

An Introduction to 5G

Second Edition

The New Radio, 5G Network,
5G Advanced and Beyond

Christopher Cox

WILEY

An Introduction to 5G

An Introduction to 5G

The New Radio, 5G Network, 5G Advanced and Beyond

Second Edition

Christopher Cox
Chris Cox Communications Ltd
Cambridge, UK

WILEY

This edition first published 2025
© 2025 John Wiley & Sons Ltd

Edition History

John Wiley & Sons Ltd (1e, 2021)

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 law. Advice on how to obtain permission to reuse material from this title is available at <http://www.wiley.com/go/permissions>.

The right of Christopher Cox to be identified as the author of this work has been asserted in accordance with law.

Registered Offices

John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA

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

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

The manufacturer's authorized representative according to the EU General Product Safety Regulation is Wiley-VCH GmbH, Boschstr. 12, 69469 Weinheim, Germany, e-mail: Product_Safety@wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Limit of Liability/Disclaimer of Warranty

While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials or promotional statements for this work. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Library of Congress Cataloging-in-Publication Data applied for

Hardback ISBN: 9781394284726

Cover design by Wiley

Cover image: © Weiquan Lin/Getty Images

Set in 9.5/12.5pt STIXTwoText by Straive, Pondicherry, India

To Susie

Contents

Preface *xxiii*

Acknowledgements *xxv*

List of Abbreviations *xxvii*

1	Introduction	1
1.1	Architecture of a Mobile Telecommunication System	1
1.1.1	High-level Architecture	1
1.1.2	Internal Architecture of the Mobile	2
1.1.3	Architecture of the Radio Access Network	2
1.1.4	Coverage and Capacity	3
1.1.5	Architecture of the Core Network	4
1.1.6	Communication Protocols	4
1.2	History of Mobile Telecommunications	5
1.2.1	Introduction	5
1.2.2	Global System for Mobile Communications (GSM)	6
1.2.3	Universal Mobile Telecommunication System (UMTS)	6
1.2.4	Long-term Evolution (LTE)	7
1.2.5	LTE-Advanced	7
1.2.6	LTE-Advanced Pro	8
1.2.7	Other Mobile Communication Systems	8
1.2.8	Early Research into 5G	9
1.3	Technologies for 5G	9
1.3.1	Network Function Virtualization	9
1.3.2	Software-defined Networking	10
1.3.3	Network Slicing	10
1.3.4	Technologies for the Radio Access Network	11
1.3.5	Technologies for the Air Interface	12
1.3.6	Artificial Intelligence and Machine Learning	13
1.4	The 3GPP 5G System	13
1.4.1	The 3GPP Specifications for 5G	13
1.4.2	Technical Performance Capabilities	15
1.4.3	High-level Architecture	17
1.4.4	Architectural Options	17
1.5	Enhanced Mobile Broadband	19
1.5.1	eMBB Applications	19

1.5.2	The Market for eMBB	19
1.6	Massive Machine-type Communications	21
1.6.1	mMTC Applications	21
1.6.2	The Market for MTC	22
1.7	Ultra-reliable Low-latency Communication	23
1.7.1	URLLC Applications	23
1.7.2	The Industrial Internet of Things	23
1.7.3	Vehicle-to-everything Communication	24
1.7.4	Extended Reality and Media	24
	References	24
2	Architecture of the Core Network	29
2.1	The Evolved Packet Core	29
2.1.1	Release 8 Architecture	29
2.1.2	Control and User Plane Separation	30
2.2	The 5G Core Network	31
2.2.1	Representation Using Reference Points	31
2.2.2	Representation Using Service-based Interfaces	32
2.2.3	Data Transport	33
2.2.4	Roaming Architectures	34
2.2.5	Data Storage Architectures	36
2.3	Network Areas and Identities	36
2.3.1	Network Identities	36
2.3.2	AMF Areas and Identities	37
2.3.3	UE Identities	37
2.3.4	UE Registration Areas	38
2.4	State Diagrams	38
2.4.1	Registration Management	38
2.4.2	Connection Management	39
2.5	Network Slicing	39
2.5.1	Architecture	39
2.5.2	Identification	40
2.5.3	Slice-specific Attributes	41
2.6	Non-3GPP Access to the 5G Core	42
2.6.1	Untrusted Non-3GPP Access	42
2.6.2	Non-3GPP Access Enhancements	43
2.7	Signalling Protocols	43
2.7.1	Signalling Protocol Architecture	43
2.7.2	Example Signalling Procedures	44
2.8	The Hypertext Transfer Protocol	45
2.8.1	HTTP/1.1 and HTTP/2	45
2.8.2	Representational State Transfer	45
2.8.3	The HTTP/2 Data Layer	46
2.8.4	JavaScript Object Notation (JSON)	47
2.9	Example Network Function Services	48
2.9.1	Network Function Service Registration	48
2.9.2	Network Function Service Discovery	49

2.9.3	Network Function Service Subscription and Notification	50
2.9.4	Use of a Service Communication Proxy	51
	References	52

