

ULRR

Consumer-oriented incoming call connection service for the ubiquitous consumer wireless world

Item Type	Thesis
Authors	Wang, Ning
Download date	2026-05-16 22:57:49
Item License	https://creativecommons.org/licenses/by-nc-sa/1.0/
Link to Item	https://hdl.handle.net/10344/5997

Consumer-Oriented Incoming Call Connection Service for the Ubiquitous Consumer Wireless World



Ning Wang

BEng, MSc

The research work was under supervision and direction of

Dr. Ivan Ganchev

Dr. Máirtín Ó Droma

Dip Eng (honors), PhD, SMIEEE

BE, PhD, CEng, FIEE, SMIEEE

Telecommunications Research Center

Department of Electronic and Computer Engineering

University of Limerick

A thesis submitted for the degree of

Doctor of Philosophy

July 2010

Consumer-Oriented Incoming Call Connection Service for the Ubiquitous Consumer Wireless World

Ning Wang

Department of Electronic and Computer Engineering

University of Limerick

Abstract

This thesis proposes a novel consumer-oriented Incoming Call Connection (ICC) service as an important enabling infrastructural component of the recently proposed ubiquitous consumer wireless world (UCWW), a new Consumer-centric Business Model (CBM) environment for wireless communications. The ICC solution proposed here will be offered by third-party providers who are autonomous of the access network providers. Compared to the present ICC service in the legacy subscriber-based networks, the consumer-oriented ICC service will offer to mobile users greater flexibility and management control over incoming calls, enable users to receive incoming calls via multiple access networks/providers by means of a single identity, support user-driven, seamless, network-transparent Hot Access network Change (HAC), largely eliminate roaming charges and develop a new wireless networking business opportunity among other benefits.

This thesis advocates for a coming paradigm change from the existing ICC service established on the Subscriber-based Business Model (SBM-ICC) towards the CBM-based ICC (CBM-ICC) service. The investigation, design and implementation of all the protocols and other elements required for building the CBM-ICC service especially in terms of transport, signaling and mobility support are addressed. The existence of other key UCWW infrastructural components of third-party authentication, authorization and accounting (3P-AAA) service provision, IPv6 personal address, and service offerings advertisements over wireless billboard channels (WBCs) is assumed. An architecture and protocol infrastructure for the CBM-ICC service is elaborated. Components and interfaces relying upon existing protocols or requiring new signaling protocols (or modification/new elements of existing protocols) are identified and for the latter solutions are suggested. The concept of user-driven HAC is promoted and described. The introduction of the Stream Control Transmission Protocol (SCTP) as a potential solution for enabling this HAC is motivated.

Furthermore, the thesis elaborates a generic CBM-ICC service scenario, which shows how the CBM-ICC service offers to mobile users greater freedom and operation control over incoming calls, enables the novel attribute of users being empowered to receive incoming calls simultaneously, and otherwise, from various homogeneous and heterogeneous access networks, owned by the same or different providers, and enables user-driven HAC on active calls in keeping with, or matched to, user's Always Best Connected and Best Served (ABC&S) policies. A CBM-ICC proof-of-concept system-level testbed is implemented to perform experimental tests, probe different communications scenarios, evaluate the service performance, and further elaborate the service architecture. In this, approaches towards evaluating the performance of the CBM-ICC service based on designed testbed are elaborated, and sample numerical results are presented and analyzed.

Declaration

This thesis is presented in fulfillment of the requirements for the degree of Doctorate of Philosophy. This thesis has not been submitted to any other University or higher education institution, or for any other academic award in this University. Where use has been made of the work of other people it has been fully acknowledged and fully referenced.

Signed:

Date:

Ohana means family.

Family means nobody gets left behind, or forgotten.

Dedicated to Mum, Dad and my wife.

Without your love and support I would not be at this point today.

Dedicated to the loving memory of my grandma.

1939 – 1999

Acknowledgments

First of all, I have to show my great appreciation for my supervisors, Dr. Ivan Ganchev and Dr. Máirtín Ó Droma. They have given me guidance and advice in both academic and non-academic fields throughout my Ph.D. research at the University of Limerick.

I would like to acknowledge the financial support from Science Foundation Ireland under the Basic Research Grant Ref. No. 04/BR/E0082. The project would not be ever completed without this funding.

Most importantly, I have to present my immense gratitude to my parents, and my wife. They have offered huge support and encouragement which is beyond anyone's expectation. I would like to especially thanks to my wife for tolerating my irregular working habits and help me go through the most difficult time in my research. For that, I think there is no words in this world can express all my appreciation.

Last, but by no means least, I would like to thank the people those ever helped me and gave suggestions to my research. I wish to give thanks all my lovely friends who ever shared joy with me during my academic career. I also want to say thanks to my Lab colleagues at the Telecommunications Research Centre for their valuable discussions and friendship. Furthermore I am also grateful to Donald E. Knuth for T_EX and would like to thank *Leslie Lamport* and the L^AT_EX3 Project.

Table of Contents

Abstract	i
Declaration	ii
Dedication	iii
Acknowledgement	iv
List of Figures	xiii
List of Tables	xviii
List of Acronyms	xix
1. Introduction	1
1.1. Background	1
1.2. Overview	8
1.3. Motivation	10
1.4. Thesis Contribution	12
1.5. Thesis Outline	13
2. TCP/IP Background: Relevant Protocols	16
2.1. Introduction	16
2.2. Layered Communication Model	17
2.3. Network-Layer Protocols	17
2.3.1. Internet Protocol Version 6 (IPv6)	17
2.4. Transport-Layer Protocols	20
2.4.1. Stream Control Transmission Protocol (SCTP)	20
2.4.1.1. SCTP Features	20
2.4.1.2. SCTP Protocol Data Unit (PDU) Structure	22
2.4.1.3. Multi-streaming in SCTP	26

Table of Contents

2.4.1.4.	Multi-homing in SCTP	28
2.4.1.5.	Reliable Transmission and Congestion Control	29
2.4.2.	Partial Reliability SCTP (PR-SCTP)	30
2.4.3.	Real-time Transport Protocol (RTP)	32
2.5.	Application-Layer Protocols	35
2.5.1.	Domain Name System (DNS)	35
2.5.2.	Dynamic Host Configuration Protocol v6 (DHCPv6)	37
2.5.3.	Lightweight Directory Access Protocol (LDAP)	38
2.5.4.	Session Initiation Protocol (SIP)	39
2.5.4.1.	SIP server and address	39
2.5.4.2.	SIP Messages	40
2.5.4.2.1.	Request Message	40
2.5.4.2.2.	SIP Response Message	40
2.5.5.	TELEPHONE Number Mapping (ENUM)	42
2.6.	Mobility Management	46
2.6.1.	Location Management	47
2.6.1.1.	Secure Dynamic DNS (DDNS)	47
2.6.1.2.	SIP Location Management	49
2.6.1.3.	Location Management Comparison	50
2.6.2.	Handoff Management	50
2.6.2.1.	Mobile IPv6 (MIPv6)	51
2.6.2.1.1.	Comparison between MIPv6 and MIPv4	53
2.6.2.2.	MIPv6 enhancement	54
2.6.2.2.1.	Hierarchical MIPv6	55
2.6.2.2.2.	Cellular IPv6	55
2.6.2.3.	SIP Handoff Management	56
2.6.2.4.	Mobile SCTP Extension	56
2.7.	Conclusions	58
3.	Related Work	59
3.1.	Introduction	59

3.2. Related Services	59
3.2.1. Skype Service	60
3.2.2. Voice over IP (VoIP)	61
3.2.3. Cisco Call Manager	62
3.3. Related Work within Academia	64
3.4. Related Work within Organizations and Industry	66
3.5. Related Work in Mobility Management	67
3.6. Conclusions	68
4. CBM-ICC Service	70
4.1. Introduction	70
4.2. Traditional SBM-ICC Service	71
4.3. New CBM-ICC Service	73
4.4. Comparison of CBM-ICC with Other Services	75
4.5. CBM-ICC Operational Demonstration	78
4.5.1. CBM-ICC Operational Modes	80
4.5.1.1. Enquiry Mode (E-Mode)	80
4.5.1.2. Redirection Mode (R-Mode)	82
4.6. Addressing Issues	83
4.6.1. IPv6 Personal Address	83
4.6.2. Contact Address Identifier (CAI)	85
4.6.3. Consumer Identity Module (CIM)	86
4.6.4. The Use of Contact Address Identifiers (CAIs), Contact Ad- dresses (CAs), and Personal Addresses	87
4.7. Conclusions	88
5. CBM-ICC Service Architecture	90
5.1. Introduction	90
5.2. CBM-ICC Service Architecture Overview	90
5.3. CBM-ICC Service Architecture Components	92
5.4. CBM-ICC Service Interfaces and Signaling Protocols	93
5.4.1. Ia/Ia* Interface	93

5.4.2. Ic Interface	94
5.4.3. Id Interface	95
5.4.4. It and In Interfaces	96
5.4.5. Ie Interface	96
5.5. Hot Access Network Change (HAC)	96
5.6. Conclusions	99
6. CBM-ICC Service Scenarios and Signaling Flows	101
6.1. Introduction	101
6.2. Generic CBM-ICC Service Scenario with No Mobility	102
6.2.1. Advertisement, Discovery and Association (ADA)	104
6.2.2. Contact Address Update	104
6.2.3. ICC Session Setup	105
6.2.3.1. E-Mode	105
6.2.3.2. R-Mode	106
6.2.4. ICC Session Release	106
6.2.4.1. E-Mode	106
6.2.4.2. R-Mode	106
6.3. Generic CBM-ICC Scenario with HAC	107
6.3.1. E-Mode	107
6.3.2. R-Mode	108
6.4. Conclusions	109
7. CBM-ICC Experimental Testbed	110
7.1. Introduction	110
7.2. Testbed Layout	110
7.3. Testbed Design and Implementation	112
7.3.1. ICC Service-Provider (ICC-SP) Design and Implementation . . .	112
7.3.2. ICC Service-Supporting Entity (ICC-SE) Design and Implemen- tation	115
7.3.3. ICC-client Design and Implementation	116
7.3.3.1. Software Design	116

7.3.3.2. Modifications on SCTP	118
7.4. Conclusions	120
8. CBM-ICC Service Performance Evaluation and Results	122
8.1. Introduction	122
8.2. QoS Metrics	123
8.3. Testbed Configuration	125
8.4. Signaling Overhead Evaluation	128
8.4.1. Generic Scenario with No Mobility	128
8.4.2. Generic Scenario with HAC	131
8.5. HAC Performance Evaluation	135
8.5.1. ICC Data Service	135
8.5.2. ICC Voice Service	142
8.5.3. ICC Video Service	147
8.6. Conclusions	155
9. Conclusions and Future Work	160
9.1. Thesis Conclusions	160
9.2. Future work	162
References	165
Index	194
Appendices	198
A. A List of Relevant Author's Publications	199
B. MPEG-4	201
C. Evalvid Video Evaluation Framework	203
D. Peak Signal-to-Noise Ratio (PSNR)	205

E. Code Reference

206

List of Figures

1.1.	The dual mode mobile terminal market volume growth published by Disruptive Analysis [1] in June 2005. It is shown that the globe dual-mode VoIP phone drives the worldwide mobile market and grows significantly to almost 35-40 million handsets by 2009 [2].	6
1.2.	A high-level view of the CBM-ICC scheme where a mobile user may be simultaneously accessible through various ANPs and ICC-SPs.	10
2.1.	The IPv6 Header. IPv6 has a 128-bit IP address space, which offers 2^{128} (about 3.4×10^{38}) addresses.	19
2.2.	The SCTP 4-way connection setup vs. TCP 3-way connection setup. SCTP uses a 4-way handshake to initiate a new connection, which may introduce additional delay but will protect against “Denial-of-Service” [3] attacks.	23
2.3.	The SCTP 3-way connection termination vs. TCP 4-way connection termination. SCTP employs a 3-way termination procedure to completely terminate the association. However, if an immediate shutdown is expected, SCTP needs to send an ABORT message.	23
2.4.	The structure of the SCTP Protocol Data Unit (PDU) (Source:[4]). The standard SCTP PDU consists of a common header, and one or more chunks. The chunk could be either a control chunk or a DATA chunk, which is recognized by distinct chunk type. The DATA chunk contains the actual data payload incorporated with various flags such as transmission sequence number (TSN), and Stream Sequence Number (SSN). The format of control chunk varies depending on the chunk type.	24

2.5. The multi-streaming feature in SCTP. This unique function avoids HOL blocking by independently transmitting data in separated streams, and provides the flexibility on transferring diverse streams of data inside the overall SCTP message flow.	27
2.6. The multi-homing feature in SCTP. This unique function enables an association have multiple IP addresses (or network interface cards) between two end-points.	28
2.7. The Optional Parameter Type in the INIT and INIT ACK chunks for PR-SCTP.	32
2.8. The new Chunk Type (Forward Cumulative TSN) for PR-SCTP.	32
2.9. The RTP header structure. The format refers to RTP version 2 in RFC1889 [5].	33
2.10. The structure of the DNS Naming Space (Source:[6]). The hierarchical structure of DNS is convenient to convert domain names readable to humans into IP addresses linked with networking equipment.	36
2.11. An example of ENUM usage in CBM-ICC scenario where a user wishes to make his/her telephone number as his/her permanent contact number and the incoming call can be redirected in diverse approaches.	46
2.12. The overall format of the secure DDNS UPDATE message [7]. This format based on the DNS message format in [8] extends a number of fields.	48
2.13. An example of the REGISTER message which can be used to update location information by registering a new IP address to the server.	49
2.14. A schematic diagram of the MIPv6 Binding Update to the Home Agent.	51
2.15. A schematic diagram the Binding Update to the Correspondent Host.	53
3.1. The protocol stack for VoIP. The VoIP layered hierarchy complies with the theoretical model developed by the OSI model.	62

4.1.	The traditional SBM-ICC service. In this service a mobile user often has a long-term contract with one ANP, often named 'Home ANP'. All incoming calls will first come to this 'Home ANP' even if the user is roaming.	72
4.2.	The novel CBM-ICC service. In this service, all incoming calls will come to independent ICC-SP. Each call will be forwarded via the most appropriate ANP according to user's preferences. The callee could be dynamically associated with multiple ANPs	74
4.3.	The CBM-ICC service schematic.	78
4.4.	The CBM-ICC service in enquiry operational mode (E-Mode).	81
4.5.	Signaling flows for the CBM-ICC enquiry operational mode (E-Mode).	81
4.6.	The CBM-ICC service in redirection operational mode (R-Mode).	82
4.7.	Signaling flows for the CBM-ICC redirection operational mode (R-Mode).	83
4.8.	The format of the IPv6 personal address suggested in [9].	84
4.9.	The Consumer Identity Module (CIM) structure.	87
4.10.	The CAIs, CAs, and Personal Addresses in the CBM-ICC service.	88
5.1.	The CBM-ICC Service Architecture. In this architecture, a multi-mode MT is capable to simultaneously associate with more than one ANP. MT may switch between heterogeneous ANs and may receive calls via more than one ANPs simultaneously.	91
5.2.	The Hot Access network Change (HAC). In a multi-access scenario, there could be more than one active links existing between the MT and the ANPs. HAC switches an active ICC session between two live access connections without user intervention and with minimal service disruptions.	97

6.1. The CBM-ICC service scenarios. It is assumed that the callee (MU2/MT2) in the ANP1 domain accepts a CBM-ICC session from the caller (MU1/MT1) and then moves to the ANP2 domain by switching the live ICC session by means of HAC. 102

6.2. Signaling flows for the generic CBM-ICC service scenario with no mobility (in both operational modes). It is assumed that MU1 and MU2 are associated with one common ICC-SP and MU2 avails of several ANPs for ICC service support. 103

6.3. Signaling flows for the generic CBM-ICC service scenario with HAC in E-Mode. It is assumed that an ICC session has been already established and the HAC is performed in the middle of this session. 108

6.4. Signaling flows for the generic CBM-ICC service scenario with HAC in R-Mode. It is assumed that an ICC session has been already established and the HAC is performed in the middle of this session. 109

7.1. The generic layout of the CBM-ICC experimental testbed. 111

7.2. The block diagram of ICM. 114

7.3. The stack diagram of the ICC-client. The API implementations for SCTP in Linux are based on the SCTP library (SCTPLIB) and SCTP Kernel (LK_SCTP). A kernel-level LK_SCTP is chosen as a development foundation for the HAC implementation. 117

7.4. The API function procedure at the sender and the receiver. 118

8.1. The CBM-ICC testbed configuration. Different ANPs are simulated using multiple access points (APs). The ICC-SP infrastructure is established as a group of PCs. A PC residing on the edge of an ANP is configured as an ICC-SE. MTs are laptop computers running the Linux operating systems (Ubuntu 8.10) with installed testbed software. A WAN emulator is used to emulate the expected network delay, packet loss and bandwidth. . . . 126

8.2. The ADA delay for R-Mode and E-Mode. 129

LIST OF FIGURES

8.3. The CA update delay for R-Mode and E-Mode.	129
8.4. The ICC session setup delay for R-Mode and E-Mode.	130
8.5. The ICC Session Release Delay for R-Mode and E-Mode.	130
8.6. The signaling performance for R-Mode and E-Mode.	132
8.7. An ICC-SP/ICM's CPU load comparison of two operational modes. . . .	132
8.8. The HAC signaling performance for R-Mode and E-Mode.	134
8.9. The main components of the HAC switching delay with comparison of R-Mode and E-Mode.	134
8.10. The accumulative number of SACKs for the ICC data service.	136
8.11. The throughput for the ICC data service.	138
8.12. The end-to-end delay for the ICC data service.	140
8.13. The jitter for the ICC data service.	141
8.14. The accumulative number of SACKs for the ICC voice service.	143
8.15. The throughput for the ICC voice service.	145
8.16. The Mean Opinion Score (MOS) for the ICC voice service.	146
8.17. The end-to-end delay for the ICC voice service.	148
8.18. The jitter for the ICC voice service.	149
8.19. The accumulative number of SACKs for the ICC video service.	151
8.20. The throughput for the ICC video service.	152
8.21. The Peak Signal-to-Noise Ratio (PSNR) for the ICC video service. . . .	154
8.22. The end-to-end delay for the ICC video service.	156
8.23. The jitter for the ICC video service.	157
B.1. A Video Object Plane (VoP) in MPEG-4.	202
C.1. The video evaluation framework scheme (Source:[10]).	204

List of Tables

1.1. The IEEE 802.11 standard.	5
2.1. The TCP/IP model.	18
2.2. A comparison of SCTP with TCP and UDP (Source:[11]).	22
2.3. The SIP Request Messages.	40
2.4. The SIP response message classification.	41
2.5. The NAPTR format.	43
2.6. One possible configuration for ENUM.	45
3.1. The VoIP Codecs (commonly used).	63
4.1. A comparison of CBM-ICC service with relative services.	76
5.1. The CBM-ICC service interfaces and protocols.	94
5.2. An example of callee's preferences.	95
5.3. A mobility management protocols' comparison.	98
7.1. The testbed equipment list.	113
7.2. The SCTP API exported by the ICC-client.	117
8.1. The access networks' configuration parameters.	128
8.2. The WAN configuration parameters.	128

List of Acronyms

3G	3rd Generation Mobile Communication	CBM-ICC	CBM-based ICC service
3P-AAA	Third-party Authentication, Authorization and Accounting	CDF	Cumulative Distribution Function
3P-AAA-SP	3P-AAA Service Provider	CDMA	Code Division Multiple Access
AAA	Authentication, Authorization and Accounting	CIF	Common Intermediate Format
AAAA	Quad-A record	CIM	Consumer Identity Module
AAAS	AAA Server	CIPv6	Cellular IPv6
ABC&S	Always Best Connected and best Served	CN	Correspondent Node
ABNF	Augmented Backus-Naur Form	CoA	Care-of Address
AI	Artificial Intelligence	CoS	Class of Service
AN	Access Network	CS	Circuit Switching
ANP	Access Network Provider	CSMA	Carrier Sense Multiple Access
AP	Access Point	CSMA/CA	CSMA with Collision Avoidance
API	Application Programming Interface	CSMA/CD	CSMA with Collision Detection
AR	Access Router	CWND	Congestion Window
ARP	Address Resolution Protocol	DAD	Duplicate Address Detection
ARQ	Automatic Repeat reQuest	DDDS	Dynamic Delegation Discovery System
BA	Binding Acknowledgement	DHCP	Dynamic Host Configuration Protocol
BU	Binding Update	DNS	Domain Name System
CBM	Consumer-centric Business Model	DoS	Denial-of-Service
		DRCP	Dynamic Registration and Configuration Protocol
		DSL	Digital Subscriber Line
		E-Mode	Enquiry Mode

LIST OF ACRONYMS

EDGE	Enhanced Data Rates for GSM Evolution	HoA	Home Address
ENUM	Telephone Number Mapping	HSDPA	High-Speed Downlink Packet Access
EVDO	Evolution-Data Optimized	IANA	Internet Assigned Numbers Authority
FA	Foreign Agent	ICC	Incoming Call Connection
FDD	Frequency Division Duplex	ICC-SE	ICC Service-Supporting Entity
FDMA	Frequency Division Multiple Access	ICC-SP	ICC Service Provider
FHA	Foreign Home Agent	ICM	Intelligent Call Manager
FIFO	First-In-First-Out	ICMP	Internet Control Message Protocol
FMC	Fixed Mobile Convergence	IEEE	Institute of Electrical and Electronic Engineers
FMIP	Fast Handovers for Mobile IP	IETF	Internet Engineering Task Force
FSRA	Fast Solicited Router Advertisement	IPSec	IP Security Protocol
GGSN	Gateway Support Node	IPv4	Internet Protocol Version 4
GOP	Group of Pictures	IPv6	Internet Protocol Version 6
GPL	GNU Public License	IS-95	Interim Standard 95
GPRS	General Packet Radio Service	ISM	Industrial, Scientific, and Medical radio bands
GSM	Global System for Mobile communications	ISP	Internet Service Provider
GTP	GPRS Tunnelling Protocol	ITU-T	International Telecommunication Union Telecommunications Standardization
HA	Home Agent	L2	Layer 2 or Data Link Layer
HARQ	Hybrid Automatic Repeat Request	L3	Layer 3 or Network Layer
HAWAII	Handoff-Aware Wireless Access Internet Infrastructure	LCoA	Local Care-of address
HMIPv6	Hierarchical Mobile IPv6	LMA	Localised Mobility Agent

LIST OF ACRONYMS

LMM	Localised Mobility Management	PR-SCTP	Partial Reliability SCTP
MAP	Mobility Anchor Point	PS	Packet Switching
MIH	Media Independent Handoff	PSNR	Peak Signal-to-Noise Ratio
MIP	Mobile IP	QoE	Quality of Experience
MMC	Mobile-Mobile Convergence	QoS	Quality of Service
MMS	Multimedia Message Service	R-Mode	Redirection Mode
MOS	Mean Opinion Score	RFC	Request For Comments
MPEG4	Moving Picture Experts Group 4	RO	Route Optimisation
MPLS	Multi Protocol Label Switching	RR	Resource Record
MT	Mobile Terminal	RS	Router Solicitation
MUSE	Mobile Ubiquitous Service Environment	RTCP	Real-Time Transport Control Protocol
NA	Neighbour Advertisement	RTO	Retransmission TimeOut
NAPTR	Naming Authority PoinTeR	RTP	Real-time Transport Protocol
NAT	Network Address Translation	RTT	Round-Trip Time
NIC	Network Interface Card	SACK	Selective Acknowledgment
OWA	Open Wireless Architecture	SBM	Subscriber-based Business Model
PAR	Previous Access Router	SBM-ICC	SBM-based ICC service
PCA	Personal Call Agent	SCTP	Stream Control Transmission Protocol
PCS	Personal Communication System	SIGTRAN	Signaling Transport
PDU	Protocol Data Unit	SIP	Session Initiation Protocol
PESQ	Perceptual Evaluation of Speech Quality	SLA	Service Level Agreement
PPP	Point-to-Point Protocol	SOA	Start Of Authority

LIST OF ACRONYMS

SRV	Service Record	URI	Uniform Resource Identifiers
SS7	Signaling System No.7	URL	Uniform Resource Locator
SSTHRESH	Slow-Start Threshold	User-DB	User Database
TDMA	Time Division Multiple Access	VoIP	Voice over IP
Teleservice	Telecommunication services to encompass all network services	WBC	Wireless Billboard Channel
TSPs	Teleservices Providers	WBC-SP	WBC Service Provider
TTL	Time-to-Live	Wi-Fi	Wireless Fidelity Alliance
UAC	User Agents Client	Wi-MAX	Worldwide Interoperability for Microwave Access
UAS	User Agent Server	WLAN	Wireless Local Area Network
UCWW	Ubiquitous Consumer Wireless World	WMAN	Wireless Metropolitan Area Networks
UDP	User Datagram Protocol	X.509	ITU-T framework for provision of authentication services by means of certificates
UMA	Unlicensed Mobile Access	XML	eXtensible Markup Language
UML	User Mode Linux		
UMTS	Universal Mobile Telecommunications System		

If you want a thing done, go - if not, send.

— Benjamin Franklin (1706 - 1790)

1

Introduction

This thesis is focused on a novel consumer-oriented Incoming Call Connection (ICC) service. This chapter first presents the historical background and the current trend in the communications industry. It then proceeds with an overview of the ubiquitous consumer wireless world (UCWW) established over the Consumer-centric Business Model (CBM) and the associated CBM-based ICC service. The motivation and objectives of this research follow after that. Then the main contribution of this research is given. In the end, the outline of this thesis is presented.

1.1 Background

The technological and infrastructure innovations for modern telephony had been pushed forward for over a century since Alexander Graham Bell [12] invented the first telephone in 1876. The era of the voice communication started from the development of Public Switched Telephone Networks (PSTNs), which originally was known as a fixed-line analog telephone system with full duplex conversation, narrowband speech and circuit switching (CS). Though it is very common today, cellular networks did not become attractive when it was born. It had taken more than 30 years to go through the first call made by mobile handheld to today's third generation (3G). It is very interesting to note

that the history of the mobile communications is named by a "generation" terminology. The first generation analogue cellular system was designed for voice telephony, and did not achieve market success due to the lack of roaming and coverage, poor battery life-time, heavy terminals and relative high cost. In recent years, the mobile communications market had enjoyed impressive growth owing to the proposed standards for the second generation (2G) digital system. There were several standards for 2G, such as Global System for Mobile Communications (GSM¹), Interim Standard 95 (IS-95²), and Personal Digital Cellular (PDC³), etc. The one that dominated the market was GSM with over 3.5 billion subscribers worldwide covering more than 85% of the global mobile market [13]. GSM provides many benefits, such as CS connections to carry low-bit-rate coded speech and Short Messaging Service (SMS). More importantly, users may have coverage virtually everywhere; especially the users are allowed to use the mobile services abroad under the existing international roaming agreements. The success of 2G mobile system had prompted the development of third-generation (3G) mobile systems. The most successful one was Universal Mobile Telecommunications System (UMTS⁴) based on the WCDMA [14]. Since it has been launched publicly, commercial 3G mobile systems are expected to provide higher-data-rate services multimedia services. Although CS technology has been used at the very beginning of telecommunication, 3G networks are proposed to evolve into a more efficient packet-switched (PS) domain, where Internet Protocol (IP) based core network is adopted to allow users do virtually everything on the Internet via data connections. With the aid of advanced mobile terminals (MTs), 3G networks are increasingly supporting more attractive wireless data services, e.g. Multimedia Messaging Service (MMS), online radio and music, and video telephony, etc.

Besides telephony, the Internet is another main technology that has revolutionized the way on how people communicate with each other in the modern civilization. The proliferation of personal computing devices led to a dramatic Internet growth in last decades. The key

¹ TDMA-based System originally from Europe but used in almost all countries.

² The first CDMA-based digital cellular standard pioneered by Qualcomm.

³ TDMA-based used exclusively in Japan.

⁴ UMTS is specified by 3GPP as a part of the global IMT-2000 standard for 3G mobile communications technologies. The most popular mode of UMTS makes use of W-CDMA [14] as the underlying air interface but the system also contains TD-CDMA and TD-SCDMA .

driver for the Internet is the TCP/IP protocol suit, which creates an open and common platform to improve the innovation of flexible services. With the intensive research and development, IP technologies have been greatly improved in terms of the network-layer routing, signaling and transporting of real-time streams, mobility management, network security, QoS⁵ and QoE⁶. The Internet has become capable to provide a variety of useful services, such as, World Wide Web (WWW), email, instant messaging, etc. In addition, there are a great number of new services are coined due to the wide openness of protocol suits that can be accessed for any service developers. In the early-1990s, researchers discussed to support telephony functions via the Internet. The industrial and market did not show any interests until a number of international standards bodies launched a group of protocols, e.g. H.323⁷ [15] and Session Initiation Protocol (SIP) [16]. This had promoted the developments of Voice over IP (VoIP), which refers as the digitization of voice streams and transmitting the digital voice as packets over conventional IP-based packet networks [17]. With the advent of those technologies, the transmission of voice traffic over a PS network becomes more and more efficient. However, it has introduced a number of challenges on management and handling of voice traffic over IP network [18]. One typical example is the problem raised from the QoS guarantees for real-time services over heterogeneous wireless networks, i.e., the special requirement on latency and jitter is more important in real-time services rather than the bit rate requirements.

The exponential growth of the Internet gave a strong impetus to provide the Internet access to mobile networks. Initially GSM (2G) was designed to provide 9.6 kbps data rate over fixed rate circuit switched links. This was enhanced by 2.5G systems such as General Packet Radio Services (GPRS⁸) with up to 114 kbps [19]. This was improved by

⁵ Quality of Service (QoS) defines how well the network performs its task, that is, transporting packets between the users' end-points in terms of objective quantities such as delay, loss, throughput and similar.

⁶ Quality of Experience (QoE) defines how well the users perceive the service offered by the network. It is more user-centric than QoS and there is a mapping between QoS and QoE.

⁷ The ITU-T recommendation that defines the protocols to provide audio-visual communication sessions.

⁸ General Packet Radio Services (GPRS) is a packet oriented mobile data service between the 2G and 3G. It gives regular speed data transfer by using empty TDMA channels.

the Enhanced Data rates for GSM Evolution (EDGE⁹), which uses 8PSK to improve the maximum bit rate and is capable to provide up to 236.8 kbps [19]. UMTS with Dedicated Channel (DCH) mode was referred as 3G to support up to 384 kbps and beyond [20]. It was further enhanced by the introduction of High Speed Downlink Packet Access (HSDPA¹⁰), which uses QPSK and 16-QAM modulation to support download rates of up to 14.4 Mbps per host [21]. Currently 3G Partnership Project (3GPP) had proposed a new standard towards Long-Term Evolution (LTE¹¹) to provide a high-data-rate, low-latency and packet-optimized radio access technology supporting flexible bandwidth deployments [22]. In parallel to the circuit switched links provided for narrowband voice telephony, an increasingly higher speed packet access to the Internet is offered over various radio access networks. Another key enabler is the Wireless Fidelity Alliance (Wi-Fi¹²) that provides a shared radio media for users to communicate with each other. In recent years, our mobile landscape is rich in Wi-Fi "hot-spot", providing higher speeds and cost-effective wireless connectivity and more flexible deployment. Today, it is common to see the deployment of Wi-Fi technologies in private, public, and commercial business. The most widely adopted Wi-Fi standard around the world is IEEE 802.11. As shown in Table 1.1, Wi-Fi typically uses the unlicensed Industrial, Scientific, and Medical (ISM) radio frequency bands, such as 900-MHz band (902-928 MHz), 2.4-GHz band (2400-2483.5 MHz), and the 5.7-GHz band (5725-5850 MHz). Beside the frequency, IEEE 802.11 also defines a family of standards, which define the physical layer (PHY) and the Medium Access Control (MAC) layer, network architectures, the security, and QoS.

Although the Internet Engineering Task Force (IETF) originally designed IP protocol for fixed networks, we have seen the dramatic increasing of IP application on wireless networks, i.e., UMTS Release 5 has claimed an all-IP architecture for UMTS to integrate IP

⁹ Enhanced Data rates for GSM Evolution (EDGE) allows enhanced data transmission rates by introducing advanced techniques on coding and transmitting data.

¹⁰ High Speed Downlink Packet Access (HSDPA) is an enhanced 3G system supporting high-speed data transmissions using WCDMA.

¹¹ Long-Term Evolution (LTE) is a project of the 3GPP toward the 4th generation of radio technologies intended to increase the efficiency and speed of mobile telephone networks.

¹² Wireless Fidelity Alliance (Wi-Fi) aims to improve the interoperability of WLAN products based on the IEEE 802.11 standard.

Table 1.1.: The IEEE 802.11 standard.

IEEE 802.11	RF Frequency	Channels	Data Rates
a	5.2 GHz	22	6, 9, 12, 18, 24, 36, 48, 54 Mbps
b	2.4 GHz	14	1, 2, 5.5, 11 Mbps
g	2.4 GHz	14	1, 2, 6, 9, 12, 18, 24, 36, 48, 54 Mbps
n	2.4 GHz, 5.2 GHz	22	Up to 300 Mbps

and wireless technologies [23]. It is a consensus that all IP network is the main trend for next generation wireless systems. The reasons could be explained as follows. First, IP is more suitable for supporting the rapidly increased data and multimedia services. Second, it is independent of the lower-layer protocols. This is especially important for supporting mobile services over different radio technologies. Third, its openness and flexibility provides a proven successful platform to foster future mobile services. However, there is still a lot of room for improvement for the IP protocol (including its mobile versions) in order to be properly deployed over wireless networks. There are some serious limitations, especially in terms of mobility management, signaling and control of real-time streams, network security and QoS.

Over the last few years, we have witnessed that a variety of wireless technologies have been deployed. At the same time Wi-Fi and Wi-Max¹³ technologies become widely available to common people. This leads to a dramatic development in the mobile phone industry. There are an increasing number of mobile terminals, such as PDAs¹⁴, smart phones, micro PCs, and laptops, etc, that are designed to connect to the Internet. We have seen that the commitment of all the major worldwide vendors to multi-mode terminals has

¹³ Worldwide Interoperability for Microwave Access (Wi-Max) is a WMAN telecommunications technology that provides wireless transmission of data using a variety of transmission modes.

¹⁴ Personal Digital Assistant (PDA) is a smart mobile device which functions as a personal information manager.

greatly accelerated the growth of the multi-mode handset market. Many equipment vendors have already developed multi-mode terminals, which are able to access at least two different network interfaces (e.g. GSM and Wi-Fi/Wi-Max) enabling them to connect to the corresponding radio access networks. The multi-mode terminals will soon be highly reconfigurable and capable to accommodate various transport technologies. This trend will continue for the foreseeable future. As shown in Figure 1.1, the globe dual-mode Voice over IP (VoIP) phone drives the worldwide mobile market, which grows significantly to almost 35-40 million handsets by 2009. The explosion of multi-mode terminals have driven the development of a flexible service to adjust the access technology and activate the appropriate profile, in order to be connected with the most appropriate available access network at all times. The benefits of such services include user-driven operations, efficient cost, large bandwidth, etc.

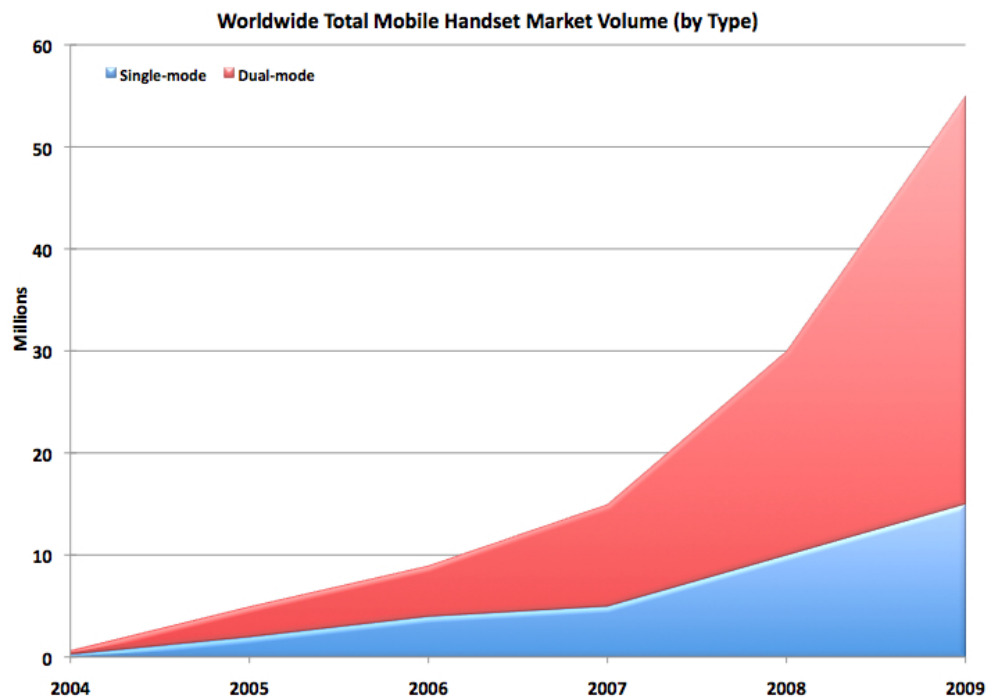


Figure 1.1.: The dual mode mobile terminal market volume growth published by Disruptive Analysis [1] in June 2005. It is shown that the globe dual-mode VoIP phone drives the worldwide mobile market and grows significantly to almost 35-40 million handsets by 2009 [2].

Bearing in mind all of the above, where will the telecommunication systems go in future? It can be anticipated that the current trend of wireless networks is toward the ubiquitous consumer wireless world (UCWW) [24]. In this, many different technologies, such as Wi-Fi, UMTS, HSDPA, EVDO¹⁵, Wi-MAX, LTE will exist simultaneously around the mobile users in different range of areas. Many researchers accept that in the UCWW connectivity will be available at anytime, anywhere and anyhow, and services will be rapidly deployed on-demand, customized to the user's needs, and adapted to the current wireless and connection environment, in the best possible way, independent of the users' movement across heterogeneous access networks. It is foreseen that UCWW will provide enormous benefits, for instance, multimedia services, global mobility, service portability, user number portability, interoperability, support of different terminals and greater competition among network and service providers. Since different networks have different performances, coverages, and prices, a great opportunity will be offered to the users to choose the best network and best teleservice. As heterogeneous approach is able to achieve extremely large coverage and ultra broad bandwidth at a reasonable cost, the users are allowed to be in some sense Always Best Connected and best Served (ABC&S) [25, 26] based on different service requirements and radio environments. The UCWW is being enhanced with interoperability of different Access Network Providers (ANPs) and Teleservices Providers (TSPs), which compete aggressively with each other in both traditional Internet and multimedia service markets to provide ABC&S experience. The mobile terminals (MTs) in UCWW will utilize the multi-mode technology and be highly intelligent, reconfigurable and capable to accommodate various ANPs' and TSPs' service offerings. This provides the possibility to choose between the increased number of available ANPs and TSPs with new advanced services such as live voice and video telephony and so on.

¹⁵ Evolution-Data Optimized (EVDO) is a telecommunications standard for the wireless transmission of data by means of radio signals, generally for broadband Internet access. It takes advantage of multiplexing techniques such as CDMA together with TDMA to increase the overall system throughput.

1.2 Overview

The UCWW concept is viewed as a heterogeneous wireless environment where various Access Network (AN) technologies can coexist and different ANPs and TSPs compete with each other to provide personalized and customized services. It represents a paradigm shift in the approach towards evolving future wireless networking environment from being subscriber-based and network-centric one to being consumer-centric. The business foundation of UCWW is established on the Consumer-centric Business Model (CBM) [27], which is seen as a natural evolution and an alternative to the traditional Subscriber-based Business Model (SBM). The novel UCWW infrastructural ideas include new services and network entities such as trusted third-party authentication, authorization and accounting (3P-AAA) [28] service and its providers (3P-AAA-SPs), access-network independent incoming call connection (ICC) service and ICC service providers, wireless billboard channels (WBC) [29] and their service providers, a consumer identity module (CIM) card [9] to replace the present subscriber identity module (SIM) card in mobile units, and a new network-independent and device-independent personal address class.

In the light of existing networks and the history of networking, CBM-oriented ICC (CBM-ICC) [30, 31, 32, 33] service is deemed as a key service and one of the most important developments towards the new UCWW environment. The definition of CBM-ICC service not only includes the traditional speech-oriented communications but also the multimedia communications like SMS, MMS, and video telephony. The initial idea is to provide the users with freedom of choice in relation to whom they get what service from and when. Users will move back and forth anytime-anywhere-anyhow among access networks for any and all services. They may opt out of having any long-term ANP relationship, or may have several, simultaneously and without conflict, with many different ANPs. CBM-ICC promises spin-off benefits such as full mobility for users among networks (e.g., among the various generations and types of pervasive cellular networks and fixed networks); user-driven integrated heterogeneous networking and ABC&S experience; a much more open market for new wireless ANPs; and an elimination of roaming charges. This will empower the consumer to dynamically associate with a number of ANPs simultaneously,

and to choose the best ANP for each particular type of incoming call according to the caller's type, callee's location and preferences, and time/day/week configurations.

Apart from allowing users to move round and be tracked by the caller, mobility in UCWW also means to roam vertically among different access networks and providers. More importantly, only one identification is needed for mobile users. Mobile users are associated with a unique number (IPv6 personal address). Users are not permanently tied to any ANP and may choose the best available ANP for each particular teleservice in accordance with the ABC&S paradigm. The permanent IPv6 address will allow mobile user to receive the incoming call wherever they go and through the any access network chosen by the user and with the any mobile terminal currently in use. Moreover, due to the ubiquitous Consumer-centric Business model, the roaming costs will be eliminated to the benefit of all mobile users. Since it is economic to transfer data packets in all-IP networks, the connection cost and conversation cost are also largely reduced. Another major benefit of the CBM-ICC in the UCWW is the intelligent call management system. Therefore, the mobile user will be able to define his/her own profile based on different roles and the incoming calls can be filtered by the system based on time, location, and profile.

The CBM-ICC service is also supported by a more advanced billing and accounting system. The legacy SBM-based ICC service uses a simple billing scheme by charging users based on the call duration or transferred data volume, etc. However, in the CBM-ICC service the users are no longer locked to only one ICC-SP, but associate to a number of service providers at the same time. It is inconvenient for a consumer to waste time handling all the financial transactions involved with multiple service providers. Instead, the proposed 3P-AAA-SP [28] can be involved to formulate one single billing method that covers all the billing involved. This new 3P-AAA service is designed with a new business architecture, accounting processes, and accounting data maintenance in order to handle billing schemes, which may be used for different types of services and all the different charging schemes [34].

Figure 1.2 shows a possible scenario, where a mobile user is looking for a CBM-ICC service in the UCWW. His/her mobile terminal may simultaneously connect to different ANPs via different wireless systems. These wireless systems may include the cellular

networks like GSM or UMTS with large coverage areas but limited bandwidth for data transfer, or other technologies like IEEE 802.11a/b/g/n or Wi-MAX that provide higher data rates but limited transmission ranges. A typical usage example is for a user to use a lower cost, lesser QoS access network (e.g., Wi-Fi) for personal/family VoIP calls, another access network (e.g., UMTS) for business calls requiring the best QoS available, and a third one (e.g., GSM) for international calls to/from specific countries because of special rate arrangements. The present limited clumsy solutions are made redundant, e.g., having multiple SIM cards. Roaming can be even better supported in the new CBM-ICC approach and roaming costs are all but eliminated because users will appear always as 'local' to each ANP from whom they receive communication services.

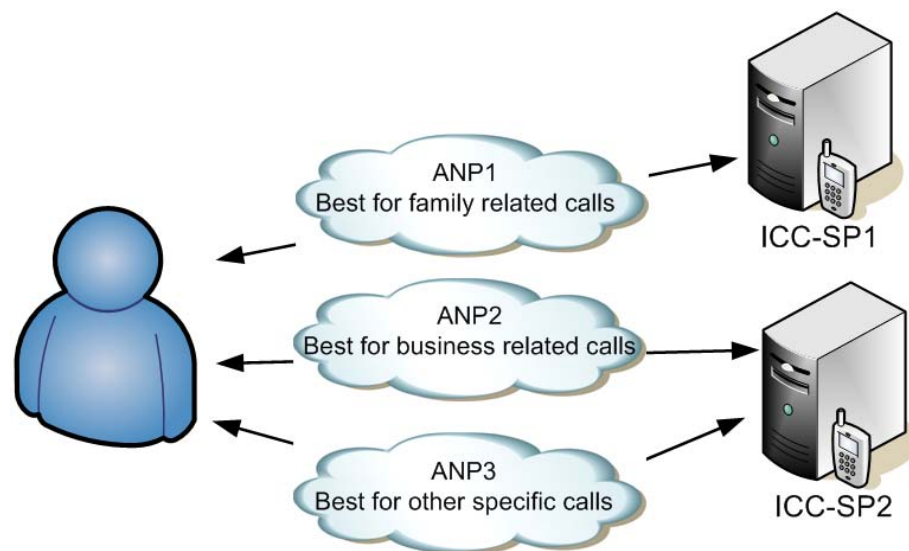


Figure 1.2.: A high-level view of the CBM-ICC scheme where a mobile user may be simultaneously accessible through various ANPs and ICC-SPs.

1.3 Motivation

There are several new services that have been proposed in the market to establish cost-efficient voice communication over the Internet in the past years. Skype [35] is one of the most popular and successful application with tremendously increased number of users. Other solutions based on VoIP architecture such as Gizmo [36] and Ekiga [37] also receive

a lot of attentions. However, to the best of our knowledge, those existing architectures are still constrained by subscribed relationship within SBM context, and lack support for the multi-access scenario and access network change from one ANP to another ANP. Though the SBM still dominates the market, there are many deficiencies both on a technical and business level. One major problem for SBM based services is the costly roaming fees. Therefore, the traditional SBM based service is no longer suitable to heterogeneous wireless networks environment, and a truly consumer-oriented service is required to meet the growing demand for the convergence of existing and newly developed fix and wireless systems. Some publications has introduced a potential for transition to the CBM, for example, [38] which presented a generic architecture for integrated systems and [39] which proposed a policy-based framework to support the integration of 4G networks. This trend raises a new service direction in various research areas, such as mobile terminal and architecture level, and also motivates us to design a novel service with flexibility and user customization to meet the growing demand for the convergence of existing and newly developed fix and wireless systems.

The upcoming UCWW calls for the integration and interoperation of various kinds of access technologies in an IP-based infrastructure. It is expected that mobile users in the UCWW will be capable of selecting the best access communication service and dynamically associate with a number of ANPs in a simultaneous manner. Since different systems have their own merits and defects, combining the advantages of these heterogeneous networks is a challenging task for the next generation of mobile communication systems. The changes in business modes and consumer's behaviors in UCWW also open up a wide range of new technological research ideas, including the emerging CBM-ICC service aiming at a new autonomous mobility and call control architecture (open and partially controlled by the user), which will better meet user's ABC&S requirements. One motivation for this research is to present a solution for a truly ANP-independent service with a user's ability to dynamically switch to the most desirable ANP in the middle of a service session without disruption of the ICC service. Many similar ideas has been discussed in several previous studies, e.g., [40] has proposed a novel architecture for ubiquitous mobile communication using a third-party interoperating agent and [41] has presented the

designing issues on the implementation of the architecture of future wireless communication system as Mobile Ubiquitous Service Environment (MUSE). The main difference for utilizing CBM-ICC service spawns from its ability to achieve Hot Access network Change (HAC¹⁶) [24]. Although mobility management is widely investigated, to the best of our knowledge, there is no mobile infrastructure or service, which is truly ANP-independent with dynamic HAC switching to the most desirable ANP. In this thesis, we attempt to develop a CBM-ICC framework by integrating the HAC to keep seamless service continuity when transitioning among various access technologies across different networks without loss or disruption of the ICC service. This HAC approach concerns on a more flexible and effective mobility scheme for real-time multimedia services across heterogeneous networks. However, some other aspects and application areas, such as AAA, are also covered in the project to some extent, but will not be described further in this thesis.

1.4 Thesis Contribution

The contributions of the thesis may be summarized as follows:

- A critical survey of relative protocols with exploring their suitability for use in the CBM-ICC service is provided. The potential protocols are analyzed in the context of building a CBM-ICC service in terms of transport, signaling and mobility support. Previous proposals for mobility management are presented and compared.
- A proposal for a CBM-ICC service with autonomous mobility and call control architecture is made. A CBM-ICC service with two different operational modes is proposed. Finally the addressing issues are examined. Issues related to a personal IPv6 address scheme, a Contact Address Identifier (CAI), and a Consumer Identity Module (CIM) are investigated.

¹⁶ Hot access network change (HAC) is analogous to the handoff concept, but its structure as a user-driven integrated heterogeneous network, the reasons for it, and the consequences of it are quite different, so a different term is needed. A typical ABC&S reason for HAC would be the availability of a better access option and offer for the same teleservice from another access network.

- A CBM-ICC framework and architecture supporting the heterogeneous UCWW environment and the consumer-driven ABC&S paradigm realization is proposed. The main components and interfaces relying on existing protocols or requiring new signaling protocols (or modification/new elements of existing protocols) are discussed and explained.
- Relative communications scenarios and signaling flows with suitable protocols in line with this architectural framework are proposed and elaborated. A generic CBM-ICC service scenario is described, which shows how CBM-ICC service offers mobile users greater flexibility and management control over incoming calls, and enables users to receive incoming calls via multiple access networks/providers.
- A user-driven, seamless, network-transparent Hot Access network Change (HAC) scheme is proposed. A HAC switching approach at the transport layer is suggested to provide better performance for real-time services.
- A CBM-ICC proof-of-concept system-level testbed is developed. The main components of the CBM-ICC service infrastructure are implemented. A software for the evaluation of the HAC scenario is developed.
- Evaluation of the performance of CBM-ICC service based on the system-level experimental testbed is completed. Both the signaling performance and the HAC performance are assessed. The signaling performance is tested in terms of the delay in five signaling phases. The HAC performance is evaluated on data, voice and video streaming services regarding throughput, delay and jitter, in the testbed environment. The performance of the two operational modes is compared.

A list of author's publications related to this research is provided in Appendix A.

1.5 Thesis Outline

The structure of this thesis is organized as follows.

Chapter 2 describes the potential works and protocols that are suitable to build the CBM-ICC service. This chapter analyzes the basic Internet protocols. It proceeds to describe

two transport layer protocols: the Stream Control Transmission Protocol (SCTP) and Real-time Transport Protocol (RTP). A signaling protocol, Session Initiation Protocol (SIP), is also introduced. Then previous proposals for mobility management are presented and compared.

Chapter 3 reviews the recent work that is relevant to the CBM-ICC service. This chapter analyzes the other related service and compares them with the CBM-ICC service. It proceeds to describe the related projects within academia, and related work within standardization organizations and industry. Related work in the area of mobility management for next generation all-IP-based wireless systems is also presented.

Chapter 4 gives an overview of the general operation of the emerging CBM-ICC service. This chapter provides a broad overview of the consumer-oriented CBM-ICC service, including the background, objectives and key innovations. It presents the main benefit and new features of the CBM-ICC service. It then describes the operational demonstration of the CBM-ICC service. An outline of two different operational modes is provided. The addressing issues are also examined.

Chapter 5 proposes a new CBM-ICC service architecture and describes its main functional entities. Then the main components and interfaces relying on existing protocols or requiring new signaling protocols (or modification/new elements of existing protocols) are described and protocol candidates are suggested. The problem of the hot access network change is identified and the introduction of SCTP as the solution for HAC is motivated.

Chapter 6 examines a generic CBM-ICC scenario and the involved signaling. It describes the category of different mobility and explains how it can be used to support the mobile user. It then elaborates the signaling flows for the scenario in both operational modes.

Chapter 7 describes the implementation of the proof-of-concept system-level testbed. It gives an overview of the experimental testbed. It elaborates main topics on building blocks for the CBM-ICC implementation to handle signaling and mobility management. The implementation issues raised in the HAC experiment are described.

Chapter 8 describes evaluation of the performance of CBM-ICC service based on the system-level experimental testbed. The evaluations of signaling performance and handoff

performance are performed separately. The two distinct operational modes are compared in respect of signaling and HAC performance for a number of key QoS parameters such as delay, jitter, throughput, etc.

Chapter 9 concludes the thesis together with suggestions for future work.

How do I work? I grope.

— Albert Einstein (1879 - 1955)

2

TCP/IP Background: Relevant Protocols

2.1 Introduction

The trends mentioned in the previous chapter have profoundly changed the way we should choose solutions for the CBM-ICC framework. The focus of this chapter is placed on analyzing the relative protocols in the context of selection of the most promising candidates for the CBM-ICC service.

The CBM-ICC service is a novel way of providing an incoming call service over an IP-based mobile and fixed telecommunication infrastructures. It contains many aspects in terms of transport, signaling and mobility support. Section 2.2 overviews the layered communication model. Section 2.3 reviews the network-layer protocols. Section 2.4 describes two-transport layer protocols: the Stream Control Transmission Protocol (SCTP) and Real-time Transport Protocol (RTP). Section 2.5 outlines the relevant application-layer protocols, such as the Domain Name System (DNS) and Session Initiation Protocol (SIP), etc. Section 2.6 discusses previous proposals for mobility management and compares these mobility solutions.

2.2 Layered Communication Model

Given that the computer network is a complicated and integrated problem, it is common to see that the whole communication functionality is split into different layers in a protocol stack. Each layer provides a subset of communication functions to the higher layer via an interface and communicates with the corresponding layer (on another system) via lower layers. The benefits for having such layered protocol design are that each layer is only responsible for a specific task and the higher-layer only needs to know a well-defined interface to drive the lower-layer protocol.

The most popular example of a reference communication model, the Open Systems Interconnection (OSI) model [46, 47], was developed by the International Standards Organization as an abstract description for layered communications and computer network protocol design. However, the “layered” structure of the OSI model gives the unnecessarily complexity for protocol design. Instead, the TCP/IP [45] protocol architecture dominates the Internet communication. This is because that TCP/IP is mature and relative simple on the network layer. As shown in Table 2.1, this model has a 5-layer hierarchy consisting of an Application, Transport, Internet, Link, and Physical Layers.

2.3 Network-Layer Protocols

2.3.1. Internet Protocol Version 6 (IPv6)

The current version of Internet Protocol, known as version 4 or IPv4 [48] was proposed in 1981. Although had proven to be robust, the initial design of IPv4 did not anticipate the exponential growth of the Internet. The 32-bit IP address space was not enough for the size of today’s Internet, needless to say for the future. The exhaustion of the IPv4 address space requires a new successor to the IPv4 protocol. Thus the IETF worked on new specifications for the IP version 6 (IPv6) [49]. In addition, the IETF also had specified the general requirements for implementing IPv6 on a network host [50] and Advanced Sockets Application Program Interface (API) for IPv6 [51].

2.3 Network-Layer Protocols

Table 2.1.: The TCP/IP model.

Layer	Name	Description
Layer 5	Application Layer	Contains application services such as Telnet, Hypertext Transfer Protocol (HTTP) [42], File Transfer Protocol (FTP) [43], and Simple Mail Transfer Protocol (SMTP) [44].
Layer 4	Transport Layer	Provides complete and transparent data transfer between end-points. The end-to-end error control and flow control are implemented at this layer.
Layer 3	Internet Layer	Provides routing functions to transmit data from one end-point to another end-point over the Internet. The IP protocol is working at this layer [45].
Layer 2	Link Layer	Not specified. Provides logical interface between the end-point and network. Link protocols operate only between adjacent network nodes.
Layer 1	Physical Layer	Not specified. Handles the physical aspects of the media being used to transmit the data. It conveys the bit stream into electrical, light or radio signal. Also defines modulation and encoding of data bits on carrier signals.

