

UMTS NETWORKS AND BEYOND

Cornelia Kappler

deZem GmbH, Germany



WILEY

A John Wiley and Sons, Ltd, Publication

UMTS NETWORKS AND BEYOND

UMTS NETWORKS AND BEYOND

Cornelia Kappler

deZem GmbH, Germany



WILEY

A John Wiley and Sons, Ltd, Publication

This edition first published 2009
© 2009 John Wiley & Sons, Ltd

Registered office

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Library of Congress Cataloging-in-Publication Data

Kappler, Cornelia.

UMTS networks and beyond / Cornelia Kappler.

p. cm.

Includes bibliographical references and index.

ISBN 978-0-470-03190-2 (cloth)

1. Universal Mobile Telecommunications System. I. Title.

TK5103.4883.K36 2009

621.3845'6-dc22

2008041818

A catalogue record for this book is available from the British Library.

ISBN 9780470031902 (H/B)

Typeset in 10/12pt Times by Thomson Digital, Noida, India.

Printed in TJ International Ltd, Padstow, Cornwall.

Contents

Preface	xv
Acknowledgement	xxi
About the Author	xxiii
Acronyms	xxv
Part I UMTS Networks	
1 Introduction	3
1.1 Mobile Telecommunication Networks and Computer Networks	4
1.2 Network Design Principles and Business Models	5
1.2.1 Business Models	5
1.2.2 The Cathedral and the Bazaar	5
1.2.3 Operator Control and User Control	6
1.2.4 In the Beginning is the Architecture and In the Beginning is the Protocol	7
1.2.5 Convergence	8
1.3 Summary	8
2 UMTS Motivation and Context	11
2.1 The Evolution of the Mobile Telecommunication Market	12
2.1.1 Overall Market Evolution	12
2.1.2 Service Evolution	14
2.2 The Evolution of Mobile Telecommunication Technology	15
2.3 The Genesis of UMTS	17
2.3.1 UMTS Services	18
2.3.2 UMTS Technical Requirements	19
2.4 Comparison of UMTS with Other Mobile Technologies	21
2.4.1 WLAN	21
2.4.2 Other Mobile Technologies	21
2.5 Summary	24
3 Standardization	25
3.1 The Importance of Standardization	26
3.2 Standardization Bodies	27
3.2.1 ITU	27

3.2.2	3GPP	27
3.2.3	3GPP2	29
3.2.4	IETF	29
3.2.5	IEEE	30
3.3	Summary	31
4	UMTS Architecture and Functionality	33
4.1	Overview of Telecommunication Network Architecture	34
4.1.1	Overview of Mobile Network Functionality	34
4.1.2	User-Plane, Control-Plane and Management Plane	35
4.2	High-Level Architecture of 3G Networks	36
4.3	GSM Architecture	37
4.4	GPRS Architecture	38
4.4.1	PS Domain and CS Domain	39
4.5	UMTS Architecture	39
4.5.1	IMS	40
4.6	3GPP System Architecture	40
4.7	WLAN Architecture	41
4.8	Summary	42
5	UMTS Radio Interface Technology—the Physical Layer	45
5.1	Information Coding	46
5.2	Sharing the Electromagnetic Spectrum	49
5.2.1	Frequency Division	49
5.2.2	Time Division	50
5.2.3	Space Division	50
5.2.4	Code Division	51
5.2.4.1	The Near-Far Effect	52
5.2.4.2	Macrodiversity	53
5.2.4.3	Channelization Code and Scrambling Code	54
5.2.5	Advanced Division Techniques	55
5.2.5.1	Orthogonal Frequency Division Multiple Access	55
5.2.5.2	Single-Carrier Frequency Division Multiplex Access	56
5.3	Summary	57
6	Packet-switched Domain—Architecture and Protocols	59
6.1	Architecture	60
6.1.1	Serving GPRS Support Node (SGSN)	61
6.1.2	Gateway GPRS Support Node (GGSN)	62
6.1.3	Home Location Register (HLR)	62
6.2	Protocols	62
6.2.1	User-Plane	62
6.2.2	Control-Plane	64
6.2.3	Discussion	65
6.3	Summary	66