3 Architecture of the Radio Access Network 57

3.1	The Evolved UMTS Terrestrial Radio Access Network	57
3.1.1	Release 8 Architecture	57
3.1.2	Carrier Aggregation	58
3.1.3	Dual Connectivity	59
3.2	The Next-generation Node B	60
3.2.1	High-level Architecture	60
3.2.2	Internal Architecture	60
3.2.3	Deployment Options	61
3.3	Architectural Options	62
3.3.1	Multi-radio Dual Connectivity	62
3.3.2	Options 1 and 3: EPC, E-UTRAN and MeNB	63
3.3.3	Options 5 and 7: 5GC, NG-RAN and MeNB	63
3.3.4	Options 2 and 4: 5GC, NG-RAN and MgNB	64
3.3.5	Dual Connectivity and Disaggregation	65
3.3.6	Data Transport	65
3.4	Network Areas and Identities	66
3.4.1	Tracking Areas	66
3.4.2	RAN Areas	67
3.4.3	Cell Identities	67
3.5	RRC State Diagram	67
3.5.1	5G State Diagram	67
3.5.2	Interworking with 4G	68
3.6	Signalling Protocols	69
3.6.1	Signalling Protocol Architecture	69
3.6.2	Signalling Radio Bearers	70
3.7	Open Radio Access Networks	71
3.7.1	O-RAN Architecture	71
3.7.2	O-RAN Use Cases	73
	References	73

4 Spectrum, Antennas and Propagation 77

4.1	Radio Spectrum	77
4.1.1	Radio Waves	77
4.1.2	Use of Radio Spectrum	78
4.1.3	Spectrum Allocations for 5G	79
4.2	Antennas and Propagation	79
4.2.1	Antenna Gain	79
4.2.2	Radio Propagation in Free Space	80
4.2.3	Antenna Arrays for 5G	81
4.3	Radio Propagation Issues for Millimetre Waves	82
4.3.1	Diffraction and Reflection	82
4.3.2	Penetration Losses	83

4.3.3	Foliage Losses	84
4.3.4	Atmospheric Losses	85
4.4	Multipath, Fading and Coherence	86
4.4.1	Introduction	86
4.4.2	Angular Spread and Coherence Distance	87
4.4.3	Doppler Spread and Coherence Time	88
4.4.4	Delay Spread and Coherence Bandwidth	89
4.4.5	Channel Reciprocity	90
	References	90
5	Digital Signal Processing	93
5.1	Modulation and Demodulation	93
5.1.1	Carrier Signal	93
5.1.2	Modulation	94
5.1.3	The Modulation Process	96
5.1.4	The Demodulation Process	97
5.1.5	Channel Estimation	98
5.1.6	Adaptive Modulation	98
5.2	Radio Transmission in a Mobile Cellular Network	99
5.2.1	Multiplexing and Multiple Access	99
5.2.2	FDD and TDD Modes	99
5.3	Orthogonal Frequency Division Multiple Access	100
5.3.1	Subcarriers	100
5.3.2	The OFDM Transmitter	101
5.3.3	The OFDM Receiver	101
5.3.4	The Fast Fourier Transform	104
5.3.5	Block Diagram of the OFDMA Downlink	104
5.3.6	Block Diagram of the OFDMA Uplink	105
5.4	Other Features of OFDMA	107
5.4.1	Frequency-specific Scheduling	107
5.4.2	Subcarrier Orthogonality	108
5.4.3	Inter-symbol Interference and the Cyclic Prefix	109
5.5	Signal-processing Issues for 5G	111
5.5.1	Power Consumption	111
5.5.2	Timing Jitter and Phase Noise	111
5.5.3	Choice of Symbol Duration and Subcarrier Spacing	112
5.6	Error Management	112
5.6.1	Forward Error Correction	112
5.6.2	Automatic Repeat Request	113
5.6.3	Hybrid ARQ	113
5.6.4	Hybrid ARQ Processes	114
5.6.5	Higher-layer Retransmissions	115
	References	116
6	Multiple-antenna Techniques	117
6.1	Beamforming	117
6.1.1	Antenna Arrays	117

