Protection and Security Aware QoS Framework for 4G Multihop Wireless Networks

by

Perumalraja Rengaraju, B.Eng., M.Eng.

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Electrical and Computer Engineering

Carleton University
Ottawa, Ontario

Abstract

The Worldwide interoperable for Microwave Access (WiMAX) and Long Term Evolution (LTE) standards have well-defined Quality of Service (QoS) and security architecture. However, the details of Radio Resource Management (RRM) components, such as Call Admission Control (CAC) and Packet Scheduling (PS), are still open research topics. Next, some security issues are not yet resolved in the WiMAX or LTE standards. Finally, the multihop networks fail to consider the performance degradation problem during relay nodes failure. Therefore, the main objectives of this research work are to: (1) develop a new RRM framework to address QoS, (2) provide stronger security without affecting QoS performance, and (3) maintain the QoS of the network in the case of relay nodes failure.

In terms of QoS, the proposed CAC in the Base Station (BS) reserves the bandwidth adaptively based on most recent requests from high priority users. When the reserved bandwidth is not fully used, the remaining bandwidth is allocated to least priority users for effective bandwidth utilization. Later, the CAC applies bandwidth pre-emption on least priority users to admit high priority users. Further, the PS scheme uses the (Priority + Earliest Due Date) scheduler to improve the multihop latency and dynamically switches to the (Priority + Token Bucket) scheduler during the CAC scheme is applied to bandwidth pre-emption on the least priority calls to ensure the bandwidth for high priority users. The proposed CAC and PS methods outperform the existing schemes where the QoS performance is verified by system level simulations.

Secondly, to provide strong security without affecting the QoS performance, distributed security architecture using Elliptic Curve Diffie-Hellman (ECDH) protocol is proposed. For the WiMAX networks, the proposed security scheme is verified using simulation and compared with existing security using testbed implementation. For LTE networks, a theoretical analysis of the proposed scheme is described where similar performance could be achieved.

Finally, the design with network coding on 4G multihop networks maintains the QoS of the network even in the case of relay nodes failure. The simulation results for multihop WiMAX networks show that the Packet Delivery Ratio (PDR) is the same for both Relay Station (RS) failure scenario and without RS failure scenario. However, latency performance is slightly increased during relay node(s) failure.

Acknowledgements

Though only my name appears on the cover of this dissertation, a great many people have contributed to its production. I owe my gratitude to everyone and because of them my graduate experience has been one that I will cherish forever.

I would like to thank Carleton University and the Systems and Computer Engineering department for giving me the opportunity and financial assistance to pursue the PhD program.

My deepest gratitude is to my advisor, Prof. Chung-Horng Lung. I have been amazingly fortunate to have an advisor who gave me the freedom to explore, and at the same time the guidance to recover when my steps faltered. I am grateful to him for holding me to a high research standard and enforcing strict validations for each research result, and thus teaching me how to do the research. Actually, there are no words to describe about his knowledgeable guidance, extremely helpful comments to improve my writing and moral support during my tough time.

I am very thankful to my co-advisor Dr. Anand Srinivasan for his invaluable technical assistance, moral support and motivation, throughout the course of this work. Right from the beginning, Dr. Anand Srinivasan helped me to select the research area, based on the recent trends in wireless technologies.

I would also like to thank Dr. Kalai Kalaichelvan, the CEO of EION wireless Inc., for providing the financial support for WiMAX research project and giving the opportunity to conduct the research in EION Inc. Without the help of Dr. Kalai Kalaichelvan and Dr. Anand Srinivasn I may not get a chance to do my PhD in Carleton University.

The financial support from EION Inc., Ontario Centres of Excellence (OCE), and Natural Sciences and Engineering Research Council of Canada (NSERC) is greatly appreciated that encouraged me to do the research at the Carleton University.

Finally, I want thank my parents, wife and other family members. Without their endless support and encouragement, I will never have finished my study.

Table of Contents

List of Tables ..... **i**

List of Figures ..... **iii**

List of Abbreviations ..... **vi**

List of Symbols or Terminologies ..... **xiii**

Chapter 1. Introduction **1**

1.1. Problem Statements and Proposed Schemes 2

1.1.1. RRM Challenges in 4G Multihop Wireless Networks 3

1.1.2. Security Threats and QoS Aware Solution for 4G Wireless Networks 6

1.1.3. QoS Issues for Relay Node Failure in 4G Multihop Wireless Networks 7

1.2. Contributions 9

1.3. Thesis Outline 10

Chapter 2. The 4G wireless standards – Overview **12**

2.1 Introduction to 4G Broadband Wireless Access Networks 12

2.1.1 Evolution of WiMAX Networks 12

2.1.2 Evolution of LTE networks 15

2.1.3 Implementation Scenarios 18

2.1.4 Physical (PHY) Layer 20

2.1.4.1 OFDM PHY 22

2.1.4.2 OFDMA PHY 23

2.1.5 WiMAX MAC Layer 25

2.1.5.1 Service Specific Convergence Sublayer 26

2.1.5.2 Common Part Sublayer 27

2.1.6 LTE – MAC and Higher Layers 32

2.1.6.1 LTE Channel Types 34

2.1.6.2. LTE OFDMA Frame Format 36

2.1.6.3. Synchronization and Network Entry 37

2.2 QoS Framework in WiMAX and LTE 38

2.2.1 Service Classes and Bandwidth Request Support in WiMAX Standards 40

2.2.2 Service Flows in LTE Standards....41
2.2.3 MAC Layer QoS Framework and QoS Provisioning....42
2.3 Security Architecture in WiMAX and LTE Standards....46
2.3.1. Security Support in Mobile WiMAX Networks....46
2.3.2. Security Support in Multihop WiMAX Networks....48
2.3.3. Security Support in LTE Networks....49
2.3.4. Security Support in Multihop LTE Networks....52
2.4. Network Coding for 4G wireless networks....52
2.4.1. XOR Network Coding....53
2.4.2. Reed-Solomon based Network Coding....54
2.4.3. Random Linear Network Coding....54

Chapter 3. Literature Review....56
3.1 Literature Review of RRM Framework in 4G Wireless Networks....56
3.1.1 Literature Review of RRM Framework in WiMAX Networks....56
3.1.1.1. Literature Review of CAC in WiMAX Networks....56
3.1.1.2. Literature Review of Packet Scheduling Scheme in WiMAX Networks....59
3.1.2 Literature Review of RRM Framework in LTE Networks....62
3.2 Literature Review of WiMAX and LTE Networks Security....63
3.2.1. Literature Review of WiMAX Network Security....63
3.2.2. Literature Review of LTE Network Security....67
3.3 Literature Review of Relay Node Protection in Multihop Wireless Networks....69

Chapter 4. Radio Resource Management Framework for 4G Wireless Networks....71
4.1 Problem Statement and Objectives....71
4.2 Adaptive CAC for 4G Multihop Wireless Networks....72
4.3 Scheduling Algorithms for 4G Multihop Wireless Networks....80
4.4 System Modeling and Performance Evaluation....82
4.5. Performance Evaluation of CAC and PS Schemes in 4G Wireless Networks....94
4.5.1. Simulation Environments and Parameter Settings....94
4.5.2. Performance Evaluation of Proposed and Conventional CAC Schemes....99
4.5.3. Performance Evaluation of Downlink Scheduling Schemes....103

4.5.4. Performance Evaluation of Uplink Scheduling Schemes 113
4.6 Chapter Summary 121

Chapter 5. QoS Aware Security Architecture for 4G Multihop Wireless Networks 123
5.1 Problem Statement 123
5.2 Security Threats in WiMAX and LTE Networks 124
5.2.1. Common Security Threats in WiMAX and LTE Networks 124
5.2.2. Security Threats in WiMAX Networks 127
5.2.3. Security Threats in LTE Networks 128
5.3 Proposed Distributed Security Architecture 129
5.3.1. Secured, Initial Ranging in WiMAX / Random Access procedure in LTE 129
5.3.2. Distributed Security using ECDH in Multihop WiMAX 131
5.3.3. Neighbour Authentication and SA 132
5.4 Performance Evaluation of Conventional and the Proposed Security Schemes in WiMAX 134
5.4.1. Performance of IPsec and Basic Security using Testbed Study 134
5.4.2. Performance Evaluation of ECDH Scheme using Simulation 139
5.4.3. Security Analysis 141
5.4.3.1. Analysis on ECDH Protocol against Security Threats in WiMAX 141
5.4.3.2. Analysis on ECDH Protocol against Security Threats in LTE Networks 142
5.4.3.3. Analysis on ECDH Protocol against Pollution and Entropy Attacks 143
5.4.3.4. Comparison of Different Security Schemes 144
5.5 Chapter Summary 145

Chapter 6. Protection Schemes for 4G Multihop Wireless Networks 147
6.1 Problem Statement 147
6.2 Relay Node Protection Using Network Coding 148
6.2.1. Protection for Single Relay Node Failure 150
6.2.2. Protection for Two (multiple) Relay Nodes Failure 151
6.3. Performance Evaluation of Relay Node Protection using Network Coding 152
6.4 Chapter Summary 165

Chapter 7. Conclusion and Future Directions 167

7.1. Future Directions 169

References 170

List of Tables

Table 2.1 IEEE802.16 Service Classes and its QoS Parameter [1], [52] 40
Table 2.2 QCI Mapping in LTE [12] 41
Table 2.3 Homogeneous Scheduling Algorithms 45
Table 3.1 Performance Analysis of Existing Schedulers [52] 61
Table 3.2 Security Threats in WiMAX Networks 65
Table 3.3 Security Threats in LTE Networks 67
Table 4.1 WiMAX and LTE Service Flow Mapping 73
Table 4.2 WiMAX System Parameters 94
Table 4.3 LTE System Parameters 95
Table 4.4 Common Parameters for WiMAX and LTE Networks Simulation 95
Table 4.5 Traffic QoS Specification [23] 96
Table 4.6 VoIP Traffic Model [114] 97
Table 4.7 Video Conference Traffic Model [114] 97
Table 4.8 Video Streaming Traffic Model [114] 97
Table 4.9 Web Browsing Traffic Model [114] 97
Table 4.10 The PDR Performance, CI Values for the Proposed PS Scheme in WiMAX 107
Table 4.11 The Delay Performance, CI Values for the Proposed PS Scheme in WiMAX 110
Table 4.12 Jitter at Various Loads in WiMAX Network 111
Table 4.13 QoS factor for Various Schedulers in WiMAX Network 112
Table 4.14 PDR with CI Values for the (P+TB) Scheduler in WiMAX Uplink 117
Table 4.15 Delay with CI Values for the (P+TB) Scheduler in WiMAX Uplink 120
Table 5.1 Symbols and parameters used in Messages for Secured Initial Ranging 130
Table 5.1 Testbed - System Parameters 135
Table 5.2 IPSec Configuration and Status Verification 135
Table 5.3 SS Connectivity Time in Testbed Study 136
Table 5.4 System Parameters for Simulation Study 140
Table 5.5 Initial Connectivity Latency in Simulation Study 140

Table 5.6 Performance Analysis of Different Security Schemes in WiMAX and LTE . 144
Table 6.1 System Parameters for Wireless Mesh Networks Simulation..... 153
Table 6.2 System Parameters for WiMAX Networks Simulation 153

List of Figures

Figure 2.1 IEEE 802.16 standard protocol layering [1] 13
Figure 2.2 WiMAX Network Reference Model [4] 14
Figure 2.3 3GPP technical specification group [12] 16
Figure 2.4 LTE-SAE network architecture [17] 17
Figure 2.5 Point-to-Point and Point-to-Multipoint WiMAX network 18
Figure 2.6 Mobile WiMAX network 19
Figure 2.7 Multihop WiMAX network 19
Figure 2.8 OFDM transmitter and receiver [18] 22
Figure 2.9 OFDM symbol -time domain representation [1] 22
Figure 2.10 Frequency domain representation of OFDM symbol [1] 23
Figure 2.11 Example of a data region that defines an OFDMA allocation [1] 24
Figure 2.12 IEEE802.16 protocol stack and its functions 25
Figure 2.13 Classification and CID mapping (BS to SS) [1] 26
Figure 2.14 Initial ranging and network entry procedures [1] 28
Figure 2.15 OFDMA-TDD frame structure in IEEE802.16e [1] 30
Figure 2.16 OFDMA-TDD frame structure in IEEE802.16j [2] 31
Figure 2.17 LTE user and control plane protocol [17] 32
Figure 2.18 Downlink OFDMA frame structure in LTE [17] 37
Figure 2.19 LTE-SAE bearer establishments [17] 39
Figure 2.20 WiMAX and LTE QoS architecture 42
Figure 2.21 Reference models for RRM: (a) split RRM (b) integrated RRM [7] 43
Figure 2.22 Initial ranging and network entry in mobile WiMAX [1] 47
Figure 2.23 Authentication and SAs during UE's network entry in LTE 50
Figure 2.24 (a) Traditional packet forwarding (b) Network coding [8] 53
Figure 2.25 RS codeword [19] 54
Figure 3.1 Parameter based CAC classification [20] 57
Figure 4.1 Flow chart of proposed CAC 75

Figure 4.2 Delay requirement timing diagram 78
Figure 4.3 Time and frequency domain scheduling in LTE..... 80
Figure 4.4 The (P+E) scheduler 81
Figure 4.5 The (P+TB) scheduler..... 82
Figure 4.6 Markov chain associated to the bandwidth reservation scheme 87
Figure 4.7 The CBP for approximations 1 and 2 for a system with C = 12, T = 6 90
Figure 4.8 The CDP for approximations 1 and 2 for a system with C = 12, T = 6..... 90
Figure 4.9 The CDP performance comparison for a system with C = 16, T = 8, λ_{nRT}=10 91
Figure 4.10 The CBP performance comparison for a system with C=16, T=8, λ_{nRT}=10... 92
Figure 4.11 The CDP performance comparison for a system with C=16, T= 8, λ_{nRT}=1 ... 92
Figure 4.12 The CBP performance comparison for a system with C=16, T=8, λ_{nRT}=1..... 93
Figure 4.13 Performance of CAC for WiMAX networks in first scenario 100
Figure 4.14 Performance of CAC for LTE networks in first scenario 100
Figure 4.15 Performance of CAC for WiMAX networks in second scenario 102
Figure 4.16 Performance of CAC for LTE networks in second scenario 102
Figure 4.17 PDR performance for the voice application..... 104
Figure 4.18 PDR performance for the video conference application..... 105
Figure 4.19 PDR performance for the video streaming application..... 106
Figure 4.20 PDR performance for the HTTP application 106
Figure 4.21 Average delay for the voice application 108
Figure 4.22 Average delay for the video conference application..... 109
Figure 4.23 Average delay for the video streaming application 109
Figure 4.24 Average delay for the HTTP application..... 110
Figure 4.25 PDR for the voice application in WiMAX uplink 114
Figure 4.26 PDR for the video conference application in WiMAX uplink 115
Figure 4.27 PDR for the video streaming application in WiMAX uplink 115
Figure 4.28 HTTP call PDR performance in WiMAX uplink 116
Figure 4.29 Average delay for the voice application in WiMAX uplink..... 118
Figure 4.30 Average delay for the video conference application in WiMAX uplink..... 118

Figure 4.31 Average delay for the video streaming application in WiMAX uplink 119
Figure 4.32 Average delay for the HTTP application in WiMAX uplink 119
Figure 5.1 Intra-flow and inter-flow network coding [8] 126
Figure 5.2 Initial ranging and connectivity using ECDH protocol 129
Figure 5.3 Distributed security architecture in WiMAX using ECDH 132
Figure 5.4 Neighbour authentication using ECDH protocol 133
Figure 5.5 IPSec testbed setup – connection diagram 134
Figure 5.6 Testbed measurements – Throughput performance 136
Figure 5.7 Testbed measurements – Frame loss performance 137
Figure 5.8 Testbed measurements – Latency performance 138
Figure 6.1 Multihop relay network architecture – WiMAX/LTE 149
Figure 6.2 Network model - Protection for single relay node failure 150
Figure 6.3 Network model - Protection for two relay node failures 152
Figure 6.4 PDR for single relay node protection scenarios in WMN 156
Figure 6.5 PDR for two relay nodes protection scenarios in WMN 157
Figure 6.6 PDR for single RS protection scenarios in WiMAX network 157
Figure 6.7 PDR for two RSs protection scenarios in WiMAX network 158
Figure 6.8 Latency for single relay node protection scenarios in WMN 159
Figure 6.9 Latency for two relay nodes protection scenarios in WMN 160
Figure 6.10 Latency for one RS protection scenarios in WiMAX network 161
Figure 6.11 Latency for two RSs protection scenarios in WiMAX network 162
Figure 6.12 Jitter for single relay node protection scenarios in WMN 163
Figure 6.13 Jitter for two relay nodes protection scenarios in WMN 163
Figure 6.14 Jitter for single relay node protection scenarios in WiMAX 164
Figure 6.15 Jitter for single relay node protection scenarios in WiMAX 164

List of Abbreviations

ACK	Acknowledgement
ADC	Analog to Digital Conversion
AES	Advanced Encryption Standard
AK	Authorization Keys
ARP	Allocation and Retention Priority
ARQ	Automatic Repeat reQuest
AS	Access Stratum
ASN	Access Network
BCCH	Broadcast Control Channel
BCH	Broadcast Channel
BE	Best Effort
BS	Base Station
BW	Bandwidth
BWA	Broadband Wireless Access
CAC	Call Admission Control
CBP	Call Block Probability
CDP	Call Drop Probability
CID	Connection Identifier
CMAC	Cipher based Message Authentication Code
CN	Core Network
CPS	Common Part Sublayer
CQI	Channel Quality Indicator
CQICH	Channel Quality Indicator Channel
CRNTI	Cell Radio Network Temporary Identifier
CS	Convergence Sublayer
CSN	Connectivity Service Network
DAC	Digital to Analog Conversion
DBA	Dynamic Bandwidth Allocation

DCD	Downlink Channel Descriptor
DeNB	Donor evolved Node-B
DFPQ	Deficit Fair Priority Queuing
DFT	Discrete Fourier Transform
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DHS	Dynamic Hybrid Scheduler
DL	Downlink
DMSI	Dynamic Mobile Subscriber Identity
DoS	Denial of Service
DRR	Deficit Round Robin
DSA	Dynamic Service Addition
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Loop
DWRR	Deficit Weighted Round Robin
EAP	Extensive Authentication Protocol
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
EDD	Earliest Due Date
EDF	Earliest Deadline First
EPC	Evolved Packet Core
EPS	Evolved Packet System
FBSS	Fast Base Station Switching
FCH	Frame Control Header
FD	Frequency Domain
FDD	Frequency Division Duplexing
FFT	Fast Fourier Transform
FIFO	First In First Out
FL	Frame level
GBR	Guaranteed Bit Rate

GC	Guard Channel
GKEK	Group Key Encryption Key
GPC	Grant Per Connection
GTEK	Group Traffic Encryption Key
HA	Home Agent
HARQ	Hybrid Automatic Repeat reQuest
HE	Home Element
HMAC	Hashed Message Authentication Code
HOL	Head of Line
HSDPA	High Speed Downlink Packet Access
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HSUPA	High Speed Uplink Packet Access
ICIC	Inter Channel Interference Cancellation
IDU	In-Door Unit
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IMT	International Mobile Telecommunications
IP	Internet Protocol
ISAKMP	Internet Security Association and Key Management Protocol
ISI	Inter-Symbol Interference
ISP	Internet Service Providers
ITU	International Telecommunication Union
KEK	Key Encryption Key
LEAP	Lightweight Extensible Authentication Protocol
LoS	Line of Sight
LPF	Local Policy Functions
LTE	Long Term Evolution
MAC	Medium Access Control
MAU	Minimum Allocation Unit

MBAC	Measurement based Admission Control
MBR	Maximum Bit Rate
MBS	Multicast Broadcast Service
MCCH	Multicast Control Channel
MCS	Modulation Coding Scheme
MDHO	Macro Diversity Hand Over
MIB	Master Information Block
MIMO	Multiple Input Multiple Output
MIP	Mobile IP
MME	Mobility Management Entity
MOS	Mean Opinion Score
MS	Mobile Stations
MSK	Master Session Key
NAP	Network Access Providers
NAS	Non-Access Stratum
NCMS	Network Control and Management Systems
NMS	Network Management System
NPC	Network Protection Codes
NRM	Network Reference Model
NSP	Network Service Providers
ODU	Out-Door Unit
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
ORS	OFDMA Relay Scheduler
PAP	Password Authentication Protocol
PAPR	Peak-to-Average Power Ratio
PBAC	Parameter Based Admission Control
PBCH	Physical Broadcast Channel
PCFICH	Physical Control Format Indicator Channel
PDCCH	Physical Downlink Control Channel

PDCP	Packet Data Control Protocol
PDR	Packet Delivery Ratio
PDU	Protocol Data Units
PF	Proportional Fair
PHY	Physical
PHS	Payload Header Suppression
PLR	Packet Loss Rate
PMP	Point-to-Point, Point-to-Multipoint
PRB	Physical Resource Blocks
PS	Packet Scheduling
PSS	Primary Synchronization Sequence
PUSCH	Physical Uplink Shared Channel
QCI	QoS Class Identifiers
QoE	Quality-of-Experience
QoS	Quality of Service
RB	Radio Bearers
RF	Radio Frequency
RLC	Radio Link Control
RLNC	Random Linear Network Coding
RNC	Radio Network Controller
RR	Round Robin
RRA	Radio Resource Agent
RRC	Radio Resource Control
RRM	Radio Resource Management
RS	Relay Station
RSA	Rivest Shamir and Adleman
RTG	Receive/transmit Transition Gap
SA	Security Association
SAE	System Architecture Evolution
SAID	Security Association Identity

SAP	Service Access Points
SDU	Service Data Units
SecS	Security Sublayer
SFID	Service Flow Identifier
SIB	System Information Blocks
SIM	Subscriber Identity Module
SLA	Service Level Agreements
SMC	Security mode command
SN	Serving Network
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SS	Subscriber Stations
SSS	Secondary Synchronization Sequence
SZ	Security Zone
TB	Token Bucket
TD	Time Domain
TDD	Time Division Duplexing
TDMA	Time Division Multiple Access
TEK	Transport Encryption Key
TFTP	Trivial File Transfer Protocol
TSG	Technical Specifications Groups
TTG	Transmit/receive Transition Gap
TTI	Transmission Time Interval
TTP	Trusted third party
TUSC	Tile Usage SubChannel
UCD	Uplink Channel Descriptor
UE	User Equipment
UGS	Unsolicited Grant Service
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module

UTRA	Universal Terrestrial Radio Access
VPN	Virtual Private Networks
WCDMA	Wideband Code Devision Multiple Access
WFQ	Weighted Fair Queuing
WiMAX	Worldwide interoperable for Microwave Access
WMAN	Wireless Metropolitan Area Network
WMN	Wireless Mesh Networks
WPKI	Wireless Public Key Infrastructure
WRR	Weighted Round Robin
WSN	Wireless Sensor Networks

List of Symbols or Terminologies

f : OFDMA frame duration (msec) in WiMAX/LTE

C: total bandwidth capacity (i.e., system capacity)

SC_i : i^{th} Service Class

$B_{SC1}, B_{SC2}, B_{SC3}$ and B_{SC1}: bandwidth allocated to SC_1, SC_2, SC_3 and SC_4 calls, respectively

$B^{NC}$and B^{HC}: total bandwidth allocated to normal calls and high priority calls, respectively

B_t: total bandwidth allocated for the SC_1, SC_2, SC_3 and SC_4 calls

d_i : maximum latency/delay requirement of connection i (ms)

l_i : modified latency, which includes multihop delay (ms)

b_i : bandwidth required for connection i

r_i : token (packet) arrival rate of a connection i (Kbps)

TB_i : token bucket size of a connection i (Kbits)

T: bandwidth reservation threshold for handoff users

$m_i = d_i$ /f , m_i must be an integer

r_n *:* number of real-time (SC_2) connections admitted into the network

n_n *:* number of non-real-time (SC_3) connections admitted into the network

u_n : number of voice (SC_1) connections admitted into the network

λ_H, λ_{nRT} and λ_{BE} : the average arrival rate for handoff, nRT and BE calls, respectively.

μ_H, μ_{nRT} and μ_{BE} : the average service rate for handoff, nRT and BE calls, respectively.

$S_1 = \{(n_1, n_2, n_3)\}$: State space of the Markov chain with the system of (n_1, n_2, n_3) where n_1, n_2 and n_3 are the number of handoff, nRT and BE calls, respectively.

Chapter 1. Introduction

Traditional wireless telecommunication networks are based on cellular architecture, where many Mobile Stations (MSs) or fixed wireless terminals (Subscriber Stations (SSs)) communicate directly with a single Base Station (BS). The BS is usually connected to the public telecommunication infrastructure. In cellular based communication architecture, there has been an evolutionary improvement in the Quality of Service (QoS) offered to the user as we see a growth of progressive generations of cellular systems. The evolution began with the First Generation (1G) for analog voice systems, followed by the Second Generation (2G) for digital voice systems, and then the current Third generation (3G) for low and medium rate data systems. Now, the 3G Partnership Project (3GPP) and IEEE standards are working on Fourth Generation (4G) to deliver a high data rate with appropriate QoS support for the tremendous use of multimedia applications. The key differences between 3G and 4G technologies are the improved data transfer rate, security and high mobility support found in 4G technologies for multimedia applications [8]. Hence, the Internet Service Providers (ISPs) are interested in 4G technologies, such as Worldwide interoperability for Microwave Access (WiMAX) and Long Term Evolution (LTE) for the internet and multimedia services.

The most important objective of delivering a multimedia service is the satisfaction of end users, that is, the Quality-of-Experience (QoE) [24]. This is strictly related to the systems' ability to deliver an application with suitable QoS. The QoE is also a consequence of a user's internal state, the characteristics of the designed system and the environment within which the service is experienced. QoE can be measured by both subjective and objective measurements [25]. The subjective measurements are related to how the user experiences the application and the objective measurements are the QoS parameters that are related to subjective measurement such as E2E delay, etc. The human perception for the subjective measurement is usually captured by a Mean Opinion Score (MOS) that includes expectations and ambiance. The MOS is expressed on a five point scale (International

Telecommunication Union –TP.800), where 5 = excellent, 4 = good, 3 = fair, 2 = poor, 1= bad [24]. Alternatively, the QoE for an individual application is calculated through objective measurements. The importance of QoE and how the QoS and QoE can be monitored by the ISPs in 4G wireless networks is described in [117].

Maintaining constant QoE at the customer end is a major task for the service providers. Hence, strong End-to-End (E2E) QoS support and QoS differentiation between different service flows are mandatory for 4G wireless networks. Therefore, providing QoS support is one of the fundamental parts of the Medium Access Control (MAC) layer design in WiMAX and LTE standards. The QoS framework in WiMAX standards defines five different service classes and LTE standards define nine QoS Class Identifiers (QCIs) for different multimedia applications and basic connectivity [1, 9]. Also, the recent WiMAX and LTE standards introduce Relay Station (RS) nodes to maintain high signal strength and extended network coverage. On the other hand, ensuring the QoS in multihop networks including multihop delay requirement and reliability of the communication are the major challenges for service providers. Therefore, a proper Radio Resource Management (RRM) framework is needed for the 4G multihop wireless networks to ensure the QoS of different provisioned connections. Furthermore, providing QoS aware strong security for E2E communication is another challenge for the service providers. The detailed description of QoS challenges, security threats and reliability in 4G multihop wireless networks is as follows.

1.1. Problem Statements and Proposed Schemes

Traditionally, the most significant challenges for wireless systems are sending a large volume of information over long distance, and providing support for multimedia applications and spectrum limitations. Hence, the 4G technologies aim at overcoming these limitations by enhancing the physical (PHY) layer throughput using the available spectrum and by adding QoS support in the MAC layer for multimedia applications. By adding QoS support, the most challenging problems that arise at the MAC layer are dealing with QoS

and QoS differentiation between service classes, resource allocation and resource reservation [21]. If the network is multihop in nature, the additional MAC layer challenges are assuring the QoS, including delay requirements and security. Therefore, the motivation of this research work is to provide a strong solution for QoS and security challenges, which is more beneficial for device vendors and ISPs.

In this section, the practical challenges on QoS and security support in 4G wireless networks are explored that motivated for this research. First, the challenges in designing a RRM framework to ensure QoS differentiation among different service flows are discussed. Next, the selection between centralized and distributed security schemes and various security threats in 4G multihop wireless networks are described. Finally, the QoS issue during relay node failure in 4G multihop wireless networks is considered.

1.1.1. RRM Challenges in 4G Multihop Wireless Networks

In general, the major challenge in designing the QoS framework for wireless access networks is balancing two sets of objectives: one for the end users and the other for the service providers. End users expect to get QoS support for their connections, while the service providers would like to improve system utilization and revenue by admitting more connections. To achieve this, an effective RRM framework design needs to satisfy both parties by fully utilizing the network resources efficiently [21]. The RRM framework consists of Local Policy Functions (LPF), CAC, Dynamic Bandwidth Allocation (DBA), Packet Scheduling (PS), handoff, load control, and power control to control the usage of radio resources. However, the QoS mainly depends on CAC and PS methods, because both are aimed at distributing all the available resources, while keeping the QoS requirements of both real-time and non-real-time applications at an acceptable level. The CAC and PS design challenges in 4G multihop wireless networks and proposed schemes to meet the challenges are as follows:

a. CAC design challenges:

The design of CAC for a fixed network is simple, where the call admission is based on the available resources and QoS requirements of the new calls. However, the mobile environment is more complicated than the fixed network, where the BS may reserve some bandwidth to admit the handoff calls. If the BS reserves some bandwidth for handoff calls and the network happens to have few or no handoff calls, then those resources may be wasted or underutilized. On the other hand, if the BS allocates minimum resources for handoff calls, then some handoff calls may be dropped. Hence, the decision of how much bandwidth the BS reserves for handoff calls is a challenging task [35]. Similarly, the amount of bandwidth reservation for real-time high priority service classes is another challenge in the CAC design. Further, the CAC design challenges for multihop networks are verification of E2E delay requirements of the multihop nodes.

b. Packet scheduler design challenges:

Once a call has been admitted by the CAC module, the DBA module should allocate the resources based on the connection's QoS provisioning and the available bandwidth resources [22]. The major challenge in DBA and PS is QoS differentiation and QoS assurance. The PS design challenges are:

- Handling both real-time and non-real-time service flows during busy traffic periods is challenging. Certain schedulers, such as priority and revenue based schedulers, always allocate resources to real-time applications first to give more priority for real-time services. Then, the non-real-time applications may be starving for bandwidth during busy traffic periods. On the other hand, if the scheduler allocates more resources to non-real-time applications, then real-time services are highly affected.

- Consider a scenario as an example: Two packets arrive at the BS at the same time that belongs to two different users with the same QoS requirement. If the scheduler allocates bandwidth resources to the single-hop user first, then the delay performance of the multihop user is highly affected. Hence, handling packets for single-hop and multihop users is another challenge for the scheduling function.

c. Proposed solutions:

In WiMAX and LTE standards, there are some similarities in PHY layer transmission (frame based transmission, Multiple Input Multiple Output (MIMO) and Orthogonal Frequency Division Multiplexing (OFDM) support) and similar QoS support at the MAC layer [26]. Hence, it is possible to use the same CAC and PS algorithms for both WiMAX and LTE networks. To solve bandwidth reservation challenges, an adaptive CAC is proposed for the multihop BS. The centralized CAC in the BS reserves some bandwidth for mobile and high priority real-time users, and changes the bandwidth reservation adaptively based on the most recent status of handoff and high priority real-time users. Suppose, the reserved bandwidth is not fully utilized by handoff and high priority real-time users, the remaining reserved bandwidth is then allocated for least priority users for effective bandwidth utilization. Later, when a high priority or handoff user arrives, the CAC pre-empt the least priority calls to admit the high priority calls. However, while admitting new calls or handoff calls, the CAC verifies both bandwidth and multihop delay requirements to satisfy the QoS of the call.

For the proposed PS scheme, the BS initially use the (P+E) scheduler that combines Priority and Earliest Due Date (EDD) scheduling methods and dynamically selects the (P+TB) scheduler that combines the Priority and Token Bucket (TB) scheduling methods. The (P+E) scheduler considers the multihop scheduling latency to improve the delay performance of the multihop users. However, when the system is overloaded by admitting handoff and high priority users through bandwidth pre-emption, the QoS performance of the voice and the real-time services are affected in (P+E) scheduler. On the other hand, the (P+TB) scheduler assures bandwidth provisioning for voice and real-time connections, only the least priority users are getting affected. Hence, during overload condition, the BS selects the (P+TB) scheduler to ensure QoS differentiation.

1.1.2. Security Threats and QoS Aware Solution for 4G Wireless Networks

Basically, the 4G wireless networks have well defined security architectures. The security support at the WiMAX security sublayer and the LTE Packet Data Control Protocol (PDCP) layer are to: (i) authenticate the user when the user enters into the network; (ii) authorize the user, if the user was provisioned by the network service provider; and then (iii) provide the necessary encryption support for key transfer and data traffic [1, 14].

WiMAX and LTE resemble each other in some key aspects, including operating frequency spectrum, high capacity, mobility, strong QoS mechanisms, and strong security with a similar key hierarchy from core network to access network. However, they differ from each other in certain aspects as they evolved from different origins [18]. Since the LTE evolved from 3GPP, the LTE network has to support the existing 3G users' connectivity, but for WiMAX there is no such constraint. Particularly, on the security aspect, the WiMAX authentication process uses either Extensive Authentication Protocol - Tunnelled Transport Layer Security (EAP-TTLS) or Extensive Authentication Protocol - Transport Layer Security (EAP-TLS) that allows enterprise customers to use X-509 certificates, which contain an enterprise controlled username or password. On the other hand, due to the telecom consumer market and usage in 3G, the LTE authentication process uses EAP- Authentication and Key Agreement (EAP-AKA) procedure, which only authenticate International Mobile Subscriber Identity (IMSI) that was stored in a Subscriber Identity Module (SIM) card. Hence, the LTE security cannot meet the enterprise security requirement, as they cannot authenticate multiple security credentials, such as identity, certificates, and usernames/passwords [26].

Even though the authentication procedure is different between WiMAX and LTE, the security key hierarchy for the encryption support from the core network to the access network is similar. Also both WiMAX and LTE use symmetric key encryption, where WiMAX uses either Advanced Encryption Standard (AES) or 3-Digital Encryption Standard (3DES) [1] and LTE uses either AES or SNOW 3G [14]. However, the introduction of the relay node increases the security threats between BS and user nodes.

Therefore, strong security is needed to solve existing security threats, without affecting the QoS performance.

a. Security threats and existing solution in WiMAX and LTE networks:

In WiMAX networks, security threats, such as Denial of Service (DoS), that exist before authentication are due to unprotected MAC management messages [86]. Similarly, DoS attacks and identity privacy vulnerability due to disclosure of IMSI exist in LTE networks [90]. Next, the multihop WiMAX standard introduces the optional distributed security mode and tunnel mode operations. The distributed security mode provides hop-by-hop authentication, but multihop RSs may not use the tunnel mode operation as they do not have Security Association (SA) with the BS. Finally, the recent research works in multihop WiMAX and LTE networks use network coding for QoS improvement that leads to network coding security threats. On the other hand, ISPs may use the Internet Protocol Security (IPSec) for the wireless access due to its popularity in wired networks [91],[92]. On the other hand, IPSec will affect the QoS performance, because the IPSec header in each packet consumes additional bandwidth.

b. Proposed solutions:

In existing research efforts, there is a lack of the integrated presentation and solution for WiMAX and LTE network security issues. It is necessary to analyze both WiMAX and LTE for network convergence that is useful for service providers. For the existing security threats in 4G wireless networks, the distributed security architecture using Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol is proposed. Moreover, security and QoS performance is compared for the proposed security scheme with IPSec and the security scheme as defined by the standards.

1.1.3. QoS Issues for Relay Node Failure in 4G Multihop Wireless Networks

In general, the wireless medium is prone to various types of interferences that cause a wireless link status to dynamically change according to the channel condition. Also, the channel condition may vary due to users' mobility. Hence, information loss and the

reliability may further deteriorate in multihop communications. In such scenarios, the physical layer error correction codes and packet retransmission techniques may help to overcome the problem of information loss. On the other hand, sometime a relay node may fail unexpectedly or the relay node's connections may go down for management purposes such as, software upgrades. If the channel goes down for a considerable amount of time, packet retransmission techniques and the physical layer error correction codes will not be able to recover the information loss.

a. Protection schemes in wired networks

For reliability, protection schemes have been proposed for high speed wired networks. Protection schemes include link protection and node protection. There is no link failure in wireless networks, because there is no physical connection between a sender and a receiver. To enhance the survivability against node failure(s), the mechanism used in the wired networks are divided into three categories: 1) protection schemes; 2) restoration schemes; and 3) hybrid schemes. The protection schemes for wired networks basically reserve a backup path before the occurrence of link/node failure, whereas the restoration schemes wait until the occurrence of failure. In a hybrid scheme, restoration takes place during protection path failure. For delay sensitive applications, protection schemes are more suitable than the restoration schemes.

b. Proposed scheme

The traditional protection schemes such as (1+1) and (1:N) for wired networks are not suitable for wireless networks as they increase the capital cost and complexity in the network layer. To overcome the drawbacks in the traditional protection scheme, research efforts have been focused on the relay node protection using network coding [106-111]. However, the QoS performance of relay node protection using network coding has not been tested for 4G wireless networks. Therefore, the motivation of this work is to design and simulate the node protection using network coding for 4G multihop wireless networks. Furthermore, it is necessary to measure the QoS performance such as Packet Delivery Ratio (PDR), latency and jitter for performance evaluation.

1.2. Contributions

Finally, aside from providing an understanding of key issues on QoS, security and reliability for the 4G wireless technologies, this section highlights the contributions that have been published or submitted for publications for the research community and wireless industry.

1. Perumalraja Rengaraju, Chung-Horng Lung, Qu Yi and Anand Srinivasan, "An Analysis on mobile WiMAX Security", *Proc. of IEEE Toronto International Conference on Science and Technology for Humanity*, 2009, pp. 439-444.
2. Perumalraja Rengaraju, Chung-Horng Lung and Anand Srinivasan, "Design of Distributed Security Architecture for Multihop WiMAX Networks", *Proc. of the 8th Annual Conference on Privacy, Security and Trust*, 2010, pp.54-61.
3. Perumalraja Rengaraju, Chung-Horng Lung and Anand Srinivasan, "QoS Assured Uplink Scheduler for WiMAX Networks", *Proc. of IEEE Vehicular Technology Conference*, Ottawa, Canada, 2010, pp. 1-5.
4. Perumalraja Rengaraju, Chung-Horng Lung and Anand Srinivasan, "Measuring and Analyzing WiMAX Security and QoS in Testbed Experiments", *Proc. of IEEE Conference on Communication,* 2011, pp. 1-5.
5. Basil Saeed, Perumalraja Rengaraju, Chung-Horng Lung and Anand Srinivasan, "QoS and Protection of Wireless Relay Nodes Failure Using Network Coding", *Proc. of International Symposium on Network Coding,* 2011, pp. 1-5.
6. Perumalraja Rengaraju, Chung-Horng Lung and Anand Srinivasan, "Adaptive Admission Control and Packet Scheduling Schemes for QoS Provisioning in Multihop WiMAX Networks", *Proc. of the 8th IEEE International Conference on Wireless Communications and Mobile Computing*, 2012.
7. Perumalraja Rengaraju, Chung-Horng Lung and Anand Srinivasan, "Communication Requirements and Analysis of Distribution Networks Using WiMAX Technology for Smart Grids", *Proc. of the 8th IEEE International Conference on Wireless Communications and Mobile Computing*, 2012.

8. Perumalraja Rengaraju, Chung-Horng Lung and Anand Srinivasan, "QoS and Protection of Relay Nodes in 4G Wireless Networks Using Network Coding", *Proc. of the 9th IEEE International Conference on Wireless Communications and Mobile Computing*, Italy, July 2013.

9. Perumalraja Rengaraju, Chung-Horng Lung, F. Richard Yu and Anand Srinivasan, "On QoE Monitoring and E2E Service Assurance in 4G Wireless Networks", *IEEE Wireless Communication Magazine*, Volume 19: Issue 4, 2012, pp. 89-96.

10. Hassan Halabian, Perumalraja Rengaraju, Chung-Horng Lung, Ioannis Lambadaris and Anand Srinivasan, "Performance Analysis of Reservation-based Call Admission Control Schemes with Channel Borrowing in Wireless Mobile Networks", submitted to *IEEE Transactions on Vehicular Technology*.

11. Perumalraja Rengaraju, Chung-Horng Lung and Anand Srinivasan, "Adaptive Call Admission Control and Dynamic Packet Scheduling Schemes for 4G Multihop Wireless Networks", in final preparation for *IEEE Transactions on Parallel and Distributed Systems*.

12. Perumalraja Rengaraju, Chung-Horng Lung and Anand Srinivasan, "QoS Aware Distributed Security Architecture for 4G Multihop Wireless Networks", submitted to *IEEE Transactions on Vehicular Technology*.

1.3. Thesis Outline

The remainder of this thesis is organized as follows: In Chapter 2, the overview of PHY and MAC layers, the existing QoS framework at MAC layer and security architecture as defined in WiMAX and LTE standards are described. In Chapter 3, the related works are reviewed to identify the research gap in QoS and security for multihop WiMAX and LTE networks. To simplify the multi-disciplinary research on QoS, QoS aware security and QoS management during relay node failure, this thesis consists of three main chapters. In Chapter 4, the proposed RRM framework to guarantee the QoS of different service classes is demonstrated. The simulation environment and the simulation results of CAC and PS are

explained in the same chapter. In Chapter 5, the proposed distributed security architecture using the ECDH protocol for the security sublayer is explained to overcome the security threats in 4G multihop wireless networks. For the design of multihop WiMAX security, the QoS parameters, including connection latency, throughput and latency are analyzed. In Chapter 6, a scheme to protect the relay node failure using network coding technique is proposed to maintain the QoS of the network. Chapter 7 is the thesis summary and future directions.

Chapter 2. The 4G wireless standards – Overview

In this chapter, the evaluation of WiMAX and LTE standards and the main functionalities on PHY and MAC layers, as defined in the 4G wireless standards, are reported for a better understanding of this research work. In the first part of Section 2.1, the evolution of WiMAX and LTE networks is introduced. Next, the different types of PHY layers supported by WiMAX and LTE standards and their functionalities are discussed. Finally, the users' network entry procedures and the other MAC functionalities are described in MAC layer subsections. In Section 2.2, the QoS framework and different types of service flows defined in 4G wireless standards are described. The existing WiMAX and LTE security architecture is highlighted in Section 2.3. Finally, Section 2.4 introduces the network coding concepts for better understanding of protection on RS failures.

2.1 Introduction to 4G Broadband Wireless Access Networks

In this subsection the evolution and implementation scenarios of 4G wireless networks and the structure of PHY and MAC layers, as defined in both WiMAX and LTE standards, are described.

2.1.1 Evolution of WiMAX Networks

The air interface of WiMAX technology is based on the IEEE802.16 standards. The purpose of the IEEE802.16 standard is to provide cost-effective and interoperable multivendor broadband wireless access. The IEEE802.16 defines the PHY and MAC layer specifications. The PHY layer specifications include the range of operating frequency, modulation, channel encoding, etc. The MAC layer functionalities are divided into convergence, common part and security sublayers. Further, the standard provides the Network Control and Management Systems (NCMS) or control entity to control and configure the PHY and MAC layers of WiMAX devices. The Simple Network Management Protocol (SNMP) is used for communication between NCMS and the

corresponding control and management Service Access Points (SAP). The protocol layering of the IEEE802.16 standard and the NCMS architecture are shown in Figure 2.1.

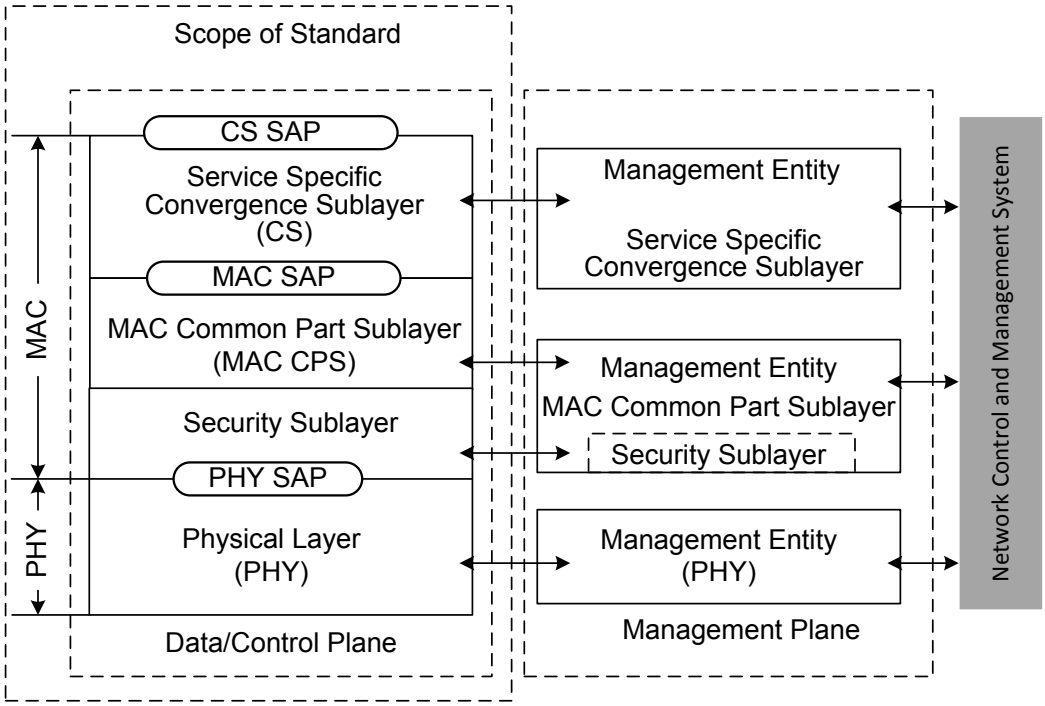


Figure 2.1 IEEE 802.16 standard protocol layering [1]

The first version of the IEEE802.16 standard was released in 2001, and the PHY layer operation was single carrier (11-66GHz) and Line of Sight (LoS) communication. To overcome the LoS communication, the frequency spectrum between 2-11GHz is proposed in IEEE802.16a-2003. The frequency selective fading and Inter-Symbol Interference (ISI) affects the system performance at 2-11 GHz frequency of operation. To overcome the frequency selective fading and ISI, the multi-carrier modulations of OFDM and Orthogonal Frequency Division Multiple Access (OFDMA) are introduced in IEEE802.16a. In the IEEE802.16d-2004, the standard merges the two previous versions. This fixed air interface is the first successful deployment for network operations. The mobility and Multicast Broadcast Service (MBS) supports are not available in fixed WiMAX networks. In IEEE 802.16e-2005, mobility and MBS supports are added to the MAC layer functionalities. The IEEE802.16e based WiMAX networks are called mobile WiMAX networks.

The multihop standard IEEE802.16j-2009 is aimed at extending the coverage region of the network [2]. In IEEE802.16j, the RS is introduced to extend the coverage region of the network and has full compatibility to legacy IEEE802.16e MS. The goal set out in the recently released IEEE 802.16m-2011, advanced air interface standard is to meet the requirements for International Mobile Telecommunications (IMT) – Advanced next generation networks [3]. According to the International Telecommunication Union (ITU), an IMT-Advanced cellular system must have a target peak data rate of approximately 100 Mbit/s at 350km/hr, and approximately 1 Gbit/s for low mobility scenarios. For multihop networks with high mobility scenarios, the security architecture and the QoS framework designs are the main challenging tasks for the researchers.

The IEEE 802.16 standards define only the protocol for PHY and MAC layers. On the other hand, the network specifications of the WiMAX products are being developed internally by the WiMAX Forum, which include the E2E networking and network interoperability specifications [4]. The primary mission of the WiMAX Forum is to ensure interoperability among IEEE 802.16 based products through its certification process. The WiMAX network architecture defined in the WiMAX Forum is logically represented by a Network Reference Model (NRM) as shown in Figure 2.2 [4].

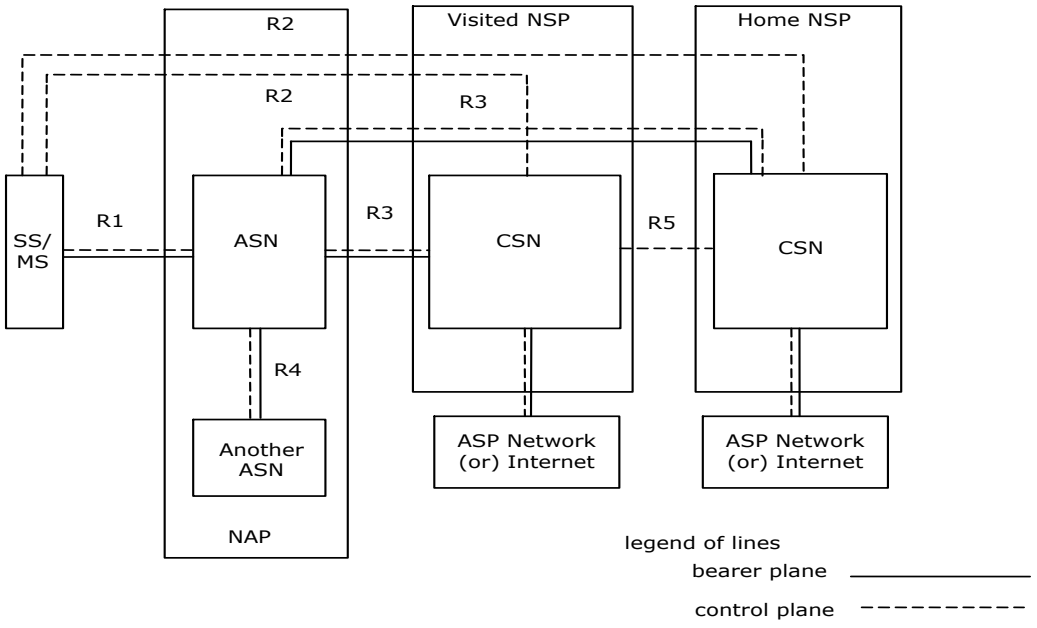


Figure 2.2 WiMAX Network Reference Model [4]

The NRM consists of Network Access Providers (NAPs) and Network Service Providers (NSPs). The detailed procedures of NRM identify the key functional entities of NAP and NSP as well as reference points for network interoperability specifications [4]. The NAP is a business entity that provides WiMAX radio access infrastructure. The NSP is the business entity that provides IP connectivity and WiMAX services to WiMAX subscribers according to their Service Level Agreements (SLAs).

The WiMAX NRM consists of MSs, an ASN, Connectivity Service Network (CSN), and reference points R1–R8. The ASN has a complete set of network functions required to provide the WiMAX connectivity to the MS. These functions include layer-2 connectivity as defined in IEEE 802.16e and the functionalities as defined in the WiMAX system profile. The WiMAX system profile functionalities are a transfer of AAA messages to the Home NSP (HNSP). The ASN may support ASN and CSN anchored mobility, paging, location management and tunnelling operations to CSN gateway. The main function of the CSN is to provide an IP connectivity services to the WiMAX customers. The network elements, which are connected to the CSN, are such as routers, AAA servers, Home Agent (HA) including user databases, location-based services, network servers and interworking gateways. Some important functions of the CSN are: IP address management; AAA functionalities; QoS policy and admission control based on user subscription; roaming; inter-ASN and CSN anchored mobility and connectivity to external servers such as IP Multimedia Subsystem (IMS), peer-to-peer services and MBS services.

2.1.2 Evolution of LTE networks

The 3GPP is the collaboration between groups of telecommunications associations, known as the organizational partners. The 3GPP defines the standard for 2G Global System for Mobile Communications (GSM) systems, 3G Universal Terrestrial Radio Access (UTRA) and the 4G LTE/LTE-Advanced network.

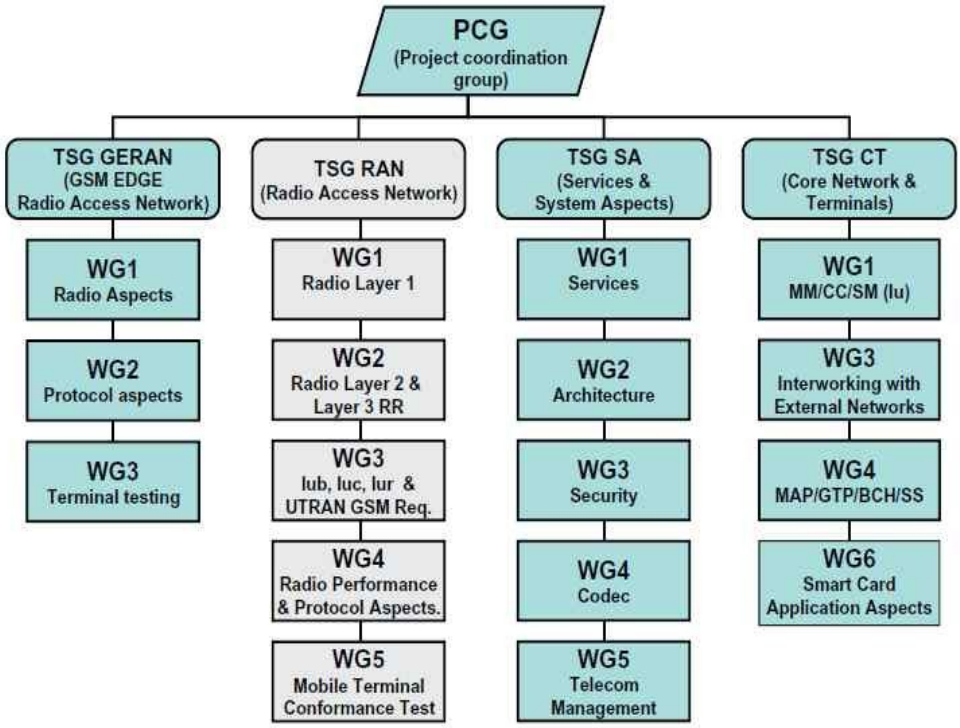


Figure 2.3 3GPP technical specification group [12]

The four Technical Specifications Groups (TSGs) of 3GPP and its services are shown in Figure 2.3 [12]. The first major addition of radio access features to Wideband Code Division Multiple Access (WCDMA) was added in Release-5 with High Speed Downlink Packet Access (HSDPA) and Release-6 with High Speed Uplink Packet Access (HSUPA). These two are combined in Release-7, also referred to as High Speed Packet Access (HSPA). The first release of the LTE specifications, Release-8, was completed in December 2008 and commercial network operation began in late 2009. The functionalities supported by the Release-8 were, multi-antenna support, Inter Channel Interference Cancellation (ICIC), Hybrid Automatic Repeat reQuest (HARQ), channel-dependent scheduling, time and frequency duplexing. The features of Multicast Broadcast Multimedia Services, beam forming and global positioning are added in Release-9 in Dec. 2009. The Release-10 in March 2011, LTE-Advanced, is aimed to support IMT-Advanced users as similar to WiMAX advanced air interface specification. The features added in Release-10 were relaying, multi-antenna extension and carrier aggregation.