The key objective for IPv6 was to adopt a relative large IP address space, that is, 128 bits, which is the major difference between IPv4 and IPv6. A 128-bit address field in IPv6 is expected to be sufficient to cover everything needed as an IP address [52]. With the enlarged address space, every IP-based device or machine can have at least one globally unique IP address. The IPv6 header format is shown in Figure 2.1, where the details are described below:

- *Version*: specifies IP version (IPv4 or IPv6).
- *Traffic class*: specifies Internet traffic priority delivery value.
- *Flow label*: used for specifying special router handling for a flow of packets.

which allows an entire subnet to move to a new router connection point without renumbering.

- Another important feature of IPv6 is that all nodes have a configuration mechanism, namely a stateless address autoconfiguration [57], which allows a node to automatically assign a suitable address for itself. The autoconfiguration procedure could be explained as follows. When a network node uses autoconfiguration to obtain a link-local address based on the network interface identifier, i.e. the Media Access Control (MAC) address, a Duplicate Address Detection (DAD) [58] is performed to ensure that no other node has the same link-local address. The link-local address consists of a link-local prefix FE80:0:0:0:0:0:0:0/64 prepended to the interface identifier. The link-local prefix is only recognized within the subnet, that is, routers will not forward these packets out of scope of the link. At the same time the node can initiate Router Discovery [59] in order to allow the node to start communicating as soon as DAD is finished.

2.4 Transport-Layer Protocols

2.4.1. Stream Control Transmission Protocol (SCTP)

2.4.1.1. SCTP Features

SCTP [66] was originally standardized by the Internet Engineering Task Force (IETF) SIGTRAN¹⁷ work group to transport Signaling System No.7 (SS7) [67, 68, 69, 70] signaling messages over IP networks. With intensive development, SCTP evolved to a general-purpose transport protocol that provides a reliable, full-duplex connection with advanced delivery options.

¹⁷ SIGTRAN is derived from signaling transport by the IETF working group that produced specifications for a family of protocols supporting the reliable datagram service and user layer adaptations for SS7 and ISDN communications protocols.

An SCTP end-point is the logical sender/receiver of SCTP packets. Before the communication starts, two end-points have established a logical connection, which is named an Association. SCTP uses chunk as the information unit to transport packets. SCTP chunk consists of a chunk header and chunk-specific content. RFC 2960 specifies 13 chunk types (more could be defined in future). Each chunk containing user data has a 32-bit Transmission Sequence Number (TSN). By using this, SCTP end-points can detect the duplication of the delivery and acknowledge the receipt of data chunks by sending a Selective Acknowledgement (SACK).

A list of SCTP's features compared to that of TCP and UDP is shown in Table 2.2. As a transport-layer protocol, SCTP shares many similar characteristics with TCP. However, SCTP offers many unique features that are not available in TCP. In addition to reliable ordered transmission, SCTP is also able to mark messages for out-of-order delivery. If no resequencing is required, unordered transport services can be used for important messages, which may bypass others, e.g., transaction abort messages of an application. SCTP also can set unordered flags on a per message basis according to the requirements of the application layer. Furthermore, SCTP also uses a 4-SACK rule to do "Fast Retransmission". Whenever the sender receives four consecutive SACKs from the receiver reporting the same data chunk missing, the data chunk is immediately retransmitted. SCTP has reduced the effect of the head-of-line-blocking by distributing the application-layer messages over several streams.

SCTP strengthens the security against the well-known "Denial-of-Service" [3] attacks by using 4-way handshake scheme for establishment of an SCTP association, which is different from the 3-way handshake mechanism of TCP. The SCTP 4-way handshake procedure is shown in Figure 2.2. The client sends an SCTP INIT chunk to the server for initiation of an SCTP association. The server will respond with the INIT-ACK chunk to the client, which contains 'cookie' information for security purposes. The client will then send the COOKIE-ECHO chunk to the server. The server completes the association establishment by sending the COOKIE-ACK chunk to the client. The advantage for this 4-way handshake scheme is that the SCTP server will allocate the relevant kernel memory for the connection from the client, only after receiving the third COOKIE-ECHO chunk. This will prevent the so-called "TCP SYN flooding" attack.

Table 2.2.: A comparison of SCTP with TCP and UDP (Source:[11]).

Feature Name	UDP	TCP	SCTP
Connection oriented	No	Yes	Yes
Reliable transport	No	Yes	Yes
Unreliable transport	Yes	No	Yes
Preserve message boundary	Yes	No	Yes
Ordered delivery	No	Yes	Yes
Unordered delivery	Yes	No	Yes
Data checksum	Yes	Yes	Yes
Checksum size (bits)	16	16	32
Path MTU	No	Yes	Yes
Congestion control	No	Yes	Yes
Multiple streams	No	No	Yes
Multi-homing support	No	No	Yes

Comparing to 4-way connection termination in TCP, SCTP uses the 3-way handshake mechanism for termination of an SCTP association, as shown Figure 2.3. The client sends a SHUTDOWN chunk to the server. The server responds with the SHUTDOWN-ACK chunk to the client in order to acknowledge the end of transmission. Finally, the client completes the association termination by sending the SHUTDOWN-COMPLETETION chunk to the server. The problem of “Half-Open State” in TCP is solved by this 3-way handshake mechanism in SCTP.

2.4.1.2. SCTP Protocol Data Unit (PDU) Structure

In general, the Protocol Data Unit (PDU) of SCTP is named as SCTP packets. As shown in Figure 2.4, a generic SCTP packet is composed of a common header and a variable number of chunks.

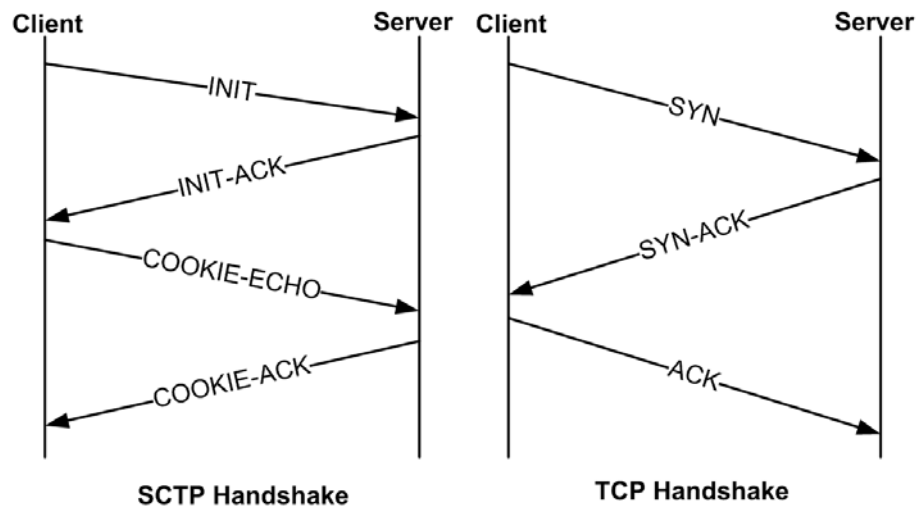


Figure 2.2.: The Sctp 4-way connection setup vs. TCP 3-way connection setup. Sctp uses a 4-way handshake to initiate a new connection, which may introduce additional delay but will protect against “Denial-of-Service” [3] attacks.

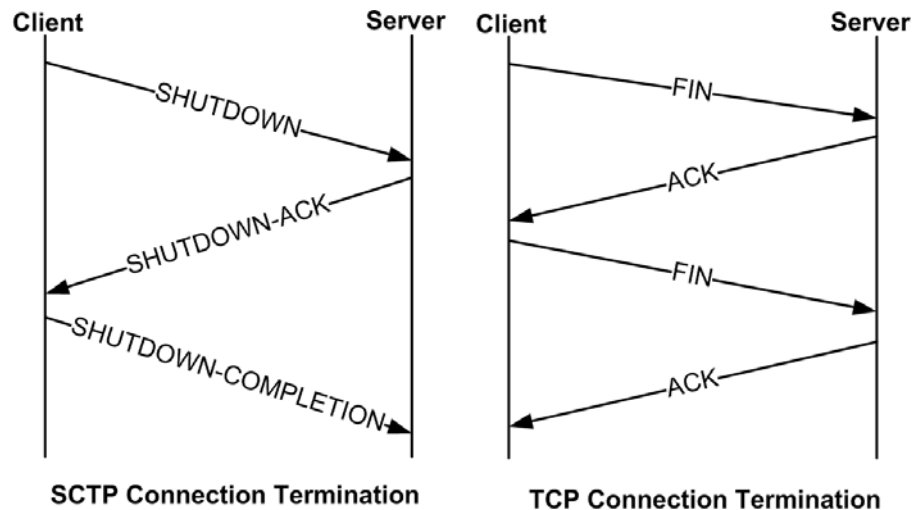


Figure 2.3.: The Sctp 3-way connection termination vs. TCP 4-way connection termination. Sctp employs a 3-way termination procedure to completely terminate the association. However, if an immediate shutdown is expected, Sctp needs to send an **ABORT** message.

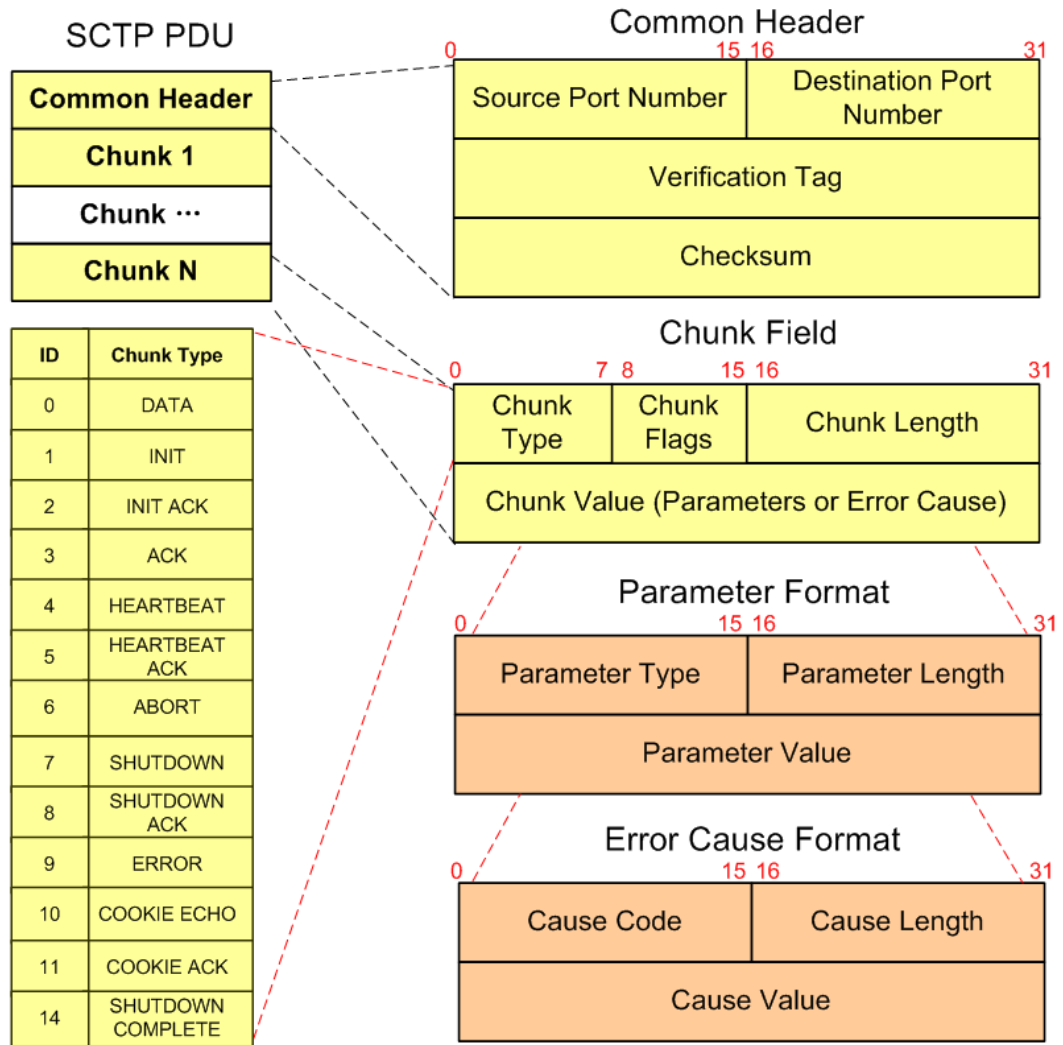


Figure 2.4.: The structure of the SCTP Protocol Data Unit (PDU) (Source:[4]). The standard SCTP PDU consists of a common header, and one or more chunks. The chunk could be either a control chunk or a DATA chunk, which is recognized by distinct chunk type. The DATA chunk contains the actual data payload incorporated with various flags such as transmission sequence number (TSN), and Stream Sequence Number (SSN). The format of control chunk varies depending on the chunk type.

The 12-byte SCTP common header is always at the beginning of the SCTP packet and consists of three basic fields:

- *Source/Destination port number*: used with Source/Destination IP addresses to ensure the receipt of the packet. SCTP uses the same port concept as TCP and UDP.
- *Verification Tag*: used with the Source/Destination Port to identify an SCTP association.
- *Checksum*: used to maintain the integrity of entire packet data and protect the data against transmission errors. Each SCTP packet has this 32-bit checksum, which is longer than the 16-bit checksum of TCP and UDP.

The common header is followed by one or more SCTP chunks, which may be either data chunks or control chunks. This format differs from TCP and UDP PDUs, which include control information in the header and offer only a single optional data field. As indicated in Figure 2.4, each chunk begins with a chunk header that contains the following fields:

- *Type field* is denoted by a number, which is used to distinguish data chunks and various types of control chunks. Some typical chunk types are listed in Figure 2.4.
- *Flags field* contains chunk specific flags.
- *Length field* defines the length of the chunk due to a variable length of different chunks.
- *Value field* contains the actual payload of the chunk.

A number of control chunks are defined for different control purposes, e.g., initiation, acknowledgements, monitoring reachability, termination, and errors. Some typical chunk types are explained concisely as follows.

- The Initiation (INIT), Initiation Acknowledgement (INIT ACK), State Cookie (COOKIE ECHO) and Cookie Acknowledgement (COOKIE ACK) chunks are used in the association establishment phase.
- The Shutdown (SHUTDOWN), Shutdown Acknowledgement (SHUTDOWN ACK) and Shutdown Complete (SHUTDOWN COMPLETE) chunks are used during the graceful termination of an association.

- The Payload Data (DATA) and the Selective Acknowledgement (SACK) chunks are used for the data transfer.
- The Heartbeat Request (HEARTBEAT) and Heartbeat Acknowledgement (HEARTBEAT ACK) chunks are used to track the state of the different network interfaces used in the association.
- The Abort (ABORT) chunk is used to report a fatal error and terminate the association.
- The Operation Error (ERROR) chunk is used to report a non-fatal error.

In addition, some control chunks are defined as protocol extensions for specific purposes. For example, RFC2960 [4] defines the Explicit Congestion Notification Echo (ECNE) and the Congestion Window Reduced (CWR) chunks. RFC3758 [71] defines FORWARD TSN chunks. RFC5061 [72] defines the Dynamic Address Reconfiguration.

2.4.1.3. Multi-streaming in SCTP

The Automatic Repeat reQuest (ARQ) [73] mechanism in TCP requires that data is delivered in a strict transmission order. If a PDU is not delivered in the original sequence, or gets lost, the retransmission mechanism will retransmit it until the lost one is fully recovered. However, if the packet loss rate is high in the connection, the performance suffers while waiting for the lost PDUs. This is known as the “Head-of-Line” (HOL)¹⁸ [74] blocking and can be avoided by the SCTP multi-streaming feature.

Multi-streaming refers to the capability of SCTP to transmit several independent streams of chunks in parallel. SCTP segments the data into chunks, which are then carried inside an SCTP PDU. Each SCTP PDU is assigned to one of several “streams” within an

¹⁸ The Head-of-Line blocking (HOL) is a phenomenon that appears in buffered telecommunication network switches. Due to the FIFO nature of the input buffers and switch design, the switch can only switch the packets at the head of the buffer per cycle. HOL arises when packets arriving at different input ports are destined for the same output port. If the HOL packet of a certain buffer at the input cannot be switched to an output port, the rest of the packets in that buffer are blocked by that HOL packet, even if there is no contention at the destination output ports for those packets.

association. At the initiation stage of an association, the number of available streams is exchanged between the sender and the receiver. All the data transferred in chunks has to be acknowledged using a scheme based on the SCTP option of Selective Acknowledgements (SACKs). All the PDUs within each stream are assigned with independent Stream Sequence Numbers (SSN), which are used at the receiver to determine the sequence of delivery. In-sequence delivery is performed in each stream in order to avoid HOL blocking within one association. The chunks can then be delivered in streams with their own characteristics, and largely independent from each other, as shown in Figure 2.5. This differs from TCP's byte-stream method, where several connections are established at the expense of additional cost and overhead.

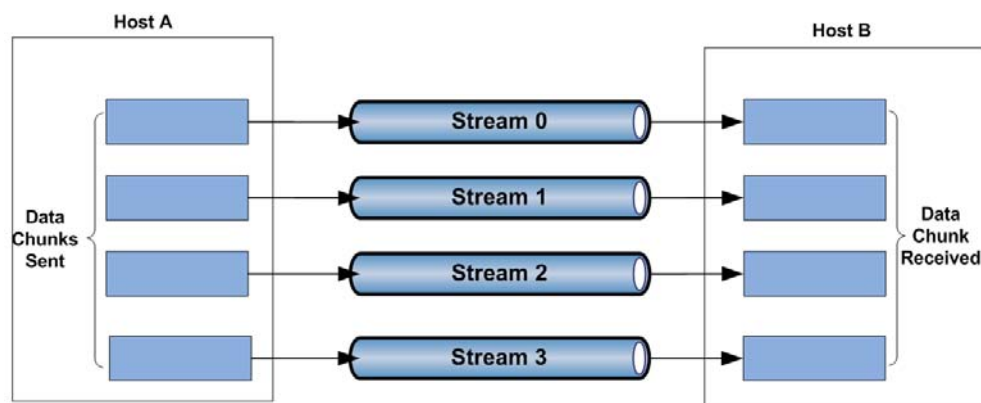


Figure 2.5.: The multi-streaming feature in SCTP. This unique function avoids HOL blocking by independently transmitting data in separated streams, and provides the flexibility on transferring diverse streams of data inside the overall SCTP message flow.

SCTP provides a flexible way to control the delivery of data depending on different streams. Each stream in SCTP can be defined as “Strictly-Ordered and Reliable”, or just “Reliable”, so that data will be delivered to the application as soon as it arrives. Newer versions of SCTP have also introduced another variation called “Partially Reliable”. SCTP also provides another feature that is similar to UDP. The message can be sent as “unordered”. When an unordered fashion is performed, it implies that the data is independent with respect to any other data sent previously. Thus the unordered message is immediately placed into the buffer upon arrival.

2.4.1.4. Multi-homing in SCTP

TCP assumes that each host has only one IP address for one connection, while SCTP introduces the possibility that an association is capable to have multiple IP addresses (or network interface cards) between two end-points as shown in Figure 2.6. At the setup of an SCTP association, each end-point includes a list of IP addresses that are available within the INIT chunk. Also port number and verification tag are included within this chunk. After receiving the INIT-ACK chunk, the end-points then accept a pair of valid addresses as the Primary Addresses, over which data chunks are transmitted by default. All other addresses are marked as secondary addresses.

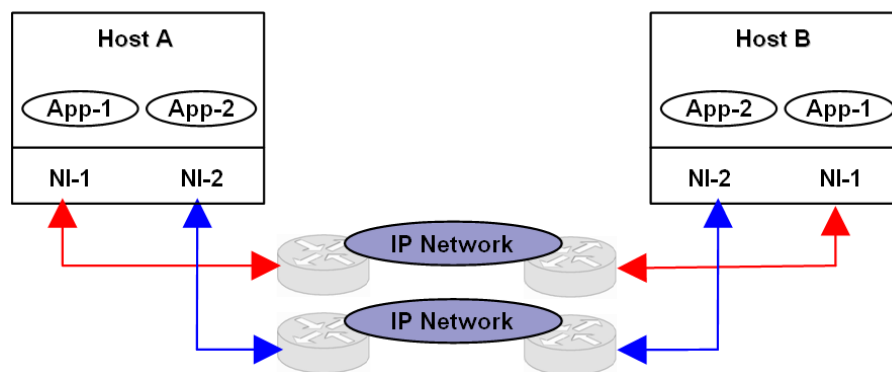


Figure 2.6.: The multi-homing feature in SCTP. This unique function enables an association have multiple IP addresses (or network interface cards) between two end-points.

SCTP regards each IP address as one transmission path towards its end-point. There are two major chunk types used by SCTP to manage the status of each path, namely, the SACK and HEARTBEAT chunks. First, the connectivity of the active path is checked by the SACK chunks, which are sent by the SCTP receiver as soon as it receives the DATA chunks from the SCTP sender. Second, the HEARTBEAT and HEARTBEAT-ACK chunks are used to periodically monitor the connectivity of the inactive path. For example, in receipt of the HEARTBEAT packets, the corresponding SCTP will send back a HEARTBEAT-ACK chunk to the original HEARTBEAT sender. In this way, the hosts can probe the connectivity of the inactive paths by checking the reception of the HEARTBEAT-ACK chunks.

In SCTP, the transmission status is monitored by sending HEARTBEAT chunks and recording error count of each path. If the transmission on a primary path fails repeatedly and the error count of this path exceeds the threshold, SCTP will retransmit the chunk to a secondary address. SCTP informs the user about the status of a transmission path if a transmission path changes its state. The user can also instruct the local SCTP instance to use another path as a primary path.

2.4.1.5. Reliable Transmission and Congestion Control

Reliable transmission is originally provided by TCP [75] as a strict order-of-transmission. SCTP inherits some ideas from TCP, such as a checksum used for detection of errors in the chunks, sequence number and selective retransmission mechanism. The Transport Sequence Number (TSN) is used to identify the loss and duplication of data chunks. In the case of error and loss, SCTP use a specific “Selective Acknowledgement” (SACK) [76] control chunk reporting all gaps in the sequence of data chunks.

In addition, SCTP has two different mechanisms for error/lost recovery, namely the timer-controlled retransmission and the fast retransmission.

The timer-controlled retransmission is based on a retransmission timer. The retransmission timeout (RTO) is derived from continuous measurements of the round trip delay. If the sent packet is not acknowledged by the receiver within a given period of time, the RTO will expire, which means that all unacknowledged data chunks should be retransmitted and the timer will start again but its value is doubled. Hence it is essential to discover a proper value of RTO. Smaller RTO is preferred to give a rapid recovery but it will also make packets to be mistakenly considered as lost when the round-trip time is suddenly increased. The typical value of RTO is suggested in [66] as one second. It is possible to choose a much lower value in relation to the round-trip time for specific environments.

Loss recovery in fast retransmit is largely based on the timer-controlled retransmission, except for the fastest loss detection in the reception of duplicate acknowledgments. The reason for receiving duplicate acknowledgments, which contain information about which packet was the last to be received in-order, is either that packets have been reordered in

the network, or that a packet has been lost, causing the subsequent packets to be out-of-order [77]. To disambiguate packet loss from unordering, SCTP requires that the fast retransmission should be invoked if sender receives four consecutive negative reports for the same data chunk (vs. three reports in TCP). In this case, the sender should immediately retransmit this data chunk. However, if the number of lost packets is less than four, the fast retransmit will not be triggered. The expiration of the retransmission timer would trigger the retransmission. In this way, fast retransmit triggers the retransmission in an early stage, and thus increases efficiency of loss detection and network resource utilization.

The congestion control mechanism in SCTP is performed in a similar way as TCP does. SCTP uses a CongestionWindow (CWND) to limit the rate at which the sender can transmit based on observed network conditions. The slow start mechanism is performed to determine the available capacity at the beginning of SCTP data transmission or after a sufficiently long idle period or when the loss is detected by the retransmission timer. Initially CWND is smaller than twice the MaximumTransmissionUnit (MTU). Every successfully acknowledged data increases the CWND by the amount of data that SACK acknowledged until it exceeds the Slow-Start-Threshold (SSTHRESH). Then SCTP enters the procedure of congestion avoidance. The SSTHRESH is used to distinguish between the slow start and congestion avoidance. If the CWND is smaller than the SSTHRESH, slow start is still in progress. Otherwise the mode changes to congestion avoidance, where the CWND should be incremented by the MTU per round-trip. However, if any packet loss is detected, the SSTHRESH is reduced to half of CWND and the CWND is set to this value.

2.4.2. Partial Reliability SCTP (PR-SCTP)

TCP – the classical Internet transport protocol – was designed to provide an ordered fully reliable transport service [78]. Many multimedia streams are tolerant with data loss but have strict latency requirements. For these applications completely reliable transport is not necessary and loss recovery mechanism can be cumbersome, as they might force the application to rely on the retransmission timer [79]. On the other hand, UDP is frequently used to provide transport-layer service with a low latency. However, the best effort service

of UDP may create troubles by continuously injecting data for large networks, which are already congested. This will make the network congestion worsen.

A flexible delivery mechanism with customized service on reliability is required for some applications that may be satisfied with partial reliability. In order to solve this problem, the Partial Reliability Extension of SCTP, also called Partial Reliable SCTP (PR-SCTP), is formally proposed as the RFC3758 [71], which defines that only some subsets of messages can be chosen for use in a SCTP association and the user can specify how reliable the transport service should be in attempting to send the message to the receiver through several independent streams within an association. A specified lifetime is defined in PR-SCTP to indicate a limit on the duration of time that the sender should try to retransmit the message. The data should not be retransmitted if its lifetime expires. Thus the bandwidth can be used to retransmit data the lifetime of which have not expired yet.

PR-SCTP inherits same loss recovery and congestion avoidance from normal reliable SCTP. The difference between PR-SCTP and normal SCTP lies in retransmission mechanism, i.e., PR-SCTP is capable of stopping retransmission of lost data chunks according to certain reliability threshold defined by upper layers. RFC 3758 defines a "timed reliability" for PR-SCTP, based on a Time-to-Live (TTL) options indicating how long a message is useful. If the TTL field in a SCTP chunk has not expired, the retransmission is carried on. If the TTL field in a SCTP chunk expires before it can be reliably delivered to the receiver, the particular data chunk is abandoned and should not be transmitted or further retransmitted. Then the sender notifies the receiver with a FORWARD TSN chunk to upgrade and advance its cumulative TSN point (otherwise the receiver is still waiting for those outstanding data chunks). On the receiver side, it only needs to recognize the FORWARD TSN chunk and to move the cumulative acknowledged point accordingly.

The general PDU structure of PR-SCTP is identical to that of the general SCTP PDU, except for the following two PR-SCTP protocol extensions:

- A new Optional Parameter Type (c.f. Figure 2.7) in the INIT and INIT ACK chunks used for association setup indicates whether the end-point supports PR-SCTP.

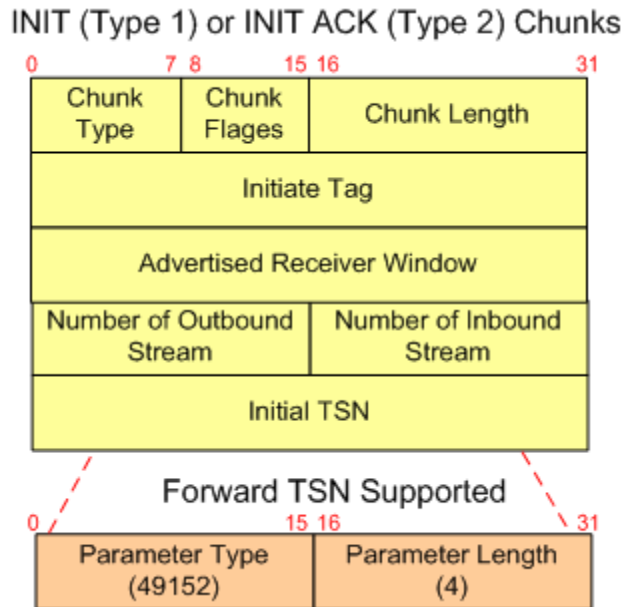


Figure 2.7.: The Optional Parameter Type in the INIT and INIT ACK chunks for PR-SCTP.

- A single new chunk type, FORWARD Cumulative TSN (c.f. Figure 2.8), indicates whether the receiver should move its cumulative ACK point forward to skip the outstanding DATA chunks that may not yet have been received and/or acknowledged.

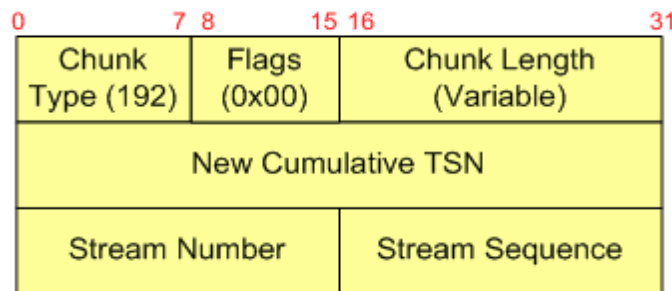


Figure 2.8.: The new Chunk Type (Forward Cumulative TSN) for PR-SCTP.

2.4.3. Real-time Transport Protocol (RTP)

RTP, first published as an IETF proposed standard RFC 1889 [80] and later replaced by the new version RFC 3550 [81], aims to provide end-to-end network transport functions

which are suitable for real-time applications, e.g. digital audio, video or data, over multi-cast or unicast networks.

Typically, RTP generally works on the top of the UDP protocol [82]. But other options are also available, such as RTP over TCP or RTP on non-IP networks. RTP over TCP [75] is standardized by RFC 4571 [83], but it is hardly used due to the inherent latency introduced by connection establishment and retransmission. Recently there have been a lot of discussions on running RTP over other transport protocols such as SCTP and Datagram Congestion Control Protocol (DCCP) [84].

RTP is usually used in conjunction with the Real Time Control Protocol (RTCP) [81], which periodically sends minimal control information on QoS parameters on the end-to-end basis. Then information transmitted by RTCP includes information for synchronization, participant membership and identification, etc. It also offers QoS feedback from receivers and synchronization between the media streams. This feedback mechanism allows RTP to adapt to current network conditions [85]. Moreover, it is capable to provide support for real-time conferencing of groups within the Internet.

In general, the RTP data packet consists of a header followed by a payload data. The header is 12 bytes for every data packet. The payload data can be either a video frame or several audio samples.

As shown in Figure 2.9, the following describes some of the important fields of the RTP header:

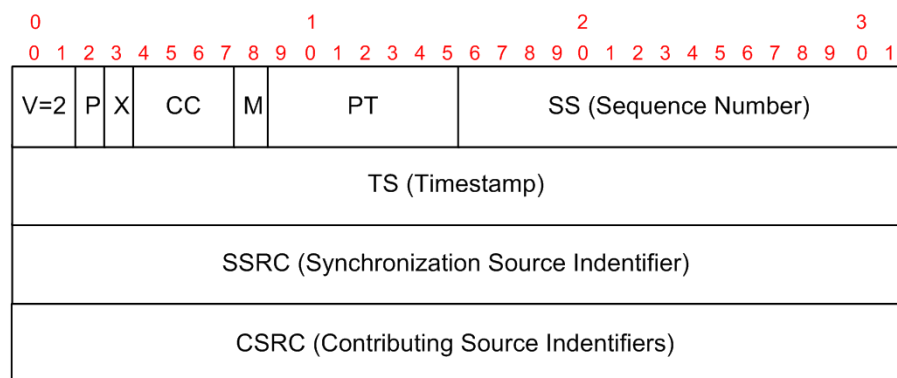


Figure 2.9.: The RTP header structure. The format refers to RTP version 2 in RFC1889 [5].

- *Version (V)* field determines the version of RTP.
- *Padding (P)* field implies that the packet includes one or more extra paddings which are not part of the payload.
- *Extension (X)* field indicates the fixed header is followed by precisely one header extension.
- *CSRC (CC)* field provides the number of CSRC identifiers that follow the fixed header.
- *Marker (M)* field identifies significant events for the payload, e.g. frame boundaries to be marked in the packet stream.
- *Payload type (PT)* field shows the format of RTP payload, e.g. H.263 [24]0.
- *Sequence number (SS)* field is increased by one for each packet sent. This field is used by the receivers to detect packet loss and out-of-sequence packets.
- *Timestamp* represents the time when the packet data is generated. This field is used for synchronization and jitter calculation.
- *SSRC* indicates the synchronization source, e.g. microphone, or camera. This identifier is selected arbitrarily so that no two synchronization sources within the identical RTP session will have the same SSRC identifier.
- *CSRC* determines the contributing sources for the payload. The number of identifiers is given by the CC¹⁹ field. CSRC identifiers are inserted by mixers using the SSRC identifiers of contributing sources.

Generally, audio and video streams are transported in separated RTP sessions, which are established with an IP address with a pair of ports for RTP and RTCP. The port numbers are chosen randomly between 1024 and 65535 and are negotiated at the beginning of a session using other protocols such as (SIP) [16] and Real Time Streaming Protocol (RTSP) [86] (using SDP [87]).

Some RTP functions depend on different profiles and payload formats. A RTP profile defines a set of features such as the use of the payload type field, resolution of the time

¹⁹ If there are more than 15 contributing sources, only 15 may be identified.

stamps, and the marking on interesting events. The common RTP profile for audio and video conference is RFC 1890 [88]. The video streams can be directly mapped to RTP packets according to RFC 3016 [89], where one MPEG-4 frame (either video or audio) is mapped in one RTP packet. If the MPEG-4 frame is too small to be mapped to the RTP packets, multiple frames can be mapped to one packet for efficient transmission. If the MPEG-4 frame exceeds the maximal packet size (MTU) of the underlying protocol, this frame can be mapped on two or more packets.

In general, RTP employs no retransmission mechanism due to the fact that the real-time media traffic is time-sensitive. RTP relies on the checksums of the lower-layer protocols to detect the errors. If unfortunately packet losses or errors are observed, the most likely response for RTP is to let the codec in upper layer to solve the problem. For example, [90] has presented a solution on top of RTP to adapt the codec output and adjust the data-sending rate according to the network condition information. [91] has proposed an adaptive video streaming system to change the transmission characteristics and the client buffer status based on varying networking conditions.

2.5 Application-Layer Protocols

2.5.1. Domain Name System (DNS)

DNS [92] is a “lightweight” hierarchical database which performs mapping between a name of host to an IP address, so that people can remember and identify the different network resources with common names instead of long boring IP addresses.

The foundational specifications for DNS is given in [93], which defines four important elements for DNS as follows.

- *Name Space* is a unique designator made up of symbols separated by dots. The DNS *Name Space* as shown in Figure 2.10 has a hierarchical structure, where query operations are attempts to extract specific types of information from domain name space tree. In this way the information can be subdivided and distributed easily and

new information could be added with little disruption to the rest of the system. The *Name Space* can be divided into a hierarchy of domains, i.e. a group of machines supported by more than one name servers, usually having a principal server and one or more secondary servers.

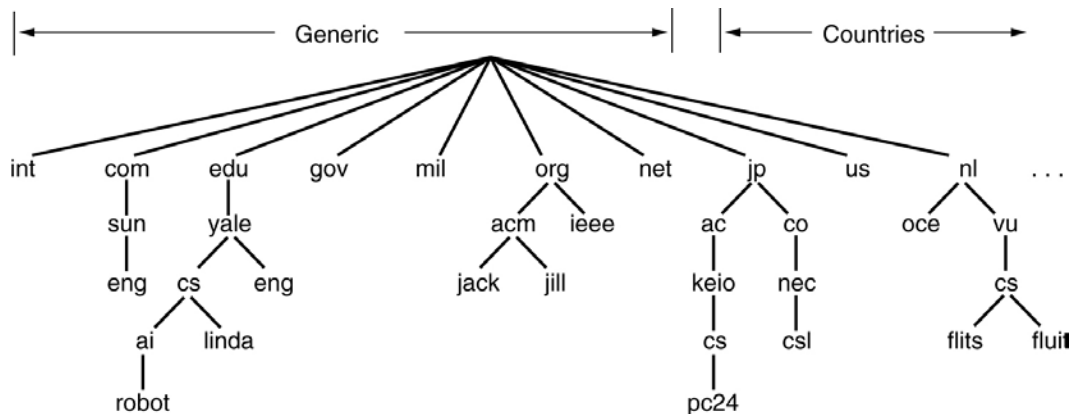


Figure 2.10.: The structure of the DNS Naming Space (Source:[6]). The hierarchical structure of DNS is convenient to convert domain names readable to humans into IP addresses linked with networking equipment.

- *Resource Record (RR)* is the basic data element in the DNS. It defines some attributes for a domain name such as an IP address, a string of text, or a mail route. Each record includes a type (A, MX, etc.), a TTL, a class and some type-specific information. The format of all RRs is specified in [8]. In order to convert a host name to IPv6 addresses, a separate resource record AAAA is defined in [94]. The format and use of the AAAA resource record are very similar to those of the traditional A record. An example of A and AAAA resource records for the same single host name is shown as follows.

www.ul.example. 3600 A 192.0.2.1

www.ul.example. 3600 AAAA 2001:db8::1

- *Name Server* performs the main DNS server mechanism, maintains the information and makes it available to clients. On TCP/IP networks, each host has one or more unique IP addresses. The DNS software implementation known as Berkeley Inter-

net Name Domain (BIND) [6] is the most commonly used domain name server on the Internet.

- *Resolver* is a host capable of performing a recursive search of the DNS to locate records that would answer a query. It usually creates queries and sends them across a network to a name server. Then the name server returns either the requested information, which in fact is an IP address or a referral to another server. In other words, a resolver is a DNS server that looks up DNS records on behalf of a client machine.

The drawbacks of DNS are also obvious. First, the huge *Name Space* may require relatively complicated management due to the hierarchical structure, i.e. if someone wants to setup a website with DNS services, s/he should endure some registration process before “getting connected”. Second, DNS has no advanced search functions and is not able to support advance enquiries. For example, if searching for people named “Tom”, you will get no answer or even an answer with abuses.

2.5.2. Dynamic Host Configuration Protocol v6 (DHCPv6)

DHCPv6 [60], similar as DHCPv4 [61], is a stateful autoconfiguration, which allows hosts to request addresses dynamically to prevent address duplication, protect reserved address pools, and simplify host configuration. DHCP specification [62] gives a full list of the DHCPv6 messages and options for the stateless services, and also the guidance for an implementation.

DHCPv6 aims to provide network configuration information based on the client-server model. In particular during the initialization procedure of clients, the server can allocate one or more IP addresses to the client for the period of lease. Using extended lease periods, the client can maintain the address for long periods of time. If the client is disconnected from the network for an extended period, the served address is returned to the pool and made available for other clients to request.

It is argued that stateless autoconfiguration in IPv6 can also configure IP addresses. However, in stateless mode DHCPv6 is also used to distribute only the other higher-level

information to nodes and does not perform any address assignment. The most important example is that the DHCPv6 can pass the IPv6 addresses of DNS servers²⁰ to the client. Moreover, Session Initiation Protocol (SIP) servers can be found via the DHCPv6 options as indicated in [64]. The specification [62] describes two options for passing configuration information related to DNS. The specification [65] explains which messages and options defined in RFC 3315 are required for stateless DHCP service.

2.5.3. Lightweight Directory Access Protocol (LDAP)

LDAP [95] is a lightweight protocol for accessing directory services, based on the Directory Access Protocol, which is a part of the comprehensive online directory developed through the standardization process of ISO and ITU. This original standard and service is known as X.500 [96]. LDAP runs only over connection-oriented reliable transfer protocols, such as TCP. [97] specifies how the LDAP Uniform Resource Locator (URL) format is resolved. The details of LDAP are in the latest version of the RFC "The Lightweight Directory Access Protocol (v3)" defined in [98].

LDAP consolidates information by replacing application-specific databases and allows more frequent data synchronization between masters and replicas. More important, it has a good compatibility with different platforms from different vendors. However, setting up and managing an LDAP naming service is complex and requires careful planning. LDAP information model consists of entries. An entry is a collection of attributes that have a globally-unique unambiguous Distinguished Name (DN) [99]. Each entry represents a real-world object, such as a person, an organization, a computer, or a nation. Each of the entry's attribute has a type and one or more values. The types are typically mnemonic strings, which are often abbreviated, like "cn" for common name, or "mail" for email address. The syntax of values depends on the attribute type. For example, a cn attribute might contain the value "Ning Wang". A mail attribute might contain the value "Ning.Wang@UL.ie".

²⁰ DNS address can be sent through Neighbor Discovery Protocol according to [63]

2.5.4. Session Initiation Protocol (SIP)

SIP [16], specified by the IETF, is an application-layer control protocol to initiate, modify, maintain, and terminate interactive sessions between one or more users in IP networks. The sessions may involve IP telephone calls and multimedia conferences, which can be communicated via multicast or a mesh of unicast relations, or a combination of these. In addition, SIP has been adopted by 3GPP (3rd Generation Partnership Project) as a mandatory protocol for handling signaling in IP multimedia services provided to 3G devices. So it is predicted that there will be millions of phones with SIP deployment in future.

Since SIP is an application-layer protocol, it is independent of the lower-layer transport protocols. SIP relies on transport protocols for any subsequent user data exchange. It can operate in conjunction with a variety of transport protocols, such as TCP [75], UDP [82], SCTP [66], and also other application-layer protocols, such as SDP [87], to create multimedia sessions. Since SIP messages are carried independently of the subsequent session content, it is unable to guarantee any QoS or control of the subsequent data flow between the end-points.

2.5.4.1. SIP server and address

There are two SIP types of entities in SIP: User Agents Client (UAC) and User Agent Server (UAS). A SIP UAC could be an end-device and may act either as a user terminal or as automated connection end-point, e.g. an Internet phone, while a UAS is an entity that processes the receiving requests and sends responses. Generally a user terminal has the functionality of both UAC and UAS.

SIP servers can be classified into following four categories:

- *Proxy Server* forwards the request to the next server. It just runs like a proxy in HTTP, i.e., forwarding the message to the next hop.
- *Redirect Server* redirects the client by replying a SIP response with an alternate address.
- *Registrar Server* performs the registration procedure.

- *Location Server* responds to location enquiries.

The term defined by SIP for addressing is called SIP Uniform Resource Identifiers (URIs), which provides a globally reachable address including the To, From, and Contact headers, and a Request-URI. The URI could be very much similar to an email address or telnet URI, i.e., sip:user@host. The user part is a user name or a number. The host part is a domain name which can be translated into an IP address via a DNS query. Once the calling terminal receives the server's IP address, it sends an invite message to the server which could be a proxy or redirect server.

2.5.4.2. SIP Messages

2.5.4.2.1. Request Message The request messages are carried in the request to identify the action that the requestor wants to invoke on the server. Generally, the type of request is specified by six methods which are shown in Table 2.3.

Table 2.3.: The SIP Request Messages.

Name	Description
INVITE	Initiate a session to peers or servers and invite a user to a call/conference.
ACK	Response to an INVITE request for acknowledgement of transmission reception.
CANCEL	Cancel a previous INVITE request sent by the client.
REGISTER	Update address listed in the header field with a SIP server based on the information carried by the message.
OPTION	Allows a user agent to request information about capabilities to process messages.
BYE	Terminate a connection between two users in a session.

2.5.4.2.2. SIP Response Message A three-digit numeric code indicates the type of SIP response messages. The first digit tells the class the message code belongs to, which is summarized in Table 2.4, and the other two digits define the response message.

Table 2.4.: The SIP response message classification.

Class	Name	Description
1XX	Provisional	Indicates the status of call prior to completion
2XX	Success	Request has succeeded
3XX	Redirection	Server return possible location
4XX	Client error	The request has failed due to an error by client
5XX	Server error	The request has failed due to an error by server
6XX	Global failure	The request should not be tried again at this or other servers

As shown in Table 2.4, there are six categories for SIP response messages. However, the following two types are most common.

1XX represents a provisional response, which is used to indicate call progress. It is issued by a User Agent Server to notify the sender that the INVITE has been received and that it is processing the message to call the invited party. For example, 100 TRYING and 180 RINGING are applied when it is expected that a final response will take more than 200ms. 100 TRYING represents that the request has been received by the next-hop server and that some unspecified action is being taken on behalf of this call (for example, a database query). A provisional response must be always followed by a 2XX response.

2XX indicates a success response and it requires an acknowledgment. Normally, if this kind of response is used to accept an INVITE request, it will contain a message body containing the media properties. It is used to indicate a successful receipt of the request in response to another request.

2.5.5. Telephone Number Mapping (ENUM)

ENUM is proposed by the IETF's Telephone Number Mapping working group to transform International Public Telephone Numbers into DNS domain names [100]. ENUM aims to enable the users in traditional telecommunications to access various services in IP domain, such as e-mail addresses, voice message or unified text messaging.

ENUM is based on DNS to find available services for a given E.164²¹ number. The rule for the unique mapping from an E.164 telephone numbers to an URI [101] is defined in RFC 3761 [102] and RFC 2916 [103]. ENUM reuses the existing protocols E.164 because (1) E.164 numbers are guaranteed to be unique; (2) People worldwide are familiar with this telephone numbering system; (3) There are still a (or the number of billions) billion of devices which only have numeric key input.

ENUM uses Naming Authority Pointer (NAPTR) [104] records in DNS to identify available ways or services for a specific domain through the E.164 number. A regular expression is used to rewrite rules in NAPTR records. ENUM introduces a new domain, e164.arpa in order to provide the infrastructure in DNS to store E.164 numbers. This domain is divided into subdomains. The look-up procedure is similar to the normal DNS operation. One possible example of conversion from E.164 to e164.arpa domain is described below.

- Remove any non-digit characters. E.164 number contains '-' which is used in the middle of the number, and '+' characters which appears at the beginning of the number. For example, the E.164 number could start out as "+353-1-79780" yielding "353179780".
- Put dots (".") between each two digits. Example: 3.5.3.1.7.9.7.8.0
- Reverse the order of the digits. Example: 0.8.7.9.7.1.3.5.3
- Append the string ".e164.arpa" to the end. Example: 0.8.7.9.7.1.3.5.3.e164.arpa

²¹ The ITU-T Recommendation E.164 suggests the international public telecommunication telephone numbering plan.

2.5 Application-Layer Protocols

In this way this domain-name is a unique record in the DNS database. These rules in this domain are encoded in NAPTR *Resource Records* in the form of URIs. A NAPTR look-up is performed when interpreting the URI results. The format of NAPTR is shown in Table 2.5 and explained briefly below:

Table 2.5.: The NAPTR format.

Domain	TTL	Class	NAPTR	Order	Preference	Flags	Service	RegExp	Replacement
--------	-----	-------	-------	-------	------------	-------	---------	--------	-------------

- *Domain* field contains the domain name to which this resource record refers. If no domain name is given, it is assumed to apply to the domain of the previous *Resource Record* (RR).
- *TTL* (Time-To-Live) field contains the number of seconds remaining on a cached record before it is purged.
- *Class* field indicates an address class, e.g. use IN²² for IP addresses. If no class is given, the class of the preceding RR is assumed.
- *Type* field for NAPTR is 35 as defined in [104].
- *Order* field is a 16-bit unsigned integer specifying the order in which the NAPTR records must be processed to ensure the correct ordering of rules. The smallest number gives the highest priority to process.
- *Preference* field is a 16-bit unsigned integer that specifies the order in which NAPTR records with equal order values should be processed. Similarly to the Order field, small numbers are processed before big numbers.
- *Flags* field is a character-string containing flags to control aspects of the rewriting and interpretation of the fields in the record. Flags are single characters from the set [A-Z ; 0-9]. The case of the alphabetic characters is not significant.
- "S", "A", "U", and "P" flags are defined as follows:

²² IN is a mnemonic for Internet and is defined in [8] as a DNS CLASS field in resource records.

- "S" flag means that the next lookup should be for Service Record (SRV) records.
 - "A" flag means that the next lookup should be for either an A²³, AAAA²⁴, or A6²⁵ record.
 - "U" flag means that the next step is not a DNS lookup but that the output of the RegExp field is an URI that adheres to the 'absolute URI' production found in the Augmented Backus-Naur Form (ABNF)²⁶ of RFC 2396 [101].
 - "P" flag means that the remainder of the application side algorithm shall be carried out in a protocol-specific fashion.
- *Service* field specifies the services available to rewrite path. It may also specify the particular protocol that is used to talk with a service. Service parameters for ENUM in the NAPTR record are described in ABNF syntax in following format:
 - service_field = "E2U²⁷" 1*(servicespec)
 - servicespec = "+" enumservice
 - enumservice = type 0*(subtypespec)
 - subtypespec = ":" subtype
 - type = 1*32(ALPHA²⁸ / DIGIT)
 - subtype = 1*32(ALPHA / DIGIT)
 - where in service_field, "E2U" is denoted as ENUM to URI, followed by 1 or more ENUM services which indicate what class of functionality a given end-point offers. Each ENUM service is indicated by an initial '+' character.

²³ The A resource record type is an address record returning a 32-bit IPv4 address.

²⁴ The AAAA resource record type is a record specific to the Internet class that stores a 128-bit IPv6 address.

²⁵ The A6 resource record type is another record specific to represent a 128-bit IPv6 address.

²⁶ Augmented Backus-Naur Form (ABNF) is used to define a formal syntax with compactness and simplicity [105].

²⁷ E2U denotes ENUM only Rewrite Rules in order to mitigate record collisions.

²⁸ ALPHA in ABNF represents 'A-Z / a-z'.

- *RegExp* field is a string containing a substitution expression that is applied to the original string held by the client in order to construct the next domain name to lookup. The syntax of this field is specified in the Dynamic Delegation Discovery System (DDDS) [106, 102] as substitution expression syntax.
- *Replacement* field is used when the regular expression is a simple replacement operation in order to query depending on the potential values found in the Flags field [106]. However, it is not currently used within ENUM.

ENUM provides a simple mapping between the E.164 number and URI. DNS is proved to be scalable and stable in the usage of Internet, and will serve ENUM as a public available, distributed database. Intelligent call preference can be stored in this database. This scheme maximally utilizes the existing protocols and infrastructure.

One possible example to use ENUM in CBM-ICC is to perform intelligent call redirection as shown in Figure 2.11. Suppose the user, Tom, wants to make his telephone number +353-1-79780 his permanent contact number. So there is a domain, 0.8.7.9.7.1.3.5.3.e164.arpa, in the DNS server. He is able to configure his NAPTR entry through a web-based interface. Tom's preference can be updated using the DNS UPDATE method [7]. One configuration could be as shown in Table 2.6. Tom's preferred method is to use a SIP phone as it is cheap. Then people can email to his email address, tom@abc.ie. He also wants to setup a telephone filtering system, e.g. all the numbers which start with 085 are redirected to his mobile phone; all the numbers which start with 086 are redirected to his fixed phone; all the other numbers are redirected to his secretary.

Table 2.6.: One possible configuration for ENUM.

Class	NAPTR	Order	Preference	Flags	Service	RegExp
IN	NAPTR	10	10	"u"	"E2U+sip"	"!^.*!sip:tom@sip.com!"
IN	NAPTR	11	11	"u"	"E2U+email:mailto"	"!^.*\$!mailto:tom@abc.ie!"
IN	NAPTR	12	12	"u"	"E2U+voice:tel"	""!^(085.*\$)\$!tel:\ 003538769780!"
IN	NAPTR	12	13	"u"	"E2U+voice:tel"	""!^(086.*\$)\$!tel:\ 00353179780!"
IN	NAPTR	12	14	"u"	"E2U+voice:tel"	""!^(.*\$)\$!tel: 00353179781!"

2.6 Mobility Management

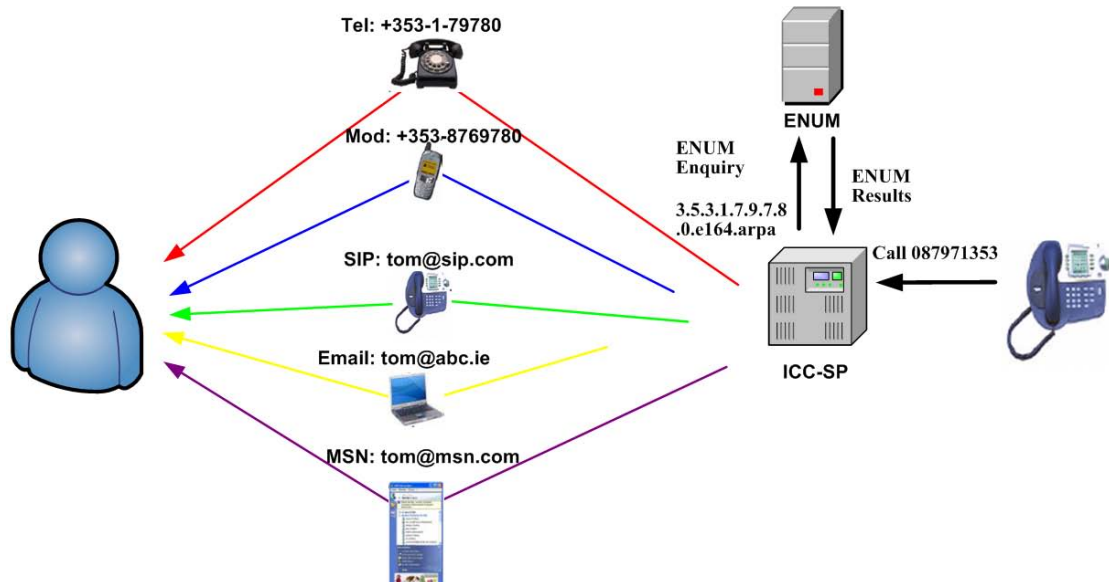


Figure 2.11.: An example of ENUM usage in CBM-ICC scenario where a user wishes to make his/her telephone number as his/her permanent contact number and the incoming call can be redirected in diverse approaches.

2.6 Mobility Management

Mobility management [107] is an essential component of the CBM-ICC service allowing mobile users to roam across various ANPs and TSPs at any time and anywhere. According to [108] and [109], mobility management in IP-based networks can be broadly classified into personal mobility²⁹, terminal mobility³⁰ and service mobility³¹. In this research, we mainly focus on terminal mobility.

As recommended in [110], terminal mobility management consists of two fundamental issues: location management and handoff management:

²⁹ Personal mobility allows an end-user to maintain contact and to access services even with different terminals. To achieve this, the network is able to identify the end-users as they change the terminal.

³⁰ Terminal mobility enables a terminal to access the network even with different location, while maintaining the ongoing communication across different networks.

³¹ Service mobility allows a user to use a set of services even when the user is moving while changing devices or network attachment points.

- *Location management* refers to the task to track and locate the current network location of a mobile terminal for possible connection, e.g., finding a valid IP address of a mobile host in order to initiate a connection. The location management is needed at the beginning of a new session in order to handle all the information about locations, authentication information, and QoS.
- *Handoff management* is required to establish a connection when a mobile device changes its point of attachment in the middle of the session. The ongoing communication should still be maintained with its peer. This mechanism can be implemented at different layers of the protocol stack.

2.6.1. Location Management

Location management indicates the way to identify the location of mobile users, i.e. the appropriate network or mobile terminal. The method of locating the called party in the CBM-ICC can be developed using the existing protocols such as Secure Dynamic DNS (DDNS) or SIP.

2.6.1.1. Secure Dynamic DNS (DDNS)

The DNS was originally designed to support queries of a statically configured database. The A query in IPv4 and AAAA query in IPv6 can look up the host addresses when receiving the host name.

However, the location data changes frequently in wireless networks, whereas the DNS architecture is almost static and changes slowly. In [7] P.Vixie *et al* proposed an extension of UPDATE message to support dynamic hostnames by updating the RRs when host's IP address changes. Therefore the Secure Dynamic DNS (DDNS) [111] is able to perform name-to-address mapping as machines move. The overall format of the UDPATE message is presented in Figure 2.12.