6.1.2	Array Gain	118
6.1.3	Beam Steering	119
6.2	Beamforming at the gNB	120
6.2.1	Analogue Beam Selection	120
6.2.2	Digital Beamforming	121
6.2.3	Hybrid Beamforming	122
6.2.4	Deployment Scenarios	124
6.3	Beamforming at the Mobile	126
6.4	Beam Management	127
6.4.1	Reference Signals	127
6.4.2	Cell Acquisition	128
6.4.3	Analogue Beam Selection	128
6.4.4	Analogue Beam Pair Selection	129
6.4.5	Digital Beam Management	129
6.5	Spatial Multiplexing	130
6.5.1	Principles of Spatial Multiplexing	130
6.5.2	Coherence Issues	131
6.5.3	Matrix Representation	132
6.6	Multiple-user MIMO	133
6.6.1	Uplink Multiple-user MIMO	133
6.6.2	Downlink Multiple-user MIMO	135
6.6.3	Management of Multiple-user MIMO	135
6.6.4	Mathematical Details	136
6.7	Massive MIMO	137
6.7.1	Architecture	137
6.7.2	Benefits	138
6.8	Single-user MIMO	139
6.8.1	Principles of Single-user MIMO	139
6.8.2	Single-user MIMO in a Sparse Multipath Environment	140
6.8.3	Management of Single-user MIMO	141
6.8.4	Mathematical Details	141
6.9	Multipoint Transmission and Reception	143
	References	144
7	Architecture of the 5G New Radio	145
7.1	Air Interface Protocol Stack	145
7.1.1	5G Protocol Stack	145
7.1.2	Midhaul Split Point	147
7.1.3	Dual Connectivity	147
7.1.4	Channels and Signals	148
7.1.5	Information Flows	148
7.2	Frequency Bands and Combinations	152
7.2.1	Frequency Bands	152
7.2.2	Band Combinations	155
7.2.3	Bandwidth Classes	156
7.3	Frequency Domain Structure	156
7.3.1	Numerologies	156

7.3.2	Transmission Bandwidth Configuration	157
7.3.3	Global and Channel Frequency Rasters	158
7.3.4	Common Resource Blocks	159
7.3.5	Bandwidth Parts	160
7.3.6	Virtual and Physical Resource Blocks	160
7.4	Time Domain Structure	161
7.4.1	Frame Structure	161
7.4.2	Timing Advance	163
7.4.3	TDD Configurations	163
7.4.4	Slot Format Combinations	164
7.4.5	Resource Grid	165
7.4.6	Dynamic Spectrum Sharing	165
7.5	Multiple Antennas	166
7.5.1	Antenna Ports	166
7.5.2	Relationships between Antenna Ports	167
7.6	Data Transmission	167
7.6.1	Transport Channel Processing	167
7.6.2	Physical Channel Processing	168
7.6.3	Analogue Processing	170
7.6.4	Fronthaul Split Point	170
	References	171
8	Cell Acquisition	175
8.1	Acquisition Procedure	175
8.1.1	Introduction	175
8.1.2	Non-standalone Operation	176
8.1.3	Standalone Operation	177
8.2	Resource Mapping	177
8.2.1	SS/PBCH Blocks	177
8.2.2	Transmission Frequency	178
8.2.3	Transmission Timing	178
8.3	Acquisition of the SS/PBCH Block	180
8.3.1	Primary Synchronization Signal	180
8.3.2	Secondary Synchronization Signal	180
8.3.3	Demodulation Reference Signal for the PBCH	181
8.3.4	Physical Broadcast Channel	181
8.4	System Information	181
8.4.1	Master Information Block	181
8.4.2	System Information Block 1	182
8.4.3	Other System Information Blocks	182
8.4.4	Transmission and Reception of the System Information	182
	References	184
9	Random Access	187
9.1	Physical Random Access Channel	187
9.1.1	PRACH Formats	187
9.1.2	Generation of the PRACH Preamble	189

9.1.3	Resource Mapping	190
9.2	Random Access Procedure	190
9.2.1	Random Access Preamble	190
9.2.2	Random Access Response	191
9.2.3	Message 3	192
9.2.4	Contention Resolution	192
9.3	Variations on the Random Access Procedure	193
9.3.1	Contention-free Procedure	193
9.3.2	Two-step Procedure	193
	References	194
10	Link Adaptation	197
10.1	CSI Reference Signals	197
10.1.1	Transmission and Reception	197
10.1.2	Resource Mapping	198
10.1.3	CSI-RS Resources	199
10.1.4	CSI-RS Resource Sets	199
10.2	Channel State Information	201
10.2.1	Introduction	201
10.2.2	CSI-RS and SS/PBCH Block Resource Indicators	201
10.2.3	Layer 1 RSRP and SINR	201
10.2.4	Rank Indication	201
10.2.5	Precoding Matrix Indicator	201
10.2.6	Channel Quality Indicator	203
10.2.7	Layer Indicator	204
10.2.8	Time Domain Channel Property	204
10.2.9	CSI Reporting	205
10.3	Physical Uplink Control Channel	205
10.3.1	Introduction	205
10.3.2	PUCCH Formats	206
10.3.3	PUCCH Resources	207
10.4	Sounding	208
10.4.1	Transmission and Reception	208
10.4.2	Resource Mapping	208
10.4.3	SRS Resources	209
	References	210
11	Data Transmission and Reception	213
11.1	Introduction	213
11.1.1	Data Transmission Procedure	213
11.1.2	Downlink Control Information	214
11.1.3	Radio Network Temporary Identifiers	214
11.2	Transmission and Reception of the PDCCH	216
11.2.1	Transmission of the PDCCH	216
11.2.2	Control Resource Sets	217
11.2.3	Search Spaces	218
11.2.4	Reception of the PDCCH	218