7	Circuit-switched Domain—Architecture and Protocols	67
7.1	Architecture	68
7.2	Protocols	69
7.2.1	User-Plane	70
7.2.2	Control-Plane	70
7.3	Summary	72
8	UMTS Terrestrial Radio Access Network—Architecture and Protocols	73
8.1	Architecture	73
8.1.1	Node B	75
8.1.2	RNC	75
8.2	Protocols and Channels	76
8.2.1	User-Plane	77
8.2.2	Control-Plane	77
8.2.3	Lower Layers and Channels	78
8.3	Summary	80
9	User Equipment—Architecture and Protocols	81
9.1	Architecture	81
9.1.1	TE	82
9.1.2	MT	82
9.1.3	UICC	83
9.2	Summary	84
10	IP Multimedia Subsystem—Architecture and Protocols	85
10.1	IMS Service Support	86
10.1.1	Basic Service Support	87
10.1.2	Advanced Service Support	87
10.2	Architecture	87
10.2.1	CSCF	89
10.2.2	IP Connectivity Access Network	89
10.3	Protocols	90
10.3.1	User-Plane	90
10.3.2	Control-Plane	90
10.4	Summary	91
10.4.1	Introduction to Chapters 11–17	92
11	Basic UMTS Functionality	93
11.1	Public Land Mobile Network (PLMN)	95
11.2	The Bearer Concept	96
11.3	UE Preparation	96
11.3.1	Searching for a Suitable Cell	97
11.3.2	Searching for a Suitable Network	97
11.4	RRC Connection Set-up Procedure	98
11.4.1	Message Flow for RRC Connection Set-up	98

11.5	GPRS Attach Procedure	99
11.5.1	Mobility Management States	99
11.5.2	Determining the Location of the UE	100
11.5.3	Message Flow for GPRS Attach	101
11.5.4	Combined GPRS/IMSI Attach	102
11.6	PDP Context Establishment Procedure	103
11.6.1	The PDP Context	103
11.6.2	PDP States	104
11.6.3	Message Flow for PDP Context Establishment	104
11.7	Detaching from the Network	105
11.8	Basic UMTS Functionality in Roaming Scenarios	106
11.9	Basic WLAN Functionality	106
11.9.1	Mobile Station Preparation	106
11.9.2	Establishing Radio Connectivity	108
11.9.3	Establishing IP Connectivity	108
11.10	Discussion	108
11.11	Summary	109
12	Mobility	111
12.1	Description of the Problems	112
12.2	Mobility in UMTS	113
12.2.1	Mobility in PMM-IDLE State	114
12.2.1.1	Routing Area Updates	114
12.2.1.2	Paging	116
12.2.2	Mobility in PMM-CONNECTED State	117
12.2.2.1	Handover	117
12.2.2.2	SRNC Relocation	117
12.3	Link-Layer Mobility in a WLAN	118
12.4	Mobility in Computer Networks	119
12.4.1	Basic Mobility Support by the IETF	120
12.4.1.1	Mobile IPv6	120
12.4.1.2	Mobile IPv4	121
12.4.2	Advanced Mobility Support by the IETF	122
12.4.2.1	Context Transfer Between Old Access Router and New Access Router	122
12.4.2.2	Seamless Mobility	123
12.4.2.3	Power-Saving Mode and Paging	124
12.5	Discussion	124
12.6	Summary	125
13	Security	127
13.1	Description of the Problems	128
13.1.1	Information Disclosure	129
13.1.2	Information Forgery	129
13.1.3	Theft of Service	130
13.1.4	Denial of Service	131