DHCP allows users to request addresses dynamically to prevent address duplication, protect reserved address pools, and simplify workstation configuration. Using extended lease

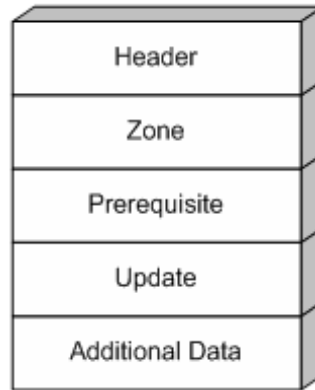


Figure 2.12.: The overall format of the secure DDNS UPDATE message [7]. This format based on the DNS message format in [8] extends a number of fields.

periods, the client can maintain this address for long periods of time. If the client is disconnected from the network for an extended period, the served address is returned to the pool and made available for other clients to request.

DHCP can coexist with DDNS services to support terminal mobility when the user terminal moves. To support DDNS, the client needs to install software which is used to dynamically update the new user's information to the DDNS servers. Usually it runs at the background and is activated when the user changes the IP address. When the client gets the new IP address via DHCP, the UPDATE procedure is performed. The DDNS just runs in a normal DNS resolving procedure and the hostname is mapped to the new IP address. In this way, all the incoming calls can be redirected to the new IP address. Through the simple mapping from fixed hostname to dynamic IP address, the terminal mobility in ICC service can be realized.

By using DDNS, we can take advantage of existing network infrastructure rather than introducing new protocols or deploying new equipment. However, the drawbacks are also obvious. The registration delay is relatively large and any application based on TCP will not survive. However, it is an economic method to keep callee being found when his/her location is changed.

2.6.1.2. SIP Location Management

SIP is another protocol that can offer location management. Before setup a call, the SIP client is required to register its new IP address with the Registrar server. Any call to the client is thereby forwarded to this new IP address. The SIP client updates the location to the Registrar server whenever the user location changes. The SIP server can handle the incoming call by querying a location server for where the called party is or which server the called party have registered to. The SIP server and location server can be integrated into one server and thus their interaction becomes an internal issue.

The location update is performed by a REGISTER message as shown in Figure 2.13. When the user moves to a new location, a registration first has to be performed by sending a REGISTER message to update location information so as to let servers know the new IP address. Here for simplicity we assume that the location server is integrated into the SIP server. The value of the *Contact* field in the REGISTER message headers should be replaced with the new IP address. For example, Tom already got SIP URI, Tom@sip.ul.ie. The IP address of the SIP server, sip.ul.ie, is 192.0.0.1. If he goes to a new location, his new IP address there is 10.0.1.2. So the REGISTER message header can be written as shown in Figure 2.13.

```
REGISTER sip:REGISTRAR.SIP.UL.IE SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;
To: UA1 <sip: Tom@sip.ul.ie >
From: UA1 <sip: Tom@sip.ul.ie>;tag=456248
Call-ID: 843817637684230@998sdasdh09
CSeq: 1826 REGISTER
Contact: <sip:Tom@10.0.1.2>
Supported: path . . .
```

Figure 2.13.: An example of the REGISTER message which can be used to update location information by registering a new IP address to the server.

Note the value of the *Contact* field is replaced by his current IP address. Also the value of the *c* field in the SDP header is changed to this new IP address. Once the registration procedure is completed, the callee is ready to receive incoming calls.

2.6.1.3. Location Management Comparison

The Internet uses IP addresses to identify the mobile terminal's location in the network topology. To achieve terminal mobility, the identifier must be retained unchanged while user terminal is moving and location is changing.

There has been a great deal of work to enable location management within the IP domains. Location management based on SIP has already been proposed in [112] where the SIP client updates its new IP address, which is acquired via DHCP, with the Registrar server by sending a REGISTER message. [113] has proposed a DDNS/DHCP method by updating the host's current IP address to the DNS server.

Both methods provide the capability to support location management. DDNS takes advantage of existing network infrastructure rather than introducing new protocols or deployment of new equipment. On the other hands, SIP is very popular nowadays in VoIP and is easy to extend its signaling messages. Also SIP is an application-layer protocol, which brings relatively small modifications in the existing Internet protocol infrastructure. The problem for SIP is that the handoff latency is large and thus increases the packet loss to support ongoing communication. One of the greatest difficulties in DDNS lies in the stringent security requirements imposed on mobile users [114].

2.6.2. Handoff Management

Handoff management protocol for CBM-ICC service should guarantee mobile users more flexible control over incoming calls, enable users to receive incoming calls via multiple access networks/providers with seamless connectivity³².

³² Seamless connectivity refers to that the services are uninterrupted by mobility.

2.6.2.1. Mobile IPv6 (MIPv6)

The famous solution for mobility support at the IP level is Mobile IP, which is designed to manage mobile devices' movements from one network to another without losing the existing connections.

There are two IETF Mobile IP Working Groups: Mobile IPv4 (MIPv4) [115] and Mobile IPv6 (MIPv6) [116]. The design of MIPv6 is based on the experiences gained from the development of MIPv4. The primary goal of the MIPv6 working group is to enhance base IPv6 mobility by continuing work on wide-scale deployments. MIPv6 supports transparency above the IP layer, including maintenance of active TCP connections and UDP port bindings. RFC3775 [116] and RFC 3776 [117] are considered as the baseline or minimum protocol set for implementing the IPv6 mobility.

Figure 2.14 shows the basic elements of MIPv6. Mobile user can get a unique static IPv6 address, which is associated to the Home Agent (HA). When an MT remains in its home network, it communicates like normal IPv6 terminal. When an MT moves to a new point of attachment, a new Care-of Address (CoA) is allocated and registered with the HA and Correspondent Host (CH). Generally, MIPv6 operates in the following three steps:

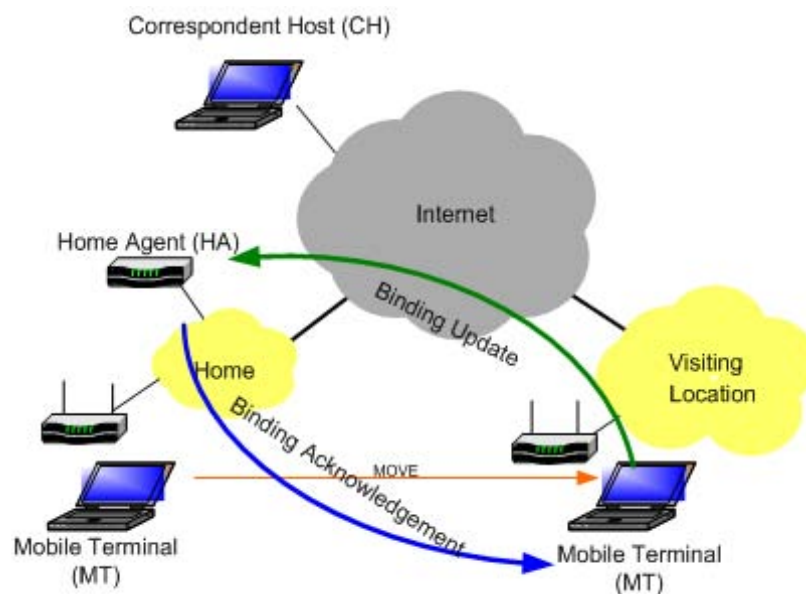


Figure 2.14.: A schematic diagram of the MIPv6 Binding Update to the Home Agent.

- Movement detection is performed. As MT moves to a new network, the new point of attachment is detected by analyzing the included network prefix information in Router Advertisements. If one of the network prefixes equals to the network prefix of the Home Address of the MT, then the MT is on its home link. Otherwise the MT is in a foreign network. The MT selects one of the advertised routers as its default router, based on the preferences configured by the mobile user beforehand. The MT can also send a Router Solicitation to request all the routers on the link to send Router Advertisements if a periodic Router Advertisement is not received. In cellular networks, this kind of so-called movement detection can be coordinated with Link Layer movement detection mechanisms.
- Acquisition of a co-located CoA is the next step that MT has to do. To do this, the MT can use IPv6 address auto-configuration that could be either stateful or stateless. For the stateful situation the MT obtains a CoA from a DHCPv6 server. For stateless situation, the MT must use information in the router advertisement to create a new CoA. As specified in [49], the uniqueness of its link-local address should be verified by the duplication address detection (DAD) .
- Once the CoA construction is done, the Registration of the new CoA with the HA is performed. There are three methods involved for MIPv6 binding management: Binding Update, Binding Acknowledgement, and Binding Request. All these methods can be either forwarded separately or piggybacked in the Destination Option field of IPv6 header. As illustrated in Figure 2.14, MT must update the binding cache in its HA and CH by sending a binding update. A Binding Update is forwarded to inform the HA and any CHs of the current binding, consisting of the new CoA, the Home Address and a binding lifetime. In the case that a CH knows only the Home Address, the packets sent from CH are redirected by HA to MT. In addition, MT can also send a Binding Update to the CH after receiving packets routed via the HA. This is Routing Optimization. As show in Figure 2.15, if a CH wants to know the CoA of a MT, it can send a Binding Request, which, however, is mainly used to refresh binding when approaching the end of the current binding lifetime. If the MT moves back to its home link, it will notify the Home Agent to delete the binding. The Binding Acknowledgement is usually sent as a response to the

Binding Update, whilst it is also sent to reject the Binding Update for some circumstances e.g. for authentication failure. Each IPv6 node (either mobile or stationary) is going to support the Binding Update message, enabling the packets destined to the MT to be efficiently routed without going through the HA. Furthermore, the security in Binding Update and Binding Acknowledgement can be enhanced by IP Security (IPSec) [118].

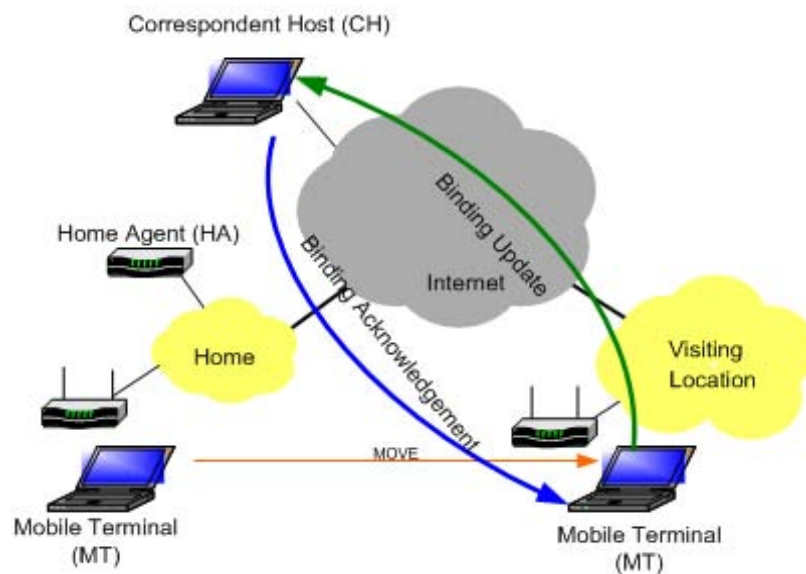


Figure 2.15.: A schematic diagram the Binding Update to the Correspondent Host.

2.6.2.1.1. Comparison between MIPv6 and MIPv4 Although the initial idea about MIPv6 is based on the specification for MIPv4, MIPv6 benefits from the new features of IPv6 and thus is different from MIPv4 as summarized in the next lines.

Firstly, optimized routing is integrated as an inherent feature in MIPv6. The problem of Triangular Routing, i.e. packets from a CH to the mobile terminal via the Home Agent, could be solved. This greatly reduces transport delay and saves network capacity. Thus there is no need to deploy special routers as Foreign Agents, like in MIPv4. MIPv6 operates in any location without any special support required from the local router. It is expected that route optimization can be deployed on a global scale between all mobile terminals and CHs.

Furthermore, security is greatly enhanced in MIPv6. Mobility signaling and security features (IPsec) are integrated in the IPv6 protocol as header extensions. MIPv6 route optimization can operate securely even without pre-arranged security associations. The Binding Updates in optimized routing and the registration procedure use the integrated IPsec for sender authentication, data integrity, and replay protection. However, standard MIPv4 only uses a separate UDP based protocol for registrations and optimized routing. Finally, foreign agent is no longer a must in MIPv6. The CoA assignment is greatly simplified by the IPv6 Address Auto-configuration. It also eases the address management in a large network infrastructure. Most packets sent to a mobile terminal while away from home in MIPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to MIPv4. On the other hand, MIPv4 is not deployed widely to satisfy current mobility needs due to the shortage of globally routable IPv4 addresses and the use of private IPv4 addresses with Network Address Translators (NATs). However, IPv6 provides enough address space for the deployment of MIPv6, and address exhaustion is not a problem in IPv6. An IPv6 CoA is always co-located at the MT, and the concept of the foreign agent has been eliminated.

2.6.2.2. MIPv6 enhancement

MIPv6 generates significant signaling to the home agent and the corresponding node for a local movement. This procedure creates a considerable delay for the location update. [119] presents that the active communications in MIPv6 are interrupted until the handoff completes. Therefore, it may cause communication interruption and packet loss during a handoff. To overcome the problems, two major extensions to MIPv6 have been proposed to improve the performance in terms of the handoff delay:

- *Hierarchical MIPv6* (HMIPv6) [120] [121] extends the idea of Mobile IP into a hierarchy of Mobility Agents, which manages movements locally within a domain.
- *Cellular IPv6* [122] [123] introduces a new dynamic layer 3 routing protocol in a localized area, which allows the use of layer 2 triggers to anticipate the handoff.

2.6.2.2.1. Hierarchical MIPv6 MIPv6 uses the same mechanisms in both macro mobility (between sites) and micro mobility (within a site). However, MIPv6 results in an inefficient use of resources in the case of micro mobility. The HMIPv6 [120] is the proposed enhancement of MIPv6 that is designed to reduce the amount of signaling required and to improve handoff speed for mobile connections. HMIPv6 considers the macro mobility and micro mobility separately. Thus, the macro mobility is handled by MIPv6 protocols, while the micro mobility is managed locally by HMIPv6.

Mobility Anchor Point (MAP) is a new node proposed by HMIPv6 that serves like a local entity to handle the handoffs. The MAP can be located anywhere within a hierarchy of routers. In MIPv6, a mobile node sends Binding Update to the Home Agent and then to any node it corresponds with each time it changes its location. However, this involves a lot of signaling and processing and a great deal of resources is wasted. The MAP helps to decrease handoff-related latency because a local MAP can be updated more quickly than a remote Home Agent. So by separating different mobility types, HMIPv6 makes it possible to deal with the updating locally. That saves the network resources and reduces the latency.

2.6.2.2.2. Cellular IPv6 In order to minimize the handoff delay and eliminate the period of service disruption, Cellular IPv6 [122] was proposed with the intention to combine the cellular technology with the Mobile IP network. Cellular IPv6 uses specialized domain routers with host-based entries for local mobility.

Cellular IPv6 operates on base stations, cellular IP node and Internet gateways. MT can find the nearest base station through the beacon signals broadcasted by the base stations. The cellular IP node serves as a router of IP packets and maintains routing caches, which can be updated by the MT. The cache mappings of older cellular IP nodes will time out after the MT initiates a handoff process and migrates to a new base station. The gateway provides the connectivity to the Internet. The MT utilizes the IP address of the gateway as its CoA for global reachability usage. All the traffic coming from the MT must pass through the gateway before delivery. Uplink packets are routed from the MT

to the gateway on a hop-by-hop basis. The downlink path is constituted by the chain of cache mappings referring to the MT.

2.6.2.3. SIP Handoff Management

SIP is the main signaling protocol for managing multimedia sessions over IP networks. Recently SIP has been extended to also support terminal mobility. SIP handoff management can be performed either at the start of a new session, or in the middle of a session. The former situation is referred to as pre-call mobility, while the latter is known as mid-call mobility [112].

SIP pre-call mobility is performed during the start of a new session. As a SIP client moves to a new visited network before a session is established, it would re-register its new contact address with the SIP server. Thus, the SIP client can always be reachable whenever it updates the new contact address.

The SIP mid-call mobility means that a SIP client moves to a new access network during an on-going session. According to [124, 125, 126, 127, 128], the basic procedure for SIP handoff in the middle of a session consists of two phases: The MT first updates its location by sending a REGISTER message to the Registrar server for future calls. The Registrar server stores the information and acknowledges it back to the MT. Then Re-invitation is performed. The MT sends a new INVITE Request directly to notify the end-point or the communicating server to notify about the changed IP address. The new INVITE message includes the same call identifier as in the original session establishment and the new IP address in the *Contact* field of the SIP message. The end-point sends an acknowledgment message to the MT to confirm the address change. The end-point can start sending data to the new location and the session can be maintained without interruption. Therefore, it guarantees that a SIP client can keep sessions continuously while moving [129].

2.6.2.4. Mobile SCTP Extension

One key feature of SCTP is multi-homing, which increases the availability by allowing end-points to use multiple interfaces and IP addresses for an association simultaneously.

This attractive feature makes mobility and seamless handoff possible at the transport layer. However, the original SCTP specification [66] does not support dynamical addition of IP addresses and does not change primary the IP address without disconnection. A new SCTP Dynamic Address Reconfiguration (DAR) extension, referred to as Mobile SCTP (mSCTP) [130, 131], was proposed in [72] to support the end-to-end controlled transport mobility. The SCTP DAR extension enables a dynamical IP address configuration on mobile hosts, which means that there are able to dynamically add new IP addresses, delete unnecessary IP addresses, and change the primary IP address in the address list on the fly withput interrupting/terminating the service session.

To accomplish the dynamic nature of handoff, the DAR extension must complete the following two steps: (1) dynamically add or delete IP addresses to an existing end-to-end SCTP association, and (2) dynamically change the primary destination during an active SCTP association. The DAR extension specifies two new chunk types: the Address Configuration Change (ASCONF) and the Address Configuration ACK (ASCONF-ACK) to notify the remote end-point about the corresponding event. Three new parameters are also introduced as follows:

- *Add IP Address* (Add-IP) parameter is used to add a new IP address to an existing association.
- *Delete IP address* (Delete-IP) parameter is used to delete an old and unused IP address from an existing association.
- *Set Primary IP Address* (Set-Primary-IP) parameter is used to set the primary IP address as the active IP address of an existing association.

With the aid of ASCONF chunks, the procedure that a mobile host moves to a new location and changes its point of attachment could be summarized as follows:

1. Obtaining a new IP address for the location through DHCP or stateless address configuration.
2. Adding the newly obtained IP address to the SCTP association.
3. Sending an SCTP ASCONF chunk with the “Set Primary IP Address” parameter to the corresponding end-point which responses with a SCTP ASCONF-ACK chunk.

4. Deleting the old IP address from the SCTP association.

After completing the above steps, the mobile host can communicate through the new primary IP address.

Dynamical addition or modification of IP addresses increases the risk of association hijacking, ASCONF chunk may need an authentication chunk bundled before the ASCONF chunk, as described in [132].

2.7 Conclusions

When considering the design of the CBM-ICC service, it is essential to achieve maximum conformance and interoperability with various ANPs and TSPs. Given that the CBM-ICC service is primarily designed for packet-switched networks employing the IP protocol, it is important for us to build the CBM-ICC service according to open standards and RFCs.

Before describing the proposed new CBM-ICC service, this chapter provides background information by analyzing the existing TCP/IP protocols and services that are relevant to the CBM-ICC service. In this chapter, we have reviewed the basic TCP/IP protocols and provided a good source for more in-depth information on relative protocols for the CBM-ICC service. Most of the standard protocols discussed in this chapter are referred to the public RFCs by IETF. Firstly, we have investigated the layered structure of the TCP/IP model. Then two transport-layer protocols: Stream Control Transmission Protocol (SCTP) and Real-time Transport Protocol (RTP) service, have been introduced. Section 2.4 has presented the application-layer protocols, such as the Domain Name System (DNS) and Session Initiation Protocol (SIP), etc. Finally, we have discussed a number of existing proposals for mobility management and compare these mobility solutions. This will help us to determine the most efficient protocol to solve the HAC switching problem.

The truth is more important than the facts.

—Frank Lloyd Wright (1869 - 1959)

3

Related Work

3.1 Introduction

Before describing the proposed new CBM-ICC service, this chapter largely surveys current relevant work and presents foundation information by analyzing the existing services that are related to the CBM-ICC service. Section 3.2 investigates numerous existing relative services including Skype, VoIP and Cisco Call Manager. Section 3.3 presents the related work within academia, while Section 3.4 concentrates on related work within standardization, organizations and industry emphasizing on the interoperability and handoff between heterogeneous networks. Related work in the area of mobility management for next generation all-IP-based wireless systems is presented in Section 3.5.

3.2 Related Services

Over the past years, several new services have been proposed in the market to establish cost-efficient voice communication. Skype [35] is one of the most popular and successful VoIP applications with tremendously increased number of users. Other VoIP solutions are Gtalk [133], MSN [134], and Ekiga [37].

3.2.1. Skype Service

Skype is based on a peer-to-peer networking and provides low-cost voice calls, instant messaging, audio conferencing and file transfers between its users. The famous benefit of Skype is that the long-distance call charges or international phone bills are greatly reduced.

Skype is a completely proprietary peer-to-peer signaling protocol and imposes a strong encryption to prevent unauthorized snooping [135]. There are no unique standard ports for Skype traffic, which obstructs the protocol analysis for potential protocol scanning. Thus only little is revealed about its internal mechanisms due to proprietary and security. There are a few publications that exposed some research on Skype recently. A brief overview of Skype can be found in [136]. [137] shows that the extensive obfuscation and anti reverse-engineering techniques are adopted to protect its proprietary. [138] reveals many details about the Skype protocols and internals, including the Skype encryption and the techniques to circumvent NAT and firewall limitations. [139] and [140] investigate the identification methods to discover Skype hosts and voice calls. Skype traffic is characterized, identified and analyzed in [141] and [142]. Skype and Google Talk are compared based on their perceptual speech quality with the proposed system using UDP packet traces in [143]. [144] investigates the characteristics of traffic streams generated by voice and video communications, and the signaling traffic generated by Skype. In [145] authors have analyzed Skype traffic delay and improved the system performance.

The Skype network consists of the following elements: *ordinary host*, *super node*, *login server*, and *buddy-list server*.

- The *ordinary host* is a Skype client, which could be an application or equipment that can be used to place voice calls or send text messages. The ordinary host must register itself with the Skype login server and must connect to a super node for a successful Skype call.
- The *super node* (SN) is an ordinary node, which has a public IP address, sufficient CPU, memory, and network bandwidth. Each SN keeps track of a small number of ordinary nodes. SNs are the switching elements in the overlay network responsible

for maintaining a global-index distributed directory which allows users to find each other.

- The *login server* is responsible for authentication and accounting, i.e., storing the account information of users and user authentication at the beginning of a session. In general, there are several login servers storing information in a distributed way. The login server should be capable to ensure that user login names are unique across the whole name space.
- The so-called *buddy-list server* [136] is responsible for storing the contact list of the users. Although this list is stored locally on the host computer, the role of this entity is to make sure that the contact list is also available if the user logs on from another host.

All online and offline user information is stored in a decentralized fashion. When a Skype client is launched it firstly contacts one of the login servers for authentication, and then investigates several SNs (about 20) to check whether they are alive and ready to accept the client. After some message exchange, the client tries to contact one of these SNs to establish a connection. A list of other SNs is stored at the client side for the next time use.

3.2.2. Voice over IP (VoIP)

The VoIP servicing provides voice transmission over IP-based packet-switched networks like the Internet, Local Area Networks (LANs) or wireless LANs (Wi-Fi). VoIP has same functionality with the Skype, e.g., voice calls, instant messaging, and buddy lists. However, the underlying protocols and techniques are quite different.

The generic protocol stack for VoIP is shown in Figure 3.1. SIP is used by many VoIP providers (Gizmo [36] and Ekiga [37]) as a signaling protocol. H.323 is another choice proposed by the ITU for multimedia communication services such as real-time audio and video over IP networks. RTP and RTCP support end-to-end network transport and control for real-time communications. At the transport layer, TCP or UDP is utilized for VoIP traffic and signaling information.

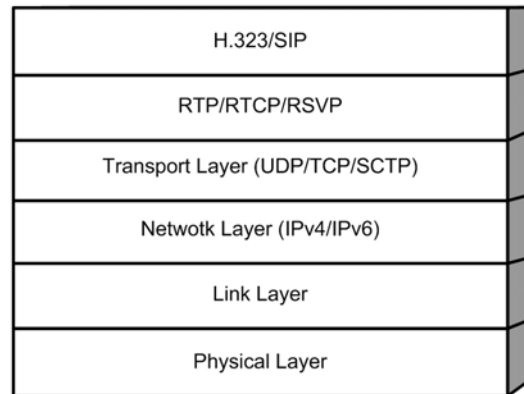


Figure 3.1.: The protocol stack for VoIP. The VoIP layered hierarchy complies with the theoretical model developed by the OSI model.

The voice codec, known as analog/digital voice signal conversion with digital compression, is the key factor that influences the speech quality or Mean Opinion Source (MOS) in the VoIP service. There are three commonly used codecs in the Internet telephony, such as G.711, G.723.1, and G.729, as listed in Table 3.1. The other audio codecs use different data rates ranging from 5.3 kbps to 64 kbps and are specified in [146].

3.2.3. Cisco Call Manager

The Cisco Call Manager (CCM), a.k.a. Cisco Unified Communications Manager, provides an interface with other telephone technologies to support voice mobility over an IP-based protocol.

The proprietary Skinny Client Control Protocol (SCCP) is proposed by Cisco as a signaling protocol to allow Cisco Wi-Fi handsets to have as little intelligence as possible [147]. SCCP signaling messages are exchanged between CCM and Cisco phones. In this way, entire logic really runs in a client-server mode. There are not too many external documentations on SCCP. [147] reveals that SCCP runs on TCP using port 2000 and bearer traffic still uses RTP.

Due to its proprietary nature, SCCP has a dramatically different architecture from SIP or H.323. SCCP operates in an event-based fashion. The buttons on a Cisco Wi-Fi handset

Table 3.1.: The VoIP Codecs (commonly used).

G.711 codec	In wireless networks, G.711 is applied for encoding telephone audio signal at a rate of 64 kbps with a sample rate of 8 kHz and 8 bits per sample. In an IP network, voice is converted into packets with durations of 5, 10 or 20 ms of sampled voice, and these samples are encapsulated in a VoIP packet.
G.723.1 codec	G.723.1 belongs to the Algebraic Code Excited Linear Prediction (ACELP) family of codecs and has two bit rates associated with it: 5.3 kbps and 6.3 kbps. The encoder functionality includes Voice Activity Detection and Comfort Noise Generation (VAD/CNG). The decoder is capable of accepting silence frames. The coder operates on speech frames of 30 ms corresponding to 240 samples at a sampling rate of 8000 samples/s and the total algorithmic delay is 37.5 ms. The codec offers good speech quality in network impairments such as frame loss and bit errors and is suitable for applications such as VoIP.
G.729 codec	G.729 belongs to the Code Excited Linear Prediction coding (CELP) model speech coders and uses Conjugate Structure ACELP (CS-ACELP). This coder was originally designed for wireless applications at fixed 8 kbit/s output rate, not including the channel coding. The coder works on a frame of 80 speech samples (10 ms) and the required look ahead delay of 5 ms. So the total algorithmic delay for the coder is 15 ms.

are mapped with user events. Whenever a button is pressed, SCCP is used to update these events to CCM in real time. The CCM then responds to the phones with any change in state that should accompany the button press. The main difference between the SCCP and traditional telephone signaling protocols is that SCCP is more like a remote control protocol.

3.3 Related Work within Academia

Although not directly addressing the UCWW concept and its infrastructural innovations, several projects are also related to aspects of similar system architectures and services integration.

The Focus project [148] is under development at the WINLAB at Rutgers University. This project is aimed at solving the issues addressed by convergence of Wi-Fi and UMTS in order to prototype the fundamentals of 4G network architectures and protocols. In this project, an open-architecture, programmable mobile network approach has been proposed to permit gradual evolution of service features via ad-hoc peer-level collaboration of wireless network entities. The proposed architecture accommodates heterogeneous radio links and permits evolution of mobile network services to include basic mobility features (such as authentication, location management and handoff) as well as newer requirements such as self-organization, ad-hoc³³ routing, QoS, multicasting, and content caching. The cross-layer approaches have been adopted for routing and transportation in ad-hoc network scenarios. The Open Access Research Testbed for Next-Generation Wireless Networks (ORBIT) has been implemented based on the open API wireless terminals, access points, switches and routers. The evaluation for different approaches both in terms of protocol functionality and software performance has been performed.

The Japanese Government project MIRAI [149] (Multimedia Integrated network by Radio Access Innovation) represents another significant effort towards the design and implementation of a next generation heterogeneous network. As part of the e-Japan Plan, this project aimed at the development of new technologies that will enable seamless integration of various wireless access systems. As indicated in [150], the most significant feature of MIRAI is the provision of a set of signaling functions: radio-access-network discovery and selection, heterogeneous paging, and vertical handoff. The seamless service between different wireless systems has been achieved by the dedicated wireless systems providing the signaling functions. A unique mobility model for next generation heterogeneous net-

³³ Ad-hoc is a decentralized wireless network infrastructure which does not rely on a preexisting infrastructure.

3.3 Related Work within Academia

works has been proposed in [151]. This model supports dormant terminals with multiple air interfaces. The model is based on Mobile IPv6 with some extensions to incorporate the paging mechanism and security. A proof-of-concept simulation and demonstration system has been developed to evaluate the performance of the model in terms of delay, network load, and signaling trade-offs.

The European Union Information Society Technologies (IST) approved for funding the seamlEss multimedia serVices Over all IP-based infrastructures (EVOLUTE) [152] project. The objective of this project is to develop an all IP-based network infrastructure that offers seamless multimedia services to users through a variety of heterogeneous wireless technologies. An efficient scheme for transferring context information has been developed to enhance the handoff performance from one access network to a new one. This project has largely investigated the current mobility management schemes based on multiple existing and emerging protocols (such as MIP, SIP, IP-based micro-mobility), in order to support multimedia services (either real-time or non-real-time) efficiently. The integration of Wi-Fis with next-generation cellular networks including both vertical hand-offs (between UMTS and Wi-Fi) and horizontal handoffs (within UMTS, or within Wi-Fi) have been studied in [153]. This project also attempts to resolve issues with scalable Authentication-Authorization-Accounting (AAA) mechanisms combined with mobility management.

The European Union also funded the DRiVE [154] project (Dynamic Radio for IP Services in Vehicular Environments), which aims to solve the conflict between the reality of scarce radio resources and the citizens' expectation for cost-efficient provision of mobile multimedia services for information, education, training, and entertainment. This research focuses on the convergence of cellular and broadcast networks in a heterogeneous multi-radio environment to deliver in-vehicle multimedia services for information, education, training, and entertainment. This project lays the foundation for provision of high-quality wireless IP communication in a cost-efficient manner. The way to do it is to optimize the inter-working of different radio networks (GSM, GPRS, UMTS, DAB, DVB-T) in a common dynamically allocated frequency range. An IP-based mobile infrastructure for optimized inter-working of radio networks has been proposed to enhance the co-operation between network elements.

3.4 Related Work within Organizations and Industry

The main drive force for incoming call service infrastructure is the Third Generation Partnership Project (3GPP), which intends to realize an IP Multimedia Subsystem (IMS) frameworks as an the IP extension to the 2G/3G networks [155]. IMS largely re-uses the existing architectures and Internet protocols, and supports the interworking with various types of access networks and legacy circuit-switched networks. 3GPP suggests that IMS integrates Wi-Fi as one of the access networks connected with IMS. The inter-networking architectures and handoff procedures are standardized in [156], where the seamless mobile multimedia applications are created by the Call Session Control Functions (CSCFs) and the AAA functions are implemented by the Diameter³⁴ protocol according to different scenarios.

The European Telecommunications Standards Institute (ETSI) has standardized the requirements and architectures for inter-networking between Wi-Fi and 3G Systems in [157], which specifies two approaches, namely, loose coupling and tight coupling. The loose coupling is suggested for Wi-Fi/Cellular framework architectures, where Wi-Fi is connected to the cellular network through an external IP network. This approach is less proprietary but real-time handoff may be more difficult to achieve [158] [159]. In tight coupling, Wi-Fi appears as another access network to the cellular core network and an inter-networking gateway is provided for adaptation between the two systems. In this way IMS treats the Wi-Fi as an access network and the traffic is routed to Wi-Fi via the IMS framework in a seamless way. However, this approach has less flexibility to transfer the traffic between the mobile and fixed networks.

The Fixed Mobile Convergence (FMC) service is proposed by the Third Generation Partnership Project 2 (3GPP2) as a collaborative 3G telecommunications specification-setting project comprising North American and Asian interests [160]. In addition to the FMC, there is a parallel activity named mobile-mobile convergence (MMC), which concentrates on the mobile convergence framework with different coverage technologies. The

³⁴ Diameter, a successor to RADIUS, is a next generation protocol for authentication, authorization and accounting.

3.5 Related Work in Mobility Management

Unlicensed Mobile Access (UMA) [161] has been supported by the UMA Consortium for mobile convergence under IMS framework. In the area of service interoperability, an Open Wireless Architecture (OWA) platform is proposed to integrate all radio access technologies into a common frameworks by a novel access discovery mechanism [162]. The OWA is a global organization including a large list of product and service manufacturers from 3GPP or 3GPP2, and is responsible for the delivery of a set of open technical specifications for application and service frameworks. Furthermore, interoperability and handoff between heterogeneous networks are also considered by the IEEE. The IEEE 802.21 [163] is actively working on the integration of 802 and non-802 networks, where a framework for interoperability between heterogeneous networks is proposed by implementing a media independent handoff (MIH) layer to coordinate multiple interfaces regardless of the underlying physical layers.

3.5 Related Work in Mobility Management

In the last several years there have been considerable publications on mobility management protocols operating at different layers of the classical protocol stack, e.g., link, network, transport, and application layer [164].

Link-layer mobility solutions have been proposed to resolve the limitation of radio coverage. Since the link layer is closely related to the wireless medium, it is challenging to have a truly unified mobility solution for heterogeneous networks. One example is the multi-link Point-to-Point Protocol (PPP) [165], which attempts to bundle multiple data-link level access channels into a single logical link. However, it is highly unlikely that the independent Internet Service Providers (ISPs) will allow arbitrary users to bundle their links into "one logical link" [166].

As for the application-layer mobility solutions, mobility supported by SIP has been discussed in many publications. [167] has proposed a SIP-based architecture to support IP-centric handoff for wireless networks while maintaining quality of service. In addition, [128] has presented an analysis of the delay associated with vertical handoff using

SIP in internetworking environments, and the analytical results showed that the handoff incurs unacceptable delay for supporting real-time multimedia services.

New approaches have been proposed by introducing a new layer. For example, [168] has introduced a new host identify layer between the IP layer and the upper layers, and further proposed Host Identification Protocol (HIP) to overcome the complexity problems of MIPv6. Furthermore, [169] has proposed the mobility support of HIP and has proven that it suffers from the same problem as MIPv6.

Lots of mobility solutions have been proposed to operate on network layer depending on the contribution made by MIP [119] and related optimizations. [170] has investigated the performance of various IP mobility architectures and has suggested to use MIP and related optimization mechanisms for selected wireless Internet applications. [171] has argued that legacy mobility management render a poor quality delivery and presented the enhancements for IP-based hierarchical mobility management. [172] has proposed a smooth mobility scheme to minimize the handoff delay by using pre-authentication and pre-registration for tightly coupled architectures. In [159] the handoff affect on an active TCP flows has been studied in a loosely-coupled MIPv6 system with a number of network-layer handoff optimization techniques. [173] and [174] have performed a real measurements of MIPv6 handoff performance on Linux testbed and discovered that the handoff delay for MIPv6, which is directly proportional to the router advertisement interval, is much higher when the router advertisement interval is large.

3.6 Conclusions

Over the past years, a number of services and projects have been promoted in the market to establish cost-efficient voice communication, and interoperability and handoff between heterogeneous networks. This chapter has reviewed recent related work and provided background information by analyzing the existing projects that are relevant to the CBM-ICC service. At the beginning, we have reviewed the three existing most popular services such us, Skype, VoIP and Cisco Call Manager. Then we have studied the related work within academia, standardization organizations and industry. Finally the chapter also

3.6 Conclusions

considered the areas of previous research on mobility management for next generation all-IP-based wireless systems. This will aid us to know the strengths and weaknesses of the CBM-ICC compared with other services/projects. It is clear that the research in this thesis is different from that carried out before and reported in the literature.

Any sufficiently advanced technology is indistinguishable from magic.

—Arthur C. Clarke(1917-2008)

4

CBM-ICC Service

4.1 Introduction

In recent years, we have witnessed an evolution on traditional telecommunication towards a consumer-oriented service. The new CBM-based Incoming Call Connection (CBM-ICC) service accommodates this evolution and aims to allow mobile users to create their own preferences based on different requirements and to dynamically switch across multiple wireless access technologies. This chapter presents in detail the CBM-ICC service. Foremost, we start with the argument that the legacy SBM-based Incoming Call Connection (SBM-ICC) is not suitable for the UCWW, and further advocate the upcoming paradigm shift from the existing SBM-ICC service towards the CBM-ICC service provision. The fundamental CBM-ICC concepts are presented in Section 4.3. Section 4.4 compares the CBM-ICC service with other exiting services on the market. Section 4.5 then explains the operational demonstration of the CBM-ICC service, and outlines the two different operational models in comparing manner. Finally the addressing issues are examined in Section 4.6.

4.2 Traditional SBM-ICC Service

The fixed-to-mobile convergence (FMC) and heterogeneous networking have profoundly changed the business roles and the competitive environments for wireless ANP and TSPs. The legacy SBM-based ICC service (SBM-ICC) had been adopted since the innovation of mobile communication services and has dominated the telecomm market for many years. With the growth of teleservices today, we begin with an argument that it is no longer suitable for fostering the multi-access wireless network environment, and thus is not flexible enough to support heterogeneous ANPs in the future UCWW.

The traditional SBM-ICC service approach is shown in Figure 4.1, where a mobile user often has a long-term contract with one ANP, often named 'Home ANP'. Compared to this, the other ANPs may be named as 'Foreign ANPs'. The legacy SBM-ICC service is based on the principal technical foundation that the mobile user has a subscriber account with one 'home ANP' (or more, e.g., through multiple SIM cards) which owns the local loop and the user's identity. While placed at the center, the home ANP acts as both the effective manager and supplier of its users' wireless access communications and AAA activities. Mobile users must have a long-term contract with the home ANP, which manages the user's address and access to the network, and the billing activities, no matter the user is local or roaming. The SBM-ICC service has shown numerous disadvantages, as described e.g. in [24]. One defective factor is that subscribers cannot easily change the ANP to take advantage of more attractive price/performance options from other providers, as this is a matter of formal subscriber contract switching.

The roaming for the SBM-ICC is complex and costly. The unique relationship with the home ANP guarantees that all incoming calls will be forwarded to this ANP first. The roaming support will in fact consist of at least one other network, e.g., ANP, the network within which user is presently roaming. Service Level Agreements (SLAs) are presumed to be in place between home ANP and foreign ANPs, both of which charge a significant fee in case of roaming.

The traditional SBM-ICC architecture is not flexible enough to support the ICC service in the future UCWW, because each mobile user is associated with a unique (telephone)

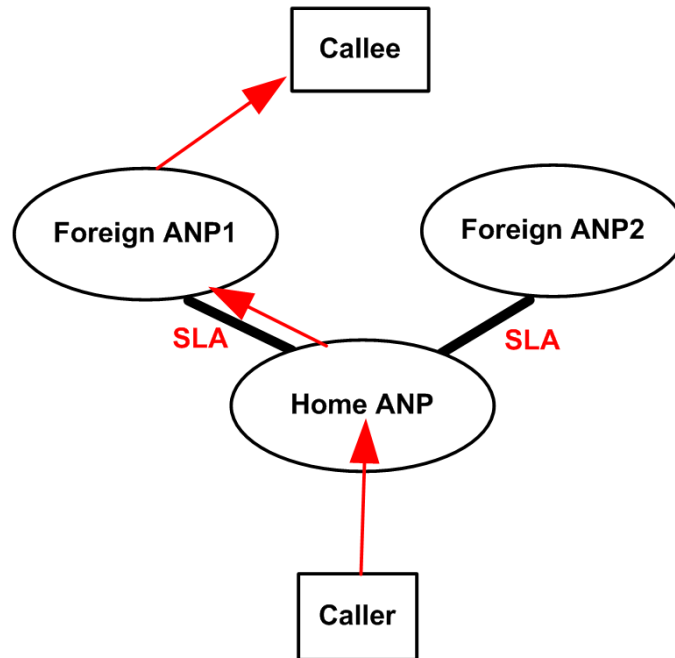


Figure 4.1.: The traditional SBM-ICC service. In this service a mobile user often has a long-term contract with one ANP, often named 'Home ANP'. All incoming calls will first come to this 'Home ANP' even if the user is roaming.

number assigned by the home ANP. Once the home ANP is changed, the number must be changed accordingly. The only way for a user to be 'multi-homed' is to buy multiple SIM cards and swap between these cards within single mobile handset (or to use multiple handsets, which is not very convenient). In order to take advantage of different service tariffs in different ANPs, the mobile user has to choose different SIM cards for work-related and personal calls to optimize economic usage of services. This, however, introduces a great deal of extra expense for both users and service providers.

Additionally, the signaling service features in SBM-ICC only support limited call control. The increasing trend for users to demand more flexible personalized call services, such as blocking and forwarding the calls according to dynamic users' preferences, requires more flexible and adaptable ICC service provision oriented towards users' needs.

4.3 New CBM-ICC Service

As a paradigm for future heterogeneous wireless communications environments, the UCWW will trigger a radical evolution towards a consumer-oriented services. A novel CBM-ICC service is proposed and described here as an alternative to the existing SBM-ICC service and a strong candidate for next generation networks. The emerging CBM-ICC service aims to develop a new autonomous mobility and call control architecture (open and partially controlled by the user), which will better meet user's subjective ABC&S requirements. The corner-stones for the UCWW are the creation of trusted 3P-AAA-SPs and a consumer-owned address, which is a globally unique, permanent, and network-independent address. The former is ANP-independent and through them users will pay service providers for the use of their services via reliable and secure charging and billing mechanisms. For the latter a new IPv6 personal address class has been proposed in [24, 9].

With the above creation, the distinction between 'home' and 'foreign' ANPs disappears, as shown in Figure 4.2. The mobile user can be easily accessible through suitable ANPs by the help of independent ICC-SPs. Different ANPs could be accessible at the same time with only one CIM avoiding the need to have multiple SIM cards in SBM-ICC service. An open autonomous flexible association is proposed to allow mobile user dynamically associate with more than one ANPs for the ICC service, (i.e. becoming multi-homed), e.g. one ANP (say Wi-Fi) used for personal or family incoming calls satisfactorily matching economic and QoS profile for these calls, and another ANP (say UMTS) for business calls requiring the best QoS available. As there is no home ANP in the UCWW, all incoming calls go directly to ICC-SP, who manages the 're-direction' of these calls to the 'current' ANP(s) of the mobile user. Besides, the user can be simultaneously accessible through different (heterogeneous) ANPs regardless of underlying transport technologies. Thus mobile user appears always as a local user and hence will not pay any roaming charges whatever ANP s/he seeks services from.

Another key innovation of the CBM-ICC service is to provide flexible and personalized Intelligent Call Management (ICM). With this new approach to the CBM-ICC service

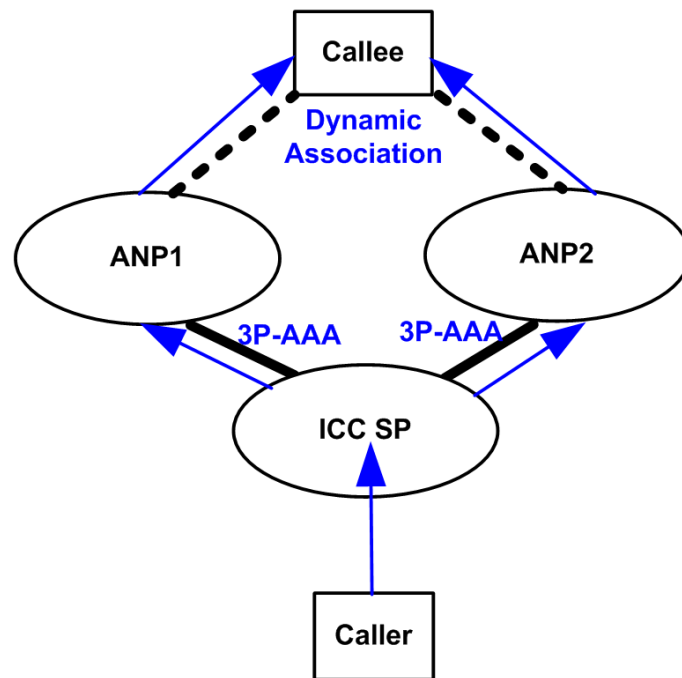


Figure 4.2.: The novel CBM-ICC service. In this service, all incoming calls will come to independent ICC-SP. Each call will be forwarded via the most appropriate ANP according to user's preferences. The callee could be dynamically associated with multiple ANPs

the range of advanced flexible and personalized ICM services opens up and provides attractive potential, e.g., incoming calls being handled and managed on the basis of access, filtering, and redirection policies pre-defined and/or dynamically defined by users (callees) according to different caller types and callee roles, callee/caller location, callee preferences, time/day/week configurations, etc. This will allow users (callees) to create their own (different) lists of callers (e.g., a 'white list' for callers allowed to contact them directly, a 'black list' for callers that are always blocked, and a 'grey list' for unknown callers whose calls are redirected to secretaries/associates, voicemails etc.).

The key benefits of the emerging CBM-ICC service include better support for multiple and heterogeneous ANPs, and reduced roaming costs. In addition, it introduces new and open environments to allow more competitive new ANP and TSP entrants making profit in fast and low-cost manner. The traditional telecommunication business will be expanded with those new ANP and TSP entrants. As a result, a more competitive business

4.4 Comparison of CBM-ICC with Other Services

environment is created, which in turn prevents the 'big brother' from monopolizing the telecom market and, in return, benefits the consumer. In order to provide the possibility to let the user control what calls should be allowed through any given ANP, the CBM-ICC service provides a Hot Access network Change (HAC) in the autonomous call control architecture for seamless handoff across different ANPs. The important feature for HAC is to switch a live CBM-ICC service session from one ANP to another seamlessly and transparently with minimum affect on the ongoing calls.

4.4 Comparison of CBM-ICC with Other Services

In this section we will compare the CBM-ICC with several relative services, namely Skype, VoIP and Cisco Call Manager (CCM), as listed in Table 4.1.

Considering the service model, VoIP and CCM are based on the traditional client-server model, while (except authentication) Skype is entirely based on a decentralized infrastructure, i.e., user information is distributed among nodes and all signaling messages are transmitted in a P2P fashion after authentication. The main difference between the CBM-ICC service and other services is that the CBM-ICC service employs two operational modes, which makes it easier to scale to large-size networks and reduces the potential costs of a centralized infrastructure.

In terms of authentication, Skype uses public-key mechanisms under the classical client-server model, while the standard VoIP employs a stateless HTTP-based authentication mechanism, which may be inadequate for assuring the identity of the end-user based on cryptography [175]. The authentication issues for the CBM-ICC service are handled by 3P-AAA-SPs, who ensure safety of the information for charging and billing purposes.

For transportation, Skype and VoIP mainly rely on either TCP or UDP, but UDP is commonly used by VoIP for both signaling and communication data. The main difference visually between CBM-ICC and other services at the transport layer is that the data in CBM-ICC is mainly carried by SCTP, which is deemed as the next generation transport-layer protocol to replace TCP and UDP, and provide advantage for seamless handoff between different ANPs.

4.4 Comparison of CBM-ICC with Other Services

Table 4.1.: A comparison of CBM-ICC service with relative services.

	Skype	VoIP	Cisco Call Manager (CCM)	CBM-ICC
Service Model	P2P	Client-server	Client-server	Two operational modes
Authentication	Public-key mechanism	AAA	Skinny	Personal IP, 3P-AAA
Service Type	Voice Video File Chat Skypein Skypeout	Voice Video File Chat	Voice	Voice Video File Chat
Transport-layer Protocols	TCP, UDP	TCP, UDP, RTP	TCP, RTP	SCTP, UDP
Codecs	iLBC, iSAC, or other unknown codec.	iLBC, GSM 06.10, MS-GSM, G.711-Alaw, G.711-uLaw, G.726, G.721, Speex, G.722, CELT	G.711-Alaw, G.711-uLaw, G.729a, G.723, GSM	iLBC, GSM 06.10, MS-GSM, G.711-Alaw, G.711-uLaw, G.726, G.721, Speex, G.722, CELT
HAC Support	No	No	No	Yes

4.4 Comparison of CBM-ICC with Other Services

Considering voice codecs, Skype and CCM choose some unknown codecs due to the proprietary. Some traffic engineering studies [138] unveil that Skype uses iLBC³⁵ [176], iSAC³⁶ [177]. [178] indicates that in Skype iSAC is one on the list for end-to-end calls, and G.729 is the preferred Codec for SkypeOut calls. The CCM comes with low bit rate (LBR) codecs, such as G.729a and G.723. The CBM-ICC service is built on an open-source platform and thus accommodates all the open-source codecs.

The CCM only provides voice services. VoIP offers end-users several services: voice communication, file transfer, and chat services. Skype and VoIP also provide video communication. In Skype, voice calls can also be directed toward the PSTN using Skypein/Skypeout service. On the other hand, the CBM-ICC service is more than just the traditional telecommunication ICC services. It also provides a list of new features such as call forwarding/transferring based on location and time, for example, the service can be re-configured based on current context of the callee, to route calls to him/her accordingly.

Skype and original VoIP are unlikely to support voice mobility deployments. The CCM supports the voice mobility only over Wi-Fi but not for heterogeneous networks. On the contrary, the CBM-ICC service supports full voice mobility networking over varying ANPs. In a sense, the voice traffic can be switch to different ANP no matter if the ICC session is active or not.

Furthermore, Skype and CCM use proprietary protocols with encryption technology, which tends to lock the user into one service provider only. It is essential for the CBM-ICC service to support an open architecture, which will empower the consumer to dynamically associate with a number of ANPs simultaneously, and to choose the best ANP for each particular type of incoming call according to the caller's type, callee's location and preferences, and time/day/week configurations. In addition, the CBM-ICC service provides open interfaces and standards, which allow mobile users to access the service in a simple and cheap fashion.

³⁵ Internet Low Bitrate Codec (iLBC) is a royalty-free narrowband speech developed by Global IP Solutions (GIPS) target for VoIP applications, streaming audio, and messaging.

³⁶ Internet Speech Audio Codec (iSAC) is a wideband speech codec, developed by Global IP Solutions (GIPS). Unlike iLBC, this codec is proprietary and implementations have to be licensed from GIPS.

4.5 CBM-ICC Operational Demonstration

Having assessed other available services, it is clear that none of the existing relative service have provided all the functionality as CBM-ICC does. The CBM-ICC service is not designed to lock the mobile user into one ANP/TSP. On contrary, the improvement of the CBM-ICC services enables users roam and handoff between various wireless networks and service providers using multi-mode handsets. Furthermore, the CBM-ICC service supports not only an open architecture but also a wide range of applications through multiple wireless networks. These applications include not only traditional telecommunication services, but also data and multimedia services. High-data-rate services with good system reliability will be supported, while a low-per-bit transmission cost will be maintained. Therefore, compared with the other services, the CBM-ICC is relatively novel in terms of voice mobility, open architecture/interfaces, and consumer-oriented features.

4.5 CBM-ICC Operational Demonstration

The general operation of the CBM-ICC service is depicted in Figure 4.3 with the main steps explained below.

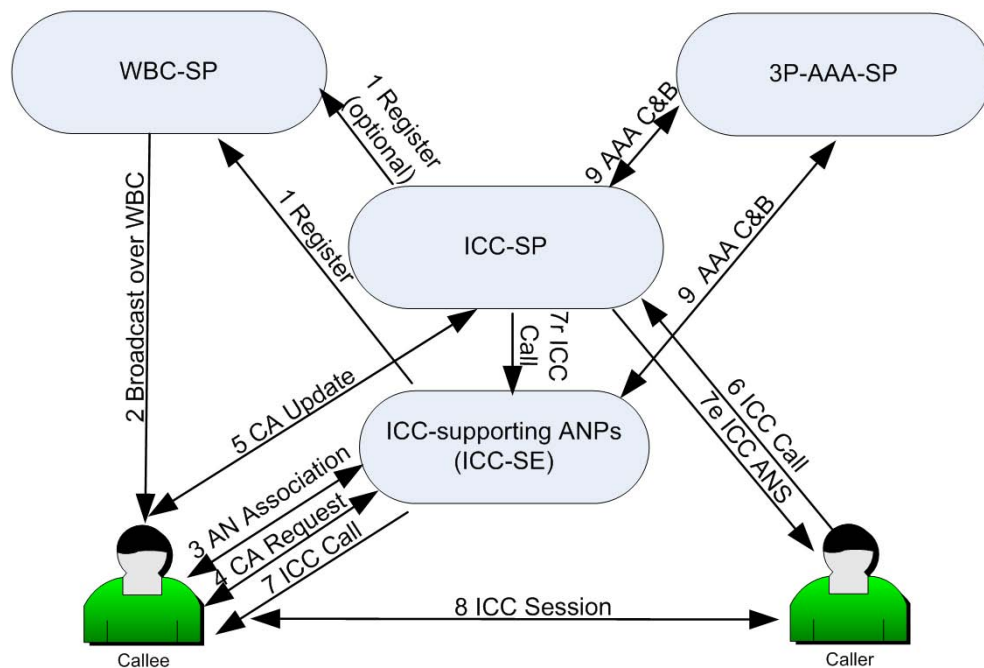


Figure 4.3.: The CBM-ICC service schematic.

4.5 CBM-ICC Operational Demonstration

Step 1: All ANPs that support ICC service³⁷ in a particular location/area register themselves with a Wireless Billboard Channel Service Provider (WBC-SP) to broadcast information about their ICC service support.

Step 2: WBC-SP periodically broadcasts the ICC service-supporting ANP's configuration and service information.

Step 3: Callee's MT listens to the broadcast channel (WBC), chooses an ICC service-supporting ANP, which best suits user's needs, and then automatically associates with this ANP/AN.

Step 4: The callee requests from ANP a temporal Contact Address (CA) to which incoming calls will be globally routed over the Internet. This CA is bound to the callee's personal address. The ANP satisfies this request after checking the user's identify and credit allowance with the 3P-AAA-SP (for the seek of clarity, this step is not shown in Figure 4.3).

Step 5: The callee updates the new CA with his/her own ICC-SP who will then be empowered to direct any incoming calls to the callee through the chosen ANP in accordance with the predefined instructions.

Step 6: The caller initiates a call to the callee via ICC-SP. The ICC-SP's name and IPv6 address are resolved by the caller from the CAI supplied by the callee (this could be done by simply clicking on a 'call me' button on the callee's personal web page).

Two modes of operation are possible further: an enquiry mode (E-Mode) and a redirection mode (R-Mode).

Step 7e: If operating in an enquiry mode, the ICC-SP informs the caller of the present callee's CA. The caller then will establish an ICC session in peer-to-peer manner (Step 8).

Step 7r: If operating in a redirection mode, the ICC-SP re-directs the call to the present callee's CA.

Step 9: The ICC service-supporting ANP has indirect business agreement with the ICC-SP via the 3P-AAA-SP. All subsequent Accounting, and Charging and Billing (C&B) activities are handled by the 3P-AAA-SP.

³⁷ Further, if not specially mentioned, 'ICC service' denotes 'CBM-ICC' service.