11.3	Scheduling Messages	219
11.3.1	DCI Formats 0_0 and 1_0	219
11.3.2	Time Domain Resource Assignment	219
11.3.3	Frequency Domain Resource Assignment	221
11.3.4	Modulation and Coding Scheme	222
11.3.5	Other Fields	222
11.3.6	Other Scheduling Formats	223
11.4	Transmission and Reception of the PUSCH and PDSCH	223
11.4.1	Transport Channel Processing	223
11.4.2	Physical Channel Processing	224
11.4.3	Downlink MIMO	225
11.4.4	Uplink Codebook-based MIMO	226
11.4.5	Uplink Non-codebook-based MIMO	226
11.5	Reference Signals	226
11.5.1	Demodulation Reference Signals	226
11.5.2	Phase-tracking Reference Signals	228
11.6	Hybrid ARQ Acknowledgements	228
11.6.1	Downlink Acknowledgements of Uplink Data	228
11.6.2	Uplink Acknowledgements of Downlink Data	229
11.6.3	Timing of Uplink Acknowledgements	229
11.7	Related Procedures	230
11.7.1	Scheduling Requests	230
11.7.2	Semi-persistent and Configured Scheduling	230
11.7.3	Slot Format Indications	231
11.7.4	Pre-emption Indications	231
11.7.5	Transmit Power Control Commands	232
11.7.6	Discontinuous Reception in RRC_IDLE and RRC_INACTIVE	232
11.7.7	Discontinuous Reception in RRC_CONNECTED	233
11.7.8	Dynamic Spectrum Sharing	233
11.8	Performance of 5G	234
11.8.1	Peak Data Rate	234
11.8.2	Typical Cell Capacity	236
	References	238
12	Air Interface Layer 2	241
12.1	Medium Access Control	241
12.1.1	Protocol Architecture	241
12.1.2	Scheduling	241
12.1.3	Logical Channel Prioritization	242
12.1.4	Multiplexing and De-multiplexing	243
12.1.5	MAC Control Elements	243
12.2	Radio Link Control	245
12.2.1	Protocol Architecture	245
12.2.2	Transparent Mode	245
12.2.3	Unacknowledged Mode	246
12.2.4	Acknowledged Mode	247

12.3	Packet Data Convergence Protocol	249
12.3.1	Protocol Architecture	249
12.3.2	Transmission and Reception	249
12.3.3	PDCP Duplication	250
12.3.4	Prevention of Packet Loss during a Change of Node	250
12.3.5	Header and Data Compression	251
12.4	Service Data Adaptation Protocol	251
	References	252
13	Registration Procedures	253
13.1	Power-on Sequence	253
13.2	Network and Cell Selection	254
13.2.1	Network Selection	254
13.2.2	Cell Selection	255
13.3	RRC Connection Establishment	256
13.3.1	RRC Connection Establishment with a gNB	256
13.3.2	Initial UE Message	257
13.3.3	RRC Connection Establishment with an eNB	258
13.4	Registration Procedure	258
13.4.1	Registration Without AMF Change	258
13.4.2	Registration with a New AMF	260
13.4.3	Registration with AMF Re-allocation	262
13.5	Deregistration Procedure	263
	References	264
14	Security	267
14.1	Security Principles	267
14.2	Network Access Security	268
14.2.1	Network Access Security Architecture	268
14.2.2	Key Hierarchy	269
14.3	Network Access Security Procedures	270
14.3.1	Subscription Concealed Identifier	270
14.3.2	Authentication and Key Agreement	270
14.3.3	Activation of Non-access Stratum Security	273
14.3.4	Activation of Access Stratum Security	273
14.3.5	Key Handling during Mobility	274
14.3.6	Key Handling during State Transitions	274
14.3.7	Ciphering	275
14.3.8	Integrity Protection	275
14.4	Network Domain Security	276
14.4.1	Network Domain Security Architecture	276
14.4.2	Network Domain Security Protocols	276
14.5	Service-based Architecture Domain Security	278
14.5.1	Security Architecture	278
14.5.2	Initial Handshake Procedures over N32-c	279
14.5.3	Forwarding of JOSE Protected Messages over N32-f	279
	References	280

15	Session Management, Policy and Charging	283
15.1	Types of PDU Session	283
15.1.1	IP PDU Sessions	283
15.1.2	Ethernet PDU Sessions	284
15.1.3	Unstructured PDU Sessions	284
15.2	Quality of Service	285
15.2.1	Packet Flows, Service Data Flows and QoS Flows	285
15.2.2	QoS Parameters	286
15.2.3	QoS Parameters for PDU Sets	290
15.2.4	Charging Parameters	290
15.3	Implementation of PDU Sessions	290
15.3.1	Bearers and Tunnels	290
15.3.2	User Plane Protocols	291
15.3.3	End-to-end Protocol Stack	292
15.3.4	Multiple PDU Session Anchors	293
15.3.5	PDU Session Anchor Relocation	294
15.4	Policy and Charging Control Architecture	295
15.4.1	High-level Architecture	295
15.4.2	Northbound API	297
15.4.3	Charging and Billing System	297
15.5	PDU Session Management Procedures	298
15.5.1	PDU Session Establishment	298
15.5.2	Interactions with the Policy and Charging Control System	300
15.5.3	Quality of Service Request	302
15.5.4	Addition of a PDU Session Anchor	303
15.5.5	PDU Session Release	305
	References	305
16	Mobility Management in RRC_CONNECTED	309
16.1	Introduction to RRC_CONNECTED	309
16.1.1	Principles	309
16.1.2	Dual Connectivity	310
16.1.3	PDU Sessions	310
16.2	Measurement Configuration and Reporting	310
16.2.1	Measurement Configuration and Reporting Procedure	310
16.2.2	Measurement Objects	312
16.2.3	Reporting Configurations	312
16.2.4	Measurement Gaps	314
16.2.5	Measurement Reporting	315
16.3	Handover Procedures	315
16.3.1	Xn-based Handover Procedure	315
16.3.2	Path Switch Procedure	317
16.3.3	NG-based Handover Procedure	318
16.3.4	Handovers between a gNB and an ng-eNB	319
16.3.5	Handovers with no Change of Central Unit	319
16.3.6	Handover Optimizations	319
16.4	Dual Connectivity Procedures	320