13.2	General Approach to Solutions	131
13.2.1	Secret Keys	131
13.2.2	Integrity Protection	132
13.2.3	Encryption	133
13.2.4	Authentication	133
13.2.5	Authorization	134
13.2.6	Discussion	134
13.3	Security in UMTS	134
13.3.1	Secret Keys	135
13.3.2	Authentication and Authorization in the PS Domain	135
13.3.3	Authentication and Authorization in the IMS	137
13.3.4	Integrity Protection	137
13.3.4.1	Integrity Protection on the Air Interface	137
13.3.4.2	Integrity Protection in Inter-PLMN Scenarios	138
13.3.5	Encryption	138
13.4	Security in a WLAN	138
13.4.1	Secret Keys	138
13.4.2	Authentication and Authorization	139
13.4.3	Integrity Protection and Encryption	140
13.5	Security Computer Networks	140
13.5.1	Authentication and Authorization	140
13.5.1.1	General Authentication Scenario	140
13.5.1.2	Network Access Authentication Scenario	141
13.5.1.3	Network Access Authentication Scenario with Roaming	141
13.5.1.4	Front end Protocols and back end Protocols	142
13.5.2	Integrity Protection and Encryption	144
13.6	Discussion	144
13.7	Summary	145
14	Quality of Service	147
14.1	Description of the Problems	148
14.1.1	QoS and Scalability	148
14.1.2	QoS Parameterization	149
14.1.3	QoS Signalling and QoS Provisioning	150
14.1.4	QoS and Seamless Mobility	151
14.2	QoS in Computer Networks	151
14.2.1	QoS Provisioning	152
14.2.1.1	Overprovisioning	152
14.2.1.2	Differentiated Services	154
14.2.1.3	Integrated Services	155
14.2.1.4	MPLS	155
14.2.2	QoS Signalling	157
14.2.2.1	RSVP	157

14.2.2.2	QoS NSLP	160
14.2.2.3	SIP	160
14.2.3	End-to-end QoS Signalling Scenarios	161
14.3	QoS in UMTS	162
14.3.1	UMTS Traffic Classes	162
14.3.2	QoS Signalling for the UMTS Bearer	163
14.3.2.1	UMTS QoS Signalling to the PS Domain	163
14.3.3	UMTS QoS Provisioning	163
14.3.4	QoS of the End-to-End Bearer in UMTS	164
14.3.4.1	Service Level Agreements	164
14.3.4.2	UMTS End-to-end QoS Scenarios	164
14.4	Link-Layer QoS in a WLAN	166
14.5	Discussion	166
14.6	Summary	167
15	Session Control	169
15.1	Description of the Problems	170
15.2	SIP	171
15.2.1	SIP Identifiers	171
15.2.2	SIP Infrastructure	172
15.2.3	SIP Transactions	173
15.2.4	Session Description	174
15.2.5	SIP Example Message Flows	175
15.3	SIP in the IMS	177
15.3.1	SIP Infrastructure in the IMS	178
15.3.1.1	Proxy CSCF	178
15.3.1.2	Serving CSCF	179
15.3.1.3	Interrogating CSCF	179
15.3.1.4	SIP Octagon	179
15.3.2	UE Registration in the IMS	180
15.3.2.1	Message Flow for UE Registration in the IMS	181
15.3.3	Session Creation in the IMS	182
15.3.3.1	Message Flow for Session Creation in the IMS	183
15.3.4	Session Release and UE Deregistration in the IMS	185
15.4	Discussion	186
15.5	Summary	186
16	Charging	189
16.1	Description of the Problems	190
16.2	Charging in Computer Networks and WLAN	192
16.3	Charging in UMTS	192
16.3.1	Offline Charging and Online Charging	193
16.3.2	UMTS Charging Architecture	194
16.3.2.1	Offline Charging Architecture	195
16.3.2.2	Online Charging Architecture	196
16.3.2.3	Flow-based Charging	197

16.3.3 Charging in the PS Domain	200
16.3.3.1 Offline Charging in the PS Domain	201
16.3.3.2 Online Charging in the PS Domain	201
16.3.3.3 Roaming Scenario	202
16.3.4 Charging in the IMS	202
16.3.4.1 Offline Charging in the IMS	202
16.3.4.2 Online Charging in the IMS	204
16.3.4.3 Roaming Scenario	204
16.4 Discussion	204
16.5 Summary	205
17 Policy Control	207
17.1 Description of the Problems	208
17.2 Policy Control in Computer Networks	209
17.2.1 Policy Control in Roaming	209
17.2.2 Policy Control in QoS Authorization	210
17.2.3 The IETF Policy Architecture	210
17.2.4 Policy Push	211
17.3 Policy Control in UMTS	212
17.3.1 Service-based Local Policy	212
17.3.1.1 Message Flow for Service-based Local Policy	213
17.3.2 Policy and Charging Control	215
17.3.2.1 Policy and Charging Control in Roaming Scenarios	217
17.4 Discussion	217
17.5 Summary	219
18 WLAN and Other Alternative Access Methods	221
18.1 Interworking WLAN	222
18.1.1 I-WLAN Scenarios	222
18.1.2 I-WLAN Architecture	223
18.1.2.1 Non-roaming Case	224
18.1.2.2 Roaming Case	226
18.1.3 I-WLAN Basic Functionality	226
18.1.4 I-WLAN Mobility	227
18.1.5 I-WLAN Security	227
18.1.6 I-WLAN QoS	227
18.1.7 I-WLAN Charging	228
18.1.8 I-WLAN Policy Control	228
18.2 Generic Access Network	229
18.2.1 Enhanced GAN	232
18.3 Comparison and Discussion	232
18.4 Femtocells	233
18.5 Summary	234

21 Evolution Towards 4G: 3GPP	269
21.1 3GPP Rel-8—Architecture and Protocols	271
21.2 E-UTRA	271
21.3 EPC—Architecture and Protocols	273
21.3.1 High-level View of the EPC Architecture and Protocols	273
21.3.2 Detailed EPC Architecture and Protocols	274
21.3.2.1 3GPP Access Network Architecture	274
21.3.2.2 3GPP Access Network Protocols	276
21.3.2.3 Untrusted non-3GPP Access Network Architecture	277
21.3.2.4 Untrusted non-3GPP Access Network Protocols	278
21.3.2.5 Trusted non-3GPP Access Network Architecture	278
21.3.2.6 Trusted non-3GPP Access Network protocols	279
21.3.2.7 PGW	279
21.3.3 E-UTRAN: Architecture and Protocols	280
21.3.3.1 E-UTRAN Architecture	280
21.3.3.2 Protocols and Channels	280
21.4 3GPP Rel-8 Functionality	281
21.4.1 Basic Functionality	281
21.4.1.1 Proxy Mobile IP	282
21.4.1.2 Network Attach	284
21.4.1.3 Dedicated Bearer Establishment	286
21.4.1.4 Detaching	287
21.4.1.5 Roaming	287
21.4.2 Mobility	288
21.4.2.1 Mobility within 3GPP Access Networks	289
21.4.2.2 Mobility Involving non-3GPP Access Networks	290
21.4.3 Security	291
21.4.3.1 Secret Keys	292
21.4.3.2 Authentication and Authorization	292
21.4.3.3 Encryption and Integrity Protection	292
21.4.4 QoS	293
21.4.4.1 QoS Parameterization	293
21.4.4.2 QoS Signalling	293
21.4.5 Charging	294
21.4.6 Policy Control	294
21.5 Discussion	294
21.6 Summary	294
22 Evolution Towards 4G: Non-3GPP Technologies	297
22.1 cdma2000	298
22.1.1 cdma2000-1xRTT and cdma2000-1xEV-DO	299
22.1.2 UMB	299
22.1.2.1 Radio Interface	299
22.1.2.2 Architecture and Protocols	299
22.1.2.3 Interworking with Other Technologies	301