4.5.1. CBM-ICC Operational Modes

Depending on the type of the caller, the CBM-ICC service may operate differently as follows:

- for 'white list' callers — by allowing the call;
- for 'grey list' callers — by 're-directing' the call to the callee's voicemail or to the callee's secretary/associate etc.;
- for 'black list' callers — by denying the call.

The various way the ICC-SP may handle calls requires different operational modes. Two clear ones are: (1) enquiry mode - by returning to the ('white list') caller the callee's 'current' CA retrieved from a database; the caller then will establish a direct ICC session with the callee. (2) redirection mode - by 're-directing' the call request to the callee's 'current' CA, i.e., establishing an ICC session through the ICC-SP.

Both modes have their own advantages and disadvantages as summarized in the following subsections.

4.5.1.1. Enquiry Mode (E-Mode)

The enquiry mode moves the complexity out of the network and requires relatively less network infrastructural support. In enquiry mode, ICC-SP will not forward the ICC signaling messages to another hop in the network. On the other hand, it always generates a response, e.g. ICC-MOV, with the new contact address of the callee.

The signaling flows for the enquiry mode are shown in Figures 4.4 and 4.5, and described below:

- The caller sends an ICC-STP (INVITE) message to the ICC-SP.
- The ICC-SP receives the ICC-STP message and looks up the called party on USER_DB to find its current contact address.
- The ICC-SP generates an ICC-MOV (Moved Temporarily) message and sends with the current callee's contact address to the caller.

4.5 CBM-ICC Operational Demonstration

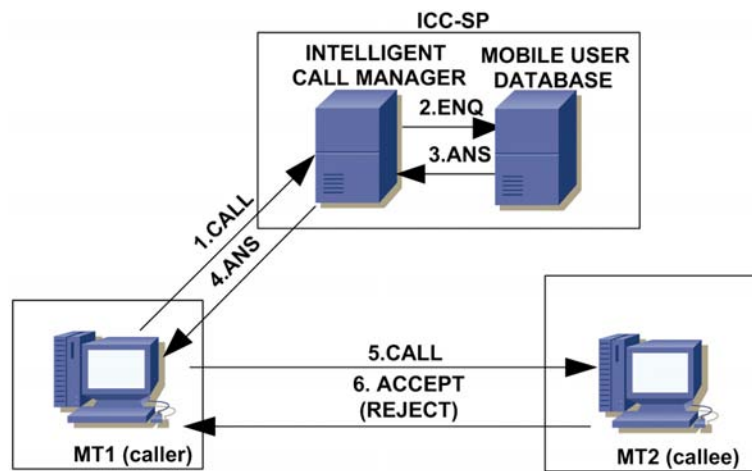


Figure 4.4.: The CBM-ICC service in enquiry operational mode (E-Mode).

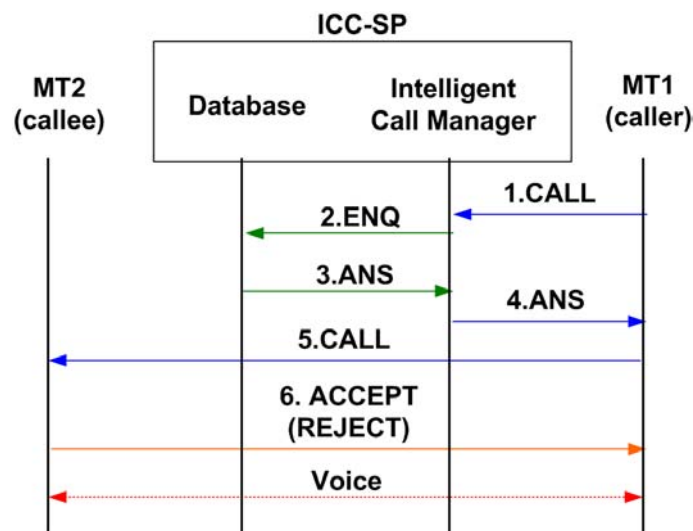


Figure 4.5.: Signaling flows for the CBM-ICC enquiry operational mode (E-Mode).

- The caller takes the routing information from the ICC-MOV and send a new ICC-STP (INVITE) message towards the callee's current address, where the Contact filed in message header contains this address.
- The ICC service (e.g. voice) session is established after receiving an ACCEPT (200 OK) message from the caller.

4.5.1.2. Redirection Mode (R-Mode)

The redirection mode tends to use a network-oriented approach. The idea behind it is to let ICC-SP figure out the next step in the route to the intended recipient of the message. ICM may query USER_DB for the callee's location information (c.f. Figure 4.6). ICC-SP acts like a client on behalf of the requesting user (caller) and forwards the request to the next SIP server.

In this mode, ICC-SP can also protect the ICC user from direct exposure to the other endpoint which could be a threat to the network security. Generally ICC-SP just forwards requests or responses to other ICC clients or servers. However, ICC-SP can also reject requests if they do not fulfill a set of criteria, specified in the callee's profile.

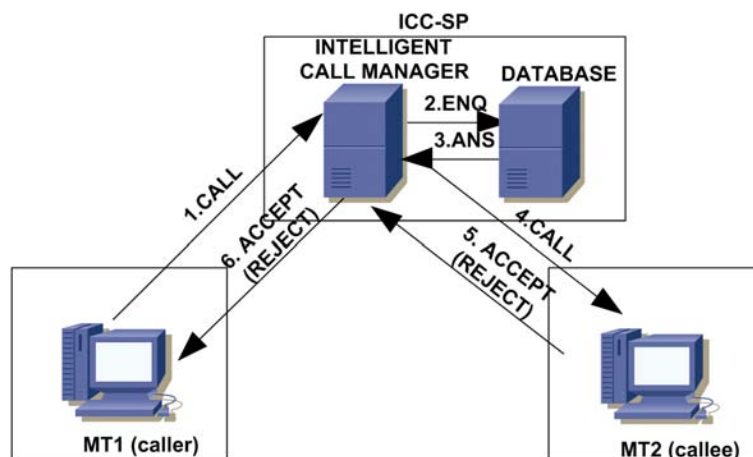


Figure 4.6.: The CBM-ICC service in redirection operational mode (R-Mode).

The signaling flows for the R-Mode are shown in Figures 4.6 and 4.7, and described as below:

- The caller sends an ICC-STP (INVITE) message to the ICC-SP.
- The ICC-SP receives the ICC-STP (INVITE) message and looks up the called party on USER_DB. The ICC-SP here acts like a proxy: it looks up the callee's new location (contact address) in USER_DB, rewrites the INVITE message, and forwards it to the callee's current contact address.

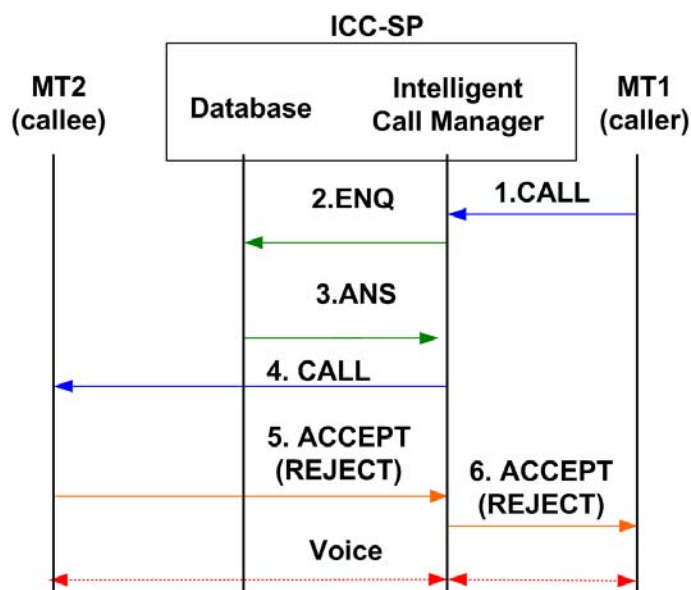


Figure 4.7.: Signaling flows for the CBM-ICC redirection operational mode (R-Mode).

- The callee replies with an ACCEPT (200 OK) message to the ICC-SP, which forwards it to the caller. Then the ICC service (e.g. voice) session is established successfully.

4.6 Addressing Issues

A new addressing system is necessary as a key component for CBM-ICC environments to replace traditional identification scheme. Several new infrastructural components are described below.

4.6.1. IPv6 Personal Address

In CBM-ICC service architecture, consumer-users should possess their own unique addresses that must be network-independent and geography independent [9]. An IPv6 personal address is proposed as unique user identification for CBM-ICC service. This address is owned by the consumer-user and would never tie to any access network. Considering global population and large addressing space in IPv6, the new class should have

at least 10 billion IPv6 addresses [24, 9], but probably several times this should be reserved. This personal IPv6 address can be obtained in a variety of ways, e.g., an ICC-SP, a 3P-AAA-SP, or an Internet shopping portal. As suggested there, a large block of IPv6 address space could be allocated for this purpose.

The personal address aims to support the following advantages to mobile users:

1. ANP independent addressing: personal address can be used independently of any ANPs and any geographical location.
2. Compatibility and scalability with existing IPv4 and IPv6 standard routing mechanisms: personal address should have no conflict with any other IPv6 address space and routing mechanism.

The format of proposed new globally significant, network- independent, person IPv6 address class can be suggested as [9] in Figure 4.8.

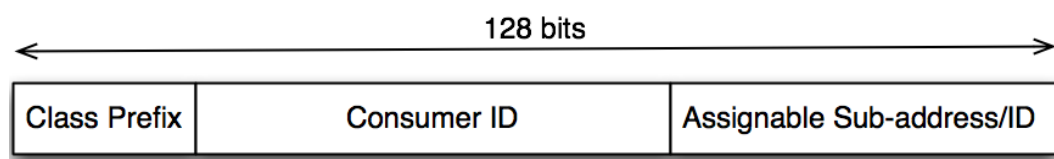


Figure 4.8.: The format of the IPv6 personal address suggested in [9].

- The person IPv6 address class can be identified by appropriately assigned *Class Prefix* field. Considering global population, the new class should contain at least 10 billion IPv6 addresses, but probably several times this should be reserved (this seems feasible, as the IPv6 address space is sufficiently large).
- *Consumer ID* field is the the primary user identification and has the length ranging from 34 to 37 bits, which will allow addressing of 17 to 137 billion people.
- *Assignable Sub-address/ID* field could be owner/consumer assignable, e.g. to be used by the owner for dependent family members, or act as an owner-defined Terminal ID. This could be useful in transition scenarios or in developing wireless scenarios, where it would greatly simplify the establishment and functioning of a user's wireless personal area network (WPAN) in any location (e.g. home, office,

hotel room etc) without a need for IP address allocation by some authority, access network provider etc [9].

Given that the IPv6 resource is finite, once allocated it must be permanently locked to specific mobile user. The mobile users may purchase as least one such address so that they may always use it for the CBM-ICC service and any other services. Once an address is purchased by a user it naturally must be prevented from being used by others. This could be achieved by a centralized purchased scheme through authorized address suppliers, each of which owning a portion/subset of this new IP address class' space and identified by an optional *Address Supplier ID* field or by characteristics in the *Consumer ID*. Personal IPv6 addresses may be sold within a 'lease-based' system. It will not be possible for the ANPs to acquire ownership of personal addresses [9].

However, since it is permanent and geographic independent, personal address is not possible to be routed over the global Internet with current routing mechanism. So it is necessary to introduce extra routing device at the border of ANP and Internet to make sure personal address is routable over Internet. From the 3P-AAA-SP point of view personal address is used to uniquely identify the mobile user for AAA purposes. Personal address is part of user's X.509 digital certificate, which is securely stored in a smart CIM card on the mobile user's terminal. The user certificate is used for AAA purposes for all types of UCWW services (including CBM-ICC service) provided to the user by respective service providers.

4.6.2. Contact Address Identifier (CAI)

Since personal IPv6 address is not globally routable, it is also necessary to define a user-friendly Contact Address Identifier (CAI) which could be associated with the personal address and point to a specific ICC-SP in a more user-friendly manner. CAI would operate in a similar manner to a Network Address Identifier [179] (NAI), in the form of user@domain. The first part of the CAI is the user identifier while the second one is information regarding the domain name, which will be used to route the CBM-ICC request to ICC-SP. It is possible for one mobile user to own and register multiple CAIs. CAI

is a public identifier which could be accessible in varying ways, such as business card, personal web pages, public directories, etc. It is possible for one mobile user to own and register multiple CAIs.

The CAI is needed to route the initial CBM-ICC request to the ICC-SP (through a domain name service, DNS/ENUM, enquiry). The ICC-SP maps the CAI to the appropriate (updated) CA of the callee for further CBM-ICC session setup.

4.6.3. Consumer Identity Module (CIM)

A secure user identity is needed to prevent personal address from being used by others. For example, it should securely store the user's personal identity and enable the user to be identified and authenticated for secure execution of CBM-ICC services. One approach we suggest for this is a system based on globally acceptable digital certificate scheme, ITU-T's X.509 [180] [5] digital certificate standard, which provides a mechanism for large-scale deployment of security, based on asymmetric cryptography. The X.509 field of "Subject alternative name" may accommodate the IPv6 personal address. A kind of universal CIM card (or its software equivalent) is proposed [9, 31] through which consumers would use their IPv6 address, and do so with whatever terminal they choose.

CIM securely stores mobile user's identity information, such as X.509 certificate (a public key used to generate dynamic security data), ICC-SP's information, user preferences, and administrative data. For security, typically, the embedding of users' digital certificates in the card and the distribution of cards (sale etc.) could be managed through the 3P-AAA-SPs. Normally, then, they will create a digital certificate to be associated with a particular consumer (analogous to a credit card). The IPv6 address incorporated could be that supplied by the consumer or be a new one. Through the relevant 3P-AAA service providers' public keys, the validity of the encrypted 3P-AAA certificates of all parties to a transaction may be mutually checked as required. So the consumer may obtain wireless services analogically in ways not unlike entering a shop and making purchases using a credit card; there is no subscriber-type agreement involved.

CIM can be implemented by latest Java smart card technology [181], which ensures the integrity protection of communication over the different ANPs. Java smart card is typically made as a plastic card that contains an embedded chip. Figure 4.9 depicts the structure of this smart card based on ideas presented in [9]. The Java Card Virtual Machine (VM) sits on the top of CIM, and defines a subset of the Java programming language. The Java Card API provides the interface for smart-card core framework, applications, and extension Java packages. A mobile user can use such smart card on any MTs to securely store/access valuable and sensitive personal information (as mentioned before).

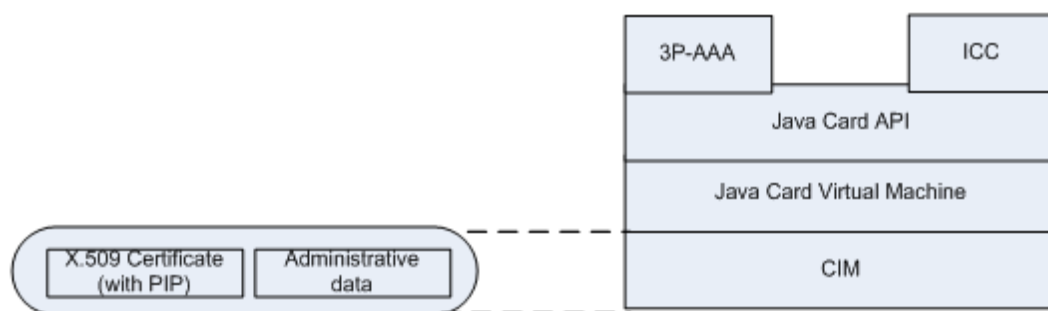


Figure 4.9.: The Consumer Identity Module (CIM) structure.

4.6.4. The Use of Contact Address Identifiers (CAIs), Contact Addresses (CAs), and Personal Addresses

Figure 4.10 demonstrates the usage concept of Contact Address Identifiers (CAIs), Contact Addresses (CAs), and Personal Addresses in the CBM-ICC service. With the personal address not being a globally routable address, a temporal CA is assigned to the callee by the consumer-chosen ANP (after a successful completion of the association and 3P-AAA procedures with this ANP). Such a function will be carried out by a CBM-ICC service supporting entity (ICC-SE) within the ANP.

For callers knowing the callee's personal address, but not having their temporal CA, a CAI is needed to route their initial ICC request to the ICC-SP (e.g. through a DNS enquiry). The ICC-SP manages the call 're-direction' (or filtering by some other means) to the current ANP(s) chosen by the callee. With this approach, the user can simultaneously

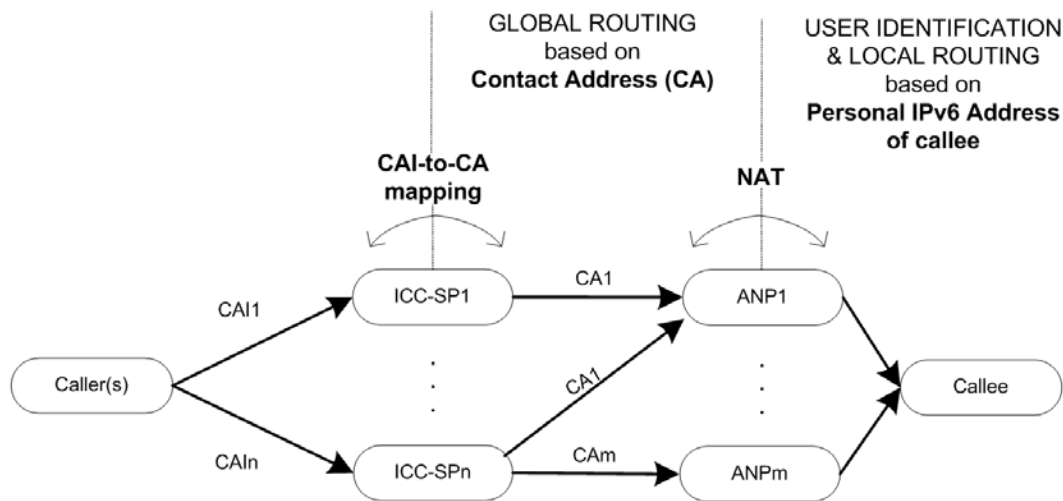


Figure 4.10.: The CAIs, CAs, and Personal Addresses in the CBM-ICC service.

accessed through different ANPs by the help of new, independent, extra-ANP ICC-SPs, which map the CAI to the appropriate CA of the callee and makes provisions for establishing the ICC session. The permanent personal address is used for user identification and local routing (within the same ANP's network), whereas the temporal contact address is used for global routing (i.e. in the Internet). As shown in the example schematic in Figure 4.10, a network address translation (NAT) between the CA and the personal address is provided by ANPs in both directions of communication.

4.7 Conclusions

The new CBM-ICC service is a truly consumer-oriented service accommodating a wide range of applications through multiple wireless networks with HAC support. This chapter has introduced the concept of the CBM-ICC service, demonstrated the basic high-level operations, and discussed the addressing issues. We started with the statement that traditional subscriber-based ICC service no longer caters for the demand and the requirements of mobile users in UCWW. The CBM-ICC service has been introduced as a substitution or a complementary technology. We then looked at the concept and benefits of the CBM-ICC service. A comparison of CBM-ICC with other existing relative services has been given in Section 4.4. By investigating the strengths and problems of these services, we

4.7 Conclusions

advocate that the main advantage of the CBM-ICC service is to offer greater flexibility in service delivery along with HAC support and more user control over service execution. A high-level CBM-ICC operation with two operational modes has been illustrated in Section 4.5. Finally, we have briefly introduced some addressing issues.

Houses are built to live in, and not to look on.

— Sir Francis Bacon (1561 - 1626)

5

CBM-ICC Service Architecture

5.1 Introduction

This chapter³⁸ introduces a novel architecture for providing the CBM-ICC service. The first step described in Section 5.2 is to extract the necessary requirements and build them into the service architecture. Then the main components and interfaces relying on existing protocols or requiring new signaling protocols (or modification/new elements of existing protocols) are described in Section 5.3 and protocol candidates are suggested in Section 5.4. Then a hot access network change (HAC) mechanism to seamlessly switch to the “best” access network is proposed and the issues for choosing a protocol for HAC are identified in Section 5.5.

5.2 CBM-ICC Service Architecture Overview

The architecture we proposed for CBM-ICC services intends to make the most of heterogeneity, ensure optimized internetworking, and provide synergy on IP-based mobile infrastructure.

³⁸ This chapter is based in part on author’s article [31] presented in IEEE 65th Vehicular Technology Conference, Dublin.

5.2 CBM-ICC Service Architecture Overview

The high-level view of the proposed CBM-ICC service architecture is shown in Figure 5.1, where the dashed arrowed lines represent logical interfaces and full lines represent physical communications links.

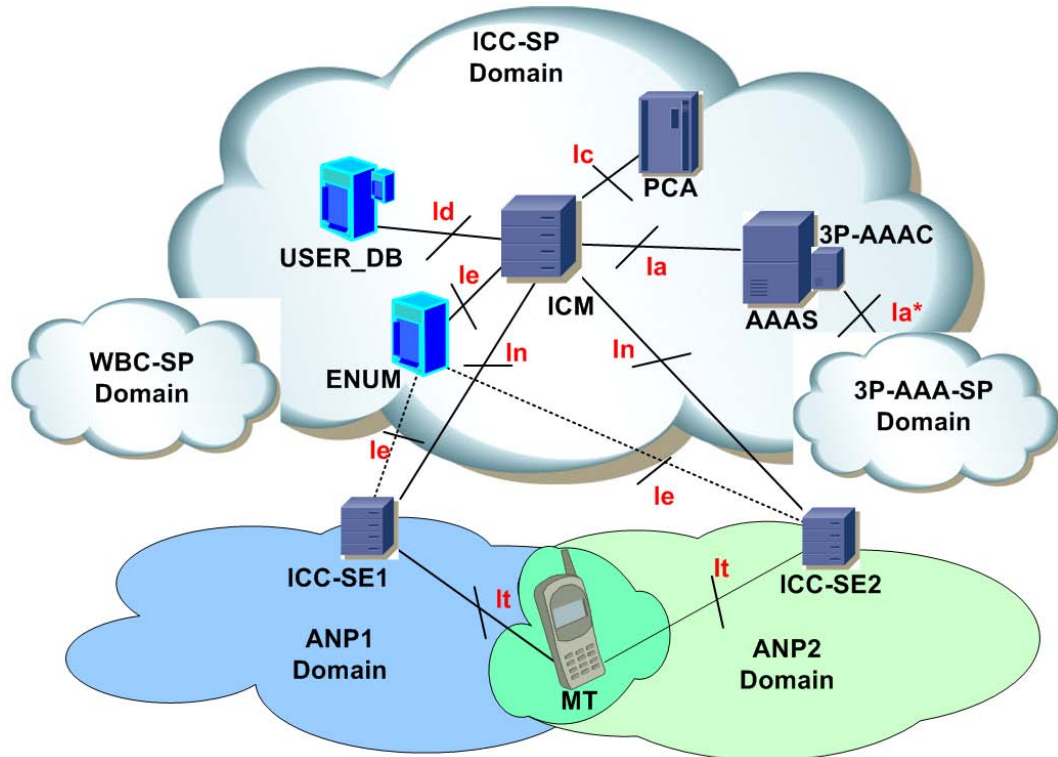


Figure 5.1.: The CBM-ICC Service Architecture. In this architecture, a multi-mode MT is capable to simultaneously associate with more than one ANP. MT may switch between heterogeneous ANs and may receive calls via more than one ANPs simultaneously.

The proposed CBM-ICC service architecture includes elements from the ICC-SP domain, and ANP domains, and involves communication with some elements in the 3P-AAA-SP domain and the WBC-SP domain:

- *ICC Service-Provider (ICC-SP)* resides externally to ANPs and consists of an Intelligent Call Manager (ICM), User Database (User_DB), AAA Server (AAAS) and 3P-AAA Client (3P-AAAC), Personal Call Agent (PCA), and ENUM Server. The detailed description of the components is given in Section 5.3;

5.3 CBM-ICC Service Architecture Components

- *ANP* domain – multiple ANPs may be involved simultaneously in the CBM-ICC service provision. The ICC service Supporting Entity (ICC-SE) is the main element of the service architecture here;
- *3P-AAA Service Provider (3P-AAA-SP)* domain - needed for AAA, charging and billing purposes for mobile users and ICC-SPs;
- *WBC Service Provider (WBC-SP)* domain - provides efficient and easy for use mechanism for service advertisement, discovery and association (ADA).

5.3 CBM-ICC Service Architecture Components

The CBM-ICC service architecture components illustrated in Figure 5.1 are explained as follows.

The **Intelligent Call Manager (ICM)** is the central ICC-SP call control entity, which handles the exchange of signaling messages and interaction with other ICC-SP's, 3P-AAA-SP's, and ANP's entities, and mobile terminals (MTs). In effect the ICM communicates directly with other components to manage and control incoming calls based on callee's preferences, and performs call re-direction or filtering/blocking, if needed.

The **User' Database (User-DB)** stores callees' profiles, i.e. their preferences, X.509 certificates (including their personal addresses), current Contact Addresses (CAs) and CAIs. The user's preferences are based on access, filtering, and redirection policies specified in a Policy Repository (PR).

The **AAA Server (AAAS)** interacts with the **3P-AAA Client (3P-AAAC)** installed on the user terminal for the purposes of users' AAA, charging and billing. The 3P-AAAC interacts with the 3P-AAA-SP infrastructure, e.g., to request credit control information (i.e., whether the caller and callee have sufficient credit for using the ICC service).

The **Personal Call Agent (PCA)** is a personal assistant employing speech recognition and text-to-voice translation (e.g., for interaction with disabled users). The PCA may be used to help the callee to create/change his/her ICC profile with preferences specifying how

5.4 CBM-ICC Service Interfaces and Signaling Protocols

each incoming call should be handled. The PCA may also provide advanced answering-machine type services for voice and other calls. The callee can interact with PCA by means of voice commands, e.g. when driving a vehicle. One typical application for PCA is to take over all incoming calls that the callee is not able to answer at some particular time, store voice mail messages, and play them later on user command. Another PCA's function is related to the management of the callee's profile stored in the database.

The **ICC Service-Supporting Entity (ICC-SE)** provides an interface between the ANP and the external world. ICC-SE makes sure all arriving packets are routed to the appropriate callee. For this, ICC-SE provides NAT translation between callee's contact address (CA) and his/her personal address in both directions of communication.

The **ENUM Server** [100] acts like a DNS server enabling the translation between public switched telephone network (PSTN) E.164 numbers and IPv6 addresses.

5.4 CBM-ICC Service Interfaces and Signaling Protocols

The interfaces between different CBM-ICC service components and envisaged protocol signaling candidates are depicted in Table 5.1.

5.4.1. Ia/Ia* Interface

Signaling messages over the Ia/Ia* interface are exchanged by means of an AAA protocol. The Diameter protocol [182], which relies on the client-server model, is considered as a promising candidate here. However an extension to this protocol needs to be developed for the case of AAA handled by a third party. 3P-AAA-SP authenticates users and provides relevant accounting, charging and billing for services used by them. ICC-SP authorizes (or not) users to use the ICC service based on information received from 3P-AAA-SP. All exchanged messages are encrypted end-to-end for security reasons.

5.4 CBM-ICC Service Interfaces and Signaling Protocols

Table 5.1.: The CBM-ICC service interfaces and protocols.

Interface	Entities	Description	Protocol
Ia/Ia*	MT ↔ AAAS 3P-AAA ↔ 3P-AAA-SP	Exchange of 3P-AAA messages	3P-AAA extension of Diameter
Ic	MT ↔ PCA	Interaction between PCA and MT	CPL/VoXML
Id	PCA ↔ DB ICM ↔ DB	Enquire/store data in the database	LDAP/SQL
It	MT ↔ ICC-SE	Interaction between MT and ICC-SE	SIP/SDP//H.323/SS7
In	ICM ↔ ICC-SE	Interaction between ICM and ICC-SE	SIP/SDP
Ie	ENUM ↔ ICC-SE ENUM ↔ ICM	Convert E.164 number to ICC support format	ENUM/DNS

5.4.2. Ic Interface

The Ic interface is implemented by Call Processing Language (CPL) [183] [184] and Voice Extensible Markup Language (VoiceXML) [185] [186] .

Call redirection, filtering and blocking can be implemented by XML-based CPL script on PCA. CPL is lightweight, efficient, and extensible. The callee controls the incoming calls through a web application, which translates the user requirements into a CPL script just like statements on how the callee prefers to receive incoming calls. The callee also can create the CPL script on MT and upload it to PCA under the security guarantee of 3P-AAA-SP.

By using VoiceXML - an XML-based language to create voice dialogs through voice-recognition technology - the callee is able to define his/her profile and change preferences in an oral manner, while the caller can interact with PCA by listening to audio output that is either prerecorded or computer-synthesized.

5.4.3. Id Interface

The Id interface is mainly used to store to and retrieve from the database the callees' profiles. A new profile is created in the database as soon as a new user purchases the ICC service from ICC-SP. In general, each callee's profile contains CAI, CA, X.509 certificate (with the user's personal address), and multiple preferences as shown in Table 5.2.

Table 5.2.: An example of callee's preferences.

From	Action	Method	To	Type	CoS
2001:881	Forward 'cheapest' CA	"sip"	1080:899::1	Family	Silver
2001:882	Forward 'best QoS' CA	"video:tel" "voice:tel"	1080:899::2	Business	Gold
2001:883	Voicemail and Forward	"SMS"	0871783344	Unknown	Bronze
2001:884	Voicemail and Forward	"email:mailto"	call@icc.com	Unknown	Gold
*	Block and redirect to voicemail	"voice:record"	N/A	Unknown	Bronze

ICM retrieves the relevant entry of this table through the Id interface and assesses it. The first entry in Table 5.2 indicates that silver type family calls from personal IP address 2001:881 are forwarded to the contact address (CA) corresponding to the lowest possible call cost. A business caller with an IPv6 address 2001:882 is able to use gold Class of Service (CoS³⁹) to make video calls and/or excellent QoS telephone calls for an incremental extra cost. An unknown incoming call from an IPv6 address 2001:883 is redirected to a voicemail along with a SMS notification sent to mobile number 0871783344. An unknown incoming call from an IPv6 address 2001:884 is redirected to a voicemail on an email address call@icc.com. All the other unknown bronze CoS incoming calls are blocked and redirected to a voicemail.

³⁹ Class of Service (CoS) specifies different types of service that can be used to differentiate traffic.

5.4.4. It and In Interfaces

The It and In interfaces are used for an exchange of call control signaling and mobility management messages. The call signaling protocol is primarily based on SIP. In cooperation with SIP, the SDP protocol is also used to describe parameters of the session and to keep track of all ongoing sessions. The MT could be viewed as a SIP User Agent (UA). The ICM in ICC-SP acts as a SIP server that processes the received requests and sends responses.

5.4.5. Ie Interface

The Ie interface is used to communicate with the ENUM server, which can translate E.164 numbers into IPv6 addresses (and vice versa) using the existing DNS hierarchical structure. For this, a new domain, e164.arpa, is introduced by ENUM. The rules in this domain are encoded in Naming Authority PoinTeR (NAPTR) Resource Records in the form of URIs. The look-up procedure of this interface is very similar to the normal DNS operations.

5.5 Hot Access Network Change (HAC)

There are different aspects of the access network change that may be involved as part of the CBM-ICC service. The traditional one is named as the cold access network change, which means choosing a different access network from the previous one before starting the actual service. In the traditional access network change, MT may only have one active connection within an area at the same time. However, in a multi-access scenario there are more than one active links existing between the MT and the ANPs. Therefore ABC&S-based switching of live connections seamlessly among access networks becomes possible, and is referred to here as a Hot Access network Change (HAC) [24], (Figure 5.2).

Unlike the conventional handoff procedure, the HAC is defined as a handoff between two live access connections while on the move without user intervention and with minimal

5.5 Hot Access Network Change (HAC)

service disruptions. But devising a unique mobility management scheme for HAC is hard and requires several aspects to be considered. Table 5.3 provides a comparison between existing mobility solutions.

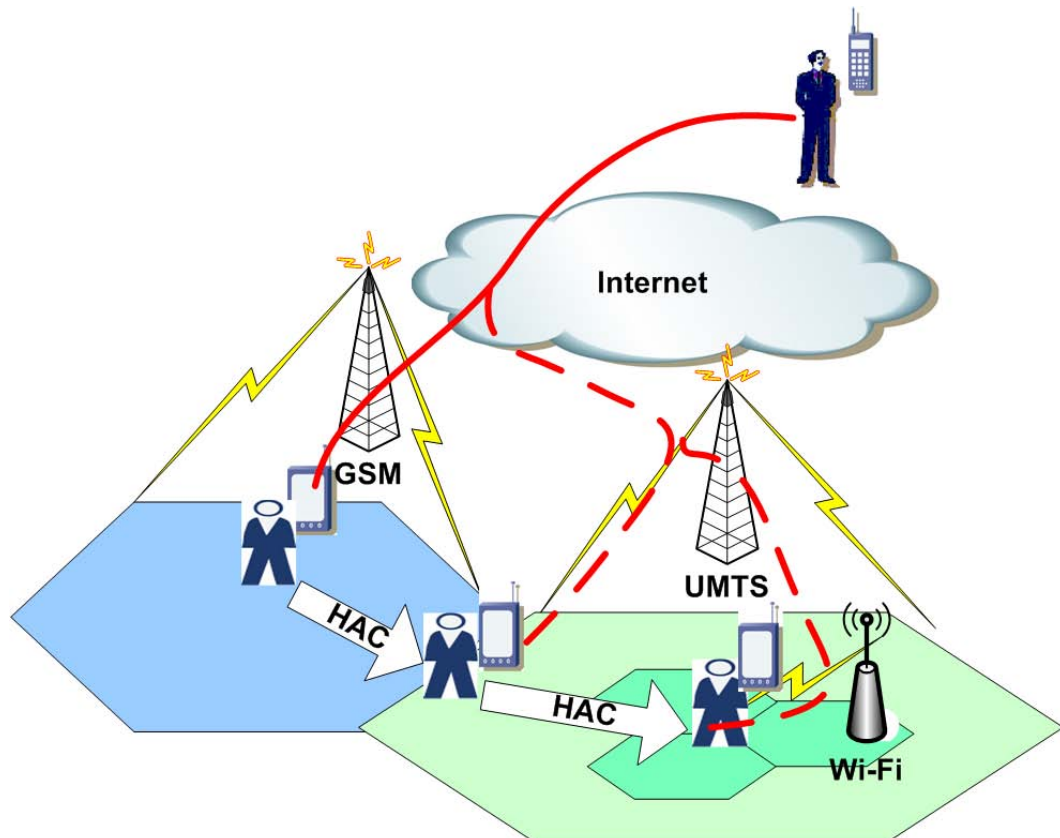


Figure 5.2.: The Hot Access network Change (HAC). In a multi-access scenario, there could be more than one active links existing between the MT and the ANPs. HAC switches an active ICC session between two live access connections without user intervention and with minimal service disruptions.

A natural solution for mobility is to solve the problem at the network layer no matter what link-layer technique is employed. Typical examples include MIPv6 and its enhancements. In order to deliver packets to the current point of attachment, the implementation of MIPv6 needs at least one additional device, the home agent. While roaming, a MT can be located by a fixed address called a Home Address. However, there are also many limitations for MIPv6. For example, the inherent feature of home agent in MIPv6 brings an extra processing delay and thus increases handoff latency and packet loss rate. Some

5.5 Hot Access Network Change (HAC)

enhanced MIPv6 schemes have been proposed, such as Cellular IP [123], or HMIPv6 [121]. However, none is well suited for our HAC requirements. The reason is that the CBM-ICC service is expected to support real-time multimedia services that are highly time-sensitive; however, network-layer handoff reveals that the connection is very likely to suffer from breaking, after the execution of a vertical handoff from one access network to another [187].

Table 5.3.: A mobility management protocols' comparison.

	MIPv6	mSCTP	SIP	DDNS/ENUM
Operation Layer	Network	Transport	Application	Application
Transport Layer	TCP/UDP	SCTP	TCP/UDP	TCP/UDP
Location Management	Yes	No	Yes	Yes
Mobile Agent	At least two agents	No agents	At least one agent	At least one agent
Handoff Performance	Limited	Better	Good	No Support

Application-layer mobility based on SIP is handled by sending an INVITE message to re-invite the end-point with the same session identifier. So at least one additional component is required, which leads to infrastructural changes. There have been many recent research works that have investigated the handoff performance of SIP over heterogeneous networks. For example, in [188] and [189] the authors have evaluated the SIP performance for a vertical handoff, and proven that handoff procedure using SIP may introduce latency for the signaling messages procedure and overhead for IP encapsulation.

In addition to the network-layer and application-layer approaches above, researchers are currently investigating the transport-layer mobility using SCTP, which is supported by the industry and deemed as the next generation transport-layer protocol to replace TCP and UDP. The authors in [190] proposed the use of SCTP to provide seamless mobility through the utilization of SCTP's multi-homing functionality and dynamic address reconfiguration

[72] (DAR) extension proposed in mobile SCTP (mSCTP). Fei *et al* have proven that using mSCTP to enable vertical handoff has many advantages, including simpler network architecture, improved throughput and delay performance [191].

Recognizing all the solutions, we propose a HAC scheme based on SCTP with mobility support. Firstly, SCTP handoff is operated at the transport layer. As transport layer is the lowest layer to provide the end-to-end data transfer, SCTP handoff is able to ignore the routing intermediate nodes, implement optimal routes, and introduce less modification on service infrastructure. This will reduce the handoff latency. Secondly, a supporting functionality with multiple ANPs is required for the HAC scheme. SCTP supports multi-homing capabilities for changing the communication path of an application. In some senses HAC benefits from the use of the multi-homed functionality provided by the SCTP protocol in both ends. More specifically, the SCTP with DAR extension [131] offers the possibility to dynamically switch a live session by adding a new IP addresses to the association. However as a transport-layer protocol, SCTP must be adopted in conjunction with support from other protocols. For example, a change of location and network type should be updated with the aid of SIP. From the service provider's point of view, DHCP or equivalent component is also needed to assign new IP address to mobile terminals.

5.6 Conclusions

This chapter has outlined the high-level architecture of the CBM-ICC service. Particular attention has been payed on the main networking components of the proposed architecture. We have made the suggestion of building the CBM-ICC architecture by choosing interface with suitable protocols. The main interfaces between these components have been identified and described. Suitable signaling protocols have been suggested. Finally a protocol candidate for HAC session switching has been selected based on initial research documented in Section 2.6 and Section 3.5, and our insight on mobility protocols. All these made us to believe that SCTP is the most attractive choice for HAC session switching due to its key characteristic including the support for multi-homing functionality and dynamic address reconfiguration. As MIPv6 and SIP schemes generate large overhead, it

5.6 Conclusions

is our opinion that a mixture of SCTP and SIP could be used as a comprehensive control of the HAC-based CBM-ICC session switching.

Everybody gets so much information all day long that they lose their common sense.

—Gertrude Stein (1874-1946)

6

CBM-ICC Service Scenarios and Signaling Flows

6.1 Introduction

The CBM-ICC service scenarios are considered as a first step of our research as to analyze each scenario step in detail from point of view of criteria for operation and protocol reference model. This chapter⁴⁰ first elaborates a generic CBM-ICC service scenario with no mobility. Then it describes a generic mobility scenario which uses a Hot Access network Change (HAC) procedure for switching a live ICC session for delivery over another access network. Both scenarios are illustrated on Figure 6.1. In the latter scenario we assume that the callee (MU2/MT2) stays in the ANP1 domain and accepts the establishment of a CBM-ICC session from the caller (MU1/MT1) and then moves to the ANP2 domain by switching the live ICC session by means of HAC. It is further assumed that both the caller and the callee have already owned an ICC service account with one common ICC-SP and have registered with the same 3P-AAA-SP with sufficient credit for the requested ICC service.

⁴⁰ This chapter is based in part on author's publications on IEEE VTC [31], IEEE ISWCS [32] and Journal of WPC [33].

6.2 Generic CBM-ICC Service Scenario with No Mobility

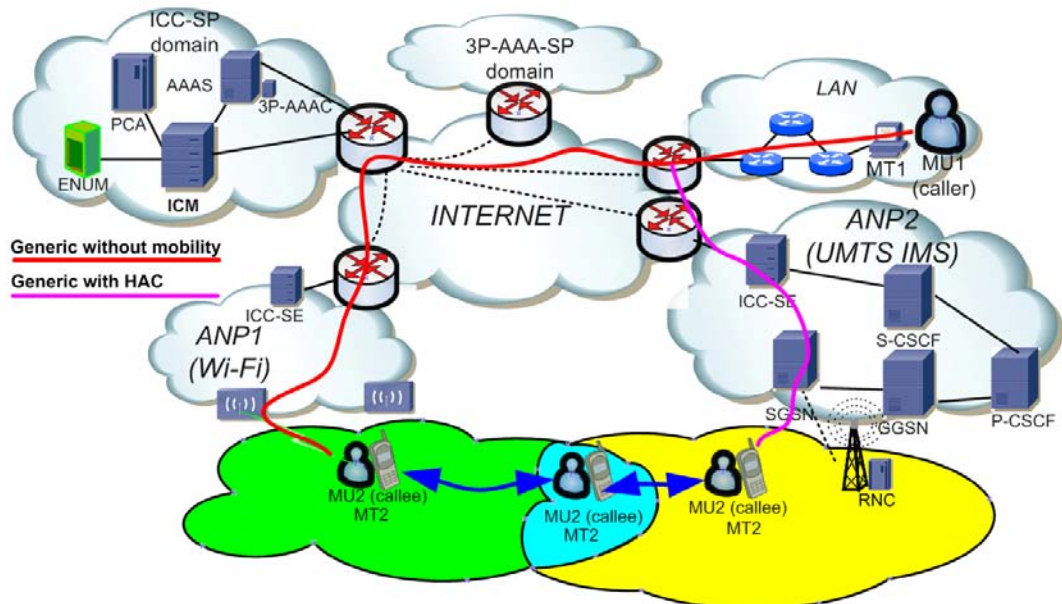


Figure 6.1.: The CBM-ICC service scenarios. It is assumed that the callee (MU2/MT2) in the ANP1 domain accepts a CBM-ICC session from the caller (MU1/MT1) and then moves to the ANP2 domain by switching the live ICC session by means of HAC.

6.2 Generic CBM-ICC Service Scenario with No Mobility

In this section we elaborate on a generic scenario with no mobility where the callee (MU2/MT2) avails of one ANP (UMTS) for ICC service support. The signaling flows elaborated for this scenario are shown in Figure 6.2. In these, different phases could be distinguished, i.e., Advertisement, Discovery and Association (ADA), Contact Address (CA) Update, ICC Session Setup, and ICC Session Release. The signaling messages are based on SIP protocol. However, the original SIP protocol is extended to take into account the CBM-ICC requirements.

6.2 Generic CBM-ICC Service Scenario with No Mobility

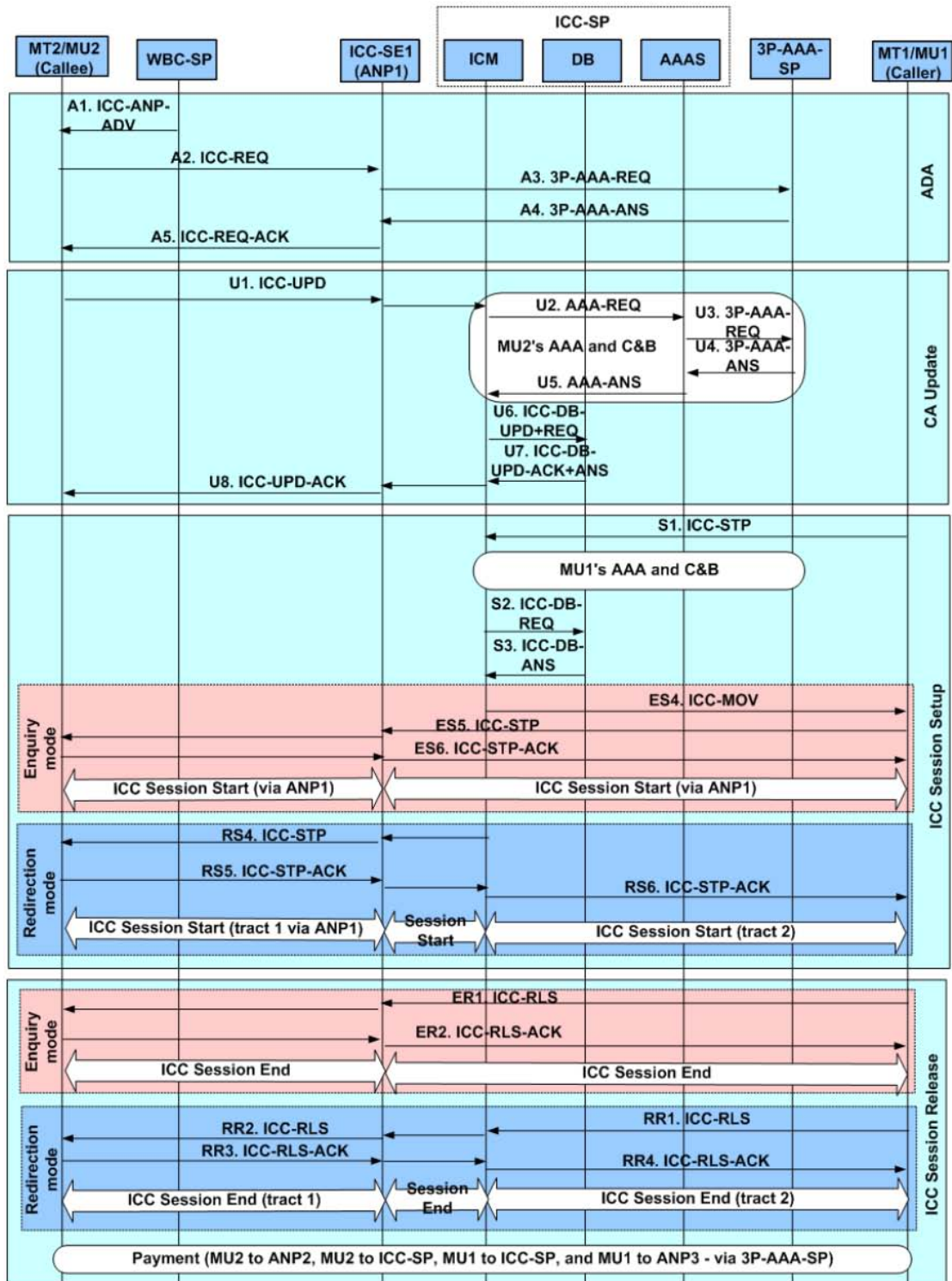


Figure 6.2.: Signaling flows for the generic CBM-ICC service scenario with no mobility (in both operational modes). It is assumed that MU1 and MU2 are associated with one common ICC-SP and MU2 avails of several ANPs for ICC service support.

6.2.1. Advertisement, Discovery and Association (ADA)

The generic ADA procedure can be described as follows. On entering the coverage area of the ANP1, the callee's terminal MT2 receives an ICC-ANP-ADV (A1) message over a Wireless Billboard Channel (WBC), informing it about the existence of ANP1 - including its association information and the IP address of its ICC service supporting entity, ICC-SE1. Upon receiving this message, the MU2/ MT2 sends an ICC-REQ (A2) message to the ICC-SE1 to request a CA1 and configuration information for ICC service provision. This is also an implicit association request. This and all subsequent messages in both directions are digitally signed for the purposes of message authentication and data integrity. (Similar scheme is used in all other phases.) Then the ICC-SE1 sends a 3P-AAA-REQ (A3) message towards the 3P-AAA-SP to request credit control information on the user (i.e., establishing user's credit-duration status for using the ICC service). If the reply message, 3P-AAA-ANS (A4), is a positive one, with user's credit-duration details, the ICC-SE1 records this, and responds affirmatively to the MU2 with an ICC-REQ-ACK (A5) message, including also the allocated CA1.

6.2.2. Contact Address Update

After obtaining the CA1, the MU2/MT2 sends an ICC-UPD (U1) update message, containing the CA1, the type of MT2, and any new ICC preferences, to the ICC-SP's ICM. As the message passes through the ICC-SE1, the necessary NAT is performed to translate from MU2's personal address to the allocated contact address CA1. On its receipt, in order to authenticate and authorize the MU2's CA1 update, the ICM sends an AAA-REQ message to the AAAS, which in turn interacts with the 3P-AAA-SP (by a 3P-AAA-REQ message) for accounting, charging and billing (C&B) purposes of the MU2. With the AAA and C&B procedures being completed successfully (3P-AAA-ANS and AAA-ANS messages), the ICM updates the MU2's new CA1 and ICC preferences on the ICC-SP database (DB) by an ICC-DB-UPD+REQ (U6) message. The DB confirms the completion of this action to the ICM via an ICC-DB-UPD-ACK+ANS (U7) message. Finally

6.2 Generic CBM-ICC Service Scenario with No Mobility

the ICM acknowledges the MU2's contact address (and preferences) update request by returning an ICC-UPD-ACK (U8) message.

6.2.3. ICC Session Setup

Next we assume the MU1 wants to make a call to the MU2 and that the MU2's CAI is already known to the MU1, e.g., from the MU2's home web page. By a normal DNS enquiry, the MU1 can resolve this CAI to the ICC-SP's relevant IP address. In order to setup an ICC session, the caller (MU1) first sends to ICC-SP's ICM an ICC-STP (S1) message, which contains the callee's (MU2's) CAI. Upon receiving the ICC-STP message, and depending on the context, the ICM executes standard AAA and C&B procedures as described in the previous phase. On successful completion of this step (if it was necessary), the ICM makes an enquiry to the DB (ICC-DB-REQ message) for the action to be performed and other relevant details. In response, the DB returns the corresponding table entry/row (ICC-DB-ANS message). Assuming that the caller falls within the 'white list', the ICM will make decision for a call establishment. To do this, two operational modes are possible as explained below.

6.2.3.1. E-Mode

In this mode, the ICM will return to the caller the callee's current CAI and supplementary information (ICC-MOV message). Then, the caller forwards a modified ICC-STP (ES5) message by putting the callee's contact address into its contact field. This message is encapsulated into an IP datagram which is sent to the ICC-SE1, where a reverse NAT is performed and the datagram/message is forwarded to the callee's terminal. If the callee wishes to answer the call, an ICC-STP-ACK (ES6) message is sent back to the caller via the ICC-SE1 and the ICC session starts.

6.2 Generic CBM-ICC Service Scenario with No Mobility

6.2.3.2. R-Mode

In this mode, the ICM will forward the (modified) ICC-STP (S4) message to MT2's CA1 via ICC-SE1 within ANP1. MT2 receives the incoming call and answers the call. Then an ICC-STP-ACK (S5-S6) message is forwarded to MU1 via ICM to acknowledge the ICC setup. With this, a real-time ICC session is established.

6.2.4. ICC Session Release

Depending on the operational mode used, this phase is accomplished differently.

6.2.4.1. E-Mode

At the end of the conversation, either communicating user can release the ICC session by sending an ICC-RLS (ER1) message to the other party. The latter replies with an ICC-RLS-ACK (ER2) message to confirm the ICC session release.

6.2.4.2. R-Mode

At the end of conversation, either party (e.g. MU1) can terminate the ICC service session by sending an ICC-RLS (RR1-RR2) message to the other party (e.g. MU2) via ICM. In response, MU2 will reply with an ICC-RLS-ACK (RR3-RR4) message to confirm the release of ICC service session.

In both modes, a final payment procedure (via the 3P-AAA-SP) completes this scenario. For example, the use of the ICC service by a caller may result in a small charge paid for each CA supplied by an ICC-SP, whereas for the callee, a flat rate (monthly) payment scheme may apply.

6.3 Generic CBM-ICC Scenario with HAC

This section mainly focuses on the additional signaling flows in a typical HAC scenario involving live ICC service session switching from an access network belonging to one ANP to an access network belonging to another ANP.

Figures 6.3 and 6.4 depict the signaling flows for a HAC switch performed from ANP1 to ANP2 in different operational modes. A mobile user (MU2) with a dual-mode terminal (MT2) wants to avail of ICC service continuity anywhere-anytime-anyhow. Further we assume that both ANPs support the ICC service by deploying a ICC-SE and all parties involved in this ICC service scenario use one common 3P-AAA-SP.

While on the move and still within the footprint of the UMTS network of ANP1, the callee's terminal MT2 continues to receive information from the billboard channel about the possible existence of other ICC service-supporting access networks available in the (new) location area. Then MT2 goes through ADA procedure to obtain a new CA2 address for its new location. After successful association with the new access network and obtaining a new contact address (CA2) from it, the live ICC session could be HAC switched for delivery over the new access network (of ANP2) in one of the two possible operational modes.

6.3.1. E-Mode

In Figure 6.3, first the MT2 informs the MT1 about new Contact Address (CA2) by sending a SCTP ASCONF (ADD_IP) chunk to the MT1, which responds with an ASCONF-ACK (ADD_IP_ACK) chunk to the MT2 for acknowledgement. While the MT2 moves further into the ANP2's domain, the MT2 sends to the MT1 a SCTP ASCONF (SET_PRI_IP) chunk to notify it about the change of its primary IP address. The MT1 acknowledges the address change by sending an ASCONF-ACK (SET_PRI_IP_ACK) chunk to the MT2. Then the HAC is finished, and the live ICC session can be switched for delivery via the new access network (of ANP2) by means of SCTP streams.

6.3 Generic CBM-ICC Scenario with HAC

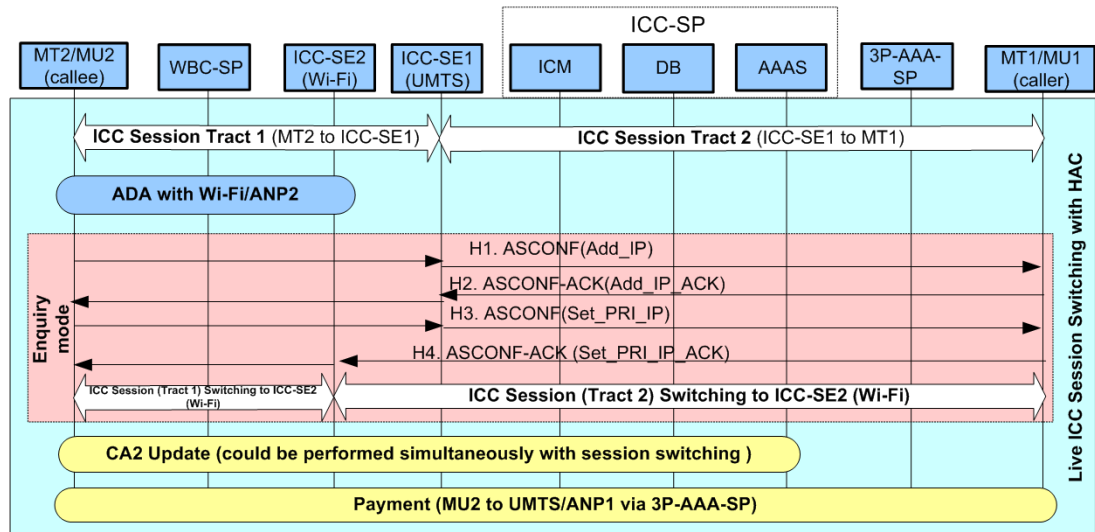


Figure 6.3.: Signaling flows for the generic CBM-ICC service scenario with HAC in E-Mode.

It is assumed that an ICC session has been already established and the HAC is performed in the middle of this session.

6.3.2. R-Mode

In Figure 6.4, the MT2 informs the ICC-SP (ICM) about its new Contact Address (CA2) by sending a SCTP ASCONF (ADD_IP) chunk. The ICM responds with an ASCONF-ACK (ADD_IP_ACK) chunk to the MT2 for acknowledgement. Then the MT2 sends to the ICM a SCTP ASCONF (SET_PRI_IP) chunk to notify it about the change of its primary IP address. The ICM acknowledges the address change by sending an ASCONF-ACK (SET_PRI_IP_ACK) chunk to the MT2. Then the HAC is finished, and the live ICC session (only tract1 and tract2) can be switched for delivery via the new access network of ANP2 by means of SCTP streams.