16.4.1	Secondary Node Addition	320
16.4.2	QoS Flow Mobility Procedure	322
16.4.3	Other Dual Connectivity Procedures	323
16.5	State Transitions out of RRC_CONNECTED	323
16.5.1	Core Network Assistance Information	323
16.5.2	Transition to RRC_IDLE	324
16.5.3	Transition to RRC_INACTIVE	325
	References	326
17	Mobility Management in RRC_IDLE	329
17.1	Introduction to RRC_IDLE	329
17.1.1	Principles	329
17.1.2	Inactive PDU Sessions	330
17.2	Cell Reselection Procedures	330
17.2.1	Introduction	330
17.2.2	Intra-frequency Measurement Triggering	331
17.2.3	Intra-frequency Cell Reselection	331
17.2.4	Inter-frequency Measurement Triggering	332
17.2.5	Inter-frequency Cell Reselection	332
17.2.6	Fast-moving Mobiles	333
17.3	Registration Updating	333
17.3.1	Registration Update Procedure	333
17.3.2	Network Reselection	334
17.4	State Transitions out of RRC_IDLE	335
17.4.1	Mobile-triggered Service Request	335
17.4.2	Network-triggered Service Request	336
	References	338
18	Mobility Management in RRC_INACTIVE	339
18.1	Introduction to RRC_INACTIVE	339
18.1.1	Principles	339
18.1.2	Suspended PDU Sessions	340
18.2	Mobility Management	341
18.2.1	RAN-based Notification Area Update	341
18.2.2	Registration Update	342
18.2.3	Mobility between a gNB and an ng-eNB	343
18.3	State Transitions	343
18.3.1	Transition to RRC_IDLE	343
18.3.2	Mobile-triggered Resumption of the RRC Connection	343
18.3.3	Network-triggered Resumption of the RRC Connection	345
18.4	Small Data Transmission in RRC_INACTIVE	347
	References	347
19	Inter-operation with the Evolved Packet Core	349
19.1	Inter-operation Architectures	349
19.1.1	Migration Architecture	349
19.1.2	Interworking Architecture	350

19.1.3	Signalling Protocols	351
19.1.4	State Diagrams	352
19.1.5	UDM-HSS Interworking	352
19.2	Registration Modes	353
19.2.1	Single Registration Mode	353
19.2.2	Dual Registration Mode	353
19.2.3	Temporary Identities	353
19.3	Use of the Migration Architecture	353
19.3.1	Configuration Procedures	353
19.3.2	Mobility in RRC_IDLE	354
19.3.3	RRC Release with Redirection from RRC_CONNECTED	355
19.4	Interworking Without N26	356
19.4.1	Configuration Procedures	356
19.4.2	Mobility in Single Registration Mode	356
19.4.3	Mobility in Dual Registration Mode	357
19.5	Interworking with N26	357
19.5.1	Configuration Procedures	357
19.5.2	Mobility in RRC_IDLE	357
19.5.3	Handovers in RRC_CONNECTED	359
	References	361

20 Foundations of 5G-Advanced 363

20.1	Location Services	363
20.1.1	Introduction	363
20.1.2	System Architecture	364
20.1.3	Positioning Reference Signal	365
20.1.4	NR Position Estimation	365
20.2	Integrated Access and Backhaul	366
20.2.1	Introduction	366
20.2.2	Underlying Architecture	367
20.2.3	Architectural Refinements	367
20.2.4	Communication Protocols	368
20.2.5	Mobility	369
20.2.6	Air Interface	369
20.2.7	Repeaters and Relays	370
20.2.8	Wireless Access Backhaul	371
20.3	Use of Unlicensed Spectrum	371
20.3.1	Introduction	371
20.3.2	Spectrum	372
20.3.3	Dynamic Channel Access	373
20.3.4	Shared Channel Occupancy	375
20.3.5	Semi-Static Channel Access	375
20.3.6	Additional Procedures	375
20.4	Multicast and Broadcast Services	376
20.4.1	Introduction	376
20.4.2	MBS Service	376
20.4.3	MBS Architecture	378

