found that FASBA offers an improved network throughput up to 10 Mbps for 60 notes. One can observe that both MP-EDCA and FASBA provide similar throughput performance for N = 4 to 36 Nodes. For 40 to 60, FASBA performs much better than MP-EDCA. For example, the proposed FASBA scheme achieved about 15% higher throughput than the standard MP-EDCA at N= 60 nodes.

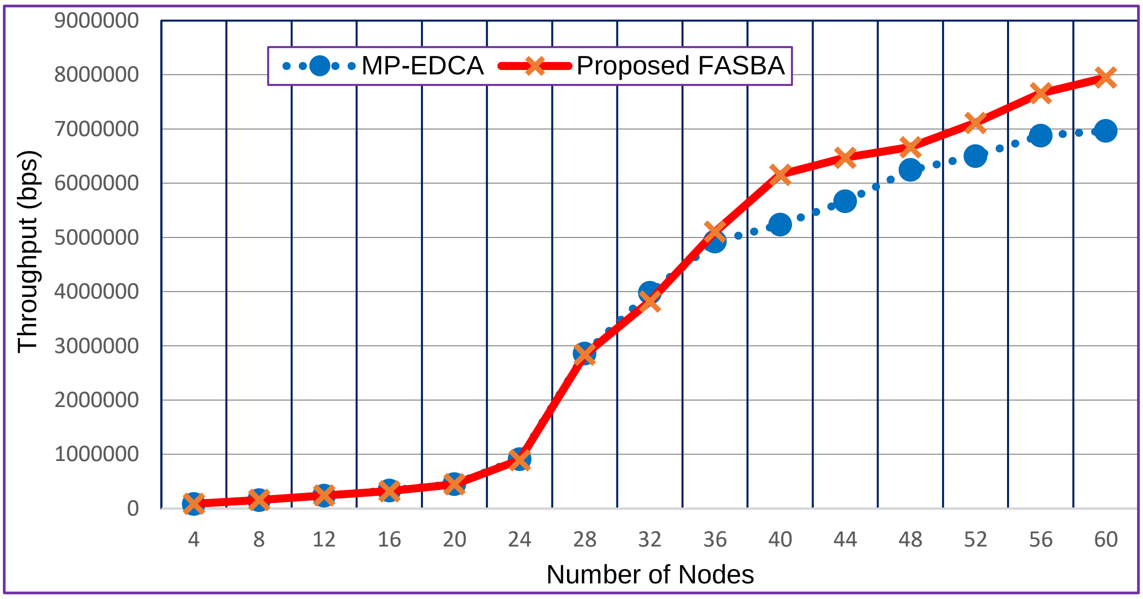

Figure 6.4: Average ad hoc network throughput performance of MP-EDCA, and proposed FASBA schemes.

Figure 6.5 exhibits the comparative average network throughput of an infrastructure network. The graphs are shown in Fig. 6.5 illustrate that the proposed FASBA offers an improved network throughput up to 15 Mbps for 60 notes. Similar to the ad hoc network 6.4(a), both schemes (MP-EDCA and FASBA) provides equal throughput for the number of nodes up to 28. While adding the nodes from 32 to 60, FASBA outperforms MP-EDCA. As shown in the graphs, FASBA achieves up to 17.5 % higher throughput than the standard MP-EDCA. Moreover, one can notice that the average throughput of both i.e., infrastructure and ad hoc networks constanty increases when the number of nodes are increased.

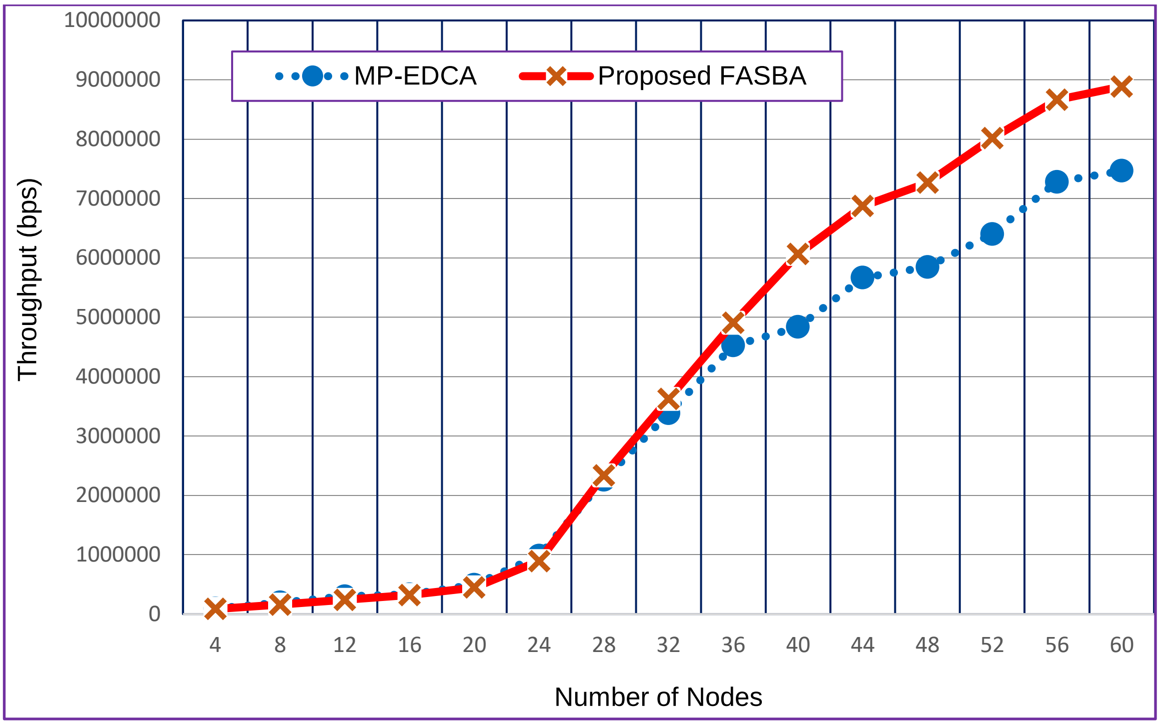

Figure 6.5: Average infrastructure network throughput performance of MP-EDCA, and proposed FASBA.

6.5.2 MAC Delay

The average network-wide MAC delay of FASBA and MP-EDCA for N = 60 stations in ad hoc network is shown in Fig. 6.6. One can observe that FASBA outperforms EDCA in delay performance when the network load is increased from node N = 24 to 60. For example, FASBA's mean packet delay is about 30% lower than MP-EDCA's in the network with N=60 nodes.

The emergency traffic and other time-sensitive applications are delay sensitive. It is found that FASBA may manage up to 32 emergency nodes. Another side, MP-EDCA can manage 24 nodes. It is observed that FASBA's mean packet delay is lower than MP-EDCA in both ad hoc and infrastructure network environment.

The main conclusion that can be drawn from Fig. 6.6 that nodes using FASBA have a substantially lower mean packet delay than the nodes using MP-EDCA, especially under medium to high traffic load.

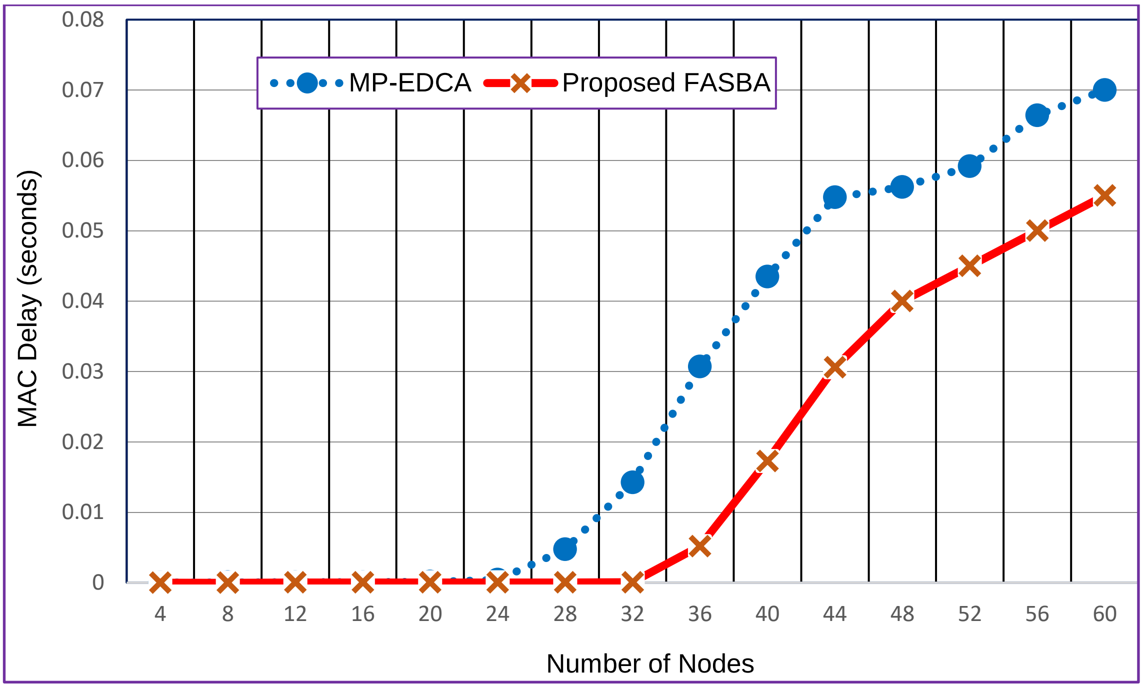

Figure 6.6: Average network-wide MAC delay. Comparison of MP-EDCA, and the proposed FASBA.

6.5.3 Packet Retransmission

Figure 6.7 exhibits the number of retransmitted packets for the two MAC protocols considered in the simulation. As it can be seen from the figure, the proposed FASBA protocol improves the retransmission of MAC by reducing the retransmissions attempts. If you look closely to the Fig. 6.7, one can notice that the number of retransmitted packets increases with the increase in the number of nodes for both schemes. The proposed FASBA achieved 60% lower re-transmitted packets over the standard MP-EDCA. This is achieved by optimisation of block acknowledgement mechanism. The proposed FASBA scheme can be used in wireless networks to achieve efficient retransmission.

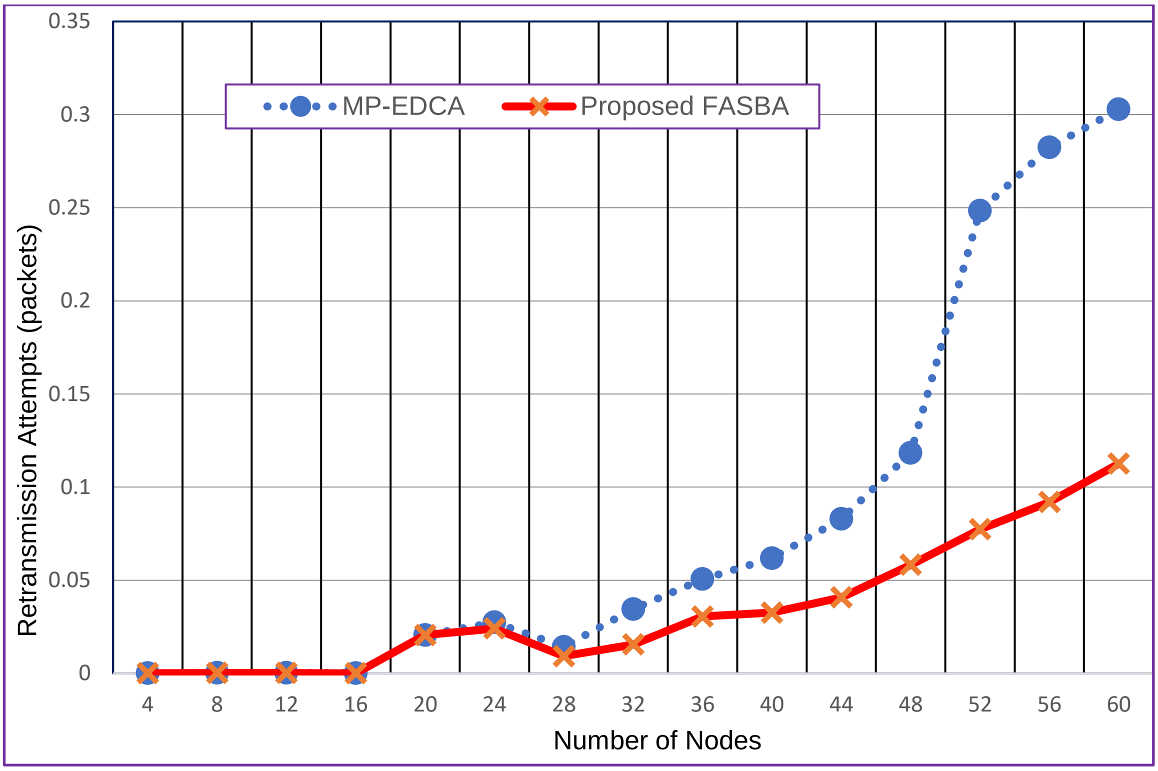

Figure 6.7: Average packets retransmission attempts against the number of nodes. Comparison of MP-EDCA, and FASBA.

6.6 Validation of Riverbed Simulation Results using MATLAB

To validate simulation models and results, we used the approach discussed in Section 3.6. In addition, to compare our FASBA's simulation results with an already implemented model of MP-EDCA in Riverbed Modeler, we implement our proposed mechanism of FASBA's SimpleBlockAck in MATLAB. The implementation aspect is discussed below.

In the Matlab, We evaluate the performance of FASBA's frame aggregation mechanism with ACK and Simple BlockAck schemes. In ACK, all three packets are resent again. Another side, FASBA's simple block acknowledgement mechanism (see Table 6.2) is used. For implementing BlockAck, and FASBA's SimpleBlockAck in Matlab, a cell variable of user-defined length is created. The simulation is run until the cell variable is not emptied. Two arrays variables i.e. (1) new-bits, and (2) old-bits are used to move the data. Iterations are used to empty the cell. In each iteration, three bits (packets) are removed from the cell variable and added into the new "new-bits" variable. These bits and any other bits in the variable "old-bits" are assigned to the variable packet. In the

SimpleBlockAck, the probability of 0.1% is used. A bit (packet) is assumed to be lost based on the probability. The lost bit is stored in the old-bits variable. The final bits are sent by removing lost bits and are stored in the variable SimpleBlockAck. In the simulation, any lost bits by the system are identified and sent with the next packets data. Another side in ACK, all bits (packets) are sent again.

The simulation was carried out to demonstrate the effectiveness of the proposed algorithm. The bit stream length of 5000 was used and three bit are transferred at once from sending to the receiver with a probability of missing a bit was set to be at 10 percent (0.1). In the first set of experiment, when if a packet is lost while sending it to the receiver, the whole packet (all three bits) are sent again, the results are shown in the Figure B.1. It took 1844 iteration to send the completed bit stream. The second set of experiment was performed where only the missing bit is sent when any bit in the packet was lost. When the experiment was repeated with the same settings, the results are shown in Figure B.2. This time, the proposed algorithm took 1718 iterations to send the complete bit stream. The proposed algorithm has taken 126 less iterations to send a complete message, which is an improvement of 7.34%.

6.7 Strengths and Weaknesses

The main contribution and strength of FASBA are to improve the performance and provide assurance of service delivery. This chapter, therefore, proposes a frame aggregation with simple block acknowledgement (FASBA) protocol, FASBA an enhancement to MP-EDCA scheme that addresses the performance issue due to transmission overhead. FASBA provides better bandwidth utilization than MP-EDCA because it wastes less transmission capacity in the backoff state, and consequently achieves higher throughput, lower MAC delay, lower retransmission attempts, and lower packets drop ratio under medium to high traffic load. This improvement is due to FASBA's frame aggregation and simple two (2) bit block acknowledgement strategies to send a single header and trailer with transmitting multiple packets.

The results show that that under an error-prone environment, FASBA enhances throughput performance in both ad hoc or infrastructure networks, provides lower MAC delay and retransmission attempt. Ultimately, FASBA accommodates more number emergency nodes in the network. However, the performance of FASBA depend upon the length of the packet, and bit error rate. The FASBA performs better in lower packet length and higher bit error rate. Network under low traffic load, FASBA performs as good as DCF. However, results present in this chapter are based on optimistic network environment. However, burst errors would affect the throughput and delay performance.

6.8 Implementation Aspects of FASBA

In the emergency such as natural or manmade disaster where high number of nodes (first responders) report an emergency, the first priority of first responders is to save human life. For saving human life, they require effective communication in saturated network conditions. However, a network may not have the required capacity to accommodate all the RtoL nodes with real-time traffic. Thus, first responders may use short emergency text messages but there is no inherit support to prioritise emergency messages.

To overcome from the situation, FASBA may be used. FASBA extends the capabilities of MP-EDCA and prioritises lifesaving emergency traffic. Moreover, FASBA provides enhances the throughput performance, reduces MAC delay, and assures guarantee of service delivery.

The FASBA protocol is easy to implement and provides cost-effective solutions to improve the performance of 802.11 based WLANs. FASBA based devices require a random access memory (RAM) for holding the frames. A buffer may be created for frame aggregation and destroyed once frames are delivered. FASBA does not require any other hardware for implementation.

Generally, end-user devices are faster, have high power processor and ram. The FASBA’s frame formulating (i.e. aggregating frames) strategy is effective. The processing time for combing frames is negligible in the current era of high-speed end-user devices. The data frame and control frame format of 802.11 can be modified for implementing FASBA.

In the dense emergency situation, FASBA performs better where high number of nodes report emergency. Network under the low traffic, FASBA performs as better as DCF by sending one frame at a time.

6.9 Summary

In this chapter, a frame aggregation scheme together with a simple two-bit block acknowledgement scheme called FASBA was reported. The FASBA extends the capabilities of MP-EDCA. Therefore, FASBA has inherent emergency traffic support, that is, prioritise emergency traffic. Moreover, FASBA enhances the throughput performance, provide a guarantee of service delivery, accommodate an increased number of emergency nodes. The improvement in the FASBA's performance achieved by addressing the protocol transmission overheads incorporating frame aggregation with block acknowledgement schemes.

In FASBA, frames such as data frame and control frames are modified for achieving higher throughput, reducing frame queueing delay and providing a guarantee of service delivery under medium to high traffic load.

The performance of FASBA and MP-EDCA were compared by simulation experiments. The simulation results showed that FASBA reduces the transmission overhead, achieve higher throughput performance, reduce MAC delay, and accommodate more number of lifesaving emergency nodes in the network.

The simulation results showed that FASBA achieved up to average 14% higher throughput (ad hoc network), 17% higher throughput infrastructure networks, MAC delay is up to 22% lower, and average packet drop ratio is 60 % lower than MP-EDCA. The FASBA can provide better QoS to emergency nodes under high traffic conditions more effectively. Next, in Chapter 7, implications for system planning, conclusion and future development of this research are outlined.

Chapter 7

Conclusion and Future Directions

The thesis is concluded in Section 7.1, while the future research directions are presented in Section 7.2. This chapter also provides a discussion on the implications for system planning and deployed in Section 7.3.

7.1 Conclusion

This thesis focused on developing a MAC framework that supports emergency traffic by providing strict QoS guarantee. The usage of time-critical applications (such as emergency services) over the WLANs is increasing. Further, addressing the lack of inherent emergency traffic support and providing of strict QoS guarantee in distributed wireless MAC protocols were the main motivations of this research. In WLANs, supporting emergency traffic and providing QoS guarantee is very challenging owing to the current WLAN MAC layer that utilises a shared medium that doesn't define emergency traffic among its type of services. This increases noise interference, particularly for the overloaded network. While there are multiple parameters that may affect QoS performance of emergency traffic at the MAC layer level, short-inter-frame space (SIFS) and slot time were identified as the main factors. Other factors, such as admission control, frame aggregation and block acknowledgement also influence the performance of WLANs for emergency traffic. To meet the research aims, the organisation dealing with emergency services were studied. Generally, emergency organisations categorise the emergency traffic into four general types (i.e., emergency to life, health, property and environment) and the highest priority is given to emergencies related to life, followed by health, property and environment. To support these emergencies, traffic type over WLANs, SIFS and slot time were modified in this thesis. Moreover, to preserve the acceptable packet delay, the admission control for managing the administration of the emergency traffic was proposed. The proposed admission control module accepts or rejects the incoming session based on its priority and the available network resources. Further, to provide better QoS to emergency traffic, frame aggregation with simple block acknowledgement scheme was proposed. The proposed scheme reduces the MAC transmission overheads, enhances throughput performance and reduces the MAC delay.

This thesis has makes several original contributions, which are reported in Chapters 4 to 6. A summary of the contributions is outlined below. The MAC protocol is among the key factors that influence the performance of WLANs. The IEEE 802.11e working group enhanced the 802.11 MAC to provide QoS to time-sensitive applications in WLANs. However, the 802.11e (EDCA) standard has limitations and it neither supports emergency traffic nor provides a strict QoS guarantee. Therefore, this research focused on providing emergency traffic support and a strict QoS guarantee in WLANs.

To overcome these limitations, this thesis developed a MAC framework, which includes several new protocols. To support emergency traffic, a new protocol termed MP-EDCA **(Chapter 4)** was developed by modifying the existing 802.11e (EDCA) standard. To provide a strict QoS guarantee, a new MAC protocol termed PAC-MP-EDCA **(Chapter 5)** was developed and to serve emergency nodes better, FASBA protocol **(Chapter 6)** was developed.

In Chapter 4, an in-channel multiple service preemptive protocol termed MP-EDCA was discussed. The MP-EDCA extends the original 802.11e capabilities by accommodating emergency traffic in 802.11 networks. The proposed MP-EDCA provides immediate channel access privileges to high priority emergency traffic in distributed networks. The performance of MP-EDCA is compared with that of CP-EDCA and EDCA by extensive simulation experiments.

Performance metrics, such as average MAC delay, packet drop ratio, packet retransmission and throughput, were used to evaluate the performance. Empirical results showed that MP-EDCA offers a significant performance gain over CP-EDCA and EDCA. For example, MP-EDCA achieved 60% lower MAC delays (network-wide), about 99% lower MAC delays for risk-to-life emergency traffic, 75% lower packet drop ratio, up to 60% lower packet retransmitted than CP-EDCA and 20% higher throughput than CP-

EDCA. The MP-EDCA can provide a better QoS to emergency nodes under medium-to-high traffic conditions more effectively. Moreover, immediate channel access for lifesaving emergency traffic is guaranteed even in a saturated emergency if nodes for emergency exist. However, when all nodes are in ‘risk to life’ (an unusual case), MP-EDCA performs as well as the CP-EDCA.

In MP-EDCA, physical parameters such as SIFS and slot time, are modified in such a way that high priority emergency (lifesaving) traffic is given the highest priority, immediate channel access and the ability to preempt any low priority emergency (health, property and environment) traffic.

In Chapter 5, the provision of a QoS guarantee using admission control is investigated. To achieve this QoS guarantee, a PAC technique was introduced in the design fabrics of MP-EDCA and the resulting protocol was termed PAC-MP-EDCA (Chapter 5). The performance of PAC-MP-EDCA was compared with that of MP-EDCA by extensive simulations. The simulation results showed that PAC-MP-EDCA offers a significant performance gain over MP-EDCA. For example, PAC achieved 88% lower MAC delays (network-wide), about 99% lower MAC delays for risk-to-life emergency nodes, 73% lower packet retransmitted and 15% higher throughput than MP-EDCA when N >= 60.

The PAC-MP-EDCA provides a strict QoS guarantee to MP-EDCA’s class 1 (lifesaving) emergency traffic under saturated network conditions. The proposed system provides strict QoS guarantee together with immediate channel access privilege to high priority emergency traffic in a saturated emergency without much starvation in the network, which is significant QoS improve over 802.11e (EDCA) and its variants, CP-EDCA and MP-EDCA.

In the PAC-MP-EDCA, admission control based on capacity analysis together with a preemptive algorithm was developed for the central coordinator node. The admission control was modified in such a way that high priority emergency (lifesaving) traffic obtains the highest priority, immediate channel access and the ability to preempt any low priority emergency (health, property and environment) traffic.

In Chapter 6, to serve more emergency nodes in WLANs, the frame aggregation with a simple 2-bit BlockAck scheme (termed FASBA) for MP-EDCA was investigated. The

802.11(DCF) MAC protocol has a problem of transmission overheads which limits its performance.

To address this problem, many researchers investigated frame aggregation to enhance throughput performance and to reduce MAC transmission overheads. However, the schemes they proposed work on UDP traffic, neither provide assurance of service delivery nor prioritise emergency traffic. Moreover, these schemes use either a smaller block size, which increases the transmission overheads or a larger block size, which increases the error rate and result in a delay for time-sensitive applications. Further, IEEE 802.11e introduced BlockAck scheme. However, recent results show that BlockAck enhances the throughput performance at the cost of resequencing delay at the receiving buffer.

The proposed FASBA (Chapter 6) extends the capabilities of MP-EDCA by enhancing throughput performance. In FASBA, frames, including the data frame and control frames, are modified for achieving higher throughput, reducing frame queuing delays and providing a guarantee of service delivery under medium-to-high traffic load.

The performance of FASBA was evaluated through Riverbed Modeler simulation and was validated by MATLAB. The simulation results showed that FASBA reduces the transmission overhead, achieve higher throughput performance, reduces MAC delay and accommodate more number of lifesaving emergency nodes in the network. For example, FASBA achieved an average of up to 14% higher throughput (ad hoc network), 17% higher throughput infrastructure networks, 22% lower MA delay and 60% lower packet drop ratio as compare to MP-EDCA. The FASBA can provide better QoS to emergency nodes under high traffic conditions more effectively.

In this thesis, the extensive simulation experiments have been performed in Riverbed Modeler. The Riverbed Modeler was chosen because of its popularity. It has wireless suit required to model the wireless network and evaluate the network performance. Moreover, it has capability to evaluate the network performance using node mobility and channel fading. Riverbed Modeler was also used for designing models and evaluating the performance of the proposed MAC protocols. For producing a credible result, it is important to validate the simulation model and make sure that simulation parameters are configured correctly. One of the validating approaches is to compare the results of implemented simulation model with the results of already implemented (valid) models.

Therefore, MP-EDCA is evaluated by comparing the simulation results with the other two related protocols: Balakrishnan's CP-EDCA and an already implemented a simulation model of EDCA. Similarly, the performance of PAC (Chapter 5) is verified against the MP-EDCA and EDCA. Finally, the performance of FASBA (presented in Chapter 6) is tested against the MP-EDCA. However, the performances of the proposed MAC schemes depend on various factors such as network load, noise, node mobility, distance between sender and receiver, and channel fading. Therefore, it is recommended for future work to test the performance of the proposed MAC protocol under the realistic environment.

7.2 Future Research Directions

This thesis provides a WLAN MAC framework for supporting emergency traffic under the dense emergency situation (disaster) where high number nodes report an emergency. The aim was to answer the research question "How emergency traffic can be supported in WLANs under medium to high traffic load?" and "How can strict QoS guarantee be provided to the time-sensitive application in WLANs under medium to high traffic load?". This section highlights some research issues that could be investigated for the future extension of this research.

- **Testbed implementation of MP-EDCA**

  In this thesis, a novel MAC protocol called MP-EDCA for supporting emergency traffic was reported in Chapter 4. A significant network performance gain with respect to lower delays for lifesaving emergency traffic is obtained with MP-EDCA under medium to high traffic loads. The performance of MP-EDCA was tested by performing the extensive simulation. The simulation results were verified by comparing the results against an already implemented simulation model of EDCA customised model of CP-EDCA.

  The performance of MP-EDCA was evaluated using simulation tools where all nodes were stationary. There are various factors such as node mobility, hidden nodes, exposed nodes, path loss, and signal fading which may affect the system's performance. Therefore, the performance of MP-EDCA must be tested in real-world environment before it can be released for the use.

In the upcoming future, the performance of MP-EDCA should be investigated on the Testbed. The real equipment may be used to verify and validate MP-EDCA performance. This will make it possible to collect real-world measurements, which shall be used for confirming the effectiveness of MP-EDCA in disaster situations. For testing the performance of MP-EDCA in the testbed environment, one may adopt the approached discuss in [128].

- **Supporting emergency traffic in other wireless networks.**

  In this thesis, the organisation who deal with emergency services, were studied for providing effective emergency traffic support in WLAN. It is reported that the emergency organisation prioritise the emergency traffic and giving priority to lifesaving emergency traffic followed by health, property, and environment. These emergency traffic priorities are incorporate elegantly in the MP-EDCA.

  In the dense emergency, people may use the other wireless networks (such as cellular or sensor network) for contacting their love-ones and cause network congestion. In the result of network congestion, people under risk to life may suffer. Therefore, there is a need to investigate and incorporate MP-EDCA based emergency traffic priority approach in other wireless networks.

  Investigating emergency traffic support in other wireless networks will be another important area of future research. For providing ubiquitous emergency traffic support, one may need to investigate other wireless networks and map their priorities with the emergency traffic priorities suggested in MP-EDCA.

- **Evaluate performance of MP-EDCA and PAC-MP-EDCA in the error-prone environment.**

  The performance of MP-EDCA and PAC-MP-EDCA protocols were tested in the error-free-environment. This is not the case for the real-world network where various communication errors are introduced by various causes such as path loss and signal fading.

As a future work, the performance of MP-EDCA, PAC-MP-EDCA and FASBA can be evaluated in an error-prone environment by considering the frame errors caused by various factors such as co-channel and adjacent channel interference, multi-path fading, and ambient noise.

- **Emergency-aware Internet of Things (EIoT)**

  The increasing number of physical objects (devices) on the network highlights the importance of IoT. In the internet of things (IoT), devices extending the internet and exchanging data without human interaction [129]. In the dense emergency, system planners may use the internet of things for saving human life if the emergency traffic support is incorporated in the devices. Therefore, an emergency aware of IoT is another area of future research.

  MAC is one of the key components which influence the performance of the network. The MAC protocols used in IoT may be groups by distance-wise i.e., shorter distance and longer distance. The MAC protocols for the shorter distance are: Bluetooth 802.15.1, radio frequency identification (RFID), Bluetooth low emergency, near field communication (NFC), IEEE 802.15.4. Another side MAC protocols for longer distance are: SigFox, long term evolution (LTE), narrow band IoT [130]. For providing emergency traffic support in IoT, MAC protocols used in IoT need to be investigated. Traffic priority mapping among the MAC protocols need to be performed so devices give priority to lifesaving traffic in an emergency.

7.3 System Implication and Deployment

The wireless MAC protocols that support emergency traffic and provide QoS were investigated in Chapters 4 to 6. A primary objective of this thesis is to develop a strict QoS guarantee framework that could be deployed for supporting emergency traffic over WLANs. To achieve this goal, system planners could apply the results presented in the previous chapters to provide emergency traffic with the provision of a QoS guarantee in the system. This section provides guidelines based on the results obtained in Chapters 4 to 6. The possible emergency scenarios and concrete guidelines for system planners are discussed next.

In the dense emergency, such as disaster may cause a huge loss of human life, property, and environment. The disaster also high affect the communication system. Moreover, Cellular or fixed infrastructure networks either get jam due to network congestion or shutdown to avoid remote detonation for more explosives.

First responders need reliable communication among them to save more and more human lives as shown in Figure 4.9. To provide reliable communications, WLAN could be the good alternative communication system, if system planners upgrade the firmware of WLAN devices with MP-EDCA, PAC-MP-EDCA and FASBA. The MP-EDCA supports emergency traffic and prioritises lifesaving emergency traffic in the network. In addition to a disaster situation, MP-ECA protocols could be also used in network saturated condition such as public event (soccer game) and may give priority to emergency traffic.

First responders need resources to save human life which are with the central coordinator node (shown in Figure 5.1). Therefore, they also need a reliable communication with the central coordinator. There may be a scenario where a high number of nodes (first responders) have lifesaving emergency traffic and want to communicate with the central coordinator node for resources. In such scenario, PAC-MP-EDCA is most useful in a situation where there is at least one central coordinator node, which can handle admission control. The PAC-MP-EDCA enhances the capabilities of MP-EDCA and prioritises lifesaving emergency traffic. Moreover. PAC-MP-EDCA dynamically activated and provides strict QoS guarantee in saturated network conditions.

In the dense emergency, the network may not have the capacity to accommodate all real-time lifesaving emergency traffic. The first responders may use short text messages instead of real-time traffic. However, there is no inherent support in WLAN to prioritise emergency text messages. In such a scenario, FASBA can help. FASBA prioritises emergency traffic, provides a guarantee of service delivery, and enhances throughput performance by reducing transmission overheads.

The FASBA protocol is easy to implement and provide a cost-effective solution to provide better QoS and assure for emergency nodes. For implementing the system, System planners may need to consider systems with higher random access memory (RAM) for holding multiple frames. In addition to the RAM, systems may use processing power for aggregating multiple frames. However, the processing power or RAM used by the FASBA is negligible in the current era of high-speed devices.

Appendix A

Riverbed Modeler Configuration

A.1. Introduction

There are various computer simulators available to design and develop IEEE 802.11 WLAN MAC protocols. The Riverbed Modeler is one of the popular network simulator tools. The Riverbed Modeler previously known as Opnet Modeler is a simulator software developed by Riverbed technologies. The Riverbed Modeler can be used to design, model, and analyse various communication networks, protocols, applications, and devices. The Riverbed Modeler is suitable for all types of networks including WLAN, WiMAX, and Cellular (4G or LTE). The Riverbed provides all built-in models to simulate IEEE standards and allows to customise or even create new network models.

There are two versions of Riverbed Modeler i.e. (1) Academic and (2) Commercial version. The academic version allows to create the network scenarios and evaluate the performance by using existing network models. Another side, the commercial version allows to customise the existing models or create your own network models. The typical example is MP-EDCA that was designed in this thesis by customising existing IEEE 802.11(EDCA) build-in models of Riverbed Modeler (commercial version).

The Riverbed Modeler is popular among network engineers, students and network researchers. There are many New Zealand based network and telecom companies including Spark Digital, Datacom Systems, 3D Networks, Fujitsu NZ are the partner of Riverbed [131]. The free academic and commercial versions of Riverbed Modeler are available for download at the https://support.riverbed.com/. The beginner of Riverbed Modeler may refer to [132] and advanced users may refer to [133].

The MAC protocols i.e. MP-EDCA, PAC, CP-EDCA, FASBA, and standard EDCA are implemented in the Riverbed Modeler version 18.0 in order to model and evaluating the performance.

A.2. Strengths and Weaknesses of Riverbed Modeler

The Riverbed Modeler is available for Windows operating system. The C/C++ programming languages are used to develop Riverbed Modeler. Riverbed provides a graphical user interface (GUI) to create network scenarios. Moreover, Riverbed allows users to modify their C/C++ writing code and implement users customized model.

The Riverbed Modeler provides a development environment with many built-in tools to develop wireless technologies and protocols, and evaluate the performance before the actual commercial production. The modeller allows users to create high-fidelity models, scalable simulation and analyses a wide range of wired and wired networks. Many network organisations use Riverbed Modeler to improve their network productivity and enhance network performance. Modeler enables users to:

- Create wireless and wired protocols and technologies.
- Test and Evaluate performance
- Enhance research and development productivity and accelerate time-to-market.

However, the main disadvantage of Riverbed Modeler is its licensing costs, memory consuming models, and insufficient tutorials.

A.3. Creation and Customization of Riverbed Models.

The Riverbed code can be modified by using Riverbed interface or Microsoft Visual C++ integrated development environment (IDE). The Riverbed Modeler has four models i.e. (1) Network (2) Node (3) Process and (4) State. The state model is based on C/C++

programming code. The state model consists of four programming blocks i.e. (1) head (2) functional (3) static and (4) temporary variables.

Figure A.1 shows a Riverbed representation of a fully connected network scenario for simulating MP-EDCA with PAC. The scenario consists total of 60 nodes. Each MP-EDCA scenario consists of an equal number of (Class 1 to 4) emergency nodes (identical configuration). Fig. A.1 also shows Application Definition and Profile Definition objects. Each scenario uses voice traffic generated by the Application Definition. Another side, application start time, duration and number of repetitions are configured in Profile Definition. We increase the number of nodes up to 40 to observe the effect of system performance for various emergency priorities. MP-EDCA supports four types of emergencies with various priorities (uniform node distribution). The new MP-EDCA node model is built by modifying the existing Riverbed Modeler's "wlan_station_adv" node model.

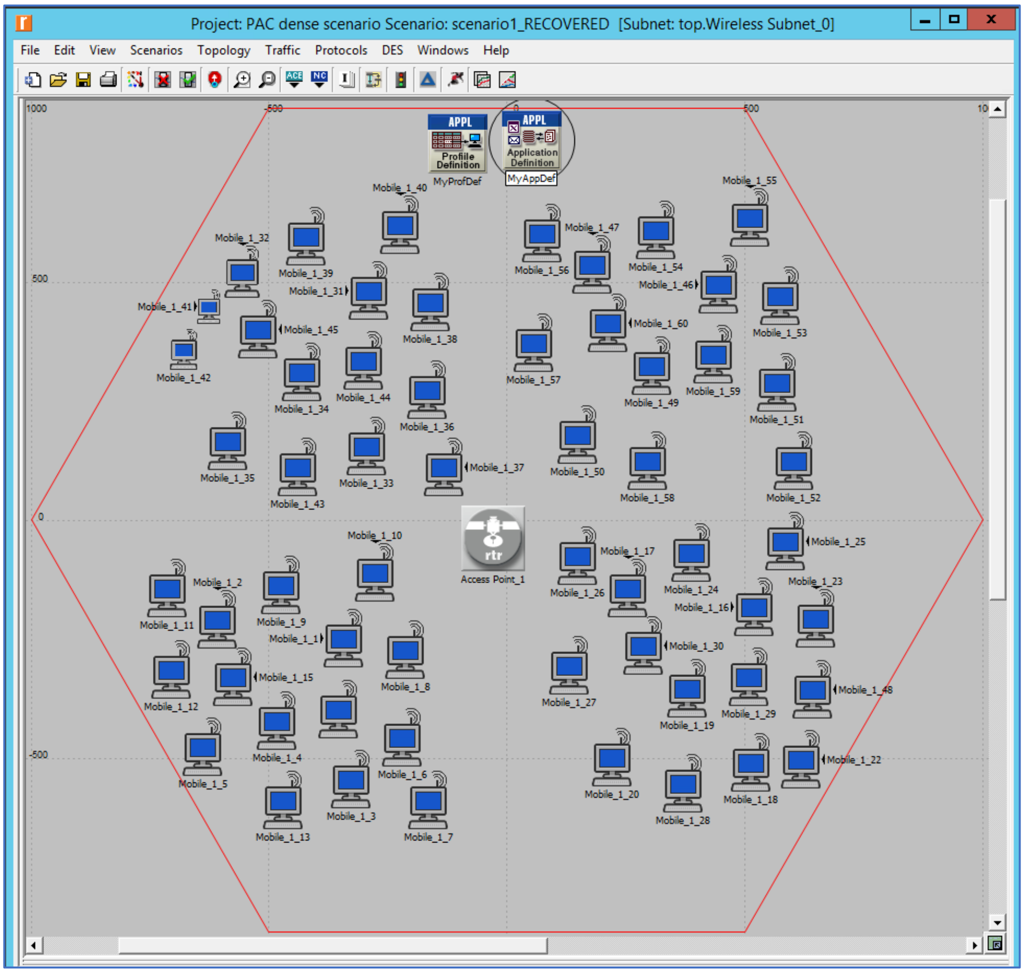

Figure A.1: Riverbed network simulation scenario.

The following changes have been made:

This section highlights how to customise process models, nodes and routers by modifying existing process model, nodes and routers for WLANs and see how the performance is affected by changes in the configuration. We will also learn how to dynamically modify physical characteristics, like the Slot Time, the SIFS (Short Interframe Space), the Minimum and Maximum Contention Windows which we cannot normally modify in the Riverbed Modeler. For modifying these physical characteristics, we need to customise the Riverbed Modeler's standard process models such as wlan_dispatch, wlan_mac and wlan_mac_hcf, and the node models wlan_ethernet_router_adv and wlan_wkstn_adv.

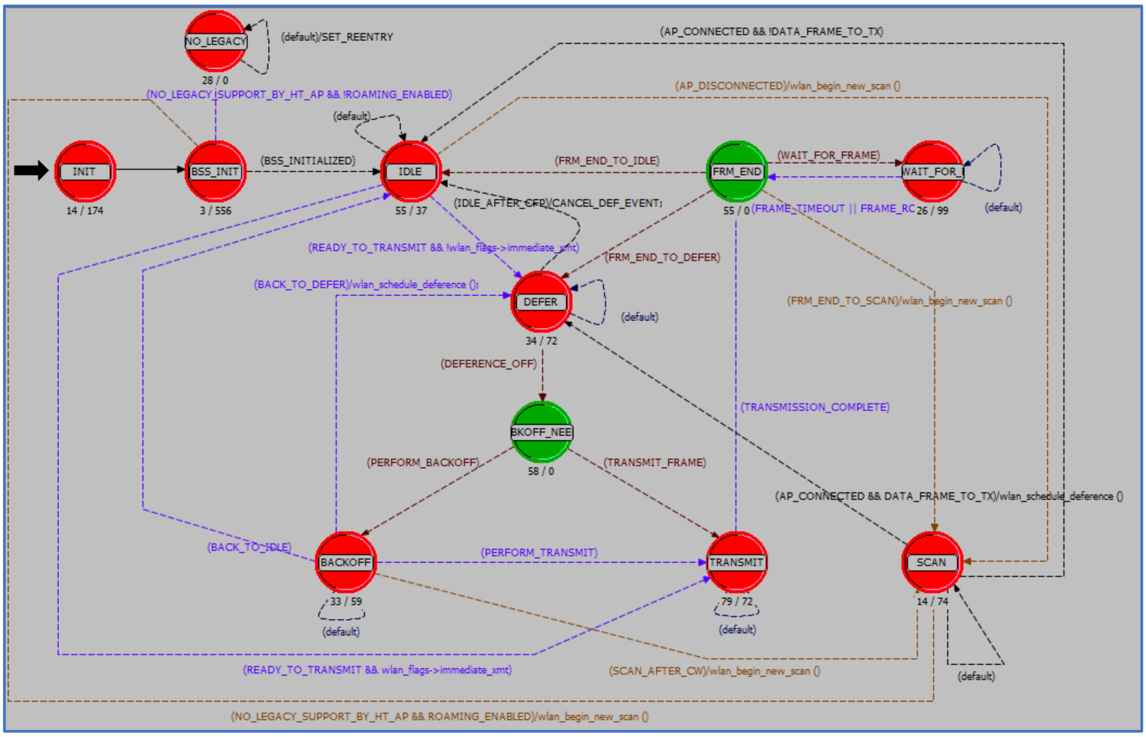

Figure A.2: Customised WLAN MAC process model.

A.3.1 Modifying wlan_mac Process Model

Steps:

1 Riverbed the process model "wlan_mac" in Riverbed Modeler

2 Open function block (FB) of wlan_mac from the toolbar and

3 Compile the wlan_mac process model.

4 Modify the required code.

5 Compile the process model

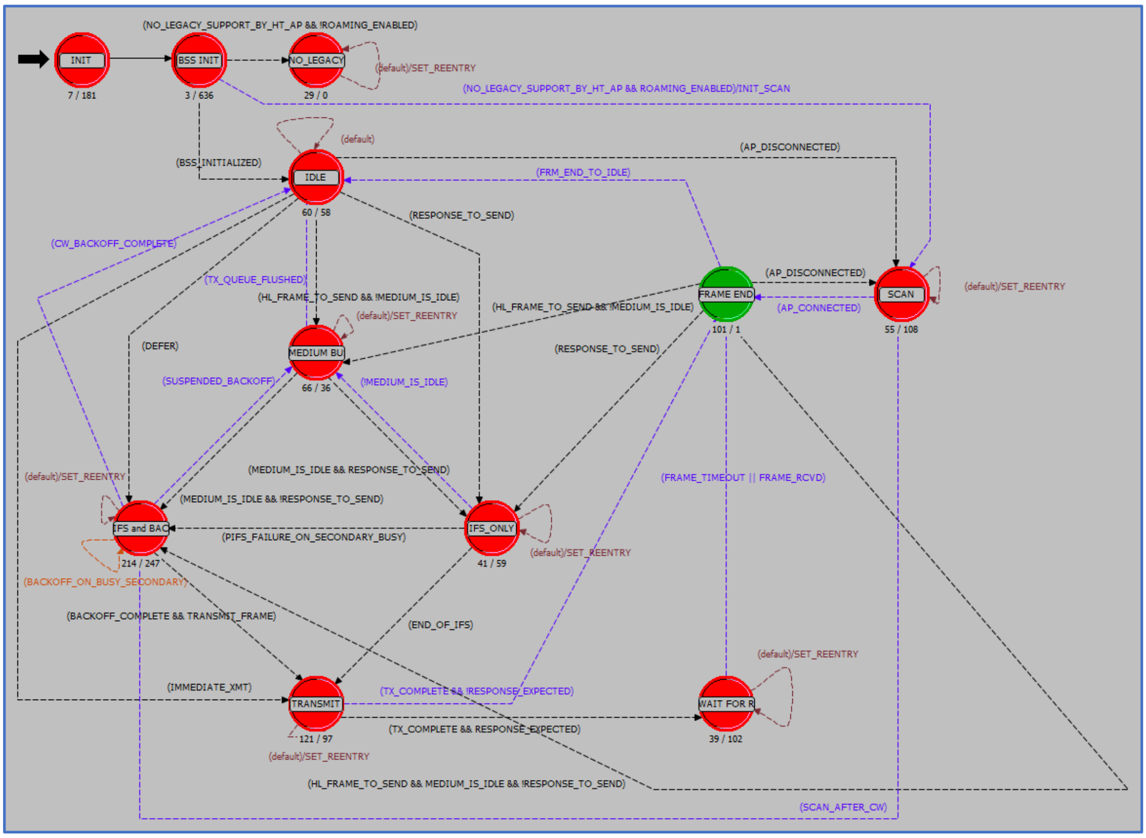

Figure A.3: Customised MAC hybrid coordination function process model.

A.3.2 Modifying wlan_mac_hcf Process Model

Steps:

1 Open the process model “wlan_mac_hcf” in the Riverbed Modeler

2 Save “wlan_mac_hcf” as demo_wlan_mac_hcf

3 Open function block (FB) of wlan_mac from the toolbar and

4 Compile the wlan_mac process model.

5 Modify the required code.

6 Compile the process model

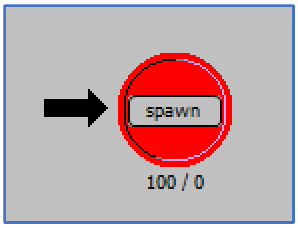

Figure A.4: Customised WLAN dispatch model.

A.3.3 Customisation of wlan_dispatch Process Model

Steps:

1. Open the Riverbed process model "wlan_dispatch" in Riverbed Modeler
2. Save as demo_wlan_dispatch
3. Open the model attributes from interfaces menu
4. Select Wireless LAN parameters then click edit properties
5. Add properties i.e. slot time, SIFS
6. Add attributes name "Slot Time; Type double; Unit secs; Default Value = 20E-06".
7. Add attribute name "SIFS; Type double; Units secs; Default Value = 10E-06"
8. Double click on the Test Spawn and modify the code as required.
9. Compile the process model and
10. Close the process model.
11. Modify the required code.
12. Compile the process model

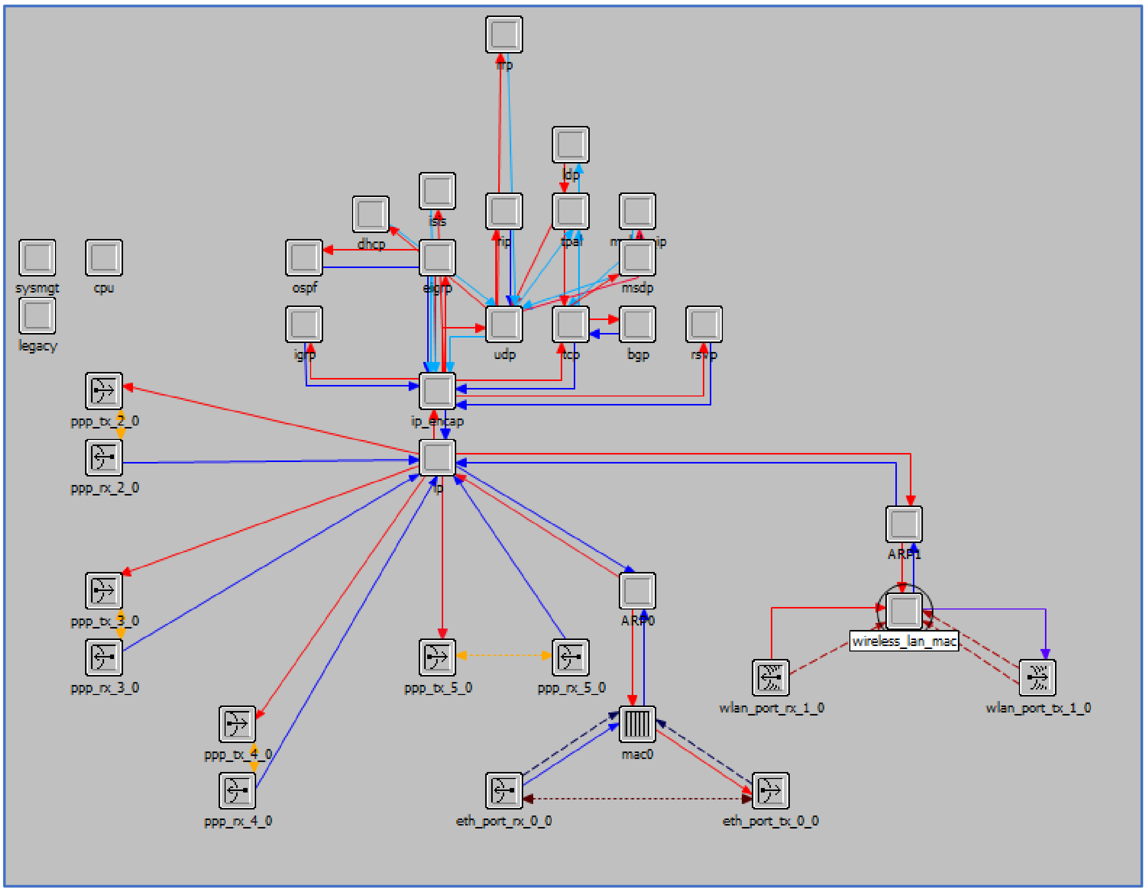

Figure A.5: Customisation of WLAN node model.

A.3.4 Customisation of Workstation

Steps:

1 Open the Riverbed node model wlan_wkstn_adv for workstation

2 Save wlan_wkstn_adv as demo_wlan_wkstn_adv

3 Right click on wireless_lan_mac and select edit attributes

4 Change the process model from wlan_dispatch to demo_wlan_dispatch.

5 Click Ok to save the attributes

6 Compile the demo_wlan_wkstn_adv node model and close the node model.

A.3.5 Creating Custom Router (Access Point)

Steps:

1 Open the node model wlan_ethernet_router_adv for workstation

2 Save as demo_wlan_ethernet_router_adv

3 Right click on wirless_lan_mac, and select attributes

4 Change the process model from wlan_dispatch to demo_wlan_dispatch

5 Click Ok to save the attributes

6 Compile the demo_wlan_ether_router_adv node model and close the node model.

Right click on application definition and set the following properties

1. Name = AppDef
2. Application Definition (Number of Rows) = 1
3. Name = voice
4. Voice attributes
    a. Silence length = default
    b. Talk spurt length = default
    c. Symbol destination name = voice destination
    d. Encode scheme = G.711
    e. Type of service = Interace voice (6)

Right click on profile definition and set the following properties

1. Name = ProfDef
2. Profile Definition (number of Rows) = 1
3. Name = voice
4. Application Number of Rows = 1
    a. Name = voice
    b. Start time offset = no offset

c. Duration = end of profile

d. Inter-repetition = exponential (300)

e. Number of repetition = unlimited

f. Repetition pattern = serial

    i. Operation mode = serial

    ii. Start time = uniform (50, 60)

    iii. Duration = end of simulation

g. Inter-repetition = constant (3000)

h. Number of repetition = constant (0)

i. Repetition patter = serial

5. Right click on the first workstation and set the following properties

    a. Name = voice source

    b. Application supported profile

        i. Number of rows = 1

        ii. Profile name = voice

        iii. Start time = start of simulation

        iv. End time = end of simulation

A.4 Radio Propagation and Error Models in Riverbed Modeler

The path loss models are generally categorized into four classes i.e. (1) free space, (2) suburban fixed, (3) outdoor or indoor, (4) vehicular. To estimate the path loss through the use of empirical radio propagation models are widely used by the research community as these models are easy to implement in a simulation environment and produce satisfactory results [134, 135]. The Riverbed Modeler supports several radio propagation models, and allow users to create or customise any propagation model. **Table A.1** lists the three radio propagation models with their formula and the brief description. In order to customise the propagation model in Riverbed Modeler, network model, node model, process model, and transceiver objects need to be modified. The source code of these objects can be found in the STD folder of Riverbed Modeler.

Table A.1: Radio Propagation Models in Riverbed Modeler.

Model	**Free Space**
Formula	$P_{rx}(r) = \frac{P_{tx} G_{tx} G_{rx} \lambda^2}{(4\pi)^2 r^2 L}$
Description	Widely used for an empty (ideal) environment where no or very little obstruction. P_{rx} is a received signal power (in Watts) and function of distance. Another side, P_{tx} is the power transmitted in watts. G_{rx} is the gain of receiving antenna and G_{tx} is gain of transmitting antennas. Where L represents the path loss in decibels.
Model	**Okumura-Hata**
Formula	$L = L_{FSL} + A_{MU} - H_{MG} - H_{BG} - \sum K_{CORRECTION}$
Description	Widely used model for urban areas. In the formula, L is average path loss, L_{FSL} is the free space loss, and A_{MU} is average attenuation. All measure in decibel. H_{BM} and H_{BG} are the mobile station and base station gain respectively. $K_{correction}$ represents obstacles i.e. environmental or water.
Model	**Erceg's Suburban Fixed**
Formula	$PL = H + 10\gamma \log_{10}(d/d_0) + X_f + X_h + s$ for $d > d_0$
Description	This model is based on extensive simulations and suitable for the suburban environment. In this model, PL represents instantaneous attenuation, H is an interception, γ is wavelength, d is distance, and X denotes the height of base (AP) or STA.

A.5. IEEE 802.11 WLAN Packet Types

The IEEE 802.11 WLAN packets may be categorized into three (3) types i.e. (1) management, (2) control and (3) Data. These three packets types may also have subtypes. The IEEE uses six (6) bits to identify the type of packet. The first two (2) bits are used to identify the type of packet. The bits 00 refers that packet is management type, bits 01 refers packet is control type, whereas bit 11 refers the packet is data. The remaining four (4) bits are used to identify the subtype of the packet.

The management packets are used by the STA or AP to get authentication, association and synchronization. Table A.2 illustrates the management packet types. Another side, control packets are used to control the transmission. The packets such as RTC, CTS, ACK, power saving packets and CFP are examples of control packet types. Table A.3 highlight the control packets, subtypes and usage. The data packet may vary and may have various subtypes. Table A.4 highlights the WLAN data packets.

Table A.2: WLAN management packets.

Two bits	Packet type	Four bits	Subtype	Usage
00	Management	0000	Associate request	An STA sends this packet to an AP or other neighbouring STA for getting the association.
00	Management	0001	Associate response	AP or neighbouring STA responds on the association request.
00	Management	0010	Re-associate request	Similar to associate request but includes information of current association.
00	Management	0011	Re-associate response	AP or neighbouring STA responds on the re-association request.
00	Management	0100	Probe request	STA seeks AP or BSS.
00	Management	0101	Probe response	AP or STA respond to the probe request with supported parameters.
00	Management	1000	Beacon	AP sends Beacon packets for announcing CFP.
00	Management	1001	ATIM	ATIM (Announcement Traffic Indication Message) used synchronise STAs in IBSS.
00	Management	1010	Disassociate	Used for announcing dis-association.
00	Management	1011	Authentication	STA uses for handshaking.
00	Management	1100	De-authentication	Used to announcing de-authentication with other STA or BSS.

Table A.3: Subtypes of WLAN control packets.

Two bits	Packet type	Four bits	Subtype	Usage
01	Control	1010	Power saving mode	An STA in the power saving mode may awake periodically to listen.
01	Control	1011	Request to send (RTS)	AP or neighboring STA responds on the association request,
01	Control	1100	Clear to send (CTS)	
01	Control	1101	Acknowledgement	STA acknowledges the acceptance of receiving data.
01	Control	1110	Contention Free Period (CFP)	Announcing the end of CFP.
01	Control	1111	Ending CFP with Acknowledgement	STA ends the CFP and acknowledges the acceptance of receiving data in a single packet.

Table A.4: WLAN data packets.

Two bits	Packet type	Four bits	Subtype	Usage
10	Data	Any	Any	There are various subtypes of data packets.

The Riverbed Modeler is available for Windows operating system. The C/C++ programming

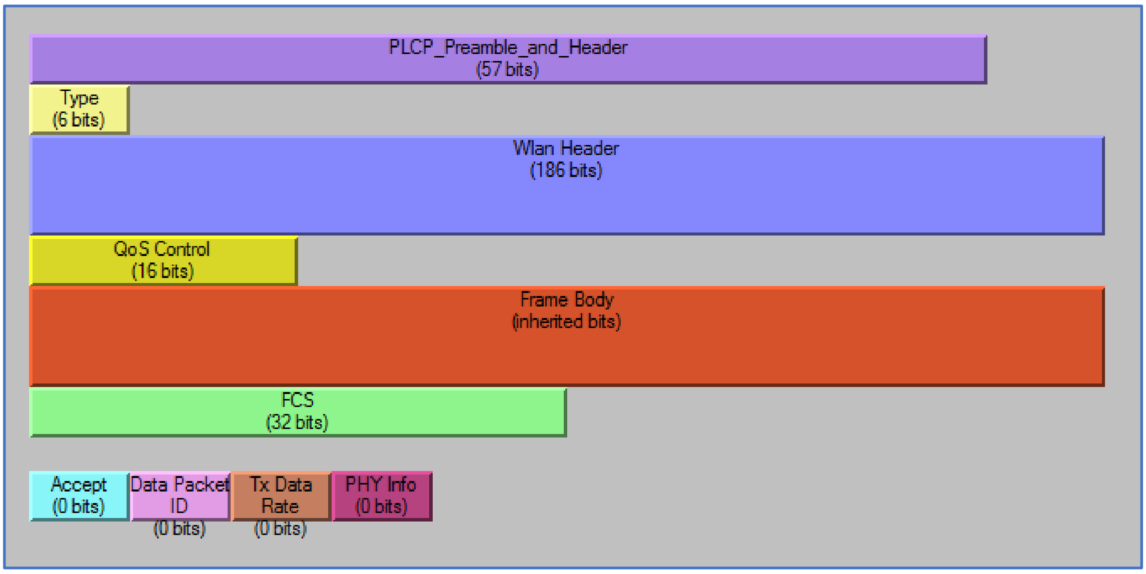

Figure A.6: Packet format of WLAN MAC.

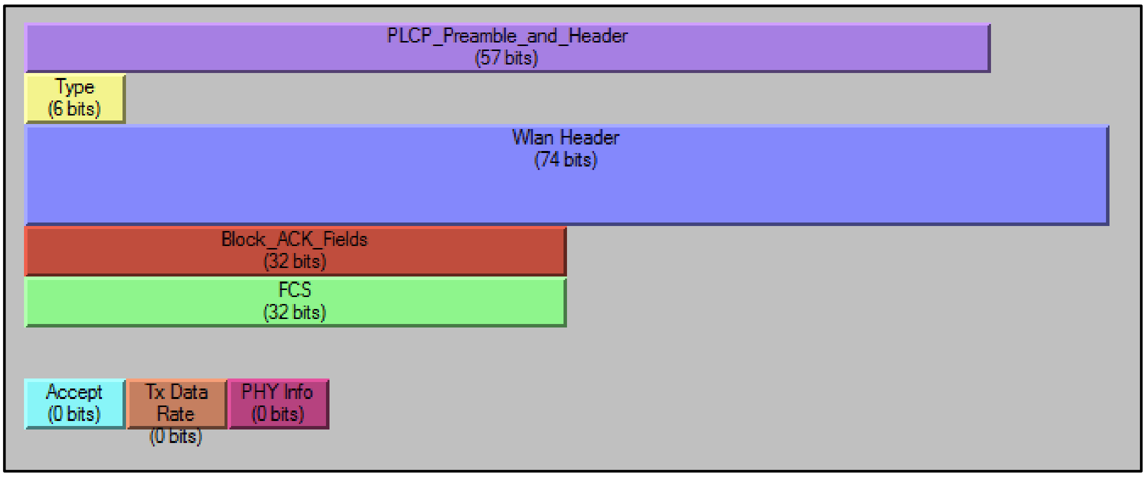

Figure A.7: Packet format of WLAN AMSDU sub-frame.

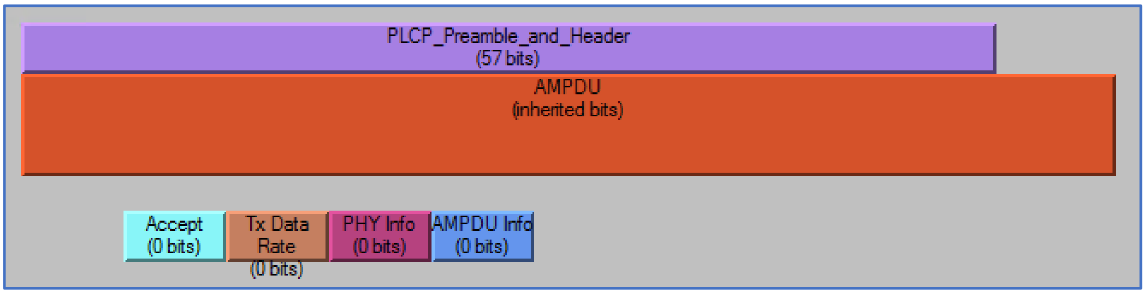

Figure A.8: Packet format of WLAN AMPDU frame.

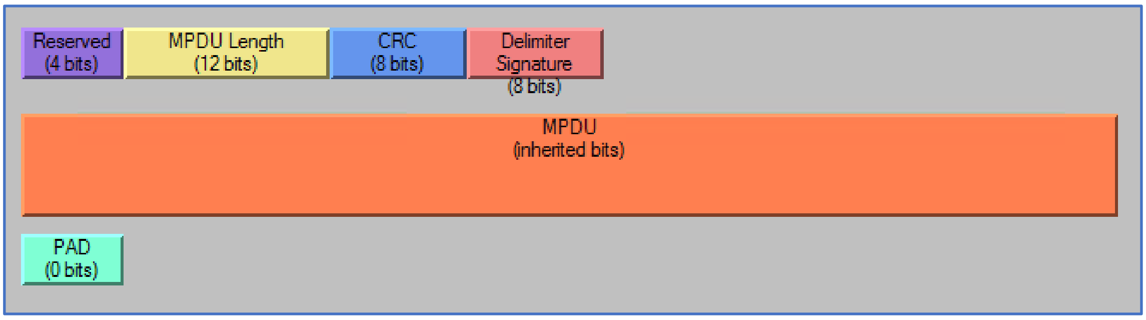

Figure A.9: Packet format of WLAN AMPDU sub-frame.

Appendix B

Implementation of FASBA in MATLAB

B.1. Introduction

In the Matlab, We evaluate the performance of FASBA's frame aggregation mechanism with BlockAck and Simple BlockAck schemes. In BlockAck, all three packets are resent again. Another side, FASBA's simple block acknowledgement mechanism (see Table 6.2) is used. For implementing BlockAck, and FASBA's SimpleBlockAck in Matlab, a cell variable of user-defined length is created. The simulation is run until the cell variable is not emptied. Two arrays variables i.e. (1) new-bits, and (2) old-bits are used to move the data. Iterations are used to empty the cell. In each iteration, three bits (packets) are removed from the cell variable and added into the new "new-bits" variable. These bits and any other bits in the variable "old-bits" are assigned to the variable packet. In the SimpleBlockAck, the probability of 0.1% is used. A bit (packet) is assumed lost from. The lost bit is stored in the old-bits variable. The final bits are sent by removing lost bits are stored in the variable SimpleBlockAck. In the simulation, any lost bits by the system are identified and sent with the next packets data. Another side in BlockAck, all bits (packets) are sent again. The Matlab code is given below:

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Frame aggregation scheme with Block Acknowledgement and Simple Block
Acknowledgement
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
function [BlockAck, SimplBlockAck] = NumberofPackets(int1)
clc
cell = 1: 1 : int1;
final = [];
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
time_as = cputime;
cell = 1: 1 : int1;
t = 3;
SimpleBlockAck = [];
old_bits = [];
```

```
new_bits = [];
packet = [];
len_new_bits = [];
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Simple Block Acknowledgement Mechanism.
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
while ~isempty(cell)
   if isempty(old_bits)
        if length(cell)< t
            t = length(cell);
        end
    new_bits = cell(1:t);
    old_bits = [];
    cell(1:t) = [];
    packet = [];
    packet = [old_bits new_bits];
    len_new_bits = [len_new_bits t];
    else
    tt = t - length(old_bits);
    new_bits = cell(1: tt);
    cell(1: tt) = [];
    packet = [old_bits, new_bits];
    new_bits = [];
    old_bits = [];
    len_new_bits = [len_new_bits tt];
    end
    w = rand;
    if w <= 0.001
%       disp('. . . . . . ')
        lostBit = randperm(3);
        lostBit = lostBit(1);
        old_bits = [old_bits packet(lostBit)];
        packet(lostBit) = [];
        final2 = [final2 packet];
    else
        final2 = [final2 packet];
        old_bits = [];
        new_bits = [];
    end
end
SimpleBlockAck;
% plot(final2, '-o')
e = cputime-time_as
disp('CPU time...............................................')
figure;
plot(len_new_bits, '-o')
length(len_new_bits)

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Block Acknowledgement Mechanism.
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
time_as = cputime;
cell = 1: 1 : int1;
t = 3;
BlockAck = [];
old_bits = [];
new_bits = [];
packet = [];
len_new_bits = [];
```

```
while ~isempty(cell)
    if isempty(old_bits)
        if length(cell)< t
            t = length(cell);
        end
    new_bits = cell(1:t);
    cell(1:t) = [];
    packet = [];
    packet = [old_bits new_bits];
    len_new_bits = [len_new_bits t];
    else
    new_bits = old_bits;
    old_bits = [];
    packet = [];
    packet = [old_bits, new_bits];
    len_new_bits = [len_new_bits 0];
    end

    w = rand;
    if w <= 0.001
%          disp('. . . . . . ')
        lostBit = randperm(3);
        lostBit = lostBit(1);
        old_bits = [old_bits packet];
        packet = [];
        final = [final packet];
    else
        final = [final packet];
        old_bits = [];
        new_bits = [];
    end
end

BlockAck;
% plot(final, '-o')
e = cputime-time_as
disp('CPU Time .........................')
figure;
plot(len_new_bits, '-o')
length(len_new_bits)
*********************************************************************/
```

Figure B.1: Matlab code for implementing BlockAck and Simple BlockAck.

The simulation was carried out to demonstrate the effectiveness of the proposed algorithm. The bit stream length of 5000 was used three bit are transferred at once from sending to the receiver with a probability of missing a bit was set to be at 10 percent (0.1). In the first set of experiment, when if a packet is lost while sending it to the receiver, the whole packet (all three bits) are sent again, the results are shown in the Figure B.1. It took 1844 iteration to send the completed bit stream. Second set of experiment was performed where only the missing bit is sent when any bit in the packet was lost. When the experiment was repeated with the same settings, the results are shown in the Figure B.2. This time, the proposed algorithm took 1718 iterations to send the complete bit stream. The proposed algorithm has taken 126 less iterations to send a complete message, which is an improvement of 7.34%.

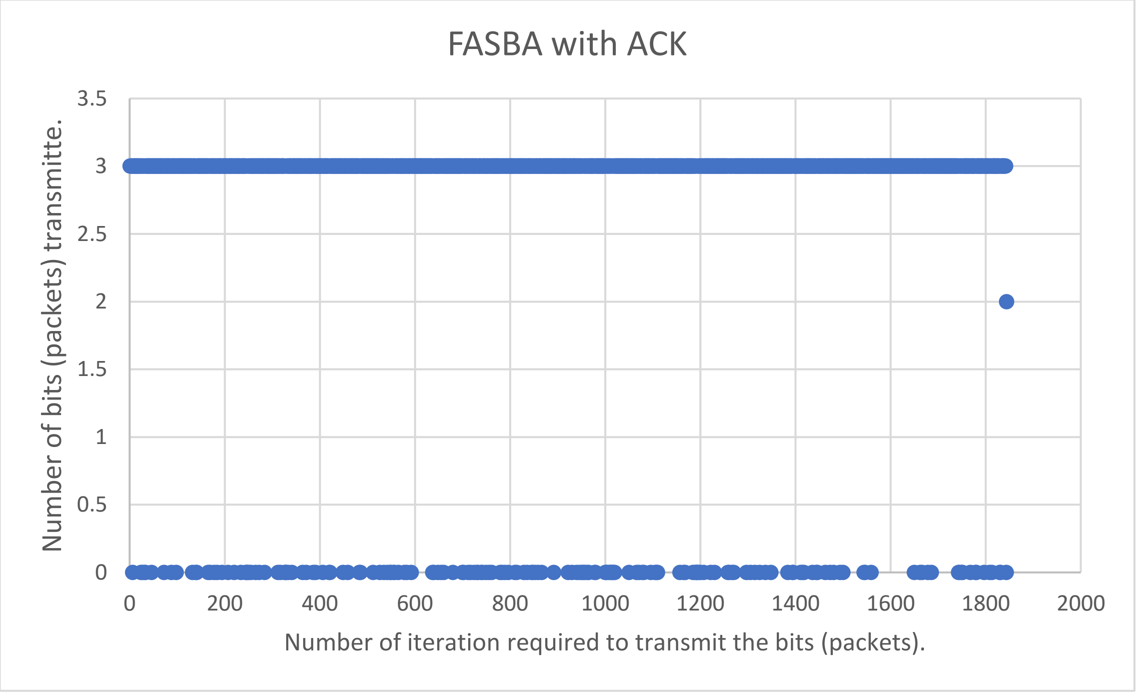

Figure B.2: FASBA sending three bits and three frames for lost message.

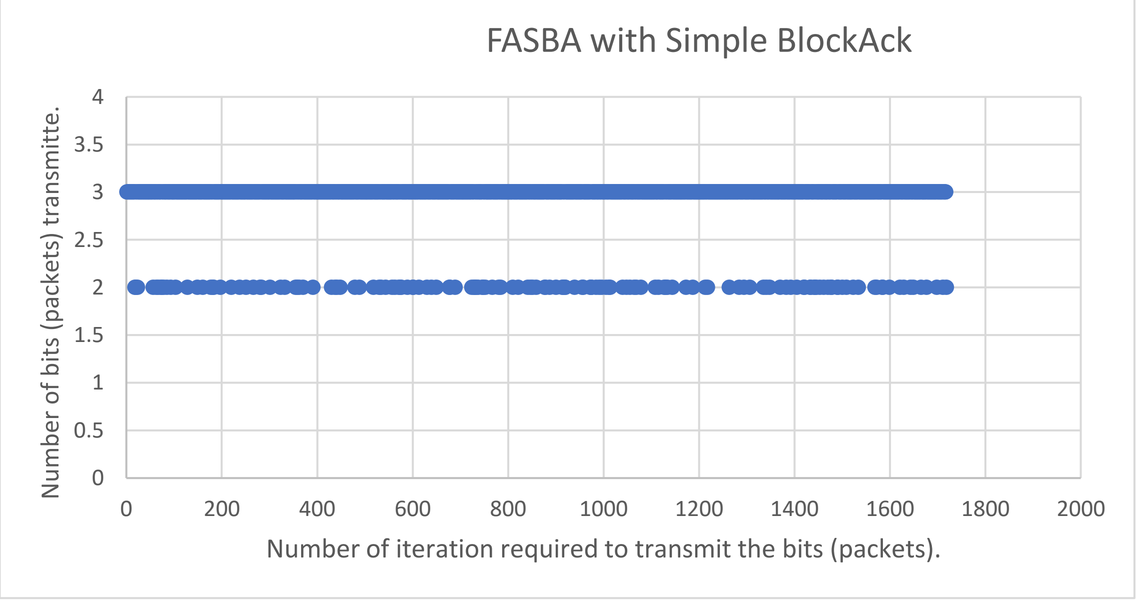

Figure B.3: FASBA with Simple BlockAck.

References

[1] M. M. Mulhanga, S. Rito Lima, and P. Carvalho, "Characterising University WLANs within Eduroam Context," in *Smart Spaces and Next Generation Wired/Wireless Networking* vol. 6869, ed, 2011, pp. 382-394.

[2] G. Daqing and J. Zhang, "QoS enhancement in IEEE 802.11 wireless local area networks," *IEEE Communications Magazine*, vol. 41, pp. 120-124, 2003.

[3] "IEEE Std. 802.11i-2004. IEEE Standard for Information Technology: Telecommunications and Information Exchange between Systems, LAN/MAN-Specific Requirements Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 6: MAC Security Requirements," ed, 2004.

[4] F. Chiti, R. Fantacci, L. Maccari, D. Marabissi, and D. Tarchi, "A broadband wireless communications system for emergency management," *IEEE Wireless Communications,* vol. 15, pp. 8-14, 2008.

[5] H. F. Rashvand, V. T. VSalcedo, E. M. Sanchez, and D. Iliescu, "Ubiquitous wireless telemedicine," *IET Communications* vol. 2, pp. 237-254 February 2008.

[6] X. Yang, "QoS guarantee and provisioning at the contention-based wireless MAC layer in the IEEE 802.11e wireless LANs," *IEEE Wireless Communications,* vol. 13, pp. 14-21, 2006.

[7] R. Zhang, L. Cai, and J. Pan, *Resource Management for Multimedia Services in High Data Rate Wireless Networks*: Springer, 2016.

[8] M. Balakrishnan, D. Benhaddou, Y. Xiaojing, and D. Gurkan, "Channel preemptive EDCA for emergency medium access in distributed wireless networks," *IEEE Transactions on Wireless Communications,* vol. 8, pp. 5743-5748, 2009.

[9] "IEEE 802.11u-2011, Part II: wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Amendment 9: Interworking with External Networks," ed, 2011.

[10] C. Yeong-Sheng, C. Min-Yen, T. Fan-Chun, and K. Chih-Heng, "High Performance Distributed Coordination Function with QoS support in IEEE 802.11e networks," in *Australasian Telecommunication Networks and Applications Conference (ATNAC)*, Melbourne, VIC, 2011, pp. 1-6.

[11] P. E. Engelstad and O. N. Osterbo, "Non-Saturation and Saturation Analysis of IEEE 802.11e EDCA with Starvation Prediction," in *In Proceedings of ACM MSWiM'05*, New York, 2005.

[12] A. Hamidian and U. Korner, "An enhancement to the IEEE 802.11e EDCA providing QoS guarantees " *Special Issue: Next Generation Networks—Architectures, Protocols, Performance*, vol. 33, pp. 195-212, 2006.

[13] D. J. He and C. Q. Shen, "Simulation study of IEEE 802.11e EDCF," in *The 57th IEEE Semiannual Conference on Vehicular Technology*, 2003, pp. 685-689.

[14] P. E. Engelstad and O. N. Osterbo, "Analysis of the Total Delay of IEEE 802.11e EDCA and 802.11 DCF," in *IEEE International Conference on Communication* 2006, pp. 552-559.

[15] A. M. Abbas and K. Al Soufy, "Saturation Analysis of IEEE 802.11 EDCA for Ad Hoc Networks," in *Contemporary Computing*. vol. 306, M. Parashar, D. Kaushik, O. Rana, R. Samtaney, Y. Yang, and A. Zomaya, Eds., ed: Springer Berlin Heidelberg, 2012, pp. 419-430.

[16] "IEEE Std. 802.11u-2011, IEEE Standard for Information Technology - Telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part:11: Wireless Medium Access Control (MAC) and Physical Layer (Phy) Specifications, Amendment 9: Interworking with External Networks ", New YorkFebruary 2011.

[17] Y. Xiao, L. Haizhon, and C. Sunghyun, "Protection and guarantee for voice and video traffic in IEEE 802.11e wireless LANs," in *The 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, 2004, pp. 2152-2162 vol.3.

[18] X. Chen, H. Zhai, X. Tian, and Y. Fang, "Supporting QoS in IEEE 802.11e wireless LANs," *IEEE Transactions on Wireless Communications,* vol. 5, pp. 2217-2227, 2006.

[19] A. Hamidian and U. Korner, "Extending EDCA with distributed resource reservation for QoS guarantees " *Telecommunication Systems. Special Issue: QoS, Control, and Security in Next Generation Networks,* vol. 39, pp. 187-194, 20 Sep. 2008.

[20] C. C. Yang, L. Jheng Sian, L. Ruei Yi, L. Shang-Yo, and W. Jyh-Horng, "QoS Performance Improvement for WLAN Using Priority Random Early Detection," in *International Conference on Wireless Communications, Networking and Mobile Computing,* , Shanghai 2007, pp. 1996-1999.

[21] N. Sarma, A. Singh, and S. Nandi, "A Strict Priority Based QoS-Aware MAC Protocol for Mobile Ad Hoc Networks," *Distributed Computing and Internet Technology,* vol. 5375/2009, pp. 121-132, 2009.

[22] C. Cetinkaya, "Service differentiation mechanisms for WLANs," *Ad Hoc Networks,* vol. 8, pp. 46-62, April 2009 2010.

[23] N. Tadayon, S. Zokaei, and E. Askari, "A novel prioritization scheme to improve QoS in IEEE 802.11e networks," *EURASIP Journal of Computer Systems, Networks, and Communication,* vol. 2010, no. 4, pp. 112-120, January, 2010.

[24] H. Ferng, C. Setiadji, and A. Leonavich, "Fair round robin binary countdown to achieve QoS guarantee and fairness in WLANs," *Wireless Networks,* vol. 17, pp. 1259-1271, 15 May 2011.

[25] Riverbed-Technologhy. (January 10, 2019). *Riverbed (Opnet) Modeler*. Retrieved on January 10, 2019 from https://www.riverbed.com/sg/

[26] R. G. Oarroppo, S. Giordano, and S. Lucetti, "IEEE 802.11 b performance evaluation: convergence of theoretical, simulation and experimental results," in *The 11th International Telecommunications Network Strategy and Planning Symposium,* 2004, pp. 405-410.

[27] N. I. Sarkar and J. A. Gutiérrez, "Revisiting the issue of the credibility of simulation studies in telecommunication networks: highlighting the results of a comprehensive survey of IEEE publications," *IEEE Communications Magazine,* vol. 52, pp. 218-224, 2014.

[28] J. F. Nunamaker, Jr., M. Chen, and D. M. T. Purdin, "Systems development in information systems research," *Journal of Management Information Systems* vol. 7, 1990-91.

[29] E. Crawley, R. Nair, B. Rajagopalan, and H. Sandick, "A Framework for QoS-based Routing in the Internet," Network Working Group: Request for Comments: RFC - 2386Aug. 1998.

[30] "ITU-T Telecommunication Standardization Sector of ITU," in *Telephone Networks and ISDN: Quality of Service, Network Management and Traffic Engineering*, ed: ITU-T E.800, 1994.

[31] ITU-T, "Series E: Overall network operation, telephone service, service operation and human factors," Sep. 2008 2008.

[32] S. M. Obaidat, M. Denko, and I. Woungang, *Pervasive Computing and Networking* vol. 01: John Willey and Sons, Ltd. USA, 2011.

[33] "One way transmission time," ed: ITU-T G.114, 2003.

[34] R. Jordan and C. T. Abdallah, "Wireless communications and networking: an overview," *IEEE Antennas and Propagation Magazine*, vol. 44, pp. 185-193, August 7 2002.

[35] J.-Y. Seol and S.-L. Kim, "Node mobility and capacity in wireless controllable ad hoc networks," *Computer Communications*, vol. 35, pp. 1345-1354, June 15, 2012.

[36] M. Patzold, *Mobile fading channels: Modelling, analysis and simulation* vol. 1. New Yord, USA: John Wiley & Sons, Inc., 2001.

[37] J. Geier. *How to define minimum snr values for signal coverage.* Retrieved on June 1, 2019 from http://www.wireless-nets.com/resources/tutorials/define_SNR_values.html

[38] J. Wexler. *Security and QoS Unite*. Retrieved on June 10, 2019 from https://www.computerworld.com/article/2574473/security-and-qos-unite.html

[39] "IEEE Std. 802.11-2007, IEEE Standard for Information Technology - Telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part:11: Wireless Medium Access Control (MAC) and Physical Layer (Phy) Specifications, (Revision of IEEE 802.11-1999)," New YorkApril 2007.

[40] "IEEE 802.11 Stand. for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," New YorkApril 1997.

[41] "IEEE Std. 802.11a WG/D5.0, Part II: wireless LAN medium access control (MAC) and physical layer (PHY) specifications: high-speed physical layer in the 5 GHz band," New YorkApril 1999.

[42] "IEEE Std. 802.11b WG, Part II: wireless LAN medium access control (MAC) and physical layer (PHY) specifications: high-speed physical layer extension in the 2.4 GHz band," New YorkApril 1999.

[43] "IEEE 802.11g WG. Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE Stds 802.11a-1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001. IEEE 802.11g Standard," New York 2003.

[44] I. W. Group, "IEEE Project - 802.11ax - Standard for Information Technology -- Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks -- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment Enhancements for High Efficiency WLAN," 2019.

[45] "IEEE Std. 802.11e-2005, IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements," New YorkNov. 11 2005.

[46] P. Agrawal and A. Sarkeja, "A Survey on Optimum Neighbour Discovery Techniques in Mobile Ad-hoc Networks," *International Journal of Computer Applications,* vol. 162, 2017.

[47] J. Loo, J. L. Mauri, and J. H. Ortiz, *Mobile ad hoc networks: current status and future trends*: CRC Press, 2016.

[48] J. Deng and R. S. Chang, "A Priority Scheme for IEEE 802.11 DCF Access Method," *IEICE Transactions on Communications,* vol. E82-B January 1999.

[49] B. P. Crow, I. Widjaja, L. G. Kim, and P. T. Sakai, "IEEE 802.11 Wireless Local Area Networks," *IEEE Communications Magazine,* vol. 35, pp. 116-126, August 1997.

[50] K. Jong-Ok, H. Tode, and K. Murakami, "Friendly coexistence of voice and data traffic in IEEE 802.11 WLANs," *IEEE Transactions on Consumer Electronics,* vol. 52, pp. 347-354, 05 July 2006.

[51] "IEEE Std. 802.1D-2004. IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges," New YorkJune 2004.

[52] H. T. Cheng, H. Jiang, and W. Zhuang, "Distributed medium access control for wireless mesh networks," *Journal of Wireless Communications and Mobile Computing,* vol. 6, pp. 845-864, 2006.

[53] E. G. Varthis and D. I. Fotiadis, "A comparison of stop-and-wait and go-back-N ARQ schemes for IEEE 802.11 e wireless infrared networks," *Computer communications,* vol. 29, pp. 1015-1025, 2006.

[54] "IEEE Std. 802.11-2009, IEEE Standard for Information Technology - Telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part:11: Wireless Medium Access Control (MAC) and Physical Layer (Phy) Specifications, Amendment 5: Enhancements for higher throughput. ," New YorkOctober 2009.

[55] T. Li, Q. Ni, and Y. Xiao, "Investigation of the block ACK scheme in wireless ad hoc networks," *Wiley Journal of Wireless Communications and Mobile Computing,* vol. 6, pp. 877-888, 2006.

[56] Y. Liu and M. Meng, "Survey of admission control algorithms in IEEE 802.11 e wireless LANs," in *International Conference on Future Computer and Communication*, 2009, pp. 230-233.

[57] D. Gao, J. Cai, and K. N. Ngan, "Admission control in IEEE 802.11 e wireless LANs," *Journal of IEEE network,* vol. 19, pp. 6-13, 2005.

[58] L. Khoukhi, H. Badis, L. Merghem-Boulahia, and M. Esseghir, "Admission control in wireless ad hoc networks: a survey," *EURASIP Journal on Wireless Communications and Networking,* vol. 2013, p. 109, 2013.

[59] L. H. Ii and R. Tafazolli, "Admission control schemes for 802.11-based multi-hop mobile ad hoc networks: a survey," *IEEE Communications Surveys & Tutorials,* vol. 11, 2009.

[60] MathWorks. *MATLAB.* Retrieved on January 10, 2019 from https://www.mathworks.com/products/matlab.html

[61] E. N. Ekwem and K. Nisar, "An Experimental Study: Using a Simulator Tool for Modelling Campus Based Wireless Local Area Network," *International Journal of Advanced Pervasive and Ubiquitous Computing (IJAPUC),* vol. 6, pp. 35-53, 2014.

[62] B. Krupanek and R. Bogacz, "OPNET Modeler simulations of performance for multi nodes wireless systems," *International Journal of Metrology and Quality Engineering,* vol. 7, p. 105, 2016.

[63] K. Gündoğdu and A. Çalhan, "An implementation of wireless body area networks for improving priority data transmission delay," *Journal of medical systems,* vol. 40, p. 75, 2016.

[64] C. C. Secretariat, "Civil Contingencies Act 2004: a short guide (revised)," *London: Cabinet Office,* 2004.

[65] Purdue University - *Emergency Preparedness: Emergency Planning*. Retrieved on February 15, 2019 from https://www.purdue.edu/ehps/emergency_preparedness/emergency/emergency-planning.html

[66] D. Willie R. Taylor, "United States Department of the 'Interior," 30 Aug. 2006.

[67] NHS. *London Ambulance Service details of AMPDS use*. Retrieved on March 15, 2019 from http://www.londonambulance.nhs.uk/helpweoffer/help1.html

[68] N. I. Sarkar and K. W. Sowerby, "Buffer unit multiple access (BUMA) protocol: an enhancement to IEEE 802.11b DCF," in *the IEEE Global Telecommunications Conference (GLOBECOM '05),* St. Louis, USA, 2005, pp. 2584-2588.

[69] K. Zhen-ning, D. H. K. Tsang, B. Bensaou, and G. Deyun, "Performance analysis of IEEE 802.11e contention-based channel access," *IEEE Journal on Selected Areas in Communications,* vol. 22, pp. 2095-2106, December 2004.

[70] K. Younggoo, F. Yuguang, and H. Latchman, "Design of MAC protocols with fast collision resolution for wireless local area networks," *IEEE Transactions on Wireless Communications,* vol. 3, pp. 793-807, 10 May 2004.

[71] L. Romdhani, N. Qiang, and T. Turletti, "Adaptive EDCF: enhanced service differentiation for IEEE 802.11 wireless ad-hoc networks," in *Proceedings IEEE Wireless Communications and Networking Conference*, 2003, pp. 1373-1378 vol.2.

[72] W.-Y. Lin and J.-S. Wu, "Modified EDCF to improve the performance of IEEE 802.11e WLAN," *Computer Communications,* vol. 30, pp. 841-848, 26 February 2007.

[73] Y. C. Lai, Y. H. Yeh, and C. L. Wang, "Dynamic Backoff Time Adjustment with Considering Channel Condition for IEEE 802.11e EDCA " *Information Networking,* vol. 5200, pp. 445-454, 2008.

[74] W. Jian-xin, S. MAKFILE, and J. Li, "A random adaptive method to adjust MAC parameters in IEEE802.11e WLAN," *Wireless Networks,* vol. 16, p. 629−634, 2009.

[75] R. Moraes, P. Portugal, F. Vasques, and R. F. Custodio, "Assessment of the IEEE 802.11e EDCA protocol limitations when dealing with real-time communication," *EURASIP Journal on Wireless Communications and Networking,* vol. 2010, April 2010.

[76] Y. Li and I. Chen, "Design and Performance Analysis of Mobility Management Schemes Based on Pointer Forwarding for Wireless Mesh Networks," *IEEE Transactions on Mobile Computing,* vol. PP, pp. 1-1, 2010.

[77] C. C. Liang, S. W. Pan, and J. S. Wu, "A Sustained QoS Solution by Contention Adaptation in IEEE 802.11e Wireless LANs," *WSEAS TRANSACTIONS on COMMUNICATIONS,* vol. 10, October 2011.

[78] O. Shagdar, K. Sakai, H. Yomo, A. Hasegawa, T. Shibata, R. Miura, *et al.*, "Throughput maximization and network-wide service differentiation for IEEE802.11e WLAN," in *International Conference on Communications and Information Technology (ICCIT), 2011*, 2011, pp. 43-46.

[79] K. Kosek-Szott, M. Natkaniec, and A. R. Pach, "A simple but accurate throughput model for IEEE 802.11 EDCA in saturation and non-saturation conditions," *Computer Networks,* vol. 55, pp. 622–635, February 2011.

[80] T. Sanada, X. Tian, T. Okuda, and T. Ideguchi, "Estimating the Number of Nodes in WLANs to Improve Throughput and QoS," *IEICE Transactions on Information and Systems*, vol. 99, pp. 10-20, 2016.

[81] I. Syed, S.-h. Shin, B.-h. Roh, and M. Adnan, "Performance Improvement of QoS-Enabled WLANs Using Adaptive Contention Window Backoff Algorithm," *Journal of IEEE Systems* vol. 12, pp. 3260 - 3270, December 2018.

[82] A. M. Mansoor, M. A. Al-Maqri, A. Q. Sabri, H. Jalab, A. W. A. Wahab, and W. kahtan Al-kopati, "A Feedback-based Admission Control Unit for QoS provision of video Transmission over WLANs," in *IEEE Computing and Communication Workshop and Conference (CCWC)*, 2017, pp. 1-6.

[83] S. Choi, J. Prado, N. Shankar, and S. Mangold, "IEEE 802.11 e contention-based channel access (EDCF) performance evaluation," in *IEEE International Conference on Communications*, 2003, pp. 1151-1156.

[84] S. Floyd and V. Jacobson, "Random Early Detection Gateways for Congestion Avoidance," *IEEE / ACM Transactions on Networking,* vol. 1, Aug. 1993 1993.

[85] F. Hoeksema, M. Heskamp, R. Schiphorst, and K. Slump, "A node architecture for disaster relief networking," in *The IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks.*, Baltimore, MD, USA 2005, pp. 577-584.

[86] A. Conte and P. Dauchy, "Method of enabling an emergency call in an IEEE 802.11e enabled wireless local area network," United States Patent, 2006.

[87] C. Lu-ming, O. Kazunori, K. Toshihiko, and C. Xing-yl, "Performance evaluation on IEEE 802.11e considering emergency calls in congested situation," *The Journal of China Universities of posts and telecommunications,* vol. 14, pp. 50-59, October 2007.

[88] S. Son, K.-J. Park, and E.-C. Park, "Medical-Grade Channel Access and Admission Control in 802.11 e EDCA for Healthcare Applications," *PloS one,* vol. 11, p. e0160052, 2016.

[89] M. Eiger, M. Elaoud, and R. RMorera, "Latency aware service opportunity window based scheduling," United States Patent, 2008.

[90] T. L. Sheu, Y. J. Wu, and B. Li, "A Generalized Channel Preemption Model for Multiclass Traffic in Mobile Wireless Networks," *IEEE Transaction vehicular Technology,* vol. 56, pp. 2723-2732, September 2007.

[91] Z. Jiazhen and C. C. Beard, "A Controlled Preemption Scheme for Emergency Applications in Cellular Networks," *IEEE Transactions on Vehicular Technology,* vol. 58, pp. 3753-3764, 2009.

[92] M. Balakrishnan, D. Benhaddou, and Y. Xiaojing, "CP-EDCA analysis under realistic wireless channel conditions," in *IEEE Military Communications Conference*, 2009, pp. 1-6.

[93] M. Balakrishnan, D. Benhaddou, Y. Xiaojing, and D. Gurkan, "Service preemptions for guaranteed emergency medium access in Wireless Sensor Networks," in *IEEE Conference on Military Communications (MILCOM)*, 2008, pp. 1-7.

[94] N. I. Sarkar, "The impact of transmission overheads on IEEE 802.11 throughput: analysis and simulation," *Journal of Selected Areas in Telecommunications (JSAT)*, vol. 2, pp. 49-55, 2011.

[95] L. Gelman, *Advances in electrical engineering and computational science* vol. 39: Springer Science & Business Media, 2009.

[96] Y. Kim, S. Choi, K. Jang, and H. Hwang, "Throughput enhancement of IEEE 802.11 WLAN via frame aggregation," in *IEEE 60th vehicular technology conference*, 2004, pp. 3030-3034.

[97] H. Lee, I. Tinnirello, J. Yu, and S. Choi, "A performance analysis of block ACK scheme for IEEE 802.11e networks," *Computer Networks,* vol. 54, pp. 2468-2481, 6 October 2010.

[98] O. Cabral, A. Segarra, F. Velez, A. Mihovska, and N. R. Prasad, "Optimization of multi-service IEEE802. 11e block acknowledgement," in *IEEE Radio and Wireless Symposium*, 2009, pp. 380-383.

[99] P. K. Hazra and A. De, "Performance analysis of IEEE 802.11 e EDCA with QoS enhancements through TXOP based frame-concatenation and block-acknowledgement," *Intl. J. Adv. Tech,* vol. 2, pp. 542-560, 2011.

[100] A. Saif, M. Othman, S. Subramaniam, and N. A. W. A. Hamid, "An enhanced A-MSDU frame aggregation scheme for 802.11 n wireless networks," *Wireless Personal Communications,* vol. 66, pp. 683-706, 2012.

[101] P. H. Azevêdo Filho, M. F. Caetano, and J. L. Bordim, "A packet aggregation mechanism for real time applications over wireless networks," *International Journal of Networking and Computing,* vol. 2, pp. 18-40, 2012.

[102] S. Kim and Y. Cho, "Adaptive transmission opportunity scheme based on delay bound and network load in IEEE 802.11 e wireless LANs," *Journal of applied research and technology,* vol. 11, pp. 604-611, 2013.

[103] M. M. S. Kowsar and S. Biswas, "Performance improvement of IEEE 802.11n WLANs via frame aggregation in NS-3," in *International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 2017, pp. 1-6.

[104] S. Seytnazarov and Y.-T. Kim, "QoS-Aware Adaptive A-MPDU Aggregation Scheduler for Voice Traffic in Aggregation-Enabled High Throughput WLANs," *IEEE Transactions on Mobile Computing*, vol. 16, pp. 2862-2875, 2017.

[105] J. Liu, M. Yao, and Z. Qiu, "Adaptive A-MPDU retransmission scheme with two-level frame aggregation compensation for IEEE 802.11 n/ac/ad WLANs," *Wireless Networks*, vol. 24, pp. 223-234, 2018.

[106] Z. Feng, G. Wen, Z. Zou, and F. Gao, "RED-TXOP scheme for video transmission in IEEE 802. 11e EDCA " in *IEEE International Conference on Communications Technology and Applications*, 2009, pp. 371-375.

[107] R. G. Sargent, "Validation and verification of simulation models," in *in Proceedings of the 36th Winter Simulation Conference*, 2004, pp. 17-28.

[108] S. K. Memon, N. I. Sarkar, and A. Al-Anbuky, "Multiple preemptive EDCA for emergency medium access control in distributed WLANs," *Wireless Networks*, vol. 23, pp. 1523-1534, 2017.

[109] F. Haoran and W. Yong, "A priority supported MAC protocol for emergency response wireless sensor networks," in *Emergency Management and Management Sciences (ICEMMS), 2011 2nd IEEE International Conference on*, 2011, pp. 854-857.

[110] G. Einicke, D. Dekker, and M. Gladwin, "A robust WLAN for survivable emergency communications," in *TENCON '97. IEEE Region 10 Annual ConferenceIEEE Proceedings of Speec and Image Technologies for Computing and Telecommunications. 10 Annual Conference*, 1997, pp. 101-104 vol.1.

[111] M. Graaf de, H. Berg Van Den, R. J. Boucherie, F. Brouwer, and I. Bruin De, "Easy Wireless: Broadband ad-hoc networking for emergency service," in *the Sixth Annual Mediterranean Ad Hoc Networking Workshop*, Corfu, Greece, 2007, pp. 32-39.

[112] B. Yong, D. Wencai, M. Zhengxin, S. Chong, Z. Youling, and C. Baodan, "Emergency communication system by heterogeneous wireless networking," in *the IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS)*, 2010, pp. 488-492.

[113] N. I. Sarkar and J. Gutierrez, "Revisiting the Issue of the Credibility of Simulation Studies in Telecommunication Networks: Highlighting the Results of a Comprehensive Survey of IEEE Publications," *IEEE Communications Magazine,* vol. 52, pp. 218-224, May 1 2014.

[114] Y.-Y. Choong, S. T. Dawkins, S. M. Furman, K. Greene, S. S. Prettyman, and M. F. Theofanos, "Voices of First Responders–Identifying Public Safety Communication Problems: Findings from User-Centered Interviews, Phase 1, Volume 1," 2018.

[115] M. L. Hutcheson, *Software testing fundamentals: Methods and metrics*: John Wiley & Sons, 2003.

[116] D. C. Salyers, A. D. Striegel, and C. Poellabauer, "Wireless reliability: Rethinking 802.11 packet loss," in *IEEE 9th International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2008, pp. 1-4.

[117] E. Rozner, A. P. Iyer, Y. Mehta, L. Qiu, and M. Jafry, "ER: Efficient retransmission scheme for wireless LANs," in *Proceedings of the 2007 ACM CoNEXT conference*, 2007, p. 8.

[118] Riverbed Technologies. *OPNET Modeler*. Retrieved on March 10, 2019 from www.opnet.com

[119] d. a. c. m. Policy, "International Federation of Red Cross and Red Crescent Societies," *Paris, May,* 2019.

[120] R. L. S. Fernando and M. D. Kumari, "Recovery After Disasters—Problems and Prospects: The Case of Koslanda-Meeriyabedda Landslide in Sri Lanka," in *Disaster Risk Reduction*, ed: Springer, 2019, pp. 335-356.

[121] S. Lynn. (2013, January 11, 2018). It's time for cities to deploy emergency Wi-Fi strategies. Available: https://www.pcmag.com/article2/0,2817,2417956,00.asp

[122] C. C. Yang, L. Jheng Sian, L. Ruei Yi, L. Shang-Yo, and W. Jyh-Horng, "QoS Performance Improvement for WLAN Using Priority Random Early Detection," *International Conference on Wireless Communications, Networking and Mobile Computing,* , pp. 1996-1999, 21-25 Septempter 2007.

[123] W. I. Pang and D. Chieng, "A Joint Measurement Based Admission and Bandwidth Control QoS Provisioning Shceme for WLANs," presented at the

International Conference on Frontiers of Communications, Networks and Applications (ICFCNA 2014 - Malaysia), Kuala Lumpur, 2014.

[124] Lyes Khoukh, Hakim Badis, Leila Merghem-Boulahia, and M. Esseghir, "Admission control in wireless adhoc networks: a survey," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, April 13 2013.

[125] R. Laufer and L. Kleinrock, "On the capacity of wireless CSMA/CA multihop networks," in *IEEE Proceedings of INFOCOM 2013* 2013, pp. 1312-1320.

[126] I. Std., "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification: Medium Access Control Quality of Service Enhancement, September 2005.," 2005.

[127] H. Security, "HSPD-8, Homeland Security Presendential Directives," 2011.

[128] J. Geier, "Testing a Wireless LAN," in *Designing and deploying 802.11n wireless networks* ed: Pearson Education, 2010, pp. 405-419.

[129] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, pp. 2347-2376, 2015.

[130] L. Oliveira, J. J. Rodrigues, S. A. Kozlov, R. A. Rabêlo, and V. H. C. d. Albuquerque, "MAC Layer Protocols for Internet of Things: A Survey," *Future Internet*, vol. 11, p. 16, 2019.

[131] Riverbed-Technologhy. *New Zealand based Riverbed Partners*. Retrieved on January 20, 2019 from https://partnerlocator.riverbed.com/?type=VAR&country=New+Zealand

[132] Z. Lu and H. Yang, *Unlocking the power of OPNET modeler*: Cambridge University Press, 2012.

[133] N. Chen, *WAN Optimization with Riverbed: 2018 Edition*. Independntly: Cambridge University Press, 2018.

[134] J. A. Allan Braga, Josiane Rodrigues, "Implementation of a New Propagation Model for 5.8GHz systems in OPNET Simulator," *European Conference on Antenna and Propagation*, vol. 2, 2013.

[135] W. J. Krzysztofik, "Radio Network Planning and Propagation Models for Urban and Indoor Wireless Communication Networks," in *Antennas and Wave Propagation*, ed: IntechOpen, 2018.