In both modes, with closing the streaming path through the old access network (of ANP1), a payment procedure (via the 3P-AAA-SP) is executed, i.e., the MU2 pays for ANP1's (Wi-Fi) communications services used. To the ANP1 (Wi-Fi network), this HAC will be perceived as a termination of the current ICC session followed by a payment phase.

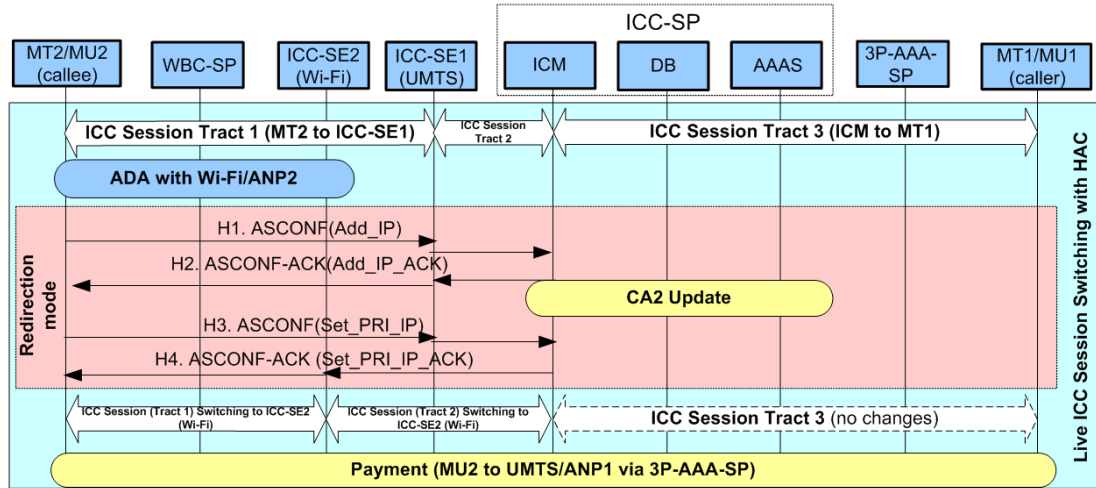


Figure 6.4.: Signaling flows for the generic CBM-ICC service scenario with HAC in R-Mode.

It is assumed that an ICC session has been already established and the HAC is performed in the middle of this session.

6.4 Conclusions

The main objective of this chapter is to develop some generic CBM-ICC scenarios for analyzing and evaluating the service performance. Although there is a possibility that a number of scenarios could exist ranging from simple to quite sophisticated one due to the diversity of different personal preferences, we have started with a generic scenario without consideration of mobility. The main signaling phases of this scenario have been briefly explained. Then a more complicated scenario is elaborated involving a live ICC session switching from one access network (provider) to another by means of a new hand-off technique, called Hot Access network Change (HAC). Being the main focus of this research, the HAC has been considered in more detail.

*It is curious that physical courage should be so common
in the world and moral courage so rare.*

—Mark Twain (1835 - 1910)

7

CBM-ICC Experimental Testbed

7.1 Introduction

In this chapter we turn our attention to the design of the proof-of-concept system-level CBM-ICC testbed. Section 7.2 provides an overview of the experimental testbed. Section 7.3 describes the testbed design and implementation, and is divided into three subsections: Subsection 7.3.1 focuses on the main ICC-SP building blocks handling the signaling and session management; Subsection 7.3.2 describes the design and implementation of the ICC-SE; Subsection 7.3.3 outlines the implementation of the ICC-client using a modified SCTP. This includes discussions on the necessary changes to the Application Programming Interfaces (APIs), and input and output packet processing. Last, some implementation issues raised in the HAC experiment are described.

7.2 Testbed Layout

A proof-of-concept system-level testbed has been set up to run experimental tests, probe different communication scenarios, evaluate the service performance, and further elaborate the service architecture (Figure 7.1). As this CBM-ICC service is quite novel and

complex, what is important is that any implementation should be scalable and standardizable. The open-source software and standard protocols are largely employed in the testbed.

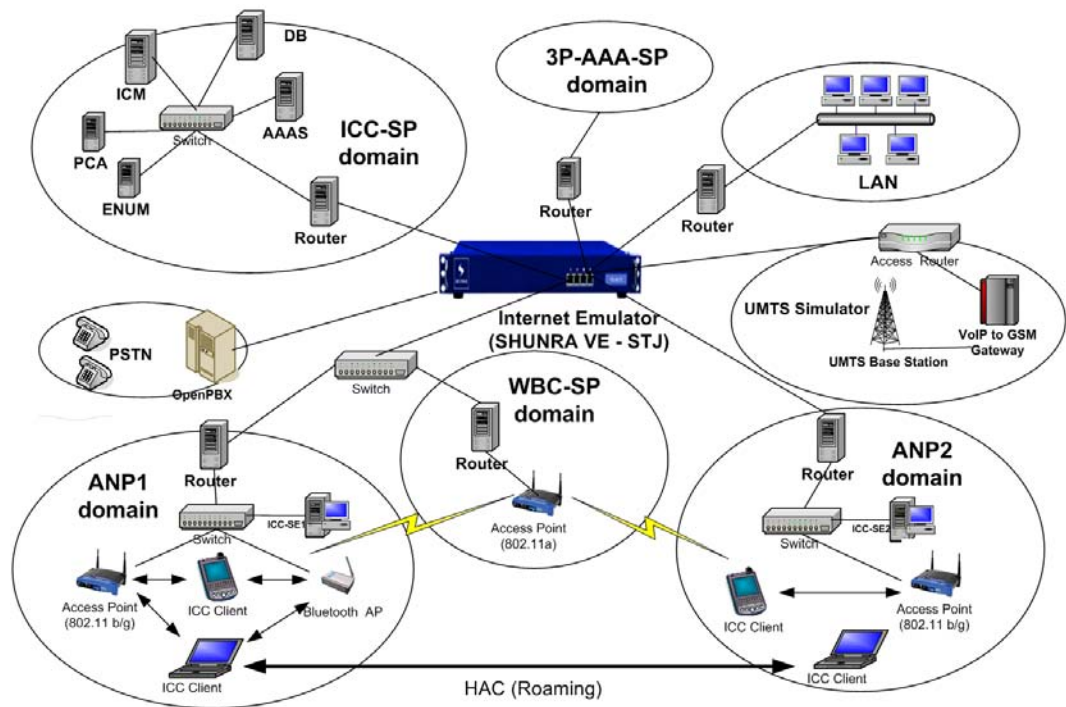


Figure 7.1.: The generic layout of the CBM-ICC experimental testbed.

The testbed contains multiple ANPs which are needed to demonstrate and experiment with terminal mobility scenarios. As IEEE 802.11 appears to be the popular and inexpensive wireless technology, we have chosen it as the main component for access networks. The different ANPs are simulated by Cisco 802.11a/b/g APs, where WAP-54G is a basic 802.11b/g access point and WAP-55AG provides all three 802.11 (a/b/g) access technologies. All APs operate in the infrastructure mode.

The Internet is emulated by a Shunra [9] WAN emulator (VE-STJ Model). This creates a virtual WAN network environment where the traffic traversing the testbed is manually exposed to a wide variety of network impairments as in the real life. The emulator also supports a flexible way to test the performance of traffic under critical networking conditions. The ANP and ICC-SP domains are connected through the Shunra WAN emulator.

7.3 Testbed Design and Implementation

The parameters used to configure the Shunra WAN emulator have a significant effect on our testbed performance. The WAN propagation delays were chosen from the Internet Tomography Measurement System (ITMS) [192], which provides laboratory simulation and emulation modeling tools with Internet parameterization data. We use the ITMS measurements, where Limerick (Ireland) is used as the central point of operations, and global Internet measurement points used are representative of regions around the globe, from USA west and USA east, Europe (U.K. - London), Middle East (Israel), Australia (Melbourne) and New Zealand (Waikato).

Mobile terminals are laptop computers with multiple wireless adapters running on Linux. The list for the testbed equipment is provided in Table 7.1.

7.3 Testbed Design and Implementation

7.3.1. ICC Service-Provider (ICC-SP) Design and Implementation

One important server implementation for ICC-SP is the ICM, which is used to handle ICC signaling and perform call redirection, filtering and blocking. The key C and C++ implementation is focused on the ICM functionality (Figure 7.2).

As a SIP extension is identified as the most suitable candidate signaling protocol for the CBM-ICC service, the implementation of the ICM core could reside on the Asterisk PBX [193]. Asterisk is an open-source implementation of VoIP base protocol (e.g. SIP and H.323) under GNU Public License (GPL) with various functionalities provided through different configurations. The Asterisk version 1.2.7.1 was used. The main challenge was to adjust SIP and Asterisk as to support the CBM-ICC service with inherent components. The other modified modules for ICC application are sitting on top of Asterisk to implement ICM. The OpenSER⁴¹ is also running on ICM with SCTP support. Features for

⁴¹ OpenSER supports the implementation of the SCTP transport layer, including multi-homing, statistics for SCTP, connection associations and auto-close, runtime re-configuration, management of attributes for retransmission at the transport layer [194].

7.3 Testbed Design and Implementation

Table 7.1.: The testbed equipment list.

Components	Equipment	Equipment Description
ICM USER_DB ENUM ICC_SE	Desktop Computer (Dell Optiplex) with 3Com NIC (3C905CX-TX- MOEM)	350MHz Intel Pentium III 256MB SDRAM Slackware Linux 11.0 Ubuntu Linux 8.10
Router	Desktop Computer (Dell Optiplex) with 3Com NIC (3C905CX-TX- MOEM)	350MHz Intel Pentium III 256MB SDRAM Installed with GNU Zebra. Zebra is open source software running on Linux and managing IP-based routing protocols. It is under the GNU General Public License. The current version of Zebra supports BGP-4 protocol as described in RFC1771 as well as RIPv1, RIPv2 and OSPFv2. IPv6 (RFC2460, RFC2373 and RFC2464) is also supported in the version 0.94.
Switch	Ethernet Switch (Linksys SR224)	Standard 24 Ports 10/100 switch.
WAN Emulator	Shunra Virtual Enterprise network appliance	SHUNRA Virtual Enterprise is a high-performance WAN emulator. It alters the speed at which traffic traverses the LAN testbed to expose packets to the same impairments to which they would be subjected on a wide area network (WAN).
ICC Client	Dell C800 Laptop with PCMCIA 802.11b (AIR-PCM352)	P4 1.6G RAM 1G PRISM2 wireless card
ANP1	802.11b/g access point (WAP-54G)	Just a basic 802.11b/g access point manufactured by Cisco-linksys. There is open source project that undertaken the development of Linux firmware for this device.
ANP2	802.11a/b/g access point (WAP-55AG)	Provides all three 802.11 (a/b/g) access technologies. This device maybe particularly useful for extending the testbed.

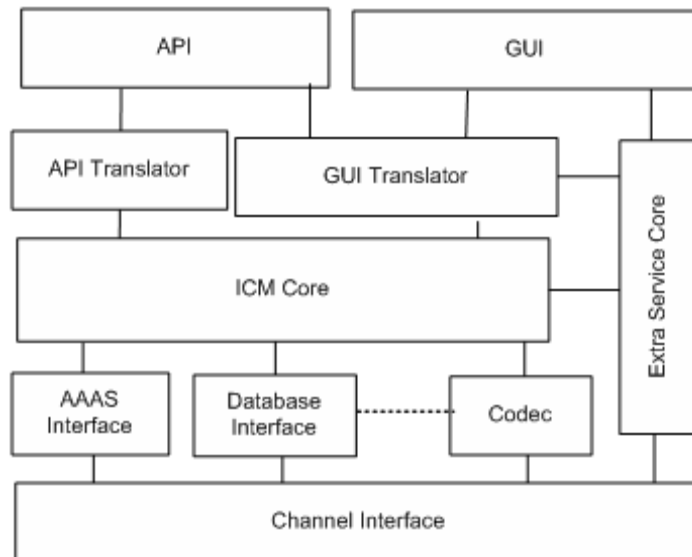


Figure 7.2.: The block diagram of ICM.

SCTP support are loadable by recompiling the source code to enable functionalities. The OpenSER can be configured in both redirection and enquiry modes. All sources were locally compiled on the test machine. Both of them were compiled with default options.

Call redirection, filtering and blocking can be implemented by a lightweight and extensible Call Processing Language (CPL) [183]. The user is capable to control the incoming call through a web application to translate user requirements into a CPL script and upload it to ICM under the security guarantee of 3P-AAA-SP. The GUI parser translates the user preferences (i.e. statements on how the user prefers to receive the incoming calls) into an ICC call control script. This CPL script can be created on the MT and uploaded to ICM under the security guarantee of 3P-AAA-SP.

The Extra Service Core is mainly implemented by XML-based language, VoiceXML [185]. Using VoiceXML, extra service can be supplied by creating voice dialogs through the voice-recognition technology [195]. The user is able to define the profile and preferences through the user's natural speaking voice, while the caller can interact with ICC-SP by listening to the latest email and news by computer-synthesized voice.

A value-added PCA service is also implemented to allow voice dialogs using voice-recognition technology. An XML-based language, VoiceXML, is adopted to allow the user to define his/her ICC profile and preferences verbally, and check his/her voicemail.

For simplicity, MU-DB is also integrated into the ICM server. The user preferences are stored through the database interface by means of an ICC call control script. We choose the open-source MYSQL as the MU-DB. A web-based graphical user interface (GUI), implemented by PHP [196] and J2EE [197], is supported in order to enable the MU/callee to specify his/her ICC preferences for the control of the incoming calls.

7.3.2. ICC Service-Supporting Entity (ICC-SE) Design and Implementation

ICC-SE acts as a NAT point between the ANP and the outside world to translate the personal address of the mobile host to the Contact Address (assigned) and vice versa. All incoming packets to the mobile host are destined first to the ICC-SE, which forwards these packets to the mobile host. Similarly in the opposite direction, all outgoing packets from the mobile host are intercepted by the ICC-SE, which performs the reverse address translation and forwards the packets to the other communicating host.

The implementation of ICC-SE is mainly based on open-source software. The ICC-SE in the ANP domain is configured with NAT and OpenSER. DHCP server is also included in ICC-SE. Internal Linux kernel modules, IP_TABLES and IP_QUENE, are used to implement the NAT function by configuring the corresponding actions according to the packet format. The IP_TABLES define the filtering rules according to the protocol type, IP address, port, MAC address, etc. The IP_QUENE is used to intercept IP packets and transmit them according to the filtering rules of IP_TABLES. However, there were some issues related to IP_TABLES to overcome: (1) As the signaling could not the IP_TABLES, we used OpenSER to translate signaling messages; (2) As the existing IP_TABLES are not designed to support HAC (for example the port number is changed during the HAC operation when the primary address is changed), the connection is very likely to suffer from

breaking. To solve this, a multi-homing function in OpenSER combined with network address port translation was used to translate the new assigned port to the original port.

7.3.3. ICC-client Design and Implementation

This section briefly discusses the ICC-client implementation for testing purposes, and looks into some design issues encountered.

7.3.3.1. Software Design

Figure 7.3 shows the diagram of the ICC-client stack. Popular API implementations for SCTP in Linux are the SCTP library (SCTPLIB) [198] and SCTP Kernel (LKSCCTP) [199], both of which provide initial functions at the Application Programming Interface (API) layer according to the RFC 4960 [66]. SCTPLIB uses an ASCONF API named `setRemotePrimary` to allow users to specify the primary address to use. However, we discovered that when the ASCONF chunk with the Set Primary Address parameter is sent over primary path, the primary paths used by peers of an SCTP association are not changed. This may cause data loss during the handoff. To solve this problem, we choose a kernel-level implementation of LKSCCTP as a development foundation.

For the HAC implementation, a user-level application was developed based on a lower level SCTP socket API specified in [200], which provides Linux kernel-level socket. This makes development of SCTP applications similar to writing applications for TCP or UDP. LKSCCTP SCTP control messages such as INIT, INIT_ACK, HEARTBEAT, COOKIE_WAIT, etc are supported. As listed in Table 7.2 12, SCTP sessions are instantiated using the `socket()` function. The addition/removal of the IP address is performed by the `sctp_bindx()` function. The HAC is realized by the `setsockopt()` function with different parameters. In order to properly invoke the function and ensure SCTP peers change the primary address, a set of flags have been defined to specify various default behaviors. For example, the peer should change the primary address by using the `SCTP_PRIMARY_ADDR` flag and set primary address parameter with the `SCTP_SET_PEER_PRIMARY_ADDR` flag.

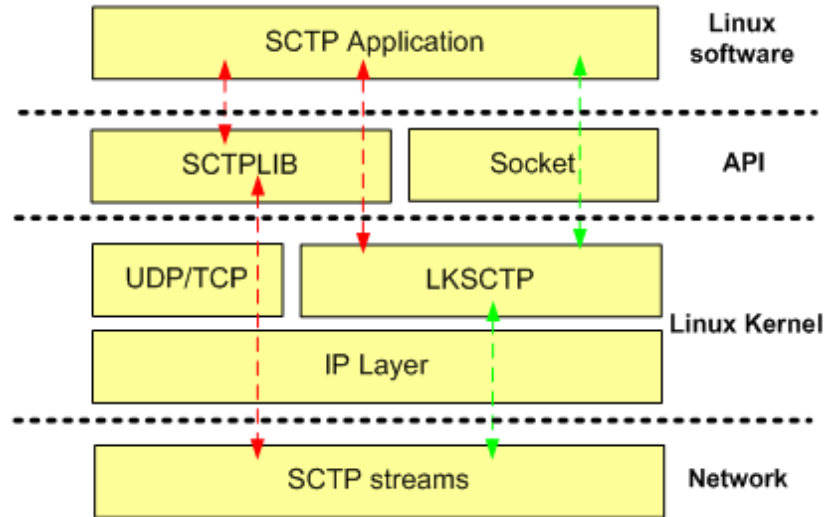


Figure 7.3.: The stack diagram of the ICC-client. The API implementations for SCTP in Linux are based on the SCTP library (SCTPLIB) and SCTP Kernel (LKSCTP). A kernel-level LKSCTP is chosen as a development foundation for the HAC implementation.

Table 7.2.: The SCTP API exported by the ICC-client.

Method	Description
<code>int socket(AF_INET, SOCK_STREAM, IPPROTO_SCTP)</code>	Creates a socket for a SCTP association.
<code>int sctp_bindx(sd, addrs, addrcnt, ADD)</code>	Adds a new IP address to a SCTP association.
<code>int sctp_bindx(sd, addrs, addrcnt, REMOVE)</code>	Deletes an old IP address from a SCTP association.
<code>setsockopt(sd, IPPROTO_SCTP, PRIMARY_PEER_ADDR, *setpeerprim, len)</code>	Changes the primary IP address when the user or application triggers the HAC.
<code>setsockopt(sd, IPPROTO_SCTP, SCTP_SET_PEER_PRIMARY_ADDR, *setpeerprim, len)</code>	Changes the peer's primary IP address when the user or application triggers the HAC.

7.3 Testbed Design and Implementation

To facilitate our implementation, we have developed our own SCTP classes in C++ specifying all the functions needed by the ICC-client (for more details see Appendix E). The ICC-client can be divided into a sender and a receiver part. The sender is the main component, which is able to initiate the ICC session and trigger the HAC. To communicate with the receiver, the sender should execute the socket API functions shown in Figure 7.4(a). The receiver should execute the socket API functions depicted in Figure 7.4(b).

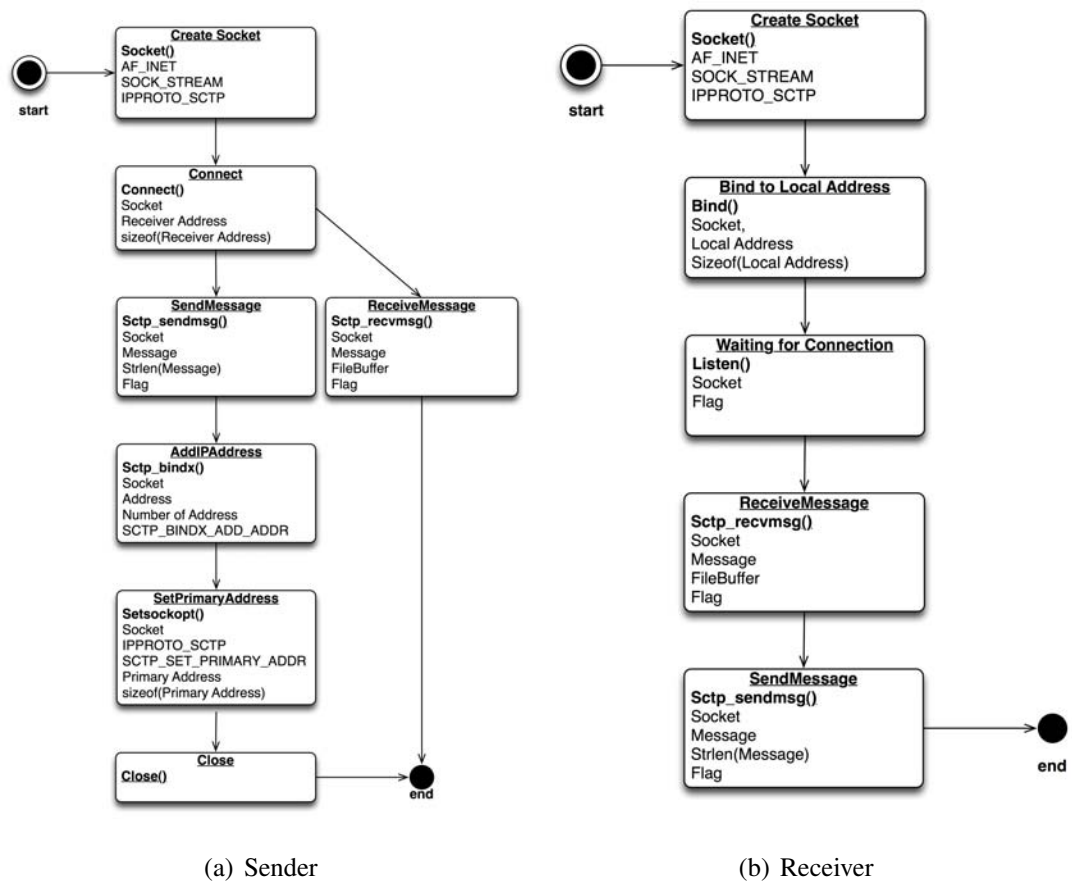


Figure 7.4.: The API function procedure at the sender and the receiver.

7.3.3.2. Modifications on SCTP

The SCTP protocol was chosen to provide the transport-layer services because it is capable of allowing dynamic reconfiguration of IP addresses of an existing association between two SCTP end-points. However, since SCTP uses a similar congestion control

7.3 Testbed Design and Implementation

mechanism as TCP, it will also encounter same problems as TCP. Many studies have disclosed that adopting a SCTP-like reliable protocol without proper modification to transport real-time multimedia data results in significant performance degradations [201]. This is mainly due to: (1) the loss recovery in SCTP, which introduces extra delays, i.e., when the handoff is performed, the missing chunks will trigger a retransmission; (2) the congestion window (CWND) used to control the transmission rate in slow start and congestion avoid procedure. However, generally real-time streaming is based on constant bit rate, and thus the sudden degradation in transmission rate causes significant performance degradation. To solve these problems, a modification on SCTP is needed for the real-time multimedia traffic.

The PR-SCTP protocol supports partially reliable data transmission at required level. There are two ways to implement the PR-SCTP, namely the timer-based reliability and retransmission-based reliability. The timer-based reliability in PR-SCTP uses a “lifetime” to stop the transmission before triggering the retransmission. If the “lifetime” of a packet expires within the Retransmission TimeOut (RTO) of the initial transmission, the retransmission will not be triggered. However, it is difficult to find a proper “lifetime” for timer-based reliability, i.e., large “lifetime” would increase delay, whilst smaller “lifetime” would end up with discarding packets as fast as they get to the receiver. For this reason, we chose to use the retransmission-based reliability, which defines how many retransmissions should be preformed. In this way, after a pre-defined transmission timeout, the packet will be released from sender’s transport buffers without receiving an ACK. Thus this approach can disable the retransmission and fulfill the requirements of diverse multimedia applications. To do this, we need to set the retransmission number with SCTP_PR_RTX option to zero. Such a modification is only applied on the sender because the sender can decide independently when to discard a data packet while the receiver does not need to know.

Another modification is related to changing the congestion control parameters. In the standard PR-SCTP, there are two kinds of event indicating a packet loss: (1) receiving four duplicated SACKs and (2) retransmission timeout. If a packet loss is detected, the Slow-Start Threshold (SSTHRESH) value is reduced to half of the current CWND value and then the CWND is set to this value. However, HAC over multiple connections with

different bandwidth and delay may lead to unneeded CWND reductions. This further increases the delay of the subsequent packets sent after the HAC, which does not satisfy the timing requirements for real-time multimedia communications. To provide a solution to this problem, we propose an adjustment on congestion control parameters. We change the minimum Ssthresh value to be corresponded to the original CWND. In this way, the CWND value cannot be reduced only during the HAC. The pseudo-code of the proposed SCTP modification is shown in Algorithm 1.

```
1 Initially :
2 transport→cwnd = 2*transport→asoc→pathmtu;
3 transport→ssthresh = large number;
4 Newackreceived :
5 If (transport→cwnd <= transport→ssthresh)
6 transport→cwnd = transport→cwnd + acked chunk size from receiver;
7 Retransmissions :
8 If (receivedAduplicateSACK)
9 transport→ssthresh = max(transport→cwnd, 2*transport→asoc→pathmtu);
10 transport→cwnd = transport→ssthresh;
11 If (timeout)
12 transport→ssthresh = max(transport→cwnd, 2*transport→asoc→pathmtu);
13 transport→cwnd = transport→ssthresh;
```

Algorithm 1: The pseudo-code for the modified SCTP Congestion Control Algorithm

7.4 Conclusions

In this chapter, the design of experimental testbed has been explained in detail together with its implementation. The overview of the experimental testbed has been given in Section 7.2. Section 7.3 has shown that the testbed implementation contains three main

parts. First, we have described the implementation of the ICC-SP's ICM building blocks using the open-source PBX. Second, we have described the implementation of the ICC-SE using NAT. Third, we have described the internal implementation of the ICC-client including a discussion on two proposed modifications to the standard SCTP protocol, as to make it more suitable for the new CBM-ICC service.

*A little knowledge that acts is worth infinitely more than
much knowledge that is idle.*

—Kahlil Gibran (1883-1921)

8

CBM-ICC Service Performance Evaluation and Results

8.1 Introduction

This chapter⁴² presents a systematic evaluation of the CBM-ICC service performance through extensive analytical simulation studies based on the system-level experimental testbed presented in Chapter 7.

Section 8.2 presents the QoS metrics used for the evaluation. Section 8.3 describes the configuration of the CBM-ICC testbed. Section 8.4 evaluates the signaling performance in terms of the delay contributed by different signaling phases. In Section 8.4.1, a simple scenario with no mobility is employed for analyzing the signaling delay. The performance for the two ICC-SP operational modes, i.e. Enquiry Mode (E-Mode) and Redirection Mode (R-Mode), in diversified ANP environments is studied to determine how the service performance differs with different operational modes. Section 8.4.1 employs a more complicated mobility scenario to study the service performance during HAC. We carry out theoretical and experimental measurements to discover the HAC switching delay in two

⁴² This chapter is based in part on author's publication in Wireless Personal Communications [33].

scenarios, namely UMTS-to-Wi-Fi and Wi-Fi-to-UMTS scenario. The two operational modes are compared in terms of the HAC switching delay.

Besides signaling performance, our experiments evaluate the HAC implementation in a laboratory testbed environment as presented in Chapter 7. The HAC switching performance is characterized by several key QoS parameters such as throughput, end-to-end delay, and jitter. Our first evaluation is to investigate the impact of HAC on the performance of data services in UMTS-to-Wi-Fi and Wi-Fi-to-UMTS scenarios. To be able to ensure the integrity during the transmission, we select the reliable SCTP as the transport-layer protocol for the data service. Furthermore, we also measure the QoS parameters of a real-time traffic (such as voice and video), which is delay-sensitive and thus must be processed as a steady and continuous stream. In this measurement we use the modified PR-SCTP as the transport-layer protocol in an effort to reduce the overhead delay attributed to congestion control and retransmission. We also assess the simulation results for both operational modes when the proposed PR-SCTP is applied.

8.2 QoS Metrics

QoS metrics in IP networks are utilized to analyze the overall performance as well as reliability of the networking components. In this thesis we are explicitly interested in the network load and network performance parameters, such as latency, jitter, throughput, and packet loss rate, which are briefly described below as per [192, 202, 203, 204].

Throughput is the amount of data transmitted successfully from one node to another in a given time period. The throughput is usually measured in bits per second (bit/s or bps), or in bytes per second. In technical and commercial terminology, it is also known as the bandwidth which represents the capacity of a networking connection. Throughput can be modeled either by a constant bit rate (CBR) or by a variable bit rate (VBR).

Packet loss is the percentage of packets that failed to reach the destination in a specific time interval. Packet loss probability is mostly determined by two features, i.e., packet errors as a result of bad link quality (particularly on wireless connections) and packet drops resulting from congestion. Various applications may have distinctive tolerance of

packet loss. For example, the voice is quite predictive and if the packet loss is isolated the voice can be heard in a quite optimal way. The problem is greater when packet loss occurs in burst. It can be calculated as follows.

$$\text{Packet Loss Rate} = \frac{\text{Packets Sent} - \text{Packet Received}}{\text{Packets Sent}} \quad (8.1)$$

Latency or Delay is usually known as end-to-end delay, which is technically defined as how much time is used by a packet traveling from the source to the destination. In a real IP networking environment, end-to-end delay is certainly not constant but differs with time, due to the fluctuation of the Internet traffic. The delay is usually affected by many aspects, such as, distinct communications layers, various entities and routers, as well as multiple sub-networks. The overall performance of the end-to-end delay could be indicated with regard to minimum and maximum delay bound parameters.

In general, the delay parameter is usually divided into four primary components:

- **Propagation delay (D_{ew})** is the time needed to propagate a bit through a communication link. In this way, the D_{ew} is determined by the travel time of the electromagnetic wave over the physical channel of the communication path. Thus the D_{ew} usually is independent of the specific traffic on the link and can be calculated as follows.

$$\text{Propagation Delay} = \frac{\text{Physical Distance}}{\text{Propagation Velocity}} \quad (8.2)$$

- **Transmission delay (D_t)** is the time needed to transmit an entire packet at a specific bit rate over a communication link. The transmission delay is determined mainly by the link speed. It is usually calculated as per the following equation.

$$\text{Transmission Delay} = \frac{\text{Number of Bits to Transmit}}{\text{Transmission Rate}} \quad (8.3)$$

- **Queuing delay (D_q)** is the time need by an IP packet to wait in a queue in network elements. The D_q varies from router to router and is subject to congestions situation and traffic patterns, volumes, packet length characteristics, etc. Normally

queuing delay together with propagation delay are deemed as essential contributors to the end-to-end delay provided that no serious processing like heavy encryption is performed.

- **Processing delay (D_p)** is the time required to process a IP packet by network components like routers or the end devices, which can be viewed as unaffected by the traffic. D_p mostly depends upon the processing speed on the networking hardware, which may rely on the computational power of the processor and the capacity of the memory. Furthermore, it is also determined by the complexity of the networking protocol, including complicated payload adjustments and encryption.

Jitter is known as the delay variation experienced by subsequent packets on a one-way transit from source to destination. Jitter is used to measure variability of the latency across a network according to the same definition for the delay variation as the ITU-T for the Instantaneous Packet Delay Variation (IPDV). The jitter in this thesis is calculated as the difference between the end-to-end delays of the present i th and the previous $(i - 1)$ th data units transmitted between the same source and destination. The formula is as follows.

$$J_i = |D_i - D_{i-1}| \quad (8.4)$$

8.3 Testbed Configuration

A multi-access experimental environment is configured as shown in Figure 8.1 in order to conduct the signaling and handoff measurements for the CBM-ICC service.

Different ANPs are simulated using multiple Cisco access points (APs), where WAP-54G is a basic 802.11b/g access point and WAP-55AG provides all three 802.11 (a/b/g) access technologies. Two PCs residing on the edge of an ANP are configured as ICC-SEs, which act as a gateway and network emulator for the MTs they are currently serving. Each ICC-SE usually is connected to at least one AP.

The ICC-SP infrastructure is simulated by a collection of PCs, which are loaded with Ubuntu 8.10 Linux with a kernel version of 2.6.27-14. ICM and DB are configured on

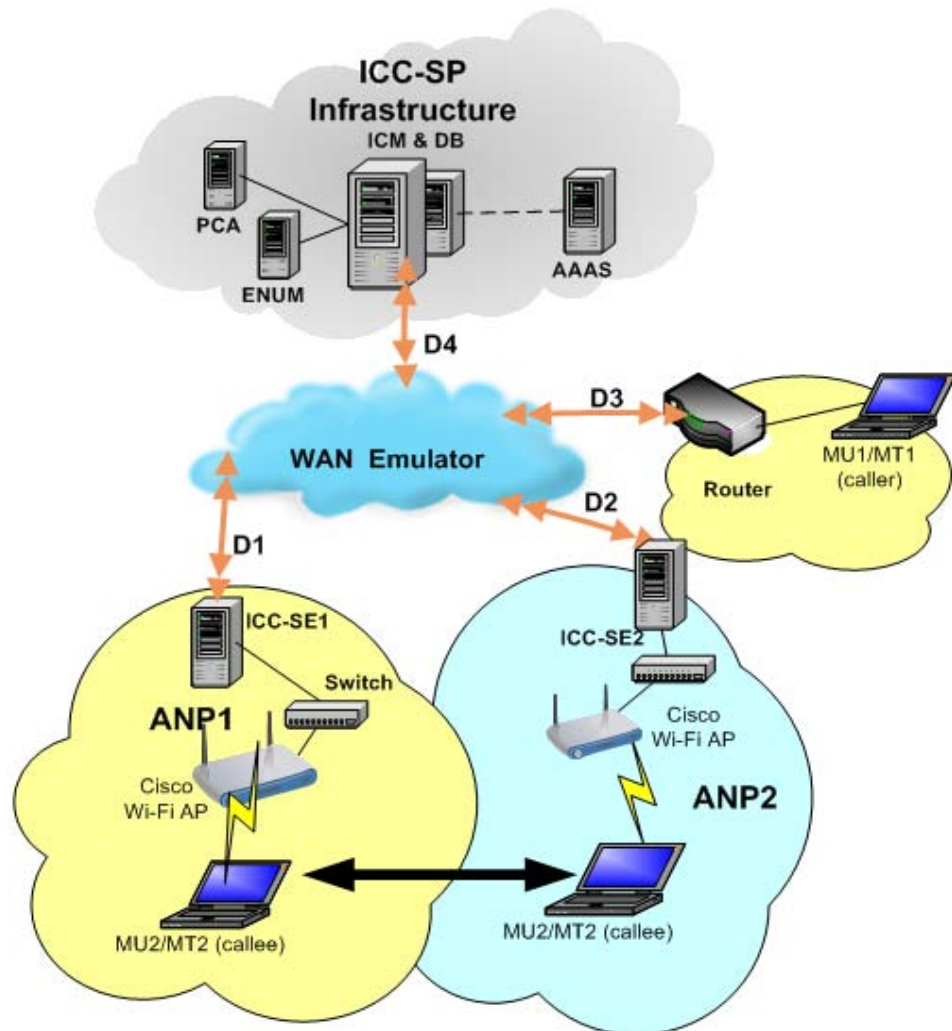


Figure 8.1.: The CBM-ICC testbed configuration. Different ANPs are simulated using multiple access points (APs). The ICC-SP infrastructure is established as a group of PCs. A PC residing on the edge of an ANP is configured as an ICC-SE. MTs are laptop computers running the Linux operating systems (Ubuntu 8.10) with installed testbed software. A WAN emulator is used to emulate the expected network delay, packet loss and bandwidth.

the same PC with the installation of Asterisk, OpenSER, and SQL server. The Ethernet interface of the ICM is connected to a 100 Mbps switch that connects to the WAN emulator.

MTs are laptop computers running the Linux operating systems (Ubuntu 8.10) with installed testbed software. MT1 (caller) directly connects to the WAN emulator via a router. MT2 (callee) is equipped with multiple Cisco 802.11a/b/g wireless adapters so as to establish multiple independent communication paths to APs. The Cisco 802.11a/b/g wireless adapters support the Atheros AR5212 chipset, with the MadWi-Fi Drivers [205] installed. One Wi-Fi interface of MT2 is associated with one Wi-Fi access point (ANP1), which is in turn connected to the ICC-SE1. Another Wi-Fi interface is associated with a simulated Wi-Fi access point (ANP2 or ANP3), which connects to the Internet via ICC-SE1 or ICC-SE2.

The WAN emulator has the ability of emulating the expected network delay, packet loss and bandwidth by defining rules for pairs of source and destination addresses. A Linux emulator that runs the NISTNet software and a commercial Shunra emulator are used in this testbed. The general WAN configuration is shown in Table 8.2. Link delays are configured so that the packets are delayed by the given latency chosen from the ITMS [192]. In our experiments, we assume that all related 3P-AAA signaling messages are handled locally within a fixed processing time.

The emulator's configuration on access networks varies in terms of different ANP models. Wi-Fi access points joint with ICC-SE and WAN emulator are configured to emulate varying ANPs. The maximum transfer bit rates and propagation delay reflect values that may be reached by current wireless technologies such as UMTS, and thus are set in the WAN emulator and ICC-SE to model different wireless access scenarios. Table 8.1 shows the simulated access networks' configuration parameters, while Table 8.2 contains configuration parameters representing different ANPs. For example, as shown in Table 8.2, in the case of Wi-Fi, we use default data transfer rate of 54Mbps with delay time of 50ms. As for UMTS/GPRS, a base station would be referred to as AP. A 3G/UMTS data transfer rate of 384Kbps with delay time of 70ms is configured. These settings for different ANPs are chosen based on previous studies, e.g. [206, 207, 192]. The same philosophy has been adopted by many research such as [208, 209]. Signaling packets and traffic are directly captured from the network interface with a Wireshark Protocol Analyzer [210].

8.4 Signaling Overhead Evaluation

Table 8.1.: The access networks' configuration parameters.

	Data Rate	Delay
Wi-Fi	54 Mbps	50 ms
UMTS	384 kbps	70 ms

Table 8.2.: The WAN configuration parameters.

Link Delay	Delay (Normal Distribution)		Packet Loss	Bit Error	Congestion
	Average	Standard Deviation			
D1	50 ms/70 ms	10 ms	0%-5%	No	No
D2	50 ms/70 ms				
D3	50 ms				
D4	20 ms				

8.4 Signaling Overhead Evaluation

The message flows presented in Sections 6.2 and 6.3 have been implemented in a simulation environment. The performance evaluation of the main generic scenarios is carried out in this section in order to observe the overhead of the proposed operational modes under different scenarios.

8.4.1. Generic Scenario with No Mobility

The performance parameters used here are delay incurred in each signaling phase, which is an expression of how much time it takes for completing the signaling in each stage, i.e. ADA, Contact Address Update, ICC Session Setup, and ICC Session Release.

Figures 8.2–8.5 present the delay overhead comparison results on each signaling phase for the two CBM-ICC operational modes. Not surprisingly, the delay increases as the packet loss rate increases. It can be observed from Figures 8.2 and 8.3 that the latency contributed by ADA and CA update procedures is identical for both R-Mode and E-Mode. However, different operational modes lead to different delay performance in the other

8.4 Signaling Overhead Evaluation

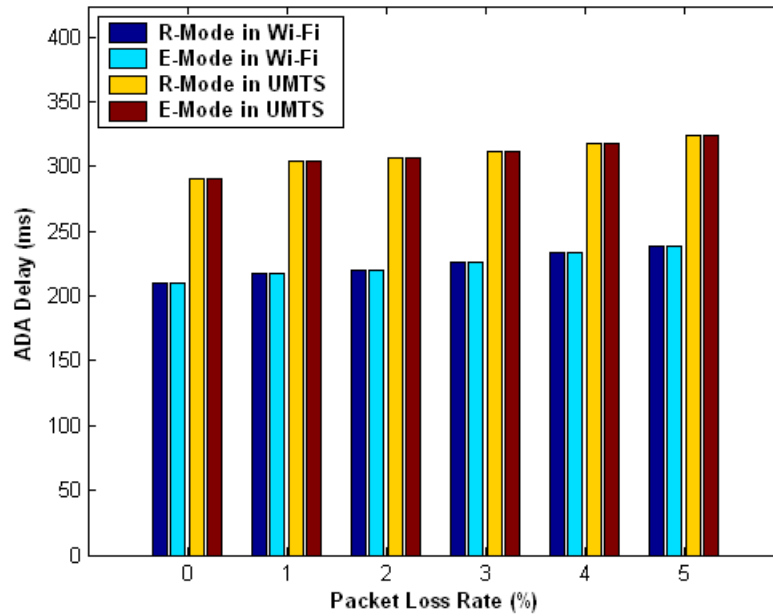


Figure 8.2.: The ADA delay for R-Mode and E-Mode.

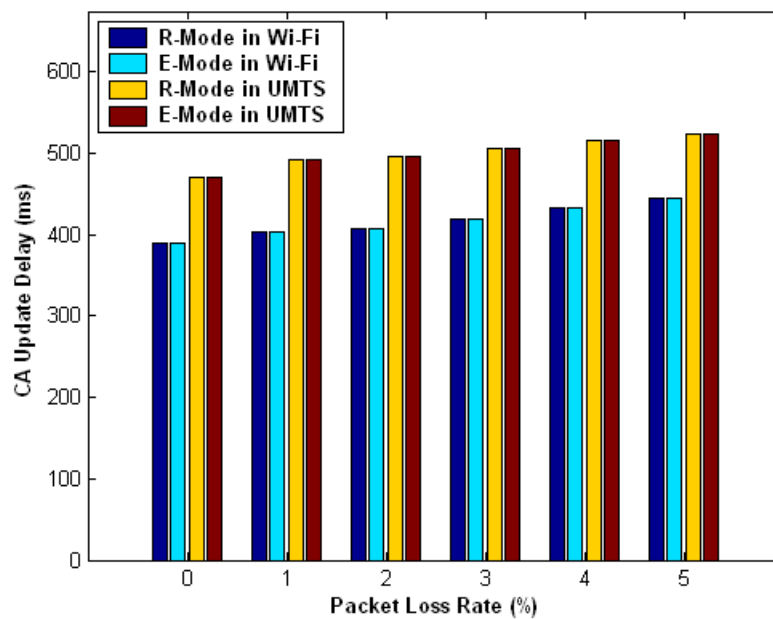


Figure 8.3.: The CA update delay for R-Mode and E-Mode.

8.4 Signaling Overhead Evaluation

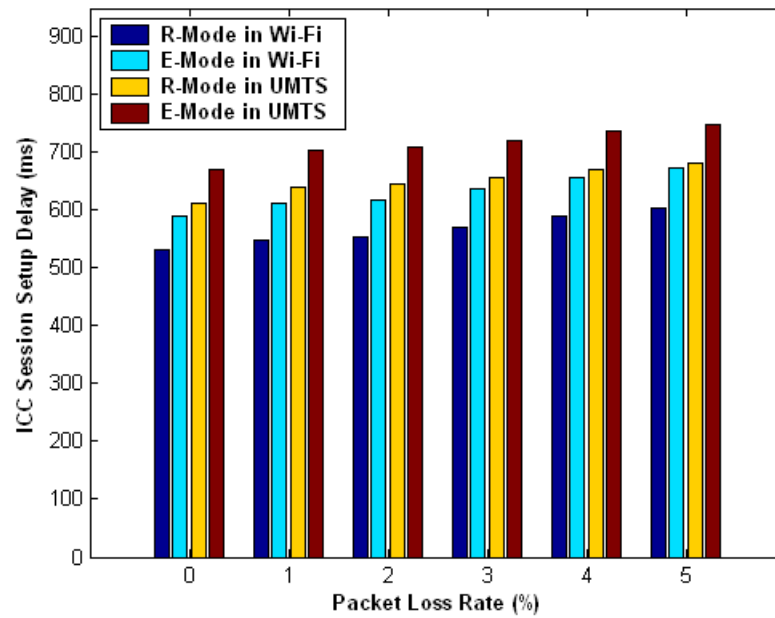


Figure 8.4.: The ICC session setup delay for R-Mode and E-Mode.

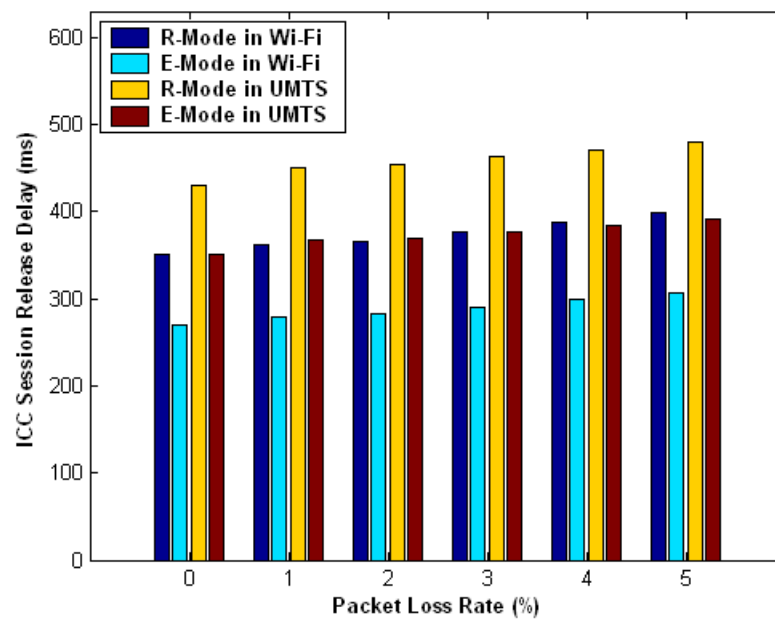


Figure 8.5.: The ICC Session Release Delay for R-Mode and E-Mode.

signaling phases. In Figure 8.4, the R-Mode outperforms the E-Mode in terms of the call setup delay. This is because the E-Mode involves signaling from the ICC-SP back to the caller and more complicated end-to-end signaling between the caller and the callee. This imposes a larger delay. On contrary, in the “ICC session release” phase as shown in Figure 8.5, the E-Mode outperforms the R-Mode. The reason is that all signaling is handled end-to-end in the E-Mode, which avoids the delay incurred by sending a signaling message to the ICC-SP. Furthermore, it also can be observed that in all scenarios Wi-Fi gives better performance than UMTS. This is because the signaling messages in Wi-Fi experience a relatively smaller latency than in UMTS.

The average delay performance and average ICM's CPU load in different phases were tested. To avoid repeated work, we only test the Wi-Fi settings with packet loss of 0.5%. Figure 8.6 compares the two modes in terms of latency in each phase based on 1000 measurements. The results further prove that: (1) the R-Mode outperforms the E-Mode in the “ICC session setup” phase by 10%; (2) in the “ICC session release” phase, the E-Mode outperforms the R-Mode by 18%. On the other hand, Figure 8.7 compares the ICC-SP/ICM's CPU utilization with respect to the call arrival rate. It is noted that the CPU usage increases rapidly as the number of simultaneous calls increases. It can be also observed that on average the CPU load for the R-Mode is higher than that in the E-Mode by 45%, and the CPU utilization reaches 100% when the number of calls reaches 10000 calls/s for the R-Mode. This is due to the fact that all signaling is performed through the ICM in the R-Mode and the memory copy operations in the ICM impose additional system load.

8.4.2. Generic Scenario with HAC

In this section, we analyze the HAC signaling performance in two typical scenarios, i.e., UMTS-to-Wi-Fi and Wi-Fi-to-UMTS.

Figure 8.8 illustrates the HAC switching delay for different packet loss rates in UMTS-to-Wi-Fi and Wi-Fi-to-UMTS HAC scenarios. It is shown that the Wi-Fi-to-UMTS scenario features higher HAC switching delay for both the R-Mode and the E-Mode, especially when the packet loss rate is high. This can be explain in Figure 8.9 that association (ADA)

8.4 Signaling Overhead Evaluation

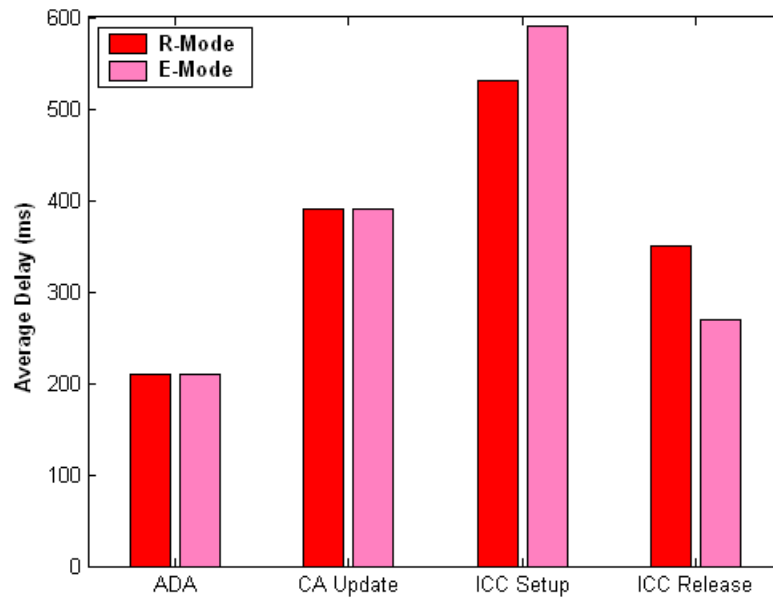


Figure 8.6.: The signaling performance for R-Mode and E-Mode.

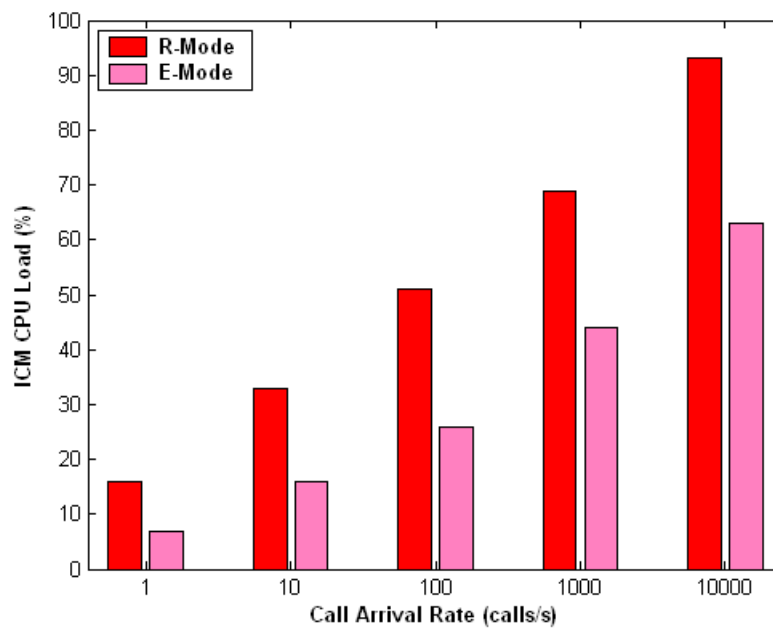


Figure 8.7.: An ICC-SP/ICM's CPU load comparison of two operational modes.

procedure in a UMTS introduces larger delay. Furthermore, the results also demonstrate that for the same scenario the R-Mode outperforms the E-Mode in terms of the HAC switching delay. This is due to the fact that the signaling messages in R-Mode only need to be transmitted to the ICC-SP rather than to the callee. In this way, the propagation delay imposed by signaling exchanges with the callee can be avoided and thus the HAC switching delay is reduced in the R-Mode.

To understand the reasons for the above statement, we break down each measured HAC switching delay into its components. Figure 8.9 presents the main components of the mean HAC switching delay when employing the R-Mode and E-Mode. The standard HAC consists of ADA, ICC session switch, and CA update procedure. The results in Figure 8.9 show that for each scenario the ADA and CA Update delay in the R-Mode are the same as in the E-Mode. The main difference exists in the ICC session switching delay. As illustrated in Figure 8.9, the R-Mode experiences much less mean session switching delay compared with the E-Mode. On average the ICC session switching delay can be reduced by about 10% if the R-Mode is employed in both UMTS-to-Wi-Fi and Wi-Fi-to-UMTS scenarios. However, it is evident that the CA update procedure contributes a large proportion of delay. Thus the CA update should be performed after the HAC switch is triggered to minimize the impact on the overall HAC switching performance.

It is interesting to see that the Wi-Fi-to-UMTS scenario results in smaller delay for the ICC session switching procedure than the UMTS-to-Wi-Fi scenario for both modes. This is mainly because most signaling messages in the Wi-Fi-to-UMTS scenario are exchanged over Wi-Fi, which provides higher bandwidth and lower propagation delay. In addition, not surprisingly, the R-Mode in Wi-Fi-to-UMTS scenario gives the smallest delay overhead for the ICC session switching procedure. However, this does not result in dramatic performance improvement on the overall HAC switching delay. This is because the association (ADA) procedure in UMTS is complicated and contributes larger delay.

8.4 Signaling Overhead Evaluation

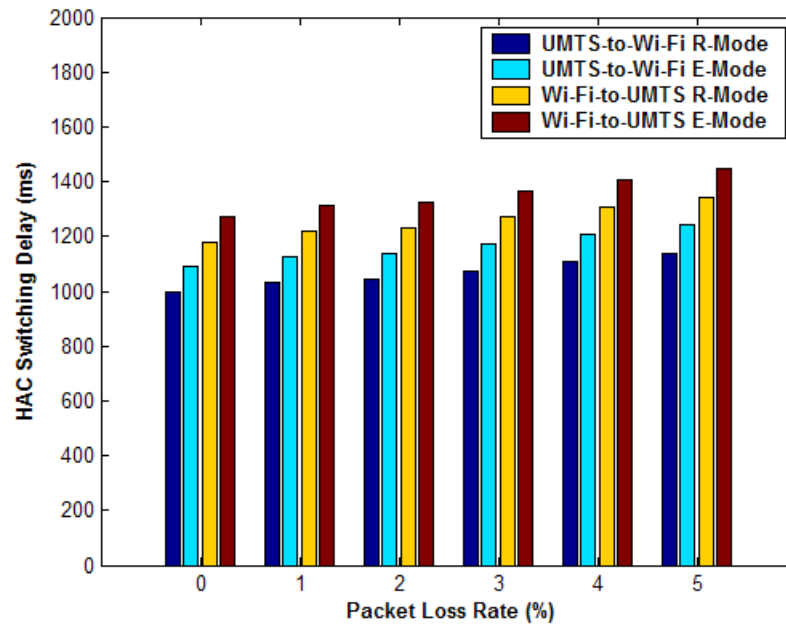


Figure 8.8.: The HAC signaling performance for R-Mode and E-Mode.