20.4.4	MBS User Service	378
20.4.5	Enhancements to the 5G New Radio	379
20.5	Non-terrestrial Networks	380
20.5.1	Introduction	380
20.5.2	Non-terrestrial Platforms	380
20.5.3	Radio Access Architecture	380
20.5.4	Enhancements to the 5G New Radio	382
20.5.5	Mobility Management	383
20.5.6	Satellite Backhaul	384
20.6	Network Automation, Artificial Intelligence and Machine Learning	385
20.6.1	TDD Interference Management	385
20.6.2	Self-Optimizing Networks	385
20.6.3	AI/ML in the Radio Access Network	386
20.6.4	Network Data Analytics	387
20.7	Service Enabler Architecture Layer	388
	References	389
21	The Internet of Things	395
21.1	Time-sensitive Communications	395
21.1.1	Cyber-physical Control Applications	395
21.1.2	Example Applications	396
21.1.3	Time Synchronization	397
21.1.4	Time Synchronization Architecture for 5G	397
21.1.5	Architecture for Network Exposure	398
21.1.6	Signalling Procedures	399
21.2	Non-public Networks	400
21.2.1	The Market for NPNs	400
21.2.2	5G Support for NPNs	400
21.3	5G Virtual Networks	402
21.3.1	Capabilities	402
21.3.2	Virtual Network Groups	402
21.3.3	Data Transport	403
21.4	Edge Computing	404
21.4.1	Requirements and Applications	404
21.4.2	Architecture	404
21.4.3	EAS Deployment Information	405
21.4.4	EAS Discovery Procedure	406
21.4.5	Edge Relocation Procedure	407
21.4.6	Edge Enabler Layer	408
21.5	Massive Machine-type Communications	410
21.5.1	Air Interfaces for mMTC	410
21.5.2	Reduced Capability NR Devices	411
21.5.3	Enhancements to the 5G Core Network	412
21.6	Messaging Services	412
21.6.1	Short Message Service	412
21.6.2	5G Messaging Service	413
	References	414

22	Vehicle Communications and the Sidelink	417
22.1	Vehicle-to-Everything (V2X) Communications	417
22.1.1	V2X Services	417
22.1.2	V2X Architecture	418
22.1.3	V2X Identities	419
22.1.4	Sidelink Quality of Service	419
22.1.5	V2X Policy	420
22.1.6	Sidelink Security	422
22.1.7	V2X Layer	422
22.1.8	V2X Application Enabler Layer	423
22.2	Uncrewed Aerial Vehicles	423
22.2.1	UAV Support in 5G	423
22.2.2	UAV Architecture	424
22.3	Proximity-based Services	425
22.3.1	Applications	425
22.3.2	ProSe Architecture	426
22.3.3	ProSe Relays	428
22.3.4	ProSe Identities	429
22.3.5	ProSe Policy	430
22.3.6	Additional Security Procedures	430
22.4	Architecture of the Sidelink	430
22.4.1	Protocol Stack	430
22.4.2	Channels, Signals and Information Flows	430
22.4.3	Physical Layer	434
22.4.4	Resource Pools	434
22.5	Sidelink Timing Synchronization	435
22.5.1	Acquisition of Timing Synchronization	435
22.5.2	Transmission of Sidelink Synchronization Blocks	436
22.6	Sidelink Transmission and Reception	437
22.6.1	Signalling Procedure	437
22.6.2	First-stage SCI	438
22.6.3	Second-stage SCI	439
22.6.4	Resource Mapping	440
22.6.5	Hybrid ARQ Acknowledgements	441
22.7	Access Stratum Procedures for the Sidelink	442
22.7.1	Resource Allocation by the NG-RAN	442
22.7.2	Autonomous Resource Selection	442
22.7.3	Conflict Resolution	443
22.7.4	Channel State Information	443
22.7.5	Sidelink Operation in Unlicensed Spectrum	443
22.7.6	Ranging-based Services and Sidelink Positioning	444
22.8	Operation of Sidelink Communication	444
22.8.1	Broadcast and Groupcast Vehicle Communication	444
22.8.2	Unicast Vehicle Communication	445
22.8.3	Aircraft and ProSe Direct Communication	446
22.9	Operation of ProSe Direct Discovery	447
22.9.1	Model A Procedure for Open Direct Discovery	447

22.9.2	ProSe Direct Discovery Variations	448
	References	448
23	From 5G-Advanced to 6G	453
23.1	Release 19	453
23.1.1	AI/ML for the Air Interface	453
23.1.2	Integrated Sensing and Communication	454
23.1.3	Ambient Internet of Things	454
23.1.4	Low-power Wake-up Signal and Receiver	455
23.1.5	Sub-band Non-overlapping Full Duplex Transmission	455
23.1.6	Other Topics for Release 19	455
23.2	6G	456
23.2.1	Specification Process	456
23.2.2	Usage Scenarios	457
23.2.3	Applications	457
23.2.4	Spectrum Allocations	458
23.2.5	Technologies	459
23.2.6	Performance Targets for 6G	461
	References	461
	Further Reading	465
	Index	469

Preface

This book is an introduction to fifth-generation (5G) mobile telecommunication systems and to the enhancements that have been made to those systems under the name of 5G-Advanced.