At a high level, the LTE network is the evolution of radio access through Evolved UTRAN (E-UTRAN) and the Core Network (CN) through Evolved Packet Core (EPC). The EPC is also referred to as System Architecture Evolution (SAE). The entire system composed of both LTE and SAE is called the Evolved Packet System (EPS).

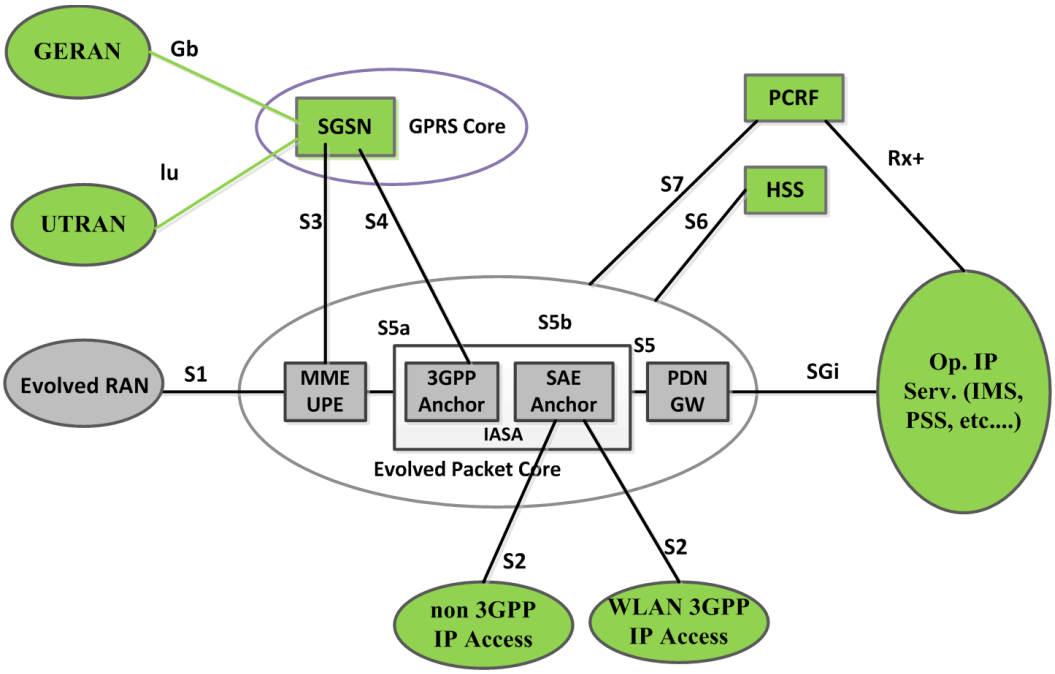


Figure 2.4 LTE-SAE network architecture [17]

The SAE simplifies the network design and provides seamless integration of the mobile network to other IP based communications networks. Figure 2.4 shows the high level flat IP architecture of LTE-SAE and its interfaces [17]. Here, the Evolved Radio Access Network (E-RAN) is maintained by the access provider to deliver the LTE radio access for the users. The EPC is maintained by the LTE service providers to be responsible for the IP connectivity and other services according to negotiated SLAs. The logical entities in the E-RAN network have User Equipment (UE) and evolved Node B (eNB), also called BS. The eNB, which supports multihop connectivity, is called Donor eNB (DeNB). One major change in LTE with the third generation network is that the Radio Network Controller (RNC) in third generation network is eliminated from the data path and its functions are incorporated in eNB.

2.1.3 Implementation Scenarios

The WiMAX/LTE network can be deployed in a number of ways depending upon the service requirements, geographical area and financial considerations. Some practical WiMAX/LTE network implementations are wireless backhauling, fixed Broadband Wireless Access (BWA) and mobile services. The network implementations for WiMAX networks are described as follows: for LTE network implementations, the BS is replaced by eNB and SS or MS is replaced by UEs.

Wireless backhauling: A backhaul network is designed to bring the wireless last-mile broadband access as an alternative to typical Digital Subscriber Loop (DSL) and cable infrastructures. The high bandwidth support offered by 4G wireless backhaul makes it a superior backhauling technique for enterprises, hotspots and Point-to-Multipoint (PMP) networks. The network topology considered for this scenario is Point-to-Point network.

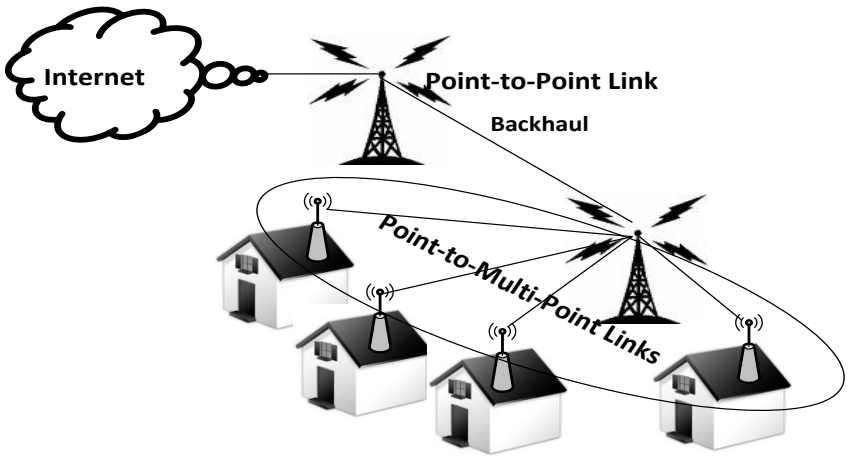


Figure 2.5 Point-to-Point and Point-to-Multipoint WiMAX network

Fixed BWA: In this scenario, broadband wireless (high speed internet) is provided to home and business users in a Wireless Metropolitan Area Network (WMAN). The network topology considered for this connection is PMP, where multiple SSs are connected to one BS. Figure 2.5 shows the practical implementation scenario for wireless backhauling and fixed BWA.

Mobile wireless services: The practical deployment of single-hop and multihop mobile WiMAX networks follows the network architecture as defined by the WiMAX Forum. The WiMAX Forum released the system profile version-1.0 in 2007 for the mobile WiMAX network, which is based on IEEE802.16e. Some practical implementations of the mobile WiMAX network are as shown in Figure 2.6.

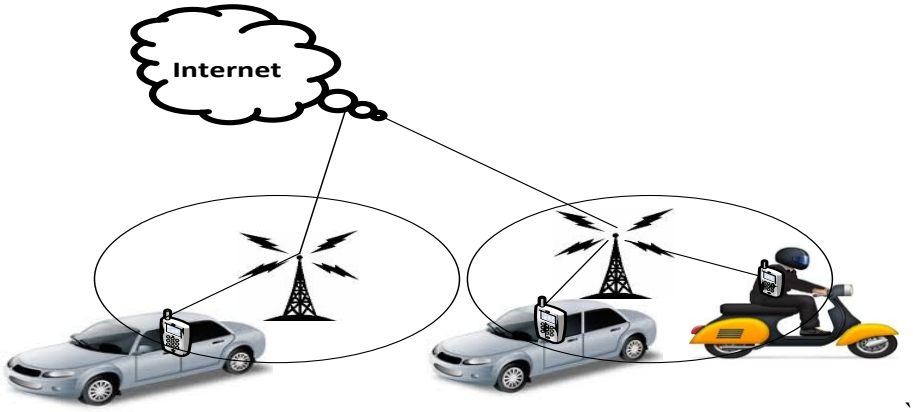


Figure 2.6 Mobile WiMAX network

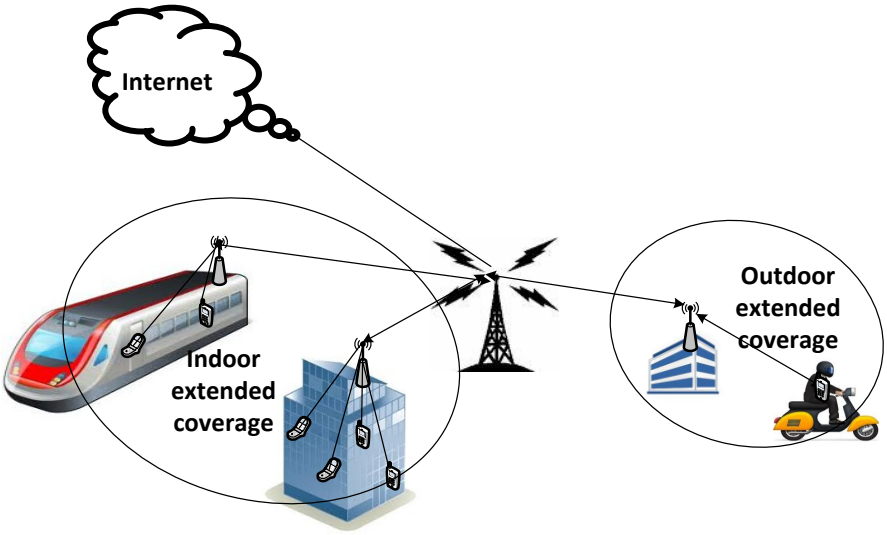


Figure 2.7 Multihop WiMAX network

Figure 2.7 shows the 4G multihop wireless network model as defined in Release-10 and IEEE802.16j. The multihop WiMAX network is aimed to extend the coverage region of the mobile WiMAX network and also to increase the throughput for cell edge users. The

WiMAX Forum is currently working on the multihop WiMAX network with IMT – Advanced air interface specifications as defined in the IEEE802.16m standard. This network will support peak data rates of approximately 100 Mbit/s for very high mobility (up to 350km/hr) and approximately 1 Gbit/s for low mobility scenarios.

2.1.4 Physical (PHY) Layer

The purpose of the PHY layer is to transport and receive the physical data in a wireless medium. For data transmission, the MAC layer Protocol Data Units (PDUs) is the input for PHY layer, received through PHY-SAP interface. The reverse operation takes place for the data reception. The PHY layer frequency of operation in the IEEE802.16-2001 standard is from 10 to 66GHz and single carrier; however, the network requires LoS operation. To overcome the LoS issues, the frequency spectrum between 2-11GHz is used in the mobile and multihop WiMAX standards. On the other hand, LTE uses the frequency spectrum of 700 MHz to 3.8 GHz. To overcome the frequency selective fading and ISI, OFDM technology is introduced in both the WiMAX and LTE standards. The PHY layers defined in WiMAX and LTE standard are as given below:

- Wireless MAN SC: Wireless MAN SC is a single carrier PHY layer intended for frequencies beyond 11GHz operation requiring a LoS condition in WiMAX. Both the Frequency Division Duplexing (FDD) and Time Division Duplexing (TDD) are used for separating the uplink and downlink communication. The bandwidth allocations to the individual users are based on Time Division Multiple Access (TDMA).
- Wireless MAN SCa: Wireless MAN SCa is a single carrier PHY layer for frequencies between 2GHz and 11GHz operations in WiMAX standard. It supports both FDD and TDD to separate the uplink and downlink, and the user allocations are based on TDMA.
- Wireless MAN OFDM: Wireless MAN OFDM is a 256-point Fast Fourier Transform (FFT) based OFDM PHY layer for the frequencies between 2GHz and 11GHz in WiMAX. In OFDM PHY, the spectrum is broken up into many narrowband channels known as “subcarriers”, where the data stream is transmitted on each subcarrier. The multiple access technique used in this PHY layer is TDMA.

- OFDMA: Wireless MAN OFDMA is a 2048-point FFT based OFDMA PHY layer for the frequencies between 2GHz and 11GHz in WiMAX for both uplink and downlink operations. In the IEEE 802.16e specifications, this PHY layer has been modified to scalable OFDMA, where the FFT size is variable and can take any of the following values: 128; 512; 1024 and 2048. On the other hand, LTE uses OFDMA for downlink transmission only. The FFT size used in LTE standard is 2048.

- Single Carrier FDMA (SC-FDMA) [16]: The uplink transmission scheme for LTE network is based on Single Carrier FDMA. SC-FDMA can be interpreted as a linearly pre-coded OFDMA scheme in the sense that it has an additional Discrete Fourier Transform (DFT) processing preceding the conventional OFDMA processing. The distinguishing feature of SC-FDMA over OFDM and OFDMA is that it's transmit signal has a lower Peak-to-Average Power Ratio (PAPR); this results in easier design parameters in the transmit path of a subscriber unit.

The existing deployed networks and the upcoming WiMAX and LTE networks use OFDM techniques for PHY layer operations, because the OFDM has more advantages than single carrier operation. The advantages are [21]:

- OFDM system combats the ISI and reduces the Inter-Channel Interference (ICI)
- High spectral efficiency because of overlapping spectra
- Simple implementation by FFT
- Low receiver complexity, as the transmitter combat the channel effect
- Suitable for high data rate transmission
- High flexibility in terms of link adaptation
- Low complexity multiple access schemes like OFDMA
- It is possible to use maximum likelihood detection with reasonable complexity

On the other side, the OFDM system has few drawbacks [21]:

- An OFDM system is highly sensitive to timing and frequency offsets. Demodulation of an OFDM signal with an offset in the frequency can lead to a high bit error rate.

- An OFDM system with large numbers of subcarriers will have a higher PAPR than a single carrier system. If the system's PAPR is at a high level, then the implementation of Digital to Analog Conversion (DAC) and Analog to Digital Conversion (ADC) is extremely difficult. A small description of OFDM, OFDMA and SC-FDMA PHY specifications are as follows:

2.1.4.1 OFDM PHY

The OFDM technique combines the concepts of modulation and multiplexing. The block diagram of OFDM transmitter and receiver is shown in Figure 2.8 [18]. In OFDMA system, the input data stream is divided into several parallel sub-streams, and then each sub-stream is modulated and, finally, transmitted on each orthogonal subcarrier. The modulated signals are repeated by introducing the cyclic prefix to completely eliminate ISI as long as the cyclic prefix duration is longer than the channel delay spread. Figure 2.9 shows the time domain representation of OFDM symbol [1].

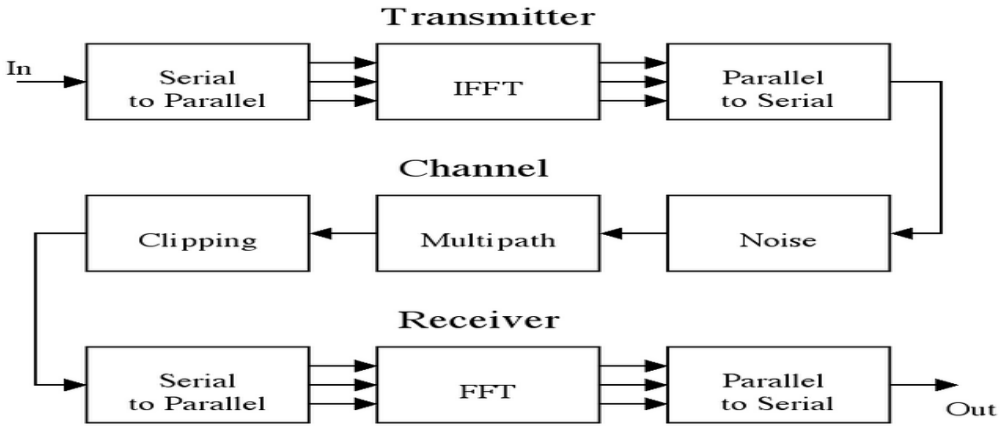


Figure 2.8 OFDM transmitter and receiver [18]

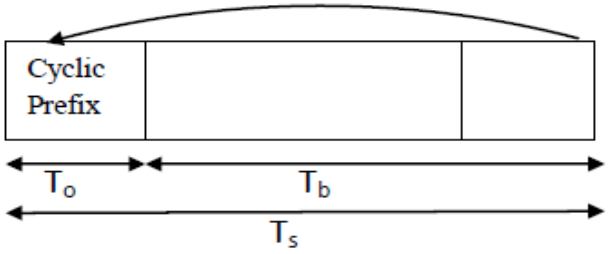


Figure 2.9 OFDM symbol -time domain representation [1]

***Frequency domain*:**

The frequency domain representation of an OFDM symbol and its orthogonal subcarriers is shown in Figure 2.10 [1]. The size of the FFT point determines the number of subcarriers. There are three subcarrier types.

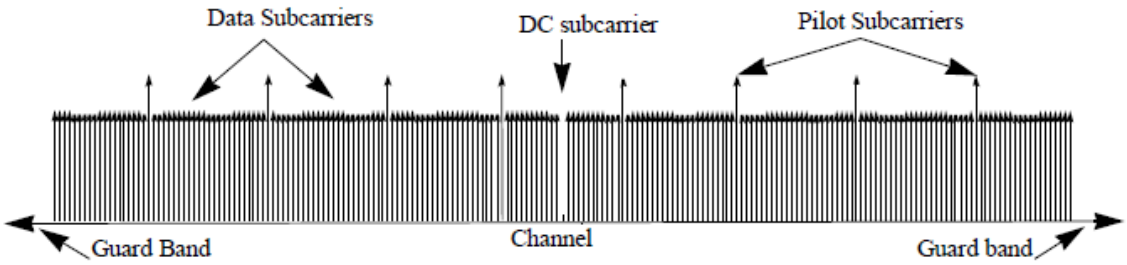


Figure 2.10 Frequency domain representation of OFDM symbol [1]

- Data subcarriers: For data transmission
- Pilot subcarriers: For various estimation purposes
- Null subcarriers: No transmission at all, for guard bands, non-active subcarriers and the DC subcarrier.

Minimum Allocation Unit (MAU):

The MAU is the smallest bandwidth that can be allocated in frequency and time for sending information across the channel [1]. In the OFDM PHY, the MAU's useful capacity is variable and depends on the chosen modulation and coding rate. The downlink MAU is one OFDM symbol by all (192) data subcarriers. However, the MAU is one OFDM symbol by one subchannel (i.e. 16 subcarriers) for uplink.

2.1.4.2 OFDMA PHY

OFDMA extends the functionality of OFDM by adding additional multiple access features in the frequency domain which means the user bandwidth can be allocated in both time and frequency domain in terms of OFDMA slots.

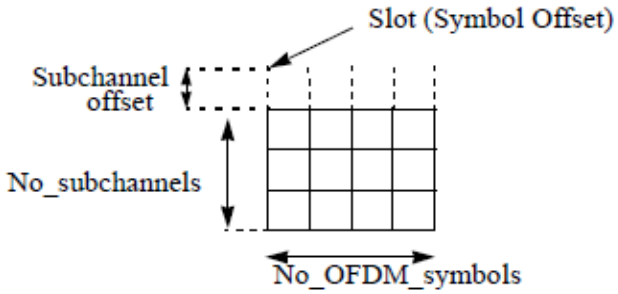


Figure 2.11 Example of a data region that defines an OFDMA allocation [1]

The frequency domain specifications are pretty much the same as OFDM PHY specifications. In OFDMA, a data region is a two-dimensional allocation of a group of contiguous subchannels in frequency and OFDMA symbols, in time. A two-dimensional allocation of OFDMA PHY may be visualized as a rectangle, such as the 4 × 3 rectangle shown in Figure 2.11 [1].

MAU in WiMAX OFDMA PHY:

In WiMAX OFDMA PHY, the minimum frequency domain resource unit is one slot, which is equal to 48 subcarriers. However, the definition of MAU depends on the OFDMA symbol structure that varies between uplink and downlink, Fully Used Subcarrier (FUSC) and Partially Used Subcarrier (PUSC), and then between distributed subcarrier and adjacent subcarrier permutations in WiMAX network.

- For downlink FUSC, one slot is one subchannel by one OFDMA symbol.
- For downlink PUSC, one slot is one subchannel by two OFDMA symbols.
- For uplink PUSC and for downlink Tile Usage Sub Channel (TUSC), one slot is one subchannel by three OFDMA symbols.
- For the adjacent subcarrier permutation, one slot is one subchannel by two, three, or six OFDMA symbols. The allowed (bins and symbol) combinations are [(6, 1), (3, 2), (2, 3), (1, 6)], where a bin consists of 9 contiguous subcarriers in a symbol, with 8 assigned for data and one assigned for a pilot.

MAU in LTE OFDMA PHY:

In LTE, the smallest time-frequency unit in a OFDMA resource grid is denoted as a resource element [16]. The resource block is the basic element for radio resource allocation. From the available radio resource grid, MAU is one Transmission Time Interval (TTI) in the time domain, that is, one subframe of 1 ms. Each subframe contains two resource blocks; the size of each resource block is the same for all bandwidth, which is 180kHz in the frequency domain. There are two kinds of resource blocks defined for LTE: physical and virtual resource blocks.

2.1.5 WiMAX MAC Layer

The main focus of the IEEE802.16 MAC layer is to manage the wireless resources in an efficient manner. The IEEE802.16 MAC protocol is designed to support for Point-to-Point, Point-to-Multipoint (PMP), mesh and multihop network models.

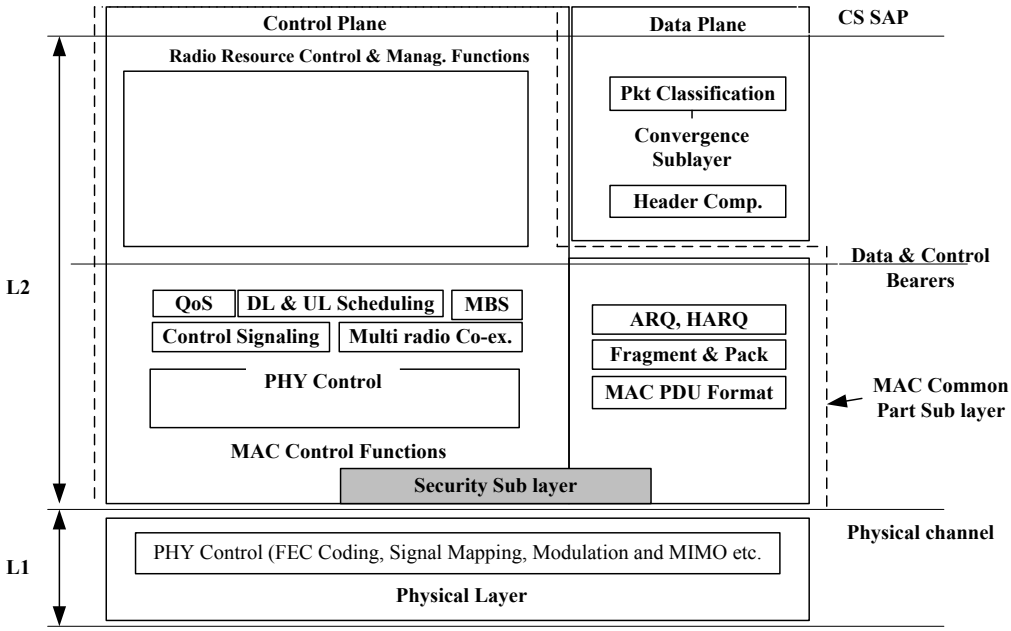


Figure 2.12 IEEE802.16 protocol stack and its functions

The MAC layer is divided into Convergence Sublayer (CS), Common Part Sublayer (CPS) and Security Sublayer (SecS) that are shown in Figure 2.12. The CS provides an interface to upper layers such as ATM and IP network interfaces. The CPS does the core

functionalities of WiMAX MAC operation and finally, the SecS manages the user authentication and data encryption procedures.

2.1.5.1 Service Specific Convergence Sublayer

The CS is responsible for all initial packet processing operations. The main function of the CS layer is to map the external PDUs that are received from SAP of the CS into the MAC Service Data Units (SDUs) based on certain classifiers. The downlink classifiers are applied by the BS, and the uplink classifiers are applied at the SS/MS as shown in Figure 2.13 [1].

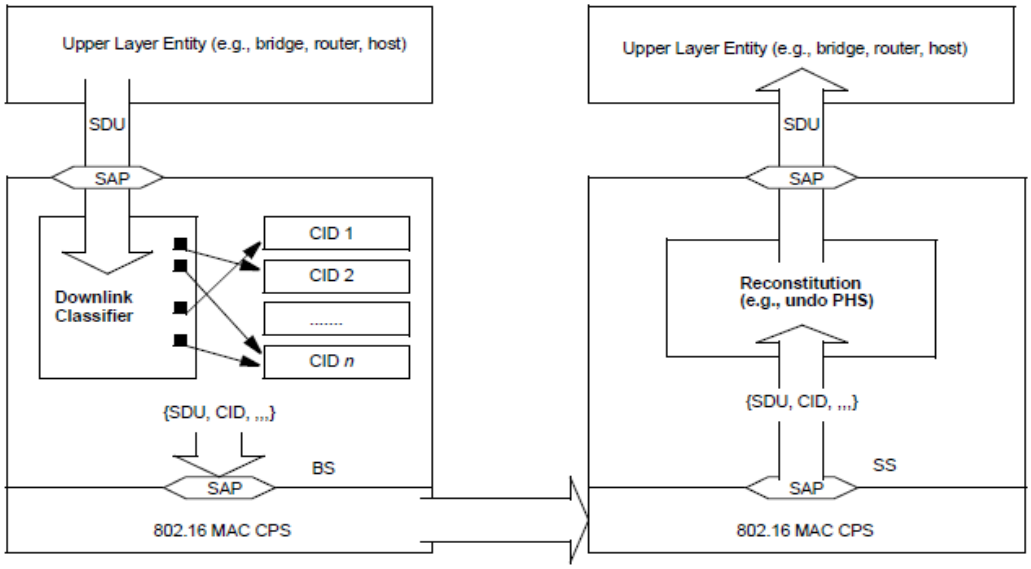


Figure 2.13 Classification and CID mapping (BS to SS) [1]

The classifiers are used to differentiate the service flows based on protocol-specific packet matching criteria (e.g. IP address), connection's Service Flow Identifier (SFID), Connection Identifier (CID) and Classifier priority. If a packet fails to match the set of defined classifiers, it will be discarded. Another packet processing operation provided by the CS layer is Payload Header Suppression (PHS). The PHS removes the repetitive information such as MAC address and IP address in the header elements (e.g. The PHS feature replaces 802.3 header with 1 byte PHS index). From the PHS index, original headers will be reconstructed at the receiver.

2.1.5.2 Common Part Sublayer

The WiMAX MAC protocol is connection oriented, where the MS creates one or more connections to transmit or receive the data with the BS. Each connection is identified by 16bit CID, but the MS is identified by its 48 bit MAC address. Upon entering the network, the SS, MS and RS establish basic, primary and secondary management connections in both uplink and downlink directions. These connections are used for the following MAC management operations:

- Basic Connection is responsible for transferring critical MAC and Radio Link Control (RLC) messages.
- Primary Management Connection is responsible for transferring longer and more delay-tolerant control messages that are used for authentication and connection setup.
- Secondary Management Connection is used for the transfer of standard based management messages such as Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP) and SNMP.

The core functionalities provided by the MAC CPS are system access using network entry procedures, connection establishment and connection maintenance, local RRM functionalities, Radio Resource Agent (RRA) functionalities for Radio Resource Control (RRC), support for MBS, data retransmission and framing that includes fragmentation and packing. The following subsections describe the functionalities supported by the MAC CPS, except for the RRM and RRA functionalities as they are described in the next section.

Network entry procedures:

In order to communicate with the WiMAX network, SS, MS and RS should successfully complete the network entry process with the desired RS or BS. The network entry process is divided into downlink channel synchronization, initial ranging, capabilities negotiation, authentication message exchange, registration, and IP connectivity stages. Upon completion of the network entry process, the SS/MS creates one or more service flows to send data to the superordinate RS or BS. On the other hand, the RS may establish one or more service flows or traffic tunnel with the superordinate RS or BS, based on the

connected SS/MS. Figure 2.14 depicts the network entry process of MS and RS. The network entry stages are described below.

Downlink Channel Synchronization: When the MS or RS wishes to enter the network, it scans for a WiMAX channel from the range of frequencies as configured by the user (usually the ISPs). If the MS or RS finds a downlink channel and is able to synchronize at the frame preamble at PHY layer, then the MAC layer looks for Downlink Channel Descriptor (DCD) and Uplink Channel Descriptor (UCD) to get information on modulation and other downlink and uplink parameters.

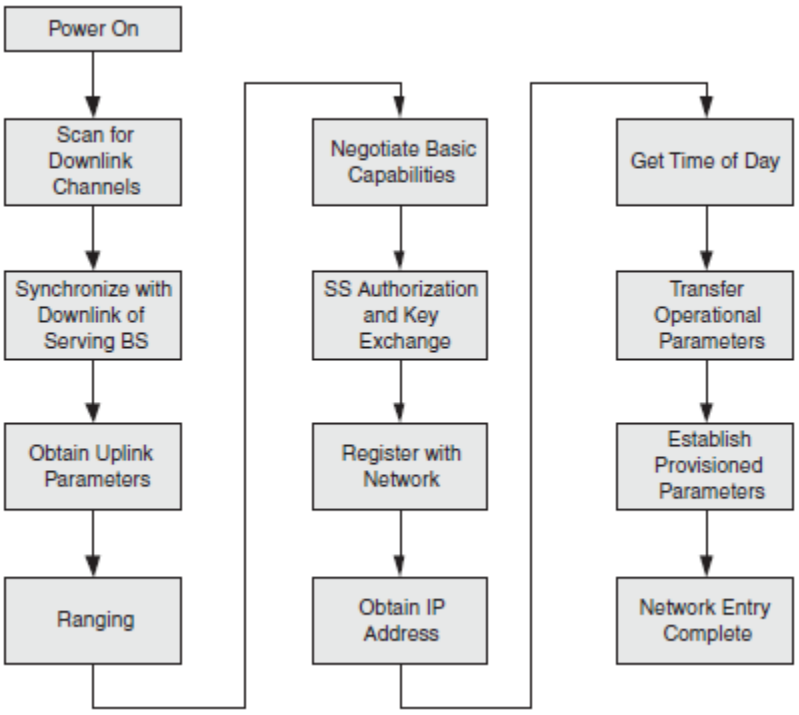


Figure 2.14 Initial ranging and network entry procedures [1]

Initial ranging: When the MS or RS has synchronized with the downlink channel, they receive the downlink broadcast messages. Then, they begin the initial ranging process by sending a ranging request MAC message on the initial ranging interval using the minimum transmission power. The ranging response indicates the power, frequency and timing corrections for successful ranging process. If the response indicates success, the MS or RS are ready to send data on the uplink.

Capabilities Negotiation: After successful completion of initial ranging, the MS or RS send a capability request message to the superordinate RS or BS describing their supported modulation levels, coding schemes and rates, and duplexing methods. The superordinate RS or BS accept or deny the MS/RS, based on their capabilities.

Authentication: After capability negotiation, the BS or superordinate RS authenticate the MS or RS and provide a key material to enable the ciphering of data. The MS/RS send the manufacturer's X.509 certificate and supported cryptographic algorithms to its BS or superordinate RS. The BS or superordinate RS validate the identity of the MS/RS and send an authentication response along with a selected crypto algorithm to the MS/RS. The MS/RS is required to perform authentication and key exchange procedures periodically to refresh its key material.

Registration: After successful completion of authentication, the MS/RS register with the network. The MS/RS send a registration request message to the BS or superordinate RS that, in turn, send a registration response to the MS/RS. The registration exchange includes IP version support, SS managed or non-managed support, Automatic Repeat reQuest (ARQ) parameters support, classification option support, CRC support, and flow control.

IP Connectivity: The MS/RS then start DHCP procedure to get the IP address and other parameters to establish IP connectivity. Then the MS/RS update the current date and time with day time server using time of the day protocol.

Transport Connection Creation: After completion of registration, transport connections are created for the MS based on its provisioned services. For preprovisioned service flows, the connection creation process is initiated by the BS or superordinate RS. The BS or superordinate RS send a Dynamic Service Addition (DSA) request message to the MS, and the MS sends a response to confirm the creation of the connection.

Framing:

The WiMAX standards support both TDD and FDD for data transmission and reception. For implementation, mostly TDD operation is selected due to its simple hardware design. For data transmission in FDD and TDD, packing and fragmentation of

MAC SDUs is executed in tandem with the bandwidth allocation process to maximize efficiency and flexibility. Fragmentation is the process by which a MAC SDU is divided into one or more SDU fragments. Packing is the process in which multiple MAC SDUs are packed into a single MAC PDU payload. Either functionality can be initiated by the BS in the downlink or by the MS in the uplink.

OFDM-TDD (fixed WiMAX): In OFDM-TDD, the length of the frame is configurable, and it is from 2msec to 20 msec. The frame is divided into downlink and uplink subframes. The downlink and uplink subframes are separated by small Transmit/receive Transition Gap (TTG) and Receive/transmit Transition Gap (RTG), respectively to prevent downlink and uplink transmission collisions. The downlink subframe consists of preamble, Frame Control Header (FCH), and a number of broadcast control messages including UL-MAP, UL-MAP, DCD, UCD and unicast data bursts. The uplink subframe consists of ranging channel, which is contention based, and uplink data bursts for an individual user.

OFDMA-TDD (mobile WiMAX – IEEE802.16e): The mobile, multihop and advanced air interface WiMAX networks use OFDMA PHY. The length of the mobile and multihop WiMAX networks' frame is configurable, and it is from 2msec to 20 msec. Figure 2.15 illustrates the OFDMA frame structure in the mobile WiMAX network for TDD mode.

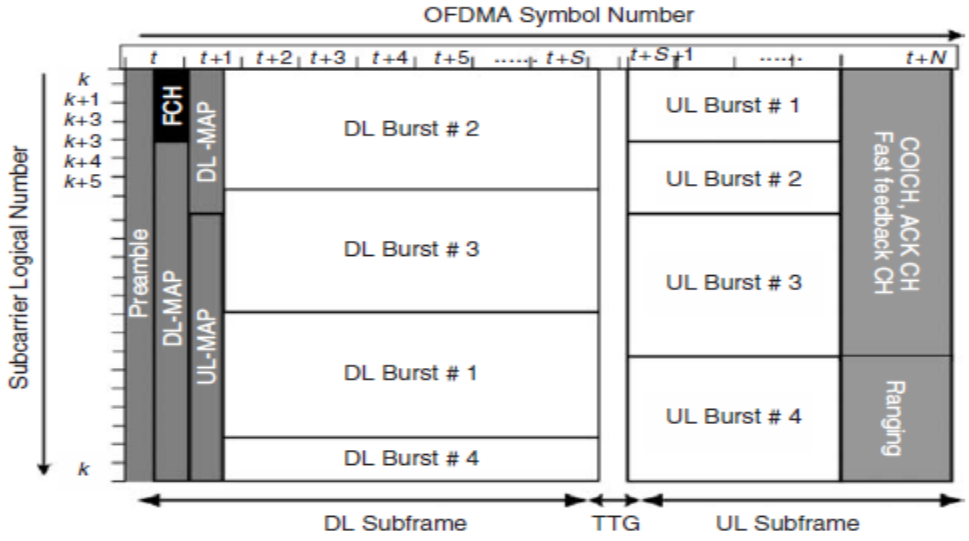


Figure 2.15 OFDMA-TDD frame structure in IEEE802.16e [1]

The additional supports for mobile users in OFDMA frame are:

- UL CQICH: The uplink Channel Quality Indicator Channel (CQICH) channel is allocated for the MS to feedback channel state information.
- UL ACK: The uplink Acknowledgement (ACK) is allocated for the MS to feedback downlink HARQ ACKs.

OFDMA-TDD for multihop WiMAX (802.16j): In the multihop WiMAX network, there are two different modes of operation: transparent mode and non-transparent mode.

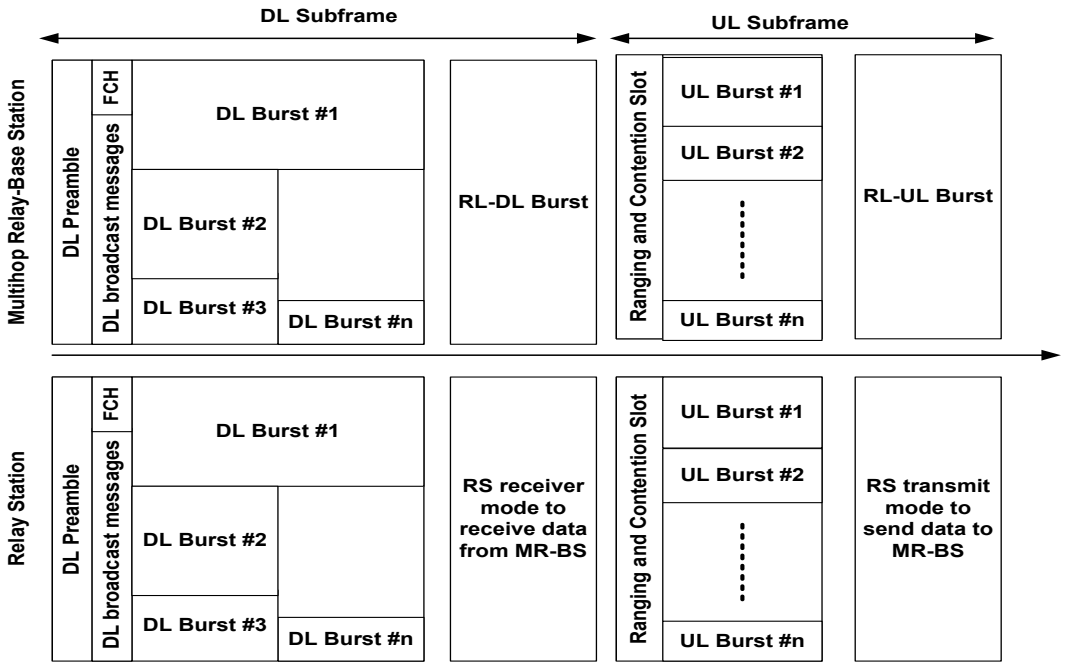


Figure 2.16 OFDMA-TDD frame structure in IEEE802.16j [2]

In a transparent mode, Multihop Relay BS (MR-BS) is responsible for broadcasting the control information and network connectivity. The RSs are responsible for just forwarding the data traffic. On the other hand, in a multihop WiMAX network in non-transparent mode with distributed scheduling architecture, both MR-BS and RS are responsible for scheduling the bandwidth and frame control. The MR-BS allocates bandwidth to both RSs and MSs in a separate zone. Figure 2.16 shows the OFDMA-TDD frame format for non-transparent mode operation [2]. In both downlink and uplink

subframes, the relay links and access links are time separated by the RS time allowances, RS-RTG (RSRTG) and RS-TTG (RSTTG). The downlink/uplink access zones are dedicated for transmission between MR-BS and MSs, and they are fully compatible with the 802.16e frame structure.

2.1.6 LTE – MAC and Higher Layers

Figure 2.17 shows the LTE protocol layering architecture of both user and control plane [17]. In the user plane, the protocols included are the PDCP, the RLC, MAC and PHY protocols. The control plane additionally includes the RRC protocols. The main functionalities carried out in each layer are summarized below.

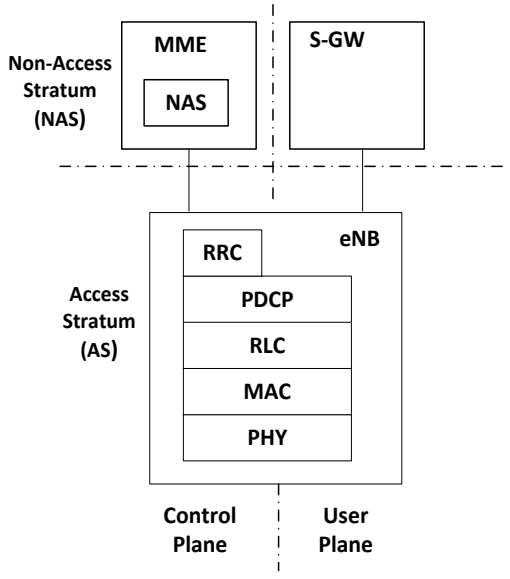


Figure 2.17 LTE user and control plane protocol [17]

NAS (Non-Access Stratum):

- Connection/session management between UE and the CN
- Authentication
- Registration
- Bearer context activation/deactivation
- Location registration management

RRC:

- Broadcast system information related to NAS and Access Stratum (AS)
- Establishment, maintenance and release of RRC connection
- Security functions including key management
- Mobility functions
- QoS management functions
- UE measurement reporting and control of the reporting
- NAS direct message transfer between UE and NAS

PDCP:

- Header compression
- In-sequence delivery and retransmission of PDCP
- Session Data Units for acknowledge mode radio bearers at handover
- Duplicate detection
- Ciphering and integrity protection.

RLC: RLC offers services to PDCP in the form of radio bearers

- Error correction through Automatic Repeat reQuest (ARQ)
- Segmentation according to the size of the transport block and re-segmentation in case they need to be retransmitted
- Concatenation of SDUs for the same radio bearer
- Protocol error detection and recovery
- In-sequence delivery

MAC: MAC offers services to RLC in the form of logical channels.

- Multiplexing/demultiplexing of RLC packets
- Scheduling information reporting
- Error correction through HARQ
- Local Channel Prioritization
- Padding

PHY offers services to MAC in the form of transport channels.

2.1.6.1 LTE Channel Types

In LTE, radio channels are used to segregate the different types of data and allow them to be transported across the radio access network. There are three categories into which the various data channels may be grouped [13].

- Physical channels: These are transmission channels that carry user data and control messages.
- Transport channels: The physical layer transport channels offer information transfer to MAC and higher layers.
- Logical channels: These channels provide services for the MAC layer within the LTE protocol structure.

LTE physical channels:

The LTE physical channels vary between the uplink and the downlink, as each has different requirements and operates in a different manner.

Downlink:

- Physical Broadcast Channel (PBCH): This physical channel carries system information for UEs requiring access to the network. It only carries what is termed Master Information Block (MIB), messages.
- Physical Control Format Indicator Channel (PCFICH): As the name implies, the PCFICH informs the UE about the format of the signal being received.
- Physical Downlink Control Channel (PDCCH): The main purpose of this physical channel is to carry mainly scheduling information of different types, which are Downlink resource scheduling.
- Physical Hybrid ARQ Indicator Channel (PHICH): As the name implies, this channel is used to report the Hybrid ARQ status.

Uplink:

- Physical Uplink Control Channel (PUCCH): The Physical Uplink Control Channel, PUCCH, provides the various control signaling requirements.
- Physical Uplink Shared Channel (PUSCH): This physical channel found on the LTE uplink is the Uplink counterpart of PDSCH.
- Physical Random Access Channel (PRACH): This uplink physical channel is used for random access functions.

LTE transport channels:

The LTE transport channels vary between the uplink and the downlink as each has different requirements and operates in a different manner. Physical layer transport channels offer information transfer to MAC and higher layers.

Downlink:

- Broadcast Channel (BCH): The LTE transport channel maps to Broadcast Control Channel (BCCH).
- Downlink Shared Channel (DL-SCH): This transport channel is the main channel for downlink data transfer. It is used by many logical channels.
- Paging Channel (PCH): To convey the PCCH.
- Multicast Channel (MCH): This transport channel is used to transmit Multicast Control Channel (MCCH) information to set up multicast transmissions.

Uplink:

- Uplink Shared Channel (UL-SCH): This transport channel is the main channel for uplink data transfer. It is used by many logical channels.
- Random Access Channel (RACH): This channel is used for random access requirements.

LTE logical channels:

The logical channels cover the data carried over the radio interface. The SAP between the MAC sublayer and the RLC sublayer provides the logical channel.

Control channels: LTE control channels carry the control plane information and configuration information necessary for operating an LTE system.

- Broadcast Control Channel (BCCH): This control channel provides system information to all mobile terminals connected to the eNodeB.
- Paging Control Channel (PCCH): This control channel is used for paging information when searching a unit on a network.
- Common Control Channel (CCCH): This channel is used for random access information, e.g. for actions including setting up a connection.
- Multicast Control Channel (MCCH): This control channel is used for information needed for multicast reception.
- Dedicated Control Channel (DCCH): This control channel is used for carrying user-specific control information, e.g. for controlling actions including power control, handover, etc.

Traffic channels: LTE traffic channels carry the user plane data:

- Dedicated Traffic Channel (DTCH): This traffic channel is used for the transmission of user data.
- Multicast Traffic Channel (MTCH): This channel is used for the transmission of multicast data.

2.1.6.2. LTE OFDMA Frame Format

In the downlink OFDMA frame, each user is assigned a number of subchannels for a certain number of time slots. Together, the time slots and subchannels compose Physical Resource Blocks (PRBs). A PRB consists of 12 consecutive subchannels that are allocated for the time of one time slot (0.5 ms). Short time slots assure small network delays. The number of available PRBs depends upon the available bandwidth.

Figure 2.18 shows the downlink OFDMA frame format in an LTE network, where time slots are combined into frames [17]. Each frame has a length of 10 msec and is divided into ten subframes of equal size. Each subframe can be viewed as a transport block. A subframe consists of two equal-sized time slots. For each time slot, 6 or 7 OFDM symbols are carried depending on the length of the cyclic prefix. The transport block PDU has MAC header and padding where, each MAC SDU has a RLC header and RLC SDUs. Within RLC SDU there can be a number of PDCPs.

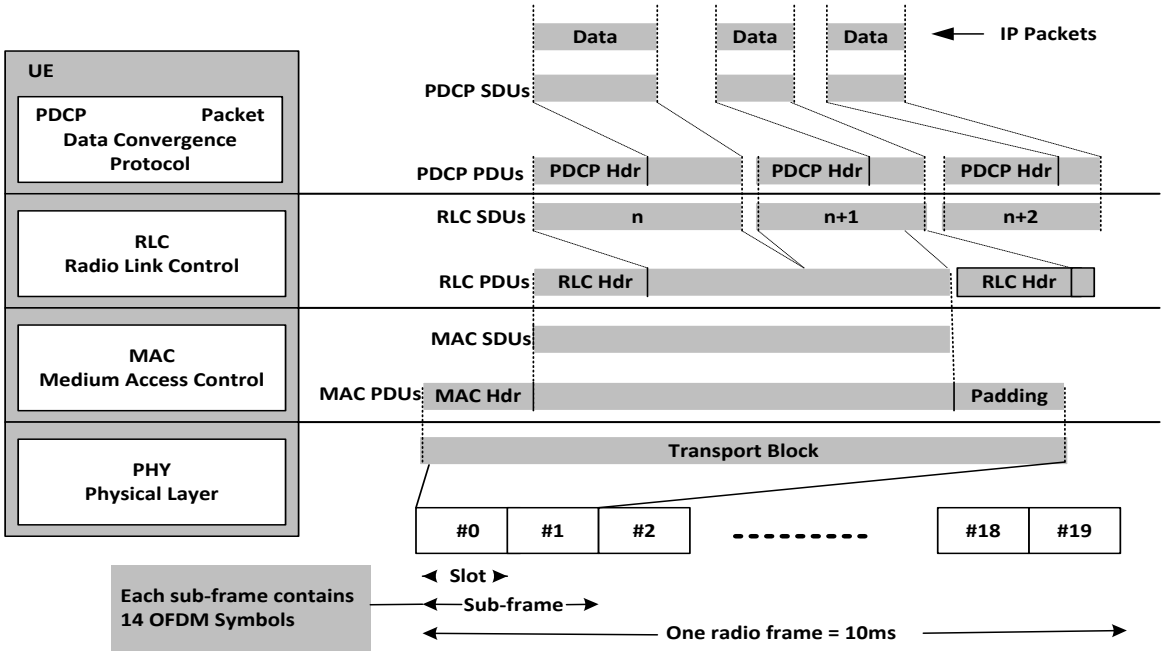


Figure 2.18 Downlink OFDMA frame structure in LTE [17]

2.1.6.3. Synchronization and Network Entry

In LTE, the frame synchronization is obtained by detecting the Primary Synchronization Sequence (PSS) which is sent twice in a frame [18]. Identification of the PSS in the received signal gives two potential starting points in the frame as there are two PSS transmissions in the frame. On the other hand, the Secondary Synchronization Sequence (SSS) is sent one OFDM symbol ahead in the same set of subcarriers as the PSS. The detection of the SSS gives information about the cyclic prefix duration and the cell ID. Hence, irrespective of bandwidth, a common processing is evolved to achieve frame

synchronization, cyclic prefix duration detection, and cell identifier detection. These signals are also used for achieving frequency synchronization.

In LTE, irrespective of bandwidth and the number of subcarriers, the first step is locating the PSS, SSS and obtaining the cell identifier. This step is the same for all mobiles. However, to read complete system information, the mobile needs to read PBCH which contains information about the bandwidth of the LTE signal. Then the mobile needs to read the PCFICH, which gives information about the number of OFDM symbols allocated for the resource allocation messages. Finally, the last step before initiating network entry is to read the PDCCH information which conveys the allocation information to the mobile.

2.2 QoS Framework in WiMAX and LTE

In wired networks, the QoS is commonly provided by two approaches, the Integrated Services (IntServ) and the Differentiated Services (DiffServ). The IntServ [53] uses a Resource Reservation Protocol (RSVP) to reserve the resources in a network, before establishing the connection. In DiffServ services, the packets are tagged by 6-bit Differentiated Services Code Point (DSCP) based on the services requested by the end node. The packet forwarding properties in DiffServ services are associated with a class of traffic in DSCP marking.

On the other hand, the QoS support in wireless networks involves the process of providing users' requirements by the service provider. These SLAs are defined and agreed between the users and the service providers at the time of signing the service contracts. The SLA should satisfy the users' objectives such as high data rate, minimum delay, QoS guarantees, security, etc. In contrast, the service providers' objectives are to minimize the overall cost of operation and maximize their total revenue. Hence, assuring SLA for the customer is a big challenge for the service providers. For that, the ITU has a list of standards to be followed by the service providers to provide better services to users.

In WiMAX, the QoS support is an integral part of MAC layer functionality, and it is based on service flows. A service flow is a logical unidirectional flow of packets between the ASN-GW and the MS with a particular set of QoS attributes (e.g., maximum latency, throughput, etc.). These service flows are created, changed, or deleted through a series of

MAC management messages. On the other hand, the BS temporarily assigns CID for each service flow and for basic connectivity. The traffic mapping between layer-2 and layer-3 QoS for appropriate service flows is done at the ASN-GW for downlink and at the MS for uplink directions, respectively. Between the ASN-GW and the BS, backhaul transport QoS is enabled for each service flow. The IEEE 802.16 standards define five types of service classes and their QoS requirements to handle different applications efficiently.

Similarly in an LTE network, the E2E QoS is established from UE to the PDN-GW in a CN. The E2E connectivity between UE and PDN-GW in an LTE-SAE network is established using bearer service. It provides the QoS level of granularity in the LTE for different service flows.

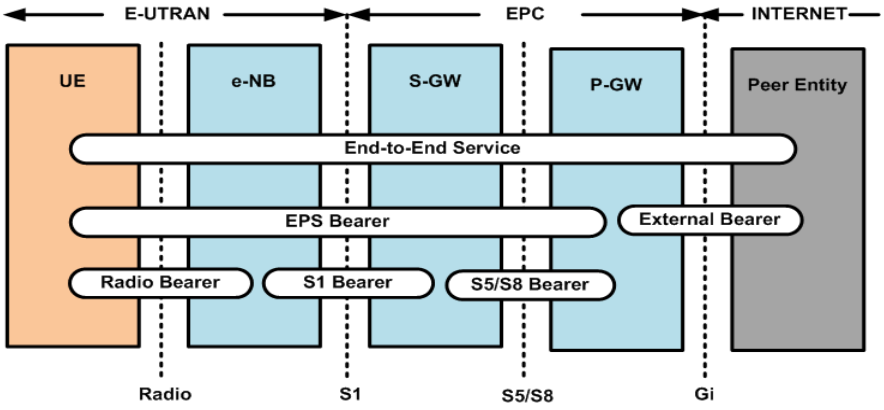


Figure 2.19 LTE-SAE bearer establishments [17]

Figure 2.19 shows the E2E QoS support and EPS bearer establishment in the LTE networks [17]. The radio bearers are established using the RRC protocol. While it carries information on radio interface, the S1 bearer forwards the information between eNB and Mobility Management Entity (MME)/SGW, and the S5 bearer transports the packets to Packet Data Network – Gateway (PDN-GW). EPS bearers are established between UE and PDN-GW. Hence, the uplink and downlink bearer mapping of an individual radio bearer and EPS bearer is done in UE, eNB, Serving-GW and PDN-GW.

2.2.1 Service Classes and Bandwidth Request Support in WiMAX Standards

The MAC layer is responsible for the scheduling of bandwidth for different users. The MAC layer performs bandwidth allocation based on the QoS provisioning of each connection. To accommodate the different user's QoS profiles, the 802.16 standard has defined five service flow classes. They are summarized in Table 2.1 [52].

Table 2.1 IEEE802.16 Service Classes and its QoS Parameter [1], [52]

QoS Category	Definition	Applications	QoS Specifications
Unsolicited Grant Service (UGS)	Real-time data streams comprised of fixed size data packets at periodic intervals.	VoIP, T1/E1, ATM CBR	Maximum Sustained Traffic Rate (MSTR), Maximum Latency Tolerance, Jitter Tolerance, etc.
real-time Polling Service (rtPS)	Real-time data streams consisting of variable sized data packets that are issued at periodic intervals.	Streaming Audio or Video	Minimum Reserved Traffic Rate (MRTR), MSTR, Maximum Latency, Traffic Priority, etc.
non-real-time Polling Service (nrtPS)	Delay-tolerant data streams consisting of variable sized data packets for which min. data rate is required.	File Transfer Protocol (FTP)	MSTR, MRTR, Traffic Priority, Request/Transmission policy, etc.
Best Effort Service (BE)	Data streams for which no data minimum service level is required.	Data Transfer, Web Browsing, etc.	MSTR and Traffic Priority
extended real-time Polling Service (ertPS)	Real-time service flows that generate variable sized data packets on a periodic basis.	Voice with Activity Detection (VoIP)	MSTR, MRTR, Latency, Jitter, Request/Transmission policy, etc.