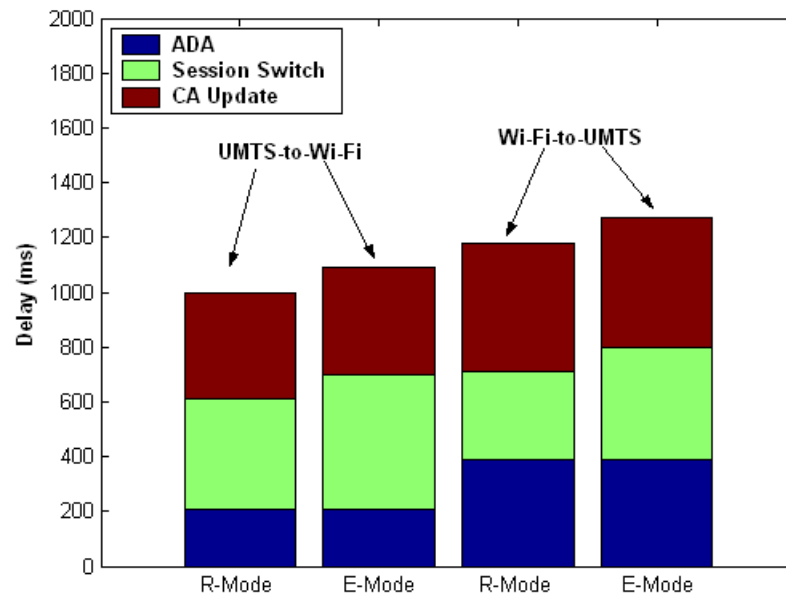


Figure 8.9.: The main components of the HAC switching delay with comparison of R-Mode and E-Mode.

8.5 HAC Performance Evaluation

Based on the generic scenario defined in Section 6.3 and referring to the experimental testbed configuration in Section 8.3, the obtained experimental results are presented in this section to evaluate the HAC performance when switching the delivery of an active ICC session from UMTS to Wi-Fi and vice versa.

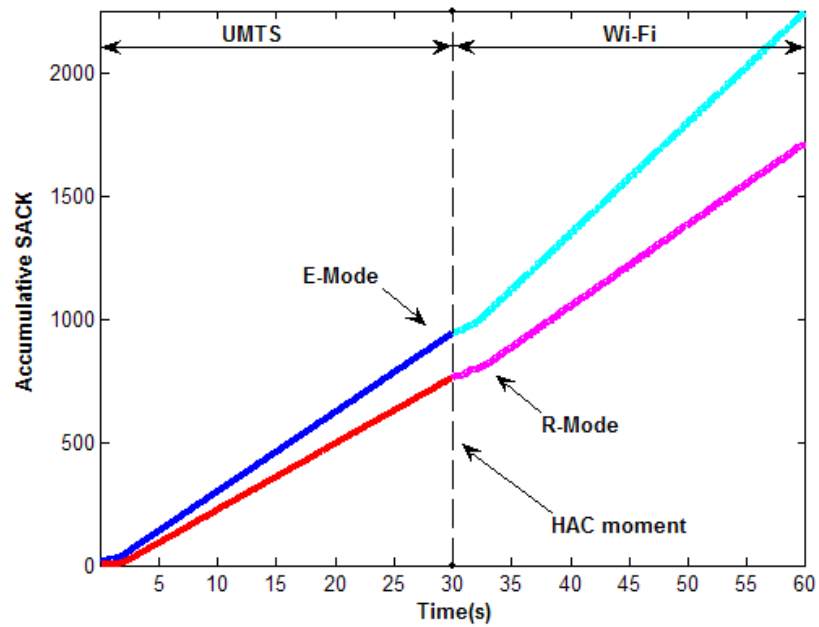
It is assumed that as the experiment starts the callee (MU2/MT2) moves towards a new ANP while HAC is triggered to maintain the ICC live session from the caller (MU1/MT1), and the primary-change is manually triggered in the middle of the session, which corresponds to roughly 30s after the start of the measurement. In our scenario the callee has two different wireless network interfaces including a simulated UMTS interface and a Wi-Fi interface. We configured the Wi-Fi settings corresponding to IEEE 802.11g with delay of 50 ms and bandwidth of 54 Mbps, while the simulated UMTS is configured with maximum transfer bit rates of 384 kbps and delay of 70 ms (c.f. Table 8.1). In order to observe the packet loss during the HAC operation, we assume there is no packet loss during the transmission. The testbed configuration is shown in Figure 8.1.

For all measurements conducted in this section, the main focus is placed on the impact of HAC on the service continuity (video and audio streaming) when switching between Wi-Fi and UMTS. Specifically, we concentrate on several main parameters, which have significant impact on the overall system performance for multimedia traffic, such as throughput degradation, increased end-to-end latency, and jitter. Three different subtypes of the ICC service were studied, namely the data, voice, and video service.

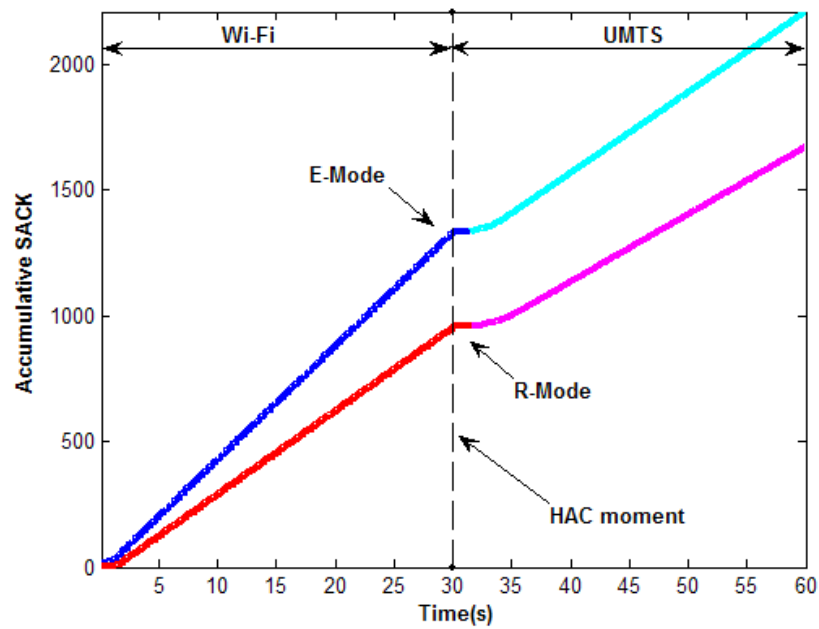
8.5.1. ICC Data Service

This section studies the impact of HAC on the performance of the ICC data service. We assume that data service transmits data using FTP while a smooth HAC is performed. The reliable SCTP is used here as a transport-layer protocol in order to ensure the integrity of the file transfer.

8.5 HAC Performance Evaluation



(a) UMTS-to-Wi-Fi scenario.



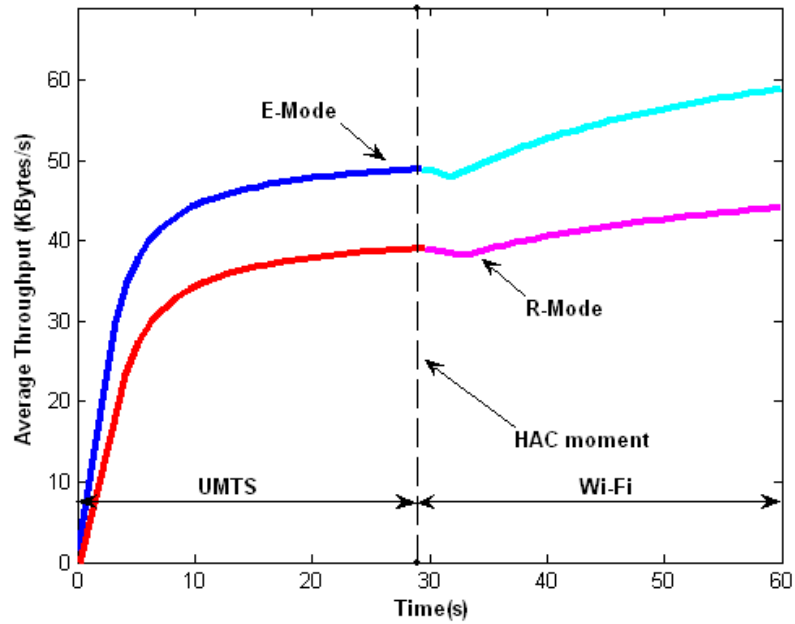
(b) Wi-Fi-to-UMTS scenario.

Figure 8.10.: The accumulative number of SACKs for the ICC data service.

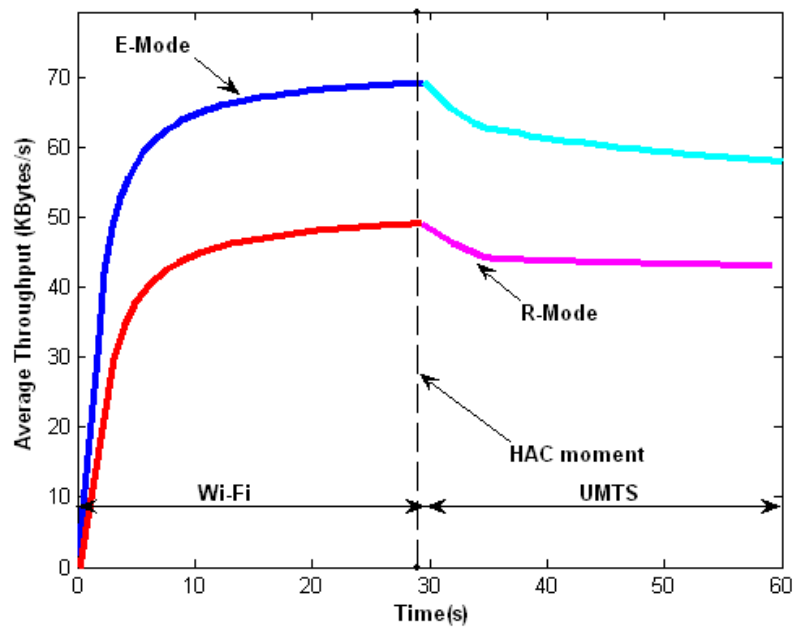
Figure 8.10 depicts the accumulative number of Selective Acknowledgment (SACK) progression for data service in UMTS-to-Wi-Fi and Wi-Fi-to-UMTS scenarios. The number of SACKs indicates the successful transmission of SCTP DATA packets. It can be observed from Figure 8.10 that the accumulative number of SACKs stops increasing for a few seconds after the HAC execution. This is because the data service adapts the “full reliability”, and HAC provokes the slow start mechanism. Figure 8.10(a) shows that the accumulative number of SACKs increases more rapidly after the HAC execution, whilst Figure 8.10(b) indicates that the increase rate of accumulative number of SACKs decreases after the HAC operation in the Wi-Fi-to-UMTS scenario due to the bandwidth reduction from Wi-Fi to UMTS.

Figure 8.11 plots the experimental results of data throughput in both UMTS-to-Wi-Fi and Wi-Fi-to-UMTS scenarios. It can be observed from both scenarios that: (1) the E-Mode provides a higher throughput than the R-Mode and (2) at the beginning of the transmission the throughput is low for both modes; this is because the reliable SCTP increases its congestion window size gradually within the slow start procedure, which limits the transmission rate from the sender. It is noted in Figure 8.11(a) that: (1) after the HAC operation, the throughput drops a little and then it rapidly recovers the transmission for both modes, and (2) the E-Mode can recover more rapidly than the R-Mode after the handoff; this is because the E-Mode has less Round-Trip Time (RTT), and the reliable SCTP increases the CWND per RTT. The Wi-Fi-to-UMTS scenario as shown in Figure 8.11(b) gives some more interesting insights: the throughput experiences a sudden decrease of the available bandwidth after the HAC. This is due to the fact that the old Wi-Fi path has a large congestion window, whereas the new UMTS path has lower bandwidth and higher delay. Since the throughput in data service is governed largely by the available network capacity on the path between the sender and receiver, the data rate over the new path is initially significantly lower than that of the old path. This leads to packet missing reports and thereby the CWND drops and the data rate slows down but recovers only after a while. This implies that it is necessary to make a estimation in advance of the use of appropriate traffic control schemes in the data service for HAC in a Wi-Fi-to-UMTS scenario.

The end-to-end delay is defined as a period of time from the moment at which the sender passes the packet for transmission to the moment at which the receiver receives the packet.



(a) UMTS-to-Wi-Fi scenario.



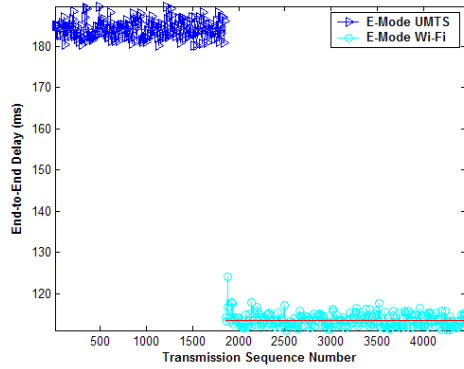
(b) Wi-Fi-to-UMTS scenario.

Figure 8.11.: The throughput for the ICC data service.

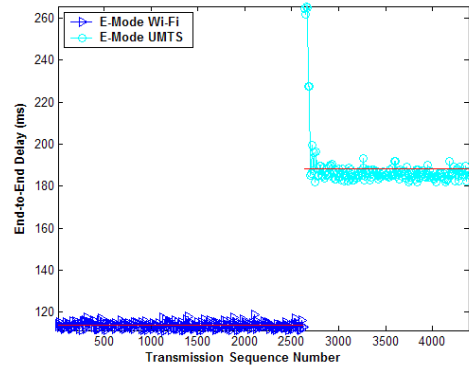
The results in Figure 8.12 depict the instantaneous end-to-end delay performance of SCTP packets for both modes in UMTS-to-Wi-Fi and Wi-Fi-to-UMTS scenarios. It is shown that the end-to-end delay measured in UMTS-to-Wi-Fi scenario is reduced after the HAC switching, whilst in Wi-Fi-to-UMTS scenario the end-to-end delay experiences a significant increase after HAC. Furthermore it can be observed that in all four cases the end-to-end delay experiences a sudden short-time increase after HAC. The end-to-end delay after HAC increases significantly especially in the E-Mode, causing a delay spike. This is because the latency between the last packet received before the handoff and the first packet received after the handoff is larger in the E-Mode as explained in Section 8.4.2. In addition, the cumulative distribution function (CDF) observation is shown in Figures 8.12(e) and 8.12(f). It is indicated that the R-Mode appears more costly than the E-Mode with respect to the end-to-end delay. Compared with the R-Mode, the E-Mode reduces the mean end-to-end delay of the ICC data services by around 24% in both scenarios. The reason is that when the R-Mode is employed, the increase of delay is mostly a result of the processing delay experienced with the respect of the ICC-SP. Given that the average transfer rate for the ICC data service is large, the processing delay in the ICC-SP is also high and thus the end-to-end delay is larger in the R-Mode.

Figure 8.13 presents the instantaneous jitter performance achieved by the ICC data transfer for both modes. The jitter is typically a measure of the variance of the end-to-end delay as shown in Equation (8.4). We can observe that there is a jitter spike existing at the beginning of HAC operation for both modes in Wi-Fi-to-UMTS scenario. The main reason for this is that the end-to-end delay is increased and bandwidth is decreased after HAC in this scenario. Since the instantaneous jitter on the ICC data service features slight differentiation under the same scenario, we demonstrate the performance gain by analyzing the cumulative distribution function (CDF) of jitter performance for data transfer in Figures 8.13(e) and 8.13(f). The overall steepness of the jitter CDF slope proportionally indicates the stability of the operational mode. Numerically it is noted that in both scenarios the steepness of slope for the R-Mode is bigger than the E-Mode and thus the R-Mode is less reliable.

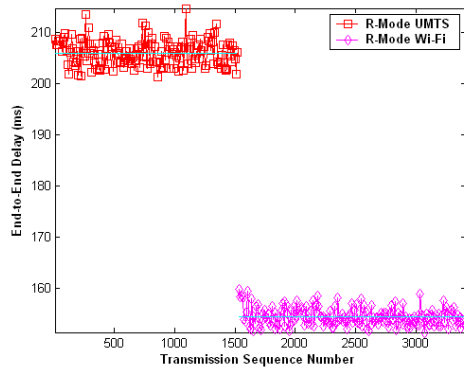
8.5 HAC Performance Evaluation



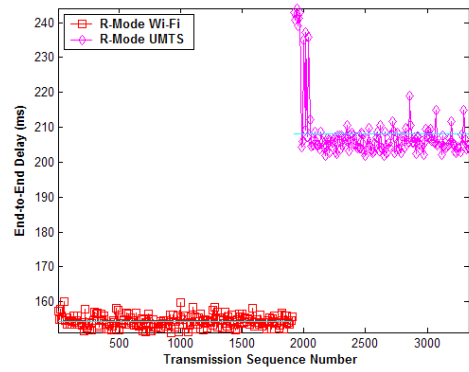
(a) E-Mode in UMTS-to-Wi-Fi scenario.



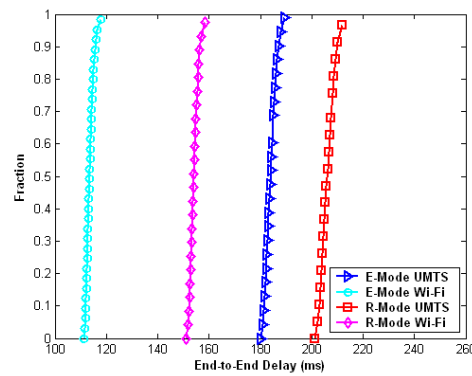
(b) E-Mode in Wi-Fi-to-UMTS scenario.



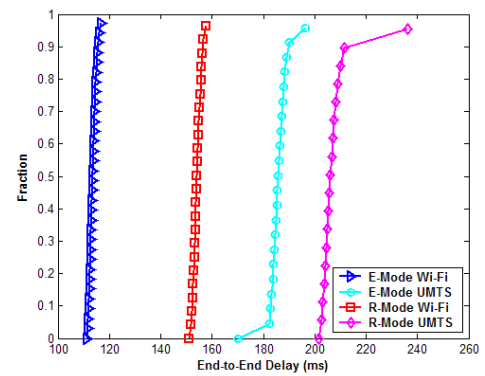
(c) R-Mode in UMTS-to-Wi-Fi scenario.



(d) R-Mode in Wi-Fi-to-UMTS scenario.



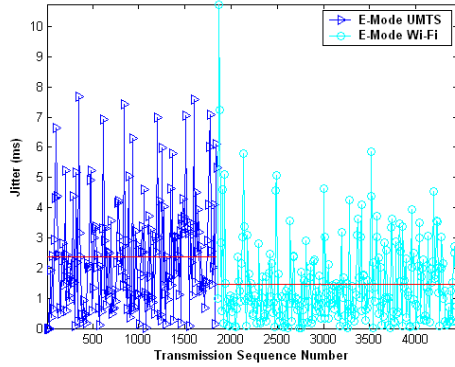
(e) Cumulative distribution of end-to-end delay in UMTS-to-Wi-Fi scenario.



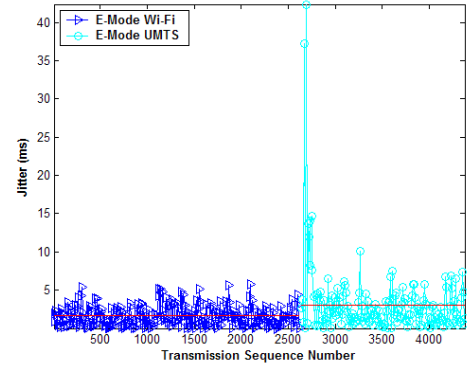
(f) Cumulative distribution of end-to-end delay in Wi-Fi-to-UMTS scenario.

Figure 8.12.: The end-to-end delay for the ICC data service.

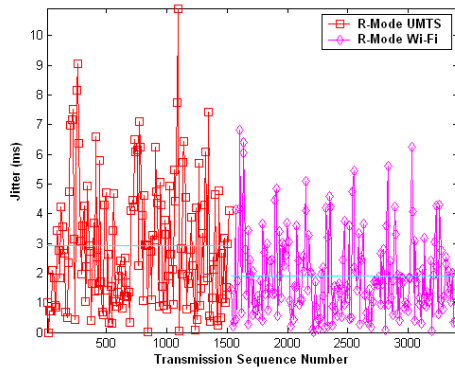
8.5 HAC Performance Evaluation



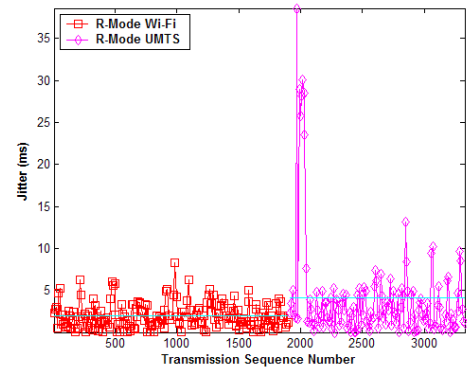
(a) E-Mode in UMTS-to-Wi-Fi scenario.



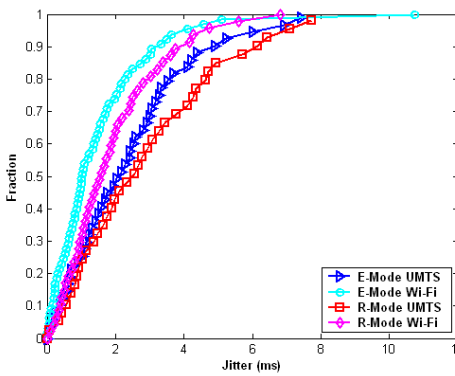
(b) E-Mode in Wi-Fi-to-UMTS scenario.



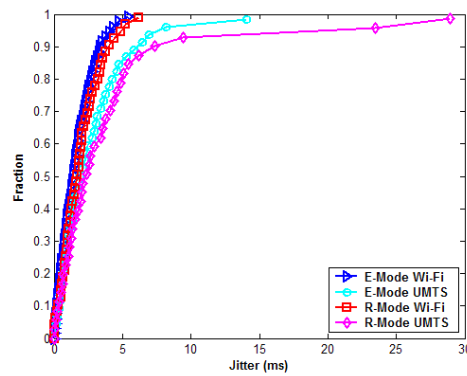
(c) R-Mode in UMTS-to-Wi-Fi scenario.



(d) R-Mode in Wi-Fi-to-UMTS scenario.



(e) Cumulative distribution of jitter in UMTS-to-Wi-Fi scenario.



(f) Cumulative distribution of jitter in Wi-Fi-to-UMTS scenario.

Figure 8.13.: The jitter for the ICC data service.

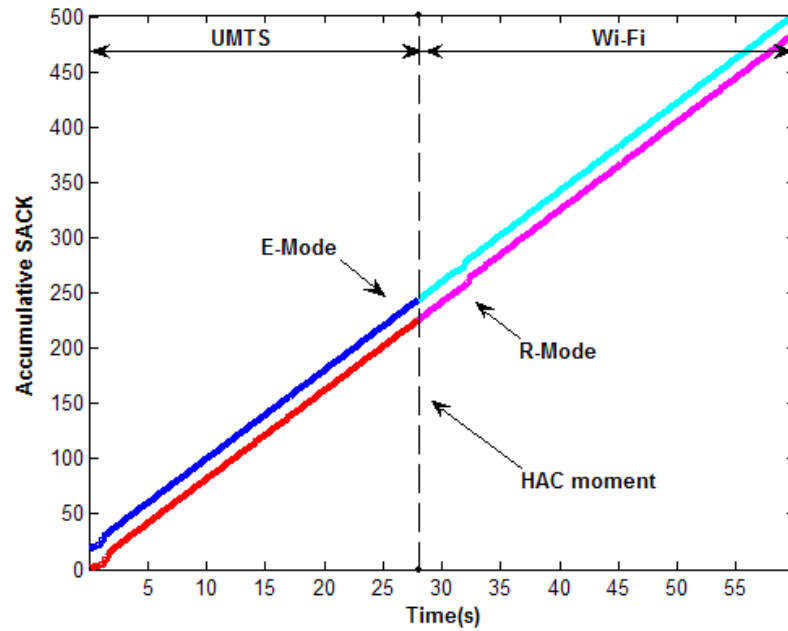
8.5.2. ICC Voice Service

This section presents the experimental results on how the proposed HAC scheme reflects on the performance of the ICC voice service in both UMTS-to-Wi-Fi and Wi-Fi-to-UMTS scenarios. In general, the ICC voice service deals with time sensitive traffic, and thus is primary concerned with delay and jitter rather than throughput. In other words, the voice service may tolerate some loss in transmission rather than delay, as loss of a packet in audio application may be unnoticeable with suitable error concealment algorithms. For this, the modified PR-SCTP is adapted here to minimize the affect of delay caused by retransmission and congestion control. The modified details have been described in Section 7.3.

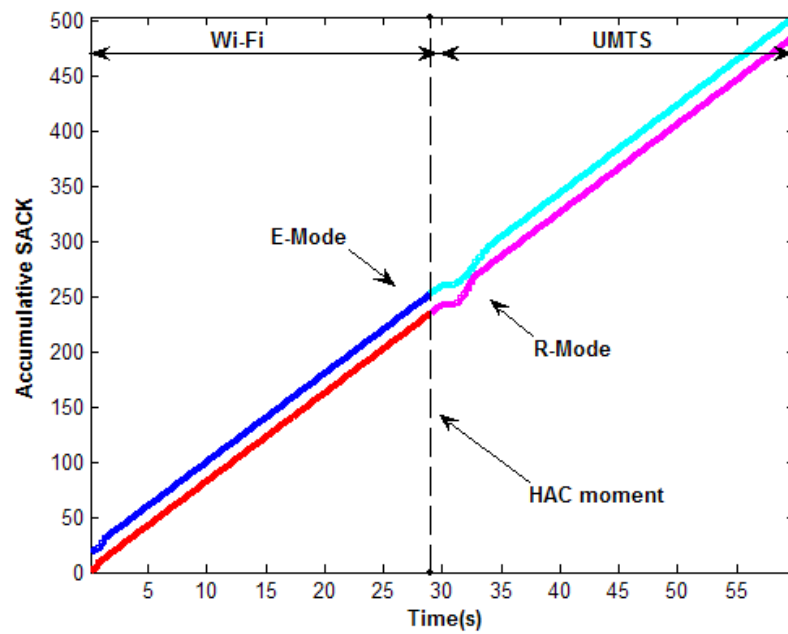
For evaluating the performance of the ICC voice service, we transmitted voice traffic with G.711 codec at a rate of 64 kbit/s over the testbed environment. We aimed to measure the throughput, delay and jitter for the voice stream by provoking the HAC in the middle of the session. In addition to the traditional QoS parameters, we also implemented a objective measurement based on Perceptual Evaluation of Speech Quality (PESQ) [211], which was primarily designed for application-level voice QoS measurement in telecommunications. The PESQ is measured by comparing the reference recorded audio files with the received recorded files, and the Mean Opinion Score (MOS) value is further calculated by the PESQ as indicated in [212].

Figure 8.14 presents the accumulative number of SACKs progression for the ICC voice service with comparison of the R-Mode and E-Mode. The results show that the accumulative number of SACKs progression keeps increasing at the same rate after the HAC execution. Furthermore it can be observed that the performance degradation caused by the congestion avoidance procedure is eliminated by comparison with the the ICC data service. This is generally due to the modified PR-SCTP scheme, which prohibits SCTP going into congestion avoidance and retransmission phase. The situation in Wi-Fi-to-UMTS scenario is slightly different in that there is a slight decrease on transmission rate in case of HAC operation for both modes. This is due to the sudden decrease of the

8.5 HAC Performance Evaluation



(a) UMTS-to-Wi-Fi scenario.



(b) Wi-Fi-to-UMTS scenario.

Figure 8.14.: The accumulative number of SACKs for the ICC voice service.

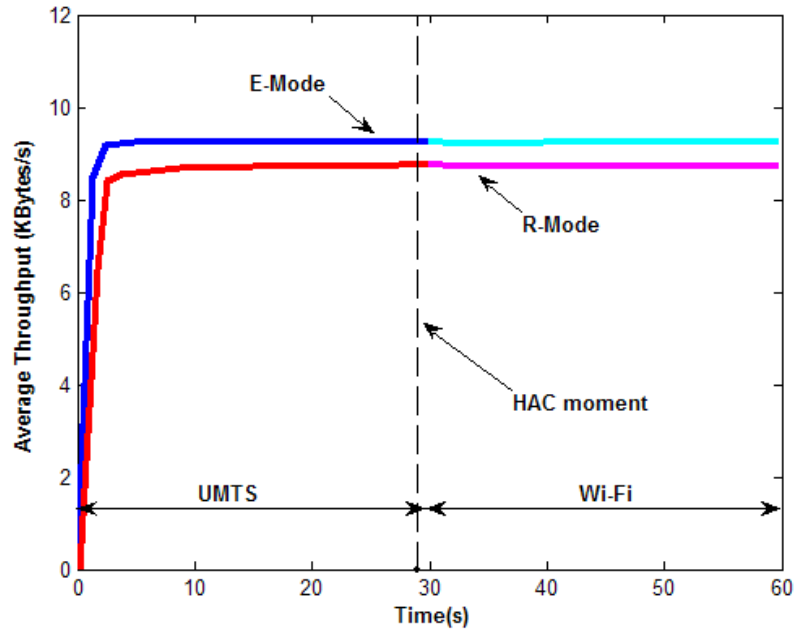
available bandwidth during the HAC from Wi-Fi to UMTS. Finally, it can be seen that the modified PR-SCTP scheme adapts fast to the new path even for the R-Mode where the SCTP packets are transmitted via the ICC-SP.

Figure 8.15 presents the throughput performance for the ICC voice service on separate paths with the comparison of the E-Mode and R-Mode. Recall from the ICC data service that in case of a reliable SCTP a large delay can cause spurious re-transmissions and even lead to retransmission timeouts. However, the results from Figure 8.15 show that there is no behavior performance degradation due to congestion avoidance procedure. As illustrated in Figure 8.15(a) the instantaneous throughput in the R-Mode is very similar to that in the E-Mode with difference of 0.5 KByte/s, and even at the moment of HAC the transmission data rate keeps steady for both modes. In addition, the measurements in the Wi-Fi-to-UMTS scenario (c.f. Figure 8.15(b)) illustrate that there is a notch on the throughput performance during the HAC operation in the both modes and then it rapidly recovers transmission to the normal data rate. However, the notch phenomenon is more significant in the E-Mode, where the disruption lasts longer. The effect of a sudden decrease of the available bandwidth during the HAC causes a throughput degradation lasting for roughly 4s in the E-Mode and 3s in the R-Mode. This is because the HAC in the E-Mode is performed end-to-end and thus the throughput takes more time to recover.

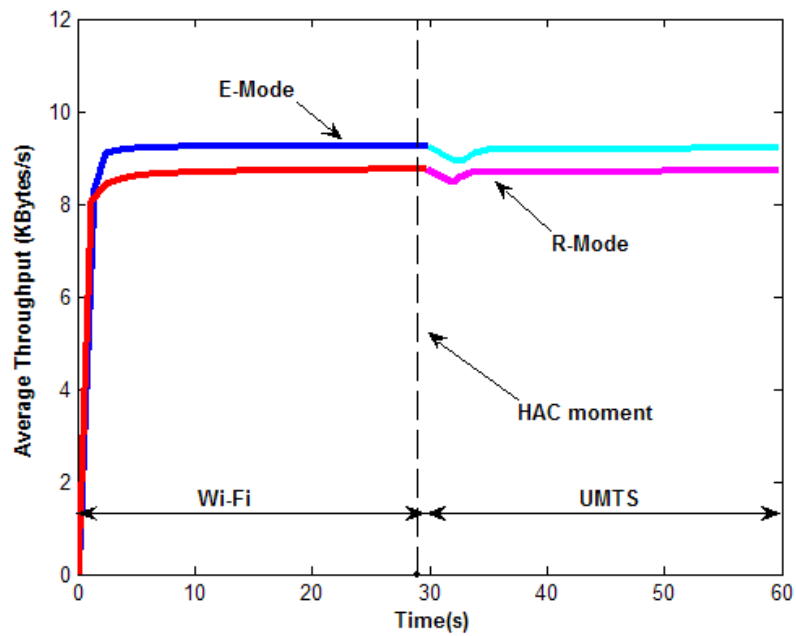
Figure 8.16 shows the mean Mean Opinion Score (MOS) values for different operational modes and scenarios. It is shown that the E-Mode provides better performance by achieving a higher MOS score. It is obvious that higher delay and jitter in the R-Mode result in degradation of audio playout. This is mainly due to the fact that the R-Mode employs a client-server architecture with the involvement of the ICC-SP, which produces extra system overhead.

Figure 8.17 shows the performance of the instantaneous end-to-end delay with respect to Transmission Sequences Number (TSN). It is seen from Figures 8.17(a) and 8.17(c) that the end-to-end latency decreases after the moment of HAC in UMTS-to-Wi-Fi scenario. On the other hand, it is shown in Figures 8.17(b) and 8.17(d) that the end-to-end delay increases when switching to the UMTS. Recall that the end-to-end delay performance for the ICC data service suffers from significant performance problems in case of HAC

8.5 HAC Performance Evaluation



(a) UMTS-to-Wi-Fi scenario.



(b) Wi-Fi-to-UMTS scenario.

Figure 8.15.: The throughput for the ICC voice service.

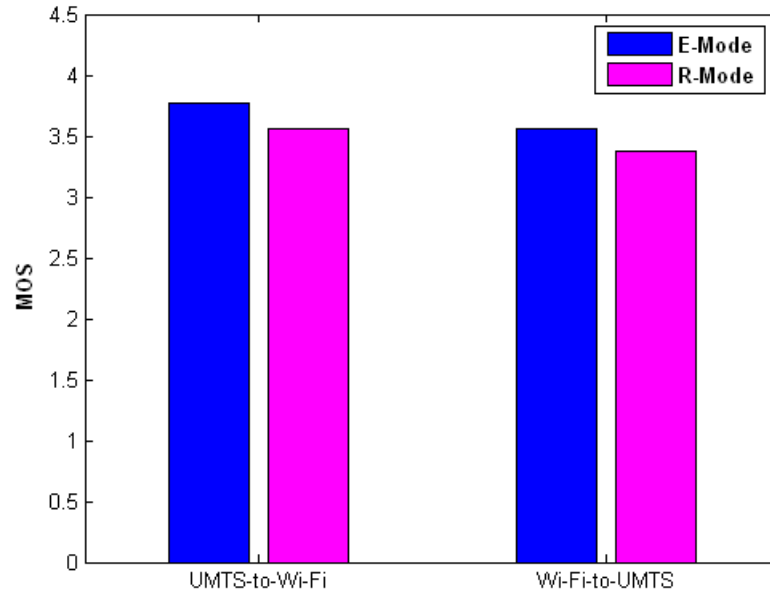


Figure 8.16.: The Mean Opinion Score (MOS) for the ICC voice service.

operation. However, the modified PR-SCTP scheme, adapts faster to the new (worse) link conditions as a HAC in Wi-Fi-to-UMTS scenario. It should be emphasized that there is no sudden spike of the end-to-end delay during the HAC operation, as it was the case in the ICC data service. In addition, the cumulative distribution function (CDF) of the end-to-end delay for the ICC voice service is shown in Figures 8.17(e) and 8.17(f). It is clear in Figure 8.17(e) that the mean end-to-end delay for the R-Mode is larger than that for the E-Mode. The reason for that is because of the packet routing via the ICC-SP which increases the delay. As indicated in Figure 8.17(f), the E-Mode gives relatively less end-to-end delay also in Wi-Fi-to-UMTS scenario. Overall, compared with the R-Mode, the E-Mode reduces the mean end-to-end delay of the ICC voice services by around 30% in both scenarios.

Figure 8.18 presents instantaneous jitter performance for the ICC voice service in both UMTS-to-Wi-Fi and Wi-Fi-to-UMTS scenarios. It can be observed from Figures 8.18(a) and 8.18(c) that the HAC in UMTS-to-Wi-Fi scenario gives no long-term effect on jitter performance for voice traffic. The most observed delay jitter is less than 10 ms, which can be easily smoothed out by using a playout and jitter buffer on the receiving terminal

device. However as illustrated in Figures 8.18(b) and 8.18(d) the jitter increases in Wi-Fi-to-UMTS scenario due to the sudden bandwidth reduction after the HAC switching. Moreover, the CDF of jitter is analyzed to compare the performance of different operational schemes. From the CDF distributions shown in Figures 8.18(e) and 8.18(f), it is further seen that the E-Mode distributes over a fairly small time interval and thereby the E-Mode improves the overall stability of the system.

8.5.3. ICC Video Service

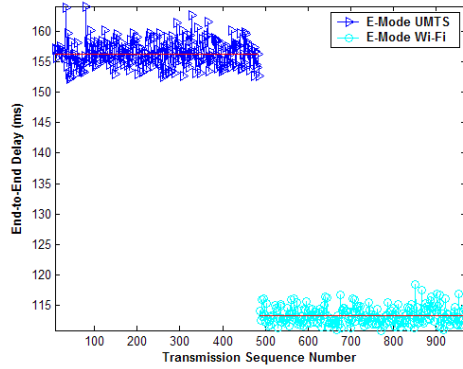
This section provides the obtained results used to compare the HAC performance of the ICC video service for different operational modes. Here we present similar figures but for different service, where the experiment is performed by streaming a MPEG4 (c.f. Appendix B) video, which consists of a number of frames that must be sequentially viewed at a constant rate and in the proper order, over the Wi-Fi and UMTS simulated access networks.

We conducted the experiments by adjusting the existing Evalvid [213] framework with modifications on the transport layer to enable our proposed HAC scheme (c.f. Appendix C). The video quality assessment is evaluated by Peak Signal-to-Noise Ratio (PSNR), which is used to compare a single video source to a reconstructed video at the receiver in the frame-by-frame basis. Here we used Common Intermediate Format (CIF) [214] video source with dimension of 352x288 pixels/frame. The raw Y'UV⁴³ video clip is encoded by FFmpeg⁴⁴ video encoder and converted into RTP hint track at 30 frames per second (fps), which results in a sequence of 1065 frames. The transmission of the MPEG4

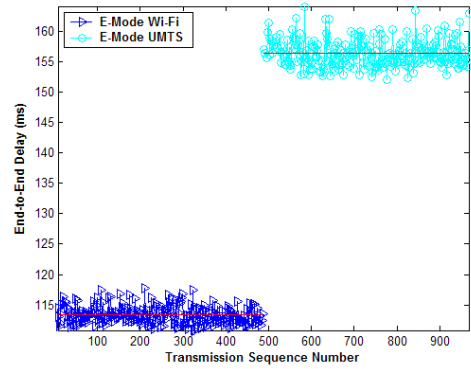
⁴³ The Y'UV is a raw color video standard defined a color space in terms of one luma (Y') and two chrominance (UV) components. The Y'UV color model is widely used in the NTSC, PAL, and SECAM.

⁴⁴ FFmpeg based on libavcodec, is a cross-platform audio/video codec library to record, convert and stream audio and video [215].

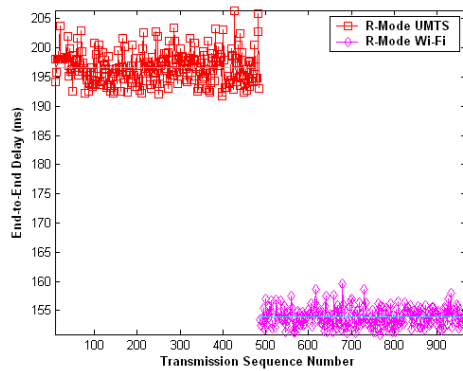
8.5 HAC Performance Evaluation



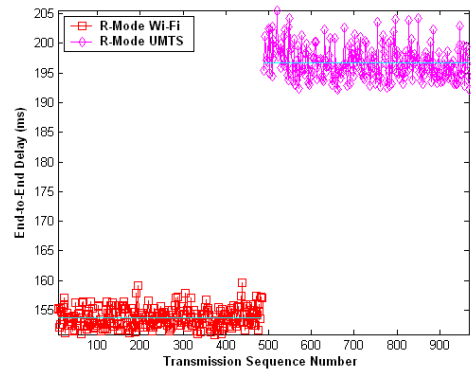
(a) E-Mode in UMTS-to-Wi-Fi scenario.



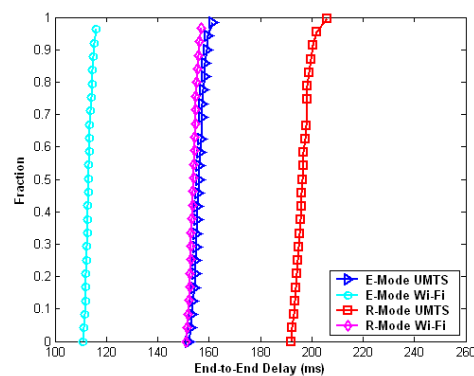
(b) E-Mode in Wi-Fi-to-UMTS scenario.



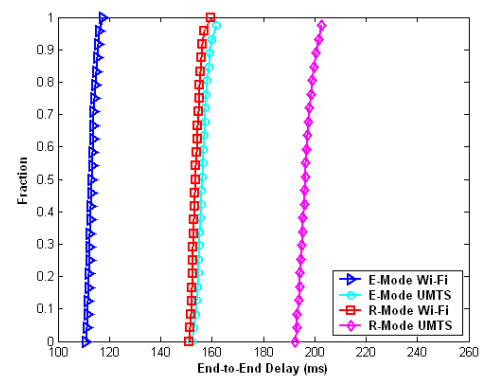
(c) R-Mode in UMTS-to-Wi-Fi scenario.



(d) R-Mode in Wi-Fi-to-UMTS scenario.



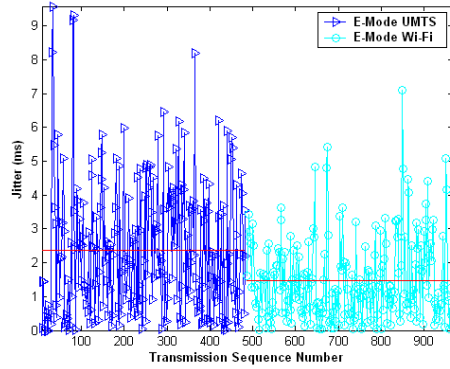
(e) Cumulative distribution of end-to-end delay in UMTS-to-Wi-Fi scenario.



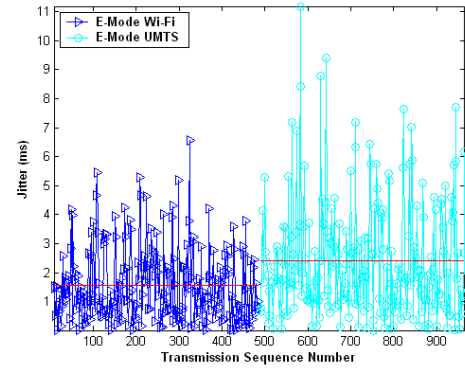
(f) Cumulative distribution of end-to-end delay in Wi-Fi-to-UMTS scenario.

Figure 8.17.: The end-to-end delay for the ICC voice service.

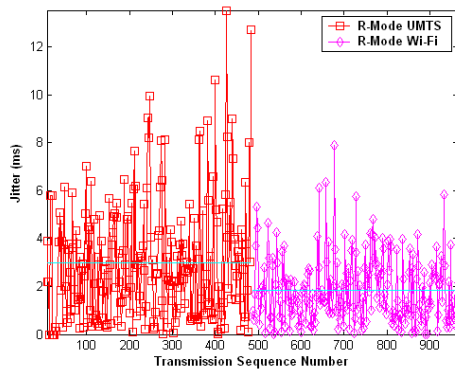
8.5 HAC Performance Evaluation



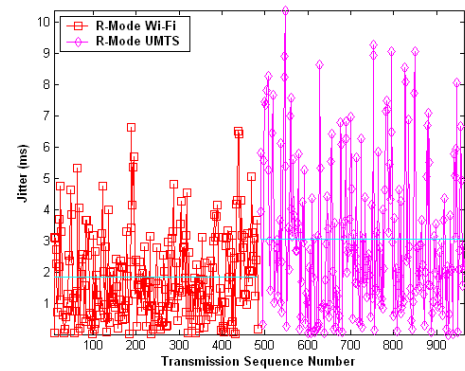
(a) E-Mode in UMTS-to-Wi-Fi scenario.



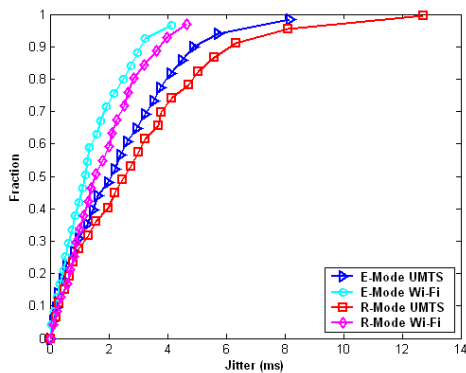
(b) E-Mode in Wi-Fi-to-UMTS scenario.



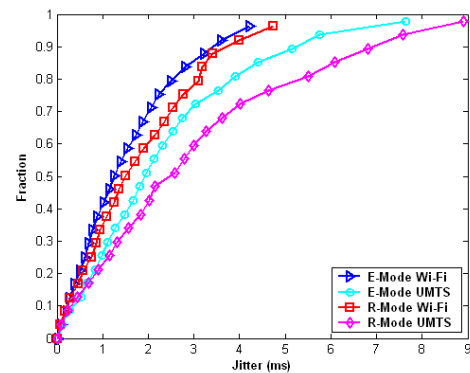
(c) R-Mode in UMTS-to-Wi-Fi scenario.



(d) R-Mode in Wi-Fi-to-UMTS scenario.



(e) Cumulative distribution of jitter in UMTS-to-Wi-Fi scenario.



(f) Cumulative distribution of jitter in Wi-Fi-to-UMTS scenario.

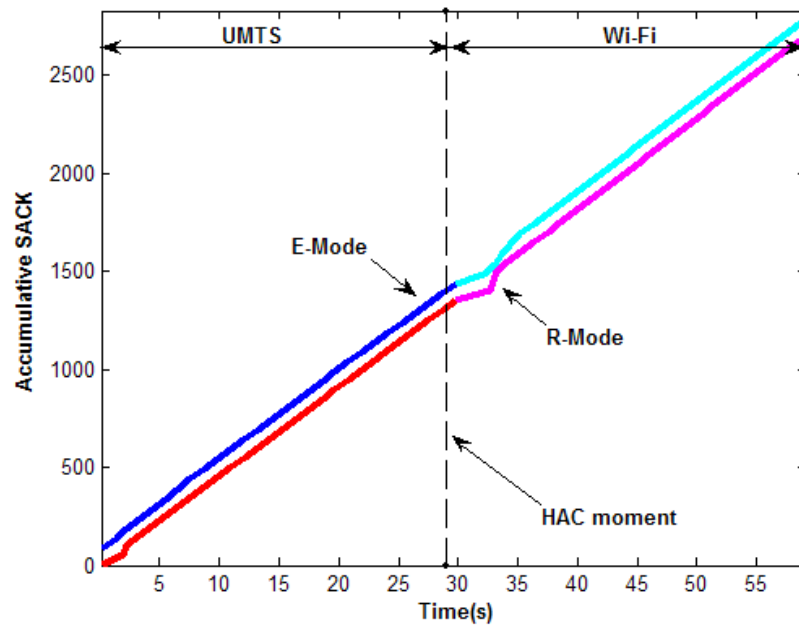
Figure 8.18.: The jitter for the ICC voice service.

video traffic adopts the PR-SCTP transmission to disable retransmission as described in Section 7.3. In order to measure the PSNR, the video sender reads the compressed video file (output of video encoder), fragments each video frame into segments of 1024 bytes, and then transmits these segments encapsulated into SCTP packets. At the receiver, a trace file is generated. We use the original video file, the video trace file, the sender trace file, and the receiver trace file to generate a possibly corrupted video, which is also viewed as the reconstructed video file at the receiver side. To do this, we use a trace program in [10], which in fact is a part of the Evalvid framework, to copy the original video trace file frame-by-frame and omit frames indicated as lost or corrupted at the receiver side. Finally the PSNR is calculated by comparing the original YUV video file and reconstructed YUV video.

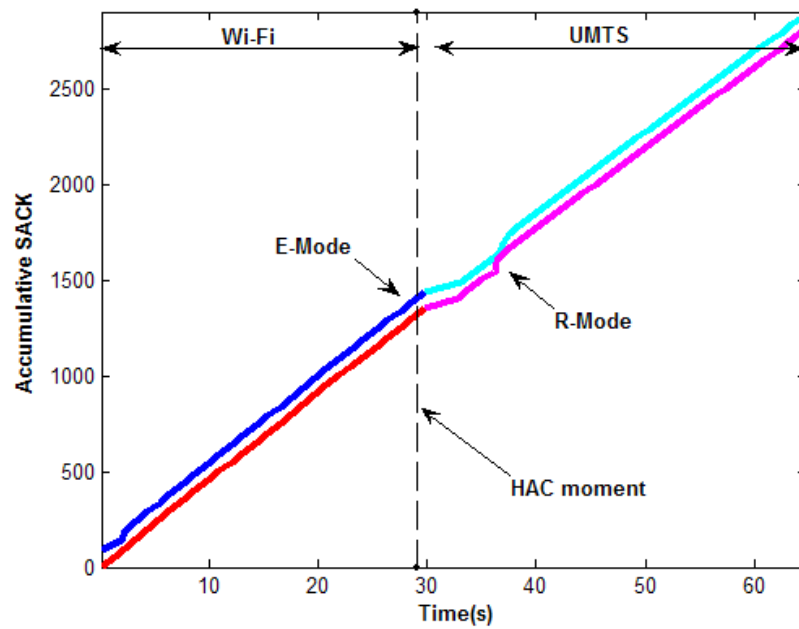
Figure 8.19 presents the accumulative number of SACKs for the ICC video service with comparison of the E-Mode and R-Mode in different scenarios. Note that the PR-SCTP is especially modified to meet the low-delay and low-jitter requirements for multimedia flows. The results in Figure 8.19(a) show that there is a slight disruption after the HAC execution in the UMTS-to-Wi-Fi scenario, after which the accumulative number of SACKs keeps increasing at the same rate. Furthermore, it worth mentioning in Figure 8.19(b) that there is a more significant degradation on the accumulative number of SACKs progression in the Wi-Fi-to-UMTS scenario. This is due to that video traffic is very demanding on bandwidth, and the HAC from the high bandwidth to low bandwidth causes a large portion of packets being lost. However, there is a dramatic increase at the time of 38s, because we employ the modified PR-SCTP, where the FORWARD message is sent to move the cumulative ACK point forward. This prevents the continuous degradation on the SACK progression.

Figure 8.20 compares the instantaneous throughput for the ICC video service in UMTS-to-Wi-Fi and Wi-Fi-to-UMTS scenarios. It is noted from Figure 8.20(a) that the E-Mode introduces a small notch in the throughput graph in the case of HAC. It is obvious that R-Mode suffers from a deeper performance degradation due to the involvement of the ICC-SP. However, the R-Mode adapts faster to the new link conditions after HAC. This is because the R-Mode has less HAC session switching delay. It is shown in Figure 8.20(b) that although the normal transmission is quickly resumed after the HAC operation, the

8.5 HAC Performance Evaluation

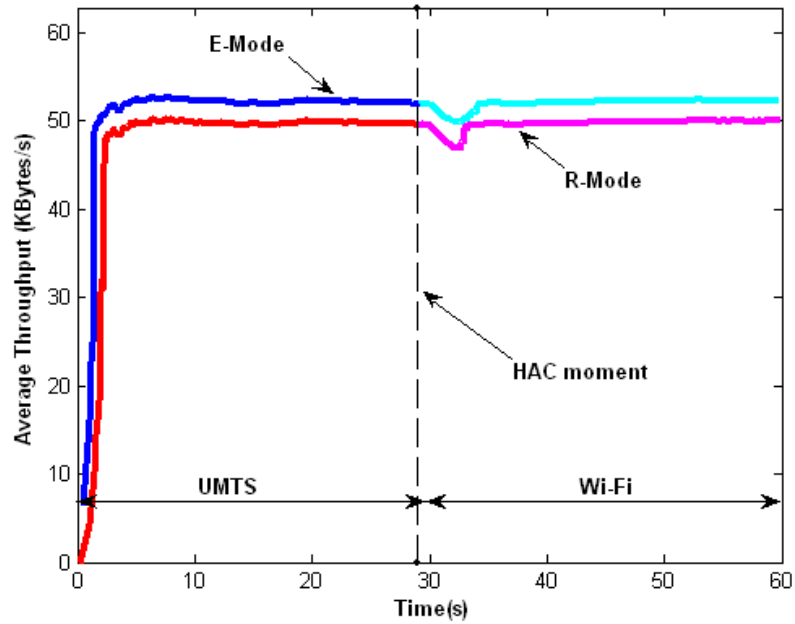


(a) UMTS-to-Wi-Fi scenario.

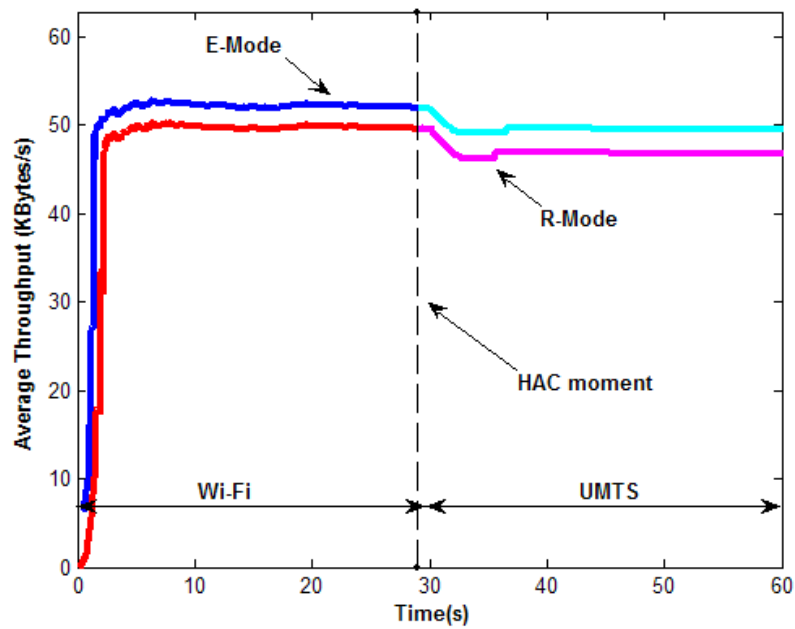


(b) Wi-Fi-to-UMTS scenario.

Figure 8.19.: The accumulative number of SACKs for the ICC video service.



(a) UMTS-to-Wi-Fi scenario.



(b) Wi-Fi-to-UMTS scenario.

Figure 8.20.: The throughput for the ICC video service.

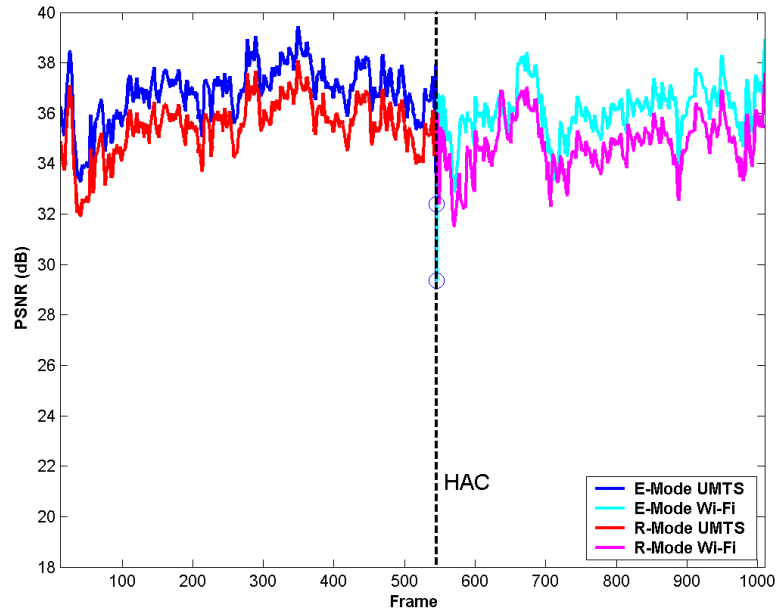
mean throughput experienced by the ICC video service is reduced by 1.9 Kbytes/s for the E-Mode and by 1.6 Kbytes/s for the R-Mode. This is because the Wi-Fi-to-UMTS scenario leads to the video stream passing from a high-bandwidth to a low-bandwidth connection. As a result, the bandwidth reduction introduces a continuous data loss and degrades the throughput performance in Wi-Fi-to-UMTS scenario.