5G builds on earlier generations of mobile telecommunications, but it differs in several ways. It is designed for a wider range of applications than before: not only consumer applications such as voice, video and data, but also industrial applications such as machine-type communications. In turn, those applications have a wider range of requirements than before: some require a peak data rate of several gigabits per second, others require the delivery of data packets with delays as low as a few milliseconds, while others require a battery life of several years. To help meet those requirements, the network uses technologies such as network function virtualization, software-defined networking and network slicing to provide a flexible, underlying resource that can be easily reconfigured to support new requirements as they arise. In pursuit of higher data rates and higher system capacities, the air interface supports higher radio frequencies than previous generations have done and makes extensive use of multiple antennas.

There are many other books on 5G which contain detailed accounts of the underlying technologies, the likely applications, the system architecture and the air interface. The aim of this book is to complement them by offering an end-to-end, system-level perspective. It contains fewer details about individual topics than many of the others, but it is broader in scope, covering the requirements and architecture of 5G, the principles and implementation of the air interface, the signalling procedures within the network, and the new capabilities that have been added in 5G-Advanced. It is aimed at mobile telecommunication engineers who want an introduction to the architecture and operation of 5G, at those who are experts in one part of the system but who want to understand what is taking place elsewhere, and as a technical foundation for those in related roles such as management, marketing, intellectual property and consultancy.

The first few chapters cover the foundations. Chapter 1 reviews the history of mobile telecommunications and introduces the applications, requirements and key technical features of 5G. Chapter 2 covers the architecture of the core network and the signalling protocols that it uses, while Chapter 3 covers similar ground in the case of the radio access network.

The next three chapters address the underlying technologies that are used by the air interface. Chapter 4 reviews the use of radio spectrum and discusses the coverage issues that appear when operating at high radio frequencies. Chapter 5 reviews the techniques that are used for digital signal processing, for example modulation, demodulation, orthogonal frequency division multiple access and error correction. (Much of that chapter has been condensed from the author's previous work, *An Introduction to LTE*.) Chapter 6 explains how 5G uses multiple antennas to

compensate for the coverage problems that appear at high radio frequencies and to improve the system capacity when the radio frequency is low.

The next six chapters describe how the air interface is actually implemented. Chapter 7 is an introduction to the air interface, Chapter 8 describes the acquisition procedure in which a mobile discovers a nearby cell and Chapter 9 describes the random access procedure in which the mobile makes its initial communication. Chapter 10 covers the procedures for link adaptation, which compensate for changes in the amplitude and phase of the incoming radio signal, and help to control the use of multiple antennas. Chapter 11 addresses the procedures that are used for scheduling and data transmission, while Chapter 12 explains how the air interface's higher-level protocols handle tasks such as scheduling and re-transmission.

We then move on to the end-to-end operation of 5G. Chapter 13 covers the procedures that a mobile runs when it switches on to discover a nearby cell and register with its chosen network. Chapter 14 addresses the security procedures in 5G, while Chapter 15 covers the procedures which connect a mobile to an external data network and which allow an external application server to monitor and influence its behaviour.

The next four chapters address different aspects of mobility management, in which the network keeps track of the mobile's location and controls the cells with which it is communicating. Chapter 16 covers the procedures in a state known as `RRC_CONNECTED`, in which the mobile is carrying out normal communications with the network. Chapter 17 addresses the state of `RRC_IDLE`, in which the mobile is on standby, while Chapter 18 deals with the new state of `RRC_INACTIVE`, which is an optimization for low data rate communications. Chapter 19 covers the procedures used for inter-operation between the core networks of 4G and 5G.

The last four chapters address the enhancements that have been made to 5G in later releases of the specifications. Chapter 20 covers the general-purpose capabilities that form the foundations of 5G-Advanced, including location services, unlicensed spectrum, non-terrestrial networks, and artificial intelligence and machine learning. Chapter 21 focuses on system enhancements for the industrial internet of things and for massive machine-type communications. Chapter 22 addresses device-to-device communications on the 5G sidelink, as well as the vehicle, aircraft and proximity-based services that the sidelink helps to support. As the final topic, Chapter 23 reviews the enhancements that are planned for future releases of 5G and looks ahead to the introduction of a sixth generation of mobile telecommunications.

Like any technical subject, 5G uses a large number of acronyms and abbreviations. To help make the text readable, I have tried to strike a balance between the uses of abbreviations and text, for example by using 'downlink' in place of DL, but AMF in place of 'access and mobility management function'. New terms are highlighted in italics throughout the text, and there is a full list of abbreviations at the start of the book.

Unavoidably, some of the topics are mathematical ones. Some previous knowledge of Fourier transforms would help the reader understand the discussion of orthogonal frequency division multiple access in Chapter 5. Similarly, some previous knowledge of matrices would help with the discussion of multiple antennas in Chapter 6, while familiarity with complex numbers would be helpful for both. However, I have attempted to make the maths as lightweight as possible and to explain the important concepts using English instead. The Bibliography contains some references for further reading.