In IEEE 802.16 standards, there are two modes of transmitting a standalone bandwidth request: contention mode and contention-free mode (polling). In contention mode, MSs send a BW_Request during the contention period. Contention is resolved using back-off resolution. The decision of standalone bandwidth request or contention is based on the service flow type and is implementation specific. Similarly, the bandwidth allocations are either Grant Per Connection (GPC) or Grant Per SS (GPSS).

In a multihop relay network, scheduling with RSs, an RS-SCH message may be used to ensure QoS requirements for UGS, ertPS, and rtPS are met. In that, the MR-BS and RSs along the path shall grant fixed size bandwidth for an UGS services. For other service flows, the MR-BS or an RS may send RS scheduling information (RS-SCH) to its subordinate RS to indicate when it will schedule a poll in the future.

2.2.2 Service Flows in LTE Standards

In LTE, the QoS profile for each service flow (EPS bearer) includes the parameters QCI, Allocation and Retention Priority (ARP), Guaranteed Bit Rate (GBR) and Maximum Bit Rate (MBR) [12]. Each of them is highlighted below.

QCI: It is a scalar that is used as a reference to control bearer level packet forwarding treatments (scheduling, admission control, etc.). The QCI mapping for different applications are shown in Table 2.2.

Table 2.2 QCI Mapping in LTE [12]

QCI	Resource type	Priority	Application
1	GBR	2	Conversational voice
2		4	Video streaming
3		3	Real time gaming
4		5	Buffered streaming
5	Non-GBR	1	IMS Signaling
6		6	Buffered Video, TCP apps.
7		7	Voice, video streaming
8		8	Buffered Video, TCP apps.
9		9	Default bearer (video)

ARP: The call admission control in the eNB uses the ARP to decide whether a bearer establishment or modification request is to be accepted or rejected.

GBR and non-GBR: Dedicated network resources related to a GBR value associated with the bearer are permanently allocated when a bearer becomes established. On the other hand, a non-GBR bearer may experience congestion-related packet losses.

One EPS default non-GBR bearer is established when UE connects to the LTE network. A dedicated bearer can either be a GBR or non-GBR bearer.

MBR: This is the maximum sustained traffic rate the bearer may not exceed; only valid for GBR bearers. An additional QoS attribute, Aggregate MBR, is used to define the total amount of bit rate of a group of non-GBR bearers.

2.2.3 MAC Layer QoS Framework and QoS Provisioning

The generic QoS architecture as defined by the 4G standard is shown in Figure 2.20. In this QoS architecture, the BS/eNB is responsible for managing and maintaining the QoS for all packet transmissions. For multihop networks with distributed scheduling, both BS/eNB and relays are responsible for maintaining the QoS for each of the service flows.

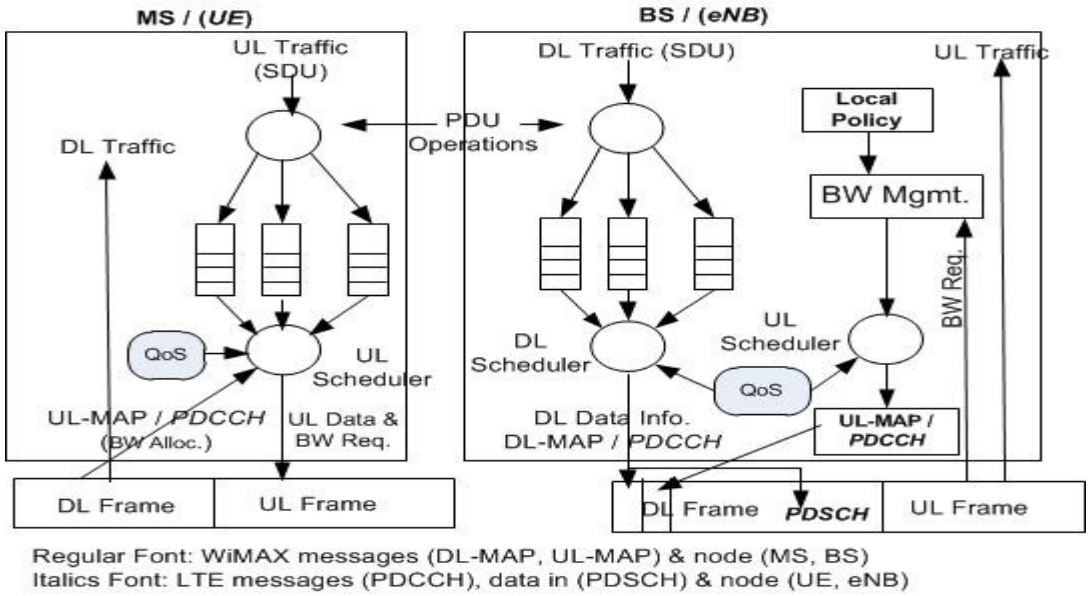


Figure 2.20 WiMAX and LTE QoS architecture

In a WiMAX network, when the MS (user) is authenticated by the network, the BS, or both BS and access RS (for a multihop WiMAX network with distributed scheduling), downloads the QoS provisioning information and stores in a LPF. Each service flow is assigned a unique 32-bit long SFID by the BS that is characterized by a range of QoS parameters including latency, jitter, and throughput assurances. Based on these QoS specifications, a service flow may be in provisioned, admitted and in active states.

Similarly in LTE, when the UE is authenticated by the network, the eNB downloads the QoS specification and Traffic Flow Template (as similar to classifier in WiMAX) of the UE. Then, eNB establishes basic and dedicated radio bearers for connectivity. These radio bearers are identified by the corresponding bearer identifiers.

Once the service flows are authorized, both BS/eNB and an access RS manages the QoS of an active service flow by allocating a bandwidth dynamically to the MS/UE. The most complex aspect of the provision of QoS to an individual packet is performed by the three schedulers: (i) downlink scheduler in the BS/eNB to manage the BS-to-MS / eNB-to-UE service flows; (ii) uplink scheduler in the BS/eNB to allocate a bandwidth for MS-to-BS / UE-to-eNB service flows; and (iii) uplink scheduler in the MS/UE to manage the MS-to-BS / UE-to-eNB flows from the allocated bandwidth. The downlink scheduler's task is relatively simple as compared to the uplink scheduler, because all downlink queues reside in the BS and their state is accessible to the scheduler. On the other hand, the queue states of the the MSs /UEs need to be obtained through BW_Requests. Then, the uplink scheduler shares the bandwidth among different users in different type of queues.

RRM Function in WiMAX and LTE:

RRM function is a set of algorithms that control the usage of radio resources. RRM functionality is aimed to improve the QoS and to maximize the overall system capacity.

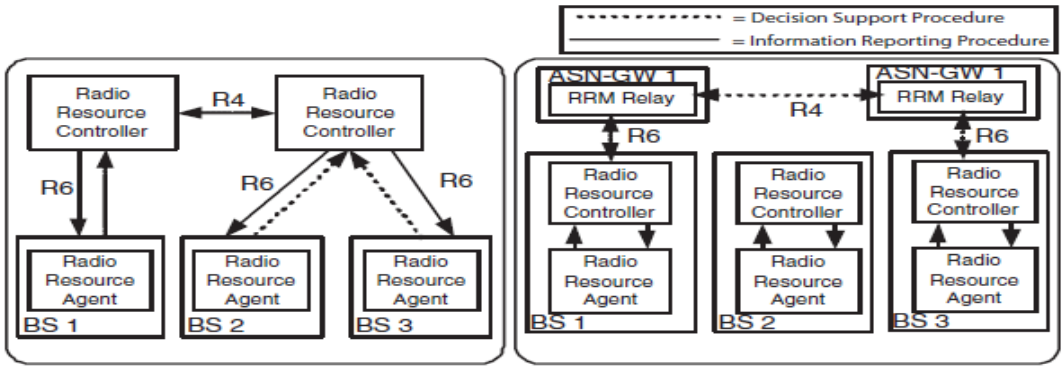


Figure 2.21 Reference models for RRM: (a) split RRM (b) integrated RRM [7]

For WiMAX networks, the major components of RRM functions in the ASN gateway and the BS are RRC, RRA and RRM relays as shown in Figure 2.21 [7]. When the

RRC and RRA are implemented separately in the ASN gateway and in the BS, they communicate over the R6 reference point. If, the RRC and RRA are implemented in the same BS, the RRM relay functions are implemented in the ASN gateway. The basic and important RRC functions (part of RRM) to control the QoS of the connections are CAC, DBA, PS, handoff, load control and power control.

On the other hand, the RRM functions in LTE perform radio bearer control, radio admission control, connection mobility control, and dynamic allocation of resources to UEs in both uplink and downlink (scheduling). These RRM functions are implemented at eNB, which is similar to integrated RRM in WiMAX networks. Therefore, various CAC and PS schemes that exist in cellular networks are described below.

Radio Call Admission Controller in 4G Wireless Networks:

The goal of the CAC mechanism is to regulate admission of new users, while controlling the quality of current connections without any call drops. The CAC is performed on a call, to determine whether the call should be admitted to the network or not, based on the availability of radio resources and the evaluation of QoS requirements. The QoS parameters to measure the performance of CAC are call blocking and call dropping ratios. The forced termination of a call in progress is more frustrating than the blocking of a new call. Thus, handoff calls are treated differently by prioritizing handoff calls over new calls. Similarly, the newly originated with high priority calls should be treated differently to satisfy the high priority customers.

Scheduling and Bandwidth Allocation in 4G wireless Networks:

The main objective of PS and bandwidth management is to efficiently allocate radio resources based on the connections the QoS parameters set. The PS could achieve fairness by allocating available bandwidth resources among all service classes according to the SLA. In WiMAX and LTE networks, scheduling for uplink and downlink is performed separately on a frame-by-frame basis. The scheduler decides which user traffic from the queues to be scheduled and then mapped into a frame first. In the WiMAX network, the scheduling information is sent using DL-MAP messages and it is used in the downlink data

burst generation. Similarly, in the LTE network, the scheduling information is signaled to UEs on the PDCCH, where the UE monitors the PDCCH on every TTI.

In general, the schedulers can be classified into homogenous and hybrid types. The homogenous schedulers strictly follow only one scheduling algorithm. On the other hand, hybrid schedulers combine more than one scheduling algorithm to satisfy the QoS requirements of multiple service classes. Some typical scheduling discipline in the homogeneous schedulers is given in Table 2.3.

Table 2.3 Homogeneous Scheduling Algorithms

Queue Discipline	Name	Functionality
RR	Round Robin	Works in a pre-emptive fashion. Provides fair treatment to all types of services. If a user does not need BW, schedules BW for the next user
WFQ	Weighted Fair Queuing	Allows traffic from different service priorities to be statistically multiplexed according to their weights
Priority	Priority	Always serves packet in the order of service flow priority. Highest priority queues are served first, and lowest priority queues are last
EDF	Earliest Due First	Serves the packets in the order of their deadline. Guarantees delay and throughput required by the traffic

Hybrid scheduling algorithm: No one homogenous scheduling algorithm meets all the QoS requirements for different service classes or all of the applications. Researchers have been trying to find hybrid algorithms that combine more than one homogeneous scheduling principle to satisfy the QoS for different classes. The main drawback in hybrid schedulers is the complexity in their design. Apart from homogeneous and hybrid scheduling principles, the schedulers in wireless networks are classified into two main categories: channel-unaware schedulers; and channel-aware schedulers. Finally, the schedulers for multihop (WiMAX) networks are further classified into centralized or distributed schedulers.

Channel-unaware schedulers: The channel-unaware schedulers are simple in design, where the schedulers assume that channels are error free.

Channel-aware schedulers: In a wireless environment, there is a high variability of the radio link, such as channel attenuation, fading and noise interference. Hence, the channel-aware schedulers consider the channel state information while scheduling the packet. Channel-aware schedulers are one kind of opportunistic scheduler, whereby each MS is assigned a priority based on its channel quality and service status.

Centralized and distributed scheduling in multihop networks: In centralized scheduling, the resource is managed by the BS/eNB and they determine the bandwidth allocations for all MSs/UEs in their MR-cells. In a multihop WiMAX network, first, the BS collects the BW_Request from different MSs and calculates the bandwidth allocation for each MS. Finally, the BS sends the grant message to all MSs. The implementation of centralized scheduling is simple in nature and suitable for downlink scheduling, but in uplink, the time between sending the BW_Request message from the MS and receiving the bandwidth allocation message from the BS is large. This significant amount of time will affect the QoS performance in the uplink traffic.

2.3 Security Architecture in WiMAX and LTE Standards

In this section, the security architecture defined by WiMAX and LTE standards is described for better understanding of existing security threats and the proposed solution. For single-hop networks, the detailed authentication and SA procedures with the BS are presented and for multihop, the additional security features are highlighted.

2.3.1. Security Support in Mobile WiMAX Networks

The security architecture defined by the mobile WiMAX network is a two-component protocol: (i) an encapsulation protocol for data encryption and authentication algorithms; and (ii) a key management protocol (Privacy Key Management – version2 (PKMv2)) providing the secure distribution of keying data from the BS to the MS [4]. PKMv2 based Initial Ranging and connectivity is shown in Figure 2.22.

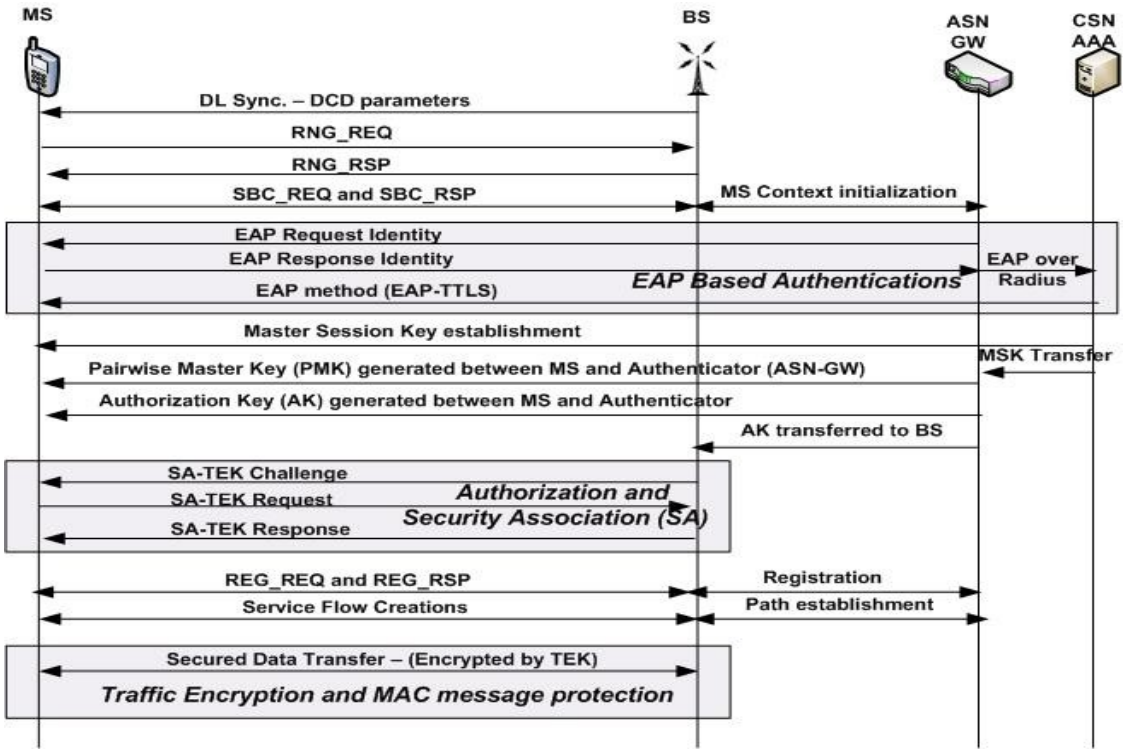


Figure 2.22 Initial ranging and network entry in mobile WiMAX [1]

As presented in Figure 2.22, after downlink channel synchronization using the specified WiMAX system parameters in the DCD message, the MS will send the ranging request (RNG-REQ) message. In turn, the BS informs the frequency, time and power offset values in the RNG_RSP message. If any collisions occur during the request, the BS sends the failure notification in a RNG_RSP message and the MS will repeat the ranging process. Once the MS has succeeded in ranging process, it negotiates for basic capabilities in the Subscriber Basic Capability Request (SBC_REQ) message. The subsequent processes: EAP authentication, authorization and SA, and then secured data transfer are shown in shaded blocks in Figure 2.22, which are described in the passage that follows.

EAP based Authentication: Authentication addresses establishing the genuine identity of the device or user, wishing to join a wireless network. The message flows in EAP-TTLS based authentication are shown in Figure 2.22. The authenticator in the Access Network Gateway (ASN-GW) sends an EAP Identity request to the MS, and the MS will respond to the request by sending PKM-REQ (PKMv2 EAP-Transfer) message. A PKM-

REQ message contains the details of SIM or X509 certificate. Then the ASN-GW forwards the PKM-REQ to the AAA server over radius protocol. The AAA server authenticates the device and provides the Master Session Key (MSK) in an EAP-TTLS protocol. Then, it forwards MSK to the authenticator. The authenticator generates Authorization Keys (AK) from the MSK and forwards to the BS. At the same time, the MS also generates the same AK from the MSK. Now, the BS and MS can mutually authenticate each other using AK.

Authorization and Security Association: Once the device or the user is authenticated by the network, the BS has to authorize the user by its unique Security Association Identity (SAID) using SA-Transport Encryption Key (SA-TEK) challenge messages, as depicted in the second shaded block in Figure 1. The Authorization Request includes the MS's X.509 certificate, encryption algorithms and cryptographic ID. In response, the BS sends the AK encrypted with the MS's public key, a lifetime key and a SAID. After the initial authentication/authorization from AAA, the BS reauthorizes the MS periodically.

Traffic Encryption and MAC Message Protection: The MS establishes a SA for each service flow where the BS provides both uplink and downlink TEK to encrypt the data. Advanced Encryption Standard - Counter with Cipher-block chaining Mode (AES-CCM) is the ciphering method used for protecting all the user data. TEK used for driving the cipher of unicast traffic is generated from the EAP authentication. TEK is refreshed by the BS periodically to add further protections. On the other hand, MAC Control messages are protected using AES-based CMAC (Cipher based Message Authentication Code), or MD5-based HMAC (Message Digest based Hashed MAC) schemes.

2.3.2. Security Support in Multihop WiMAX Networks

The security architecture defined in IEEE 802.16j is similar to mobile WiMAX standards. However, some additional features are added to support the multihop communications. The additional features are [2]:

- The network may use either centralized or distributed security mode. The distributed security mode will reduce the burden on the BS as well as reducing the delay to reestablish the SA for multihop RSs/MSs.

- An establishment of a Security Zone (SZ): SZs are the set of trusted relationships between a BS, RSs and MSs. RSs and MSs become members of a BS's SZ by authenticating using PKMv2.
- Transport tunnel connections may be established between the BS and an access RS to encapsulate the payload. For tunnel mode operation, one or more tunnels may be established between the BS and the access RS after the network entry is performed. In the tunnel mode, MAC PDUs that traverse a tunnel will be encrypted and encapsulated in a relay MAC PDU with the relay MAC header carrying the T-CID (Traffic tunnel-CID) or MT-CID (Management Tunnel-CID). The station at the ingress of the tunnel is responsible for encapsulating the MAC PDUs into relay MAC PDU where the station at the egress of the tunnel is responsible for removing the MAC header.

The security architecture in the IEEE 802.16m standard has a few modifications to adapt to the advanced air interface network conditions [3]. The modifications are:

- Only EAP based authentications are supported.
- SAs are static, no dynamic associations are supported.
- TEKs are derived at Advanced MS (AMS) not in Advanced BS (ABS) and the encryption algorithms are AES-CCM and AES-CTR.
- Three levels of MAC management message protections are supported: no protection; CMAC; and Encrypted by AES-CCM.
- Instead of re-authentication, key renewal is used (using key agreement protocol) during fast handover. AMS-ID is used for key derivation and ranging purpose.

2.3.3. Security Support in LTE Networks

The security support used in LTE networks is described in [14]. In LTE EPS, multiple SAs exist in the system to protect different layers of the network [101]. The first security layer is to protect control plane signaling and user plane data between UE and eNB. This control plane signaling between UE and eNB is also called AS signaling. The second layer security is to protect the control plane between UE and the MME, also called NAS. Third layer is the long term SA between UE and the Home Subscriber Server (HSS).

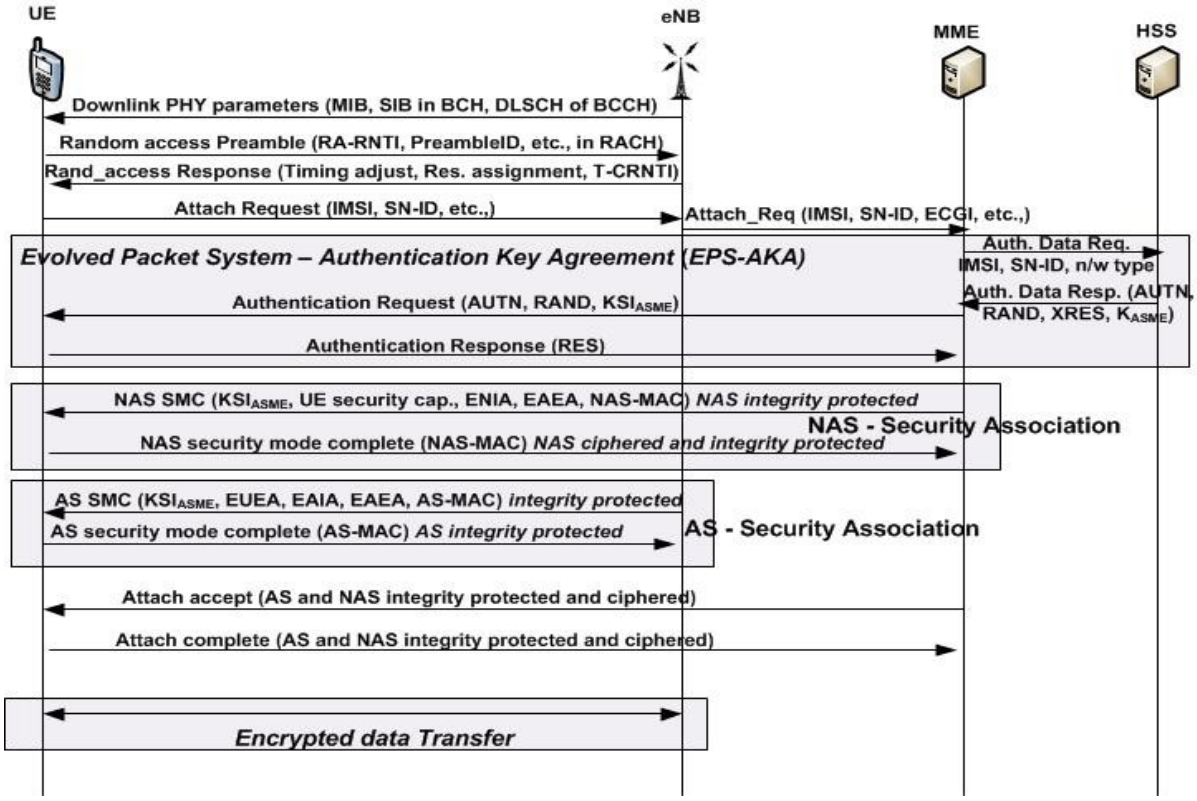


Figure 2.23 Authentication and SAs during UE's network entry in LTE

Figure 2.23 shows the establishment of AS and NAS security contexts during UE's initial attach. The network elements in LTE EPS architecture are similar to those used in WiMAX, but several terms are different in LTE: for example, UE replaces MS, eNB replaces BS, MME replaces ASN-GW and HSS replaces CSN-GW. As in the WiMAX network, the UE first synchronizes with the downlink channel to receive and decode the cell system information in order to communicate and operate properly within the cell. The downlink, MIB is transmitted using the Broadcast Channel (BCH), while System Information Blocks (SIBs) is transmitted using the downlink shared channel (DL-SCH).

The next step in initial attaches and connection setup procedure is Random Access. Random Access procedure nullifies the timing offset for uplink communication. Also in Random Access procedure, a unique Cell Radio Network Temporary Identifier (CRNTI) is assigned to the terminal. Once the Random Access Preamble is transmitted, the UE monitors for Random Access Response, including CRNTI with the same PreambleID. If the received preamble identifier that does not match the transmitted Random Access

Preamble, the Random Access Response is considered not successful and the UE continues until the count reaches PREAMBLE_TRANS_MAX.

Authentication in EPS AKA: The mutual authentication between user and the network takes place by ensuring the Serving Network (SN) authenticates the user's identity and the UE validates the signature of the network provided in the Authentication Token (AUTN). During the initial Attach Request, the UE send its identity and Serving Network Identity (SN ID), and eNB forwards the information along with its identifier to the MME. Then, the MME sends a request to the Home Element (HE) querying the authentication vector for a specific SN ID and IMSI. The HSS in the HE, responds with an authentication vector. Each vector has AUTN, RAND, XRES and K_{ASME}. The derived keys, K_{ASME}, Ck, and Ik are stored in a key set and identified by a Key Set Identifier (KSI_{ASME}). The KSI_{ASME} is sent by the MME to the UE in the Authentication Request message along with the AUTN and RAND. The Universal SIM (USIM) computes the K_{ASME}, Ck, Ik, and the RES, stores K_{ASME} along with the received KSI_{ASME}, and sends back the calculated RES in the Authentication Response message. The MME compares the RES with the received XRES from the HSS. If the RES and XRES are the same, the MME starts procedure for ciphering and integrity protection at the next establishment of an NAS signaling connection without executing a security mode command (SMC) procedure [98].

Security Association for ciphering and integrity protection: Ciphering (encryption) ensures the confidentiality of the data communicated over the radio link. In EPS AKA, ciphering is applied to both NAS and AS signaling messages and user plane data at the AS. On the other hand, integrity protection ensures that the data received at an entity is what was sent by the sender. Integrity protection is applied to all signaling messages at both the NAS and AS levels. In EPS AKA all integrity and cipher keys are derived from the master key K, which is unique to a user and is stored in a secure manner in both the USIM and the HE. Hence, the HSS in the HE and UE use the same procedure to generate the Ck and Ik from the K using same keying functions. Then, HSS forwards the Ck and Ik to the MME. K_{ASME} is also computed as part of this procedure in HSS and UE. The subsequent session keys for ciphering and integrity protection are derived using K_{ASME}.

2.3.4. Security Support in Multihop LTE Networks

To support multihop operations, RNs are introduced and some additional functions are added to the eNB that are: (1) S-GW/P-GW functionality for the RN; and (2) proxy functionality between the RN and MME-UE. This new eNB is called DeNB. The additional security functions are [14]:

- A removable Universal Integrated Circuit Card (UICC) is inserted into the RN to provide authentication between itself and the network.
- AS level encryption is switched on between the RN and DeNB.
- The RN acts as UE for DeNB and eNB for regular UEs. Hence, distributed security architecture is realized in multihop LTE networks.

One-to-one binding is realized between RN and a USIM, either by using symmetric pre-shared keys or by certificates. For certificates, the UICC inserted into RN contains two USIMs, where USIM-INI is used for initial IP connectivity in an unsecured channel and USIM-RN communicates only via a secure channel.

2.4. Network Coding for 4G wireless networks

Network coding is a popular technique in both wired and wireless networks for data distribution. Network coding utilizes information theory to encode several packets. The receiver decodes these packets to recover the original data when it receives enough coded packets. Network coding could reduce the times of data transmissions, which is greatly helpful while there is scarce medium for transmission. Hence, the recent WiMAX standard introduces network coding for retransmission in order to guarantee that data are successfully distributed to all the MBS users. The network coded packets are transmitted separately in an OFDMA frame, and the necessary MAC supports for network coding are described in the IEEE 802.16m standard. Also, the network coding is studied in many research efforts for various applications in WiMAX LTE networks such as redundancy, packet retransmission, handover scenarios, and etc. There are several variants including XOR network coding, Reed-Solomon based network coding, Random Linear Network Coding (RLNC), etc.

2.4.1. XOR Network Coding

XOR-based network coding is the simplest algorithm to encode the data packets and they make use of XOR operation while encoding the packet. Consider a simple multihop network topology as shown in Figure 2.24 [8].

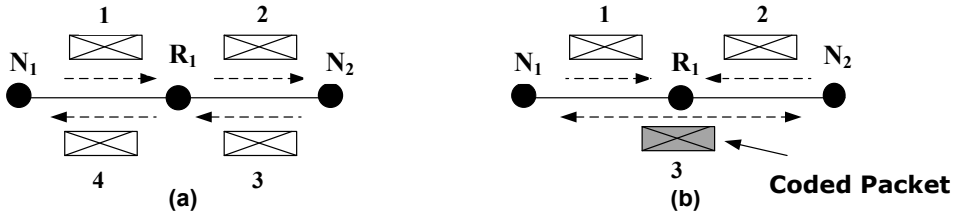


Figure 2.24 (a) Traditional packet forwarding (b) Network coding [8]

Assume that the nodes N1 and N2 want to transmit a packet to each other, which is relayed by the node R1. Figure 2.24a shows the behaviour of nodes without the application of network coding. Here, N1 transmits a packet to the next hop R1 in slot 1. The received packet is relayed by R1 in slot 2 to node N2. Similarly, a packet transmitted by N2 addressed to node N1 is transmitted and relayed in slots 3 and 4, respectively. Figure 2.24b shows how the same data can be transferred to the destinations using a simple form of network coding. The relay node R1 receives the packets to be relayed in slots 1 and 2, and then R1 encodes the received packets using the XOR operation, e.g., N1⊕N2. Next, R1 broadcasts the XOR-coded packet in slot number 3. Hence, both N1 and N2 recover the data address to them using the XOR decoding operation with the preserved local copies of the packets that they transmitted. For example, the node N1 transmits the codeword of "01110111" to R1 in time slot 1. In slot 2, the node N2 forwards the codeword "10101010" to R1. Next, the relay R1 does the XOR operation on received codewords in slot 1 and 2 that results "11011101". The XOR encoded information "11011101" is broadcasted in slot 3. Finally, N1 does the XOR operation on the received codeword "11011101" with the transmitted code "01110111" and retrieves the original information. Similarly, N2 retrieves the original information that was transmitted by N1.

2.4.2. Reed-Solomon based Network Coding

Reed-Solomon codes are block error correcting codes in the digital communications area. A Reed-Solomon code is specified as (n, k) for s-bit symbols. This means that the encoder takes k data symbols of s bits and adds parity symbols to generate an n symbol codeword. The generated codeword is shown in Figure 2.25 [19]. A Reed-Solomon decoder can correct up to t symbols that contain errors in a codeword, where 2t = n-k. A popular Reed-Solomon code is (255,223) with 8-bit symbols. Each codeword contains n = 255 code word bytes, of which k = 223 bytes are data and 2t = n-k = 32 bytes are parity. If the locations of the symbols in error are not known in advance, then a Reed-Solomon code can correct up to t = (n − k) / 2 erroneous symbols. This implies t = 16. The decoder can correct any 16 symbol errors in the code word. The Reed-Solomon based network coding technique makes use of Reed-Solomon codes for encoding the coded packets.

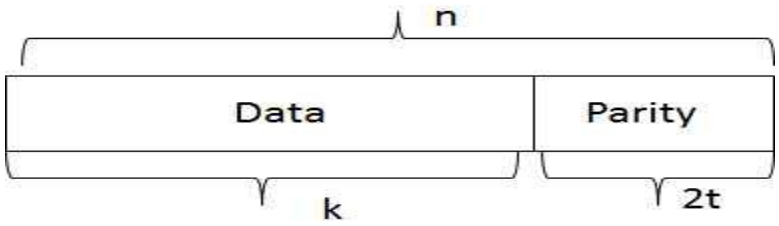


Figure 2.25 RS codeword [19]

2.4.3. Random Linear Network Coding

In RLNC, the data segment is divided into n blocks, denoted as [b1, b2, · · · , bn], where each block has a fixed number of bytes. The sender randomly chooses a set of coding coefficients [c1, c2, · · · , cn] in the Galois field GF(2^8), and produces one coded block x as a linear combination of the original data blocks [19]:

$$x = \sum_{i=1}^{n} C_i b_i \qquad (2.8)$$

The sender keeps on transmitting the coded blocks to the receiver. At the other side, the receiver collects the coded blocks and progressively decodes the segment using Gauss-Jordan elimination. Immediately after n linearly independent blocks have been received for

a segment, the receiver is able to recover the original data segment, and sends the ACK back to the sender. This feedback will request the sender to stop the transmission of the current segment and switch to the next segment. During this process of transmission, it is not necessary to transmit ACK/NACK and retransmission packets with each individual packet, as in HARQ, which generates much overhead.

The network coding techniques can be applied for different applications in the WiMAX networks. However, to best of my knowledge no one analyzed the network coding technique for WiMAX relay node failure.

Chapter 3. Literature Review

This chapter covers the literature review including several works done by researchers in three different areas: (1) RRM framework that includes CAC policies and PS schemes in WiMAX and LTE networks; (2) existing security threats and solutions in WiMAX and LTE networks; and (3) Relay node protection scheme in multihop wireless networks using network coding, to maintain the QoS of the network.

3.1 Literature Review of RRM Framework in 4G Wireless Networks

The QoS of 4G multihop wireless networks is mainly based on the design of efficient RRM functions. The RRM function mainly relies on CAC, PS and DBA modules. Since the DBA function is closely integrated with PS function, the CAC and PS schemes are studied for this research.

3.1.1 Literature Review of RRM Framework in WiMAX Networks

For CAC and scheduling, many research efforts have been conducted for fixed and mobile WiMAX networks. The first part identifies the research gap in CAC and design, and next part focus the PS schemes in mobile and multihop WiMAX networks.

3.1.1.1. Literature Review of CAC in WiMAX Networks

In general, the aim of the CAC design is to minimize the Call Drop Probability (CDP), maximize the system utilization, assure bandwidth and delay guarantee for the users. From the existing research efforts, the available CAC methods for wireless networks fall into the following categories [20].

- Centralized or distributed approaches
- Parameter or measurement based approaches
- Uniform cell based, non-uniform cell based or user based

Centralized or distributed CAC: In a distributed CAC, the admission control decision is made based on the information from the BS, ASN gateway and an access RS. Since the CAC decision is based on information from multiple nodes, the distributed CAC scheme has the complete knowledge of the network. On the other hand, the BS alone makes the final decision in the centralized CAC design. Therefore, the centralized CAC can make a quick decision based on limited information available only at the BS.

Measurement based Admission Control (MBAC) or Parameter Based Admission Control (PBAC): In the MBAC scheme, the admission control decisions are made based on network measurements of actual traffic loads. The behaviour of the existing calls is observed to make admission decisions, rather than assuming a statistical model or bandwidth calculation. On the other hand, the PBAC scheme calculates the amount of system resources required to maintain a set of flows based on a prior flow of traffic descriptions or stochastic model. The admission decision is based on the specifications of ongoing and new calls. The parameter based approach offers assured QoS but often yields low network utilization.

The MBAC policy is adopted to satisfy both the minimum bandwidth and maximum delay guarantees [27]. However, the authors did not consider all service types and CDP for handoff users. On the other hand, the classification of parameter based CACs are based on the parameter used to make a decision [20]. However, the most important reason is to guarantee the QoS. Figure 3.1 shows some examples of parameter based CAC methods studied for WiMAX networks [20].

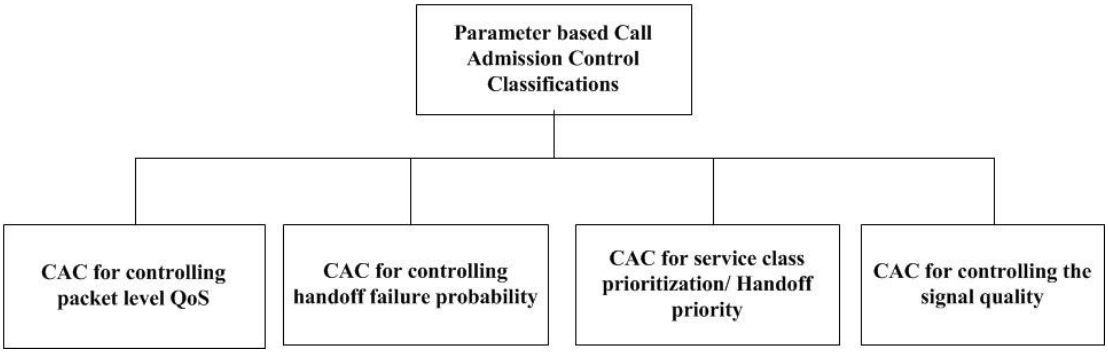


Figure 3.1 Parameter based CAC classification [20]

CAC for controlling packet level QoS: As the QoS is one of the main targets of 4G wireless networks, many CACs schemes are concentrated on packet level QoS parameters such as bandwidth, delay etc. In [28] and [29] the authors proposed a scheduling algorithm and CAC policy for QoS in IEEE 802.16 fixed WiMAX, where the CAC scheme provides both bandwidth guarantees to all service flows and delay guarantees to rtPS service flows. Both CAC schemes used the TB principle. The main research gaps in those papers are not considering bandwidth utilization, and their proposed scheme considers a fixed network environment. In [30], the CAC scheme for mobile WiMAX was proposed to satisfy both bandwidth and delay guarantee. The proposed CAC scheme provides higher priority to handoff calls and UGS calls. The connections are admitted, only when they satisfy the delay and bandwidth requirement. Admission control using a game-theoretic approach was studied in [38] for IEEE 802.16 networks. In [38], the delay performance of real-time traffic has been analyzed based on a queuing model. A new call will be accepted when equilibrium can be reached between the BS and a new connection. In [39], the EDD based combined CAC and scheduling algorithm was studied to support the QoS requirements of real-time video applications in IEEE 802.16 networks. The delay based scheme succeeds in providing good throughput improvement with acceptable delay and fairness requirements among SS.

CAC for controlling call drop probability: Certain CAC methods are controlling the CDP for handoff users using Guard Channel (GC) policy [31] and Fractional Guard Channel Policy (FG) [32]. The GC policy was introduced by Hong and Rappaport in [31], and became a well-known approach that reserved a number of channels to handoff calls. The amount of GCs, reserved by the GC policy, is denoted by 'T'. The GC policy starts to decline new calls when the channel occupancy goes beyond a certain threshold, T, until the channel occupancy becomes below T. This policy admits handoff calls as long as channels are available. In addition to bandwidth reservation, some CAC methods apply bandwidth degradation policy to improve the CDP for handoff calls. In [33] and [34], bandwidth degradation policy is introduced in the CAC methods to admit handoff calls. In bandwidth degradation, the bandwidth assigned to individual active service flow (admitted connection) is reduced during the CAC process in order to accommodate a greater number

of connections. In [34], the authors proposed a dynamic CAC scheme for IEEE 802.16d fixed WiMAX. The proposed CAC scheme uses bandwidth reservation and degradation from maximum rate to minimum reserved rate. This scheme does not provide any delay guarantees to the admitted connections and also does not support mobility. Therefore, it is not directly applicable to mobile WiMAX. The CAC proposed in [35] reserves an adaptive temporal channel bandwidth for mobile users based on most recent requests. However, the scheme does not provide any delay guarantee, and the reserved bandwidth is wasted when there are few or no handoff calls existing in a network.

CAC for service class prioritization/ Handoff priority: One of the major challenging tasks in the design of QoS provisioning is QoS differentiation between service classes. In the QoS differentiation, handoff calls are given high priority in the design of certain CACs [36]. Similarly, in [37], the authors gave priority to handoff connections by allowing them to use the degraded bandwidth of the admitted connections. However, both the schemes do not provide any delay guarantees to admitted connections.

CAC for controlling the signal quality: Some CAC methods are based on signal quality approaches, where a new call flow is accepted, only when the Signal to Interference is greater than a predefined threshold value [20].

3.1.1.2. Literature Review of Packet Scheduling Scheme in WiMAX Networks

As similar to CAC, many uplink and downlink scheduling algorithms have been analyzed for the fixed and mobile network environment. However, very few research efforts are concentrated on multihop 4G wireless networks. Some important scheduler designs under different classifications studied for the WiMAX environment are given below.

Channel-unaware homogenous scheduler: The earlier, WRR and Deficit Weighted Round Robin (DWRR) schedulers [40-42] have been applied to WiMAX scheduling. The weights can be used to adjust for the throughput and delay requirements. The DWRR scheduler can be used for variable size packets. The WFQ scheduling scheme is used for variable size packets [22]. In WFQ, the weights play an important role to assure the QoS,

and it can be calculated based on the queue length [43], the minimum reserved rate of the connection [44] and the pricing of the connection [45]. Here, the goal is to maximize the service provider revenue. The main drawback of the WFQ scheduler is that it is difficult to find the optimum weights for practical implementations.

In order to guarantee the QoS for different classes of service, priority based schemes can be used in the WiMAX scheduler [46-48]. The simple priority schedulers are often used in practical implementations, but they do not guarantee the specified QoS for nrtPS and the performance of BE services is highly affected. To mitigate the starving of the lower priority service class, Deficit Fair Priority Queuing (DFPQ) was introduced in [50]. Instead of assigning priorities based on service classes, queue length was used to set the priority level in [49]. However, the priority assignment based on queue length and others may not provide the high QoS for real-time services at high load conditions.

The delay based algorithm is specifically designed for both real-time traffic and non-real-time traffic, where the delay tolerance is the primary QoS parameter. Earliest Deadline First (EDF), or EDD, is the basic algorithm for the scheduler to serve the connection based on the deadline [52-54]. This algorithm, however, does not guarantee the throughput for UGS [51].

Channel-unaware hybrid scheduling algorithm: No one homogenous scheduling algorithm meets all the QoS requirements for different service classes [56]. Hence, researchers have been trying to find hybrid scheduling algorithms to satisfy QoS for different service classes. The proposed hybrid scheme in [55] used the EDF for the rtPS service class and WFQ for the nrtPS and BE service classes. In [56], a hybrid scheduling algorithm that combines EDF, WFQ and FIFO scheduling algorithms was advocated. The overall allocation of bandwidth is done in a strict priority manner. EDF scheduling algorithm is used for the rtPS class; WFQ for the nrtPS class; and FIFO for the BE class. Besides the scheduling algorithm, an admission control procedure and a traffic policing mechanism were used for the simulations. However, the main challenge in the hybrid scheduling is the selection and implementation of different scheduling policies. Further, combination of more than one schedulers such as, EDF, WFQ and FIFO schedulers may

increase the complexity of the system. The QoS performance of some existing hybrid and homogeneous schedulers was analyzed in [52] that are given in Table 3.1.

Table 3.1 Performance Analysis of Existing Schedulers [52]

Scheduler	Inter-Class Fairness	Complexity	QoS Performance (Throughput, Delay, Packet Loss)
Homogenous Schedulers			
Weighted Round Robin (WRR)	High	Simple	Unfair for variable size packet. Weight selection is critical.
Weighted Fair Queue (WFQ)	Medium	Complex	Optimum and dynamic weight selection are needed to assure QoS.
Priority	Low	Simple	QoS of nrtPS and BE service classes are poor.
EDD	Medium	Simple	Delay performance is assured. Throughput and packet loss is poor for UGS and rtPS.
Hybrid Schedulers			
EDD + WFQ	Medium	Complex	Dynamic weight selection is needed for WFQ to assure QoS.
EDD + WFQ + First In First Out (FIFO)	Low	Complex	Dynamic weight selection is needed for WFQ to assure QoS.

Channel-aware schedulers: These are also called as an opportunistic schedulers, whereby each MS is assigned a priority based on its channel quality and service status [57]. The standard provides a basic link adaptation framework that's MCS can be adapted to the channel conditions, but the scheduling and bandwidth allocations are implementation specific. In [52], various channel-aware schedulers are well analyzed for different QoS objective functions. In [59 and 60], a channel-aware Deficit Round Robin (DRR) and Dynamic Hybrid Scheduler (DHS) are studied for the mobile WiMAX environment. The DHS scheduler in [60] is designed to balance between two scheduling disciplines such as guaranteed and a dynamic delay based rate allocation policy. Thus, the scheduler combines their merits in an effective manner.

Multihop schedulers: Only a few schedulers are studied for the multihop WiMAX network [61-63]. In [61], a Queue-aware scheduling algorithm is studied under concurrent transmission scenarios for a multihop relay environment. In that, a back-pressure flow control mechanism reflects the queue status of each RS. Then, the linear program scheduling principle is used to schedule the packet based on queue status which maximizes the network throughput and achieves fairness. In [62], OFDMA Relay Scheduler (ORS) is studied for the multihop WiMAX network. In that, the scheduler adaptively computes the zone boundaries (relay and access) in the uplink scheduling frame, based on the number of RSs and MSs, the bandwidth demands and the link conditions. Finally in [63], uplink scheduling mechanism with Multi-device Transmission and Maximum Latency Fulfillment (MT-MLF) is studied for the multihop WiMAX network. In MT-MLF, the interference relationships among devices within the coverage of one BS are identified first. Based on that information, MT-MLF schedules non-interfering connections in a data burst to improve the average system transmission rate.

3.1.2 Literature Review of RRM Framework in LTE Networks

As similar to WiMAX networks, many CAC and scheduling algorithms were analyzed for LTE networks. Within that, few important works are considered for this literature review. The CAC scheme proposed in [65] combines the complete sharing and virtual partitioning resource allocation model and develops a service degradation scheme in case of resource limitations. They modeled the system as the K-dimensional Markov Chain model. A delay-aware CAC algorithm proposed in [68] utilizes statistical data for packet delay and PRB utilization in order to guarantee packet delay requirements for ongoing calls.

For scheduling, Maximum Rate (MR), Round Robin (RR), Proportional Fair (PF), Exponential/Proportional Fair (EXP/PF) and Modified Largest Weighted Delay First (M-LWDF) scheduling algorithms were simulated in [73]. From the simulation results, the authors showed that the M-LWDF algorithm outperforms other PS algorithms by providing a higher system throughput, supporting a higher number of users and guaranteeing fairness at a satisfactory level for video services. An adaptive proportional fair scheduling is compared with PF scheduling in [66]. The adaptive PF scheduling changes the fairness

based on channel condition. In [67], authors proposed two scheduling algorithm, where algorithm-1 schedules the urgency packet, first based on delay and then the remaining packets. The algorithm-2 schedules Radio Bearers (RBs), based on channel state information. From their results, algorithm-1 outperforms algorithm-2 in delay and packet loss rate. Similarly, a delay-aware PS algorithm is simulated in [69] and [70] that consider QoS requirements of delays for various traffic classes, channel conditions, and fairness. In [70], delay-optimal opportunistic scheduling using EXP and LOG rules has been presented for delay sensitive applications.

3.2 Literature Review of WiMAX and LTE Networks Security

The main cause for the MAC layer security threats in 4G vehicular networks is due to certain unprotected MAC management messages between MS and BS. When the control messages are in plain text, the attackers/intruders can easily spoof, modify, and reply those control messages for the intended receiver node. The severity of the security threats may vary based on the modification of those control messages. Similarly, the attackers may send the continuous false packets unnecessarily to the receiving node for the water torture attacks. Many research efforts have been published on MAC layer security threats in both WiMAX and LTE networks and a few of them discussed the implementation of IPSec security for WiMAX networks. This section systematically analyzes the security threats that exist in WiMAX and LTE networks separately in the following subsections.

3.2.1. Literature Review of WiMAX Network Security

The major security threats in mobile WiMAX networks are DoS and rogue BS Reply attacks during MS initial network entry, latency issues during handover, downgrade attack, bandwidth spoofing, etc. This DoS and rogue BS Reply attack that exists before authentication is solved by the Diffie-Hellman (D-H) key agreement [76]. Also, the D-H key based Secured Initial Network entry Process (SINP) [77] solves Auth-Request vulnerability issues. The Auth-Request vulnerability can also be solved by either introducing nonce or time stamps [80]. When comparing nonce and time stamp, time stamp

is more secure and avoids the replay attack. In [86], the authors suggested the Wireless Public Key Infrastructure (WPKI) to solve the authentication vulnerability.

For Latency issues during handover and unsecured pre-authentication, there are three possible approaches from the existing works. The first is a shared key based EAP method using MSK; using old MSK, both MS and authenticator generate the new AK before handover [78]. The second approach for reducing the handover latency is using Public Key Infrastructure (PKI) [81] for mutual authentication between target ASN and the MS before the handover. Since the messages are encrypted using the public key, security is assured. The last approach is the Mobile IP (MIP) scheme [87]. In this scheme, pre-negotiation with the target BS is in layer 3 MIP tunnelling protocol. The handover latency can be reduced by simple pre-authentication schemes [83]. However, pre-authentication schemes are inefficient and insecure [78].

For multihop WiMAX networks, hop-by-hop authentication of relay nodes and the selection between centralized or distributed security architecture are major security problems that was addressed in [93] and [94]. The authors in [93] proposed a hybrid authentication scheme, in which, initially, the MS will be authenticated by the service provider's authentication server; later, the authentication was managed by the access RS. To establish the distributed hop-by-hop authentication, the RSs exchange their AK through the BS. Since the AK is the root of all other keys generation, exchanging AK is not advisable. In [94], the distributed trust relationship is established between RSs using k-degree bivariate polynomial keys generated by the AAA server. This leads to the high overhead in AAA server, because a single AAA server has to manage the whole service provider's network. Another overhead in [94] for mobility-related scenarios is a new shared secret must be distributed. In [90], authors addressed the security threats in multihop wireless mesh networks when the network elements use network coding for forwarding the packet. They analyzed both intra-flow and inter-flow network coding security threats.

A comprehensive taxonomy of various attacks and countermeasures on single-hop WiMAX networks was reported in [128]. However, in the recent multihop WiMAX standard (IEEE 802.16m) [3], once the user is registered with the home network the security layer may use three levels of protections for the MAC management messages, i.e.,

No protection, CMAC, and Encrypted by AES-CCM. As a consequence of adding the encryption support for MAC messages, some of the security threats discussed in [128] no longer exist for multihop WiMAX, which will be highlighted in Table 3.2. Further, the security threats that exist in multihop WiMAX networks were not discussed in [128]. Therefore, the security threats and countermeasures discussed in [128] and the security threats in multihop WiMAX networks [129] have been investigated and analyzed, which are summarized in Table 3.2.

Table 3.2 Security Threats in WiMAX Networks

Category	Attack	Network mode	Existing works / short description
Ranging attacks	• RNG-RSP DoS Attack • RNG-RSP Downgrading Attack • RNG-RSP Water Torture Attack • RNG-REQ Downgrading Attack • RNG-REQ DoS Attack • MOB ASC-REP DoS Attack	Exist in both single-hop and multihop networks (Initial RNG messages are in plain text. in 802.16m std.). No longer exist in 802.16m	[77], [130], [131] to [135] For these attacks, the attackers spoof, modify and reply the RNG-REQ and RSP messages. Association report message (MOB ASC-REP) is no longer in 802.16m
Power saving attacks	• MOB TRF-IND Water Torture Attack • BW stealing and UL Sleep DoS attack • Secure Location Update (LU) Distributed DoS (DDoS) Attack	Only in single-hop networks, no longer exist in IEEE802.16m. Control messages after registration may be encrypted.	[77], [121] and [137]. For power saving, the MS may go the sleep and Idle mode. In that mode, MS updates the location for handover and the BS informs the MS for data arrival. The attackers play in those control messages.
Handover attacks	• MOB NBR-ADV Downgrading Attack • MOB NBR-ADV DoS Attack • Handover latency and re-authentication	Only in single-hop networks, no longer exist in IEEE802.16m.	[77] and [131]. The attackers play with neighbour advertisement message and long handover delays for re-authentication of MS from the home nodes.

Mis. attacks	• SBC Downgrade Attack • FPC Downgrade Attack • FPC Water Torture Attack • RES-CMD DoS Attack • DBPC-REQ DoS Attack	Exist in both Only in single-hop Only in single-hop Only in single-hop Only in single-hop	[76], [131], [134], [135] and [136]. The attackers modify the control messages which are in plain text and used for offset correction.
Attacks against WiMAX security	• AUTH-REQ Replay DoS Attack • PKM-RSP: Auth-Invalid DoS Attack • DES CBC IV Attack • DES CBC Insecurity Attack	Exist in both Only in single-hop Only in single-hop Only in single-hop	[80], [120], [131] and [134]. For these attacks, the attackers modify and reply the key request and response message during authorization and SA in Figure 1.
Multicast / Broadcast attacks	• GTEK - Group Key DoS Attack • GTEK Theft of Service Attack • MCA-REQ DoS Attack	Only in single-hop networks, no longer exist in IEEE802.16m.	[122] and [135]. The attackers modify and reply in key request and response messages in MBC service.
Mesh mode attacks	• Malicious Sponsor Node Attacks • PKM-REQ: Auth Req. Replay Attack • PKM-RSP Replay Attack • PKM-REQ: Key Request DoS Attack	No specific discussion of mesh mode in 802.16 - 2009 and in 802.16m. Exist only in 802.16e	[138] and [139]. The attackers act as a fake node for malicious attack. For the other attacks, the attackers modify and reply the key request and response message during authorization.
Multihop security threats	• Rouge relay node attack • Hop-by-Hop authentication • Network coding specific threats	Exist only in multihop WiMAX networks (802.16j and 802.16m)	For rouge RS, the attacker act as a fake RS node [129]. Other two attacks are described in our previous work [46].

On the other hand, ISPs have tried IPSec in practice for the implementation perspective. The default security mechanism provided by the layer-3 Virtual Private Networks (VPNs) is IPSec. However, IPSec affects the QoS performance, as the 40-byte IPSec header in each packet consumes additional bandwidth. While providing strong security for an access network with IPSec, the existing QoS support should not be affected. Similar studies have been conducted only in simulations [91], [92] and [123]. Actual measurements are essential for practitioners and researchers for better analysis.

3.2.2. Literature Review of LTE Network Security

Many research efforts in LTE networks are concentrated on the disclosure of user identity. In [99], authors proposed a scheme for assuring end-to-end user identity privacy to the users of LTE. In the proposed scheme, knowledge of the permanent identity of the user is restricted to the UE and the HE where Dynamic Mobile Subscriber Identity (DMSI) is transmitted by the UE instead of the IMSI. In [105], authors discussed the lack of identity protection at the first initial attach and the lack of perfect forward secrecy in the EAP-AKA. For the perfect forward secrecy issue, Password Authenticated Key Exchange by Juggling (J-PAKE) protocol was proposed in the authentication process, instead of the AKA protocol. The performance of various authentication protocols such as Password Authentication Protocol (PAP), Lightweight Extensible Authentication Protocol (LEAP), and EAP-TLS were implemented on a LTE testbed environment [103]. From the experimental results, EAP-TLS provided the robust security than PAP and LEAP.

A comprehensive survey of various attacks and solutions in LTE networks was presented in [140]. In [140], security threats are categorized based on the location of the network or security domain. The major categories are vulnerabilities in: (i) access network, (ii) IMS domain, (iii) HeNB, and (iV) MTC domain. However, this research work focuses only on the security threats in the access network. The various security threats in a LTE access network have been studied and summarized in Table 3.3. Further, the DoS and rogue eNB reply attack in LTE access procedure was newly identified, which is one of the major security threats in LTE. The detailed description of DoS and rogue eNB reply attack is presented immediately after the Table 3.3.

Table 3.3 Security Threats in LTE Networks

Category	Attacks, existing works	Short description / Comment
LTE System Architecture	Injection, modification, eavesdropping attacks [125], [126]	The occurrence of these security threats are due to flat IP-based architecture of the 3GPP LTE networks.
	HeNB physical intrusions [140]	The actual implementation of HeNB is in unsecure region of the Internet.
	Rogue eNB/RN attack.	The attackers may act as a legitimate

	[103]	eNB/RN. Also, it is possible to insert traffic before the authentication takes place.
LTE Access Procedure	DoS/Reply attacks during network attach	As this attack is identified newly, a detailed description is provided below this table.
	Privacy protection [103]	There are many instances resulted in disclosure of the IMSI
	IMSI - water torture attacks [103]	Attackers constantly send fake IMSIs to overwhelm the HSS/AuC. Henceforth, the HSS has to consume its computational power to generate excessive authentication vectors for the UE.
Handover attacks	Lack of backward security [141].	During handover, key chaining architecture is used to derive the key for target eNB. Hence, attacker may compromise source eNB to obtain subsequent keys.
	Location tracking [119]	The passive attacker can determine the location of the UE by sniffing the CRNTI information, because CRNTI is transmitted in clear text.
	De-synchronization attacks [142].	The attacker can disrupt refreshing of the NCC value by either manipulating the handover request message
	Replay attacks [142].	The attacker may send a previous handover request of legitimate UE to target eNB due to NCC value mismatch, the actual connection is aborted.
Miscellaneous attacks	Lack of sequence number (SQN) synchronization[127]	EAP-AKA protocol is used for authentication of UE from non-3GPP access that causes this attack.
	Signaling overhead [124]	When the UE stays in the SN for a long period, authentication between the SN and the HN requires unnecessary signaling overhead.
	additional bandwidth consumption [119]	Attackers may request more data to send than are actually buffered by the real UE. If the eNB sees many fake reports, the admission controller may not accept the newly arrived UE.
Multihop network	Rogue RN attack	(same as the rogue RN attack in LTE system

security threats		architecture threats category)
	Network coding specific threats	Pollution and entropy attacks may be introduced due to network coding

DoS and rogue eNB reply attack during initial attach: In LTE networks, DoS attacks may be possible during the initial attachment because the UE is sending MAC messages in plain text to eNB. DoS attack during the initial attachment is very critical as the UE cannot register with the home network. This is similar to the DoS attack in WiMAX networks during initial network entry. During the Random Access process, first the UE sends Random Access Preamble to eNB and waits for the response until the predefined time limit. eNB responds to UE for timing adjustments and bandwidth allocation by sending an Attach Request message along with the PreambleID. If the received Random Access PreambleID does not match the transmitted Random Access Preamble, the Random Access Response is considered not successful and the UE continues the Random Access process until the count reaches PREAMBLE_TRANS_MAX. Since the response is in plain text, an attacker can easily change the PreambleID continuously. As a result, UE cannot register with the home network and it leads to the DoS attack. On the other hand, security threats for multihop LTE networks are still under research, because, the standard finalized the security architecture recently [14].

3.3 Literature Review of Relay Node Protection in Multihop Wireless Networks

Network coding has recently been introduced as a new transmission paradigm in wireless networks [97]. Initially network coding was introduced for wired networks. Even though network coding is ideally suited for wired networks it has some limitations in traditional wireless cellular networks due to the centralized network architecture and the occurrence of interference in the transmission of network coded data. Therefore, the extension of network coding to wireless networks is not straightforward, but network coding is well suited for multihop wireless networks for its reliability. On the other hand, the recent research efforts are concentrated on relay node protection using network coding

[106] – [111]. In [106], the author addressed the problem of many-to-one flows in Wireless Mesh Networks (WMNs) and wireless sensor networks. A polynomial time algorithm was presented to perform the coding with {0,1} coefficients for router (relay) nodes. They also analyzed the required time slots for data transmissions between the sender node and the receiver node using their network coding scheme with 1+1 and 1+N protection schemes.

In [107], the authors considered the problem of providing protection against a single node failure using network coding and reduced capacity technique for wired networks. Their protection scheme is against any single node failure in equal sender and receiver nodes with multiple forwarding links from router (relay) node to receiver.

In [108], the authors proposed Network Protection Codes (NPC) using network coding to protect the operation of the network against link and node failures. Their interest was to find the limits of their NPC and where to deploy their NPC using several network graphs with a minimum number of edges.

In [109] and [110], the authors considered the network coding based protection strategies against node failure in an optical mesh network. The authors in [109] also considered adversarial errors in an overlay (above the optical layer) layer. The authors [110] demonstrated that if there are n_e errors and n_f failures on primary or protection paths, $4n_e+2n_f$ protection paths are sufficient for correct decoding at all the end nodes.

In [111], the authors surveyed the different classes of survivability mechanisms like proactive protection, reactive protection, hybrid methods and a network coding based mechanism.

In these existing research efforts, the authors implemented the relay node protection using network coding for different networks such as wired networks, WMNs, Wireless Sensor Networks (WSNs) and optical networks. However, the QoS performance of network coding for relay node protection in a multihop wireless network is not tested until now. Also, the relay node protection is very useful for multihop 4G wireless networks.

Chapter 4. Radio Resource Management Framework for 4G Wireless Networks

In wireless cellular networks, the design of RRM functions has a direct impact on the QoS for individual connections and the overall system efficiency. The RRM function in the BS has a set of algorithms, such as CAC, PS, DBA, handoff, load control, and power control, to control the usage of radio resources. The function of the CAC is to regulate admission of new users, while controlling the quality of current connections without any call drops. Similarly, the PS and DBA algorithms ensure the QoS among different users while allocating bandwidth between different service-flows of admitted calls. The CAC and PS in wireless networks have been receiving a great deal of attention as the QoS mainly depends upon the CAC, PS and DBA algorithms. Therefore, the proposed QoS framework for RRM functions considers only the CAC and PS. This chapter describes the proposed CAC and PS schemes for 4G multihop wireless networks.

4.1 Problem Statement and Objectives

In 4G wireless networks, the QoS mainly depends on the CAC and PS methods because they aim to distribute all the available resources, while keeping the QoS requirements of both real-time and non-real-time applications at an acceptable level. The design of CAC for a fixed network is simple, as the call admission is based on the available resources and QoS requirements of the new calls. However, the mobile environment is more complicated than the fixed network, as the BS may reserve some bandwidth to admit the handoff calls. If the BS reserves some bandwidth for handoff calls, and the network happens to have few or no handoff calls, then those resources may be wasted or underutilized. On the other hand, if the BS allocates minimum resources for handoff calls, then the handoff calls may be dropped. Hence, the decision of how much bandwidth the BS reserves for handoff calls is a challenging task. The performance of the network for dropping handoff calls is analyzed by CDP. Similarly, the amount of bandwidth reservation for high priority real-time service classes is another challenge in the CAC design. If the resource is not available for accepting a new call, the call will be blocked. In general, the

performance of the network for blocking newly originated calls is analyzed by Call Blocking Probability (CBP). Further, the CAC design challenges for multihop networks are verification of E2E delay requirements of the multihop nodes.

Once a call has been admitted by the CAC, the PS module should allocate the resources based on the connection's QoS provisioning and the available bandwidth resources. The major challenge in DBA and PS is QoS differentiation and QoS assurance among different service classes. In the PS design, the handling of both real-time and non-real-time service flows during busy traffic period is more challenging. Similarly, the handling of two similar QoS level packets belonging to single-hop and multihop users is another challenge for the PS scheme. Therefore, the selection of CAC and PS are crucial and necessary for multihop WiMAX and LTE networks to satisfy the QoS among different service flows.

4.2 Adaptive CAC for 4G Multihop Wireless Networks

In practical scenarios, the CAC at the multihop BS/DeNB calculates the required bandwidth in terms of resource elements (slots/PRBs) and checks whether or not the system has enough resource elements to admit the call. However, the MS in the WiMAX network starts ranging (or UE in LTE network starts random access procedure) with minimum power and then increases the power level to the required signal strength. Similarly, when the user is moving at different speeds, the current channel quality may change instantly or in the next upcoming period. Therefore, the instantaneous resource elements requirement for total calls is time varying. Hence, it is not necessary to differentiate CAC based on channel quality and bandwidth measurements. Thus, reservation based CACs are more suitable for 4G wireless networks because the major requirement is to provide QoS assurance for the existing calls.

The bandwidth reservation policy was introduced in [31] where the bandwidth reservation is only for handoff calls. However, to maintain QoS of the existing calls and to minimize CDP, the proposed CAC in the multihop BS/DeNB reserves some bandwidth for the mobile and high priority users and changes the bandwidth reservation adaptively based on the most recent requests from handoff and high priority users. Suppose, the reserved

bandwidth is not fully utilized by handoff and high priority users, the remaining reserved bandwidth is then allocated for least priority (BE/non-GBR) users for effective bandwidth utilization. Later, when a high priority or handoff user arrives, the CAC applies bandwidth pre-emption on least priority calls to admit that call. However, while admitting new calls or handoff calls, the CAC verifies both bandwidth and multihop delay requirements to satisfy the QoS of the call.

The CAC procedure is the same for both uplink and downlink traffic. Hence, for simplicity, the following theoretical analysis considers only the downlink. Further, the proposed CAC scheme considers the partial bandwidth allocation policy for the least priority BE/non-GBR users. According to WiMAX and LTE standards, the BE and non-GBR connections do not provide any QoS guarantees. However in the real world, the subscriptions available from ISPs are mostly the BE/non-GBR connections for home users and non-BE/GBR connections for corporate users. Therefore, in order to satisfy the BE/non-GBR connection, a portion of maximum sustained bandwidth is given for BE/non-GBR users (in WiMAX, portion of MSTR, i.e., $k \times MSTR$, where $0 < k \leq 1$). Therefore, the proposed CAC scheme limits the least priority connections to admit into the system that improves the QoS performance of the existing BE/non-GBR connections. In this work, there are four different types of applications considered for theoretical analysis and simulation study. In that, voice calls are given high priority than other applications. Also, the minimum bandwidth guarantee, k for least priority users is 0.5. The WiMAX service class type and LTE QCI mapping of those applications are given in Table 4.1.

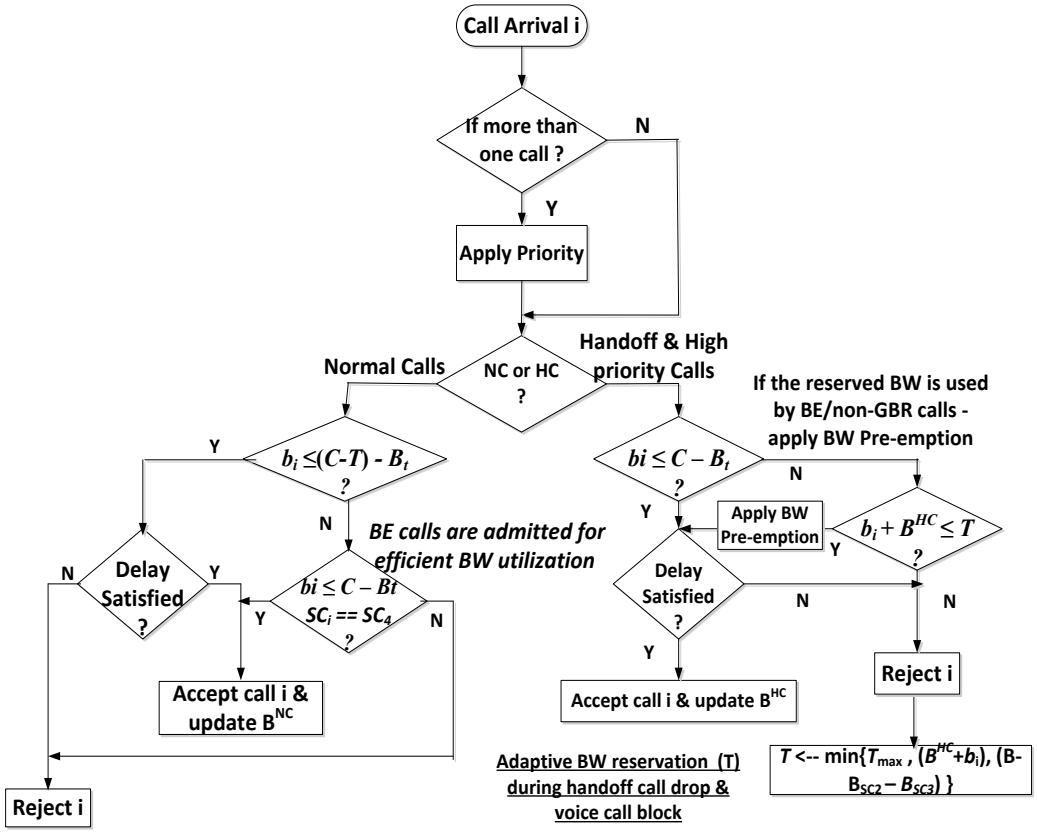
Table 4.1 WiMAX and LTE Service Flow Mapping

Application	**WiMAX service class**	**LTE QCI**	**Mapping notation**	**Priority**
Voice,	UGS	1	SC_1	1
Video Conference	rtPS	3	SC_2	2
Streaming Media	nrtPS	2	SC_3	3
Web Browsing, HTTP	BE	8	SC_4	4

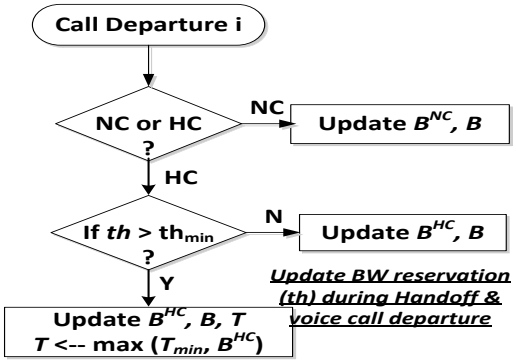
To derive general equations, the service class and the QCI of applications are mapped to the generic notation SC_i. where "*i*" represents the priority of the service flow. For readability, the terminology used in this article is as follows.

- b_i: bandwidth required for connection i
- $B_{SC1}, B_{SC2}, B_{SC3}\ and\ B_{SC1}$: bandwidth allocated to SC_1, SC_2, SC_3 and SC_4 calls, respectively
- $B^{NC}$and B^{HC}: total bandwidth allocated to normal calls and high priority calls, respectively
- B_t: total bandwidth allocated for SC_1, SC_2, SC_3 and SC_4 calls
- *C*: total bandwidth capacity in downlink available at the multihop BS/DeNB
- d_i : maximum latency/delay requirement of connection i (ms)
- f : frame duration (msec).
- High priority calls: newly originated SC_1, calls and all types of handoff calls
- l_i : modified latency, including multihop delay (msec); $l_i = d_i - (nih \times f)$
- m_i : maximum number of frames period for the packet to transmit; $m_i = d_i / f$, m_i must be an integer
- *nh*: number of hops between BS/eNB and the user
- Normal calls: newly originated Service Class 2, 3 and 4 (SC_2, SC_3 and SC_4) calls
- $r_{n,}\ n_{n\ and}\ u_n$: number of real-time (SC_2), non-real-time (SC_3) and voice (SC_1) connections admitted into the network
- r_i : token (packet) arrival rate of a connection i (Kbps)
- TB_i : token bucket size of a connection i (Kbits)
- *T:* bandwidth reservation threshold for high priority users
- W_i: token weight of connection '*i*'
- *k*: bandwidth serving factor

The flow chart for the proposed CAC is shown in Figure 4.1. The working of the CAC scheme is described as follows. Whenever a call arrives at the BS/eNB, the CAC module first verifies whether the sufficient amount of the resource is available to allocate and whether the connection meets the multihop delay requirement or not.



(a) BW allocations and Threshold (*T*) update during call arrival



(b) Threshold (*T*) update during call departure

Figure 4.1 Flow chart of proposed CAC

The key functions of an adaptive CAC are highlighted as follows:

Arriving calls priority: For a given frame period, if more than one call arrives at the multihop BS/DeNB, the CAC module assigns priority for the incoming calls. The voice calls and handoff calls are given higher priority than normal calls. Further, the priority order of the calls is SC_1, SC_2, SC_3 and SC_4.

Bandwidth verification for normal calls: Now, consider a normal call 'i' arrives at the BS/DeNB with a requested bandwidth of 'b_i' and requesting the service for data transfer. The CAC module at the BS/DeNB first verifies the bandwidth requirement that was shown in Figure 4.1a (on left side of the flowchart is for normal call). In bandwidth verification process, the CAC checks whether the remaining bandwidth ($b_i \leq (C\text{-}T) - B_t$) is greater than or equal to the requested bandwidth (b_i). The remaining bandwidth calculation includes the adaptive bandwidth reservation 'T'. If the remaining bandwidth is enough to admit, the CAC accepts the connection for the next stage. Otherwise, the CAC checks, whether the reserved bandwidth (T) is not fully used by the high priority calls and whether the connection is SC_4 traffic or not. If both conditions are true, the CAC accepts the SC_4 call for efficient bandwidth utilization. For SC_4 traffic, the delay verification is not necessary. However, the bandwidth verification for different service classes is based on the QoS provisioning. If the connection 'i' belongs to a WiMAX connection with the bandwidth requirement 'b_i', then the aim of the CAC and the scheduler at the BS is to ensure the bandwidth of a maximum sustained or minimum reserved traffic rates, i.e. for UGS service class the bandwidth requirement is *MSTR*, *MRTR* for the rtPS and nrtPS and finally, $k \times MSTR$ for the BE service which is given in Eqn. 4.1.

$$b_i = \begin{cases} MSTR\ for\ SC_1 traffic \\ MRTR\ for\ SC_2\ and\ SC_3\ traffic \\ k \times MSTR\ for\ SC_4, where\ 0 < k \leq 1 \end{cases} \tag{4.1}$$

Bandwidth verification for high priority calls: Now, consider a high priority call 'i' that arrives at the BS/DeNB with a requested bandwidth of 'b_i' and requests the service for data transfer. The CAC module at the BS/eNB verifies whether the remaining bandwidth is greater than or equal to the requested bandwidth ($b_i \leq C - B_t$). If the remaining bandwidth is enough to admit, the CAC accepts the connection for the next stage (*delay guarantee*).

Otherwise, the CAC verifies if the reserved bandwidth 'T is allocated to any SC_4 connections for normal calls by checking the condition ($b_i + B^{HC} \leq T$). If the condition ($b_i + B^{HC} \leq T$) is true, then it is clear that the reserved bandwidth is allocated to SC_4 connections for new calls. Therefore the CAC pre-empt the SC_4 traffic to accept the connection 'i' for the next stage. Otherwise, the CAC rejects the connection and updates the threshold value. The functional implementation is shown in Figure 4.1 (right side of the flowchart).

Adaptive bandwidth reservation: The CAC reserves the bandwidth adaptively for high priority calls by defining two levels of threshold, 'T_{min}' and 'T_{max}', where $T_{min} < T_{max} <$ C. Let 'T' be some value such that $T_{min} < T < T_{max}$. Initially, the CAC module reserves the minimum bandwidth for high priority calls, where $T = T_{min}$. Later, when the reserved bandwidth is fully utilized by the high priority calls then the CAC method will not be able to accommodate a recently requested high priority calls. Hence, the CAC increases the threshold 'T' with 'b_i' which is a bandwidth requested by the recent high priority call. While increasing the threshold, the CAC verifies whether the bandwidth reservation exceeds the maximum threshold and affects the bandwidth allocated for non-real-time calls. The threshold increment for the high priority calls is shown in Figure 4.1a (bottom of the right side of the flowchart). Similarly, the CAC method reduces the bandwidth reservation for leaving of a high priority call departing from the current BS/eNB that was shown in Figure 4.1b. Therefore, the bandwidth reservation is adaptively changed based on the most recent requests and the leaving of high priority calls.

Delay guarantee: The next stage of the bandwidth verification in CAC process is to verify the multihop delay guarantee. In a multihop network, once the BS/DeNB schedules the packet for transmission, the subordinate RS can forward the packet in the next frame itself. The packet forwarding in next frame is possible because the RS's bandwidth capacity is the same as the BS and downlink traffic is only from BS/eNB. The network connectivity and data transfer in multihop 4G wireless networks are only through BS/eNB i.e. the RSs are not allowed to transfer the traffic internally between two users (MSs) for accounting purposes. With this assumption, the delay requirement for the TB scheduling in [14] is modified to consider the multihop latency because when the CAC is applied to bandwidth pre-emption the (P+TB) scheduler is dynamically selected. Hence, during

system overload condition the (P+TB) scheduler is scheduling the traffic where each connection (i) is controlled by two token bucket parameters, r_i and TB_i.

According to the token bucket mechanism, the maximum data scheduled for the connection over the session length n is;

$$r_i \times n \times f + TB_i \quad (4.2)\ [14]$$

The average bandwidth used by the connection in one frame is:

$$r_i + \frac{TB_i}{n \times f} \quad (4.3)\ [14]$$

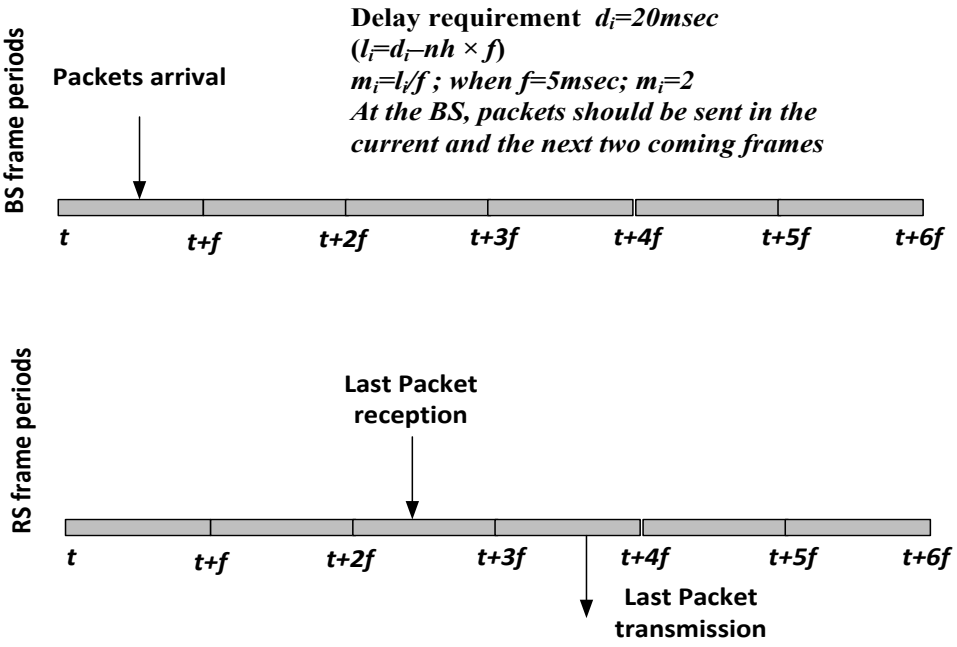


Figure 4.2 Delay requirement timing diagram

Now, consider the case as shown in Figure 4.2. Assume that the maximum delay requirement d_i for the service flow is 20msec. As the frame length is 5msec, the modified latency of the packet at the BS/eNB is 15msec. Hence, the modified maximum number of frame periods for the packet to transmit at the BS/eNB is 3. As a result, if the packet arrives during the first frame period then that packet should be transmitted in third frame period. Since, the (P+TB) scheduling scheme is adopted when the CAC pre-empts the BE calls, we also need to use the TB scheduling for delay verification. According to the TB mechanism,

the maximum number of packets (in terms of the number of bits) that arrive and available in the time frame t and (*t+f*) for a connection 'SC_2' is $r_i \times f + TB_i$. These arriving bits must be scheduled in time frames (*t+f, t+2f*) and (*t+2f, t+3f*) to avoid delay violation. Therefore, the relay node forwards the packets in a time frame (*t+3f, t+4f*). In the worst case scenario, all other SC_1, SC_2 and SC_3 sessions are active and the total bandwidth requirement of all other connections in each time frame (*t+f, t+2f*) and (*t+2f, t+3f*) is (B_{SC1} + B_{SC2} + B_{SC3}). However, the (P+TB) scheduler allocates the remaining bandwidth ($C - B_{SC1}$) $W_i f$ for each SC_2 in each time frame [14], where, *Wi* is the token weight of connection '*i*' for bandwidth sharing within the service flow. If the connection belongs to SC_2, then $W_i = r_i / \sum r_{SC2} = r_i / B_{SC2}$. Therefore, the necessary condition is that TB capacity should not exceed the remaining bandwidth for the next two frame periods:

$$TB_i + r_i f \leq 2(C - B_{SC1}) W_i f \quad (4.4)\ [14]$$

$$TB_i + r_i f \leq 2(C - B_{SC1})\ (r_i / B_{SC2})\ f \quad (4.5)\ [14]$$

Substituting 2 = (4 – *nh*) and subtracting $r_i f$ on both sides of Eqn. 4.5, we get,

$$TB_i \leq [(4 - nh)\ (\ (C - B_{SC1}) / B_{SC2}\ ) - 1]\ r_i f \quad (4.6)$$

For the general case m_i, the necessary condition will be

$$TB_i \leq [(m_i - nh)\ ((C - B_{SC1}) / B_{SC2}) - 1]\ r_i f \quad (4.7)$$

For the general case m_i, the necessary condition for SC_3, is

$$TB_i \leq [(m_i - nh)\ ((C - B_{SC1} - B_{SC2}) / B_{SC3}) - 1]\ r_i f \quad (4.8)$$

Eqn. 4.8 shows the necessary condition for accepting a call at the BS, where the size of the token bucket TB_i should not exceed the total bandwidth allocation over the upcoming frame periods. If the condition fails then the connection may not get enough bandwidth for the available tokens and the packet will be dropped. Thus, the CAC method has an adaptive bandwidth reservation for high priority calls and ensures the multihop delay requirement for all service flows.

4.3 Scheduling Algorithms for 4G Multihop Wireless Networks

In general, the wireless MAC scheduler is responsible for scheduling the air interface resources among the users in both the downlink and the uplink time periods. Since OFDM technology is used in WiMAX and LTE networks, the scheduler effectively distributes the radio resources (slots/PRBs) in both time and frequency domains. In LTE, most of the existing MAC schedulers' first schedule radio resources in Time Domain (TD), and then Frequency Domain (FD) as shown in Figure 4.3. The TD scheduler is used to differentiate the users according to their QoS characteristics. The FD scheduler is responsible for assigning the radio resources (i.e. PRBs) based on the user's priority and channel condition. Alternatively, the existing WiMAX schedulers schedule radio resources at frame level (FL) while the slot assignment in TD or FD is done by solving a bin packing algorithm for efficient bandwidth utilization. However, this proposed scheduler for WiMAX and LTE networks concentrates only on FL to ensure QoS satisfaction among different users. Later, the WiMAX and LTE network may use FD scheduling for PRBs or slot allocation.

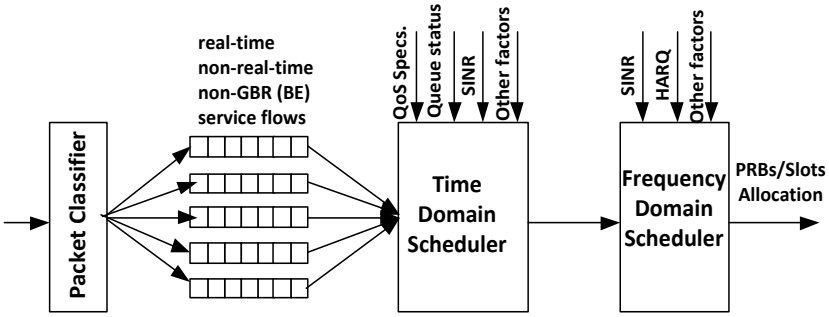


Figure 4.3 Time and frequency domain scheduling in LTE

The main objective of FL scheduling and bandwidth management is to allocate the radio resources based on the set of connection QoS parameters in each frame period. The literature study for FL scheduling shows that the EDD scheduler performs well in ensuring delay performance for all service classes. Also, throughput and other performance are good until the system reaches full load condition, where the total bandwidth required for admitted calls is equal to the system bandwidth. However, when the system is overloaded, the QoS performances of voice and real-time services are highly affected. On the other

hand, the simple priority scheduler ensures the QoS performance of voice and real-time services, even in the case of overload condition. Hence, the (P+E) scheduler is initially proposed, where the high delay sensitive voice application is scheduled by the priority scheduler and other service flows are scheduled by the EDD scheduler.

The (P+E) scheduler combines the EDD scheduling and priority scheduling that is shown in Figure 4.4. The inner EDD scheduler first schedules the SC_2, SC_3 and SC_4 traffic into the EDD queue. The outer priority scheduler schedules the SC_1 queue first and then the EDD queue for the remaining bandwidth in each frame. The priority scheduler ensures the packet deadlines while scheduling the packet and it drops the packet if the deadline time exceeds the limit. In this work, the packet deadline in the EDD queue is modified according to the number of hops from the BS/eNB to the user node ($l_i = d_i - nh \times f$). Thus, the BS/eNB schedule the packet before the modified latency (l_i) and the packet can reach the destination within the specified maximum latency (d_i).

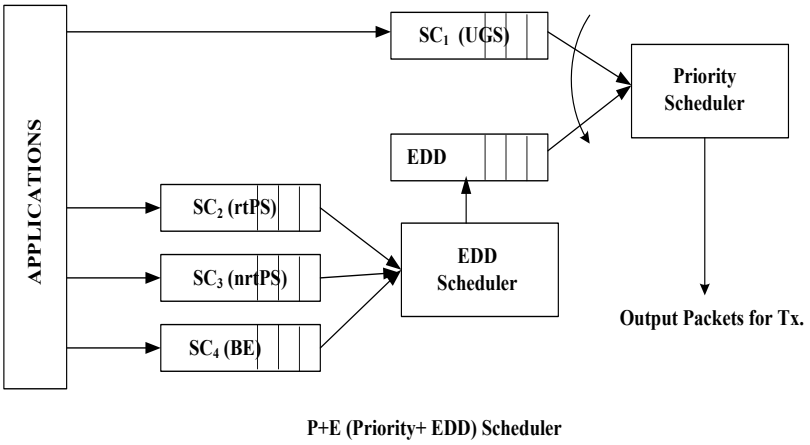


Figure 4.4 The (P+E) scheduler

The QoS performance of network will be improved by the (P+E) scheduler as it considers the multihop latency. However, when the CAC pre-empt the least priority calls to accept handoff and high priority calls, the packet loss performance of real-time applications is reduced. Therefore, the (P+TB) scheduler is proposed for multihop BS/eNB to ensure bandwidth pre-emption for least priority service flows. When comparing the priority scheduler, the TB scheduler allocates bandwidth only for the generated tokens that ensure the QoS performance of non-real-time service flows.

The (P+TB) scheduler combines the TB scheduling and priority scheduling that is shown in Figure 4.5. The inner TB scheduler generates tokens for SC_2, SC_3 and SC_4 traffic. The outer priority scheduler schedules the SC_1 queue first and then for the remaining bandwidth, it schedules the SC_2, SC_3 and SC_4 queues for the available tokens in a TB scheduler. In a TB scheduler, a packet is not allowed to be transmitted until the scheduler possesses a token. Therefore, over a period of time t, the maximum data allowed by the TB scheduler is $r_i \times t + TB_i$. Thus, the (P+TB) scheduler assures the bandwidth provisioning for voice, real-time and non-real-time services. However, the QoS of SC_4 (BE) services are highly affected as the standard also do not provide any QoS assurance for BE traffic.

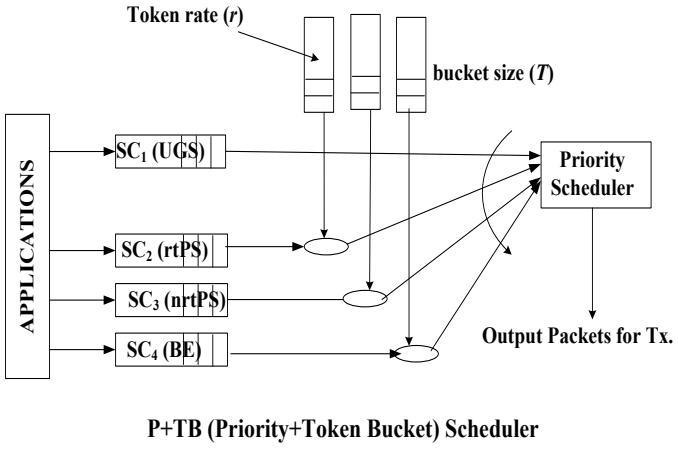


Figure 4.5 The (P+TB) scheduler

The proposed (P+E) scheduler improves the QoS performance until the CAC applies bandwidth pre-emption on least priority calls and during the bandwidth pre-emption stage, the (P+TB) scheduler ensures that the QoS requirements can be met for real-time traffic. Therefore, the proposed scheduling method considers the dynamic selection of the (P+E) and (P+TB) schedulers.

4.4 System Modeling and Performance Evaluation

The system modeling for the proposed adaptive CAC is to analyze the system states during the call arrival and departure process, and to decide call admissions. Further, the CBP and CDP performance of the system is analyzed for various system states. For simplicity, a homogeneous system in statistical equilibrium is considered, in which any cell

is statistically the same as any other cell, and the mean handoff arrival rate to a cell is equal to the mean handoff departure rate from the cell. Hence, it is possible to decouple a cell from the rest of the system and evaluate the system performance by analyzing the performance of the cell. Such single cell analysis is mostly used in modern CAC analysis [20] and [28].

The evolution of the number of occupied resources under multiple class admission control can be modeled by a finite state M-dimensional Markov Chain [21]. The dimension of the Markov chain, M, is equal to the number of classes in the system. The following assumptions are considered for the analysis and simulation.

- Actual mathematical modeling for a bandwidth reservation scheme with four service classes requires the four dimensional Markov chain for newly originated calls and another four dimensional Markov chain for handoff calls. To simplify the model, the given wireless network considers two main traffic classes: high priority class, denoted by HP-class; and the low priority class, denoted by LP-class. In this model, it was assumed that the HP-class is the class of all the handoff calls. The low priority class can be sub-categorized to non-Real-Time (nRT) new calls and BE calls.
- The arrival processes of handoff, nRT and BE calls are Poisson distributed with parameters λ_H, λ_{nRT} and λ_{BE}, respectively. Further, the service time for the handoff, nRT and BE calls is exponentially distributed with parameters μ_H, μ_{nRT} and μ_{BE}, respectively.

The channel borrowing idea on a reservation-based CAC system can be built on a fixed reservation scheme that was initially proposed in [31]. Henceforth, the fixed reservation scheme is reviewed in detail and the proposed channel borrowing approach is incorporated into the fixed reservation scheme.

A. Review of the conventional bandwidth reservation scheme

Let us consider a wireless system with *C* channels and two traffic classes: handoff calls and new calls. In this CAC scheme, it was assumed that *T* channels (out of *C* channels in the system) are reserved for handoff calls and the rest are shared among handoff and new calls. A new call is blocked if the total number of admitted new calls in the system are

more than $C - T$ or there are no more channels available to serve the new call. However, a handoff call is blocked only if there is no channel available in the system to serve it. By defining the state of the system as the pair (n_1, n_2) where n_1 and n_2 are the number of handoff and new calls in the system, respectively, the authors in [31] derived a two-dimensional Markov chain for this system. As this Markov chain is time-reversible, one may easily write the local balancing equations for it and derive the closed form formulas for CBP of new calls and CDP of handoff calls.

From the conventional fixed reservation scheme in [31], the generalization of the proposed scheme can be described with three classes (handoff, nRT and BE). Now, the state of the system is depicted as (n_1, n_2, n_3) where n_1, n_2 and n_3 are the number of handoff, nRT and BE calls in the system, respectively. Therefore, the proposed system will have a three-dimensional Markov chain with the state space

$$S_1 = \{(n_1, n_2, n_3) \mid n_1 \geq 0, 0 \leq n_2 + n_3 \leq C - T, n_1 + n_2 + n_3 \leq C\}. \quad (4.9)$$

By defining q(n_1, n_2, n_3; n'_1, n'_2, n'_3) as the transition rate from state (n_1, n_2, n_3) to state (n'_1, n'_2, n'_3), we have the following transition rules for the three-dimensional Markov chain associated to the proposed scheme:

$$q(n_1, n_2, n_3; n_1, n_2, n_3 - 1) = n_3\mu_{BE} \ (0 \leq n_1 < C, \ n_3 > 0, 0 < n_2 + n_3 \leq C - T, n_1 + n_2 + n_3 \leq C) \quad (4.10)$$

$$q(n_1, n_2, n_3; n_1, n_2, n_3 + 1) = \lambda_{BE} \ (0 \leq n_1 < C, 0 \leq n_2 + n_3 < C - T, n_1 + n_2 + n_3 < C) \quad (4.11)$$

$$q(n_1, n_2, n_3; n_1, n_2 - 1, n_3) = n_2\mu_{nRT} \ (0 \leq n_1 < C, \ n_2 > 0, 0 < n_2 + n_3 \leq C - T, n_1 + n2+n3 \leq C \quad (4.12)$$

$$q(n_1, n_2, n_3; n_1, n_2 + 1, n_3) = \lambda_{nRT} \ (0 \leq n_1 < C, 0 \leq n_2 + n_3 < C - T, n_1 + n_2 + n_3 < C) \quad (4.13)$$

$$q(n_1, n_2, n_3; n_1 - 1, n_2, n_3) = n_1\mu_H \ (0 < n_1 \leq C, 0 < n_2 + n_3 \leq C - T, n_1 + n_2 + n_3 \leq C) \quad (4.14)$$

$$q(n_1, n_2, n_3; n_1 + 1, n_2, n_3) = \lambda_H \ (0 \leq n_1 < C, 0 < n_2 + n_3 \leq C - T, n_1 + n_2 + n_3 \leq C) \quad (4.15)$$

Similar to the two-dimensional case, derivation of a closed form solution for this Markov chain is possible by solving the local balance equations. Also, it may give compact formulas for the CBP and CDP of the system.

B. Proposed channel barrowing system in bandwidth reservation scheme

In the proposed CAC scheme, the BE traffic barrows the unused reserved bandwidth (channel) for effective bandwidth utilization. Later, the CAC pre-empts the BE call for admitting the HP-calls. Now, let us consider the system with a bandwidth capacity of C and T channels are reserved for handoff calls (HP-calls). When admitting a new nRT call, the CAC do not violate the reservation of handoff calls. However, for the BE calls are allowed to use all the channels in the system. In other words, a new BE call can borrow a channel from the reserved channels of handoff calls. Later, the BE call returns the borrowed channel whenever a handoff call arrives and needs that channel. Hence, the pre-empted BE calls will wait in a queue and the call will be served as soon as a channel becomes available. The size of the queue at time t is denoted by $X(t)$. Note that, if $X(t) > 0$ then the CAC will block the new BE arrival. The number of handoff calls, nRT calls and BE calls are denoted in the system by n_1, n_2 and n_3, respectively. The blocking and dropping of handoff calls, nRT calls and BE calls are given by:

- A handoff arrival will be dropped if $n_1 + n_2 + n_3 = C$ and $n_1 \geq T$.
- If $n_1 + n_2 + n_3 = C$ and $n_1 < T$, a handoff call will be admitted by pre-empting a BE call.
- A nRT arrival will be blocked if $n_1 + n_2 + n_3 = C$ or $n_2 + n_3 \geq C\text{-}T$.
- A BE arrival will be blocked if $X(t) > 0$ or if $X(t) = 0$ and $n_1 + n_2 + n_3 = C$.

The channel borrowing CAC scheme is not easy to analyze mathematically because it is a mixed loss-queuing system [118]. In this scheme, there is no queue for the handoff and nRT calls while we keep the pre-empted BE calls in a queue. Therefore to analyze the proposed (channel borrowing) system, two approximations is required which are

System Approximation 1

The input arrival rate to the queue for keeping the pre-empted BE calls is equal to

$$\lambda_H \sum_{\substack{n_1+n_2+n_3=C \\ n_1<T}} p(n_1, n_2, n_3) \tag{4.16}$$

Where p (n_1, n_2, n_3) is the probability of the system states during which the handoff calls arrive the BS and the system is at the state of $n_1 + n_2 + n_3$= C and n_1 < T. Hence, the call arrival rate of the BE call is modified into:

$$\lambda_{BE}^{(new)} = \lambda_{BE} + \lambda_H \sum_{\substack{n_1+n_2+n_3=C \\ n_1<T}} p(n_1, n_2, n_3) \tag{4.17}$$

As it is observed, the arrival rate $\lambda_{BE}^{(new)}$ depends on the state probabilities and the arrival rate of the handoff calls. Such a dependency is expected since there is a feedback in the system which makes a loop in the mixed loss-queuing system. By applying such an approximation, we will get rid of the queue in the system and obtain a loss system with a loop inside. We can derive the three-dimensional Markov chain for this approximation with the state space

$$S_2 = \{(n_1, n_2, n_3) \mid n_1, n_3 \geq 0, 0 \leq n_2 \leq C - T, n_1 + n_2 + n_3 \leq C\} \tag{4.18}$$

The transition probabilities for the Markov chain associated to this System Approximation 1 are the following.

$$q(n_1, n_2, n_3; n_1, n_2, n_3 - 1) = n_3\mu_{BE} \ (0 \leq n_1 < C, \ n_3 > 0, 0 \leq n_2 \leq C - T, n_1 + n_2 + n_3 \leq C) \tag{4.19}$$

$$q(n_1, n_2, n_3; n_1, n_2, n_3 + 1) = \lambda_{BE}^{(new)} \ (0 \leq n_1 < C, 0 \leq n_2 \leq C - T, n_1 + n_2 + n_3 < C) \tag{4.20}$$

$$q(n_1, n_2, n_3; n_1, n_2 - 1, n_3) = n_2\mu_{nRT} \ (0 \leq n_1 < C, 0 \leq n_2 \leq C - T, n_1 + n_2 + n_3 < C) \tag{4.21}$$

$$q(n_1, n_2, n_3; n_1, n_2 + 1, n_3) = \lambda_{nRT} \ (0 \leq n_1 < C, 0 \leq n_2 + n_3 < C - T, n_1 + n_2 + n_3 < C) \tag{4.22}$$

$$q(n_1, n_2, n_3; n_1 - 1, n_2, n_3) = n_1\mu_H \ (0 < n_1 \leq C, 0 \leq n_2 \leq C - T, n_1 + n_2 + n_3 \leq C) \tag{4.23}$$

$$q(n_1, n_2, n_3; n_1 + 1, n_2, n_3) = \lambda_H \ (0 \leq n_1 < C, 0 \leq n_2 \leq C - T, n_1 + n_2 + n_3 \leq C) \tag{4.24}$$

$$q(n_1, n_2, n_3; n_1 + 1, n_2, n_3 - 1) = \lambda_H \ (0 \leq n_1 < T, 0 \leq n_2 \leq C - T, n_1 + n_2 + n_3 = C) \tag{4.25}$$

It is hard to illustrate the three-dimensional Markov chain on paper. If we assume that the nRT class does not exist (or $\lambda_{nRT} = 0$) for illustration purpose, we will obtain a two-dimensional Markov chain since we will have only two classes of BE and handoff calls. Note that the idea of channel borrowing is not affected by this simplification and can be still applied without nRT class, since, in channel borrowing scheme, a BE call is borrowing a channel from handoff calls. Figure 4.6 depicts the two-dimensional Markov chain associated with this System Approximation 1.

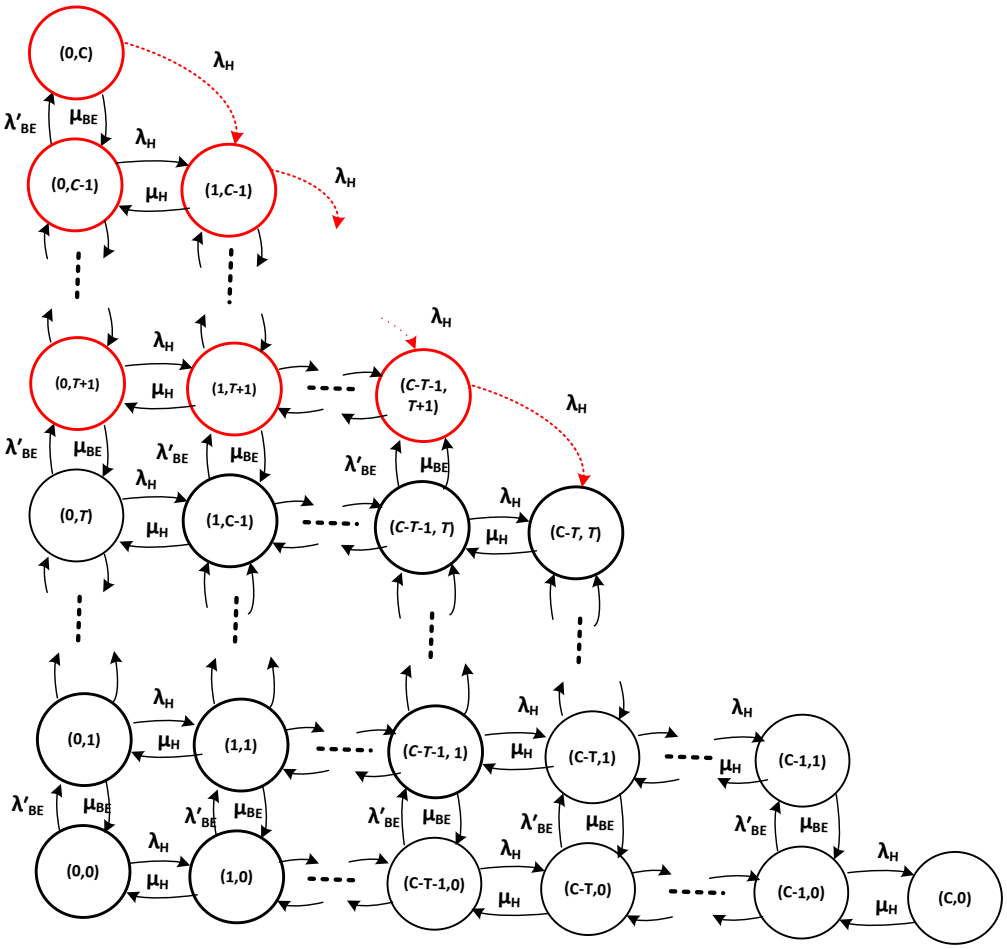


Figure 4.6 Markov chain associated to the bandwidth reservation scheme

The states shown in black are the states that also appear in the conventional bandwidth reservation scheme. The states shown in red are the states that do not exist in the new call bounding scheme, but appear in the proposed channel borrowing scheme. In this figure, the arrival rate of BE calls is denoted by $\lambda_{BE}^{'}$. For the conventional bandwidth reservation

scheme, $\lambda'_{BE} = \lambda_{BE}$. Based on the approximation 1, $\lambda'_{BE} = \lambda_{BE}^{(new)}$. Further, there are some transitions going from one origin state to another state, but there is not a reverse transition from the second state to the origin state (See for example states $(0,C)$ and $(1,C-1)$) in an approximated Markov chain. Therefore, the Markov chain associated with this System Approximation 1 is not time-reversible. As a result, local balance equations cannot be applied to solve such a Markov chain, and we have to use global balance equations. Moreover, in this system approximation, instead of constant λ_{BE} values, we have to use the new BE arrival rate $\lambda_{BE}^{(new)}$ in the global balance equations. Since $\lambda_{BE}^{(new)}$ is a function of the system states, the global balance equations will result in a system of non-linear equations that should be solved using non-linear solvers in Matlab. To clarify this fact, consider the global balance equation associated to state $(0,C)$ in Figure 4.6.

$$p(0,C)(\lambda_H + C\mu_H) = p(0,C-1)\lambda_{BE}^{(new)}$$
$$= \lambda_{BE}p(0,C-1) + \lambda_H \sum_{\substack{n_1+n_3=C \\ n_1<T}} p(0,C-1)p(n_1,n_3) \qquad (4.26)$$

In the above equation, the term $p(0,C)(\lambda_H + C\mu_H)$ is the state of the system for being zero handoff call arrival and all the handoff calls are departed already. Therefore, the system capacity 'C' is only occupied with the BE calls. As it is observed from the right side of the equation we have multiplicative terms $p(0,C-1)p(n_1, n_3)$ which make it a non-linear equation. As the total number of channels in the system increases, the size of such a non-linear system of equations increases rapidly. For example, for a system with 16 channels, we may end up with a system of non-linear equations with more than 800 variables which may become very time-consuming and inefficient to solve for a practical systems. Therefore, System Approximation 2, presented in the following passage, will result in a system of linear equations.

System Approximation 2

In System Approximation 2, the assumption for the call arrival rate for BE call is $\lambda'_{BE} = \lambda_{BE}$. This is equivalent to assume that the pre-empted BE calls are dropped without being fed back to the system into a queue. Such an approximation will result in a system of linear global equations. A large system of linear equations can be efficiently solved in a

reasonable amount of time. Therefore, the second approximation is useful for system performance evaluation, especially for systems with large number of channels (e.g., in realistic wireless systems).

Performance evaluation of analytical models and simulation

In this section, the performance of the proposed channel borrowing scheme is evaluated and compared with that of the conventional bandwidth reservation scheme in terms of CBP and CDP. Further, it has been showed that the two approximations described earlier will result in very close CBP and CDP values. To show this, the CBP and CDP associated to the system approximations 1 and 2 are derived by solving the global balance equations numerically. The CBP and CDP values for these approximations are calculated then as follows:

$$CDP = \sum_{\substack{(n_1,n_2,n_3):n_2+n_3\geq C-T \\ n_1+n_2+n_3=C}} p(n_1,n_2,n_3) \tag{4.27}$$

$$\begin{aligned} CBP = & \sum_{(n_1,n_2,n_3):n_2+n_3\geq C-T} \frac{\lambda_{nRT}}{\lambda_{nRT}+\lambda'_{BE}} p(n_1,n_2,n_3) \\ & + \sum_{\substack{(n_1,n_2,n_3):n_2+n_3\geq C-T \\ n_1+n_2+n_3=C}} \frac{\lambda'_{BE}}{\lambda_{nRT}+\lambda'_{BE}} p(n_1,n_2,n_3) \\ & + \sum_{\substack{(n_1,n_2,n_3):n_2+n_3\geq C-T \\ n_1+n_2+n_3=C}} p(n_1,n_2,n_3) \end{aligned} \tag{4.28}$$

Where the CBP for system approximation 1 is calculated if in (4.28) we put $\lambda'_{BE} = \lambda_{BE}^{(new)}$ and the system approximation 2 is calculated by substituting $\lambda'_{BE} = \lambda_{BE}$. The performance of system approximation 1 and system approximation 2 are compared using Matlab simulations.

To compare the analytical results for System Approximation 1 and 2 using Matlab, a system is considered with C = 12 and T = 6 and the average service rate and arrival rate are considered as $\mu_H = \mu_{BE} = \mu_{nRT} = 1$ and $\lambda_{nRT} = 0.5$ respectively. Then the CBP and CDP

results are plotted for $\lambda_H = 0.5 \times i$ and $\lambda_{BE} = 0.5 \times i$ where $i = 1, 2, \ldots, 10$. The CBP and CDP results in 3D graphs are presented in Figure 4.7 and 4.8. On the other hand, to compare analytical and simulation results, 16 servers were considered, because solving the global balance equations for System Approximation 1 with more than 12 servers takes a considerable amount of time.

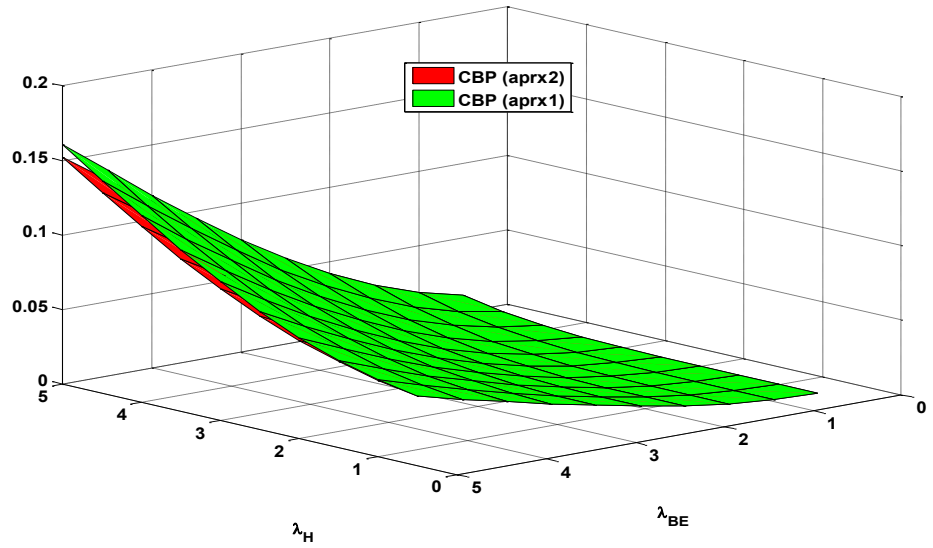


Figure 4.7 The CBP for approximations 1 and 2 for a system with C = 12, T = 6

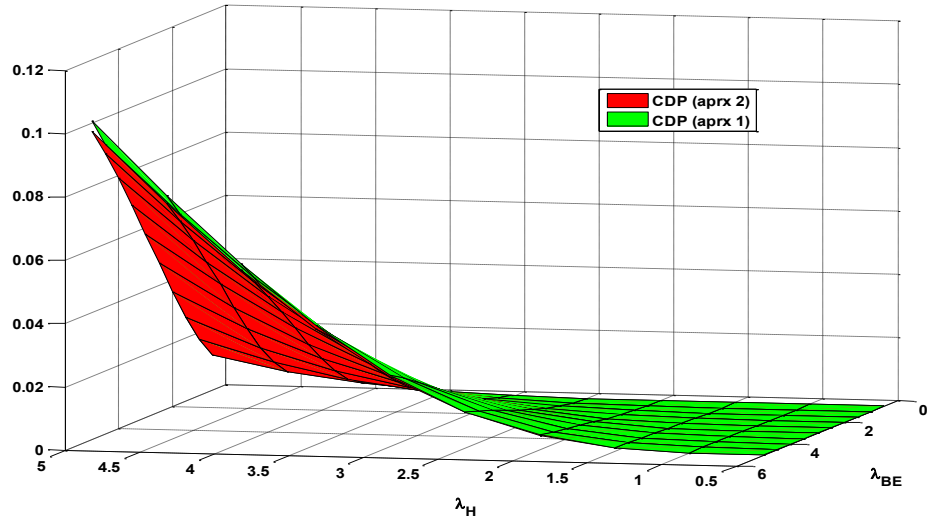


Figure 4.8 The CDP for approximations 1 and 2 for a system with C = 12, T = 6

From Figures 4.7 and 4.8, it is clear that the two system approximations result in close CBP and CDP values. The CBP and CDP values for the System Approximation 2 are slightly lower than that of the System Approximation 1, since in Systems Approximation 2, we will drop all the pre-empted BE calls and, therefore, the BE load in the Systems Approximation 2 is a slightly less than the Systems Approximation 1. Therefore, the Systems Approximation 2 is suggested for the performance evaluation in large networks (with large amount of channels).

As mentioned earlier, to compare the analytical and simulation results for the proposed bandwidth barrowing scheme and then with the conventional scheme a system of C = 16 servers is considered and T = 8. In results comparison, first the CDP and CBP values are calculated using Matlab for the Systems Approximation 2, and then the actual simulation is performed. The CDP and CBP values for the mixed loss-queuing system are calculated in Matlab by solving the system using global balance equations. In analytical studies and the actual simulations, the CBP and CDP values are calculated for λ_H = 4, 7, 10 ; λ_{BE} = i where i = 1, 2, . . . , 10 and; λ_{nRT} = 10 and λ_{nRT} = 1 that are presented in Figures 4.9 to 4.12.

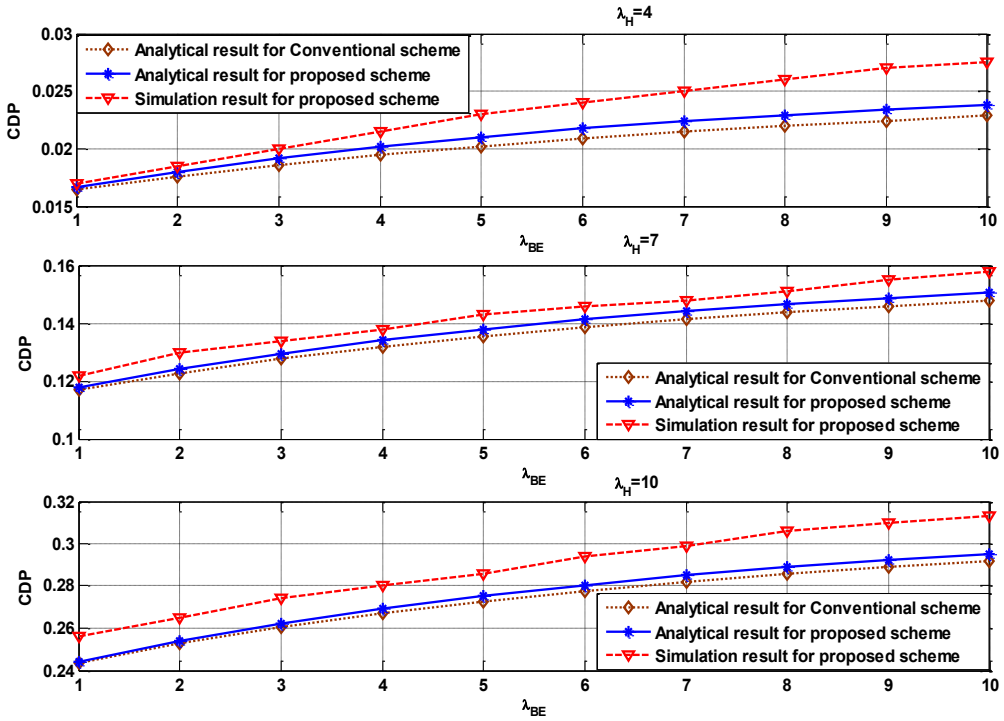


Figure 4.9 The CDP performance comparison for a system with C = 16, T = 8, λ_{nRT}=10

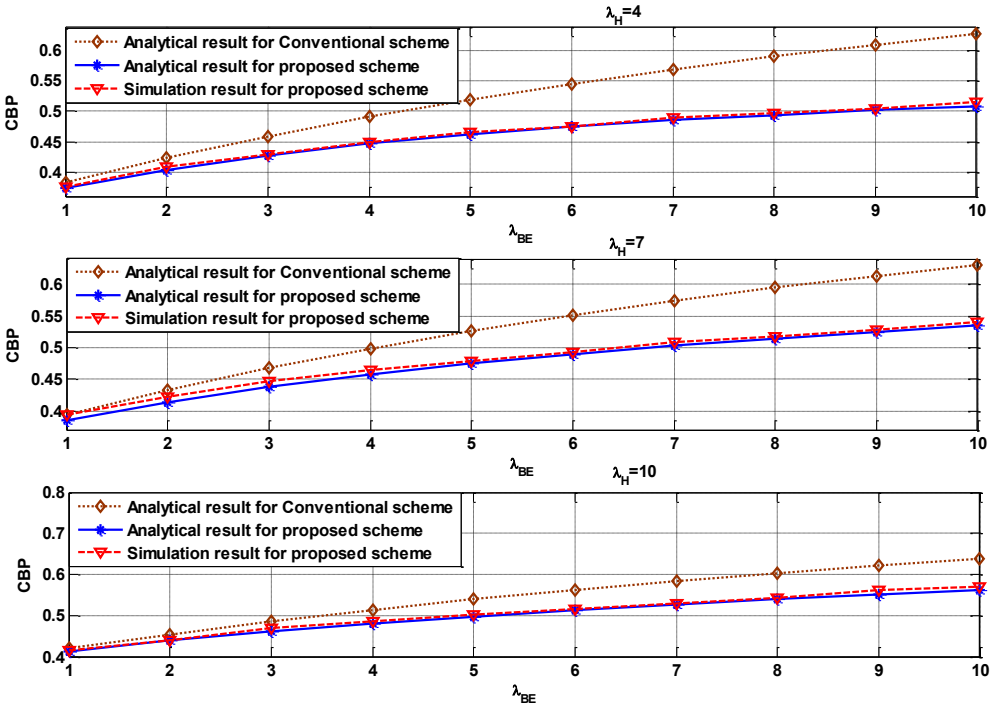


Figure 4.10 The CBP performance comparison for a system with C=16, T=8, λ_{nRT}=10

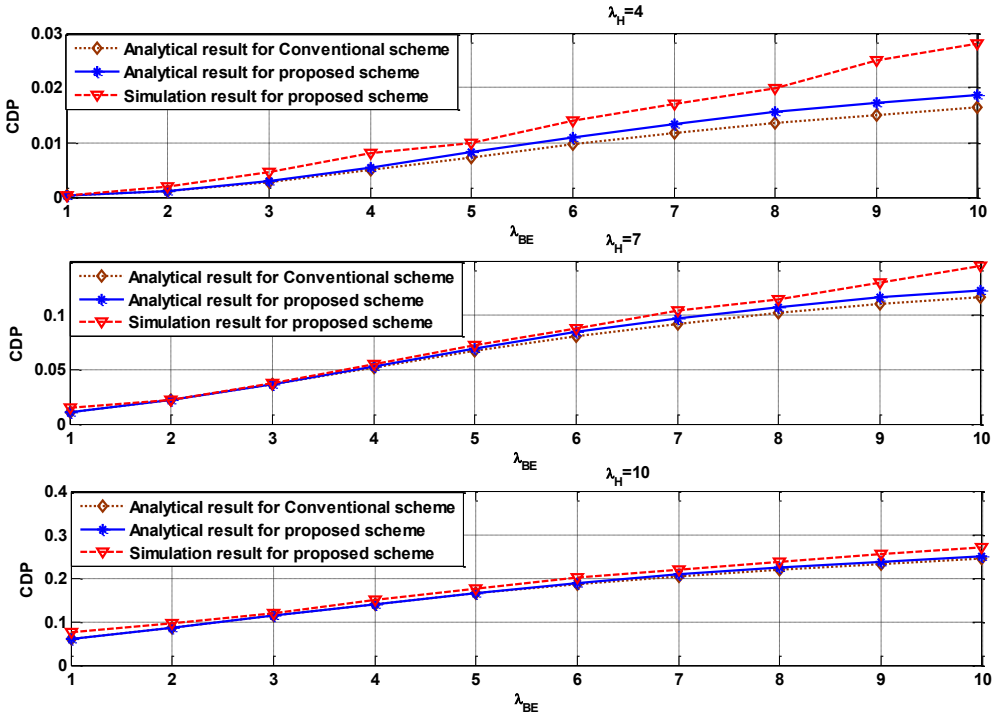


Figure 4.11 The CDP performance comparison for a system with C=16, T= 8, λ_{nRT}=1

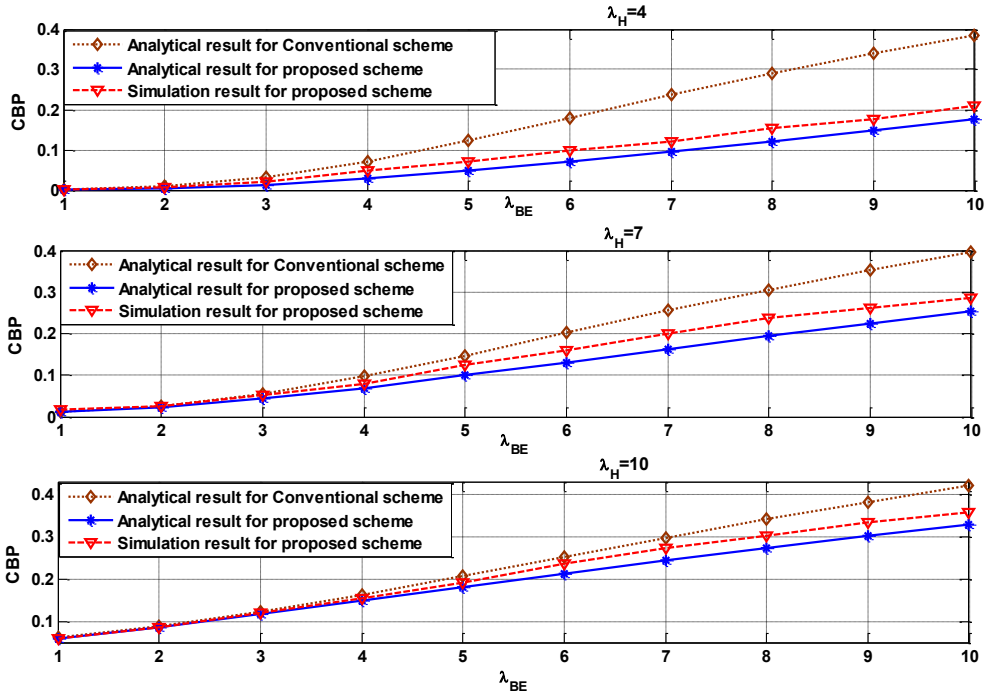


Figure 4.12 The CBP performance comparison for a system with C=16, T=8, λ_{nRT}=1

From the CBP performance results, it is evident that the channel borrowing scheme will result in a considerable decrease in CBP compared with the conventional bandwidth reservation scheme. Similarly, the CDP in the channel borrowing scheme is slightly less than the conventional bandwidth reservation scheme. Conversely, the channel borrowing scheme admits more BE calls for the unused reserved channel, and then keeps the pre-empted ones in a queue to resume their service in future. Therefore, more BE calls are using the unreserved channels and less handoff calls have the opportunity to use the unreserved channels. This makes the probability of the call dropping of handoff calls increase. However, the amount of increase for CDP in the proposed channel borrowing scheme is very small compared to the gain obtained in terms of the CBP decrease. For example, for λ_H = 4, λ_{nRT} = 10 and λ_{BE} = 10, the CBP of the proposed scheme is 0.11 less than that of the conventional scheme, while the CDP of the conventional scheme is 0.004 less than that of the channel borrowing scheme. Also, the simulation results show that the System Approximation 2 performs very closely to the original mixed loss-queuing system.

4.5. Performance Evaluation of CAC and PS Schemes in 4G Wireless Networks

The performance evaluation of the proposed CAC for WiMAX and LTE networks are verified using system level simulation on a C framework because it is difficult to simulate on NS2 for a huge call arrival and departure process. The maximum number of calls attempted in the BS for the CAC simulation is 1 million. Later, the proposed CAC and PS modules are integrated into NS2, and then the performance evaluation of the proposed PS scheme is tested for multihop WiMAX networks. The WiMAX system parameters and traffic models in NS2 follow the guidelines of the WiMAX forum specification [6]. For LTE networks, the available open source simulators do not support the relay functionality. Therefore, the performance of the proposed PS schemes is verified for LTE using NS2 on single-hop LTE network (i.e. without relay node implementation). The following sections describe the simulation environments and the result analysis of the proposed scheme.

4.5.1. Simulation Environments and Parameter Settings

The WiMAX and LTE networks' simulation parameters are given in Table 4.2 and Table 4.3. The call arrival pattern, traffic model, mobility model and channel model are the same for both WiMAX and LTE simulations. Hence, the common simulation parameters are given in Table 4.4.

Table 4.2 WiMAX System Parameters

Parameter	**Value**
Physical Layer	Wireless MAN OFDMA, TDD
Bandwidth and Frame duration	10MHz and 5msec
No of OFDM symbols and subchannels	47, 35 (out of 47, 24 for DL and 23 for UL)
Cell type	3 cells, 200m radius, at 100m radius RSs are distributed
# of RSs and MSs	6 RS and 100 MS in each cell. RSs are placed at 60^0

Table 4.3 LTE System Parameters

Parameter	Value
Physical layer	Wireless MAN OFDMA, TDD
Bandwidth,	10MHz
No. of resource elements	50PRBs
Cell type	3 cells, 125m radius
# of UEs	100 UE in each cell

Table 4.4 Common Parameters for WiMAX and LTE Networks Simulation

Parameter	Value
User distribution	Uniform
Mobility model	fixed, random walk, Random Way Point (RWP)
Velocity of MSs/UEs	0, 4km/h and 80km/h for fixed, walk and moving users
Flight time of MSs/UEs	[10, 20] sec uniform distribution
Propagation model	COST-231 Hata,
Lognormal shadowing	Standard deviation = 8 dB
Simulation time	10,000 sec 0–2,000 sec is ignored
Service duration	360sec exponential distribution
Carrier frequency	2GHz
Modulation & coding scheme	QPSK, QAM-16 and QAM-64

Mobility models: The mobility models considered in this simulation are Random Walk at 4Km/h and RWP at 80Km/h. These mobility models and the corresponding Block Error Rate (BLER) lookup table for different channel variations are used in NS2 that are suggested by the WiMAX Forum. The Random Walk mobility model has proven to be one of the most widely used mobility models, because it describes individual movements relative to cells [5]. The MS begins its movement from its initial position (x, y) and at each position, the MS randomly chooses a direction between 0 and 2π and a speed between 0 and 4Km/hr. The MS is allowed to travel for a total of 1 second before changing direction and speed.

On the other hand, the RWP mobility model includes pause times between changes in direction and/or speed. In this model, a mobile node selects a random position (x, y) in the simulation area as a destination point and a velocity (v) from a uniformly distributed range [0, 80Km/h]. Then, MS starts to travel to the chosen destination position with the selected speed, 80Km/h. When the node arrives at the destination point, it pauses for a specific time and then the node selects a new destination and speed and repeats the process.

Channel model: The channel model considered in this simulation is COST 231-Hata model [5]. COST 231-Hata model is designed for large and small macro-cells networks. Hence, many existing research works on WiMAX and LTE networks used the COST 231-Hata model. The closed form expressions to calculate path loss is [5]:

$$PL_i(t)=46.3+33.9\ log_{10}(f_c)-13.82\ log_{10}(h_t)-a(h_r) + (44.9-6.55\ log_{10}(h_t))\ log_{10}(d_i(t)) + C_M \quad (4.29)$$

$$a(h_r) = (1.1log_{10}(f_c)-0.7)hr - (1.56log_{10}(f_c)-0.8) \quad (4.30)$$

Where $PL_i(t)$ is the path loss (in dB), $d_i(t)$ is distance (in km) of user i at time t, f_c is the carrier frequency (in MHz), h_t and h_r are the heights of BS/eNB and MS/UE (in m), respectively, and finally, $a(h_r)$ is the mobile antenna correction factor.

Traffic models: The packet arrival pattern and the average simulation time for different applications are different. The QoS specifications of applications and its traffic distribution are given in Table 4.5 [23] and Tables 4.6 to 4.9. Here, the traffic and channel models used in this simulation are readily available in NS2 for the WiMAX network [114].

Table 4.5 Traffic QoS Specification [23]

Class	Application	Bandwidth	Latency required	Jitter	Packet loss
SC_1	Voice,	64Kbps	150msec	50msec	1E-03
SC_2	video conf.	128Kbps	150msec	100mse	1E-04
SC_3	Video stream	1.1Mbps	200msec	100ms	1E-05
SC_4	HTTP	400Kbps	400msec	N/A	0

Table 4.6 VoIP Traffic Model [114]

VoIP Traffic Model	
Average Call Holding Time	Exponential: μ =210 sec
Talk spurt length	Exponential: μ =1026 ms
Silence length	Exponential: μ =1171 ms

Table 4.7 Video Conference Traffic Model [114]

Video Conference Traffic Model	
Scene Length	Lognormal(μ =5.1 sec , σ =9.05 sec)
I frame size	Lognormal(μ =18793,σ =5441)
P frame size	Lognormal(μ =8552, σ =3422)
B frame size	Lognormal(μ =6048 , σ =2168)

Table 4.8 Video Streaming Traffic Model [114]

Media (Video) streaming Traffic Model	
Scene Length	Lognormal(μ =5.1 sec , σ =9.05 sec)
I frame size	Lognormal(μ =19504 , σ =2213)
P frame size	Lognormal(μ = 9891, σ = 2310)
B frame size	Lognormal(μ = 6496 , σ = 1896)

Table 4.9 Web Browsing Traffic Model [114]

Web browsing (HTTP) traffic model	
Number of Pages per session	Lognormal Mean = 17 pages SD = 22 pages
Page request size	constant 350 B
Main object size (SM)	Truncated Lognormal Mean = 52390B SD= 49591B Min = 1290B Max = 0.25MB
Embedded object size (SE)	Truncated Lognormal Mean = 8551B SD = 59232B Min = 5B Max = 6MB
No of objects per page (Nd)	Truncated Pareto Mean = 51.1 Max = 165

In this simulation, the call arrival and departure processes are Poisson distributed. The average service time for the applications SC_1, SC_2, SC_3 and SC_4, are 200sec, 600sec, 180sec, and 300sec respectively [5]. To observe the effective performance of the proposed CAC in multihop WiMAX and LTE networks, the proposed scheme (adaptive bandwidth reservation) is compared with fixed bandwidth reservation scheme. The fixed reservation scheme reserves the bandwidth reservation for handoff calls only, whereas the proposed scheme reserves the bandwidth for high priority calls. The high priority calls include the handoff calls and newly originated voice calls. Further, the threshold of the fixed scheme is set at th_{mim}, while the th of the adaptive scheme varies between th_{mim} (20 percent) and th_{max} (80 percent) [35]. The bandwidth reservation varies based on the most recent high priority call requests.

The CAC and scheduling simulations have been repeated 25 times for different call arrival and departure patterns to increase statistical reliability of results. Hence, the CAC simulation results show the average values together with a 95% confidence interval. For PS simulation results, it is difficult to show the confidence interval in the Y axis as the simulation results for certain schedulers have closer performance at different load conditions.

For the proposed scheduling scheme, the QoS performance is compared with priority, EDD and TB scheduling schemes for downlink. For downlink, initially the BS use the (P+E) scheduling scheme and then, when the CAC starts pre-empting the SC_4 (BE) traffic, the BS selects (P+TB) scheduling scheme. Similarly, the (P+E) and (P+TB) scheduling are compared for uplink at the MS/UE, where (P+TB) scheduling outperforms (P+E) scheduler. The following assumptions are considered for simulations and result analysis.

- For simplicity, the maximum number of hops considered in a multihop WiMAX network is two.
- The number of OFDMA subcarriers in PHY layer and the channel bandwidth are the same in both the RS and the BS in WiMAX networks. Further, the RS

handles the downlink traffic only from the BS. Hence, the RS can forward the downlink traffic in the next frame period itself.

- The user nodes are expected to receive good signal strength of at least QAM-16 for MCS.
- The call arrival rate at which the CAC starts pre-empting the least priority traffic is assumed as system full load condition. After that, the system is overloaded.
- The BS/eNB should have the knowledge of the number of hops away for each user. In multihop WiMAX networks, when the MS is trying to get the wireless connectivity, the MS will first synchronize the channel the access node and start performing the ranging procedure with the access node. Then, the MS will request the uplink and downlink connections for data transfer. The access node may be the BS or any other RS in a network. If the MS tries to connect from multihop, the access RS will forward the connection request to the BS for call admission. At that time, the centralized CAC at the BS comes to know the MS details and the number of hops away from the BS. As a result, the BS can use the number of hops later for the downlink packet scheduling.

4.5.2. Performance Evaluation of Proposed and Conventional CAC Schemes

The performance metrics for the CAC are CDP for handoff calls and CBP for new calls. The proposed CAC is analyzed for two different scenarios: (1) In the first scenario, the call arrival rate for all Service Classes (applications) are equal; and (2) in second scenario, the call arrival rate for the least priority traffic (BE/non-GBR) is doubled than other Service Classes (i.e., if $\lambda_{SC1} = \lambda_{SC2} = \lambda_{SC3} = 0.2$, then $\lambda_{SC4} = 0.4$. However the X axis indicates the basic call arrival rate of the applications (λ_{SC1})). The second scenario would help in analyzing the real-time environment, where the subscriptions available from ISPs are mostly the BE/non-GBR connections for home users and non-BE/GBR connections for corporate users. In both scenarios, the handover ratio, i.e., the ratio of the rate of handover calls to the aggregate arrival rate on the system is 0.5.

The results presented in Figures 4.13 and 4.14 show the performance comparison of the proposed CAC with the fixed reservation scheme for the first scenario in the WiMAX and LTE networks. The upper and lower limits of the confidence interval for each call arrival rate are also shown in figures.

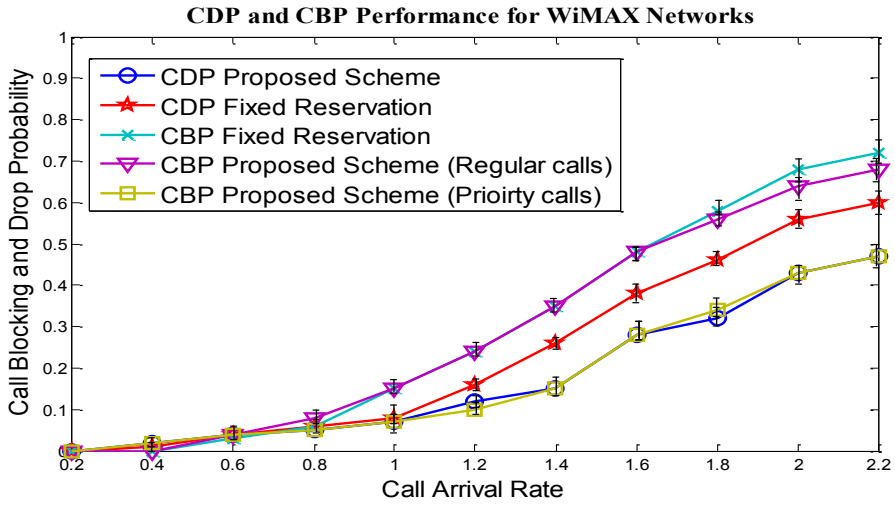


Figure 4.13 Performance of CAC for WiMAX networks in first scenario

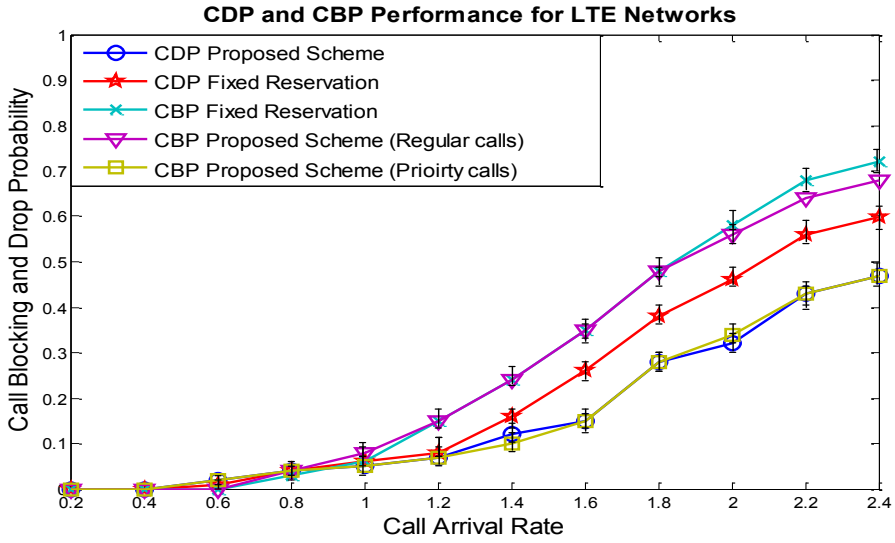


Figure 4.14 Performance of CAC for LTE networks in first scenario

The following points are observed from the simulation results:

- From Figure 4.13 and 4.14, it is clear that the CBP and CDP performances of WiMAX network are the similar to that of LTE networks. However, the CDP and

CBP values in the LTE network are slightly lesser than the WiMAX network because the LTE has more system capacity than WiMAX.

- Until the system has the call arrival rate of 1 (λ_{SC1} =1), the CDP and CBP performance of the adaptive scheme are similar to that of the fixed reservation scheme.
- Later, when the call arrival rate is increased, the CDP performance of handoff calls is better than the fixed reservation scheme and the CBP performance of voice calls is greatly improved over the fixed reservation scheme. The CDP for handoff calls and the CBP for SC_1 calls are improved by adaptive bandwidth reservation. On the other hand, the CBP performance of the fixed and the adaptive schemes is closer. In the system modeling Section, the CBP for the proposed scheme is greatly improved as shown in Figure 4.10 because the bandwidth reservation for high priority call is fixed. When the bandwidth reservation for high priority calls is increased, the CBP performance of normal calls should be reduced. However, the CBP performance is improved by admitting more SC_4 (BE) calls for the unused reserved bandwidth. In the WiMAX network, the CDP and CBP performances at the call arrival rate of 1.6 are; CBP for SC_1 calls in the fixed reservation scheme (without bandwidth reservation) is ~0.47, whereas in the proposed scheme it is ~0.28; the CDP of the handoff calls in the fixed reservation is 0.38, whereas in the proposed scheme is ~0.275; the CBP of the normal call in the fixed reservation is ~0.475, whereas in the proposed scheme it is 0.48.
- At the call arrival rate of 2.0 in WiMAX network, the CDP and CBP performances are: the CBP for SC_1 calls in the fixed reservation scheme is ~0.64, whereas in the proposed scheme it is ~0.43. In fixed reservation scheme, bandwidth is reserved only for the handoff calls, not for the new calls; the CDP for the handoff calls in the fixed reservation is 0.56, whereas in the proposed scheme it is ~0.44; the CBP for the normal call in the fixed reservation is ~0.655, whereas in the proposed scheme it is 0.69.

The performance comparison of proposed CAC for the second scenario in the WiMAX and LTE networks are shown in Figure 4.15 and 4.16. This scenario simulates closer to the real-time environment for ISPs, where more residential customers are connected to the network than corporate customers.

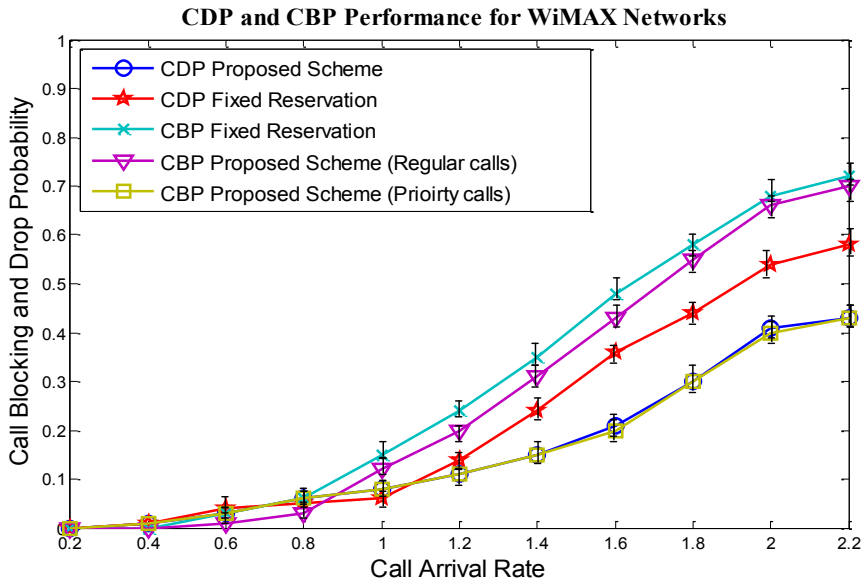


Figure 4.15 Performance of CAC for WiMAX networks in second scenario

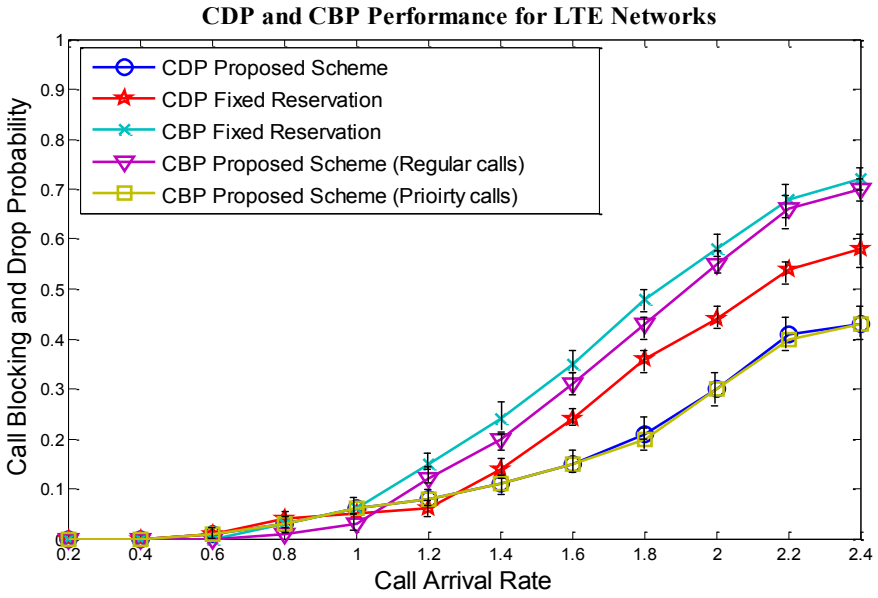


Figure 4.16 Performance of CAC for LTE networks in second scenario

The following points are observed from the simulation results:

- The CBP and CDP performances for the proposed scheme are similar to that of the first scenario for both WiMAX and LTE networks.
- When the system has low call arrival rate, the CDP and CBP performances of both the fixed and the proposed schemes are the same.
- In the second scenario, both CBP and CDP performances of the proposed scheme are better than the fixed bandwidth reservation scheme, even better than the first scenario during medium load conditions. The CBP performance is improved by admitting least priority calls for the unused reserved bandwidth and the CDP performance is improved by bandwidth pre-emption. At the call arrival rate of 1.6 in the WiMAX network, the CDP and CBP performances are: CBP for SC_1 calls in the fixed reservation scheme (without bandwidth reservation for new calls) is ~0.48, whereas in the proposed scheme it is ~0.25; the CDP of the handoff calls in the fixed reservation is 0.385, whereas in the proposed scheme it is ~0.255; the CBP of the normal call in the fixed reservation is ~0.48, whereas in the proposed scheme it is 0.455.

4.5.3. Performance Evaluation of Downlink Scheduling Schemes

In this simulation, the performance metrics for analyzing the PS schemes are PDR, also called normalized throughput, delay, jitter and QoS factor. The QoS factor is useful for evaluating QoS satisfaction of the service flow, which is a function of packet loss and delay performance of the connection.

The PDR for the given connection or service flow is calculated by dividing the total number of packets received divided by total number of packets transmitted.

$$PDR = \frac{Total\ no.of\ packets\ received}{Total\ no.of\ packets\ transmited} \tag{4.31}$$

The PDR for the service flows SC_1 to SC_4 are shown in Figures 4.17 to 4.20. The PDR performance for the PS schemes are similar in both LTE and multihop WiMAX networks, but the LTE network has more system capacity.

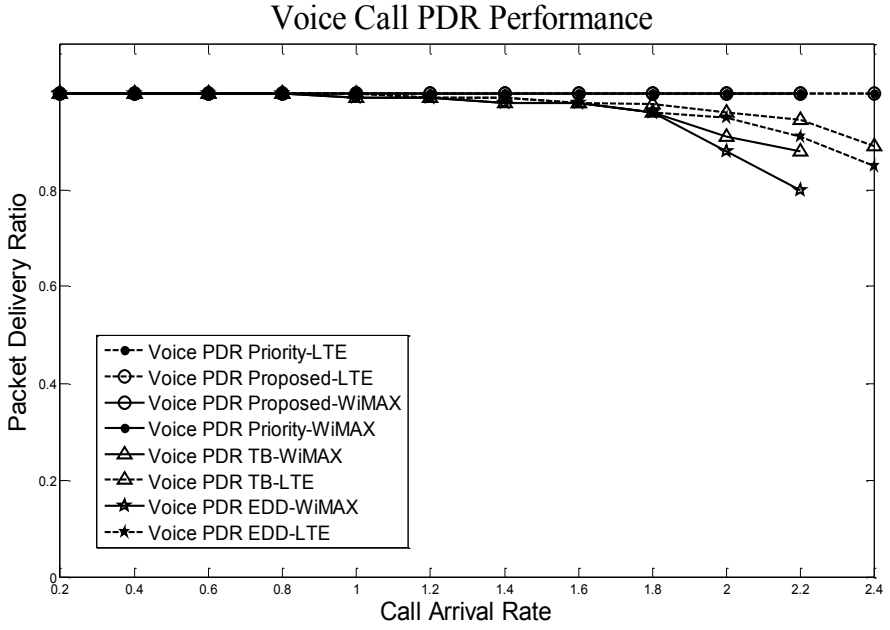


Figure 4.17 PDR performance for the voice application

Figure 4.17 shows the PDR performance of voice application (SC_1). The PDR performance of the proposed and priority scheduler are same. Since the voice application (SC_1) is scheduled first in both schedulers, the PDR performance is ~1. The packet loss, or error, during transmission is negligible and there is no packet drop due to long waiting time in a queue. Conversely, EDD and TB scheduling has a similar PDR performance of ~1 at minimum load condition. After the call arrival rate of 1.0, few packets are getting dropped in TB and EDD. Further, when the system is at over load condition (beyond the call arrival rate1.4) more packets are getting dropped in the EDD scheduler. The PDR performance at the call arrival rate of 2 in WiMAX and 2.2 in LTE are ~0.88 and ~0.91. The starvation of voice packets in EDD is due to the bandwidth allocation for low priority packets when deadline timing is shorter than the voice packet.

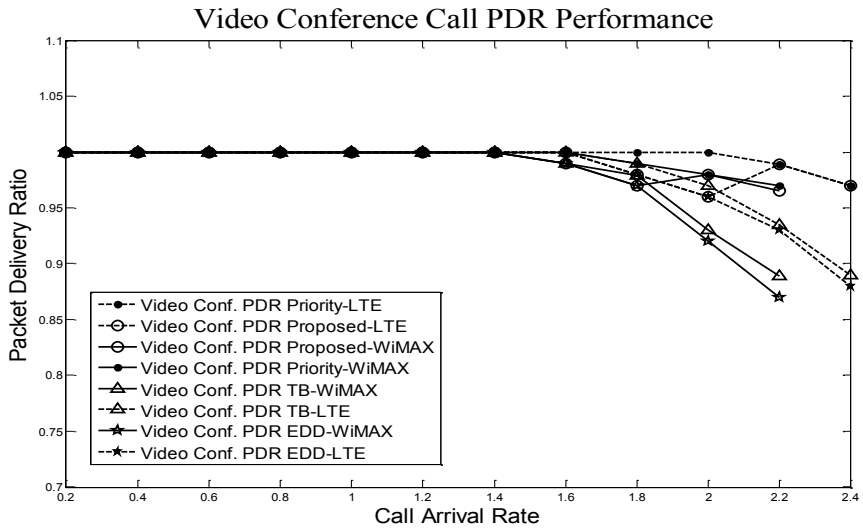


Figure 4.18 PDR performance for the video conference application

The PDR performance of the video conference application (SC_2) is shown in Figure 4.18. From the simulation results, it is clear that the priority and the proposed schedulers perform better than other schedulers, because it schedules SC_2 traffic immediately, next to voice application. On the other hand, the performance of TB and EDD scheduling is similar to the voice application. For example, when the system is overloaded more packets are dropped in the EDD and TB schedulers. The EDD and TB schedulers fail to pre-empt the SC_4 traffic that causes the bandwidth starvation for real-time video packets. However, the proposed scheduler has closer performance with EDD until the system reaches full load, where the PDR is 0.96. After that, the PDR is increased to 0.98 and the performance is closer to priority scheduling 0.99. The (P+TB) scheduler provides QoS assurance even when the system is overloaded.

The PDR performance of the video streaming application (SC_3) is shown in Figure 4.19. The performance of the proposed EDD and TB schedulers are closer until the system reaches full load condition (call arrival rate of 1.0). After that, priority and the proposed schedulers have closer performance levels. On the other hand, the PDR for the EDD scheduler is slightly reduced at overload condition, because the bandwidth is shared for SC_4 traffic. In a WiMAX network, the PDR for the EDD, TB, priority and proposed schedulers at the call arrival rate of 2 are 0.93, 0.96, 0.99 and 0.975.

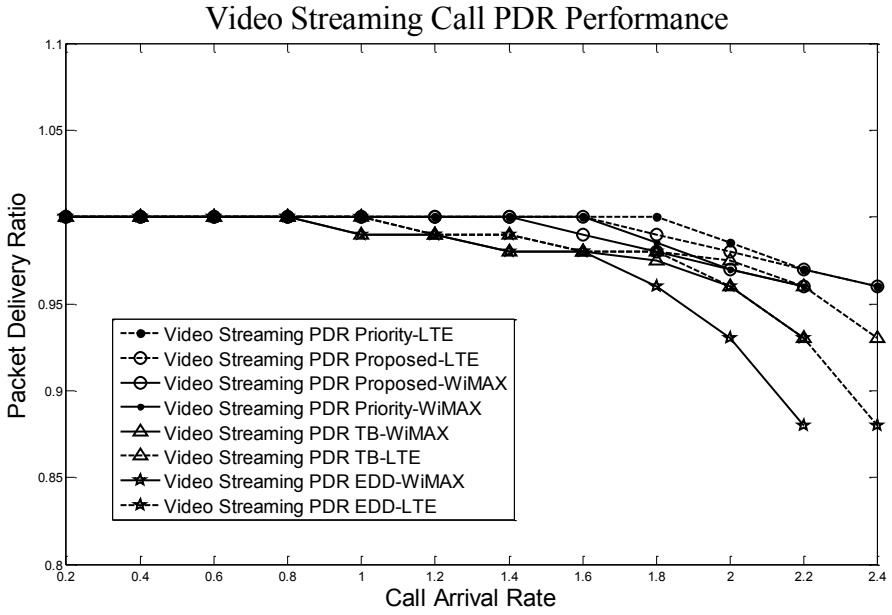


Figure 4.19 PDR performance for the video streaming application

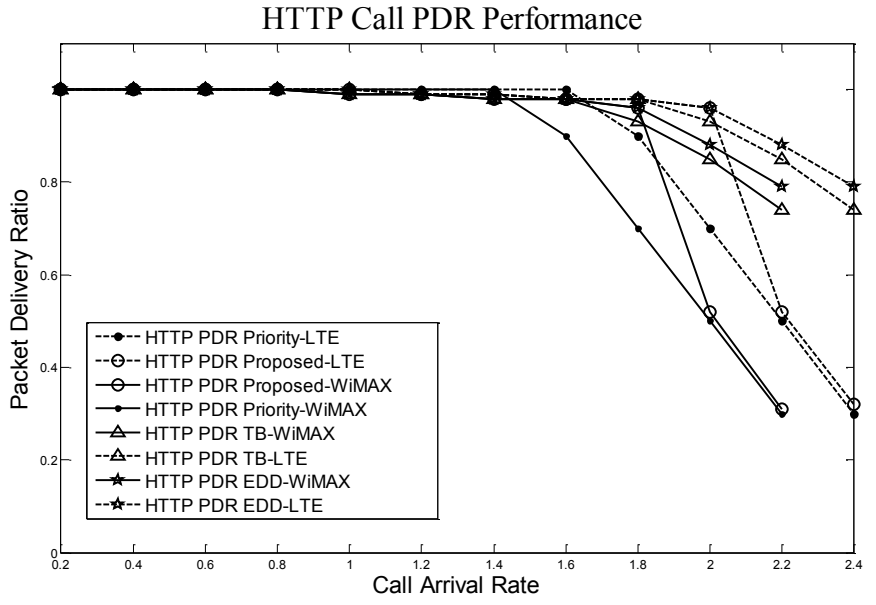


Figure 4.20 PDR performance for the HTTP application

Figure 4.20 shows the PDR performance for HTTP application (SC_4). From the simulation results, it is evident that the PDR performance of the proposed EDD and TB schedulers are closer until the system reaches full load condition. After that, the PDR performance of the EDD is higher than the other schedulers. The PDR for the EDD at the

call arrival rate of 2.0 is 0.88 for the WiMAX network. However, PDR for the TB scheduler is 0.6, because the bandwidth allocation is only for the generated tokens. On the other hand, the PDR for the priority scheduler starts reducing at medium load condition and is drastically reduced during overload condition. Also, the PDR performance of the proposed scheduler is drastically reduced from full load condition as the scheduling algorithm is switched from (P+E) to (P+TB). The PDR for the priority and the proposed schedulers at the call arrival rate of 2.1 is 0.35 and 0.46 for the WiMAX network.

Table 4.10 The PDR Performance, CI Values for the Proposed PS Scheme in WiMAX

Call arrival rate	Applications								
	Video conference			Video streaming			HTTP		
	Lower	Mean	Upper	Lower	Mean	Upper	Lower	Mean	Upper
0.2	~1	~1	~1	~1	~1	~1	~1	~1	~1
0.4	~1	~1	~1	~1	~1	~1	~1	~1	~1
0.6	~1	~1	~1	~1	~1	~1	~1	~1	~1
0.8	~1	~1	~1	~1	~1	~1	.9985	~1	~1
1.0	~1	~1	~1	~1	~1	~1	0.988	0.992	0.996
1.2	~1	~1	~1	0.989	0.994	~1	0.985	0.989	0.993
1.4	0.991	0.995	~1	0.984	0.991	0.998	0.979	0.984	0.989
1.6	0.979	0.986	0.993	0.980	0.988	0.996	0.905	0.916	0.927
1.8	0.987	0.993	~1	0.970	0.979	0.988	0.849	0.860	0.871
2.0	0.972	0.980	0.988	0.955	0.965	0.975	0.516	0.526	0.536
2.2	0.956	0.965	0.974	0.946	0.954	0.962	0.333	0.349	0.365

PDR performance along with confidence interval: The PDR performance of the proposed PS scheme along with the lower and upper bounds of the 95% confidence interval for video conference, video streaming and HTTP application is given in Table 4.10. As the performance of the voice application for the proposed PS scheme is very closer for all iterations, confidence interval is not presented. In the table, if the PDR value is greater than 0.999, it was represented as ~1.

Average delay: It is calculated by dividing the total delay of an individual transmitted packet by total transmitted packets. When the packet exceeds the deadline time

period, the packet will be dropped. Hence, the delay measurement of an individual packet will be less than the packet deadline length. The average delay is given by

$$Average\ delay\ (in\ msec) = \frac{\sum D_{ik}(in\ msec)}{T_k} \tag{4.32}$$

Where, D_{ik} is the delay of i^{th} transmitted packet from k^{th} service flow (SC_1, SC_2, SC_3 and SC_4) and T_k is the total transmitted packets for the k^{th} service flow.

The average delay or latency for the service flows SC_1 to SC_4 are shown in Figures 4.21 to 4.24. From the latency performance results, it is observed that the LTE network has very good latency performance than the WiMAX network because in LTE, the MAC layer has a support to schedule the downlink traffic for 1msec time intervals. On the other hand, the average latency presented in this simulation for the WiMAX networks include two hop transmissions and 5msec frame period.

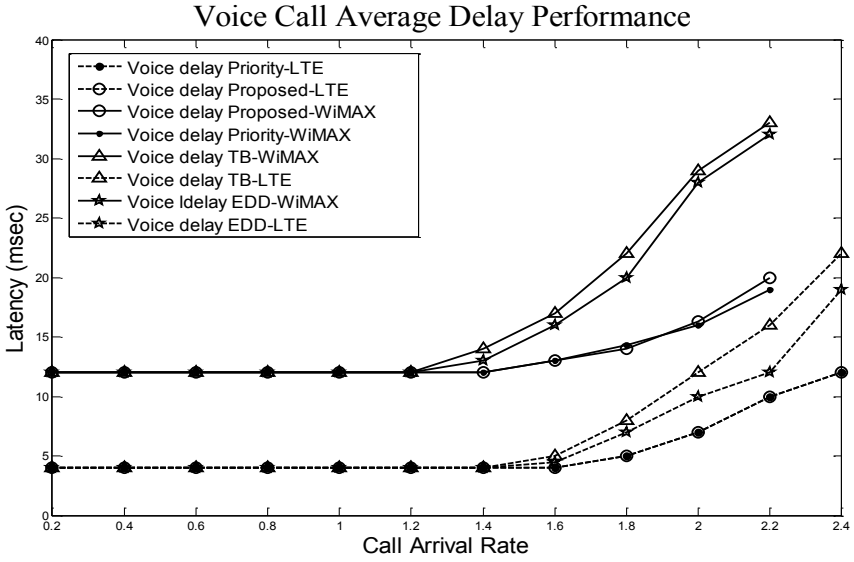


Figure 4.21 Average delay for the voice application

The average latency for voice application (SC_1) in both LTE and multihop WiMAX networks is shown in Figure 4.21. From the simulation results, it is clear that the average latency for the proposed scheduling scheme and priority scheduler are the same. On the other hand, latency for EDD and TB scheduling starts increasing from the call arrival rate of 1.0 and has a significant delay difference of ~15msec at the call arrival rate of 2.0 for

multihop WiMAX networks. The latency values of priority, EDD, TB and the proposed schedulers are ~15msec, ~28msec, ~30msec and ~16 msec.

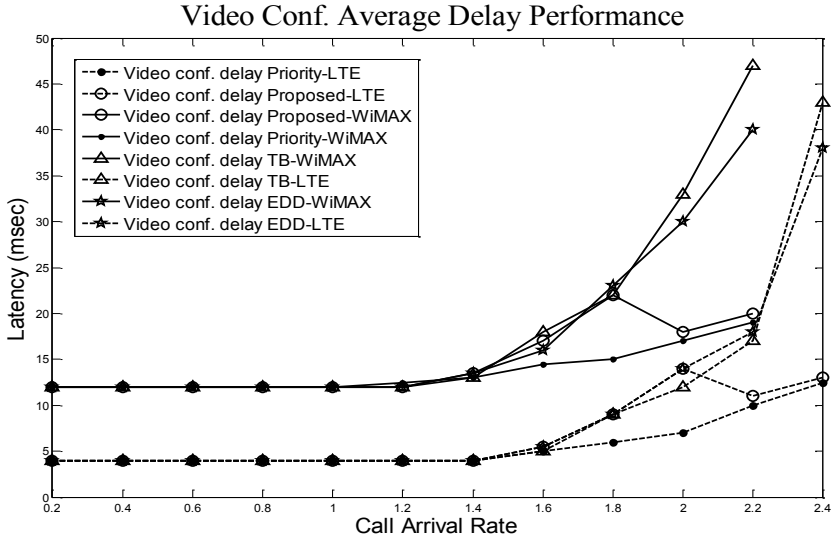


Figure 4.22 Average delay for the video conference application

The average latency performance of video conference application (SC_2) is shown in Figure 4.22. The scheduler's behaviour for the latency performance is similar to voice application. The latency performance of the priority, EDD, TB and the proposed schedulers at the call arrival rate of 2.0 is ~17msec, ~31msec, ~33msec and ~18msec. Similarly, for the LTE network at the call arrival rate of 2.2 is ~9msec, ~32msec, ~31msec and ~11msec.

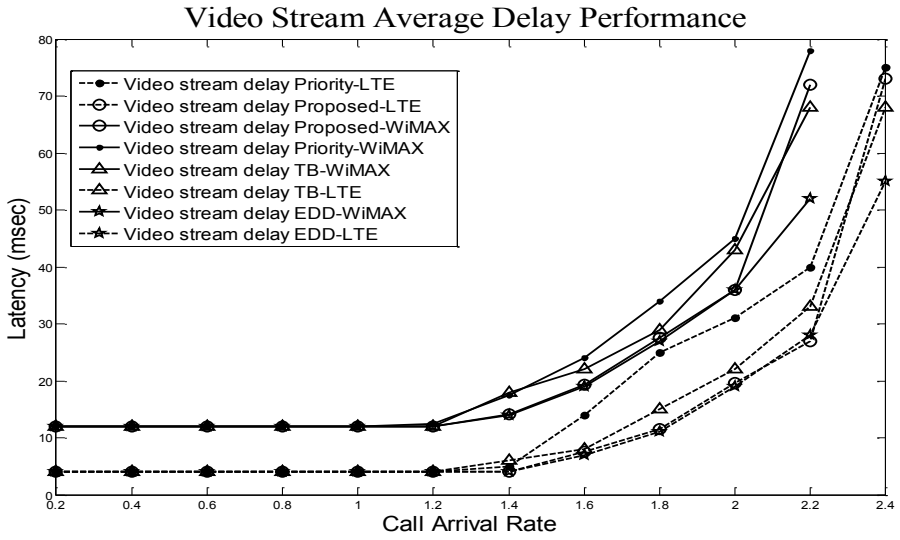


Figure 4.23 Average delay for the video streaming application

Figures 4.23 and 4.24 show the latency performance of video streaming (SC_3) and HTTP application (SC_4). For both applications, the proposed, EDD and TB schedulers have similar performance until the call arrival rate of 1.0. After that, EDD and TB schedulers have higher performance than the other schedulers. On the other hand, latency for video streaming and HTTP applications in priority scheduler starts reducing from the call arrival rate of 1.2 and there is a significant difference at the call arrival rate of 2.0.

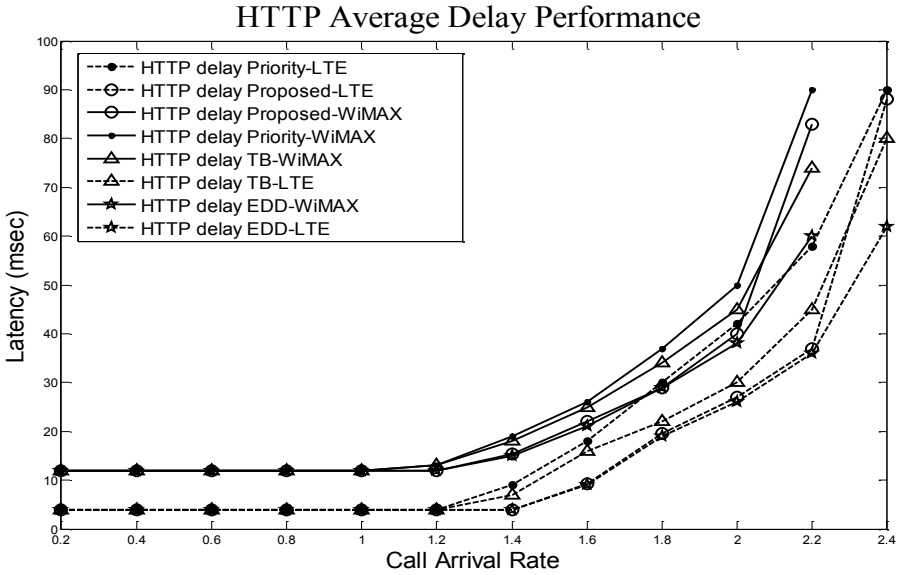


Figure 4.24 Average delay for the HTTP application

Average delay along with confidence interval: The average delay for the proposed scheduler along with the lower and upper limits of the 95% confidence interval for video conference, video streaming and HTTP application is given in Table 4.11.

Table 4.11 The Delay Performance, CI Values for the Proposed PS Scheme in WiMAX

Call arrival rate	**Applications**								
	Video conference			**Video streaming**			**HTTP**		
	Lower	**Mean**	**Upper**	**Lower**	**Mean**	**Upper**	**Lower**	**Mean**	**Upper**
0.2	11.91	11.98	12.07	11.95	12.05	12.15	12.93	13.08	13.23
0.4	11.90	12.00	12.1	12.31	12.46	12.61	13.25	13.40	13.55
0.6	12.01	12.12	12.23	12.76	12.88	13.00	13.37	13.72	14.07

0.8	12.25	12.40	12.55	12.85	13.10	13.25	13.49	14.00	14.51
1.0	12.36	12.55	12.64	13.11	14.56	16.01	13.17	14.64	16.11
1.2	12.58	12.78	12.98	14.44	15.24	16.04	16.23	17.50	18.77
1.4	13.05	14.10	15.15	18.0	19.50	21.00	20.85	22.45	24.05
1.6	19.04	20.05	21.06	33.45	35.05	36.65	36.20	37.20	38.20
1.8	17.03	18.98	20.93	32.32	34.02	35.72	34.84	35.95	37.06
2.0	18.71	19.75	20.79	34.84	36.49	38.14	39.44	41.25	43.06
2.2	20.01	21.51	23.01	70.62	72.82	75.02	82.11	84.10	86.09

Average jitter: It is calculated by dividing the total jitter of an individual transmitted packet by the total transmitted packets. Jitter is calculated by measuring delay difference between i^{th} transmitted packet and $(i\text{-}1)^{th}$ packet.

$$Average\ jitter\ (in\ msec) = \frac{\sum J_{ik}(in\ msec)}{T_k} \tag{4.33}$$

Where j_{ik} is the jitter of i^{th} transmitted packet from k^{th} service flow and $j_{ik} = |D_{ik} - D_{(i-1)k}|$

The behaviour of the schedulers for jitter performance for different applications is similar to latency performance. Therefore, the results at different call arrival rates for the multihop WiMAX networks are given in Table 4.12. Here, as the jitter performance for HTTP application is not applicable, only other applications are tabulated. For the proposed PS scheme, the mean jitter value along with lower and upper bound of the 95% confidence interval values are tabulated.

Table 4.12 Jitter at Various Loads in WiMAX Network

Application	**Priority**	**EDD**	**TB**	**Proposed with CI values**		
				Lower	**Mean**	**Upper**
Jitter measurement at the call arrival rate of 0.8 (in msec)						
Voice (SC_1)	0.03	0.28	0.23	0.0281	0.031	0.0339
Video conference (SC_2)	0.17	0.29	0.21	0.242	0.250	0.258
Video streaming (SC_3)	0.52	0.35	0.39	0.371	0.382	0.393

Jitter measurement at the call arrival rate of 1.2 (in msec)						
Voice (SC_1)	0.15	0.33	0.41	0.149	0.155	0.161
Video conference (SC_2)	0.46	0.54	0.57	0.574	0.586	0.598
Video streaming (SC_3)	2.61	1.38	1.42	1.911	1.930	1.949
Jitter measurement at the call arrival rate of 2, Overload condition (in msec)						
Voice (SC_1)	0.30	2.14	2.93	0.290	0.302	0.314
Video conference (SC_2)	1.55	3.89	4.35	4.210	4.261	4.312
Video streaming (SC_3)	12.11	6.32	8.91	9.265	10.130	10.995

QoS factor: It is a function of the QoS parameters measured versus the requirement for the connection/service flow. The two important QoS parameters, Packet Loss Rate (PLR) and delay are considered for measuring the QoS factor [73].

$$\text{QoS factor} = f(QoS_k) = \frac{PLR_k}{PLR_{req,k}} \cdot \frac{D_k}{D_{max,k}} \tag{4.34}$$

Where PLR_k and D_k is the packet loss rate and delay for the service flow k, and $PLR_{reg,k}$ and $D_{max,k}$ denotes the packet loss and delay requirement for the service flow k.

Table 4.13 QoS factor for Various Schedulers in WiMAX Network

Application	**Priority**	**EDD**	**TB**	**Proposed**
At the call arrival rate of 1.2, full load condition				
Voice (SC_1)	0.43	0.63	0.57	0.43
Video conference (SC_2)	1.12	1.91	1.90	1.89
Video streaming (SC_3)	2.71	1.93	1.96	1.94
HTTP (SC_4)	5.39	2.40	2.45	2.84
At the call arrival rate of 2, overload condition				
Voice (SC_1)	0.52	1.72	1.43	0.52
Video conference (SC_2)	1.36	3.41	2.90	1.41
Video streaming (SC_3)	4.97	3.68	3.88	4.99
HTTP (SC_4)	11.69	5.24	6.01	10.12

The QoS factor value for the multihop WiMAX network at the call arrival rate of 1.2 and 2.0 are given in Table 4.13. The QoS factor is useful for analyzing the QoE support

for the given service flow and QoS differentiation among different schedulers. The basic parameters for evaluating QoE are packet loss, delay and jitter. Other parameters are application specific parameters such as noise level for voice, media delivery index for video streaming, etc. [116]. From the equation (4.34), it is clear that the QoS factor value is below one, only when the network performance is optimum. Hence, the application may achieve expected QoE value. The ideal QoS factor value is zero, but that happens only in an ideal case whereas PLR is zero. In practice, the actual packet loss requirement for the HTTP application is ~0 or very minimum. However, the packet loss requirement for both SC_3 and SC_4 is considered as 1E-04 because the retransmission is not included in this simulation. Further, the Transport Layer protocol used in this simulation is User Datagram Protocol (UDP) that won't react on the traffic flow during more packet loss and delay. Therefore, some of the results in this Table 4.13 exceed the value one.

From the QoS factor evaluation, it is visible that the proposed PS scheme provides a well QoS differentiation among different service classes. At full load condition, the QoS factor for the priority and the proposed scheduler in voice and video services have closer performance, but the performance of HTTP is more affected in the priority scheduler. However, the least priority service flow is highly affected in both schedulers at overload condition. On the other hand, even though the EDD and TB schedulers provide QoS differentiation, the performance of real-time services are highly affected at overload condition. This is an undesirable effect of the EDD and TB schedulers.

4.5.4. Performance Evaluation of Uplink Scheduling Schemes

In general, the design of uplink scheduler is more complex than the downlink scheduler because the BS/eNB knows the traffic details in the downlink. For uplink, the uplink scheduler in the BS decides the amount of bandwidth allocation, based on the bandwidth requests made by the MSs/UEs and the QoS provisioning whereas the uplink scheduler in the MS/UE allocates bandwidth among different applications. In this simulation, the uplink scheduler residing in the BS allocates bandwidth for every frame period using the PF scheme. The QoS parameters measured in this simulation are PDR and

average delay for the (P+E) and (P+TB) schedulers and compared with the real-time priority, EDD and TB schedulers.

$$BW\ Alloc.of\ MS_i = BW.req\ from\ MS_i * \frac{remaining\ BW}{\sum_{i=1}^{n} BW.req\ from\ MS_i} \quad (4.43)$$

Where the remaining bandwidth = total BW (capacity) – total UGS BW.

PDR Performance

Figures 4.25 – 4.28 illustrate the PDR performance of the UGS, rtPS, nrtPS and BE traffic classes (SC_1, SC_2, SC_3 and SC_4), respectively. Figure 4.25 shows the PDR performance of UGS service class for multihop WiMAX networks. In that, priority, (P+E) and (P+TB) schedulers schedule the UGS traffic immediately, and their performance is ~1.0. Hence, the graphs are overlapping each other. On the other hand, the EDD and TB schedulers handle the UGS traffic as similar to the other traffics (applications). Therefore, more packets are getting dropped in the queue due to long waiting time and the PDR performance is reduced after the call arrival rate of 1.2 (i.e., system is fully loaded). In Figure 4.25, the PDR performance of the EDD and TB schedulers at the call arrival rate of 1.6 is ~0.99 and ~0.986. When the call arrival rate is further increased, the PDR performance for EDD and TB schedulers is significantly reduced.

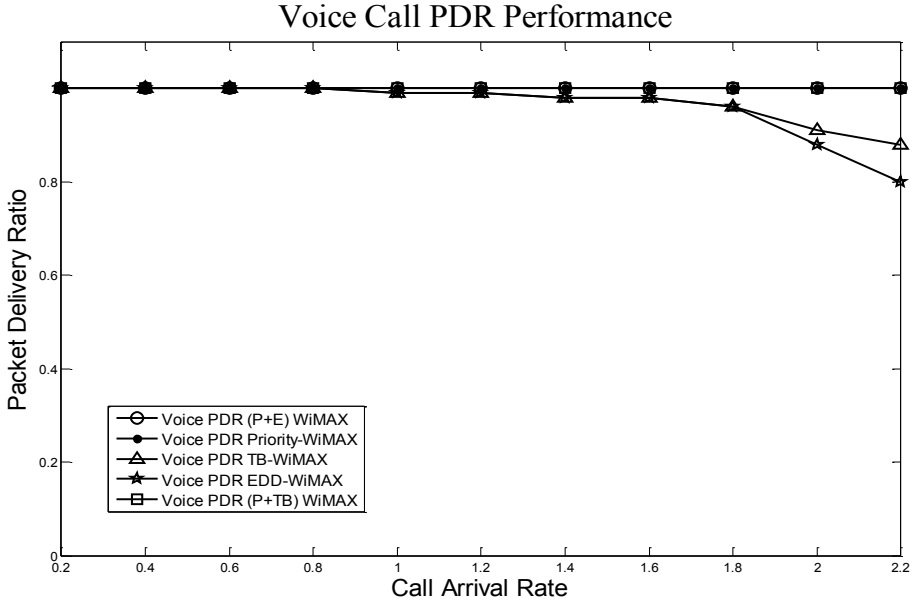


Figure 4.25 PDR for the voice application in WiMAX uplink

Figure 4.26 – 4.28 shows the PDR performance for the rtPS, nrtPS and BE service classes. The PDR performance is pretty much similar to the downlink traffic.

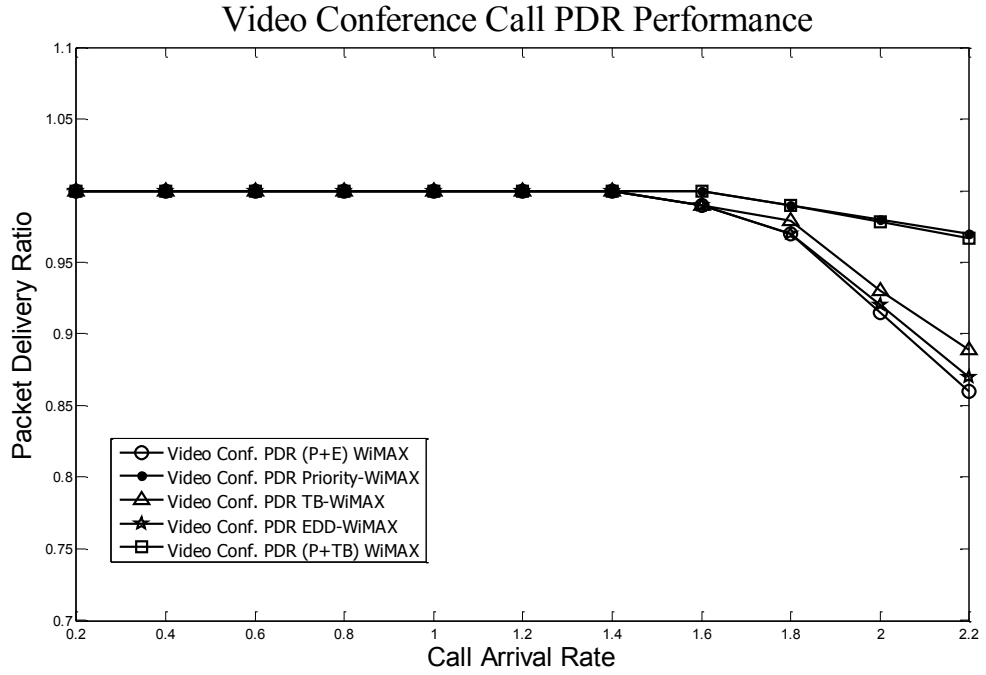


Figure 4.26 PDR for the video conference application in WiMAX uplink

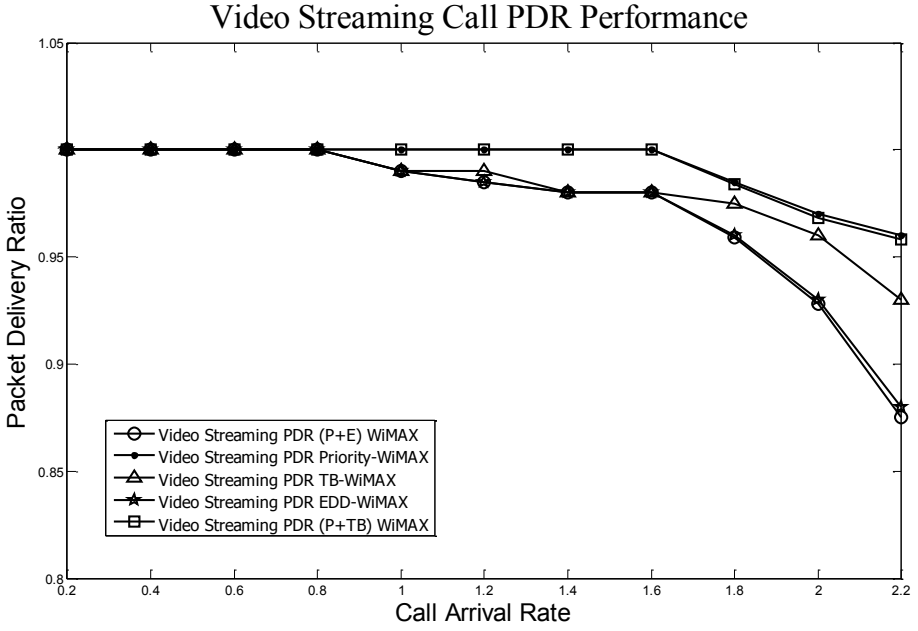


Figure 4.27 PDR for the video streaming application in WiMAX uplink

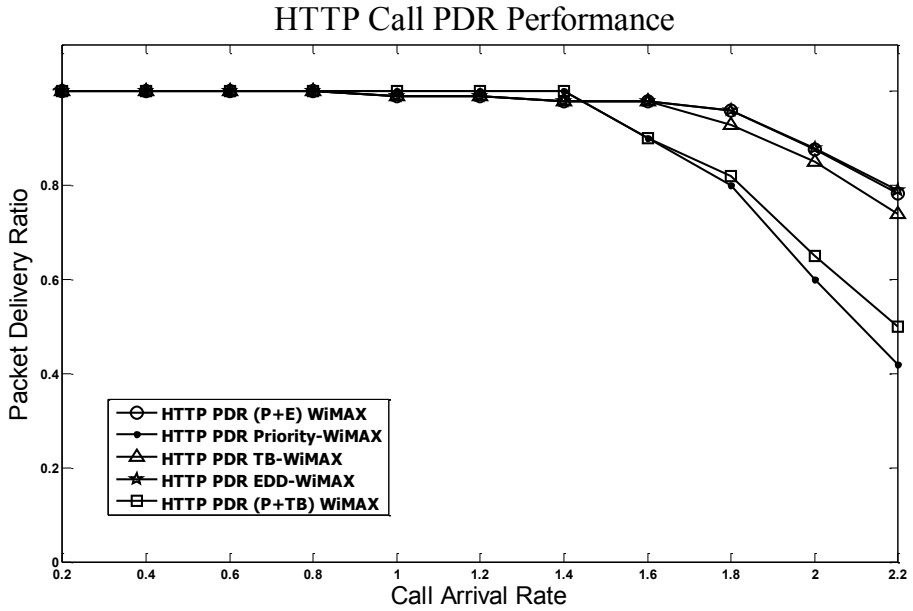


Figure 4.28 HTTP call PDR performance in WiMAX uplink

From the simulation results the following points are inferred.

- The performance of (P+E), EDD and TB schedulers are similar. These schedulers provide a very good inter-class fairness, but the real-time service flows are getting affected during the system overload conditions.
- As the (P+TB) scheduler performs closely to the priority scheduler, the inter-class fairness is lower than the (P+E), TB and EDD schedulers. On the other hand, priority and (P+TB) schedulers provide a QoS assurance during the system overload condition.
- At the call arrival rate of 1.6, the PDR performances are:
    - For the rtPS service class, the (P+E), EDD and TB schedulers have a closer performance of ~0.99, ~0.986 and ~0.982, whereas the priority and the (P+TB) schedulers have a performance of ~1. When the call arrival rate is increased, the PDR performance of (P+E), EDD and TB schedulers is highly reduced.

- For the nrtPS service class, the priority and (P+TB) schedulers have the performance of ~0.92 and ~0.926, whereas the (P+E), EDD and TB schedulers have the performance of ~0.98, ~0.976 and ~0.978.
- For the BE service class, the priority and (P+TB) schedulers, the PDR is significantly reduced to ~0.9 and ~0.91. On the other hand, the (P+E), EDD and TB schedulers have the PDR performance of ~0.98, ~0.985 and ~0.982.

PDR performance along with confidence interval: The PDR performance of the (P+TB) uplink scheduler along with the lower and upper bounds of the 95% confidence interval for video conference, video streaming and HTTP application is given in Table 4.14.

Table 4.14 PDR with CI Values for the (P+TB) Scheduler in WiMAX Uplink

Call arrival rate	**Applications**								
	Video conference			**Video streaming**			**HTTP**		
	Lower	**Mean**	**Upper**	**Lower**	**Mean**	**Upper**	**Lower**	**Mean**	**Upper**
0.2	~1	~1	~1	~1	~1	~1	~1	~1	~1
0.4	~1	~1	~1	~1	~1	~1	~1	~1	~1
0.6	~1	~1	~1	~1	~1	~1	~1	~1	~1
0.8	~1	~1	~1	~1	~1	~1	0.9986	~1	~1
1.0	~1	~1	~1	~1	~1	~1	0.984	0.990	0.996
1.2	~1	~1	~1	0.991	0.994	0.997	0.984	0.988	0.992
1.4	0.992	0.995	0.998	0.984	0.989	0.994	0.978	0.984	0.990
1.6	0.981	0.986	0.991	0.979	0.984	0.989	0.910	0.916	0.922
1.8	0.989	0.993	0.997	0.970	0.975	0.980	0.845	0.855	0.865
2.0	0.970	0.980	0.990	0.955	0.968	0.981	0.509	0.520	0.531
2.2	0.957	0.965	0.973	0.940	0.952	0.964	0.333	0.369	0.402

Average Delay: Figures 4.29– 4.32 demonstrate the average delay of UGS, rtPS, nrtPS and BE traffic for the priority, EDD, TB, (P+E) and (P+TB) schedulers, respectively.

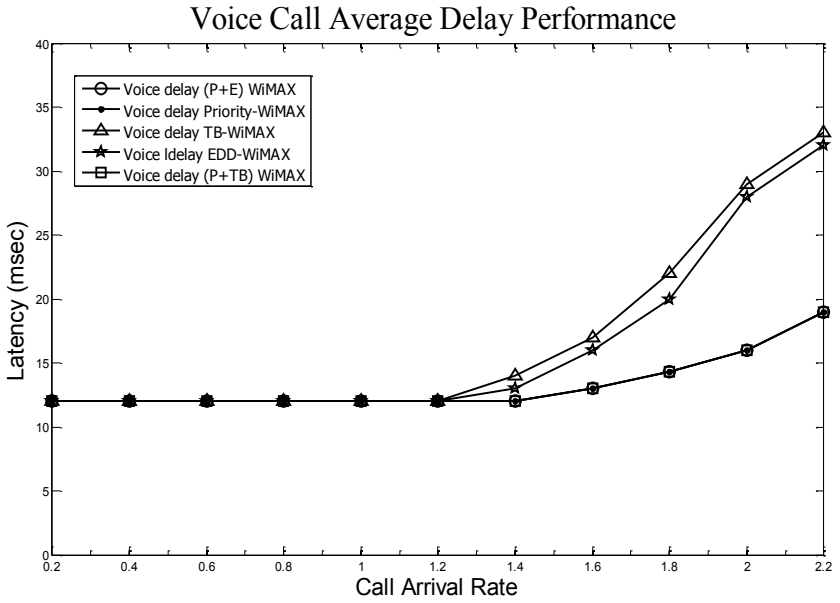


Figure 4.29 Average delay for the voice application in WiMAX uplink

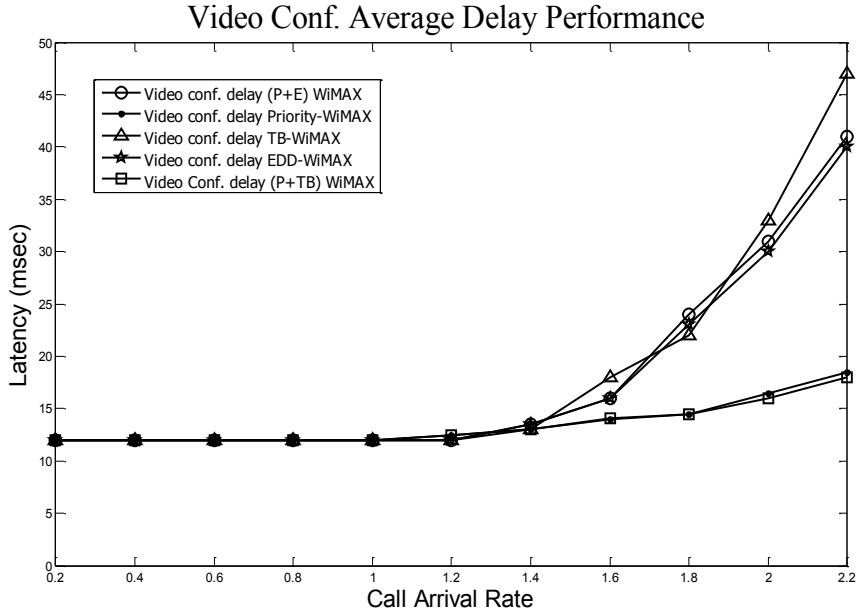


Figure 4.30 Average delay for the video conference application in WiMAX uplink

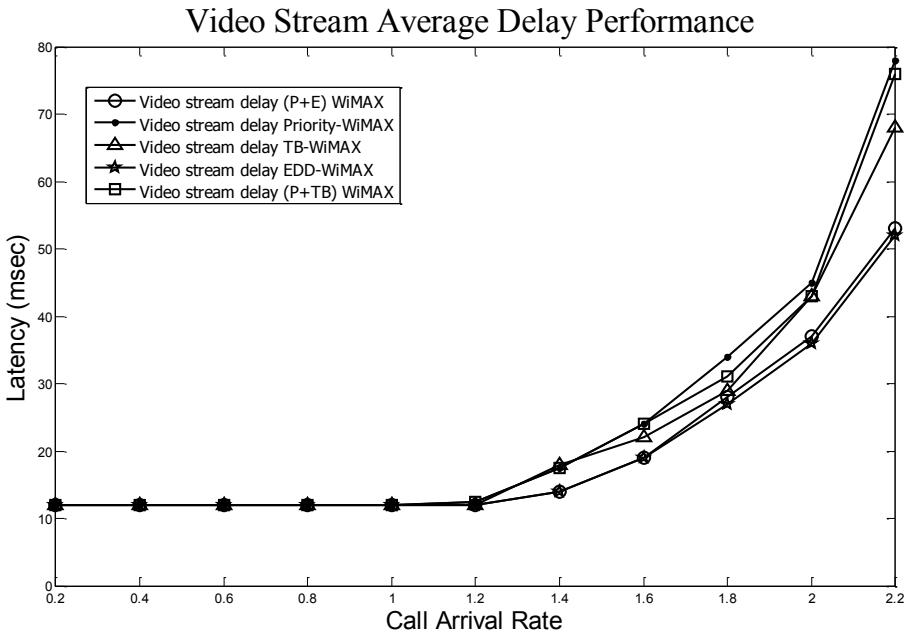


Figure 4.31 Average delay for the video streaming application in WiMAX uplink

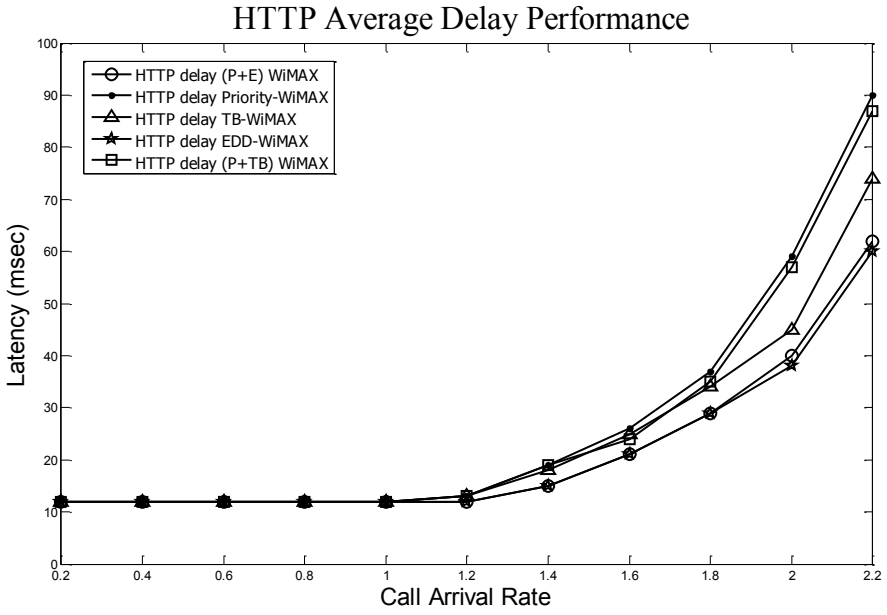


Figure 4.32 Average delay for the HTTP application in WiMAX uplink

When the call arrival rate of the system is at 2.0, the following points are observed:

- The average delay for the UGS traffic for (P+E), (P+TB) and priority schedulers are the same, because both schedulers schedule the packet immediately for the allocated

bandwidth. The latency values of the priority, (P+E) and the (P+TB) schedulers are ~14msec, whereas the EDD, and the TB schedulers are ~26msec and ~28msec.

- For rtPS traffic, the average delay for priority, (P+TB), EDD, (P+E) and TB schedulers is ~17.5msec, ~16.9msec, ~30msec, ~31msec and ~31msec respectively. The average delay for (P+E), EDD and TB schedulers is longer than priority and (P+TB) schedulers.
- For nrtPS traffic, the priority and (P+TB) schedulers take a longer time to schedule the packet: ~47msec and 43msec. On the other hand, the average delay for the EDD (P+E) and TB schedulers is ~35.4msec, ~36msec and ~37msec.
- The latency performance of priority and (P+TB) schedulers is significantly reduced for BE traffic. The average delay for the priority, (P+TB), EDD, (P+E) and TB schedulers is ~58.7msec, ~57msec, ~33msec, ~34msec and ~37msec respectively.

Average delay along with confidence interval: The average delay for the (P+TB) uplink scheduler along with the lower and upper bounds of the 95% confidence interval for video conference, video streaming and HTTP application is given in Table 4.15.

Table 4.15 Delay with CI Values for the (P+TB) Scheduler in WiMAX Uplink

Call arrival rate	Applications								
	Video conference			Video streaming			HTTP		
	Lower	Mean	Upper	Lower	Mean	Upper	Lower	Mean	Upper
0.2	11.92	12.01	12.09	12.35	12.45	12.55	13.05	13.21	13.37
0.4	11.92	12.04	12.16	12.41	12.66	12.81	13.40	13.55	13.70
0.6	12.00	12.15	12.30	12.76	12.88	13.00	13.67	14.02	14.37
0.8	12.30	12.42	12.54	12.85	13.20	13.45	13.59	14.10	14.61
1.0	12.36	12.56	12.66	13.11	14.61	16.11	13.28	14.75	16.22
1.2	12.58	12.78	12.98	14.44	15.24	16.04	16.23	17.50	18.77
1.4	13.15	14.20	15.25	18.05	19.51	20.97	21.45	23.05	24.65
1.6	19.04	20.05	21.06	33.45	35.05	36.65	36.15	37.20	38.25
1.8	17.03	18.98	20.93	32.42	34.12	35.82	34.84	35.95	37.06
2.0	18.61	19.75	20.89	35.84	37.49	39.14	39.84	41.65	43.66
2.2	21.10	22.51	23.02	70.65	72.85	75.05	83.06	85.05	87.04

4.6 Chapter Summary

In this chapter, the proposed RRM framework for the 4G multihop wireless networks was analyzed using the mathematical model and system level simulations. The RRM framework consists of adaptive CAC and dynamic PS schemes for the downlink traffic. The proposed CAC scheme was modeled using the Markov chain model. In the Markov chain modeling, the numerical solutions for CBP and CDP were derived by solving global balance and local balance equations. However, the system was first approximated to consider the pre-emption queue for BE calls and further approximated due to the non-linearity of the system that was introduced in the first approximation. The results for CBP and CDP from both modeling of the approximated system and the simulation are close, whereas the CBP in the proposed CAC scheme is much better than that in the fixed reservation scheme. Finally, the proposed CAC scheme was simulated for the WiMAX and LTE network environments. The performance metrics, CBP and CDP, are compared with the fixed reservation scheme where the proposed scheme significantly improves the CDP for handoff calls and the CBP for high priority new calls.

In the proposed RRM framework, when the CAC pre-empts the least priority calls, the scheduler is responsible to avoid distributing the bandwidth allocation to least priority users to ensure the bandwidth assurance for real-time service flows. Hence, the dynamic selection of (P+E) and (P+TB) scheduling was proposed for the WiMAX and LTE networks. Using NS2 simulation, the QoS performance such as PDR, latency, jitter and QoS factors were studied for the proposed and existing schedulers. The simulation results for the scheduling policy and QoS factor evaluation shows that the proposed dynamic selection of the (P+E) and (P+TB) scheduling schemes ensure QoS differentiation among different service flows at various load conditions and improves latency performance. Similarly, the (P+TB) scheduler outperforms the priority, EDD, TB and (P+E) schedulers for the uplink data.

In both CAC and PS simulations, the relay nodes were fixed. However, if the simulation is extended for mobile relay nodes, similar performance results could be achieved, because the bandwidth reservation in the CAC method is adaptive and the

latency in the PS scheme is modified for handover users. Further, the downlink simulation for LTE networks is single-hop, because the available open source simulator included in NS2 does not support multihop. Therefore, similar performance results could be achieved for multihop simulation, because the network architecture for WiMAX and LTE is similar and the proposed scheme works well for the multihop WiMAX networks.

Chapter 5. QoS Aware Security Architecture for 4G Multihop Wireless Networks

Providing a strong security is necessary for any wireless access networks, but it is a more challenging task for the multihop networks and high mobility environment. The WiMAX and LTE standards provide well defined security architecture for both service providers and users to support multihop and high mobility environment. However, some security threats, such as DoS, an introduction of rouge node, long authentication delay for WiMAX handoff users, etc., still exist in 4G wireless networks. Hence, strong security architecture is needed to solve the existing security threats in these networks. Conversely, the network QoS performance should not be degraded while enhancing the security. This chapter describes the proposed security architecture to solve the existing security threats in 4G wireless networks (WiMAX and LTE), and analyze the security and QoS performance.

5.1 Problem Statement

In wireless communications, security threats may occur in both the PHY and the MAC layers. The attacker can attack the Radio Frequency (RF) channel for the PHY layer threats. For the MAC layer threats, the attackers can spoof, modify and replay the MAC layer messages. In this research work, only on the MAC layer security threats are concentrated to provide QoS aware security solutions. The most important MAC layer security threats, such as a DoS attack before authentication, identity privacy vulnerability due to disclosure of IMSI in the WiMAX and LTE networks, are due to unprotected MAC management messages. Next, the multihop WiMAX standard introduces the optional distributed security mode and tunnel mode operations. The distributed security mode provides hop-by-hop authentication, but multihop RSs may not use the tunnel mode operation as they do not have SA with the BS. Finally, the recent research works in multihop WiMAX and LTE networks use network coding for QoS improvement that leads to network coding security threats. In existing research efforts, there is a lack of the

integrated presentation and solution for WiMAX and LTE networks' security issues. It is necessary to analyze both WiMAX and LTE for network convergence that may be useful for service providers.

On the other hand, service providers may use the IPSec for wireless access due to its popularity in wired network [91, 92]. Usually, IPSec will affect the QoS performance, because the IPSec header in each packet consumes additional bandwidth and takes some time to establish the tunnel. Based on real-time experiments, only a little research has been reported comparing standard security and IPSec. Therefore, a distributed security architecture using ECDH key exchange protocol is proposed for the existing security threats in 4G wireless networks. Also, the security and QoS performance of the proposed security scheme is compared with IPSec and the default security scheme.

5.2 Security Threats in WiMAX and LTE Networks

A comprehensive study of various attacks and countermeasures in WiMAX and LTE networks were investigated in Chapter 3. From that literature study, the major security threats that exist in WiMAX and LTE networks are summarized in this section. The first part describes the common security threats in WiMAX and LTE networks and remaining subsections describe the specific threats in WiMAX and LTE networks individually.

5.2.1. Common Security Threats in WiMAX and LTE Networks

The main cause for the MAC layer security threats in WiMAX and LTE networks are due to certain unprotected MAC management messages. The following security threats are common in both WiMAX and LTE networks:

- Rogue node's DoS and replay attacks during network entry
- Bandwidth stealing
- Network coding specific security threats

Rogue node's DoS and replay attacks during network entry: In WiMAX networks, MS scans the downlink channel for synchronization during network entry. Then, MS starts the Initial Ranging process by sending a RNG_REQ message. BS/RS responds to a MS

with a RNG_RSP message to nullify the frequency, time and power offsets. These RNG_REQ, RNG_ RSP and subsequent MAC messages are in plain text. Consequently, the attacker may act as rogue BS/RS and respond to RNG_REQ message of MS or they intrude and modify the RNG_RSP message of BS/RS. Then, the rogue node sends the RNG_RSP message with the status of RNG_REQ failed instead of actual information sent by the BS/RS. Therefore, the MS continues Initial Ranging until the maximum limit. Finally, the MS failed to connect with the network that leads to DoS attack.

Similarly, the rogue node's DoS and reply attacks in LTE networks may be possible at two stages: one is during initial attachment and the other is after IP connectivity, when UE is sending MAC messages in plain text to eNB. DoS attack during initial attachment is more critical than the one during IP connectivity, because even the UE cannot register with the home network. This is similar to the DoS attack in a WiMAX network during initial network entry. During Random Access procedure, first UE sends Random Access Preamble to the eNB and waits for the response until the predefined time limit. eNB responds to UE for timing adjustments and bandwidth allocation for sending Attach Request message along with PreambleID. If the received Random Access PreambleID do not match with the transmitted Random Access Preamble, the Random Access Response reception is considered unsuccessful and the UE continues the Random Access procedure until the count reaches PREAMBLE_TRANS_MAX. Finally, UE cannot register with the home network that leads to DoS attack.

Bandwidth stealing: This may happen in WiMAX networks, when the attackers continuously send bandwidth request messages to the BS. As a result, the BS may allocate more resources to the fake users that will make bandwidth scarce for original users.

Similarly, in LTE networks, the attackers may requests more data to send than is actually buffered by the real UE [113]. If the eNB sees many fake reports, the Call Admission Controller may not accept the newly arrived UE.

Network coding specific security threats: Network coding technique is recently introduced in the IEEE 802.16m network for enhanced MBS. Also, the recent research efforts in WiMAX and LTE networks use network coding for QoS improvement. In

network coding, multiple packets are linearly or randomly combined together to generate a network coded packets. Some security threats may be introduced when the networks use network coding technique.

There are two general approaches for applying network coding in wireless multihop networks: intra-flow network coding and inter-flow network coding [90]. The intra-flow network coding scheme mixes packets within individual flows, i.e., the source or intermediate nodes mix packets heading to the same destination. The simple example for intra-flow network coding is shown in Figure 5.1a, where the packets, p1 and p2 for the same destination node 'C' is encoded at the intermediate nodes B1 and B2. As a result, each received packet contains some information about all packets in the original file. As a result, the encoding node does not need to learn which particular packet the destination misses, it only needs to get feedback from the destination once the receiving node has received enough packets to decode the whole file.

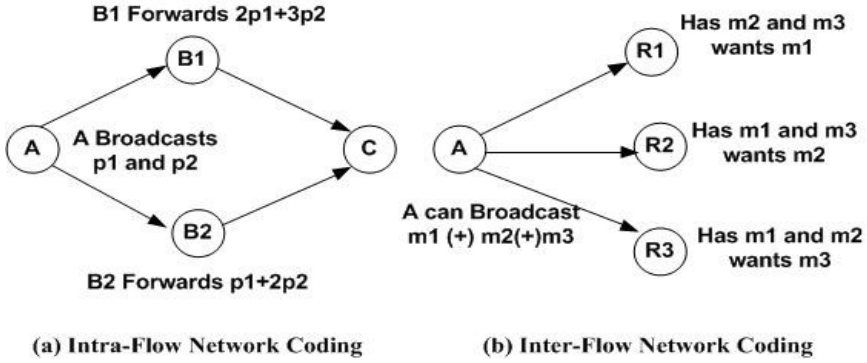


Figure 5.1 Intra-flow and inter-flow network coding [8]

On the other hand, inter-flow network coding scheme mixes packets across multiple flows. The simple example for the inter-flow network coding is shown in Figure 5.1b, where the packets, m1, m2 and m3 for the destinations R1, R2 and R3 are encoded at the sender node A. This scenario is simulating the packet re-transmission in multicast and broadcast applications, where different receiver nodes fail to receive a different packet for the same application.

In WiMAX and LTE networks the traffic flow for unicast communications is specific to a particular connection/bearer. Hence, intra-flow network coding is possible at intermediate nodes for unicast communications in 4G networks. The possible threats in intra-flow network coding are forwarding node selection with rate assignment, pollution attacks and entropy attacks in data forwarding and acknowledgement delivery. The pollution attacks can be launched by injecting polluted information or modifying messages, and entropy attacks can be regarded as a special replay attack. These two attacks are more vulnerable in network coding techniques. On the other hand, encoding for inter-flow network coding in 4G wireless networks is possible only at the BS/eNB. Therefore, the encoded packets can be encrypted with Group Traffic Encryption Key (GTEK).

5.2.2. Security Threats in WiMAX Networks

The major security threats in mobile and multihop WiMAX networks are:

- Latency and re-authentication issues during handovers
- Downgrade attack
- Hop-by-hop authentication issues in a multihop network
- Tunnel mode data forwarding issues in a multihop network

Latency and re-authentication issues during handovers: When a handover occurs, the MS is re-authenticated and authorized by the target BS/RS. These re-authentication and key exchange procedure increase the handover time that affects the delay sensitive applications. In the handover response message, serving BS/RS informs the MS, whether or not the MS needs to do re-authentication with the target BS/RS. If the MS is pre-authenticated by the target BS/RS before handover, then there is no need of device re-authentication, but user authorization is still necessary.

Downgrade attack: This attack may happen if the intruder modifies the security level to low in MS basic capability message. Consequently, the BS/RS uses a low level security algorithm for that MS and the attacker may easily hack the system.

Hop-by-hop authentication and tunnel mode forwarding issue: In a multihop wireless network, the intermediate nodes between the sender and the receiver should be legitimate users, otherwise the intruder may hack the system and the whole system is

vulnerable. This issue can be solved when all the nodes between the sender and the receiver establish the hop-by-hop authentication. The distributed security mode in multihop WiMAX enables the hop-by-hop authentication. Conversely, data forwarding using tunnel mode in distributed security architecture is a hidden problem since there is no SA between multihop access RS and the BS. Network coding issues in multihop wireless network are described separately.

5.2.3. Security Threats in LTE Networks

Similar to the WiMAX network, some security threats exist in LTE networks only. For multihop LTE networks, the standards address the possible security threats, when finalizing the multihop standards. However, a few major security threats still exist in LTE networks, they are:

- Disclosure of User's Identity privacy
- Location tracking
- Rogue RN attack

Disclosure of User's Identity privacy: During Initial Attach, SN requests the UE to send IMSI in plain text, thus the attacker gets the private information (IMSI) of the user, later that may be used to hack the UE [99].

Location tracking: CRNTI is a unique temporary identifier at the cell level. The passive attacker can determine the location of UE by sniffing CRNTI information, because CRNTI is transmitted in a clear text. During handover, a new CRNTI is assigned in a handover command message. As a result, the attacker can easily find the location of the UE. Similarly, it is possible to map the old and new CRNTI during handover by mapping of continuous user plane or data plane packets before and after handover [113].

Rouge relay node attack: An introduction of a rogue RN may insert the traffic into the network. Before the actual RN authentication has taken place the network cannot distinguish between a RN and a rogue RN. Hence, the attacker injects a packet in to the network. However, the LTE multihop security avoids the injecting of traffic, but rogue RN eavesdrop IMSI information from Attach Request message [102].

5.3 Proposed Distributed Security Architecture

In many practical implementations, it has been proven that ECDH can establish a shared secret over an insecure channel at highest security strength [95, 96]. Based on this, the proposed architecture considers ECDH as part of layer-2 in every node. Using EDCH protocol, MS/RS establishes the secured tunnel with BS in the ranging process. Similarly in LTE, the UE/RN establishes a secured channel with eNB/DeNB. The two main tasks of the proposed solution are: (1) initial ranging (random access for LTE) using ECDH; and (2) neighbour authentications using ECDH. The following passage describes the tasks in more detail.

5.3.1. Secured, Initial Ranging in WiMAX / Random Access procedure in LTE

The secured Initial Ranging (for a WiMAX network) or Random Access Procedure (for an LTE network) for the 1st hop and the nth hop node is shown in Figure 5.2.

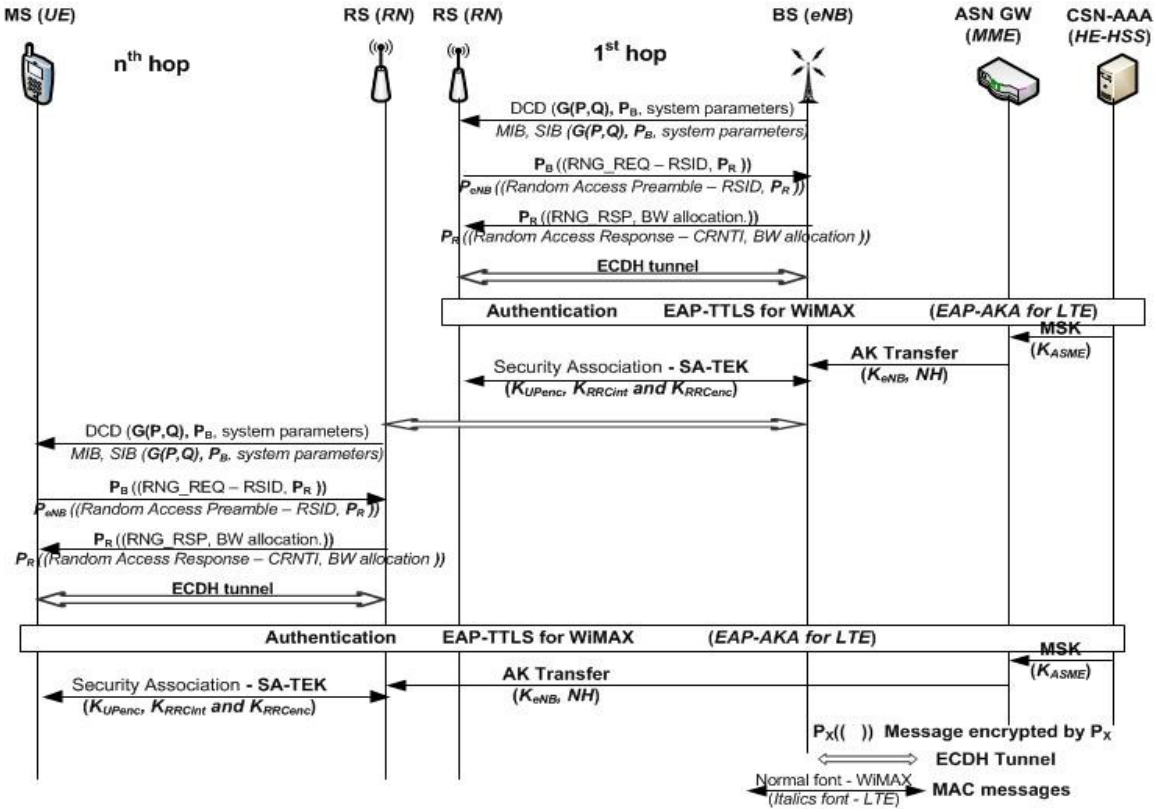


Figure 5.2 Initial ranging and connectivity using ECDH protocol

Table 5.1 Symbols and parameters used in Messages for Secured Initial Ranging

Symbols and Parameters	Description
DCD	Downlink Channel Descriptor message for broadcasting system parameters
G(P, Q)	Global parameters for Diffie-Hellman protocol
P_B	Public key for the BS
MIB and SIB	Message and System Information Block
P_B((RNG_REQ))	Ranging request message is encrypted using P_B
RSID, MSID	Relay, Mobile Station Identifier
P_R	Public key for the RS/RN
P_{eNB}((Randon Access))	Random Access Preamble is encrypted using P_{eNB}
P_R((RNG_RSP))	Ranging response message is encrypted using P_R
MSK, AK, SA-TEK	Security keys in WiMAX for establishing the SA
K_{ASME}, K_{eNB}, K_{UPenc}, K_{RRCint} and K_{RRCenc}	Security keys in LTE for establishing SA

In secured initial ranging and connectivity at the 1st hop, the BS/eNB broadcasts the physical layer and system parameters, including ECDH global parameters. The symbols and parameters description is given in Table 5.1. In first step, the public key of the BS/eNB is added in the DCD message in case of WiMAX, MIBs and SIBs in case of LTE. Consider the initial ranging process, any WiMAX node (MS/RS) wanting to connect with the BS first generates public and private key pairs, and then sends the public key to the BS, along with the initial ranging code in the RNG_REQ message. Hence, RNG_REQ message is encrypted using the BS public key. In turn, the BS will send a RSG_RSP message, which is encrypted with the MS/RS public key. Thus, MS/RS establish a secure tunnel with the BS during the initial ranging process itself and the subsequent MAC messages are encrypted using the ECDH public key of the receiver. The remaining steps follow the standard, like the initial device/user authentication was done by the AAA server.

Similarly, any LTE node (UEs/RNs) wanting to connect with the eNB first generates public and private key pairs, and then send the public key to the eNB in a Random Access preamble message which is encrypted using the eNB's public key. The

eNB's Random Access Response message is encrypted by the UE/RN public key. The subsequent Attach Request and other communication is encrypted using the receiver's public key.

In this secured Initial Ranging process, the only additional bandwidth overhead is the exchange of global parameters and public keys, e.g., in WiMAX, the global parameter G(P, Q), and the BS's public key P_B in the DCD message, and then the RS's public key P_R in the RNG-REG message, which are highlighted in the first three messages as depicted in Figure 5.2. The information in the subsequent messages follow the standard, i.e. WiMAX messages are presented in regular font and LTE messages are presented in italic font in Figure 5.2. The computational overhead is added for BS and RS to encrypt the MAC messages using the receiver's public key until the SA is established. In total, the additional overhead for the proposed scheme is only slightly higher compared to the original initial ranging and connectivity tasks.

5.3.2. Distributed Security using ECDH in Multihop WiMAX

To establish hop-by-hop authentication and to reduce the computation overhead of the centralized node, distributed security architecture is necessary for multihop networks. In a multihop LTE network, the security architecture defined by the 3GPP standard is distributed security. On the other hand, selection of the distributed security mode in WiMAX is optional, but usage of the tunnel mode for data transfer is an open issue. Hence, the distributed security architecture using ECDH protocol is proposed for multihop WiMAX networks. For multihop (n^{th} hop) connectivity using ECDH (as shown on the left of Figure 5.2), the cell edge RS broadcasts its public key, ECDH global parameters, RS-ID and system parameters in the DCD broadcast message. The MS/RS wishing to join with access RS, starts the ranging and connectivity procedure. Here, the access RS acts as a BS for the new user. After the initial device/user authentication (done by the AAA server), the MS/RS establishes a SA with the connected RS (superordinate/Access RS). If the new connected node is an RS, then the superordinate RS will share the public key of BS and the corresponding global parameters. The new RS will associate with the BS by sending its public key to the BS. Any RS that is more than one hop away from BS is connected to the

superordinate RS and associated with BS. Hence, the RS that is more than one hop away can send its traffic over the tunnel mode by encrypting the traffic (payload) with BS public key. The intermediate RSs cannot decrypt/encrypt the traffic.

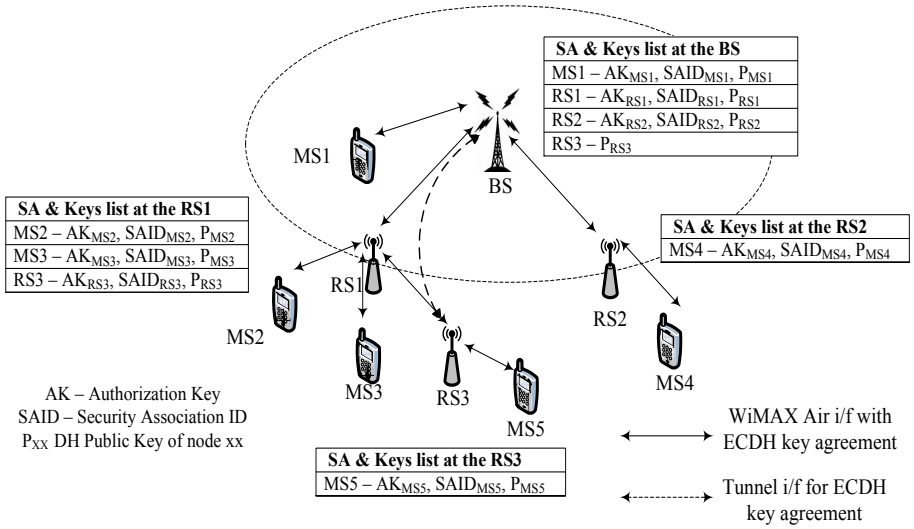


Figure 5.3 Distributed security architecture in WiMAX using ECDH

Figure 5.3 shows the SA and key management in proposed security architecture. Management of AK, SAID and ECDH public keys are distributed at BS and RSs. For multihop (n^{th} hop) users, the access RS maintains the encryption and SA keys as similar to BS, where BS maintains the SA keys for the connected nodes and ECDH public key of all RSs. In Figure 5.3, the BS maintains the SA and encryption keys of MS1, RS1 and RS2 as well as ECDH public key of RS3. The RS1 maintains the SA and encryption keys of MS2, MS3 and RS3. RS2 and RS3 maintain the encryption keys of MS4 and MS5, respectively. Suppose MS5 wants to send encrypted data in a tunnel mode, first it encrypts the traffic using SA-TEK associated with the RS3. Now, RS3 decrypts the traffic using SA-TEK, and then encrypts the data using BS's public key. Therefore, the intermediate RS1 cannot decrypt/encrypt the traffic. This architecture is useful for supporting tunnel mode operation.

5.3.3. Neighbour Authentication and SA

Neighbour authentication and SA in multihop WiMAX/LTE networks eliminates network coding security threats and secured pre-authentication for fast handover. Consider

the WiMAX network, if any new RS is connected with the network, the BS will inform the updated members list to the existing RSs group in a regular DCD message. Now, if the new RS finds another RS during channel scanning, it verifies, whether the RS is genuine or not by verifying RS-ID. Then it will associate the neighbour RS by sending its public key and the RS-ID. The neighbour RS also sends its public key in the response. At the end of association both RSs generate the uplink and downlink CMAC digital signatures from AK and exchange between them.

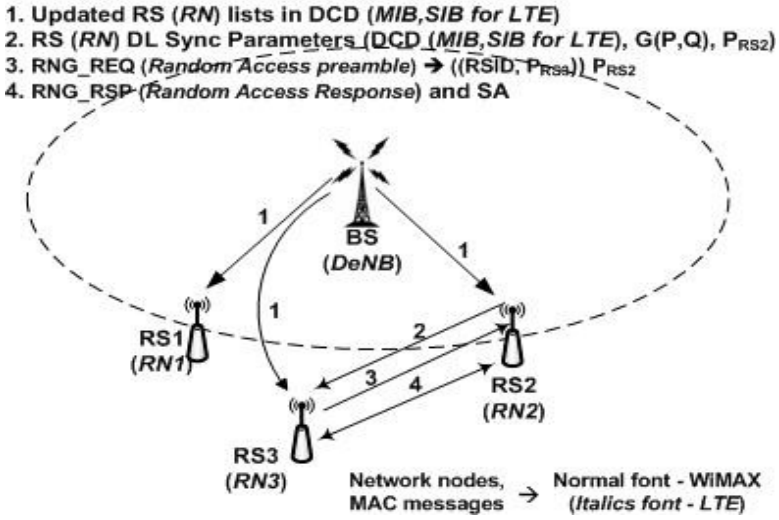


Figure 5.4 Neighbour authentication using ECDH protocol

Figure 5.4 shows the neighbour authentication process. In step 1, the RS3 receives the updated RSs list after the ECDH agreement with the BS. During the scanning process, it may find the DCD and other downlink parameters of RS2 as shown in step 2. Since the RS3 knows that RS2 is a legitimate node based on the list that it received from the BS, it establishes the ECDH agreement with the RS2. After the ECDH key agreement, both RS2 and RS3 share their digital signatures as shown in step 3 and step 4. For LTE networks, multihop UE/RN connectivity and SA with neighbour RS is similar to WiMAX networks where the message sequences from step 1 to step 4 are in a closed bracket with italic font.

In this proposed neighbour authentication, the additional bandwidth overhead is the exchange of global parameters and public keys with neighbour nodes using ranging messages. The only computational overhead is to encrypt the pre-authentication message during a handover. The total overhead is small compared to the WiMAX/LTE standards.

5.4 Performance Evaluation of Conventional and the Proposed Security Schemes in WiMAX

Measuring and analyzing both security level and QoS performance is mandatory for the existing and the proposed security schemes in 4G wireless networks, as they intend to provide high QoS and security for customers. For the performance evaluation, default security, IPSec and the proposed ECDH scheme with default security are compared. Conceptually, Layer 2 and Layer 3 security schemes may not be a good comparison. However, though IPSec is a Layer 3 security technology, it is considered for the performance evaluation because ISPs and device vendors are interested in IPSec due to its popularity in wired networks. In this section, first the performance of IPSec security for WiMAX networks is compared with a default security scheme using testbed implementation. Then, connectivity latency performance of the proposed ECDH security scheme is measured using NS2 simulation. Finally, security and QoS performance of the proposed ECDH security was analyzed for both WiMAX and LTE network.

5.4.1. Performance of IPsec and Basic Security using Testbed Study

The WiMAX testbed experiments consist of one IEEE 802.16d based EION's Libra MAX BS Out-Door Unit (ODU), one In-Door Unit (IDU) and two Libra MAX SSs, where the BS-ODU and SSs are wireless devices and the BS-IDU acts as gateway for the BS-ODU unit. The NCMS and AAA severs are running on the BS-IDU unit. The performance analysis tool used for the testbed is IXIA. The BS and SSs connectivity setup is shown in Figure 5.5 and the system parameters are given in Table 5.1.

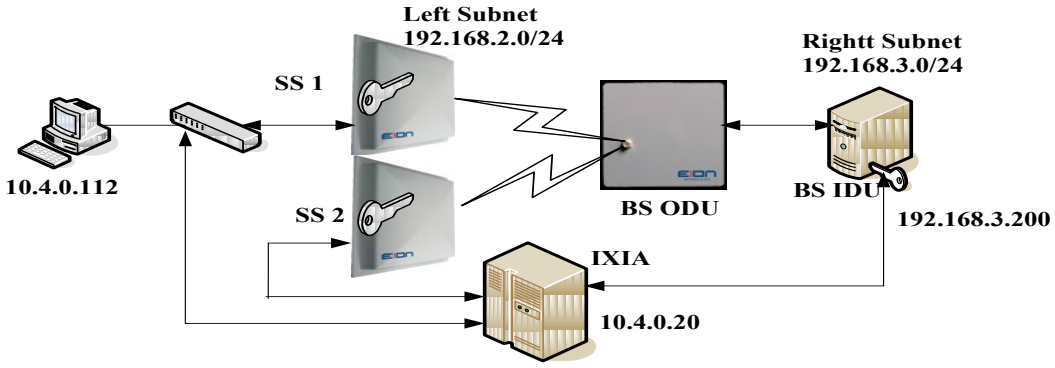


Figure 5.5 IPSec testbed setup – connection diagram

Table 5.2 Testbed - System Parameters

Parameter	Value
Components	LibraMAX BS-ODU, BS-IDU and SSs
Compliance	IEEE 802.16d
Frequency Specifications	3.5Ghz operating freq. 7Mhz BW
Performance Analyzer	IXIA
IXIA Frame specification	1500 bytes Pkt. Size, TCP packet
IPSec	Openswan ver. 2.6 in BS-IDU, 2.4 in SSs

In Figure 5.5, the network, 192.168.2.xxx which is on the left side of the IPSec tunnel is the Left Subnet, and right side is the Right subnet. Both SS1 and SS2 are at the left side of the IPSec tunnel interfaces, whereas BS IDU is on the Right subnet. For configuration and management purposes, one of the SSs (SS1 in Figure 5.5) is connected to the PC through the switch. The IPSec configuration and the status are verified in that PC that are shown in Table 5.2. Ethernet cables are used to connect the devices other than wireless interface. Wireless connectivity is established by wireless RF cables with 60dB attenuators instead of a wireless medium. The provisioning of wireless link capacity is configured in AAA server. The BS and SSs are operating in a static routing mode.

Table 5.3 IPSec Configuration and Status Verification

IPSec.conf file in SS	IPSec.conf file in BS-IDU
Inter faces="ipsec0=ofdm" left=192.168.2.214 leftsubnet= 192.168.2.0/24 right=192.168.3.200 Rightsubnet= 192.168.3.0/24	interfaces="ipsec0=eth0" left=192.168.2.214 leftsubnet= 192.168.2.0/24 right=192.168.3.200 Rightsubnet= 192.168.3.0/24
IPSec handshake messages - Console (serial port) output at SS 1	
pluto[874]: "my_conn" #1: STATE_MAIN_I3: sent MI3, expecting MR3 108 "my_conn" #1: STATE_MAIN_I3: sent MI3, expecting MR3 pluto[874]: "my_conn" #1: Main mode peer ID is ID_IPV4_ADDR: '192.168.2.214' pluto[874]: "my_conn" #1: transition from state STATE_MAIN_I3 to state STATE_MAIN_I4 pluto[874]: "my_conn" #1: **STATE_MAIN_I4: ISAKMP SA established { auth=OAKLEY_PRESHARED_KEY cipher=oakley_3des_cbc_192 prf=oakley_md5 group=modp15 36**}	
IPSec connection - status verification (command execution)	
/sub/lm_scripts # ipsec eroute 0 192.168.2.0/24 -> 192.168.3.0/24 => tun0x1002@192.168.2.214	

For mobile networks, MS connectivity latency is one of the main QoS requirements. When handover occurs, the MS needs to be re-authenticated and authorized

for existing service flows that may affect the QoE of an application. Table 5.3 shows the SS connectivity time for default MAC layer security and IPSec. From the results, it is evident that the SS connectivity latency is higher (~67% for SS1 and 100% for SS2) for IPSec, as it consumes significantly more time for IPSec connection. For mobile WiMAX networks, IPSec tunnel has to be broken with current BS and re-established with target BS during handover. Therefore, the IPSec solution is not suitable for mobile networks.

Table 5.4 SS Connectivity Time in Testbed Study

Security scheme	Connection latency
WiMAX MAC security	SS1 = 6 Sec and SS2 = 6 Sec
Both MAC layer and IPSec security	SS1 = 10 Sec and SS2 = 12 Sec

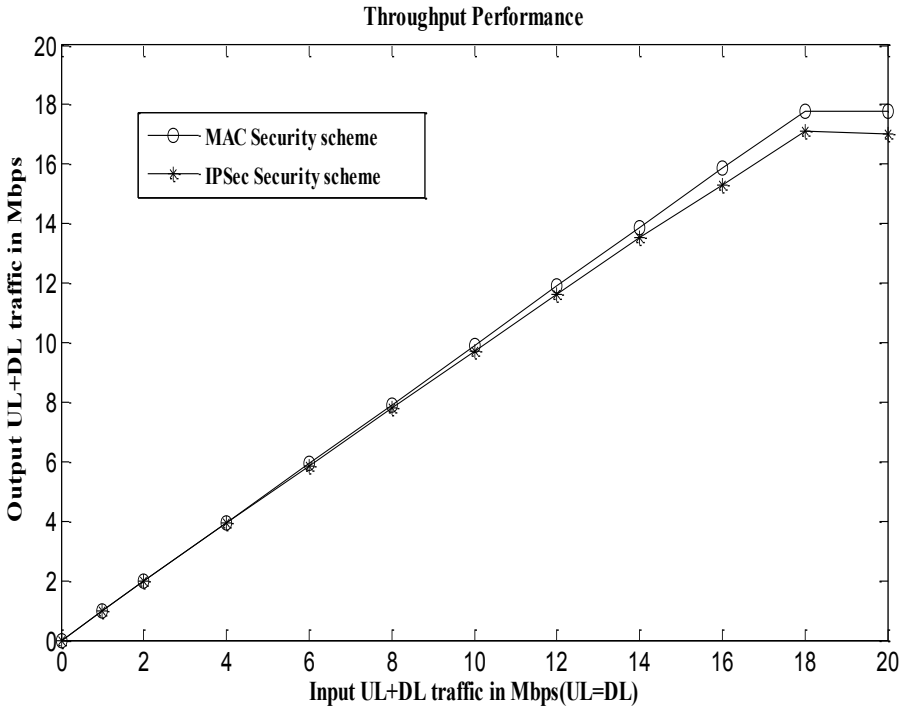


Figure 5.6 Testbed measurements – Throughput performance

Figure 5.6 shows the throughput (in Mbps) of the system for both security schemes. The uplink and downlink provisioning for both SSs in a AAA server is varied from 0 to

20Mbps (~ the theoretical limit for 7 Mhz bandwidth). For 20Mbps provisioning, 5Mbps uplink and 5Mbps downlink are configured for both the SSs. Using IXIA, traffic is transmitted for the total provisioned wireless capacity, and the receiving traffic is also noted. From the results, it is clear that the E2E throughput of IPSec security scheme is less than that of the MAC layer security scheme for the same capacity. The difference in throughput performance is due to additional overhead of 40 bytes IPSec header for each frame. Since the system capacity (BS) is close to 19Mbps, E2E throughput will not increase beyond ~18.5Mbps.

Figure 5.7 shows the E2E frame loss performance with respect to the total link capacities of the two SSs. The frame losses in the IPSec scheme increase as the link capacity increases. For the standard MAC layer security scheme, there are small drops in frames due to the 10-byte MAC layer overhead. On the other hand, the IPSec security scheme has much higher packet losses (> 3 times of the MAC layer security scheme). Since 40-byte IPSec header is added to each frame at BS-IDU for downlink traffic and at the SS for uplink traffic before entering into the IPSec tunnel. This 40-byte overhead in the IPSec tunnel and 10byte MAC layer overhead increases the frame losses for the IPSec security scheme. The packet drop increases in both schemes when the input traffic exceeds the practical system capacity of ~18.5Mbps.

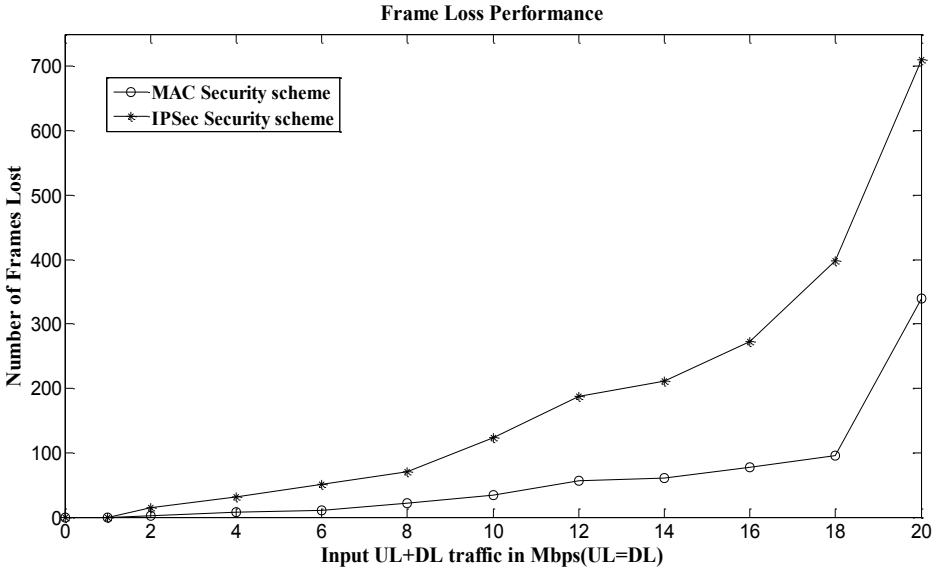


Figure 5.7 Testbed measurements – Frame loss performance

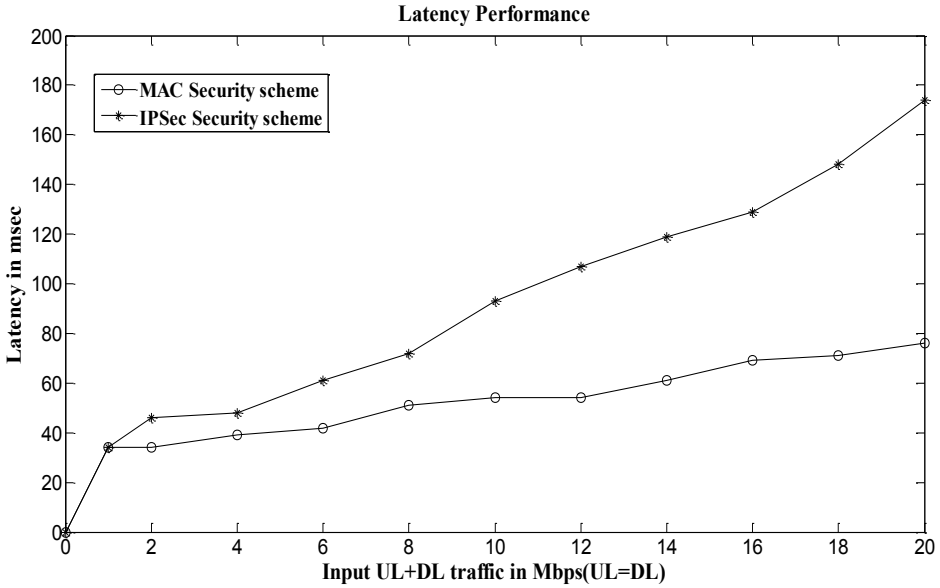


Figure 5.8 Testbed measurements – Latency performance

The average delay/latency experienced by the traffic for different link capacity is shown in Figure 5.8. Delay experienced in the IPSec security scheme is much higher (~100% for > 10Mbps) than the default MAC layer security scheme. This increase in delay is due to the processing time for IPSec encryption and additional queuing delay at SSs and BS. Even though, the wireless link capacity is the same, additional overhead in layer-3 and layer-2 headers increases the payload size before entering into the wireless interfaces. For 20Mbps traffic, the average delay experienced by the IPSec scheme is very high.

From the testbed results for using IPSec the following points are observed:

- IPSec security is established only after the MAC layer connectivity. Hence, the major security threats during initial connectivity still exist.
- Internet Security Association Key Management Protocol (ISAKMP) is used to establish a secured tunnel in IPSec that requires long time. As a result, the initial and handover latency is highly increased.
- Moreover, IPSec only encrypts and encapsulates the Layer 3 payload, i.e., IPSec does not provide security at Layer 2 and there is no protection for control messages for the MAC layer.

- IPSec introduce 40Bytes overhead for the header for each packet that leads to reduction in QoS performance.
- If the number of nodes is increased in a network, the average initial connectivity is highly increased. Therefore, IPSec is not scalable for wireless networks.

5.4.2. Performance Evaluation of ECDH Scheme using Simulation

Earlier, the performance of IPSec security is compared with default WiMAX security. In that, the Layer-3 IPSec is cross-compiled and running as a module in the WiMAX target board. Consequently, the IPSec tunnel is established between SS and BS-IDU, only after the IP connectivity. On the other hand, the requirement for ECDH implementation is at Layer-2. Since the lower MAC and security functions are embedded on the chips, it is not possible to test ECDH using testbed. Therefore, the simulation environment is selected for ECDH performance evaluation. The simulation environment has the following assumptions:

- The main aim of an ECDH implementation is to protect the MAC messages, which are in plain text.
- The WiMAX and LTE standard provide a secure environment for data transfer, once SA is established with the BS.
- In many practical implementations, it has been proven that ECDH can establish a shared secret over an insecure channel at the highest security strength [29] [30]. Hence, the intention for this simulation is to find the QoS performance, not for measuring the ECDH security strength.
- Once the SA is established, the network adopts the default security (compliance to standard). Therefore, the security level and the QoS performance such as, latency for traffic, throughput and frame loss are the same.

Based on the above assumptions, the main aim of this simulation is only to find the MS initial connectivity latency, because the security level and the remaining QoS performance is same as the default security scheme. However, the available WiMAX

patches for NS2 simulators and other simulators, such as OPNET, etc., do not have the WiMAX security functions. Hence, the DH algorithm is integrated with NS2 (multihop relay, National Institute of Standards and Technology) for generating a shared secret. Then, MAC messages are encrypted using the public key of the receiver. The WiMAX system parameters and DH parameters used for this simulation are given in Table 5.4.

Table 5.5 System Parameters for Simulation Study

Parameter	**Value**
Physical Layer	Wireless MAN OFDMA, TDD
Network elements	One BS, one RS and two MS
No of OFDM symbols and subchannels (DL)	24, 35
System Bandwidth	20MHz
Frame duration	5msec
D-H parameters (Prime P and generator G)	P=997, G=8
Private keys configured	BS=853,RS=854, MS1=855, MS2=856

Computation:

DH Public key $A=G^a \bmod P$; where a=private key

Public keys of network nodes BS=155, RS=243, MS1=947, MS2=597

Shared secrets between A and B = $B^a \bmod P = A^b \bmod P$; where 'A' and 'a' are public and private keys of A

Shared secrets between BS and RS = 810; RS and MS1 = 609; RS and MS2 = 431

Simulation result:

Table 5.6 Initial Connectivity Latency in Simulation Study

Simulation scenario	**Connection latency**
Without ECDH	MS1 = 67.3msec and MS2 = 68.01msec
With ECDH implementation	MS1 = 67.6msec and MS2 = 68.01msec

From the simulation results, it is clear that both MS1 and MS2 are connected at the same frame period (14^{th} frame) for both scenarios. The time needed to compute the key values and share the secret is less than one frame period (5msec). Hence, it is possible to schedule the subsequent MAC messages for both scenarios to be the same. On the other hand, handover latency is not measured, because the simulator does not support the CN functionalities. However, the handover process does not require authentication steps and it only requires key renewal for the user that reduces the handover latency.

5.4.3. Security Analysis

There are three security schemes considered for this analysis: default MAC layer security defined by WiMAX/ LTE the standards; IPSec security on top of MAC layer security; and the proposed ECDH protocol at the MAC layer with default security.

5.4.3.1. Analysis on ECDH Protocol against Security Threats in WiMAX

1 *DoS/Replay attack during Initial Ranging*: In our proposed security architecture, RNG_REQ and RNG_RSP messages are encrypted by the public key of the receiver. As a result, the intermediate rogue node could not process the message in a short period and the system is free from DoS/Replay attack during initial ranging.

2 *Latency issue during handover*: For latency issue during handover, two scenarios are considered: (i) RS mobility (e.g., RS is installed on the top of a train and WiMAX users are inside the train); (ii) MS mobility. For RS mobility in the proposed security architecture, re-authentication for RS is not necessary because the BS or target RS know the list of RSs and the corresponding RS_ID in the network. Otherwise, if the target node is another BS, serving the BS can send the RS authentication information, including AK, in a secured manner as defined in IEEE 802.16m. As a result, only the key renewal is needed to refresh the SA that reduces latency during RS handover. For MS mobility, when the MS moves within the network, MS authentication information including AK is transferred to the BS or target RS using the ECDH tunnel. Otherwise, if the target node is another BS, serving BS can send the RS authentication information, in a secured manner as defined in IEEE 802.16m.

3 *Downgrade attack and bandwidth spoofing:* For downgrade attack, if the level of security is low in the MS basic capability request message, the BS should ignore the message. For bandwidth spoofing, the BS should allocate the bandwidth only based on the provisioning of the MS. This downgrade attack and bandwidth spoofing can be solved by using the basic intelligence in the BS.

4 *Hop-by-hop Authentication for rogue RS*: One of the major issues in multihop wireless networks is the introduction of a rogue node in a multihop path. In our distributed security mode, once the joining node is authenticated by the home network (AAA server), mutual authentication takes place between the joining node and the access node (RS or BS). Also, the MAC messages before authentication are encrypted by ECDH and the authentication request message is encrypted by EAP-TTLS protocol (i.e. the home network's shared secret). Hence, the new node identifies the rogue node during the mutual authentication step and no other credential information is shared. Thus, the proposed solution avoids the introduction of the rogue node problem.

5 *Tunnel Mode Support*: In a multihop scenario, if the intermediate nodes decrypt and then encrypt the payload before forwarding, it leads to an additional overhead. On the other hand, if the tunnel mode is used, then BS should know the key for decrypting the traffic. In our approach, the BS public key is known to all RSs and the BS also knows the public key of all RSs. Therefore, the network supports tunnel mode operation using the ECDH tunnel.

5.4.3.2. Analysis on ECDH Protocol against Security Threats in LTE Networks

1. *DoS and Replay attacks*: As similar to the WiMAX network, the intruder introduces DoS/Replay attack during Random Access procedure, as the messages are in a plain text. In our proposed security architecture, Random Access Request was encrypted by the public key of eNB and the response is encrypted by the public key of UE. As a result, the Random Access procedure messages are encrypted and the DoS/Replay attack is avoided.

2. *Disclosure of User's Identity privacy*: In the Attach Request message, the UE sends the IMSI information to eNB in a plain text. This leads to disclosure of the user's identity and the attacker may introduce bandwidth stealing and other attacks later. In our proposed architecture, the Attach Request message is encrypted by eNB's public key. As a result, it is difficult for the attacker to decrypt the Attach Request message to know the IMSI. Thus, disclosure of the user's identity is avoided.
3. *Bandwidth stealing*: The attacker eavesdrops the CRNTI information in Random Access Response or handover command message. Later, using CRNTI, the attacker sends a fake bandwidth request or false buffer status to allocate the bandwidth unnecessarily. In ECDH implementation, eNB encrypts the Random Access Response message using the UE's public key. Therefore, bandwidth stealing attack is avoided.
4. *Location tracking*: Similar to the bandwidth stealing attack, location tracking is possible using CRNTI information, before and after handovers. This attack is avoided, because the CRNTI information is encrypted.
5. *Rogue relay node attack*: The default multihop LTE security suggests mutual authentication between RN and DeNB. However, the rogue RN may broadcast system information to receive an Attach Request from the UE's to eavesdrop IMSI information. However, UE identifies the rogue RN during mutual authentication, but IMSI information is disclosed. For this attack, EAP based authentication is recommended as similar to WiMAX, where the Attach Request is encrypted by home network shared secrets or by enterprise credentials.

5.4.3.3. Analysis on ECDH Protocol against Pollution and Entropy Attacks

Pollution and entropy attacks are the major security threats in multihop wireless networks when network coding is used for data transmission. Since packets are unencrypted, attackers may introduce the polluted or stale packets (pollution and entropy attacks). In our approach, every RS authenticates the neighbour RSs and shares the digital signatures information. Hence, the attackers cannot introduce the pollution attacks. For the

entropy attack, the RS may introduce a time stamp field in the message header. Subsequently, the RS can verify the time stamp of a received (stale) packet with the older packets. If the time stamp is older, the RS may drop the packet to avoid the entropy attacks.

5.4.3.4. Comparison of Different Security Schemes

Finally, the QoS and security performance of the existing and the proposed security scheme is compared. The comparison is given in Table 5.6.

Table 5.7 Performance Analysis of Different Security Schemes in WiMAX and LTE

Criterion	**Security compliance to standards (default)**	**IPSec on the top of default security**	**ECDH at MAC layer with default security**
System overhead	Default security architecture as defined in standards	High overhead, because Layer 3 IPSec tunnel is established only after a few handshake messages and IPSec needs 40 bytes header for each PDU additionally	Slightly increased than the default scheme: Bandwidth overhead is to exchange public key and global parameters. Computational overhead is to encrypt MAC messages. Also, neighbor authentication requires the similar overhead.
Security for data	High	Very high. As IPSec tunnels are difficult to break, provides strong security	High
Security for MAC control messages	Some MAC control messages are unprotected. It leads to some major security threats which are defined in Section IV	Also suffers the same security threats defined in Section IV	It eliminates all security threats against MAC messages, except disclosure of IMSI due to rouge RN in LTE
Initial connectivity and handover latency	Both initial and handover latency time are same in WiMAX,	Both initial and handover latency are high. For mobility	Initial latency is same as default, where handover latency is

	where handover latency in LTE is less (Authentication is not required)	support, IPSec is combined with mobile IP and requires some modifications [123]	lower than IPSec in LTE and lower than both IPSec and default in WiMAX
In WiMAX, tunnel mode forwarding & hop-by-hop authentication	Hop-by-hop authentication exists only when distributed security mode is selected but tunnel mode issue is open	Hop-by-hop authentication exists only when distributed security mode is selected and tunnel mode is possible using IPSec tunnels	It provides hop-by-hop authentication and supports tunnel mode forwarding
Threats in LTE system architecture, lack of backward secrecy, rogue RN, synchronization attack and, disclosure of IMSI due to rouge RN	Exits	Exits	Exits
QoS performance (LTE, WiMAX)	Throughput and latency are close to theoretical. Minimum frame losses	Throughput is slightly reduced. Latency and frame losses are high	Same as default security scheme

5.5 Chapter Summary

The 4G wireless networks, WiMAX and LTE are intended to provide high QoS and security for their customers. Even though WiMAX and LTE have strong security architectures, some major security threats, like DoS/Replay attack exist in a network. Most of the security threats in LTE and WiMAX networks are due to unprotected MAC messages, that is, the information are in a plain text. Hence, the distributed security architecture using ECDH implementation in layer 2 is proposed for 4G multihop wireless networks. In the proposed scheme, the wireless nodes (MS/RS in WiMAX, or UE/RN in LTE) are initially authenticated by the home network and then authorized with the access node (RS/BS in WiMAX, or RN/eNB in LTE). The proposed scheme overcomes most of

the existing security threats, including pollution and entropy attacks due to network coding. However, disclosure of IMSI due to rogue RN in LTE still exists. For that issue, enterprise authentication, such as EAP-TTLS for LTE network is recommended.

On the other hand, ISPs are interested in IPSec security due to its popularity in wired networks. Usually, IPSec consumes additional bandwidth (for header) that may affect the QoS performance. Hence, the performance of IPSec and the default MAC layer security is measured and analyzed using a testbed implementation. Then, initial connectivity latency of the proposed ECDH scheme is measured using simulation. The QoS performance of the ECDH scheme is the same as the default security, because the proposed scheme is used only for encrypting certain MAC messages, before establishing the SA. From the measurement results and ECDH analysis, it is clear that the IPSec scheme provides strong security for data, but the QoS performance is highly affected due to overhead. However, no articles have reported actual experiments on, or real measurements of, the overhead of IPSec. Also, the major security threats due to unprotected MAC messages exit in IPSec. Conversely, ECDH protocol eliminates most of the MAC layer security threats in the network and has the same QoS performance as the default MAC layer security in 4G wireless networks. Thus, this thesis strongly suggests ECDH protocol for 4G wireless networks.

Chapter 6. Protection Schemes for 4G Multihop Wireless Networks

In general, node protection in a communication network guarantees the traffic flow from source to destination. Traditional protection schemes in wired networks introduce either resource-hungry solutions, such as the (1+1) protection scheme, or a delay and interrupt to the network operation as in the (1:N) protection scheme. Node protection using network coding could solve the above issues [106]. However, the existing research efforts are mostly concentrated on wired networks, and not much research has been conducted on wireless multihop or mesh networks. This chapter describes the relay node protection using network coding for 4G multihop wireless networks and analyzes the QoS performance with the proposed scheme. The QoS performance, such as PDR, latency and jitter, are measured for different scenarios. The scenarios for 4G wireless networks include failure of a single and two relay nodes, with and without the protection scheme, and user's mobility.

6.1 Problem Statement

The data transmission using RSs extends the coverage region and capacity in 4G multihop wireless networks. However, the wireless communication medium is prone to various types of interferences and the user's mobility that causes a wireless link status to dynamically change according to the channel conditions. Sometime the channel may go down for a considerable amount of time. In addition to that, the RSs may fail sometimes unexpectedly or for management purposes, like software upgrade, etc. Relay node failures in multihop networks cause the QoS degradation for certain users and for the system too. Therefore, it is necessary to implement the relay node protection to maintain the QoS of the network.

In traditional (1:1) node protection, transmissions on the backup path only take place in case of a failure and in the (1+1) protection the traffic is simultaneously transmitted on two link disjoint paths. Implementing the traditional (1+1) protection scheme increases the capital cost, and resources cannot be fully utilized. On the other hand,

the design and implementation of the (1:N) protection scheme in wireless networks is more challenging for the system design and is difficult as well. On the other hand, the network coding is introduced in wireless networks for traffic redundancy for the replacement of HARQ techniques. Now, the network coding is extended for the protection of wireless relay nodes. In multihop wireless networks, very few research efforts are concentrated on node protection schemes using network coding. However, no reports have been published on network protection for 4G wireless networks using network coding and the QoS performance analysis.

6.2 Relay Node Protection Using Network Coding

Network coding has recently been introduced as a new transmission paradigm in wireless networks [97]. Initially network coding was introduced for wired networks. Even though network coding is ideally suited for wired networks, it has some limitations in traditional wireless cellular networks due to the centralized network architecture and the occurrence of interference in the transmission of network coded data. Therefore, the extension of network coding to wireless networks is not straightforward. However, the existing research efforts show that the network coding is well suited in 4G wireless networks for a few different applications [112 – 114]. Those applications are mainly focused on data reliability.

Initially, WiMAX and LTE standards use HARQ to transmit the data packets reliably. However, HARQ may underutilize the wireless medium in the cases of multipath and multihop transmissions. Hence, network coding is tested for various scenarios such as single-hop, handover and multihop, where network coding outperforms HARQ [114]. Later, network coding is studied for various applications such as video traffic, multicast, etc., for reliable transmission in WiMAX and LTE networks [112, 113]. Similarly, the recent research efforts are concentrating on node protection using network coding [106-111] on WSN and WMN. However, the QoS performance of network coding for node protection has not been tested until now. Therefore, the QoS performance of node protection using network

coding is studied for WMNs and then extended for multihop WiMAX networks. For multihop LTE networks, similar performance could be achieved.

The multihop WiMAX/LTE network architecture is shown in Figure 6.1 (for simplicity, only two-hops are considered). The network elements in WiMAX networks include the BS, RS and MS, whereas the network elements in LTE consist of eNB, Relay Node and UE. The relays, RS1 and RS2, are used to extend the coverage region of the network. Hence, the cell edge mobile users are connected to the network through the relay RS1 or RS2. For the WMN, the BS in Figure 6.1 is replaced by the gateway node, the RS is replaced by a relay (r) and MS is replaced by the user's source node (S).

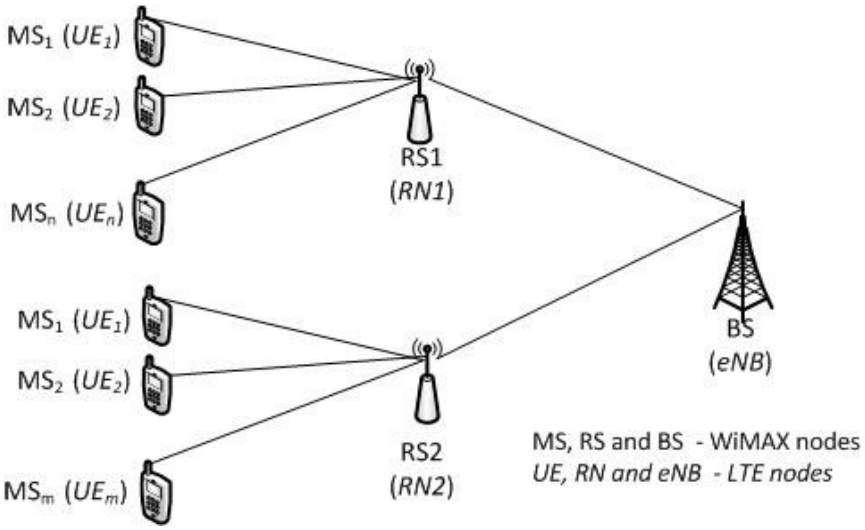


Figure 6.1 Multihop relay network architecture – WiMAX/LTE

To enable the protection for wireless relay nodes XOR network coding can be used, where XOR is simple to understand and for concept validation. The following passage describes the requirement for proper decoding of a network encoded packet.

In XOR network coding, when the source node transmits an encoded packet that consists of n embedded packets, p_1, p_2 ..., p_n, (i.e., $p_1 \oplus p_2 \ldots \oplus p_n$), the receiver will be able to correctly decode those n packets only if the receiver has at least $n - 1$ original packets.

In general, the node protection scheme demonstrates the following statement in the case of relay node failures [108]:

In a multihop relay network, if each of the n source nodes has m disjoint paths to the receiver node, then the receiver node can correctly retrieve the n independent messages from the sources if and only if the network has at most m-1 relay node failures.

Hence, the relay node protection using network coding should demonstrate the above statement. In 4G, the multihop network architecture is the similar for both WiMAX and LTE networks. However, in this work the QoS performance of the protection scheme is studied on multihop WiMAX networks because the available open source simulator for WiMAX supports the multihop functionality. The protection for a single and multiple relay nodes in multihop WiMAX networks is described in the following two subsections.

6.2.1. Protection for Single Relay Node Failure

For protection against single relay node failure for the network topology as shown in Figure 6.1, an extra RS is added to the network and all relay nodes should use network coding. This design emulates the 1:N relay node protection scheme for wireless networks.

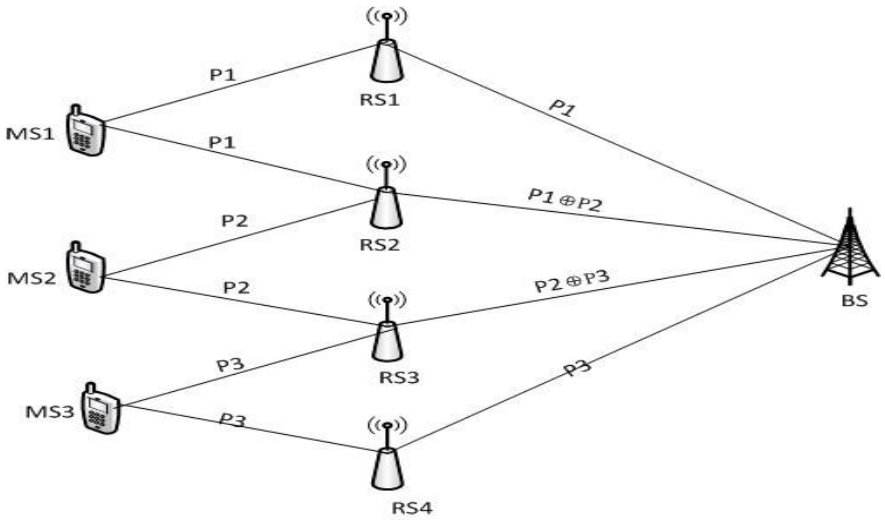


Figure 6.2 Network model - Protection for single relay node failure

The network topology considered for protection of a single RS failure is shown in Figure 6.2. The network consists of three cell edge users, namely MS1, MS2 and MS3, one

BS (eNB for LTE) and four forwarding relays, RS1, RS2, RS3 and RS4. For instance, without protection, the network requires, at most, three RSs, each connecting to a MS. With the protection, four RSs are used. Each relay node is capable of encoding the packets from different sources using the XOR network coding scheme. The receiver node, BS, is capable of decoding the XOR coded packets from different relays. However, to adapt to the protection in WiMAX networks, the network should use soft handover for the operations, because the MS needs to communicate with more than one BS/RS at the same time. The WiMAX standards support two types of soft handovers: Fast Base Station Switching (FBSS); and Macro Diversity Handover (MDHO). In both FBSS and MDHO, the diversity set is maintained by the BS, RS and MS. The diversity set is a list of the BS/RS that are involved in the handover procedure; it is provided for each MS during the initial stage. Hence, the MS communicates with all BSs and RSs in that diversity set. Assume the source nodes MS1, MS2 and MS3 start sending their information to the BS through intermediate relays. The diversity set maintained by MS1 is RS1 and RS2; MS2 is RS2 and RS3; MS3 is RS3 and RS4, respectively. Three relays are used to forward the traffic in the absence of a one RS failure.

From the statement for relay node protection, the receiver node BS can retrieve the information for a single relay failure if, and only if, the source node has a minimum of two edge-disjoint paths, e.g. m = 2. Since each source node is connected to two relays, they have two edge-disjoint paths to the BS. Relays RS1 and RS4 forward only the regular packets P1 and P3, respectively; but relays RS2 and RS3 forward network coded packets of P1⊕P2 and P2⊕P3, respectively. For the network topology illustrated in Figure 6.2, if RS1 fails, the BS first obtains P3 from RS4, and then the BS decodes P2 and P1 from RS3 and RS2, respectively. In other words, P2 and P1 are decoded from the coded packets P2⊕P3 and P1⊕P2. Similarly, the BS can retrieve the information for other single RS failure.

6.2.2. Protection for Two (multiple) Relay Nodes Failure

The network architecture for two relay failures scenario is shown in Figure 6.3. In this scenario, each MS has to maintain a set of three RSs in a diversity set. The diversity set maintained by MS1 is RS1, RS2 and RS3; MS2 is RS2, RS3 and RS4; and MS3 is RS3,

RS4 and RS5, respectively. Now, each source node has a minimum of three disjoint paths (i.e., m = 3) to the receiver BS. The relays RS1 and RS5 forward the original packets, P1 and P3, respectively. The remaining relays, RS2, RS3, and RS4, forward the network coded packets of P1⊕P2, P1⊕P2⊕P3 and P2⊕P3, respectively.

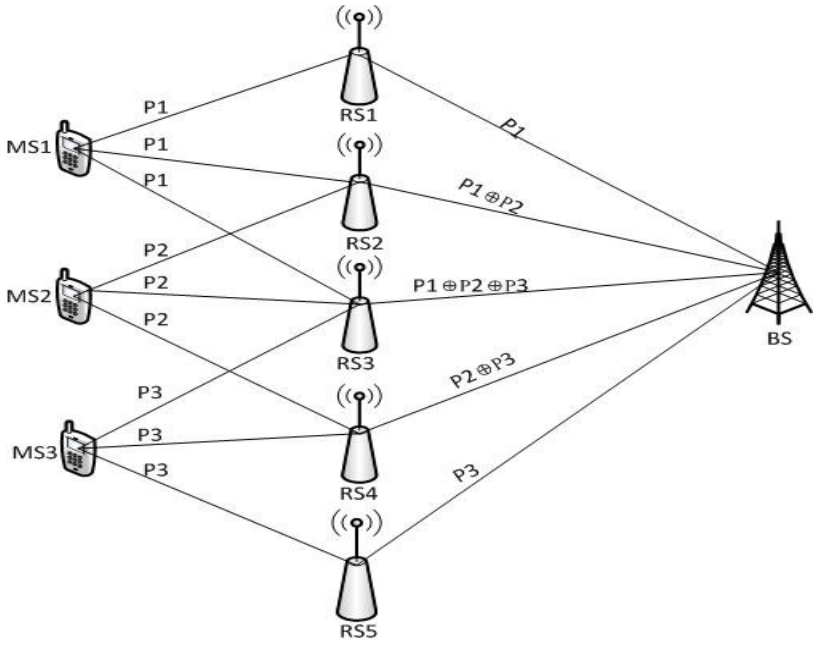


Figure 6.3 Network model - Protection for two relay node failures

Assume that two relays RS1 and RS2 failed as presented in Figure 6.3.The BS can still decode all the packets for P1, P2, and P3. The BS first obtains P3 from RS5, and then decodes P2 and P1 from RS4 and RS3, i.e., the BS decodes P2 from P2⊕P3 and finally, P1 from P1⊕P2⊕P3, respectively. Similarly, the receiver can decode all P1, P2 and P3 if, at most, two of the any relays RS1, RS2, RS3, RS4 and RS5 fail.

6.3. Performance Evaluation of Relay Node Protection using Network Coding

To analyze the QoS performance of the proposed scheme using simulation, it is necessary to investigate the existing support in available simulators. Among the existing simulators, such as NS2, OPNET, MATLAB, etc., only NS2 have the patch (extension) for multihop WiMAX networks, and, to the best of my knowledge, no one open source

simulator has the support for multihop LTE. Hence, the proposed relay node protection is tested only for the WiMAX network. However, similar performance could be achieved for LTE networks. The network considered for single and two RSs protection is shown in Figure 6.2 and Figure 6.3. The simulation tool used for WMNs simulation is NS2.28, and the network considered for protection against single and two relay node failures is similar to Figure 6.2 and Figure 6.3. For the WMNs simulation, first the network coding protocol is integrated into the IEEE 80.11b protocol in NS2. The other simulation parameters considered for this simulation are given in Table 6.1. Similarly for the WiMAX network, both network coding and WiMAX patches are integrated to NS2.28. The WiMAX and other system parameters considered for this simulation are given in Table 6.2.

Table 6.1 System Parameters for Wireless Mesh Networks Simulation

Parameters	Value
Radio-propagation model	Two Ray Ground
MAC Protocol	IEEE 802.11b
Network coding type	XOR
Routing	Broadcast (CODEBCAST)
Link capacity	54Mbps
Packet Size	1000 bytes
Data Rate (in Kbps)	64, 128, 256, 512 and 1024

Table 6.2 System Parameters for WiMAX Networks Simulation

Parameters	Value
MAC Protocol, NS2 patch	Multihop WiMAX, NIST
Physical Layer	Wireless MAN OFDMA, TDD
System Bandwidth	20MHz
Frame duration	5msec
Radio-propagation model	Cost-231
Network coding type	XOR

Parameters	Value
Routing	Broadcast (CODEBCAST)
Packet Size	1000 bytes (Fixed for all data rates)
Data Rate (in Kbps)	64, 128, 256, 512 and 1024
Mobility model	Random way point

The QoS performance is analyzed for single and two relay nodes failure scenarios as presented in Figure 6.2 and Figure 6.3 (except Case 5 and Case 8 in the below list). However, the user's mobility is not considered for the WMNs. For WiMAX network, a single RS failure scenario considers only the relay RS1 failure in Figure 6.2, because the QoS performance is the same for other RSs (RS2, RS3 and RS4) failure as in the case of WMNs. Similarly, two RS failures scenario considers only the failure of RS1 and RS2 as presented in Figure 6.3. Hence, the final scenarios considered for WiMAX networks simulation include:

- *Case 1, static user, no RS failure and no protection*: For the network as shown in Figure 6.2, relays RS1, RS2 and RS3 forward regular packets from users MS1, MS2 and MS3 to the BS. The relay R4 is not considered. All user nodes are static and there is no RS failure in a network.
- *Case 2, static user, one RS failure and no protection*: In this scenario, relays RS2 and RS3 forward regular packets from users MS2 and MS3 to the BS. The relay RS4 is not considered and RS1 fails to forward the packets (P1) as presented in Figure 6.2.
- *Case 3, mobile user, no RS failure and protection enabled*: As the protection scheme is enabled, relays RS2 and RS3 forward network coding packets as shown in Figure 6.2. The user MS1 moves away from the RS1 but within RS2 and RS3 network coverage, that is, the diversity set of MS1 is RS2 and RS3. The user movement in other directions is not considered to show the limitation of XOR network coding.

- *Case 4, static user, one RS failure and protection enabled*: For the given network scenario as presented in Figure 6.2, RS1 fails to forward packets. The relays, RS2 and RS3, forward network coding packets and RS4 forwards regular packets.
- *Case 5, mobile user, one RS failure and protection enabled*: For the given network scenario as presented in Figure 6.2, RS1 fails to forward packets. The relays, RS2 and RS3, forward network coding packets and RS4 forwards regular packets. The user MS1 moves away from the RS1 but within RS2 and RS3 network coverage (diversity set of MS1 is RS2 and RS3).
- *Case 6, static user, two RS failure and no protection*: In this scenario, the relay RS3 forwards regular packets from the user MS3 to the BS. The relays RS4 and RS5 are not considered, and relays RS1 and RS2 fail to forward packets as presented in Figure 6.3.
- *Case 7, static user, two RS failures and protection enabled*: For the given network scenario as shown in Figure 6.3, the relays, R1 and R2, fail to forward packets. Other relays, RS3 to RS5, are working properly, whereas RS3, RS4 forward encoded packets and RS5 forwards regular packets. All MSs are static in a network.
- *Case 8: mobile users, two RS failures and protection enabled*: In this scenario, the relays, RS1 and RS2, fail to forward packets in a network as shown in Figure 6.3. Other relays, RS3 to RS5, are working properly, whereas RS3, RS4 forward network coding packets and RS5 forwards a regular packet. The MSs, MS1 and MS2 are moving away from the network coverage of RS1 and RS2. Their new diversity sets are RS3, RS4 and RS5 for MS1; RS4 and RS5 for MS2.

PDR performance: PDR is the ratio of the total number of packets received at the receiver node over the total number of packets transmitted at all sender nodes.

$$PDR = \frac{Total\ number\ of\ packets\ received\ at\ R}{Total\ number\ of\ packets\ transmitted\ at\ (S1 + S2 + S3)}$$

Figure 6.4 shows the PDR results for the first four scenarios with, at most, one failure in WMNs. The fifth scenario considered in this simulation is r2/r3 relay node failure, where the relay node fails to forward the network coded packet. From the graphs, it is clear that PDR for case 1 (no protection and no failure) and case 3 to case 5 (protection with, at most, one failure) are pretty much the same and the graphs overlap. When the data rate is low (64Kbps), the PDR is approximately 99%, and it reduces for high data rate (≈90% for 1024Kbps). However, the PDR performance for case-2 (no protection and r1 failure) is only about 66% of other schemes. In case 2, the gateway receives data from S2 and S3 only, the relay node r1 fails to forward the packet P1, from S1. In case 4 and case 5, even though one relay node fails, the gateway can retrieve all the senders' information as explained in Section 6.2.1, protection of single relay node failure.

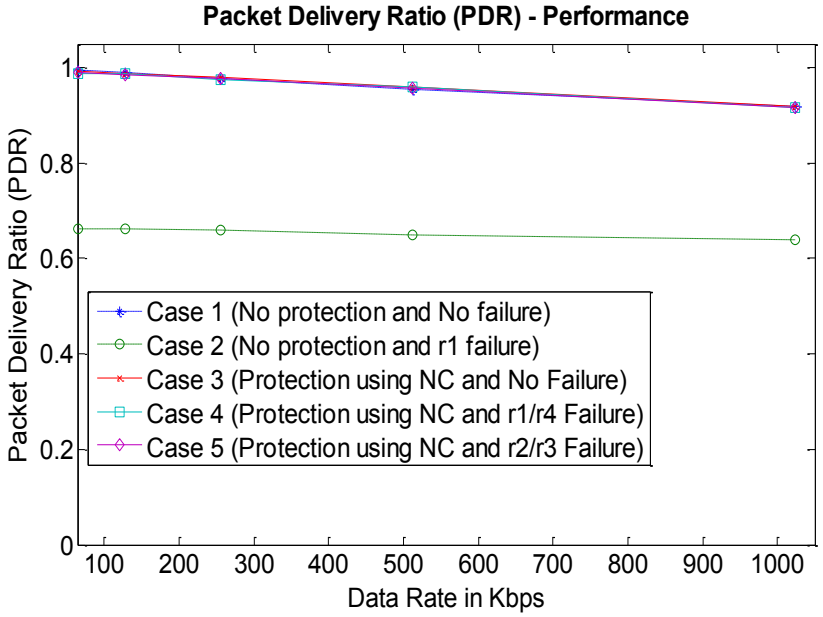


Figure 6.4 PDR for single relay node protection scenarios in WMN

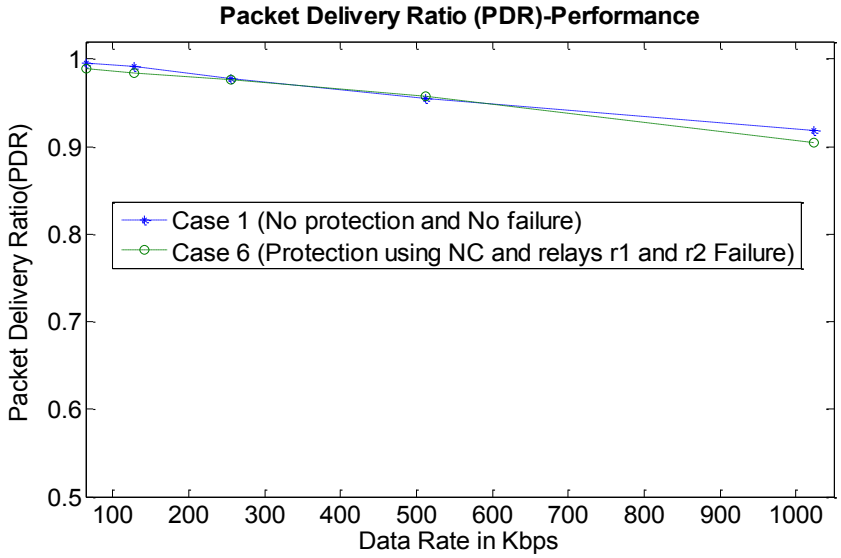


Figure 6.5 PDR for two relay nodes protection scenarios in WMN

Figure 6.5 shows the PDR performance for case 1 (no protection and no failure) and case 6 (protection against two relay nodes failure and relays r1 and r2 failure) scenarios in WMNs. From the graph, it is clear that the protection scheme works well for two relay nodes failure as well, and the PDR performance is close to the no protection and no failure scenario. If the protection scheme is not implemented, the network may achieve only 33 percentage PDR performances for two relay nodes failure.

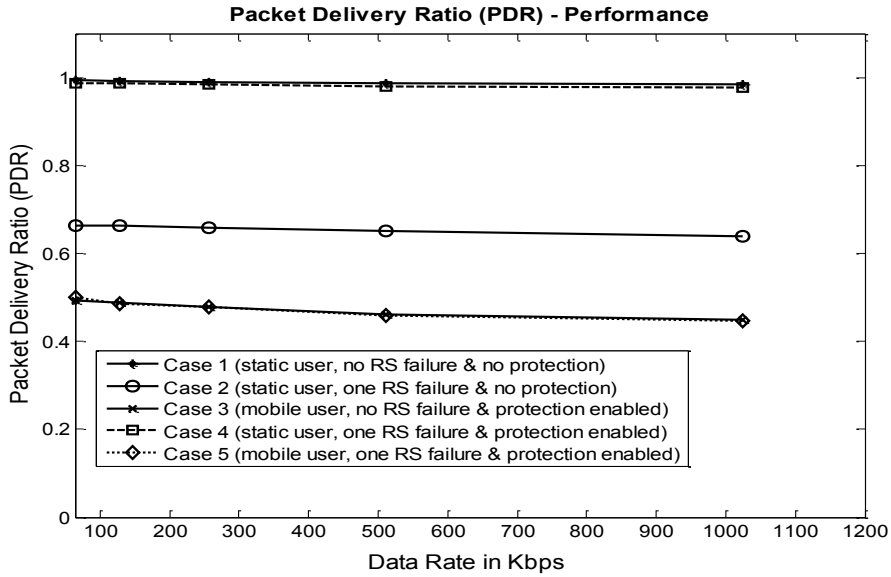


Figure 6.6 PDR for single RS protection scenarios in WiMAX network

Figure 6.6 shows the PDR performance for the first five scenarios with at most one RS failure in WiMAX networks. It can be seen that the PDR results for case 1 (static user, no failure and no protection), and case 4 (static user with, at most, one RS failure and protection enabled) are close, as the curves are overlapping. In case 4, even though the RS fails, the BS is able to decode the MS1 packets from network encoded packets. Hence, both case 1 and case 4 achieve a similar performance. The PDR is approximately 99% for both low and higher data rates. At the same time, the PDR performance for case 2 (static user, with, at most, one RS failure and no protection) is approximately 66%, because one RS (RS1) fails to forward packets (P1) from the source (MS1).

Limitation in XOR network coding: From the PDR performance results in WiMAX networks, it is shown that the PDR for mobility scenarios, such as case 3 and case 5, are very low due to a decoding problem at the receiver node (BS). In mobility scenarios, both RS2 and RS3 forward the network coding packets of P1⊕P2 and P1⊕P2⊕P3 and then RS4 forwards the regular packet P3. Therefore, the BS is able to decode P3 only and then BS has two copies of P1⊕P2.

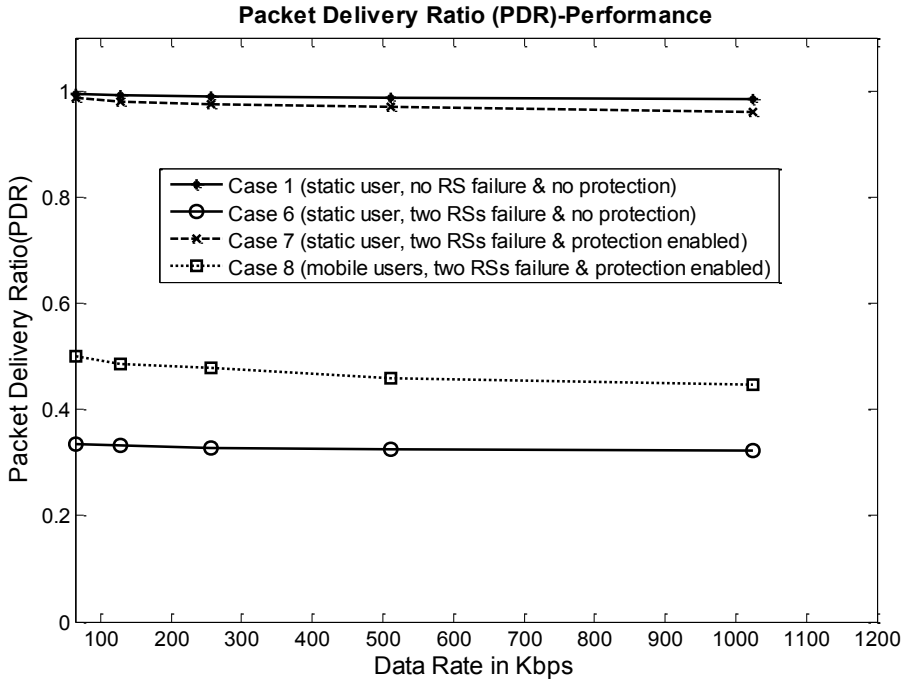


Figure 6.7 PDR for two RSs protection scenarios in WiMAX network

Figure 6.7 shows the PDR performance of no RS failure and two RSs failure cases including user's mobility. The PDR for case 1 (static user, no failure and no protection) and case 7 (static user, two RSs failure and protection enabled) are similar, and the graphs are overlapped. From the graph, it is clear that the protection scheme works well for two RSs failures. If the protection scheme is not implemented, the network may achieve ~66% PDR performances (observed from Figure 6.6) for a single RS failure and ~33% PDR performances for two RSs failures. Still, the PDR performance for mobile scenarios achieves approximately 50%, because the BS is able to decode only part of the information. For the remaining data, the BS is unable to decode from the multiple copies of same encoded packets from different RSs.

Latency performance: The average latency is calculated by dividing the total delay of an individual transmitted packet by total transmitted packets. Further, the latency is calculated only for the successfully received packets, i.e., the packets dropped at the sender node due to long waiting time, failure in transmission due to poor channel condition, and failure of relay nodes are not considered for the calculation. Otherwise, the average latency performance is very high, because the latency for unsuccessful transmissions of packets is infinite.

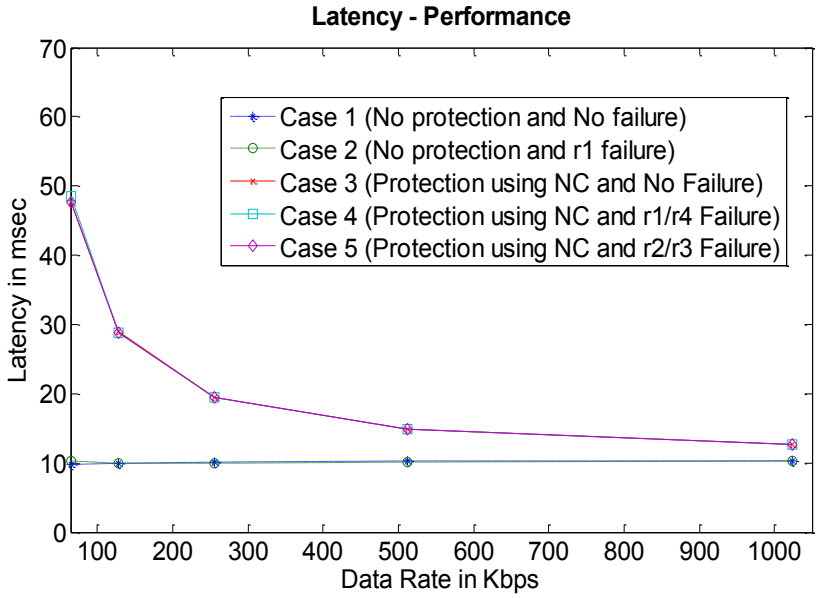


Figure 6.8 Latency for single relay node protection scenarios in WMN

Figure 6.8 shows the latency results of no protection (case 1 and case 2) and protection against single relay node (case 3 – case 5) schemes in WMNs. The latency results for the two no protection schemes are similar (overlapped in a graph), which are close to 10msec. Similarly, the latency for protection against single relay node failure schemes is pretty much the same, but the latency is higher (47msec) for low data rate and closes to 10msec for higher data rates (> 512Kbps). In case 3 – case 5, the receiver node needs network coded packets (information) from all relay nodes except the failure relay node to decode the sender's information.

Figure 6.9 shows the latency results of case 1 and case 6 scenarios. The latency of protection against two relay node failure scheme is similar to the protection against single relay failure schemes as illustrated in Figure 6.8. Apart from the transmission delay, the major factor affecting the latency performance is the inter-arrival time of the packet from different service flow at the RS. When the inter-arrival time of different service flow is high at the RS, to receive the entire encoded packet at the BS takes long time that increases the decoding delay.

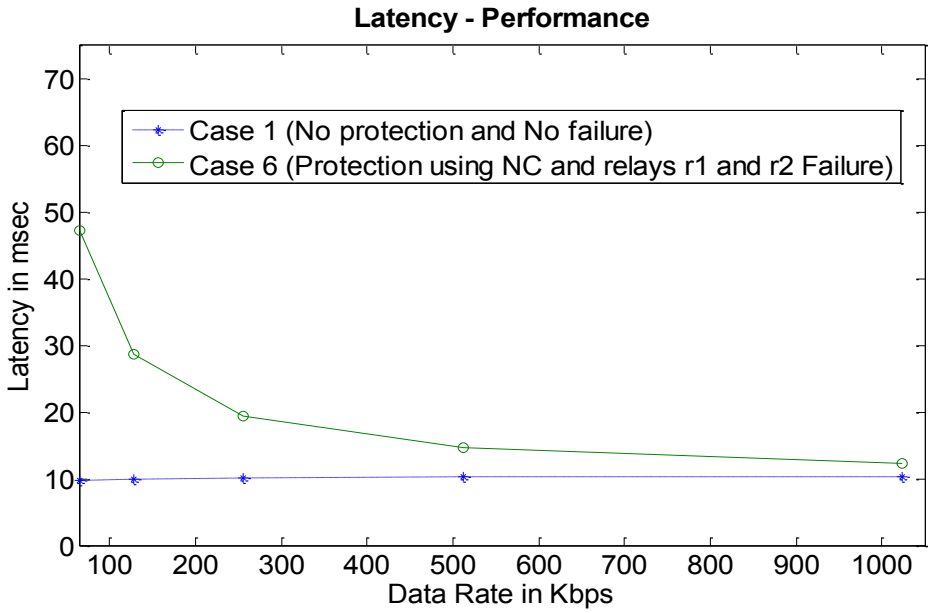


Figure 6.9 Latency for two relay nodes protection scenarios in WMN

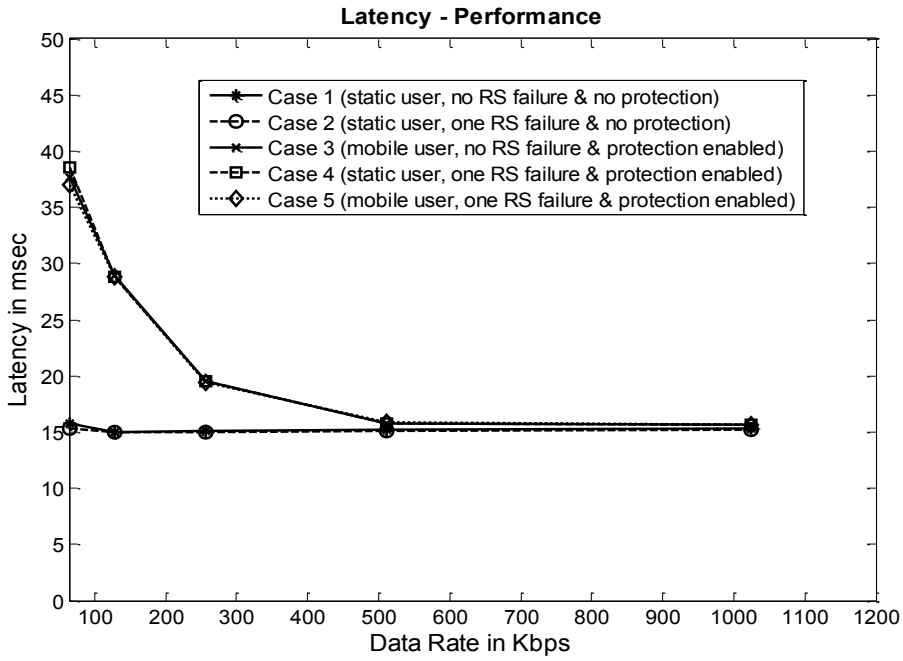


Figure 6.10 Latency for one RS protection scenarios in WiMAX network

Figure 6.10 shows the latency results for no protection scenarios and protection against single RS failure scenarios in WiMAX networks. The latency results for case 1 (static user, no RS failure and no protection) and case 6 (static user, two RS failures and no protection) are pretty much the same, approximately 15msec for all data rates. The latency for protection enabled scenarios is similar, but the latency is higher (~35msec) for low data rate and close to 15msec for higher data rates (> 512Kbps). To decode the sender's information from network encoded packets, the BS needs encoded packets from all other RSs. For instance, if RS1 (in Figure 6.2) fails, the BS first decodes P3 from RS4. Then, it decodes P2 from P2⊕P3, and, finally, it decodes P1 from P1⊕P2. Hence, the BS needs P3, P2⊕P3and P1⊕P2 from the working RSs to decode all of the senders' information. For low data rates, the inter-arrival time is high, and that increases the latency for data.

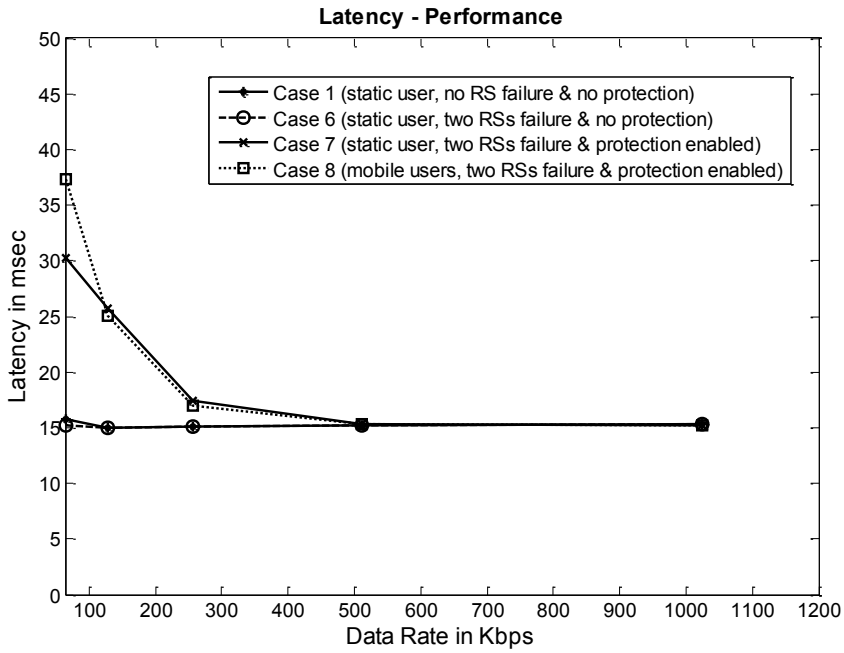


Figure 6.11 Latency for two RSs protection scenarios in WiMAX network

Figure 6.11 shows the latency results of no protection and protection against two RSs scenarios. The latency is approximately 15msec for no protection scheme. Latency for protection enabled schemes is approximately 35msec for low data rate and merges to no protection scheme at higher data rate. The reason for increase is latency is the same for single RS failure scenarios, as illustrated in Figure 6.10.

Jitter: Average jitter: It is calculated by dividing the total jitter of an individual transmitted packet by total transmitted packets. Jitter is calculated by measuring the delay difference between i^{th} transmitted packet and $(i\text{-}1)^{th}$ packet. Figure 6.12 and Figure 6.13 demonstrate the results for jitter. From Figure 6.12, it is clear that jitter for no protection schemes (case 1 and case 2) and protection against single relay node schemes are almost the same (0.3msec), except for the case 4 scenario (protection against single relay node failure and r2/r3 failure) at low data rates. In case 4, when a regular data forwarding relay node fails (r1 or r4 as presented in Figure 6.2), the gateway has to wait for P3 from r4, P2

can then be decoded through P3 and P2⊕P3, and, finally, P1 can be decoded through P2 and P1⊕P2. This leads to an increase in latency and jitter for low data rates.

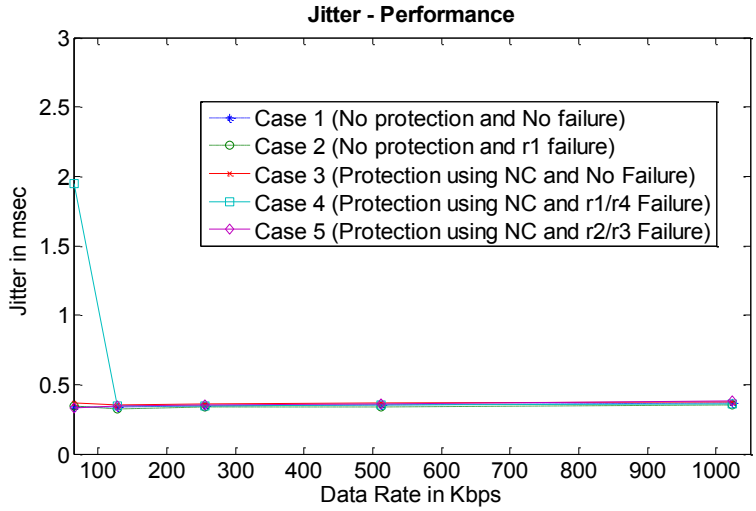


Figure 6.12 Jitter for single relay node protection scenarios in WMN

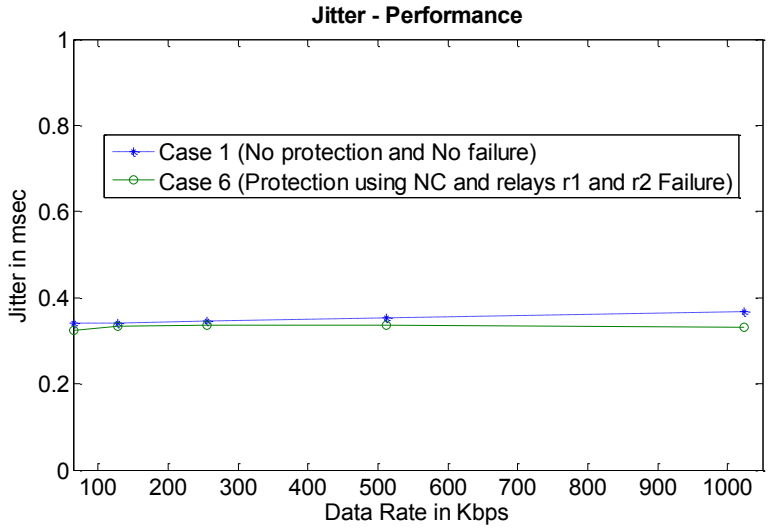


Figure 6.13 Jitter for two relay nodes protection scenarios in WMN

Figure 6.13 shows the jitter performance for case 1 (no protection and no failure) and case 6 (protection against two relays failure and the relays r1 and r2 fail as presented in Figure 6.3). Both cases have similar jitter results.

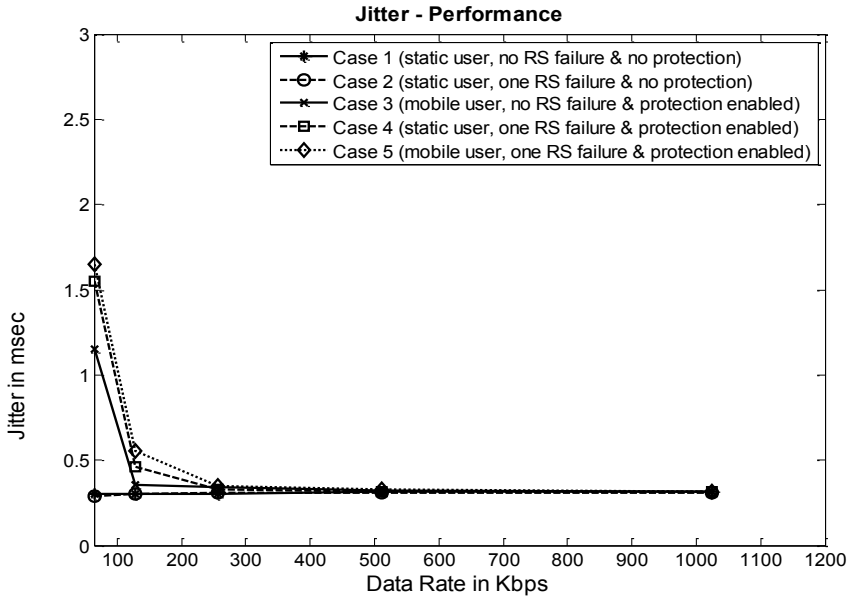


Figure 6.14 Jitter for single relay node protection scenarios in WiMAX

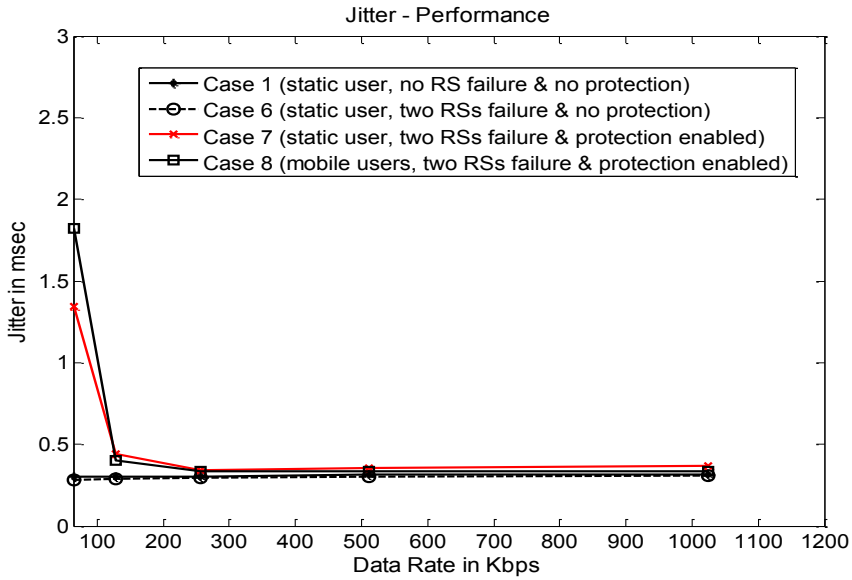


Figure 6.15 Jitter for single relay node protection scenarios in WiMAX

The jitter performance for single and two relay nodes failure scenarios are shown in Figures 6.14 and Figure 6.15. The jitter performance for case 1 and case 2 in Figure 6.14 for no protection schemes is almost the same. Also, the jitter for protection enabled scenarios (cases 3, 4, 5) is approximately 1.5msec at low data rate and merges with no

protection at 512Kbps. In case 3 to case 5, the BS has to wait for network coded data from all of the RSs to decode the packets. As a result, the jitter performance is slightly increased at low data rates (64Kbps and 128Kbps). Also, the jitter performance on protection for two RSs in Figure 6.15 is similar to protection against single RS failure scenarios as presented in Figure 6.14.

6.4 Chapter Summary

In this chapter, the protection scheme against failure of relay nodes was introduced for WMNs and 4G wireless networks to increase reliability. The QoS performance PDR, latency and jitter were measured to study the reliability, that is, the impact of the protection scheme. For a single relay node protection, the addition of one more relay node and the implementation of network coding are needed on the existing network architecture. As a result, this design simulates the 1:N relay node protection scheme for wireless networks. Similarly, protection against the two relay nodes failure scenario requires two additional relay nodes.

For the PDR results, the proposed relay node protection using XOR network coding works well in WMNs and multihop WiMAX networks for static users and the given network scenario. Since the receiver decodes the same amount of data even in the case of relay node failure(s), the PDR performance is pretty much the same as the no failure in RSs (case 1) scenario. In contrast, the BS is unable to decode all of the data from the same copies of network coded packets from different RSs in the user's mobility scenarios. This decoding problem may occur only with XOR network coding.

The latency and jitter are closer to that with no protection scheme at higher data rates (> 512Kbps, i.e., shorter inter-arrival time as the PDU size is the same for all data rates). In general, network coding reduces the time slots needed for data transmissions between the sender and the receiver. On the other hand, using the XOR network coding scheme increases the latency for unidirectional traffic, because the receiver has to wait for the data from all necessary nodes to decode the network coded data. Therefore, the real-

time applications, such as voice, video conference, etc., are getting affected due to high latency and jitter performance.

From the simulation results and study, it is shown that the reliability is assured for single and multiple relay nodes failure scenarios when the users in a network are static. Otherwise, there is a decoding problem with the XOR network coding during mobility scenarios. Hence, this research can be further carried out using other types of network coding, like RLNC. Similarly, this work can be tested on multihop LTE networks, once the open source simulator is available. However, similar results are expected for LTE, as LTE and WiMAX share common architecture.

Chapter 7. Conclusion and Future Directions

The two emerging 4G wireless networks, WiMAX and LTE, are intended to provide a BWA with seamless mobility. They are expected to deliver high performance, sensitive applications, such as live mobile TV, video calling, mobile video services, etc., with customer-perceived service quality or QoE. The major developments in 4G wireless standards, compared with 3G are high data rate, enhanced QoS, and strong security. From the literature investigations, there are three research gaps identified in the 4G wireless networks, which are: (i) the existing RRM framework fails to consider both multihop QoS and effective bandwidth utilization; (ii) little work is available for QoS aware solution for security threats in 4G multihop wireless networks; and, (iii) there is no solution for QoS degradation during RSs failure. Therefore, the proposed work is multi-disciplinary research that focuses on QoS, security and QoS management during relay node failure.

In Chapter 4, the RRM framework for 4G wireless networks was proposed. The RRM framework consists of an adaptive CAC and dynamic PS schemes to ensure the QoS of different service classes. Since the WiMAX and LTE networks have similar PHY layer characteristics and QoS support, the same CAC and PS schemes are tested for both networks. However, the simulations carried out for the WiMAX network are multihop, but LTE is not multihop in nature because the available open source simulators for LTE do not support the relay functionality. The simulation results show that the CBP and CDP performance of the proposed CAC is better than the fixed bandwidth reservation scheme. The CBP is improved by utilizing the unused reserved bandwidth for the least priority new calls. At the same time, the CDP is improved by the adaptive bandwidth reservation scheme and bandwidth degradation policy on the least priority calls. Further, the design of the PS schemes is to cope up the CAC function. When the CAC applies bandwidth pre-emption (that is, the bandwidth required for total calls is more than the system bandwidth), the BS selects the (P+TB) scheduler in the downlink to ensure the intended QoS for voice and real-time services. Otherwise, the (P+E) scheduler is selected to improve QoS

performance of multihop users. Similarly, the (P+E) scheduler at the MS is studied for uplink traffic. The simulation results for the scheduling policy, such as PDR, latency and jitter and the QoS factor evaluation, show that the proposed, dynamic selection of the (P+E) and (P+TB) scheduling schemes ensures QoS differentiation among different service flows at various load conditions and improves multihop latency performance.

In order to provide QoS aware strong security, distributed security architecture using ECDH implementation was proposed in Chapter 5. In that, the RSs and MSs were initially authenticated by the home network and then authorized by the access node (relay or the BS). The proposed scheme overcomes most of the existing security threats, such as DoS attacks and network coding security threats in both WiMAX and LTE, re-authentication issues in WiMAX, etc. The network coding security threats include pollution and entropy attacks. However, disclosure of IMSI due to rogue relay nodes in LTE still exists. For that issue, enterprise authentication, such as EAP-TTLS, is suggested for LTE networks. The security and QoS performance of the proposed security scheme is analyzed with default security scheme and the IPSec. The simulation and testbed results show that the proposed ECDH implementation with distributed security architecture provides strong security, without affecting the QoS performance of the network. The QoS parameters considered for the analysis were connection establishment time, throughput and latency.

In Chapter 6, initially, the relay node protection using network coding technique was studied on 4G multihop wireless networks to increase reliability. To study the impact of protection scheme, the QoS performance PDR, latency and jitter were measured. The simulation for the multihop WiMAX networks considers various scenarios for a single RS failure and two RS failures, including the user's mobility. For the PDR results, the proposed relay node protection using XOR network coding works well in multihop WiMAX networks for static users and the given network scenario. Since the receiver decodes the same amount of data, even in the case of relay node failure(s), the PDR performance is pretty much the same as the no failure in RSs scenario. In contrast, the BS is unable to decode all data from the same copies of network coded packets from different RSs in user's mobility scenarios. This decoding problem may occur only with XOR network coding. Similarly, the latency and jitter performances are closer to no protection

scheme during short packet inter-arrival times. In general, network coding reduces the time slots needed for data transmissions between the sender and the receiver. In contrast, the network coding increases the latency for unidirectional traffic with long packet inter-arrival times because the receiver has to wait for the data from all necessary nodes to decode the network coded data.

7.1. Future Directions

Probing deeper, the simulation results and study of this dissertation provide potential research directions. In general, the scheduler implementation and relay node protection can be tested on multihop LTE networks, once the open source simulator is available. However, similar results are expected for LTE, as LTE and WiMAX share common architecture. Apart from that, two more research areas can be extended in the future: they are extension of current RRM framework with RS mobility and relay node protection scheme using RLNC. The current RRM framework does not consider RS mobility because the available NS2 patch does not support RSs handover. Similarly, the decoding problem exists with the XOR network coding in the current relay node protection scheme. Hence, this research can be further carried out using RLNC network coding scheme. From the theoretical study, the decoding problem of XOR network coding scheme does not exist with RLNC, thus it warrants further research.

References

1. IEEE 802.16-2009, "*IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Broadband Wireless Access Systems"*, IEEE Press, 2009.
2. IEEE 802.16j-2009*, "IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Broadband Wireless Access Systems, Amendment 1: Multiple Relay Specification"*, IEEE Press, 2009.
3. IEEE 802.16m-2011, *"IEEE Standard for Local and metropolitan area networks - Part 16: Air Interface for Broadband Wireless Access Systems, Amendment 3: Advanced Air Interface"*, IEEE Press, 2011.
4. WiMAX Forum, "*WiMAX End-to-End Network Systems Architecture - Stage 3: Detailed Protocols and Procedures"*, V.1.3.0, 2008.
5. WiMAX Forum, "*WiMAX System Evolution Methodology"*, V.2.1, 2008.
6. WiMAX Forum, "*Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation"*, 2006.
7. J. Andrews, A. Ghosh and R. Muhamed, "*Fundamentals of WiMAX: Understanding Broadband Wireless Networking"*, Pearson Education, Inc., Feb. 2007.
8. M. Katz and F. Fitzek, *WiMAX Evolution: "Emerging Technologies and Applications"*, John Wiley and Sons, 2007.
9. 3GPP, Technical Specifications, "*Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) Protocol Specification",* Release 9, 3GPP TS 36.321, Mar. 2009.
10. 3GPP, Technical Specifications, "*Evolved Universal Terrestrial Radio Access (E-UTRA); Further advancements for E-UTRA physical layer aspects"*, 3GPP TR 36.814, 2010.
11. 3GPP, Technical Specifications, "*Requirements for further advancements for Evolved Universal Terrestrial Radio Access (LTE-Advanced)",* 3GPP TR 36.913, 2012.

12. 3GPP, Technical Specifications, "*Evolved Universal Terrestrial Radio Access and Evolved Universal Terrestrial Radio Access Network; Overall description; Stage 2", Release 8*, *TS 36.300 V8.8.0*, March 2009.
13. 3GPP, Technical Specifications, "*Group Radio Access Network; Evolved Universal Terrestrial Radio Access; User Equipment (UE) Radio Transmission and Reception"*, Release 9, 3GPP TS 36.101, 2011.
14. 3GPP, Technical Specifications, "*3GPP System Architecture Evolution (SAE); Security architecture"*, Release 12, 33.401, V12.5.0, 2011.
15. 3GPP, Technical Specifications, "*Feasibility study on LTE relay node security"*, Release 10, 3GPP TR 33.816 V10.0.0, 2011.
16. E. Dahlman, S. Parkvall and J. Skold, "*4G LTE/LTE-Advanced for Mobile Broadband"*, Elsevier Ltd, 2011.
17. LTE White Paper "Future Technologies for Fixed Mobile Convergence, SAE and LTE in Cellular Mobile Communications", http://www.anritsuco.com, last accessed April 06, 2012.
18. S. Ali Shah, M. Iqbal and T. Hussain, "*Comparison between WiMAX and 3GPP LTE"*, MASc Thesis, Blekinge Institute of Technology, Sweden, Aug. 2009.
19. K. Mahmood, "*Adaptive Random Linear Network Coding with Controlled Forwarding for Wireless Broadcast"*, M.A.Sc. Thesis, Carleton University, Canada, Dec. 2010.
20. R. Ibrahim Aljohani, "*Measurement-based Admission Control for Real-time Traffic in IEEE 802.16 Wireless Metropolitan Area Network"*, M.A.Sc. Thesis, University of Waterloo, Canada, 2008.
21. D. Niyato, "*Radio Resource Management in Broadband Wireless Access Networks"*, Ph.D Thesis, University of Manitoba, Canada, 2008.
22. S. Maheshwari, S. Iyer, and K. Paul, "*An Efficient QoS Scheduling Architecture for IEEE 802.16 Wireless MANs"*, Master Thesis, Indian Institute of Technology, 2005.

23. Y. Chen, T. Farley, and N. Ye, “QoS Requirements of Network Applications on the Internet*”*, *Information, Knowledge, Systems Management*”, vol. 4, no. 1, 2004, pp. 55-76.

24. ITU-T, Recommendation G. 107, “*The E-model, a computational model for use in transmission planning”,* 2002.

25. F. Kuipers, R. Kooij, D. Vleeschauwer and K. Brunnstrom, "Techniques for measuring quality of experience", *Proc. of International Conference on Wired/Wireless Internet Communication*, June 2010, pp. 216-227.

26. L. Yi, K. Miao and A. Liu, “A comparative study of WiMAX and LTE as the next generation mobile enterprise network”, *Proc. 13th International Conference Advanced Communication Technologies*, 2011, pp. 654-658.

27. N. Poudyal, H. Lee, Y. Kwon and B. Lee, “Delay-bound Admission Control for Real-time Traffic in Fourth Generation IMT-Advanced Networks based on 802.16m”, *International Journal of Advances in Electrical and Computer Engineering*, Vol. 11, 2011, pp.31-38.

28. K. Wongthavarawat, and A. Ganz, “Packet scheduling for QoS support in IEEE 802.16 broadband wireless access systems”, *International Journal of Communication Systems,* Vol. 16, Issue 1, Feb. 2003, pp. 81- 96.

29. C-H Jiang, T-C Tsai, “Token Bucket Based CAC and Packet Scheduling for IEEE 802.16 Broadband Wireless Access Networks”, *Proc. of International Conference on Consumer Comm. and Networking,* Jan. 2006, pp. 183-187.

30. K. Suresh, I. Misra and K. Saha, “Bandwidth and Delay Guaranteed Call Admission Control Scheme for QOS Provisioning in IEEE 802.16e Mobile WiMAX”, *Proc. of International Conference on IEEE GLOBECOM*, Nov. 2008, pp. 1-6.

31. D. Hong and S. Rappaport, “Traffic Model and Performance Analysis for Cellular Mobile Radio Telephone Systems with Prioritized and Non-prioritized Handoff Procedures”, ” *IEEE Transactions on Vehicular Technology*, Aug. 1986, pp. 77-92.

32. R. Ramjee, R. Nagarajan and D. Towsley, "On optimal call admission control in cellular networks. Wireless Networks", *Proc. of 5th Annual Joint Conference on IEEE Computer Societies Networking the Next Generation, INFOCOM*, Mar. 1996, pp. 43-50.

33. Y. Ge and G-S. Kuo, "An Efficient Admission Control Scheme for Adaptive Multimedia Services in IEEE 802.16e Networks", *Proc. of 64th IEEE Vehicular Technology Conference*, Sep. 2006, pp. 1-5.

34. H. Wang, W. Li and D. Agrawal, "Dynamic admission control and QoS for IEEE 802.16 Wireless MAN", *Proc. of Wireless Telecommunication Symposium*, April 2005, pp. 60-66.

35. S. Chaudhry, and R. Guha, "Adaptive Connection Admission Control and Packet Scheduling for QoS Provisioning in Mobile WiMAX", *Proc. of IEEE International Conference on Signal Processing and Communication*, Nov. 2007, pp. 1355-1358.

36. L. Wang, F. Liu, Y. Ji and N. Ruangchaijatupon, "Admission Control for Non-preprovisioned Service Flow in Wireless Metropolitan Area Networks", *Proc. of 4th European Conference on Universal Multiservice Networks*, Feb. 2007, pp. 243-249.

37. Y. Ge, G-S Kuo, "An Efficient Admission Control Scheme for Adaptive Multimedia Services in IEEE 802.16e Networks", *Proc. of 64th IEEE Vehicular Technology Conference*, Sept. 2006, pp.1 – 5.

38. D. Niyato and E. Hossain, "A game-theoretic approach to bandwidth allocation and admission control for polling services in IEEE 802.16 broadband wireless networks", *Proc. of 3rd International Conference on QoS in Heterogeneous Wired and Wireless Networks*, 2006.

39. O. Yang and J. Lu, "*Call Admission Control and Scheduling Schemes with QoS Support for Real-time Video Applications in IEEE 802.16 Networks*", International Journal of Multimedia, Vol. 1, May 2006, pp. 21-29.

40. A. Sayenko, O. Alanen, J. Karhula and T. Hamalainen, "Ensuring the QoS Requirements in 802.16 Scheduling", *Proc. of International Workshop on*

Modeling Analysis and Simulation of Wireless and Mobile Systems, 2006, pp.108-117.

41. D-H. Cho, J-H. Song, M-S. Kim and K-J. Han, "Performance analysis of the IEEE 802.16 wireless metropolitan area network", *Proc. of 1st International Conference on Distributed Frameworks for Multimedia Applications*, Feb. 2005, pp. 130 – 136.
42. C. Cicconetti, A. Erta, L. Lenzini and E. Mingozzi, "*Performance Evaluation of the IEEE 802.16 MAC for QoS Support*", IEEE Transactions on Mobile Computing, Jan. 2007, pp. 26-38.
43. N. Liu, X. Li, C. Pei and B. Yang, "Delay Character of a Novel Architecture for IEEE 802.16 Systems", *Proc. 6th International Conference on Parallel and Distributed Computing Applications and Technology*, Dec. 2005, pp. 293-296.
44. M. Hawa and D. Petr, "Quality of Service Scheduling in Cable and Broadband Wireless Access Systems", *Proc. of IEEE International Workshop on QoS*, 2002, pp. 247-255.
45. A. Sayenko, "An Adaptive Approach to WFQ with the Revenue criterion", *Proc. of 8th IEEE International Symposium on Computer and Communication*, July 2003, pp. 181-186.
46. Y. Wang, S. Chan, M. Zukerman and R. Harris., "Priority-Based Fair Scheduling for Multimedia WiMAX Uplink Traffic", *Proc. of IEEE ICC*, 2008, pp. 301-305.
47. L. Moraes and P. Maciel, "Analysis and evaluation of a new MAC protocol for broadband wireless access," *Proc. of International Conference on Wireless Networks, Communication and Mobile Computing*, June 2005, pp. 107-112.
48. W. Lilei and X. Huimin, "A new management strategy of service flow in IEEE 802.16 systems", *Proc. of 3rd IEEE Conference on Industrial. Electronics and Applications*, June 2008, pp 1716-1719.
49. D. Niyato and E. Hossain, "Queue-aware Uplink Bandwidth Allocation for Polling Services in 802.16 Broadband Wireless Networks", *Proc. of International Conference on IEEE GLOBCOM*, Dec. 2005, pp. 5-9.

50. J. Chen, W. Jiao and H. Wang, "A Service Flow Management Strategy for IEEE 802.16 Broadband Wireless Access Systems in TDD Mode", *Proc. of IEEE ICC*, May 2005, pp. 3422-3426.

51. P. Rengaraju, J. Juliet Roy and S. Radha, "Multimedia Supported Uplink Scheduling for IEEE 8021.6d OFDMA Networks", *Proc. of International Conference on Annual India Conference*, 2006, pp. 1-5.

52. C. So-In, R. Jain and A-K. Tamimi, "*Scheduling in IEEE 802.16e Mobile WiMAX Networks: Key Issues and a Survey*" IEEE Journal on Selected Areas in Communication, Feb. 2009, pp. 156 - 171.

53. J. Chen, W. Jiao and Q. Guo, "Providing integrated QoS control for IEEE 802.16 broadband wireless access systems," *Proc. of 62nd IEEE Vehicular Technology Conference*, Sep. 2005, pp.1254-1258.

54. D. Tarchi, R. Fantacci, and M. Bardazzi, " Quality of Service Management in IEEE 802.16 Wireless Metropolitan Area Networks," *Proc. of IEEE ICC*, June 2006, pp. 1789 – 1794.

55. K. Vinay, N. Sreenivasulu, D. Jayaram and D. Das, "Performance Evaluation of End-to-end Delay by Hybrid Scheduling Algorithm for QoS in IEEE 802.16 Networks", *Proc. of International Conference on Wireless and Optical Communication Networks*, Aug. 2006, pp, 1-5.

56. P. Dhrona, N. Ali and H. Hassanein, "A Performance Study of Scheduling Algorithms in Point-to-Multipoint WiMAX Networks", *Proc. of 33rd IEEE Conference on Local Computer Networks*, Oct. 2008, pp. 843 – 850.

57. Q. Liu, X. Wang and G. Giannakis, "Cross-layer Scheduler Design with QoS Support for Wireless Access Networks", *Proc. of International Conference on QoS in Heterogeneous Wired and Wireless Networks.*, Aug. 2005, pp. 21-28.

58. J-C. Lin, C-L. Chou and C-H. Liu, "Performance Evaluation for Scheduling Algorithms in WiMAX Networks", *Proc. of 22nd International Conference on Advanced Information Networks and Application - Workshops*, March 2008, pp. 68-74.

59. S. Pizzi, A. Molinaro and A. Iera, "Channel-Aware Class-Based Scheduling for QoS Support in IEEE 802.16/ WiMAX Networks", *Proc. of International Conference on Information Networking*, Jan. 2009, pp. 1-5.

60. D. Skoutas and A. Rouskas, "Scheduling with QoS Provisioning in Mobile Broadband Wireless Systems", *Proc. of European Wireless Conference,* April 2010, pp. 422-428.

61. H. Chen, X. Xie and H. Wu, "A Queue-aware Scheduling Algorithm for Multihop Relay Wireless Cellular Networks", *Proc. of IEEE Mobile WiMAX Symposium*, July 2009, pp. 63-68.

62. D. Ghosh, A. Gupta and P. Mohapatra, "Adaptive Scheduling of Prioritized Traffic in IEEE 802.16j Wireless Networks", *Proc. of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, Oct. 2009, pp. 307-313.

63. F-M. Chang, I-P. Hsieh and S-J. Kao, "An Efficient Uplink Scheduling Mechanism with enabling Multi-device Transmission and Maximum Latency Fulfillment in IEEE 802.16j Networks", *Proc. of 6th International Conference on Computer Science and Education*, Aug. 2011, pp. 1410-1415.

64. Q-l Qiu, J. Chen, L-d Ping, Q-F. Zhang and X-Z. Pan, "LTE/SAE Model and its Implementation in NS2", *Proc. of 5th International Conference on Mobile Ad-hoc and Sensor Networks*, 2009, pp.299-303.

65. M. Qian, Y. Huang, J. Shi, Y. Yuan, L. Tian and E. Dutkiewicz, "Novel Radio Admission Control Scheme for Multi Class Service in LTE Systems" *Proc. of IEEE GLOBECOM* 2009, pp.1-6.

66. X. Li, B. Li, M. Huang and G. Yu "Adaptive PF Scheduling Algorithm in LTE Cellular System", *Proc. of International Conference Information and Communication Technology Convergence* 2010, pp. 501-504.

67. M. Xue, K. Sandrasegaran, H. Ramli and C-C. Lin "Performance Analysis of Two Packet Scheduling Algorithms in Downlink 3GPP LTE System", *Proc. of 24th IEEE Conference on Advanced Information Networking and Applications Workshops,* 2010, pp.915-919.

68. S. Bae, B-G. Choi, M-Y Chung, J-J. Lee and S. Kwon, "Delay-aware Call Admission Control Algorithm in 3GPP LTE System", *Proc. of IEEE Region 10 Conference,* 2009, pp. 1-6.

69. S. Bae, B-G. Choi and M-Y. Chung, "Delay-aware packet scheduling algorithm for multiple traffic classes in 3GPP LTE system", *Proc. of 17th Asia-Pacific Conference on Communication*, 2011, pp. 33-37.

70. B. Sadiq, S. Baek and G. Veciana, "*Delay-optimal opportunistic scheduling and approximations: The log rule*", IEEE/ACM transactions on Networking 2011, Vol. 19, Issue 2*:* pp. 405-418.

71. G. Mongha, K. Pedersen, I. Kovacs and P. Mogensen, "QoS oriented time and frequency domain packet schedulers for the UTRAN Long Term Evolution", *Proc. IEEE VTC*, 2008, pp 2532-2536.

72. O. Delgado and B. Jaumard, "Joint Admission Control and Resource Allocation with GoS and QoS in LTE Uplink" *Proc. of IEEE GLOBECOM Workshops*, 2010, pp. 829-833.

73. H. Adibah, M. Ramli, R. Basukala, K. Sandrasegaran and R. Patachaianand, "Performance of Well Known Packet Scheduling Algorithms in the Downlink 3GPP LTE System", *Proc. of 9th IEEE Malaysia International Conference on Communications*, 2009, pp. 815-820.

74. H. Pham, X. Nhan and S-H Hwang, "Service Class-Aided Scheduling for LTE", *Proc. of 13th International Conference on Advanced Communication Technology*, 2011, pp. 39-43.

75. G. Piro, L. Grieco, G. Boggia, R. Fortuna, and P. Camarda, "*Two-Level Downlink Scheduling for Real-Time Multimedia Services in LTE Networks*", IEEE Transactions on Multimedia, 2011, 1052-1065.

76. T. Shon and W. Choi, "*An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions*", Lecturer Notes in Computer Science, 2007, pp. 88–97.

77. T. Han, N. Zhang, K. Liu, B. Tang and Y. Liu, "Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions," *Proc. of 5th International Conference on Mobile Ad Hoc and Sensor Systems*, Oct. 2008, pp. 828–833.

78. H-M. Sun, S-Y. Chang, Y-H. Lin and S-Y. Chiou, “Efficient Authentication Schemes for Handover in Mobile WiMAX,” *Proc. of 8th International Conference on Intelligent Systems Design and Applications*, Nov. 2008, pp. 44–49.

79. A. Altaf, R. Sirhindi and A. Ahmed, “A Novel Approach against DoS Attacks in WiMAX Authentication using Visual Cryptography”, *Proc. of 2nd International Conference on Security Information Systems and Technology*, Aug. 2008, pp. 238–242.

80. D. Johnston and J. Walker, "Overview of IEEE 802.16 Security," *IEEE Security and Privacy Mag*azine, 2004, vol.2, issue 3, pp. 40–48.

81. H-M. Sun, Y-H. Lin, S-M. Chen and Y-C. Shen., “Secure and fast handover scheme based on pre- authentication method for 802.16-WiMAX,” *Proc. of IEEE Region 10 Conference*, Nov. 2007, pp. 1–4.

82. L. Maccari, M. Paoli and R. Fantacci, “Security Analysis of IEEE 802.16, Communications,” *Proc. of IEEE ICC.,* June 2007, pp. 1160–1165.

83. J. Hur, H. Shim, P. Kim, H. Yoon and N-O. Song, “Security Considerations for Handover Schemes in Mobile WiMAX Networks,” *Proc. of IEEE International Conference on Wireless Communication and Networking*, April 2008, pp. 2531–2536.

84. S. Xu, M. Matthews and C-T. Huang, “Security Issues in Privacy and Key Management Protocols of IEEE 802.16,” *Proc. of ACM 44th Annual Southeast Regional Conference*, 2006, pp. 113–118.

85. Y. Zhou and Y. Fang, “Security of IEEE 802.16 in mesh mode,” *Proc. of IEEE MILCOM.*, Oct. 2006, pp. 1–6.

86. F. Liu and L. Lu, “A WPKI-based Security Mechanism for IEEE 802.16e, IEEE Communications Society,” *Proc. of International Conference on Wireless Communication, Networks and Mobile Computing*, Sep. 2006, pp. 1–4.

87. C-K. Chang and C-T. Huang, “Fast and Secure Mobility for IEEE 802.16e Broadband Wireless Networks,” *Proc. of International Conference on Parallel Processing*, Sep. 2007, pp. 46–46.

88. B. Sikkens, "Security issues and proposed solutions concerning", *Proc. of 8th International Twenty Student Conference on IT,* Jan. 2008.

89. H-M. Sun, Y-H. Lin, S-M. Chen and Y-C. Shen; "Secure and fast handover scheme based on pre-authentication method for 802.16-WiMAX," *Proc. IEEE Region 10 Conference*, 2007, pp. 1–4.

90. J. Donga, R. Curtmolab and C. Nita-Rotarua, "*Secure network coding for wireless mesh networks threats challenges and directions*", Journal for Computer and Communication 2009, Vol. 32: Issue 17*,* pp. 1790-1801.

91. E. Barka, K. Shuaib and H. Chamas, "Impact of IPSec on the Performance of the IEEE 802.16 Wireless Networks" *Proc. of International Conference on New Technology, Mobility and Security*, Nov. 2008, pp. 1-6.

92. L. Nazaryan, E. Panaousis, and C. Politis, "*IPSec Provisioning in WiMAX Networks*", IEEE Vehicular Technology Magazine, Issue 1, March 2010, pp 85-90.

93. Y. Lee, H-K. Lee, G-Y. Lee, H-J. Kim and C-K. Jeong, "Design of Hybrid Authentication scheme and key distribution for mobile multi-hop Relay in IEEE 802.16j", *Proc. of Euro American Conference on Telematics and Information Systems*, 2009.

94. A. DeCarlo, J. Porthy, S. Tyler, B. Xie, R. Reddy and D. Zhao, "Distributed Trust Relationship and Polynomial Key generation for IEEE 802.16m Network", *Proc. of Mobile WiMAX Symposium*, July 2009, pp 111-116.

95. S. Kumar, M. Girimondo, A. Weimerskirch and C. Paar, "Embedded End-to-End Wireless Security with ECDH key Exchange", *Proc. of 46th IEEE Midwest Symposium on Circuits and Systems*, Dec. 2003, pp. 786-789.

96. K. Lauter, "*The advantages of elliptic curve cryptography for wireless security*", IEEE Wireless Communication Magazine, 2004, Vol. 47, pp.62-67.

97. K. Lu, Y. Qian, H-H. Chen, and S. Fu, "*WiMAX networks: from access to service platform*", IEEE Network Magazine, Vol. 22, No. 3, May 2008, pp. 38-45.

98. C. B Sankaran, "*Network access security in next-generation 3GPP systems: A Tutorial*", IEEE Communication Magazine, 2009, Vol. 47: Issue 2, pp.84-91.

99. H. Choudhury, B. Roychoudhury and D.K Saikia, "Enhancing user identity privacy in LTE", *Proc. IEEE 11th International Conference Trust, Security and Privacy in Computing and Communication*, 2012, pp. 949-957.

100. J. Bou Abdo, H. Chaouchi and M. Aoude, "Ensured confidentiality authentication and key agreement protocol for EPS", *Proc. Broadband Networks and Fast International Symposium*., 2012, pp. 73-77.

101. Z. Shi, Z. Ji, Z. Gao and L. Huang "Layered security approach in LTE and simulation", *Proc. 3rd International conference Anti-Counterfeiting, Security, and Identification in Communication*, 2009, pp. 171-173.

102. X. Huang, F. Ulupinar, P. Agashe, D. Ho and G. Bao, "LTE relay architecture and its upper layer solutions", *Proc. IEEE GLOBECOM*, 2010, pp. 1-6.

103. L. Huang, Y. Huang and Z. Gao, "Performance of authentication protocols in LTE environments", *Proc. International Conference Computational Intelligence and Security*, 2009, pp. 293-297.

104. L. Xiehua and W. Yongjun, "Security enhanced authentication and key agreement protocol for LTE/SAE network", *Proc. 7th International Conference Wireless Communication, Networking and Mobile Computing*, 2011, pp. 1-4.

105. C-E. Vintila, V-V. Patriciu, and I. Bica, "Security analysis of LTE access network", *Proc. 10th International Conference Networks*, 2011, pp. 29-34.

106. O. Al-Kofahi, and A. Kamal, "*Network Coding-Based Protection of Many-to-one Wireless Flows*", IEEE Journal on Selected Areas in Communication, 2009, pp. 797-813.

107. S. Aly, and A. Kamal, "Network Coding-Based Protection Strategy Against Node Failures", *Proc. of IEEE ICC*., 2009, pp. 1-5.

108. S. Aly, A. Kamal and A. Walid, "Network Design and Protection Using Network Coding", *Proc. of IEEE Information Theory Workshop*, 2010, pp. 1-5.

109. A. Ramamoorthy, and S. Li, "Protection Against Link Errors and Failures using Network Coding in Overlay Networks", *Proc. of IEEE International Symposium on Information Theory*, July 2009, pp. 986-990.

110. A. Kamal, "*1+N Network Protection for Mesh Networks: Network Coding-Based Protection using p-Cycles*", IEEE/ACM Transactions on Networking, Feb. 2010, pp. 67-80.

111. O. Al-Kofahi and A. Kamal, "Survivability Strategies in Multihop Wireless Networks", *Proc. International Conference on IEEE Wireless Communication*, Oct. 2010, pp. 71-80.

112. V. Dejan, K. Chadi, S. Vladimir and T. John, "Random Network Coding for Multimedia Delivery over LTE-Advanced", *Proc. of International Conference on Multimedia and Expo*, 2012, pp.200-205.

113. C-C. Chou and H-Y. Wei, "Network coding based data distribution in WiMAX", *Proc. 10th International Conference on Mobile Data Management: Systems, Services and Middleware*, 2009, pp. 393-394.

114. J. Jin, L. Baochun and K. Taegon, "Is random network coding helpful in WiMAX?", *Proc. 27th IEEE Conference on Computer Communications*, INFOCOM 2008, pp. 2162-2170.

115. NS2-WiMAX-AWG [Online]. Available: http://code.google.com/p/ns2-wimax-awg/

116. NS2-LTE model [Online]. Available: http://code.google.com/p/lte-model/

117. P. Rengaraju, C-H. Lung, F.R. Yu and Anand Srinivasan, "*On QoE Monitoring and E2E Service Assurance in 4G Wireless Networks*", IEEE Wireless Communication Magazine, Volume 19: Issue 4, 2012, pp. 89-96.

118. T. L. Saaty, Elements of Queueing Theory with Applications. New York: McGraw-Hill, 1981. Republished by New York: Dover Publications, 1983.

119. N. Seddigh, B. Nandy, R. Makkar, "Security advances and challenges in 4G wireless networks", *Proc. 8th Annual Conference on Privacy, Security and Trust*, 2010, pp. 62-71.

120. C-T. Huang and J.M. Chang, "*Responding to security issues in WiMAX networks*", IEEE Computer Society IT Professional Magazine, 2008, pp. 15–21.

121. Y. Kim, H-K. Lim and S. Bahk; "Shared authentication information for preventing DDoS attacks in mobile WiMAX Networks," *Proc. 5th IEEE Conference on Consumer Communication and Networking*, 2008, pp. 765–769.

122. G. Kambourakis, E. Konstantinou and S. Gritzalis, "*Revisiting WiMAX MBS security*", International Journal for Computer and Mathematics With Applications, 2010, Vol. 60: Issue 2, pp. 217-223.

123. K. Byoung-Jo, S. Srinivasan "Simple mobility support for IPsec tunnel mode" *Proc. 58th IEEE VTC Conference*, 2003, pp. 1999-2003.

124. M. Purkhiabani and A. Salahi,"Enhanced authentication and key agreement procedure of next generation evolved mobile networks", *Proc. 3rd International Conference on Communication Software and Networking,* 2011, pp. 557-563.

125. Y. Park and T. Park, "A Survey of Security Threats on 4G Networks", *Proc. of IEEE Globecom Workshops*, 2007, pp.1-6.

126. M. Al-Humaigani, D. Dunn, and D. Brown, "Security Transition Roadmap to 4G and Future Generations Wireless Networks", *Proc. 41st Southeastern Symposium on System Theory*, 2009, pp.94-97.

127. H. Mun, K. Han, and K. Kim, "3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement Based on EAPAKA", *Proc. Wireless Telecommunication Symposium,* 2009, pp. 1-8.

128. C. Kolias, G. Kambourakis and S. Gritzalis, "*Attacks and Countermeasures on 802.16": Analysis and Assessment*", IEEE Communication Surveys and Tutorials, Vol. 15: N0 1, 2013, 487-514.

129. J. Huang and C-T. Huang, "Secure Mutual Authentication Protocols for Mobile Multi-Hop Relay WiMAX Networks against Rogue Base/Relay Stations", *Proc. IEEE Conference on Communication*, 2011, pp. 1-5.

130. B. Bhargava, Y. Zhang, N. Idika, L. Lilien and M. Azarmi, "*Collaborative Attacks in WiMAX Networks*", Journal on Security and Communication Networks, Wiley Interscience, 2009, Vol. 2, pp.373-391.

131. S. Naseer, M. Younus and A.Ahmed, "Vulnerabilities Exposing IEEE 802.16e Networks to DoS Attacks: A Survey", *Proc. 9th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel / Distributed Comp*uting, 2008, pp.344-349.

132. J. Hong Kok Han, M. Yusoff Alias and B. Min Goi, "*Simulating Denial of Service Attack Using WiMAX Experimental Setup*", International Journal of Network and Mobile Technologies, Vol. 2, No. 1, 2011, pp. 30-34.

133. M. Shojaee, N. Movahhedinia and B.T. Ladani, "Traffic Analysis for WiMAX Network Under DDoS Attack", *Proc. 2nd International Pacific-Asia Conference on Circuits, Communication and System*, 2010, pp.279-283.

134. J. Hong Kok Han, M. Yusoff Alias and M. Goi Bok, "Potential Denial of Service Attacks in IEEE802.16e-2005 Networks", *Proc. 9th International Conference on Communication and Information Technologies*, 2009, pp. 1207-1212.

135. F. Ibikunle, "Security Issues in Mobile WiMAX (802.16e)", *Proc. of IEEE Mobile WiMAX Symposium*, 2009, pp. 117- 122.

136. R. Rodney and A Vikas, "An Analysis of WiMAX Security Vulnerabilities", *Proc. International Conference on Wireless Networks and Embedded Systems*, 2009.

137. L. Maccari, M. Paoli and R. Fantacci, "Security Analysis of IEEE 802.16" Communications", *Proc. IEEE International Conference on Communications*, 2007, pp.1160-1165.

138. B. Kwon, R. A. Beyah and J. Copeland, "*Key Challenges in Securing WiMAX Mesh Networks*", Journal on Security and Communication Networks, John Wiley & Sons, Ltd., Vol. 2:Issue 5, 2009, pp. 413- 426.

139. B. Kwon, C. Lee, P. Chang Yusun and J. Copeland, "A Security Scheme for Centralized Scheduling in IEEE 802.16 Mesh Networks", *Proc. IEEE International Conference on Military Communications*, 2007, pp.1-5.

140. J. Cao, M. Ma, H. Li and Y. Zhang, "*A Survey on Security Aspects for LTE and LTE-A Networks*", IEEE Communications Surveys and Tutorials, Accepted for publication.

141. J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "*A Simple and Robust Handover Authentication between HeNB and eNB in LTE Networks*", Computer Networks, Vol. 56, 2012, pp. 2119-2131.

142. C-H. Han, "*Security Analysis and Enhancements in LTE-Advanced Networks*", Ph.D. Dissertation, Department of Mobile Systems Engineering, The Graduate School, Sungkyunkwan University, 2011.