PSNR is used to assess the application-level QoS of the ICC video services. Figure 8.21 shows the comparison results of the frame-by-frame PSNR performance for both operational modes in UMTS-to-Wi-Fi and Wi-Fi-to-UMTS scenarios. During the measurement 1065 video frames were transmitted and the HAC is triggered after the first 540 frames. As can be seen, on average the E-Mode maintains better PSNR performance than the R-Mode mode regardless of the scenario used. It can be observed that HAC operation has a pronounced impact on the ICC video service in terms of the PSNR. The worst PSNR values are observed for the E-Mode at the time of HAC is performed in the Wi-Fi-to-UMTS scenario, where there is a dramatic PSNR drop of about 5 dB.

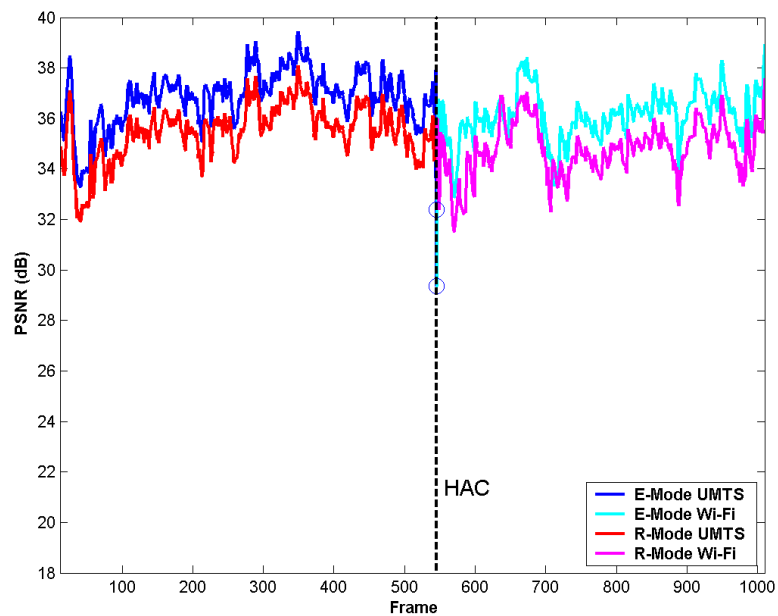
Figure 8.22 shows the performance of the ICC video service in terms of the end-to-end delay in both scenarios. Similarly to the ICC voice service, the end-to-end delay decreases in the UMTS-to-Wi-Fi scenario, and increases in the Wi-Fi-to-UMTS scenario. It can be seen from Figures 8.22(a) and 8.22(b) that the E-Mode introduces a noticeable spike at the moment of the HAC. This is due to the fact that in the E-Mode the video packets queue up at the caller side when switching to a new path. However, there is no marginal spike during the HAC operation in the R-Mode. This is because the R-Mode reduces the HAC switching time by exchanging signaling message to the ICC-SP, which prevents the performance degradation in the case of network abnormalities such as delay spikes. Thus the R-Mode is less likely to suffer from the sudden bandwidth change on connection when the ICC video service has higher data rate. Furthermore Figures 8.22(e) and 8.22(f) present the cumulative distribution function (CDF) of the end-to-end delay for the ICC video service. We can see that on average the E-Mode reduces the end-to-end delay by 29% in both scenarios.

Jitter is the main performance metric that affects the quality of video received by an end-user. The influence of HAC on jitter is presented in Figure 8.23. It can be observed from

8.5 HAC Performance Evaluation



(a) UMTS-to-Wi-Fi scenario.



(b) Wi-Fi-to-UMTS scenario.

Figure 8.21.: The Peak Signal-to-Noise Ratio (PSNR) for the ICC video service.

Figures 8.23(a) and 8.23(c) that the jitter is reduced after the HAC operation in UMTS-to-Wi-Fi scenario. Furthermore, Figures 8.23(b) and 8.23(d) show that the jitter experiences an increase in Wi-Fi-to-UMTS scenario. The reason is that the high data rate video stream is suddenly switched over a relatively low-bandwidth path. There is a jitter spike at the moment of the HAC operation for the E-Mode. This is caused by the sudden change of the end-to-end delay. In addition, Figures 8.23(e) and 8.23(f) show that the steepness of the jitter CDF slope for UMTS is steeper than that of Wi-Fi, which indicates that Wi-Fi has better jitter performance. It is further shown that the R-Mode increases the steepness of the jitter CDF slope in both scenarios.

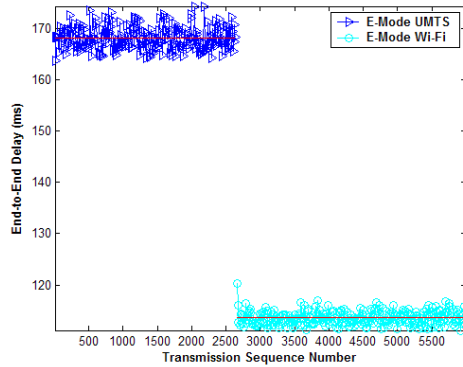
8.6 Conclusions

In this chapter, the experimental measurements of various performance metrics conducted in a testbed environment for different scenarios and ICC operational modes have been described and the obtained results explained.

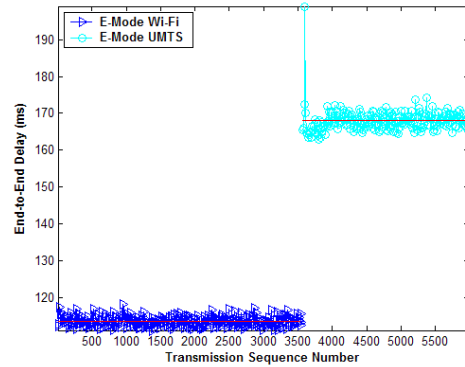
First of all, the ICC signaling performance has been evaluated in a generic scenario with indicative performance overhead. In particular, we have investigated and measured the latency when different operational modes are employed. The results show that the R-Mode performs better in the “ICC session setup” phase, but the E-Mode outperforms the R-Mode in terms of the session release delay. On the other hand, the E-Mode results in less ICM CPU load, which means the E-Mode relies less on the ICC-SP. We then have investigated the signaling performance in terms of the HAC switching delay. The experimental results show that the HAC switching delay can be reduced by the R-Mode in both UMTS-to-Wi-Fi and Wi-Fi-to-UMTS scenarios.

Then the impact of HAC on three different ICC service subtypes has been analyzed. For non-real-time traffic, the HAC performance is quantified in terms of throughput degradation. The experimental measurements show that the impact of HAC on the throughput

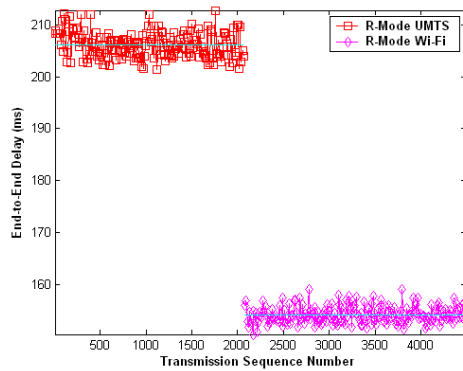
8.6 Conclusions



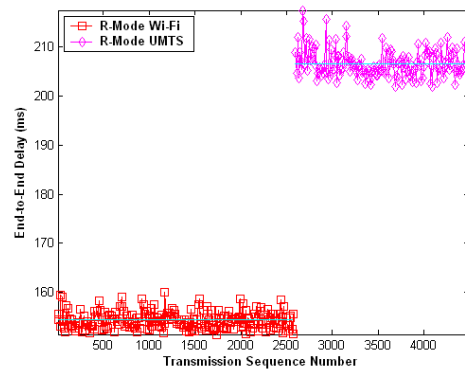
(a) E-Mode in UMTS-to-Wi-Fi scenario.



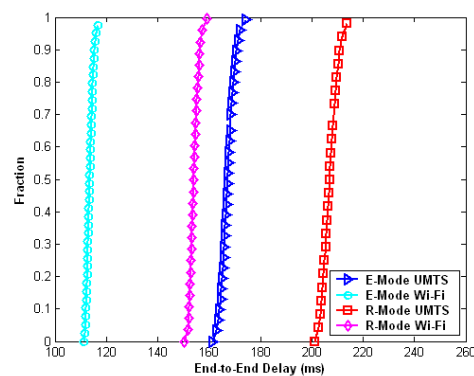
(b) E-Mode in Wi-Fi-to-UMTS scenario.



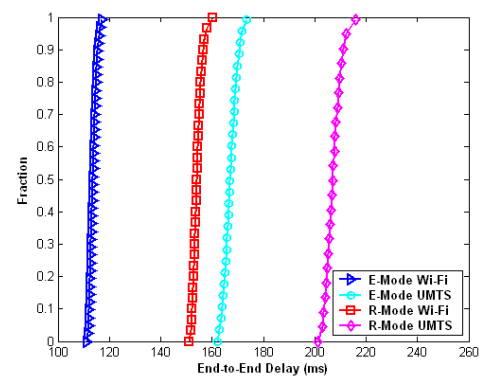
(c) R-Mode in UMTS-to-Wi-Fi scenario.



(d) R-Mode in Wi-Fi-to-UMTS scenario.

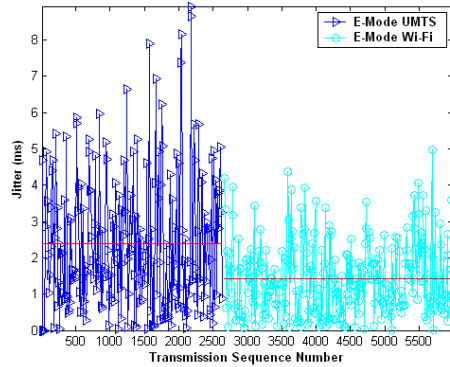


(e) Cumulative distribution of end-to-end delay in UMTS-to-Wi-Fi scenario.

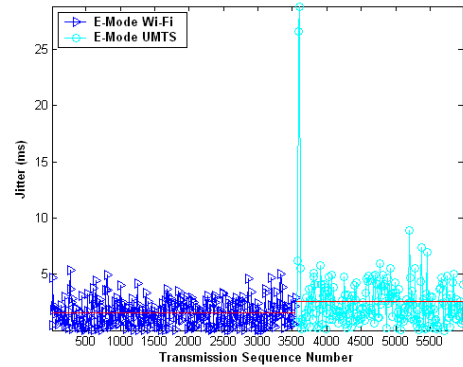


(f) Cumulative distribution of end-to-end delay in Wi-Fi-to-UMTS scenario.

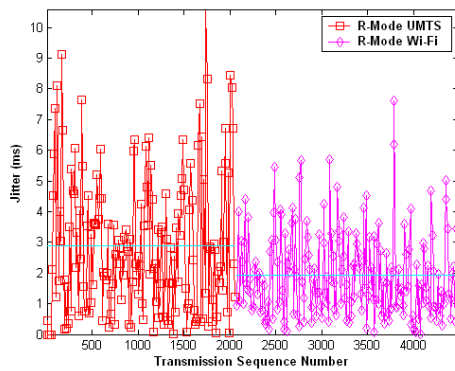
Figure 8.22.: The end-to-end delay for the ICC video service.



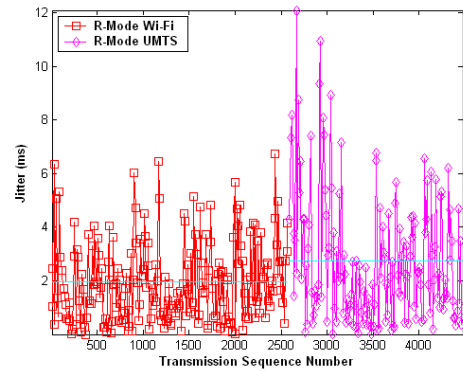
(a) E-Mode in UMTS-to-Wi-Fi scenario.



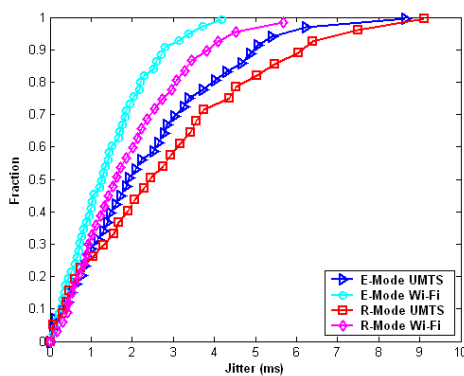
(b) E-Mode in Wi-Fi-to-UMTS scenario.



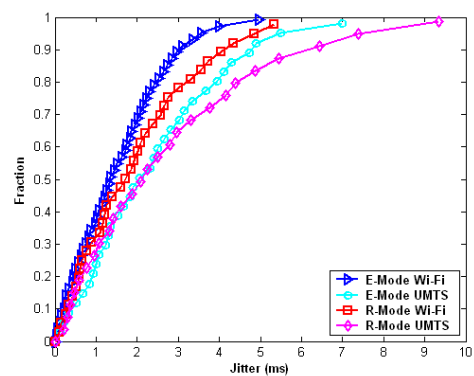
(c) R-Mode in UMTS-to-Wi-Fi scenario.



(d) R-Mode in Wi-Fi-to-UMTS scenario.



(e) Cumulative distribution of jitter in UMTS-to-Wi-Fi scenario.



(f) Cumulative distribution of jitter in Wi-Fi-to-UMTS scenario.

Figure 8.23.: The jitter for the ICC video service.

performance of the ICC data service did not impact the service continuity. However, the results also indicate that use of full SCTP reliability can cause considerable problems in terms of delay and jitter during the HAC switching. The performance degradation is worse for the R-Mode mode. Overall, the proposed E-Mode is able to provide better performance than the R-Mode for the ICC data service.

As the real-time traffic is delay-sensitive, the delay and jitter are selected as the key QoS metrics for the the ICC voice services. As a modified PR-SCTP is used to reduce the delay and jitter caused by congestion avoidance and retransmission, it is shown that the proposed HAC scheme based on a modified PR-SCTP is effective to keep the transmission steady for the the ICC voice service. The results show that use of a modified PR-SCTP in the ICC voice service is clearly advantageous and thereby the performance can be improved in terms of delay and jitter. Overall for the ICC voice service, the E-Mode gives better performance in terms of the end-to-end delay, jitter and Mean Opinion Score (MOS) value.

Analysis of the ICC video service performance demonstrates that the proposed HAC scheme based on a modified PR-SCTP is capable of offering acceptable performance. Our measurements prove that the proposed PR-SCTP scheme with HAC can deliver flexible and relatively acceptable services. In general, the E-Mode has better performance at the cost of a sudden spike in the end-to-end delay and jitter at the moment of HAC. The results show that the the E-Mode maintains better Peak Signal-to-Noise Ratio (PSNR) performance than the R-Mode, no matter before or after the HAC is triggered. However, at the moment of HAC the E-Mode causes a sudden PSNR drop, especially in Wi-Fi-to-UMTS scenario. It is also shown that the R-Mode is less likely to suffer from the sudden bandwidth change on connection when the the ICC video service has higher data rate.

The results shown in this chapter have revealed several issues that need to be addressed. First of all, for the ICC data service, the results indicate that use of full SCTP reliability can cause considerable problems in terms of delay and jitter during the HAC switching. It is also shown that for the ICC voice service the modified PR-SCTP is effective to keep the transmission steady. However, experimental measurements also show that the HAC adds an observable impact on the ICC voice service and introduces a pronounced impact

for the ICC video service in terms of the PSNR. Second, the E-Mode can effectively offer reasonably lower delay and jitter for all scenarios at the expense of high HAC switching delay. The advantage of the E-Mode is generally the less involvement of ICC-SP, which introduces less processing delay and routing delay. On the other hand, the attractive feature of the R-Mode is that it has less HAC switching delay. The results also show that the R-Mode eliminates the spike phenomena during the HAC switching especially for a high data rate ICC video service.

Sometimes a scream is better than a thesis.

— Ralph Waldo Emerson (1803–1882)

9

Conclusions and Future Work

This chapter provides the conclusions drawn from the research work done and presents the directions for future work.

9.1 Thesis Conclusions

As an essential part of the emerging Ubiquitous Consumer Wireless World (UCWW) established on the newly proposed Consumer-centric Business Model, the presented Incoming Call Connection (CBM-ICC) service provision has inherent consumer-oriented nature, which has no equivalent among today's teleservices. This thesis has presented the research and development of this novel consumer-oriented CBM-ICC service and its architecture. The unique consumer-oriented nature poses challenges for the design of a feasible and efficient CBM-ICC service. The proposed CBM-ICC service defines a flexible multimedia delivery scheme to manage the incoming calls with respect to different users' requirements. The service facilitates the establishment (and flexible switching) of the CBM-ICC service via multiple access networks/providers through a novel user-driven, seamless, network-transparent Hot Access network Change (HAC). The key benefits of the CBM-ICC service for future generations of mobile users have been identified. A novel CBM-ICC architecture and infrastructure have been proposed. The main functions,

components and interfaces involved in the CBM-ICC service provision have been set out. A flexible HAC scheme, transparent to the access networks, has been established and proposed for effectively user-driven heterogeneous networking. The HAC makes it more convenient to simultaneously receive incoming calls via multiple access networks, and thereby responding to the requirements of the modern Always Best Connected and best Served (ABC&S) paradigm.

A classification of the main generic CBM-ICC service scenarios has been made. A generic scenario where a mobile user (equipped with a dual-mode terminal) seamlessly switches an active ICC session from one access network to another has been explained in detail and the relevant signaling elaborated. Design of a CBM-ICC proof-of-concept experimental testbed has been described and the implementation of the CBM-ICC service on the testbed has been explained. A modified PR-SCTP protocol has been proposed to provide an optimized service and user experience for real-time multimedia traffic. A generic scenario has been developed to investigate the HAC performance. Finally, we have evaluated the performance of the CBM-ICC service based on the system-level experimental testbed. Two distinct operational modes have been compared in respect to the signaling and HAC performance for a number of key QoS parameters such as delay, jitter, throughput, etc.

The CBM-ICC signaling performance has been evaluated in terms of the delay in different signaling phases. The results show that the Redirection Mode (R-Mode) outperforms the Enquiry Mode (E-Mode) in the ICC session setup, but the E-Mode gives a better performance in terms of the session release delay. On the other hand, on average the E-Mode performs better on system utility. The results also show that the HAC switching delay can be reduced by the R-Mode in both UMTS-to-Wi-Fi and Wi-Fi-to-UMTS scenarios. Furthermore, the impact of the HAC performance on the ICC data, voice and video streaming services has been evaluated in a heterogeneous network environment. The analysis shows that the influence of HAC on the service continuity is minor. However, the performance varies in different service types and scenarios used as follows:

- For the ICC data service, the results indicate that use of full SCTP reliability can cause considerable problems in terms of delay and jitter during the HAC switching.

However, the impact of HAC on data service is not significant and did not interrupt the service.

- For the ICC voice service, the results show that the modified PR-SCTP protocol is effective to keep the transmission steady. The results also indicate that the use of the modified PR-SCTP in voice service is clearly advantageous and thereby the service performance has been improved in terms of delay and jitter.
- For the ICC video service, experimental measurements show that the HAC has an observable and pronounced impact for video streaming in terms of the Peak Signal-to-Noise Ratio (PSNR).

Overall, the performance degradation immediately after the HAC is acceptable in the UMTS-to-Wi-Fi scenario, while in the Wi-Fi-to-UMTS scenario the HAC adds an observable overhead, with a pronounced impact in terms of delay and jitter. In addition, the results advocate that the E-Mode achieves significant performance gain in various aspects such as delay, jitter and throughput, whilst the R-Mode is less likely to suffer from the sudden bandwidth change on connection for higher data rate ICC service. However, from the implementation point of view, the R-Mode will introduce more computational complexity due to the ICC-SP involvement. Therefore the E-Mode is suggested as the most efficient scheme especially for low data rate ICC service.

9.2 Future work

The CBM-ICC service has merely scratched the surface of a variety of interesting research areas in future telecommunications. This completed research has focused mainly on three aspects. The first part of the work attempted to investigate the existing schemes and protocols, extract the necessary requirements and build them into the CBM-ICC service architecture infrastructure. The second part managed to inject some degree of realism into the work by elaborating generic scenarios and analyzing each scenario in detail from the point of view of criteria for operation and protocol reference model. The third part concentrated on the design and implementation of a testbed to probe signaling performance and handoff performance.

However, there are still some issues that could be investigated in the future as per the following suggestions.

An extensive work on the development of the CBM-ICC proof-of-concept testbed has been worked out to test the initial concept and evaluate the service performance. Further extensive implementation and testing will be needed in order to accommodate varying access technologies, signaling formats, and QoS mechanisms. Protocol interfaces between the ICC-SP and ANPs employing different network technology need to be elaborated. The interconnection with Third-Party Authentication, Authorization and Accounting Service Providers (3P-AAA-SPs) needs also to be probed to ensure reasonable level of security.

Development of algorithms to dynamically adapt the service prior to handoff would improve the service performance. This thesis has shown that the HAC adds an observable degradation in the performance for the ICC voice and video service. An advanced buffering algorithm is needed with a combination of the Real-Time Transport Control Protocol (RCTP). Before the detection of handoff, the use of RCTP can pause the transmission of the real-time traffic and continue to retransmit it again when the handoff is completed. Detailed analysis of how to design the algorithm and how disruption of service delivery can be minimized could be carried out.

Further optimization of the handoff performance to meet the desired specified QoS could be undertaken. As experimental results confirmed, the service performance is very likely to suffer from significant degradation when the HAC switching is performed from a high-bandwidth access network to another with low bandwidth. The HAC switching delay can be improved further by using more powerful servers and efficient configuration protocols such as the Dynamic Registration and Configuration Protocol (DRCP) [216]. Another possible approach is to apply a multi-buffer structure, giving to each interface its own send buffer, to ensure path independence as far as transmission is concerned. This solution, however, introduces the need for modifications on SCTP's SACK handling mechanism.

The automatic handoff based on the user decisions behind the proposed HAC could be examined in more detail. An example proposal is that HAC operations could depend on the support of the underlying physical- and link-layer QoS parameters, e.g. based on measurements of the wireless signal strength, packet loss rate, or end-to-end delay and

jitter. An algorithm to place a primary core to collect the lower-layer QoSs parameter with intelligent decision maker could be worked out. One possible solution might be to propose an enhanced HAC scheme to adapt to the changes of network characteristics. This enhanced HAC scheme would detect the path of available capacity to choose different QoS parameters with adaptive rate. It is likely to require the use of Artificial Intelligence (AI) algorithm, e.g. neural networks or fuzzy logic, to decide when and how to perform the handoff. One possible example has been presented in [217], which proposes a fuzzy logic for initiation and decision of vertical handovers among different radio interfaces.

References

- [1] “Multimode (Cellular/WLAN) wireless products and services,” *Disruptive-Analysis Report [Online]* <http://www.disruptive-analysis.com/research.htm>, 2008.
(Cited on pages xiii and 6.)
- [2] R. Watson, *Fixed/Mobile Convergence and Beyond: Unbounded Mobile Communications*. Newnes Elsevier Press, 2008.
(Cited on pages xiii and 6.)
- [3] M. Handley and E. Rescorla, “Internet Denial-of-Service Considerations,” *RFC 4732 [Online]* <http://www.ietf.org/rfc/rfc4732.txt>, 2006.
(Cited on pages xiii, 21, and 23.)
- [4] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson, “Stream Control Transmission Protocol,” *RFC 2960 [Online]* <http://www.ietf.org/rfc/rfc2960.txt>, 2000.
(Cited on pages xiii, 24, and 26.)
- [5] C. Adams, S. Farrell, T. Kause, and T. Mononen, “Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP),” *RFC 4210 [Online]* <http://www.ietf.org/rfc/rfc4210.txt>, 2005.
(Cited on pages xiv, 33, and 86.)
- [6] P. Albitz, *DNS and Bind*. O’Reilly & Associates, Inc. Sebastopol, CA, USA, 2001.
(Cited on pages xiv, 36, and 37.)
- [7] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, “Dynamic Updates in the Domain Name System (DNS UPDATE),” *RFC 2136 [Online]* <http://www.ietf.org/rfc/rfc2136.txt>, 1997.
(Cited on pages xiv, 45, 47, and 48.)

-
- [8] P. V. Mockapetris, “Domain names - implementation and specification,” *RFC 1035* [Online] <http://www.ietf.org/rfc/rfc1035.txt>, 1987.
(Cited on pages xiv, 36, 43, and 48.)
- [9] I. Ganchev and M. O’Droma, “New personal IPv6 address scheme and universal CIM card for UCWW,” *Proceedings of the 7th International Conference on Intelligent Transport Systems Telecommunications (ITST 2007)*, Sophia Antipolis, France., pp. 381–386, 2007.
(Cited on pages xv, 8, 73, 83, 84, 85, 86, 87, and 111.)
- [10] J. Klaue, B. Rathke, and A. Wolisz, “EvalVid - A framework for video transmission and quality evaluation,” *Computer Performance Evaluation: Modelling Techniques and Tools*, vol. 2794, pp. 255–272, 2003.
(Cited on pages xvii, 150, 203, 204, and 205.)
- [11] “Stream Control Transmission Protocol Web Site,” [Online] http://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol, 2009.
(Cited on pages xviii and 22.)
- [12] R. Bruce, *Bell: Alexander Graham Bell and the conquest of solitude*. Cornell University Press, 1990.
(Cited on page 1.)
- [13] F. Khan, *LTE for 4G Mobile Broadband: Air Interface Technologies and Performances*. Cambridge University Press, 2009.
(Cited on page 2.)
- [14] J. Korhonen, *Introduction to 3G mobile communications*. Artech House Publishers, 2003.
(Cited on page 2.)
- [15] O. Levin, “H.323 Uniform Resource Locator (URL) Scheme Registration,” *RFC 3508* [Online] <http://www.ietf.org/rfc/rfc3508.txt>, 2003.
(Cited on page 3.)
-

-
- [16] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," *RFC 3261 [Online]* <http://www.ietf.org/rfc/rfc3261.txt>, 2002.
(Cited on pages 3, 34, and 39.)
- [17] O. Ibe, *Converged Network Architectures: Delivering Voice and Data over IP, ATM, and Frame Relay*. John Wiley & Sons, Inc. New York, NY, USA, 2001.
(Cited on page 3.)
- [18] R. Reynolds and A. Rix, "Quality VoIP - an engineering challenge," *BT Technology Journal*, vol. 19, no. 2, pp. 23–32, 2001.
(Cited on page 3.)
- [19] Ericsson, "EDGE Introduction of high-speed data in GSM/GPRS networks," *Technical Paper [Online]* http://www.ericsson.com/solutions/tems/library/tech_papers/tech_related/edge_wp_technical.pdf, 2005.
(Cited on pages 3 and 4.)
- [20] H. Holma and A. Toskala, *HSDPA/HSUPA for UMTS*. Wiley, 2006.
(Cited on page 4.)
- [21] Ericsson, "Basic Concepts of HSPA," *White paper [Online]* http://www.ericsson.com/technology/whitepapers/3087_basic_conc_hspa_a.pdf, 2007.
(Cited on page 4.)
- [22] H. Holma and A. Toskala, *WCDMA for UMTS: HSPA Evolution and LTE*. John Wiley and Sons Ltd, 2007.
(Cited on page 4.)
- [23] L. Yi-Bing, P. Ai-Chun, H. Yieh-Ran, and I. Chlamtac, "An all-IP approach for UMTS third-generation mobile networks," *IEEE Network*, vol. 16, no. 5, pp. 8–19, 2002.
(Cited on page 5.)
-

- [24] M. O’Droma and I. Ganchev, “Toward a ubiquitous consumer wireless world,” *IEEE Wireless Communications*, vol. 14, no. 1, pp. 52–63, 2007.
(Cited on pages 7, 12, 34, 71, 73, 84, and 96.)
- [25] M. O’Droma, I. Ganchev, G. Morabito, R. Narcisi, N. Passas, S. Paskalis, V. Friderikos, A. S. Jahan, E. Tsontsis, C. Bader, J. Rotrou, and H. Chaouchi, ““Always Best Connected” Enabled 4G Wireless World,” *IST Mobile and Wireless Communications Summit 2003*, pp. 15–18, 2003.
(Cited on page 7.)
- [26] M. O’Droma and I. Ganchev, “Enabling an Always Best-Connected Defined 4G Wireless World,” *Annual Review of Communications, Vol.57 (Chicago, Ill.: International Engineering Consortium, 2004)*, ISBN: 1-931695-28-8, pp. 1157–1170, 2004.
(Cited on page 7.)
- [27] M. O’Droma and I. Ganchev, “Techno-Business Models for 4G,” *Proceedings of the International Forum on 4G Mobile Communications, King’s College London, London, 2004*.
(Cited on page 8.)
- [28] I. Ganchev, F. McEvoy, and M. O’Droma, “New 3P-AAA Architectural Framework and Supporting Diameter Application,” *WSEAS Transactions on Communications*, pp. 176–185, 2005.
(Cited on pages 8 and 9.)
- [29] P. Flynn, I. Ganchev, and M. O’Droma, “Wireless Billboard Channels-Vehicle and Infrastructural Support for Advertisement, Discovery and Association of UCWW Services,” *Annual Review of Communications, Vol.59 (Chicago, Ill.: International Engineering Consortium, 2006)*, 2006.
(Cited on page 8.)
- [30] M. O’Droma, I. Ganchev, and N. Wang, “On incoming call connection service in a ubiquitous consumer wireless world,” in *Proceedings of Next Generation Teletraffic and Wired/ Wireless Advanced Networking*, vol. 4003, 2006, pp. 287–297.

(Cited on page 8.)

- [31] N. Wang, I. Ganchev, and M. O'Droma, "An architecture for the provision of Incoming Call Connection service in UCWW," *IEEE 65th Vehicular Technology Conference, Vols 1-6*, pp. 649–653, 2007.

(Cited on pages 8, 86, 90, and 101.)

- [32] I. Ganchev, M. O'Droma, and N. Wang, "On CBM-ICC Service Provision in UCWW," *Proceedings of the IEEE International Symposium on Wireless Communication Systems (IEEE ISWCS07), Trondheim, Norway*, pp. 128–132, 2007.

(Cited on pages 8 and 101.)

- [33] I. Ganchev, M. O'Droma, and N. Wang, "Consumer-Oriented Incoming Call Connection Service for a Ubiquitous Consumer Wireless World," *Wireless personal communications*, vol. 50, no. 1, pp. 115–131, 2009.

(Cited on pages 8, 101, and 122.)

- [34] F. McEvoy, I. Ganchev, and M. O'Droma, "Building a testbed with new security features for UCWW research," *Proceedings of IEEE International Symposium on Consumer Electronics*, pp. 581–586, 2006.

(Cited on page 9.)

- [35] "Skype Web Site," [Online] <http://www.skype.com>, 2009.

(Cited on pages 10 and 59.)

- [36] "Gizmo Web Site," [Online] <http://www.gizmovoip.com/>, 2009.

(Cited on pages 10 and 61.)

- [37] "Ekiga Web Site," [Online] <http://ekiga.org/>, 2009.

(Cited on pages 10, 59, and 61.)

- [38] N. Alonistioti, N. Passas, A. Kaloxylos, H. Chaouchi, M. Siebert, M. O'Droma, I. Ganchev, and F. Bader, "Business Model and Generic Architecture for Integrated Systems and Services: The ANWIRE Approach," *Proceedings of the WWRP 8bis meeting, 8 pages, Beijing, China*, 2004.

(Cited on page 11.)

-
- [39] H. Chaouchi, G. Pujolle, I. Armuelles, M. Siebert, B. Carlos, I. Ganchev, M. O'Droma, and N. Houssos, "Policy based networking in the integration effort of 4G networks and services," *Proceedings of IEEE 59th Vehicular Technology Conference, Vols 1-5*, pp. 2977–2981, 2004.
(Cited on page 11.)
- [40] I. F. Akyildiz, S. Mohanty, and J. Xie, "A ubiquitous mobile communication architecture for next-generation heterogeneous wireless systems," *IEEE Communications Magazine*, pp. S29–S36, 2005.
(Cited on page 11.)
- [41] Y. Ji, P. Zhang, Z. Hu, X. Wang, Y. N. Li, and X. S. Tang, "Towards mobile ubiquitous service environment," *Wireless Personal Communications*, vol. 38, no. 1, pp. 67–78, 2006.
(Cited on page 11.)
- [42] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, "Hypertext Transfer Protocol – HTTP/1.1," *RFC 2616 [Online]* <http://www.ietf.org/rfc/rfc2616.txt>, 1999.
(Cited on page 18.)
- [43] J. Postel and J. Reynolds, "File Transfer Protocol," *RFC 959 [Online]* <http://www.ietf.org/rfc/rfc959.txt>, 1985.
(Cited on page 18.)
- [44] J. Klensin, "Simple Mail Transfer Protocol," *RFC 5321 [Online]* <http://www.ietf.org/rfc/rfc5321.txt>, 2008.
(Cited on page 18.)
- [45] R. Braden, "Requirements for Internet Hosts – Communication Layers," *RFC 1122 [Online]* <http://www.ietf.org/rfc/rfc1122.txt>, 1989.
(Cited on pages 17 and 18.)
- [46] F. Halsall, "Data communications, computer networks and OSI," *Electronic Systems Engineering Series, Wokingham: Addison-Wesley, 1988, 2nd ed.*, 1988.
-

(Cited on page 17.)

- [47] W. Stallings, *Data and computer communications*. Prentice hall, 1997.

(Cited on page 17.)

- [48] J. Postel, “Internet Protocol,” *RFC 791 [Online]* <http://www.ietf.org/rfc/rfc791.txt>, 1981.

(Cited on page 17.)

- [49] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” *RFC 2460 [Online]* <http://www.ietf.org/rfc/rfc2460.txt>, 1998.

(Cited on pages 17 and 52.)

- [50] J. Loughney, “IPv6 Node Requirements,” *RFC 4292 [Online]* <http://www.ietf.org/rfc/rfc4292.txt>, 2006.

(Cited on page 17.)

- [51] W. Stevens, M. Thomas, E. Nordmark, and T. Jinmei, “Advanced Sockets Application Program Interface (API) for IPv6,” *RFC 3542 [Online]* <http://www.ietf.org/rfc/rfc3542.txt>, 2003.

(Cited on page 17.)

- [52] IESG, “IPv6 Address Allocation Management,” *RFC 1881 [Online]* <http://www.ietf.org/rfc/rfc1881.txt>, 1995.

(Cited on page 18.)

- [53] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” *RFC 2401 [Online]* <http://www.ietf.org/rfc/rfc2401.txt>, 1998.

(Cited on page 19.)

- [54] S. Kent, “IP Authentication Header,” *RFC 4302 [Online]* <http://www.ietf.org/rfc/rfc4302.txt>, 2005.

(Cited on page 19.)

- [55] S. Kent and R. Atkinson, “IP Encapsulating Security Payload (ESP),” *RFC 4303 [Online]* <http://www.ietf.org/rfc/rfc4303.txt>, 2005.

(Cited on page 19.)

- [56] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, “Network Mobility (NEMO) Basic Support Protocol,” *RFC 3963 [Online]* <http://www.ietf.org/rfc/rfc3963.txt>, 2005.

(Cited on page 19.)

- [57] S. Thomson and T. Narten, “IPv6 Stateless Address Autoconfiguration,” *RFC 2462 [Online]* <http://www.ietf.org/rfc/rfc2462.txt>, 1998.

(Cited on page 20.)

- [58] N. Moore, “Optimistic Duplicate Address Detection (DAD) for IPv6,” *RFC 4429 [Online]* <http://www.ietf.org/rfc/rfc4429.txt>, 2006.

(Cited on page 20.)

- [59] B. Haberman and J. Martin, “Multicast Router Discovery,” *RFC 4286 [Online]* <http://www.ietf.org/rfc/rfc4286.txt>, 2005.

(Cited on page 20.)

- [60] R. Droms, J. Bound, C. Perkins, and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” *RFC 3315 [Online]* <http://www.ietf.org/rfc/rfc3315.txt>, 2003.

(Cited on page 37.)

- [61] R. Droms, “Dynamic Host Configuration Protocol,” *RFC 2131 [Online]* <http://www.ietf.org/rfc/rfc2131.txt>, 1999.

(Cited on page 37.)

- [62] R. Droms, “DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” *RFC 3646 [Online]* <http://www.ietf.org/rfc/rfc3646.txt>, 2003.

(Cited on pages 37 and 38.)

- [63] J. Jeong, “IPv6 Host Configuration of DNS Server Information Approaches,” *RFC 4339 [Online]* <http://www.ietf.org/rfc/rfc4339.txt>, 2006.

(Cited on page 38.)

- [64] H. Schulzrinne and B. Volz, “Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers,” *RFC 3319 [Online]* <http://www.ietf.org/rfc/rfc3319.txt>, 2003.
(Cited on page 38.)
- [65] R. Droms, “Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6,” *RFC 3736 [Online]* <http://www.ietf.org/rfc/rfc3736.txt>, 2004.
(Cited on page 38.)
- [66] R. Stewart, “Stream Control Transmission Protocol,” *RFC 4962 [Online]* <http://www.ietf.org/rfc/rfc4962.txt>, 2007.
(Cited on pages 20, 29, 39, 57, and 116.)
- [67] T. George, B. Bidulock, R. Dantu, H. Schwarzbauer, and K. Morneault, “Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Peer-to-Peer Adaptation Layer (M2PA),” *RFC 4165 [Online]* <http://www.ietf.org/rfc/rfc4165.txt>, 2005.
(Cited on page 20.)
- [68] K. Morneault, R. Dantu, G. Sidebottom, B. Bidulock, and J. Heitz, “Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Adaptation Layer,” *RFC 3331 [Online]* <http://www.ietf.org/rfc/rfc3331.txt>, 2002.
(Cited on page 20.)
- [69] K. Morneault and J. Pastor-Balbas, “Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA),” *RFC 4666 [Online]* <http://www.ietf.org/rfc/rfc4666.txt>, 2006.
(Cited on page 20.)
- [70] G. Sidebottom, K. Morneault, and J. Pastor-Balbas, “Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA),” *RFC 3332 [Online]* <http://www.ietf.org/rfc/rfc3332.txt>, 2002.
(Cited on page 20.)

-
- [71] R. Stewart, M. Ramalho, Q. Xie, M. Tuexen, and P. Conrad, “Stream Control Transmission Protocol (SCTP) Partial Reliability Extension,” *RFC 3758 [Online]* <http://www.ietf.org/rfc/rfc3758.txt>, 2004.
(Cited on pages 26 and 31.)
- [72] R. Stewart, Q. Xie, M. Tuexen, S. Maruyama, and M. Kozuka, “Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration,” *RFC 5061 [Online]* <http://www.ietf.org/rfc/rfc5061.txt>, 2007.
(Cited on pages 26, 57, and 99.)
- [73] G. Fairhurst and L. Wood, “Advice to link designers on link Automatic Repeat reQuest (ARQ),” *RFC 3366 [Online]* <http://www.ietf.org/rfc/rfc3366.txt>, 2002.
(Cited on page 26.)
- [74] K. J. Grinnemo, T. Andersson, and A. Brunstrom, “Performance benefits of avoiding head-of-line blocking in SCTP,” *Proceedings of Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services (ICAS/ICNS)*, pp. 271–278, 2005.
(Cited on page 26.)
- [75] J. Postel, “Transmission Control Protocol,” *RFC 793 [Online]* <http://www.ietf.org/rfc/rfc793.txt>, 1981.
(Cited on pages 29, 33, and 39.)
- [76] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow, “TCP Selective Acknowledgment Options,” *RFC 2018 [Online]* <http://www.ietf.org/rfc/rfc2018.txt>, 1996.
(Cited on page 29.)
- [77] P. Hurtig and A. Brunstrom, “Enhancing SCTP loss recovery: An experimental evaluation of early retransmit,” *Computer Communications*, vol. 31, no. 16, pp. 3778–3788, 2008.
(Cited on page 30.)
- [78] M. Scharf and S. Kiesel, “Head-of-line blocking in TCP and SCTP: Analysis and measurements,” *Proc. IEEE Globecom, San Francisco, CA, USA*, 2006.
-

(Cited on page 30.)

- [79] L. Ong, I. Rytina, M. Garcia, H. Schwarzbauer, L. Coene, H. Lin, I. Juhasz, M. Holdrege, and C. Sharp, “Framework Architecture for Signaling Transport,” *RFC 2719* [Online] <http://www.ietf.org/rfc/rfc2719.txt>, 1999.

(Cited on page 30.)

- [80] H. Schulzrinne, S. Gasner, R. Frederick, and V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications,” *RFC 1889* [Online] <http://www.ietf.org/rfc/rfc1889.txt>, 1996.

(Cited on page 32.)

- [81] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications,” *RFC 3550* [Online] <http://www.ietf.org/rfc/rfc2550.txt>, 2003.

(Cited on pages 32 and 33.)

- [82] J. Postel, “User Datagram Protocol,” *RFC 768* [Online] <http://www.ietf.org/rfc/rfc768.txt>, 1980.

(Cited on pages 33 and 39.)

- [83] J. Lazzaro, “Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport,” *RFC 4571* [Online] <http://www.ietf.org/rfc/rfc4571.txt>, 2006.

(Cited on page 33.)

- [84] E. Kohler, M. Handley, and S. Floyd, “Datagram Congestion Control Protocol (DCCP),” *RFC 4340* [Online] <http://www.ietf.org/rfc/rfc4340.txt>, 2006.

(Cited on page 33.)

- [85] C. Perkins, *RTP: Audio and Video for the Internet*. Addison-Wesley, 2006.

(Cited on page 33.)

- [86] H. Schulzrinne, A. Rao, and R. Lanphier, “Real Time Streaming Protocol (RTSP),” *RFC 2326* [Online] <http://www.ietf.org/rfc/rfc2326.txt>, 1998.

(Cited on page 34.)

- [87] J. Arkko, F. Lindholm, M. Naslund, K. Norrman, and E. Carrara, “Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP),” *RFC 4567 [Online]* <http://www.ietf.org/rfc/rfc4567.txt>, 2006.
(Cited on pages 34 and 39.)
- [88] H. Schulzrinne, “RTP Profile for Audio and Video Conferences with Minimal Control,” *RFC 1890 [Online]* <http://www.ietf.org/rfc/rfc1890.txt>, 1996.
(Cited on page 35.)
- [89] Y. Kikuchi, T. Nomura, S. Fukunaga, Y. Matsui, and H. Kimata, “RTP Payload Format for MPEG-4 Audio/Visual Streams,” *RFC 3016 [Online]* <http://www.ietf.org/rfc/rfc3016.txt>, 2002.
(Cited on page 35.)
- [90] I. Busse, B. Deffner, and H. Schulzrinne, “Dynamic QoS control of multimedia applications based on RTP,” *Computer Communications*, 1996.
(Cited on page 35.)
- [91] T. Schierl, T. Wiegand, and M. Kampmann, “3GPP compliant adaptive wireless video streaming using H. 264/AVC,” *Proceedings of the IEEE International Conference on Image Processing*, 2005.
(Cited on page 35.)
- [92] J. Postel, “Domain Name System Structure and Delegation,” *RFC 1591 [Online]* <http://www.ietf.org/rfc/rfc1591.txt>, 1994.
(Cited on page 35.)
- [93] P. V. Mockapetris, “Domain names - concepts and facilities,” *RFC 1034 [Online]* <http://www.ietf.org/rfc/rfc1034.txt>, 1987.
(Cited on page 35.)
- [94] A. Gulbrandsen and P. Vixie, “A DNS RR for specifying the location of services (DNS SRV),” *RFC 2782 [Online]* <http://www.ietf.org/rfc/rfc2782.txt>, 2005.
(Cited on page 36.)

- [95] M. Wahl, T. Howes, and S. Kille, “Lightweight Directory Access Protocol (v3),” *RFC 2251 [Online] <http://www.ietf.org/rfc/rfc2251.txt>*, 1997.
(Cited on page 38.)
- [96] M. Wahl, “A Summary of the X.500(96) User Schema for use with LDAPv3,” *RFC 2256 [Online] <http://www.ietf.org/rfc/rfc2256.txt>*, 1997.
(Cited on page 38.)
- [97] M. Smith and T. Howes, “Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator,” *RFC 4516 [Online] <http://www.ietf.org/rfc/rfc4516.txt>*, 2006.
(Cited on page 38.)
- [98] K. Zeilenga, “Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map,” *RFC 4510 [Online] <http://www.ietf.org/rfc/rfc4510.txt>*, 2006.
(Cited on page 38.)
- [99] K. Zeilenga and T. Howes, “Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names,” *RFC 4514 [Online] <http://www.ietf.org/rfc/rfc4514.txt>*, 2006.
(Cited on page 38.)
- [100] P. Faltstrom, “The E.164 to URI DDDS Application,” *[Online] <http://ietfreport.isoc.org/all-ids/draft-ietf-enum-rfc2916bis-07.txt>*, 2003.
(Cited on pages 42 and 93.)
- [101] T. Berners-Lee, R. Fielding, and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” *RFC 3986 [Online] <http://www.ietf.org/rfc/rfc3986.txt>*, 2005.
(Cited on pages 42 and 44.)
- [102] P. Faltstrom and M. Mealling, “The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM),” *RFC 3761 [Online] <http://www.ietf.org/rfc/rfc3761.txt>*, 2004.
(Cited on pages 42 and 45.)

- [103] P. Faltstrom, “E.164 number and DNS,” *RFC 2916 [Online]* <http://www.ietf.org/rfc/rfc2916.txt>, 2000.
(Cited on page 42.)
- [104] M. Mealling and R. Daniel, “The Naming Authority Pointer (NAPTR) DNS Resource Record,” *RFC 2915 [Online]* <http://www.ietf.org/rfc/rfc2915.txt>, 2000.
(Cited on pages 42 and 43.)
- [105] E. D. Crocker and P. Overell, “Augmented BNF for Syntax Specifications: ABNF,” *RFC 2234 [Online]* <http://www.ietf.org/rfc/rfc2234.txt>, 1997.
(Cited on page 44.)
- [106] M. Mealling, “Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database,” *RFC 3403 [Online]* <http://www.ietf.org/rfc/rfc3403.txt>, 2002.
(Cited on page 45.)
- [107] I. Akyildiz, J. Xie, and S. Mohanty, “A survey of mobility management in next-generation all-IP-based wireless systems,” *IEEE Wireless Communications*, vol. 11, no. 4, pp. 16–28, 2004.
(Cited on page 46.)
- [108] W. Dave, E. Philip, and B. Louise, “IP for 3G.” John Wiley & Sons Press, 2002, pp. 144–200.
(Cited on page 46.)
- [109] I. F. Akyildiz, J. McNair, J. S. M. Ho, H. Uzunalioglu, and W. Y. Wang, “Mobility management in next-generation wireless systems,” *Proceedings of the IEEE*, vol. 87, no. 8, pp. 1347–1384, 1999.
(Cited on page 46.)
- [110] M. Atiquzzaman and A. S. Reaz, “Survey and classification of transport layer mobility management schemes,” in *Proceedings of the 16th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (2005)*, vol. 4, 2005, pp. 2109–2115.

(Cited on page 46.)

- [111] B. Wellington, “Secure Domain Name System (DNS) Dynamic Update,” *RFC 3007 [Online]* <http://www.ietf.org/rfc/rfc3007.txt>, 2000.

(Cited on page 47.)

- [112] H. Schulzrinne and E. Wedlund, “Application-layer mobility using SIP,” *ACM SIG-MOBILE Mobile Computing and Communications Review*, vol. 4, no. 3, pp. 47–57, 2000.

(Cited on pages 50 and 56.)

- [113] C. Perkins and T. Jagannadh, “DHCP for mobile networking with TCP/IP,” *Proceedings of IEEE Symposium on Computers and Communications (ISCC’95)*, pp. 255–261, 1995.

(Cited on page 50.)

- [114] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, “Resource Records for the DNS Security Extensions,” *RFC 4034 [Online]* <http://www.ietf.org/rfc/rfc4034.txt>, 2005.

(Cited on page 50.)

- [115] C. Perkins, “IP Mobility Support for IPv4,” *RFC 3220 [Online]* <http://www.ietf.org/rfc/rfc3220.txt>, 2002.

(Cited on page 51.)

- [116] D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6,” *RFC 3375 [Online]* <http://www.ietf.org/rfc/rfc3375.txt>, 2004.

(Cited on page 51.)

- [117] J. Arkko, V. Devarapalli, and F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents,” *RFC 3776 [Online]* <http://www.ietf.org/rfc/rfc3776.txt>, 2004.

(Cited on page 51.)

-
- [118] N. Bonelli, S. Giordano, S. Lucetti, G. Risi, and A. Tomasi, “Automatic IPsec security association negotiation in mobile-oriented IPv6 networks,” *Proceedings of Symposium on Applications and the Internet Workshops*, pp. 14–17 474, 2005.
(Cited on page 53.)
- [119] N. Montavont and T. Noel, “Handover management for mobile nodes in IPv6 networks,” *IEEE Communications Magazine*, vol. 40, no. 8, pp. 38–43, 2002.
(Cited on pages 54 and 68.)
- [120] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier, “Hierarchical Mobile IPv6 Mobility Management (HMIPv6),” *RFC 4140 [Online]* <http://www.ietf.org/rfc/rfc4140.txt>, 2005.
(Cited on pages 54 and 55.)
- [121] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, “Hierarchical Mobile IPv6 (HMIPv6) Mobility Management,” *RFC 5380 [Online]* <http://www.ietf.org/rfc/rfc5380.txt>, 2008.
(Cited on pages 54 and 98.)
- [122] A. Jari, H. Peter, K. Gerben, S. Hesham, L. John, S. Pertti, and W. Juha, “Minimum IPv6 Functionality for a Cellular Host,” *[Online]* <http://ietfreport.isoc.org/all-ids/draft-ietf-ipv6-cellular-host-00.txt>, 2002.
(Cited on pages 54 and 55.)
- [123] H. C. Chao, Y. M. Chu, and M. T. Lin, “The implication of the next-generation wireless network design: Cellular Mobile IPv6,” *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 656–663, 2000.
(Cited on pages 54 and 98.)
- [124] N. Banerjee, K. Basu, and S. Das, “Hand-off delay analysis in SIP-based mobility management in wireless networks,” in *Proceedings of IEEE International Workshop on Wireless, Mobile Ad hoc Networks (WMAN’03), Nice, France*, 2003.
(Cited on page 56.)
-

- [125] N. Banerjee, S. K. Das, and A. Acharya, “SIP-based mobility architecture for next generation wireless networks,” *Proceedings of the third IEEE International Conference on Pervasive Computing and Communications*, pp. 181–190, 2005.
(Cited on page 56.)
- [126] N. Akhtar, M. Georgiades, C. Politis, and R. Tafazolli, “SIP-based End System Mobility Solution for All-IP Infrastructures,” *IST Mobile & Wireless Communications Summit 2003*, pp. 21–24, 2003.
(Cited on page 56.)
- [127] Y. W. Lin and T. H. Huang, “SIP-based handoff in 4G mobile networks,” *Proceedings of IEEE Wireless Communications & Networking Conference, Vols 1-9*, pp. 2808–2813 4472, 2007.
(Cited on page 56.)
- [128] W. Wu, N. Banerjee, K. Basu, and S. Das, “SIP-based vertical handoff between WWANs and WLANs,” *IEEE Wireless Communications*, vol. 12, no. 3, pp. 66–72, 2005.
(Cited on pages 56 and 67.)
- [129] E. Wedlund and H. Schulzrinne, “Mobility support using SIP,” in *Proceedings of the 2nd ACM international workshop on Wireless mobile multimedia*. ACM New York, NY, USA, 1999, pp. 76–82.
(Cited on page 56.)
- [130] M. Riegel and M. Tuexen, “Mobile SCTP,” *IETF Draft, draft-riegel-tuexen-mobile-sctp-05.txt*, 2005.
(Cited on page 57.)
- [131] S. H. Kwon, S. J. Koh, T. W. Um, and W. Ryu, “Mobile SCTP with Bicasting for Vertical Handover,” *Proceedings of the third 2008 International Conference on Convergence and Hybrid Information Technology, Vol 1*, pp. 123–125, 2008.
(Cited on pages 57 and 99.)

- [132] L. Ma, F. Yu, V. C. M. Leung, and T. S. Randhawa, "A new method to support UMTS/WLAN vertical handover using SCTP," *IEEE Wireless Communications*, vol. 11, no. 4, pp. 44–51, 2004.
(Cited on page 58.)
- [133] "Gtalk Web Site," [Online] <http://www.google.com/talk/>, 2009.
(Cited on page 59.)
- [134] "MSN messenger Web Site," [Online] <http://messenger.msn.com/>, 2009.
(Cited on page 59.)
- [135] X. Wang, S. Chen, and S. Jajodia, "Tracking anonymous peer-to-peer VoIP calls on the internet," in *Proceedings of the 12th ACM conference on Computer and communications security*. ACM New York, NY, USA, 2005, pp. 81–91.
(Cited on page 60.)
- [136] S. Skype Technologies, "Skype-Guide for Network Administrators," 2005.
(Cited on pages 60 and 61.)
- [137] D. Fabrice, "Skype uncovered," [Online] http://home.dei.polimi.it/giacomaz/courses/Telematica/materiale/Skype/EADS-CCR_Fabrice_Skype.pdf, 2005.
(Cited on page 60.)
- [138] S. A. Baset and H. G. Schulzrinne, "An analysis of the Skype peer-to-peer Internet telephony protocol," *Proceedings of 25th IEEE International Conference on Computer Communications, Vols 1-7, Proceedings Ieee Infocom 2006*, pp. 2695–2705 3337, 2006.
(Cited on pages 60 and 77.)
- [139] M. Perenyi, A. Gefferth, T. D. Dang, and S. Molnar, "Skype traffic identification," *Proceedings of IEEE Global Telecommunications Conference, Vols 1-11*, pp. 399–404 5378, 2007.
(Cited on page 60.)