Acknowledgements

My first acknowledgement is to the team at Wiley, for taking on the publication of this book and for guiding me through the writing and production process. I am particularly grateful for the support received from my Commissioning Editor, Sandra Grayson, from my Project Editors for the two editions of the book, Steve Fassioms, Kavipriya Ramachandran and Veena Rajendran, from my Production Editors, Juliet Booker and Srinivasan Kandasamy, from my Editorial Assistant, Becky Cowan, from my Copy-editor, Lesley Montford, and from the whole of the production team. I would also like to extend my appreciation to the directors and staff of Wray Castle Limited. My first exposure to 5G was as part of a contract to write training material on their behalf, and I am grateful for the opportunities that the work provided to extend my knowledge and understanding of the subject.

Particular thanks are due to Paul Mason, Jeff Cartwright, Tony Wakefield, Les Granfield and Matt Brenner for many valuable discussions about telecommunications in general and 5G in particular, to Ignacio Rodriguez Larrad, for providing the data on penetration losses underlying Figure 4.5, to David Herbert, for his guidance about the signalling protocols that are used by the internet, and to Arein Zarour and Nurudeen Salau, for highlighting issues with the first edition that I hope to have addressed in the second. I would also like to offer a big thank you to the delegates in my training classes, whose probing questions have so often proved the ideal trigger for learning new aspects of the technology. Nevertheless, the responsibility for any errors and omissions in the text, and for any lack of clarity in the explanations, is entirely my own.

Several diagrams in this book have been reproduced from the technical specifications for 5G, with permission from the European Telecommunications Standards Institute, © 2024. 3GPP™ TSs and TRs are the property of ARIB, ATIS, CCSA, ETSI, TSDSI, TTA and TTC who jointly own the copyright in them. They are subject to further modifications and are therefore provided to you 'as is' for information purposes only. Further use is strictly prohibited.

On a lighter note, I would like to thank the creators of the internet blocking application Cold Turkey for removing innumerable opportunities for procrastination and keeping me focused on the task. I would also like to thank the spirits of J.S. Bach and Frédéric Chopin for providing me with some more valuable diversions, and for reminding me that there are more things in life than mobile telecommunications.

My last and greatest thank you is to my beloved wife, Susie. The first edition of this book coincided with our engagement and marriage, while the intervening years have served to demonstrate the wisdom of those events. Her kindness, patience and understanding have been extraordinary throughout, and I dedicate this book to her.

List of Abbreviations

1G	First generation
2G	Second generation
3G	Third generation
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
4G	Fourth generation
5G	Fifth generation
5G AKA	5G authentication and key agreement
5G-AN	5G access network
5GC	5G core network
5G-EIR	5G equipment identity register
5G-GUTI	5G globally unique temporary identity
5GMM	5G mobility management
5GS	5G system
5GSM	5G session management
5G-S-TMSI	5G S temporary mobile subscriber identity
5G-TMSI	5G temporary mobile subscriber identity
5QI	5G QoS identifier
6G	Sixth generation
A/D	Analogue to digital
A2X	Aircraft to everything
AAA	Authentication, authorization and accounting
AAS	Active antenna system
ABMF	Account balance management function
ADRF	Analytics data repository function
AES	Advanced Encryption Standard
AF	Application function
AGC	Automatic gain control
AI	Artificial intelligence
AI/ML	Artificial intelligence and machine learning
A-IoT	Ambient internet of things
AKA	Authentication and key agreement
AM	Acknowledged mode

AMBR	Aggregate maximum bit rate
AMF	Access and mobility management function
AMFI	AMF identifier
AMPS	Advanced Mobile Phone System
AN	Access network
AnLF	Analytics logical function
AoA	Angle of arrival
AoD	Angle of departure
API	Application programming interface
APN	Access point name
AR	Augmented reality
ARIB	Association of Radio Industries and Businesses
ARP	Allocation and retention priority
ARPF	Authentication credential repository and processing function
ARQ	Automatic repeat request
AS	Access stratum
ATIS	Alliance for Telecommunications Industry Solutions
ATSSS	Access traffic steering, switch and splitting
AuC	Authentication centre
AUSF	Authentication server function
AUTN	Authentication token
BAP	Backhaul adaptation protocol
BCCH	Broadcast control channel
BCH	Broadcast channel
BD	Billing domain
BLER	Block error ratio
BM-SC	Broadcast/multicast service centre
BPSK	Binary phase shift keying
BSF	Binding support function
BSR	Buffer status report
BTS	Base transceiver station
BWP	Bandwidth part
C2	Command and control
CA	Carrier aggregation
CAA	Civil Aviation Administration
CAG	Closed access group
CAPC	Channel access priority class
CBG	Code block group
CCCH	Common control channel
CCE	Control channel element
CCSA	China Communications Standards Association
CDM	Code division multiplexing
CDMA	Code division multiple access
CDR	Charging data record
CE	Control element
CGF	Charging gateway function