-
- [140] Y. F. Yu, D. D. Liu, J. Li, and C. X. Shen, "Traffic identification and overlay measurement of Skype," *Proceedings of International Conference on Computational Intelligence and Security, Pts 1 and 2*, pp. 1043–1048 1868, 2006.
(Cited on page 60.)
- [141] K. Suh, D. R. Figueiredo, J. Kurose, and D. Towsley, "Characterizing and detecting Skype-relayed traffic," *Proceedings of 25th IEEE International Conference on Computer Communications, Vols 1-7*, pp. 2706–2717 3337, 2006.
(Cited on page 60.)
- [142] J. Li, S. Y. Zhang, Y. Xuan, and Y. F. Sun, "Identifying Skype Traffic by Random Forest," *Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing, Vols 1-15*, pp. 2841–2844 6743, 2007.
(Cited on page 60.)
- [143] B. Sat and B. W. Wah, "Analysis and evaluation of the Skype and Google-Talk VoIP systems," *Proceedings of IEEE International Conference on Multimedia and Expo - ICME 2006, Vols 1-5*, pp. 2153–2156 2188, 2006.
(Cited on page 60.)
- [144] D. Bonfiglio, M. Mellia, M. Meo, and D. Rossi, "Detailed Analysis of Skype Traffic," *IEEE Transactions on Multimedia*, vol. 11, no. 1, pp. 117–127, 2009.
(Cited on page 60.)
- [145] J. Li, S. Y. Zhang, Z. L. Zhang, and S. D. Liu, "Analyzing and Optimizing Skype Peer-to-Peer System," *Proceedings of IEEE International Conference on Wireless Communications, Networking and Mobile Computing, Vols 1-15*, pp. 2837–2840 6743, 2007.
(Cited on page 60.)
- [146] S. Das, E. Lee, K. Basu, and S. Sen, "Performance optimization of VoIP calls over wireless links using H. 323 protocol," *IEEE Transactions on Computers*, vol. 52, no. 6, pp. 742–752, 2003.
(Cited on page 62.)
-

-
- [147] J. Epstein, *Scalable Voip Mobility: Integration and Deployment*. Newnes, 2009.
(Cited on page 62.)
- [148] “The Focus project on 4G Mobile Network Architectures & Protocols,” WINLAB, Rutgers University, [Online] <http://www.winlab.rutgers.edu/pub/docs/focus/MobNet2.html>, 2008.
(Cited on page 64.)
- [149] G. Wu, M. Mizuno, and P. J. M. Havinga, “MIRAI architecture for heterogeneous network,” *IEEE Communications Magazine*, vol. 40, no. 2, pp. 126–134, 2002.
(Cited on page 64.)
- [150] M. Inoue, G. Wu, K. Mahmud, H. Murakami, and M. Hasegawa, “Development of MIRAI system for heterogeneous wireless networks,” *Proceedings of 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Vol 1-5, Proceedings*, pp. 69–73 2477, 2002.
(Cited on page 64.)
- [151] K. Mahmud, G. Wu, M. Inoue, and M. Mizuno, “Mobility management by basic access network in MIRAI architecture for heterogeneous wireless systems,” *IEEE Global Telecommunications Conference, Vols 1-3, Conference Records*, pp. 1708–1712 3003, 2002.
(Cited on page 65.)
- [152] T. Dagiuklas, D. Gatzounas, and C. Politis, “EVOLUTE Architecture Specification,” *IST Report on D1 EVOLUTE* [Online] http://www.mcl.hu/brozsas/cikkek/evolute/evolute_2_D021_v00.pdf, 2002.
(Cited on page 65.)
- [153] T. Dagiuklas, D. Gatzounas, D. Theofilatos, D. Sisalem, S. Rupp, R. Velentzas, R. Tafazolli, C. Politis, S. Grilli, and V. Kollias, “Seamless Multimedia Services Over All-IP Based Infrastructures: the EVOLUTE Approach,” *IST Mobile and Wireless Telecommunications Summit, Thessaloniki, Greece, June, 2002*.
(Cited on page 65.)
-

-
- [154] “DRiVE project,” [Online] <http://www.ist-drive.org>, 2005.
(Cited on page 65.)
- [155] G. Camarillo and M. Garcia-Martin, *The 3G IP multimedia subsystem (IMS): merging the Internet and the cellular worlds*. Wiley, 2004.
(Cited on page 66.)
- [156] 3GPP, “3GPP system to Wireless Local Area Network (WLAN) Interworking,” *Technical Specification 23.234 v6.3.0*, 2004.
(Cited on page 66.)
- [157] ETSI, “Requirements and architectures for interworking between HIPERLAN/3 and 3rd generation cellular systems,” *Technical Report TR 101 957*, 2001.
(Cited on page 66.)
- [158] K. Pahlavan, P. Krishnamurthy, A. Hatami, M. Ylianttila, J. P. Makela, R. Pichna, and J. Vallstron, “Handoff in hybrid mobile data networks,” *IEEE Personal Communications*, vol. 7, no. 2, pp. 34–47, 2000.
(Cited on page 66.)
- [159] R. Chakravorty, P. Vidales, K. Subramanian, I. Pratt, and J. Crowcroft, “Performance issues with vertical handovers - experiences from GPRS cellular and WLAN hot-spots integration,” in *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications(PerCom)*, 2004, pp. 155–164.
(Cited on pages 66 and 68.)
- [160] “Third Generation Partnership Project (3GPP2),” [Online] <http://www.3gpp2.org>, 2008.
(Cited on page 66.)
- [161] Y. Zhang and L. Yang, *Unlicensed Mobile Access Technology: Protocols, Architectures, Security, Standards and Applications*. AUERBACH, 2008.
(Cited on page 67.)

-
- [162] C. Yiping and Y. Yuhang, "A new 4G architecture providing multimode terminals always best connected services," *IEEE Wireless Communications*, vol. 14, no. 2, pp. 36–41, 2007.
(Cited on page 67.)
- [163] Q. Xie, "Mobility using IEEE 802.21 in a heterogeneous IEEE 802.16/802.11-based, IMT-advanced (4G) network," *IEEE Wireless Communications*, p. 27, 2008.
(Cited on page 67.)
- [164] S. Mohanty and I. Akyildiz, "Performance analysis of handoff techniques based on mobile IP, TCP-Migrate, and SIP," *IEEE Transactions on Mobile Computing*, vol. 6, no. 7, pp. 731–747, 2007.
(Cited on page 67.)
- [165] K. Sklower, B. Lloyd, G. McGregor, and D. Carr, "The PPP Multilink Protocol (MP)," *RFC 1990 [Online] <http://www.ietf.org/rfc/rfc1990.txt>*, 1996.
(Cited on page 67.)
- [166] D. S. Phatak and T. Goff, "A novel mechanism for data streaming across multiple IP links for improving throughput and reliability in mobile environments," in *Proceedings of IEEE Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 2, 2002, pp. 773–781.
(Cited on page 67.)
- [167] N. Banerjee, S. K. Das, and A. Acharya, "SIP-Based Mobility Architecture for Next Generation Wireless Networks," in *Proceedings of the third IEEE International Conference on Pervasive Computing and Communications(Percom)*, 2005, pp. 181–190.
(Cited on page 67.)
- [168] P. Nikander, "The Host Identity Protocol (HIP): Bringing mobility, multi-homing, and baseline security together," in *Proceedings of Third International Conference on Security and Privacy in Communications Networks and the Workshops*, 2007, pp. 518–519.
(Cited on page 68.)
-

-
- [169] P. Paakkonen, P. Salmela, R. Agüero, and J. Choque, "Performance analysis of HIP-based mobility and triggering," in *Proceedings of International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2008, pp. 1–9.
(Cited on page 68.)
- [170] T. Park and A. Dadej, "OPNET simulation modeling and analysis of enhanced Mobile IP," *2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003*, vol. 2, 2003.
(Cited on page 68.)
- [171] A. Misra, S. Das, A. Dutta, A. McAuley, S. Das, I. Center, and N. Hawthorne, "IDMP-based fast handoffs and paging in IP-based 4G mobile networks," *IEEE Communications Magazine*, vol. 40, no. 3, pp. 138–145, 2002.
(Cited on page 68.)
- [172] C. Hyun-Ho, O. Song, and C. Dong-Ho, "A seamless handoff scheme for UMTS-WLAN interworking," in *Proceedings in IEEE Global Telecommunications Conference (GLOBECOM)*, vol. 3, 2004, pp. 1559–1564.
(Cited on page 68.)
- [173] R. Kohn, "Transparent Mobility in Mobile IPv6: An Experience Report," *Journal of Computer Science & Technology, Sixteenth Issue: Special Issue on Selected Papers from CACIC*, 2005.
(Cited on page 68.)
- [174] A. Busaranun, P. Pongpaibool, and P. Supanakoon, "Handover Performance of Mobile IPv6 on Linux Testbed," in *Proceedings of International conference of Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI)*, 2006.
(Cited on page 68.)
- [175] C. Yang, R. Wang, and W. Liu, "Secure authentication scheme for session initiation protocol," *Computers & Security*, vol. 24, no. 5, pp. 381–386, 2005.
(Cited on page 75.)
-

- [176] S. Andersen, A. Duric, H. Astrom, R. Hagen, W. Kleijn, and J. Linden, “Internet low bit rate codec (iLBC),” *RFC 3951 [Online]* <http://www.ietf.org/rfc/rfc3951.txt>, 2004.
(Cited on page 77.)
- [177] “iSAC codec,” *[Online]* <http://www.globalipsound.com/datasheets/iSAC.pdf>, 2009.
(Cited on page 77.)
- [178] K. T. Chen, C. Y. Huang, P. Huang, and C. L. Lei, “Quantifying skype user satisfaction,” *Computer Communication Review*, vol. 36, no. 4, pp. 399–410, 2006.
(Cited on page 77.)
- [179] T. Berners-Lee, “Universal Resource Identifiers in WWW: A Unifying Syntax for the Expression of Names and Addresses of Objects on the Network as used in the World-Wide Web,” *RFC 1630 [Online]* <http://www.ietf.org/rfc/rfc1630.txt>, 1994.
(Cited on page 85.)
- [180] C. Adams and S. Farrell, “Internet X.509 Public Key Infrastructure Certificate Management Protocols,” *RFC 2510 [Online]* <http://www.ietf.org/rfc/rfc2510.txt>, 1999, obsoleted by RFC 4210.
(Cited on page 86.)
- [181] “Java Smartcard,” *[Online]* <http://java.sun.com/javacard/>, 2009.
(Cited on page 87.)
- [182] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, “Diameter Base Protocol,” *RFC 3588 [Online]* <http://www.ietf.org/rfc/rfc3588.txt>, 2003.
(Cited on page 93.)
- [183] J. Lennox, X. Wu, and H. Schulzrinne, “Call Processing Language (CPL): A Language for User Control of Internet Telephony Services,” *RFC 3880 [Online]* <http://www.ietf.org/rfc/rfc3880.txt>, 2004.
(Cited on pages 94 and 114.)

- [184] D. M. Jiang, R. Liscano, and L. Logrippo, "Personalization of internet telephony services for presence with SIP and extended CPL," *Computer Communications*, vol. 29, no. 18, pp. 3766–3779, 2006.
(Cited on page 94.)
- [185] "VoiceXML," [Online] <http://www.voicexml.org/>, 2006.
(Cited on pages 94 and 114.)
- [186] K. Singh, A. Nambi, and H. Schulzrinne, "Integrating VoiceXML with SIP services," *IEEE International Conference on Communications, Vols 1-5*, pp. 784–788 3634, 2003.
(Cited on page 94.)
- [187] S. Jinyang, J. Yuehui, G. Wei, C. Shiduan, H. Hui, and Z. Dajiang, "Performance evaluation of SCTP as a transport layer solution for wireless multi-access networks," in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, vol. 1, 2004, pp. 453–458.
(Cited on page 98.)
- [188] J. Shi, Y. Jin, H. Huang, and D. Zhang, "Experimental performance studies of SCTP in wireless access networks," in *Proceedings of IEEE International Conference on Communication Technology (ICCT'03)*, vol. 1, 2003, pp. 392–395.
(Cited on page 98.)
- [189] N. Banerjee, A. Acharya, and S. Das, "Seamless SIP-based mobility for multimedia applications," *IEEE Network*, vol. 20, no. 2, pp. 6–13, 2006.
(Cited on page 98.)
- [190] F. Siddiqui and S. Zeadally, "SCTP multihoming support for handoffs across heterogeneous networks," in *Communication Networks and Services Research Conference, 2006. CNSR 2006. Proceedings of the 4th Annual, 2006*, p. 8.
(Cited on page 98.)

- [191] M. Li, Y. Fei, V. C. M. Leung, and T. Randhawa, “A new method to support UMTS/WLAN vertical handover using SCTP,” *Wireless Communications, IEEE*, vol. 11, no. 4, pp. 44–51, 2004.
(Cited on page 99.)
- [192] A. Moloisane, I. Ganchev, and M. O’Droma, “Internet tomography in support of internet and network simulation and emulation modelling,” *Recent Advances in Modeling and Simulation Tools for Communication Networks and Services*, pp. 409–427 466, 2007.
(Cited on pages 112, 123, and 127.)
- [193] J. Smith, J. Meggelen, and L. Madsen, *Asterisk: The Future of Telephony*. O’Reilly Press, 2008.
(Cited on page 112.)
- [194] “Openser Web Site,” [Online] <http://www.openser.org/>, 2009.
(Cited on page 112.)
- [195] M. Jang and J. Woo, “GUI in VoiceXML,” *Proceedings of the 2005 International Conference on Human-Computer Interaction*, pp. 122–128 128, 2005.
(Cited on page 114.)
- [196] “PHP: Hypertext Preprocessor,” [Online] <http://www.php.org>, 2005.
(Cited on page 115.)
- [197] “J2EE,” [Online] <http://java.sun.com/javae/>, 2007.
(Cited on page 115.)
- [198] “Stream Control Transmission Protocol Library (SCTPLIB),” [Online] <http://www.sctp.de/sctp-download.html>, 2007.
(Cited on page 116.)
- [199] “Linux Kernel Stream Control Transmission Protocol (LKSTCP),” [Online] <http://lksctp.sourceforge.net/>, 2007.
(Cited on page 116.)

- [200] R. Steward, Q. Xie, L. H. P. Yarroll, J. Wood, K. Poon, and K. Fujita, "Sockets API extensions for Stream Control Transmission Protocol," *IETF Internet-Draft* [Online] <http://ietfreport.isoc.org/all-ids/draft-ietf-tsvwg-sctpsocket-04.txt>, 2002.
(Cited on page 116.)
- [201] C. Zhang and V. Tsoussidis, "TCP-real: improving real-time capabilities of TCP over heterogeneous networks," in *Proceedings of the 11th international workshop on Network and operating systems support for digital audio and video*. New York, United States: ACM, 2001, pp. 189–198.
(Cited on page 119.)
- [202] R. Steinmetz and K. Nahrstedt, *Media coding and content processing*. Prentice Hall PTR, Upper Saddle River, NJ, 2002.
(Cited on page 123.)
- [203] T. Braun, M. Diaz, J. Gabeiras, and T. Staub, *End-to-end quality of service over heterogeneous networks*. Springer-Verlag New York Inc, 2008.
(Cited on page 123.)
- [204] V. Ræisaenen, *Implementing service quality in IP networks*. John Wiley & Sons Inc, 2003.
(Cited on page 123.)
- [205] "MadWifi," [Online] <http://madwifi.org/>, 2007.
(Cited on page 127.)
- [206] R. Chakravorty, P. Vidales, K. Subramanian, I. Pratt, and J. Crowcroft, "Performance issues with vertical handovers - Experiences from GPRS cellular and WLAN hot-spots integration," *Proceedings of the second IEEE Annual Conference on Pervasive Computing and Communications*, pp. 155–164 372, 2004.
(Cited on page 127.)
- [207] A. Mercier, P. Minet, L. George, and G. Mercier, "Adequacy between multimedia application requirements and wireless protocols features," *IEEE Wireless Communications*, vol. 9, no. 6, pp. 26–34, 2002.

(Cited on page 127.)

- [208] L. Budzisz, R. Ferrus, A. Brunstrom, K. J. Grinnemo, R. Fracchia, G. Galante, and F. Casadevall, "Towards transport-layer mobility: Evolution of SCTP multihoming," *Computer Communications*, vol. 31, no. 5, pp. 980–998, 2008.

(Cited on page 127.)

- [209] S. Ehlert, S. Petgang, T. Magedanz, and D. Sisalem, "Analysis and signature of Skype VoIP session traffic," in *Proceedings of the 4th IASTED International Conference on Communications, Internet, and Information Technology*, 2006, pp. 83–89.

(Cited on page 127.)

- [210] "Wireshark," [Online] <http://www.wireshark.org/>, 2007.

(Cited on page 127.)

- [211] "Methods for subjective determination of transmission quality," *ITU-T Recommendation P.800*, 1996.

(Cited on page 142.)

- [212] ITU, "Perceptual evaluation of speech quality (PESQ): an objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs," *ITU-T Recommendation P.862*, 2001.

(Cited on page 142.)

- [213] K. Jirka, R. Berthold, and W. Adam, "Evalvid - A Framework for VideoTransmission and Quality Evaluation," in *Proceedings of the 13th International Conference onModelling Techniques and Tools for Computer Performance Evaluation CY - Urbana, Illinois, USA*, 2003.

(Cited on page 147.)

- [214] "YUV video sequences (CIF)," [Online] <http://www.tkn.tu-berlin.de/research/evalvid/cif.html>, 2007.

(Cited on page 147.)

- [215] “FFMPEG,” [Online] <http://ffmpeg.mplayerhq.hu/>, 2007.
(Cited on pages 147 and 203.)
- [216] A. G. Forte, S. Shin, and H. Schulzrinne, “Improving layer 3 handoff delay in IEEE 802.11 wireless networks,” in *Proceedings of the 2nd annual international workshop on Wireless internet*. ACM, 2006, p. 12.
(Cited on page 163.)
- [217] A. Majlesi and B. Khalaj, “An adaptive fuzzy logic based handoff algorithm for hybrid networks,” in *Proceedings of the 6th International Conference on Signal Processing*, vol. 2, 2002.
(Cited on page 164.)
- [218] J. Gross, J. Klaue, H. Karl, and A. Wolisz, “Cross-layer optimization of OFDM transmission systems for MPEG-4 video streaming,” *Computer Communications*, vol. 27, no. 11, pp. 1044–1055, 2004.
(Cited on page 205.)

Index

— Symbols —

3G, 1
3GPP, 68
3GPP2, 68
3P-AAA, 8
3P-AAA-SP, 8, 9, 82, 95
3P-AAAC, 95
802.11, 5

— A —

A record, 37
AAAA, 37, 45
AAAS, 95
ABC&S, 7, 166
ABNF, 45
ACK, 41
Ad-hoc, 66
ADA, 108
Add-IP, 58
ALPHA, 45
ANPs, 7
API, 121
ASCONF, 58
ASCONF-ACK, 58
Autoconfiguration, 21

— B —

BIND, 38
BYE, 41

— C —

CA, 82

CAI, 88
CANCEL, 41
CBM, 8
CBM-ICC, 8, 9, 76
CC, 35
CCM, 64
Cellular IPv6, 56
CIF, 152
CIM, 8, 89
CPL, 97, 119
CS, 1
CSCF, 68
CSRC, 35
CWND, 31, 124

— D —

DAD, 21
DAR, 58
DCH, 4
DDDS, 46
DDNS, 48
Delete-IP, 58
DHCP, 38
DHCPv6, 38
Diameter, 68
DNS, 36
DRiVE, 67

— E —

E-Mode, 82, 83, 109–111
E.164, 43

- E2U, 45
- EDGE, 4
- Ekiga, 10, 61
- ENUM, 43, 96
- ETSI, 68
- EVDO, 7
- EVOLUTE, 67
- F —
- FMC, 68
- Focus project, 66
- FORWARD, 32
- G —
- Gizmo, 10
- GPL, 117
- GPRS, 3
- GSM, 2
- Gtalk, 61
- GUI, 120
- H —
- H.323, 3
- HAC, 12, 99
- Handoff Management, 48
- HMIPv6, 56
- HSDPA, 4
- I —
- Ia, 96
- Ia*, 96
- Ic, 97
- ICC Data Service, 140
- ICC Video Service, 152
- ICC Voice Service, 147
- ICC-SE, 96, 120
- ICC-SP, 82, 94
- ICM, 95, 117
- Id, 98
- Ie, 99
- IETF, 4
- IMS, 68
- In, 99
- INIT, 32
- INIT ACK, 32
- INVITE, 41
- IP, 2, 5, 20
- IPv6, 18
- IPv6 personal address, 9, 86
- IS-95, 2
- ISM, 4
- ISP, 69
- IST, 67
- It, 99
- ITMS, 117
- J —
- J2EE, 120
- Jitter, 130
- L —
- LDAP, 39
- LKSCTP, 121
- Location Management, 48
- Location Server, 41

LTE, 4

— M —

MAC, 21

MIH, 69

MIPv6, 52

MIRAI, 66

MMC, 68

MMS, 2

MOS, 147

mSCTP, 58

MSN, 61

MT, 2

MT2, 105

MTU, 36

MU2, 105

Multi-homing, 29

Multi-streaming, 27

MUSE, 12

MYSQL, 120

— N —

NAPTR, 43

NAT, 120

— O —

OpenSER, 117

OPTION, 41

OWA, 69

— P —

Packet loss, 128

PCA, 95

PDA, 5

PDC, 2

Personal mobility, 47

PESQ, 147

PHP, 120

PHY, 4

PPP, 69

PR-SCTP, 31

Processing delay, 130

Propagation delay, 129

Proxy Server, 40

PSNR, 152

PSTNs, 1

PT, 35

— Q —

QoE, 3

QoS, 3

Queuing delay, 129

— R —

R-Mode, 82, 85, 110, 112

Redirect Server, 40

RegExp, 46

REGISTER, 41, 50

Registrar Server, 40

RR, 37

RTO, 30, 124

RTP, 33

RTSP, 35

— S —

SACK, 22, 30

- SBM, 8
- SBM-ICC, 74
- SCTP, 21
- SCTP PDU, 23
- SCTPLIB, 121
- SDP, 40
- Service mobility, 47
- Set-Primary-IP, 58
- Shunra, 116
- SIM, 8
- SIP, 40
- Skype, 10, 61
- SRV, 45
- SS, 35
- SSRC, 35
- SSTHRESH, 31, 124
- T —
- TCP/IP model, 19
- Terminal mobility, 47
- Throughput, 128
- Timestamp, 35
- Transmission delay, 129
- TSN, 22, 30
- TSP, 7
- TTL, 20, 32, 44
- U —
- UAC, 40
- UAS, 40
- UCWW, 7
- UMA, 69
- UMTS, 2
- URI, 41, 45
- URL, 39
- User-DB, 95
- V —
- VoiceXML, 97, 119
- VoIP, 6, 63
- W —
- WAN emulator, 116
- WBC, 8, 82
- WBC-SP, 82, 95
- Wi-Fi, 4
- Wi-Max, 5
- X —
- X.509, 89
- Y —
- Y'UV, 152

Appendices



A List of Relevant Author's Publications

Some ideas and figures have appeared previously in the following author's publications:

–International Journal

I. Ganchev, M. O'Droma, N. Wang. 2008. “Consumer-Oriented Incoming Call Connection Service for UCWW”. Springer journal “Wireless Personal Communications”, Volume 50, Number 1, Pp 115-131.

–Book Chapter

N. Wang, I. Ganchev, M. O'Droma. 2007. “Flexible Consumer-Controlled Incoming Call Connection Service Provision in UCWW,” In: Annual Review of Communications, Volume 60 (Chicago, Ill. : International Engineering Consortium), Pp. 637-647. ISBN: 978-1-931695-59-6.

–International Conference Proceedings

N. Wang, I. Ganchev, M. O'Droma. 2007. “An Architecture for the Provision of Incoming Call Connection Service in UCWW”. Proc. of the IEEE 65th Vehicular Technology Conference (VTC2007-Spring) on “Truly Ubiquitous Wireless Systems”, ISSN 1550-2252,

ISBN 1-4244-0266-2, IEEE Catalog 07CH37784C, Pp. 644-648, 22-25 April, Dublin, Ireland.

M. O'Droma., I. Ganchev, J. Jakab, Zh. Ji, N. Wang. 2008. "On Ubiquitous Consumer Wireless World – A Wireless Communications Environment for Future Wireless NGNs". Proc. of the Royal Irish Academy Research Colloquium on Emerging Trends in Wireless Communications, Pp. 6-9, 23-24 April, Dublin, Ireland. ISBN 9781-904890-45-4.

I. Ganchev, M. O'Droma, N. Wang. 2007. "On CBM-ICC Service Provision in UCWW". Proc. of the IEEE 4th International Symposium on Wireless Communication Systems (IEEE ISWCS'07). Pp. 128-132, 17-19 October, Trondheim, Norway. ISBN 1-4244-0979-9.

M. O'Droma, I. Ganchev, J. Jakab, Zh. Ji, N. Wang. 2007. "Protocol Foundations for ABC&S Paradigm Realisation in a Ubiquitous Consumer Wireless World." Science Foundation Ireland Summit. Pp. 26-27 Nov. Dublin; Also Book of Abstracts.

M. O'Droma, I. Ganchev, N. Wang. 2006. "On Incoming Call Connection Service in a Ubiquitous Consumer Wireless World," In: Next Generation Teletraffic and Wired/Wireless Advanced Networking, Lecture Notes in Computer Science (LNCS), vol. 4003, Springer-Verlag Berlin Heidelberg, Germany. Pp. 287-297. Eds. Y. Koucheryavy, J. Harju, V. Iversen, XVI, ISBN 3-540-34429-2.

B

MPEG-4

The MPEG (Moving Picture Experts Group) is a working group of the International Organization for Standards (ISO). MPEG-4 was standardized by this group for video conferencing, Internet distribution and similar applications using low bandwidth. The MPEG-4 standard offers a set of technologies to encode/decode audio and visual digital data.

A MPEG-4 movie consists of a complete image sequence, possibly of hundreds or thousands of frames. These frames are grouped into GOP (Group of Pictures), The GOP contains a small number of frames (typically 12) coded to ensure that they can be decoded completely as a unit, without reference to frames outside of the group.

MPEG-4 typically uses three types of frames. I-frames (intra-coded frames) are intra-frames that are encoded independently of other types of frames. P-frames (predictive-coded frames) are encoded with the differences from the preceding I-frame or P-frame. B-frames (bi-directionally predictive-coded frames) are encoded based on preceding and succeeding I-frame and P-frame.

- *I-frames* are the key frames which are encoded without reference to any other frame in the sequence. I-frames allow video to be played from random positions and for fast forward/reverse. The decoding of a video starts from an I-frame, which are inserted every 12 to 15 frames.

-
- *P-frames* use Motion Prediction to predict the values of each new pixel based on preceding I- or P-frames. The differences between the predicted and actual values are encoded. As a result the P-frames provide a better compression ratio than the I-frames but depending on the amount of motion present.
 - *B-frames* use prediction as for the P-frames but depend on both the previous or next I or P frame. B-frames improve compression ratio compared with the P-frames, because it is possible to choose for more macro block which is taken from the previous or the next frame.

Some of consecutive I-, P-, and B-frames consist of Group of Video Object Planes (VOPs) that is the basic building block for the video stream. VOP represents an arbitrary-shaped object plane as shown in Figure B.1. Since a video frame is encoded by a VOP with a rectangular shape, MPEG-4 video stream can be regarded as a sequence of frames. Typical VOP in MPEG-4 encoding specification is IPBBPBBP or IBPBPBPBP. The former is more difficult to encode but provides a higher compression ratio than the latter. According to encoding dependencies, I-frames are key to the play-out quality of the video. Transmission or congestion losses of I-frames give a greater degradation on the quality of the video data than the other frames.

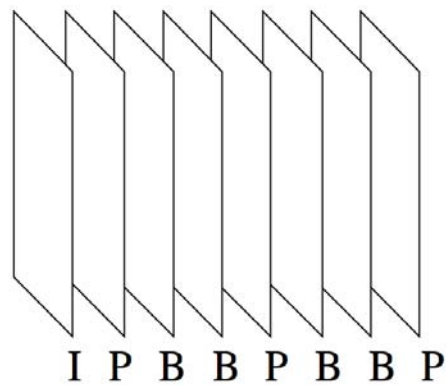


Figure B.1.: A Video Object Plane (VoP) in MPEG-4.



Evalvid Video Evaluation Framework

Evalvid is a comprehensive framework and tool-set employed to evaluate the quality of video transported over a real or simulated communication network [10]. The Evalvid framework contains a video encoder, video sender, network simulator, video decoder, evaluate trace application, fix video application, Peak Signal-to-Noise Ratio (PSNR) program and Mean Opinion Score (MOS) program.

As shown in Figure C.1, a raw video file in Y'UV⁴⁵ format is used as the source to the Evalvid framework. A video encoder encodes this raw video file into a format suitable for streaming. In this research, the FFmpeg [215] video encoder was used to encode a raw Y'UV file into MPEG4 format. The encoded video file is read by the video sender and send over a SCTP socket which generates the video and sender trace file. It is essential to extend the SCTP socket with a HAC support. The receiver trace file is generated at the receiver side. Three trace files were required to evaluate the quality of the video received by the end-user. The video, sender and receiver trace files are passed to the Evaluate Trace (ET) application which generates a possibly corrupt video file. The generated video file

⁴⁵ The Y'UV is a raw color video standard defined a color space in terms of one luma (Y') and two chrominance (UV) components. The Y'UV color model is widely used in the NTSC, PAL, and SECAM.

is in the encoded MPEG4 format. The fix video application then decodes the generated video file back into raw Y'UV format. The decoder used for this purpose was provided by the FFmpeg application. By using the PSNR and MOS programs the end-to-end video quality can be evaluated. Additional results are generated which include jitter, delay, and receive rates.

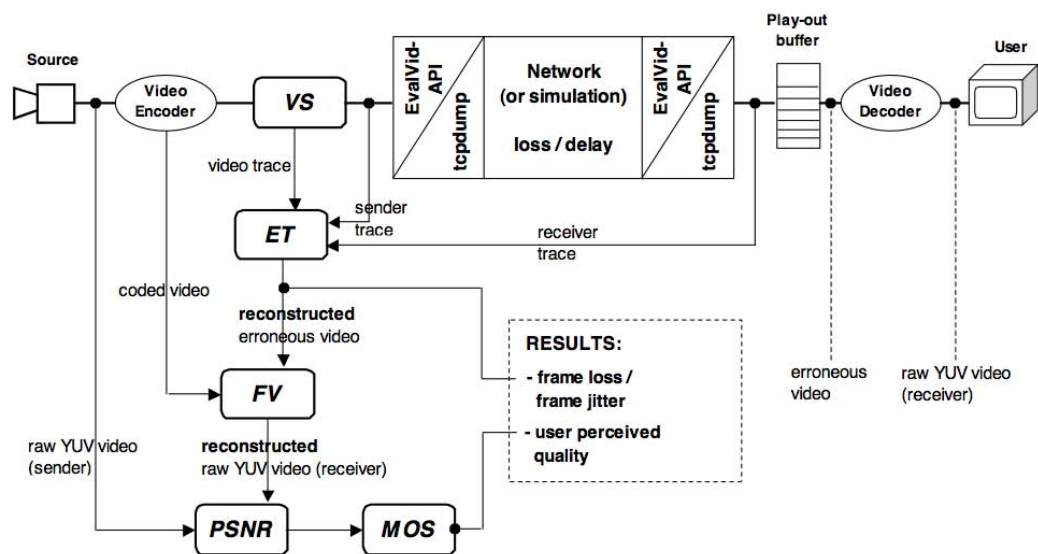


Figure C.1.: The video evaluation framework scheme (Source:[10]).

D

Peak Signal-to-Noise Ratio (PSNR)

According to [218], "video quality measurements must be based on the perceived quality of the actual video being received by the users of the digital video system." In other words, a real test of video quality can only be performed when a person looks at the video and provides a rating based on his/her subjective opinion.

PSNR [10] is a rating tools used to compare the peak signal energy to noise energy of video components on a frame-by-frame basis. PSNR is mainly derived from the Mean Square Error (MSE). MSE is often based only on the luminance component of the video due to the greater effect that the Y component has on a video image. Formula D.1 illustrates how the source and destination luminance components are used to define the MSE between the source image (I) and destination image (K). PSNR is defined in D.2 where MAX states that the maximum image point, e.g., if each sampling point is 8 bits, MAX is 255.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \|I(i, j) - K(i, j)\|^2 \quad (D.1)$$

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \quad (D.2)$$

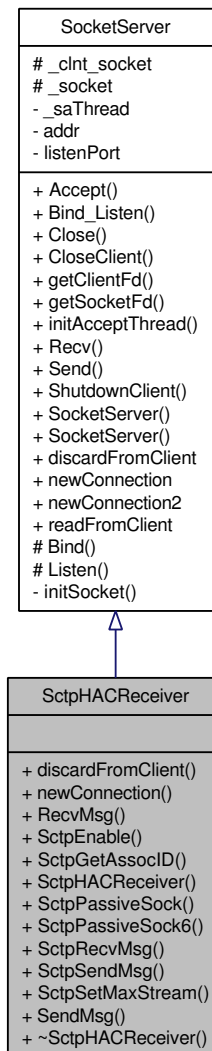


Code Reference

This appendix provides some background information for developers interested in writing applications for the CBM-ICC service. We have implemented two new classes for a SCTP-based HAC, namely the `SctpHACSender` and `SctpHACReceiver`. The key API change required is when the sender is initiating a new connection, where the application uses a mechanism for adding multiple destination addresses, and changing the primary address. There are minimal changes from the original SCTP API. For this reason, the original SCTP API guide should be consulted. This section provides the pseudocode for those parts of the HAC stack that have been modified.

E.1 SctpHACReceiver Class Reference

Inheritance diagram for SctpHACReceiver:

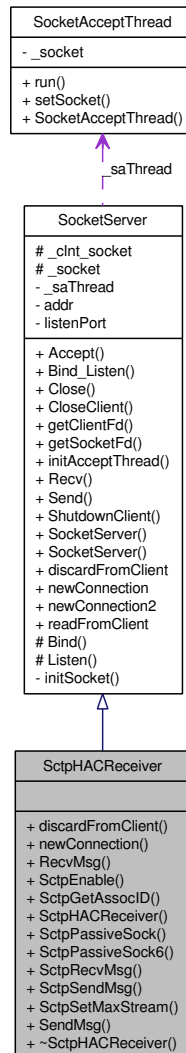


Collaboration diagram for SctpHACReceiver:

Signals

- void newConnectSCTP (int)

E.1 SctpHACReceiver Class Reference



Public Member Functions

- virtual void discardFromClient ()
- virtual void newConnection (int)

SctpHACReceiver new connection.

- int RecvMsg (int skt, char *msg)

SctpHACReceiver receive message.

E.1 SctpHACReceiver Class Reference

- `int SctpEnable ()`
SctpHACReceiver enable the SCTP by setsockopt.
- `int SctpGetAssocID ()`
SctpHACReceiver set the accociation number.
- `SctpHACReceiver ()`
SctpHACReceiver constructor.
- `int SctpPassiveSock (unsigned short int portnumber)`
SctpHACReceiver set a new socket and listen for IPv4.
- `int SctpPassiveSock6 (unsigned short int portnumber)`
SctpHACReceiver set a new socket and listen for IPv6.
- `int SctpRecvMsg (mPacket &p, int &str_num, int sock=-1)`
SctpHACReceiver receive message.
- `int SctpSendMsg (mPacket &p, int str_num=0, int sock=-1)`
SctpHACReceiver send message.
- `int SctpSetMaxStream (int num)`
SctpHACReceiver set maximum streams.
- `int SendMsg (int skt, char *msg)`
SctpHACReceiver send messge.

- virtual `~SctpHACReceiver ()`

E.1.1. Constructor & Destructor Documentation

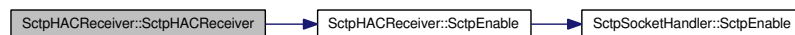
E.1.1.1. `SctpHACReceiver::SctpHACReceiver ()`

SctpHACReceiver constructor.

Definition at line 14 of file SctpHACReceiver.cpp.

References `SctpEnable()`.

Here is the call graph for this function:



E.1.1.2. `virtual SctpHACReceiver::~~SctpHACReceiver ()` [virtual]

E.1.2. Member Function Documentation

E.1.2.1. `virtual void SctpHACReceiver::discardFromClient ()` [virtual]

Reimplemented from `SocketServer`.

E.1.2.2. `void SctpHACReceiver::newConnection (int sock)` [virtual]

SctpHACReceiver new connection.

Reimplemented from `SocketServer`.

Definition at line 98 of file SctpHACReceiver.cpp.

References `newConnectSCTP()`.

E.1.2.3. void SctpHACReceiver::newConnectSCTP (int) [signal]

Referenced by newConnection().

E.1.2.4. int SctpHACReceiver::RecvMsg (int *skt*, char * *msg*)

SctpHACReceiver receive message.

Definition at line 201 of file SctpHACReceiver.cpp.

E.1.2.5. int SctpHACReceiver::SctpEnable ()

SctpHACReceiver enable the SCTP by setsockopt.

Definition at line 45 of file SctpHACReceiver.cpp.

References SocketServer::_socket, and SctpSocketHandler::SctpEnable().

Referenced by SctpHACReceiver().

Here is the call graph for this function:



Here is the caller graph for this function:



E.1.2.6. int SctpHACReceiver::SctpGetAssocID ()

SctpHACReceiver set the association number.

Definition at line 38 of file SctpHACReceiver.cpp.

References SocketServer::_socket, and SctpSocketHandler::SctpGetAssocID().

Here is the call graph for this function:



E.1.2.7. `int SctpHACReceiver::SctpPassiveSock (unsigned short int portnumber)`

SctpHACReceiver set a new socket and listen for IPv4.

setting

1. create SCTP socket
2. bind the address
3. Listen

Definition at line 107 of file SctpHACReceiver.cpp.

E.1.2.8. `int SctpHACReceiver::SctpPassiveSock6 (unsigned short int portnumber)`

SctpHACReceiver set a new socket and listen for IPv6.

setting

Definition at line 155 of file SctpHACReceiver.cpp.

E.1.2.9. `int SctpHACReceiver::SctpRecvMsg (mPacket & p, int & str_num, int sock = -1)`

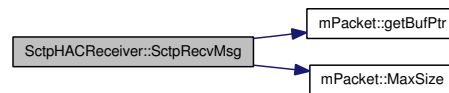
SctpHACReceiver receive message.

Definition at line 78 of file SctpHACReceiver.cpp.

References SocketServer::_socket, mPacket::getBufPtr(), and mPacket::MaxSize().

E.1 SctpHACReceiver Class Reference

Here is the call graph for this function:



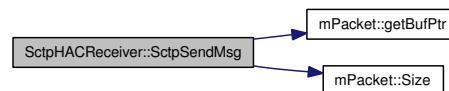
E.1.2.10. `int SctpHACReceiver::SctpSendMsg (mPacket & p, int str_num = 0, int sock = -1)`

SctpHACReceiver send message.

Definition at line 62 of file SctpHACReceiver.cpp.

References SocketServer::_socket, mPacket::getBufPtr(), and mPacket::Size().

Here is the call graph for this function:



E.1.2.11. `int SctpHACReceiver::SctpSetMaxStream (int num)`

SctpHACReceiver set maximum streams.

Definition at line 21 of file SctpHACReceiver.cpp.

References SocketServer::_socket, and SctpSocketHandler::SctpSetMaxStream().

Here is the call graph for this function:

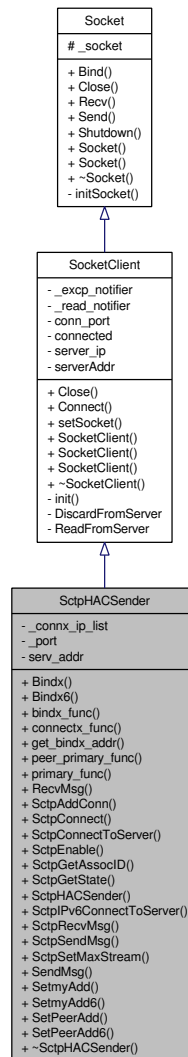


E.1.2.12. `int SctpHACReceiver::SendMsg (int skt, char * msg)`

SctpHACReceiver send message.

E.2 SctpHACSender Class Reference

Inheritance diagram for SctpHACSender: Collaboration diagram for SctpHACSender:

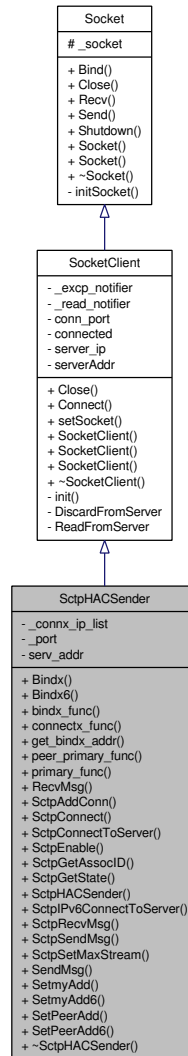


Public Member Functions

- int Bindx (int sk, char *ip, int port)

Dynamiclly add address using IPv4.

E.2 SctpHACSender Class Reference



- int Bindx6 (int sk, char *ip, int port)

Dynamiclly add address using IPv6.

- int bindx_func (char *argv0, int sk, struct sockaddr *addrs, int count, int flag)

generic bindx function

- int connectx_func (char *argv0, int sk, struct sockaddr *addrs, int count)
- struct sockaddr * get_bindx_addr (char *in, int *count)

- void peer_primary_func (char *argv0, int sk, char *cp, int set)

generic set peer address function

- void primary_func (char *argv0, int sk, char *cp, int set)

generic set primary address function

- int RecvMsg (int skt, char *msg)

Receive message.

- int SctpAddConn (QString &, int)

Addition of the IP address to the IP list.

- int SctpConnect ()

Connect to remote receiver.

- int SctpConnectToServer (QString &ip, int port)

Connect to mutiple servers.

- int SctpEnable ()

Enable receipt of SCTP Snd/Rcv Data via sctp_recvmsg.

- int SctpGetAssocID ()

Use the getsockopt to get the accociation number.

- int SctpGetState ()

Use the getsockopt to get the accociation statues.

- SctpHACSender ()
SctpHACSender Constructor.
- int SctpIPv6ConnectToServer (QString &ip, int port)
Connect to remote receiver forcing use IPv6 method.
- int SctpRecvMsg (mPacket &p, int &str_num, int sock=-1)
Receive the SCTP message.
- int SctpSendMsg (mPacket &p, int str_num=0, int sock=-1)
Send the SCTP message.
- int SctpSetMaxStream (int num)
Set the Maximum Streams.
- int SendMsg (int skt, char *msg)
Sending message.
- int SetmyAdd (int sk, char *ip, int port)
Dynamiclly set the primary address using IPv4.
- int SetmyAdd6 (int sk, char *ip, int port)
- int SetPeerAdd (int sk, char *ip, int port)
Dynamiclly set the peer primary address using IPv4.
- int SetPeerAdd6 (int sk, char *ip, int port)
Dynamiclly set the peer primary address using IPv6.

- virtual `~SctpHACSender ()`

SctpHACSender Destructor.

Private Attributes

- `QStrList _connx_ip_list`
- `int _port`
- `struct sockaddr_in6 serv_addr`

E.2.1. Constructor & Destructor Documentation

E.2.1.1. `SctpHACSender::SctpHACSender ()`

SctpHACSender Constructor.

Definition at line 14 of file SctpHACSender.cpp.

References SctpEnable().

Here is the call graph for this function:



E.2.1.2. `SctpHACSender::~~SctpHACSender ()` [virtual]

SctpHACSender Destructor.

Definition at line 21 of file SctpHACSender.cpp.

E.2.2. Member Function Documentation

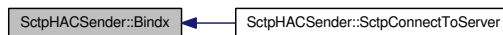
E.2.2.1. `int SctpHACSender::Bindx (int sk, char * ip, int port)`

Dynamically add address using IPv4.

Definition at line 313 of file SctpHACSender.cpp.

Referenced by SctpConnectToServer().

Here is the caller graph for this function:



E.2.2.2. `int SctpHACSender::Bindx6 (int sk, char * ip, int port)`

Dynamically add address using IPv6.

Definition at line 385 of file SctpHACSender.cpp.

E.2.2.3. `int SctpHACSender::bindx_func (char * argv0, int sk, struct sockaddr * addrs, int count, int flag)`

generic bindx function

Definition at line 433 of file SctpHACSender.cpp.

E.2.2.4. `int SctpHACSender::connectx_func (char * argv0, int sk, struct sockaddr * addrs, int count)`

Definition at line 519 of file SctpHACSender.cpp.

E.2.2.5. struct sockaddr* SctpHACSender::get_bindx_addr (char * *in*, int * *count*) [read]

E.2.2.6. void SctpHACSender::peer_primary_func (char * *argv0*, int *sk*, char * *cp*, int *set*)

generic set peer address function

Definition at line 649 of file SctpHACSender.cpp.

E.2.2.7. void SctpHACSender::primary_func (char * *argv0*, int *sk*, char * *cp*, int *set*)

generic set primary address function

Definition at line 573 of file SctpHACSender.cpp.

E.2.2.8. int SctpHACSender::RecvMsg (int *skt*, char * *msg*)

Receive message.

Definition at line 275 of file SctpHACSender.cpp.

E.2.2.9. int SctpHACSender::SctpAddConn (QString & *ip*, int *port*)

Addition of the IP address to the IP list.

Definition at line 126 of file SctpHACSender.cpp.

References `_connx_ip_list`, and `_port`.

E.2.2.10. int SctpHACSender::SctpConnect ()

Connect to remote receiver.

Definition at line 147 of file SctpHACSender.cpp.

E.2 SctpHACSender Class Reference

References `_connx_ip_list`, `_port`, `Socket::_socket`, and `SocketClient::setSocket()`.

Here is the call graph for this function:



E.2.2.11. `int SctpHACSender::SctpConnectToServer (QString & ip, int port)`

Connect to multiple servers.

Enable receipt of SCTP Snd/Rcv Data via `sctp_recvmsg`

Definition at line 211 of file `SctpHACSender.cpp`.

References `_connx_ip_list`, and `Bindx()`.

Here is the call graph for this function:



E.2.2.12. `int SctpHACSender::SctpEnable ()`

Enable receipt of SCTP Snd/Rcv Data via `sctp_recvmsg`.

Definition at line 76 of file `SctpHACSender.cpp`.

References `Socket::_socket`.

Referenced by `SctpHACSender()`.

Here is the caller graph for this function:



E.2.2.13. `int SctpHACSender::SctpGetAssocID ()`

Use the `getsockopt` to get the accociation number.

Definition at line 46 of file `SctpHACSender.cpp`.

References `Socket::_socket`.

E.2.2.14. `int SctpHACSender::SctpGetState ()`

Use the `getsockopt` to get the accociation statues.

Definition at line 60 of file `SctpHACSender.cpp`.

References `Socket::_socket`.

E.2.2.15. `int SctpHACSender::SctpIPv6ConnectToServer (QString & ip, int port)`

Connect to remote receiver forcing use IPv6 method.

Definition at line 181 of file `SctpHACSender.cpp`.

References `serv_addr`.

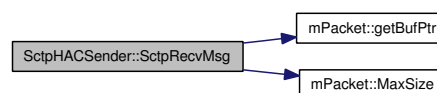
E.2.2.16. `int SctpHACSender::SctpRecvMsg (mPacket & p, int & str_num, int sock = -1)`

Receive the SCTP message.

Definition at line 107 of file `SctpHACSender.cpp`.

References `Socket::_socket`, `mPacket::getBufPtr()`, and `mPacket::MaxSize()`.

Here is the call graph for this function:



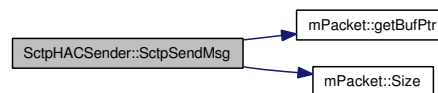
E.2.2.17. `int SctpHACSender::SctpSendMsg (mPacket & p, int str_num = 0, int sock = -1)`

Send the SCTP message.

Definition at line 92 of file SctpHACSender.cpp.

References Socket::_socket, mPacket::getBufPtr(), and mPacket::Size().

Here is the call graph for this function:



E.2.2.18. `int SctpHACSender::SctpSetMaxStream (int num)`

Set the Maximum Streams.

Definition at line 29 of file SctpHACSender.cpp.

References Socket::_socket.

E.2.2.19. `int SctpHACSender::SendMsg (int skt, char * msg)`

Sending message.

Definition at line 283 of file SctpHACSender.cpp.

E.2.2.20. `int SctpHACSender::SetmyAdd (int sk, char * ip, int port)`

Dynamically set the primary address using IPv4.

Dynamically set the primary address using IPv6.

Definition at line 334 of file SctpHACSender.cpp.

E.2.2.21. int SctpHACSender::SetmyAdd6 (int *sk*, char * *ip*, int *port*)

E.2.2.22. int SctpHACSender::SetPeerAdd (int *sk*, char * *ip*, int *port*)

Dynamically set the peer primary address using IPv4.

Definition at line 290 of file SctpHACSender.cpp.

E.2.2.23. int SctpHACSender::SetPeerAdd6 (int *sk*, char * *ip*, int *port*)

Dynamically set the peer primary address using IPv6.

Definition at line 360 of file SctpHACSender.cpp.

E.2.3. Member Data Documentation

E.2.3.1. QList SctpHACSender::_connx_ip_list [private]

Definition at line 62 of file SctpHACSender.h.

Referenced by SctpAddConn(), SctpConnect(), and SctpConnectToServer().

E.2.3.2. int SctpHACSender::_port [private]

Definition at line 63 of file SctpHACSender.h.

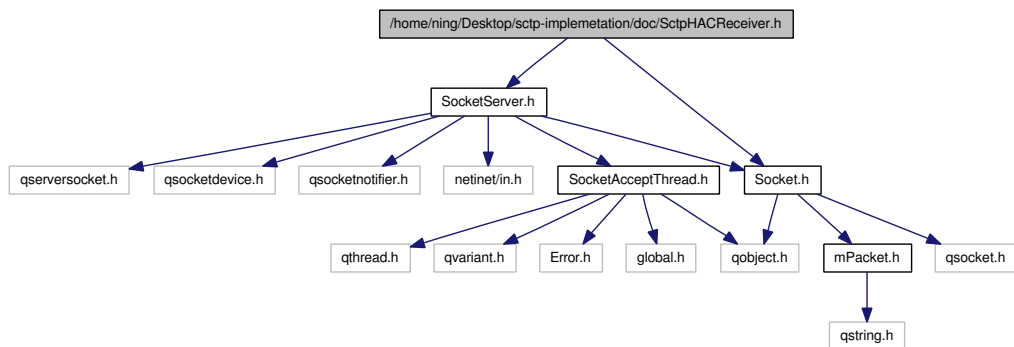
Referenced by SctpAddConn(), and SctpConnect().

E.2.3.3. struct sockaddr_in6 SctpHACSender::serv_addr [read, private]

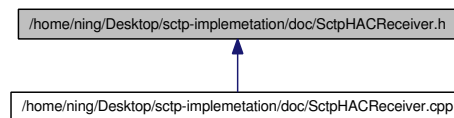
E.3 Dependency Graph

SctpHACReceiver.h File Reference

Include dependency graph for SctpHACReceiver.h:



This graph shows which files directly or indirectly include this file:



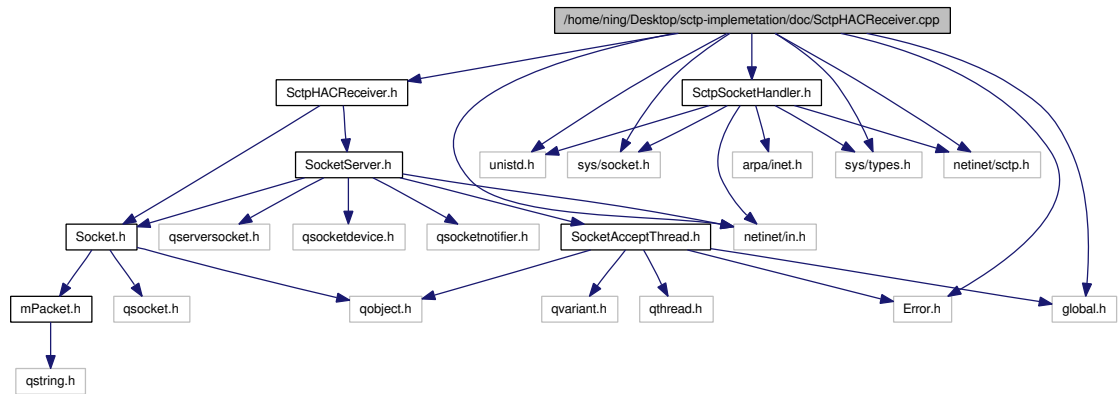
Classes

- class SctpHACReceiver

SctpHACReceiver.cpp File Reference

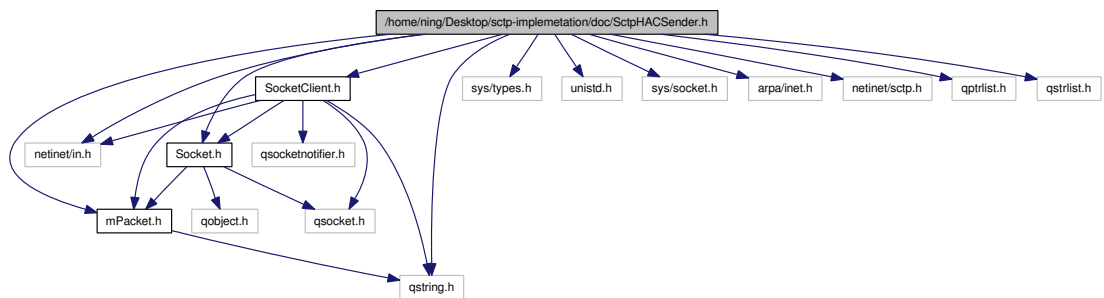
E.3 Dependency Graph

Include dependency graph for SctpHACReceiver.cpp:

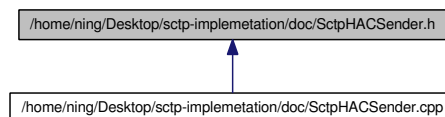


SctpHACSender.h File Reference

Include dependency graph for SctpHACSender.h:



This graph shows which files directly or indirectly include this file:

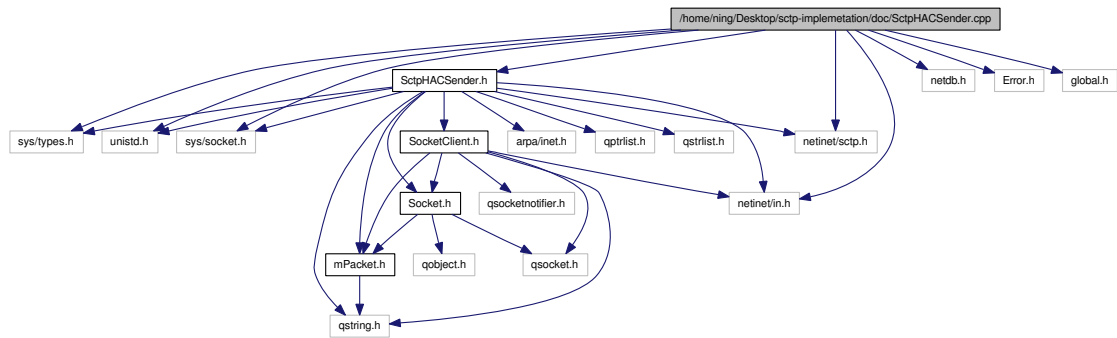


Classes

- class SctpHACSender

SctpHACSender.cpp File Reference

Include dependency graph for SctpHACSender.cpp:



Defines

- `#define _SOCKET_SCTP_CLIENT_H`

Functions

- `struct SctpHACSender::sockaddr * get_bindx_addr (char *in, int *count)`

generic get bindx address function

E.3.1. Define Documentation

E.3.1.1. `#define _SOCKET_SCTP_CLIENT_H`

Definition at line 69 of file `SctpHACSender.h`.

E.3.2. Function Documentation

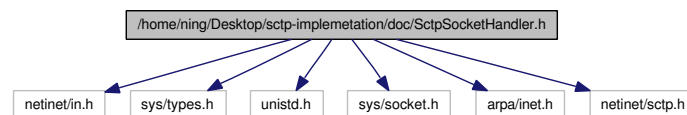
E.3.2.1. `struct SctpHACSender::sockaddr* get_bindx_addr (char * in, int * count)` [read]

generic get bindx address function

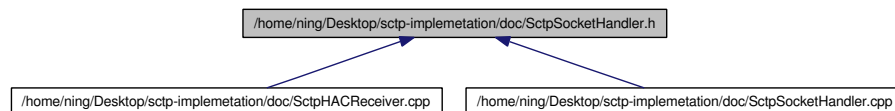
Definition at line 492 of file SctpHACSender.cpp.

SctpSocketHandler.h File Reference

Include dependency graph for SctpSocketHandler.h:



This graph shows which files directly or indirectly include this file:



Classes

- class SctpSocketHandler

SctpSocketHandler.

SctpSocketHandler.cpp File Reference

E.3 Dependency Graph

Include dependency graph for SctpSocketHandler.cpp:

