

Wireless Networking Principles: From Terrestrial to Underwater Acoustic

Shengming Jiang

Wireless Networking Principles: From Terrestrial to Underwater Acoustic

Shengming Jiang
Marine Internet Laboratory (MILAB),
College of Information Engineering
Shanghai Maritime University
Shanghai
China

ISBN 978-981-10-7774-6 ISBN 978-981-10-7775-3 (eBook)
<https://doi.org/10.1007/978-981-10-7775-3>

Library of Congress Control Number: 2018934909

© Springer Nature Singapore Pte Ltd. 2018

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd. part of Springer Nature

The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

To my wife, my son and my daughter

Preface

Today, wireless networking technologies deeply affect many social sectors and people's daily life. For example, mobile personal communication networks such as 4G and beyond as well as WiFi networks are the enabling technologies for mobile Internet used by almost everyone at anytime in terrestrial environments. These wireless networks provide the users with a great convenience for personal communication, social activities, shopping, and traveling as well as education, since many traditional activities and organizations now can be carried out simply through mobile smart terminals. The wireless networking technology as a whole is still developing. For example, mobile personal communication is under development toward 5G, aiming at providing much faster and reliable communications than the currently available one to eliminate the gap in service quality between wireless and wired networks. On the other hand, some wireless networks are still in early development stages. For example, a huge number of sensors and actuators as well as various types of vehicles have been deployed underwater, and this number is still growing. These underwater things usually equipped with communication facilities are able to construct an Internet of Underwater Thing (IoUT) [1]. How to link these nodes to cover large underwater areas and transfer the collected data to the surface processing center faces many challenges. Many issues are necessarily addressed for underwater wireless networks, which are still in infant ages.

Since the radio wave cannot propagate long enough but only acoustic signal can in underwater environments to satisfy application requirements, currently most underwater wireless networks are based on acoustic waves. Therefore, in this book we call this kind of network underwater acoustic networks (UWANs), which include underwater acoustic sensor networks. UWANs have some special features not present in most terrestrial radio wireless networks (RWNs), such as much long propagation delays, very limited channel capacities, low channel reliability, and high dynamics of communication environments. These features greatly affect the design of underwater networking protocols and schemes, preventing those well-developed for RWNs from being used directly in UWANs.

Despite many differences in networking environments between RWNs and UWANs, they still have many similar issues to be addressed by both, and many approaches and design strategies developed for RWNs can be used as references in designing UWAN protocols, and some of them can be used in UWANs after proper modifications. Therefore, a good understanding of the well-developed RWN technologies can be helpful to understand network protocols and algorithms proposed for UWANs. There are several books systematically describing RWN technologies in the literature such as [2, 3, 4], while a couple of UWANs are also available such as [5, 6]. This book is unique in terms of discussing networking technologies for both RWNs and UWANs in one.

This book aims to highlight the key networking issues and explain the basic ideas of typical networking technologies, in which the principal challenging issues and research topics are addressed and discussed in detail. The book consists of thirteen chapters. The first chapter (Chap. 1) introduces the typical wireless networks and fundamental networking issues. The remaining chapters are divided into two parts. The first part will systematically describe the well-established RWN technologies that have been standardized or applied in practice, covering the following topics: error control (Chap. 2), medium access control (MAC) protocols (Chaps. 3 and 4), routing protocols (Chap. 5), end-to-end transmission control (Chap. 6), mobility (Chap. 7), and network security (Chap. 8). The majority of this part except TCP and vertical handoff in mobile networks are relatively mature and can provide a foundation to understand the counterparts of UWANs. The second part discusses the up-to-date networking technologies for UWANs, including underwater acoustic channels (Chap. 9), UWAN MAC protocols (Chap. 10), UWAN routing protocols (Chap. 11), UWAN transfer reliability control covering both error control and end-to-end transmission control (Chap. 12), and UWAN security (Chap. 13). This part is mainly based on the author's surveys on the related topics [7, 8, 9, 10].

I hope that the book can become a useful resource for new learners, researchers, and practitioners in RWNs and UWANs.

Shanghai, China
January 2018

Shengming Jiang

References

1. Domingo, M. C.: An overview of the internet of underwater things. *J. Netw. Comput. Appl.* **35**(1), 1879–1890 (2012)
2. Smith, C., Collins, D.: *Wireless Networks: Design and Integration for LTE, EVDO, HSPA and WiMAX*, 3rd edn. McGraw-Hill Education (2014). ISBN 978-0071819831
3. Beard, C., Stallings, W.: *Wireless Communication Networks and Systems*. Pearson Education (2015). ISBN 978-0133594171
4. Agha, K.A., Pujolle, G., Yahiya, T.A.: *Mobile and Wireless Networks*. Wiley-ISTE (2016). ISBN 978-1848217140

5. Xiao, Y. (ed.): Underwater Acoustic Sensor Networks. Auerbach Publications (2010). ISBN 978-1420067118
6. Cui, J.H., Gerla, M., Zhou, Z., Peng, Z.: Underwater Wireless Networks: Principles, Protocols and Implementations. Wiley (2016). ISBN 978-1118465264
7. Lu, Q., Liu, F., Zhang, Y., Jiang, S.M.: Routing protocols for underwater acoustic sensor networks: a survey from an application perspective. In: Zak, A. (ed.) *Advances in Underwater Acoustics*, chapter 2. INTECH (2017). ISBN 978-953-51-3609-5
8. Jiang, S.M.: State-of-The-Art Medium Access Control (MAC) protocols for underwater acoustic networks: a survey based on A MAC reference model. *IEEE Commun. Surv. Tutorials* **20**(1) (2018)
9. Jiang, S.M.: On reliable data transfer in underwater acoustic networks: a survey from networking perspective. *IEEE Commun. Surv. Tutorials* **PP**(99) (2018)
10. Jiang, S.M.: Securing underwater acoustic networks: a survey. *IEEE Commun. Surv. Tutorials* Submitted. (2017)

Acknowledgements

I would like to take this opportunity to sincerely thank my following students who help me to complete this book by downloading references and drafting figures: Fan Chao, Zhang Peng, Gan Xiaolong (graduated in 2015); Qian Yanzhen, Wang Xiyang, Chen Huihui, Jiang Shuchao, Yang Fang, Yang Kaijian, Wu Shidong, and Zhang Kai (graduated in 2016); Liu Jie, Wang Yiliang, Lu Qian, Bao Zhijie, Dai Yuxi, and Cao Jun (graduated in 2017); Luo Jiawei, Li Yongfeng, Liu Haiyang, Li Fuyong, Zheng Tao, Zhang Shaofeng, Wang Fei, Xia Jie, and Wu Bi (to graduate in 2018).

This work is supported by the National Natural Science Foundation of China (NSFC) for the project “Basic theory of open network architecture for the marine Internet” under Grant 61472237.

Contents

1	Introduction and Overview	1
1.1	Typical Wireless Networks	1
1.1.1	Infrastructured Networks	2
1.1.2	Infrastructureless Networks	4
1.1.3	Network Deployment Spaces	11
1.1.4	Communication Media	13
1.2	Networking Fundamental Components	15
1.2.1	Networking Models	16
1.2.2	Networking Approaches	19
1.2.3	Networking Issues	21
1.2.4	Wired Networks Versus Wireless Networks	28
1.3	Summary	30
	References	30
 Part I Radio-Frequency Wireless Networks (RWNs)		
2	Error Control	35
2.1	Error Detection	36
2.1.1	Parity Check	36
2.1.2	Cyclic Redundancy Check (CRC)	36
2.2	Forward Error Correction (FEC)	38
2.2.1	Repetition Code	39
2.2.2	Hamming Code	39
2.3	Automatic Repeat ReQuest (ARQ)	43
2.3.1	Stop-and-Wait	43
2.3.2	Go-Back-N	46
2.3.3	Selective Repeat ARQ	47

2.4	FEC Versus ARQ	48
2.5	Summary	49
	References	49
3	Medium Access Control (MAC)	51
3.1	Fundamental Issues	51
3.1.1	Signal Collision	52
3.1.2	Capture Effect	52
3.1.3	Spatial Reuse	53
3.1.4	Hidden Terminals	53
3.1.5	Exposed Terminals	55
3.1.6	Energy Efficiency	55
3.1.7	Network Topologies	56
3.2	A MAC Reference Model	57
3.2.1	Operation Cycle	58
3.2.2	Medium Access Units	59
3.2.3	MAC Mechanisms	61
3.3	Categories of MAC Protocols	65
3.3.1	Multiplexing-Based Multiple Access Schemes	65
3.3.2	Contention-Based Protocols	70
3.3.3	Coordination-Based Protocols	70
3.4	Summary	72
	References	72
4	MAC Protocols for RWNs	75
4.1	Overview	75
4.2	ALOHA	75
4.2.1	Protocols	75
4.2.2	Performance Analysis	77
4.3	Carrier Sensing Multiple Access (CSMA)	79
4.3.1	Protocols	79
4.3.2	Performance Analysis	81
4.4	Busy Tone Multiple Access (BTMA)	84
4.5	Multiple Access Collision Avoidance (MACA)	85
4.5.1	Operational Conditions	85
4.5.2	Collision Scenarios	86
4.6	Floor Acquisition Multiple Access (FAMA)	87
4.7	MAC Protocol Standards	88
4.7.1	IEEE 802.11	88
4.7.2	High Performance Local Area Network (HIPERLAN)	92
4.7.3	Wireless Personal Area Networks (WPANs)	93
4.8	Summary	99
	References	99

5	Routing for RWNs	101
5.1	Overview	101
5.1.1	When to Relay	101
5.1.2	Implicitly and Explicit Routing	102
5.1.3	Unicast, Multicast and Broadcast	103
5.1.4	Routing Metrics	104
5.2	Basic Routing Protocols	104
5.2.1	Implicit Routing	104
5.2.2	Explicit Routing	107
5.2.3	Optimal Broadcast Routing	110
5.3	Routing in Mobile Ad Hoc Network (MANET)	113
5.3.1	Challenges	113
5.3.2	Loop Avoidance	114
5.3.3	Routing Strategies	116
5.4	Opportunistic Routing	118
5.4.1	Delay and Disruption Tolerant Network (DTN)	119
5.4.2	DTN on Top of Transport Layer	120
5.4.3	Challenges	120
5.5	De-Facto Standards for Routing Protocols	122
5.5.1	Dynamic Source Routing (DSR)	122
5.5.2	Ad Hoc On-Demand Distance Vector (AODV)	123
5.5.3	Optimized Link State Routing (OLSR)	125
5.5.4	Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)	127
5.5.5	Probabilistic Routing Protocol Using History of Encounters and Transitivity (PRoPHET)	131
5.5.6	Discussion	133
5.6	Summary	134
	References	135
6	End-to-End Transmission Control in RWNs	137
6.1	User Datagram Protocol (UDP)	137
6.2	Transmission Control Protocol (TCP)	138
6.2.1	Transmission Reliability Control	138
6.2.2	Flow Control	141
6.2.3	Congestion Control	142
6.3	TCP Standards	142
6.3.1	TCP Tahoe	142
6.3.2	TCP Reno	144
6.3.3	TCP NewReno	145
6.4	TCP for Multi-hop Mobile Networks	146
6.4.1	Challenging Issues	146
6.4.2	Splitting of TCP Connection	148

6.4.3	Precise Congestion Inference	149
6.4.4	Route Failure Notification	151
6.4.5	Congestion State Probing	153
6.4.6	MAC Contention Relief	154
6.4.7	ATM-like Control	156
6.4.8	Decoupling of TCP Functions	159
6.5	Discussion	163
6.5.1	End-to-End Semantics	163
6.5.2	Compatibility with TCP	163
6.5.3	Implementation Complexity	164
6.5.4	Evolution of TCP Research	164
6.6	Summary	165
	References	165
7	Mobility in RWNs	169
7.1	Horizontal Handoff	169
7.1.1	Handoff Policies	170
7.1.2	Handoff Initiation	171
7.1.3	Handoff Execution	174
7.2	Vertical Handoff	178
7.2.1	Handoff Scenarios	178
7.2.2	Handoff Operation	179
7.2.3	IEEE 802.21	180
7.3	Roaming	182
7.3.1	Overview	182
7.3.2	Roaming in GSM	183
7.3.3	Mobile IP	183
7.4	Grade of Service (GoS)	187
7.4.1	Approaches for Efficient Handoff	188
7.4.2	Handoff Without Priority	191
7.4.3	Queuing Handoff	192
7.4.4	Guard Channel (GC)	194
7.4.5	Distributed Call Admission Control (DCAC)	195
7.5	Summary	199
	References	200
8	Network Security in RWNs	203
8.1	Overview	203
8.1.1	Typical Targets Under Attack	203
8.1.2	Basic Network Security	205
8.1.3	Wireless Network Security	205
8.2	Security Primitives	206
8.2.1	Cryptography	206
8.2.2	Key Management	207

8.2.3	Hash Functions	207
8.2.4	Digital Signature	208
8.2.5	Digital Certificate	209
8.2.6	Virtual Private Network (VPN)	209
8.3	Standards for Network Security	211
8.3.1	Authentication Systems	211
8.3.2	Transport Layer Security	213
8.3.3	Network Layer Security	214
8.3.4	Link Layer Security	215
8.4	Standards for Securing Wireless Links	218
8.4.1	IEEE 802.11	219
8.4.2	WiFi Protected Access (WPA)	221
8.4.3	IEEE 802.11i	223
8.5	Summary	228
	References	228

Part II Underwater Wireless Acoustic Networks (UWANs)

9	Overview of Underwater Acoustic Communication	233
9.1	Underwater Acoustic Environments	233
9.2	Peculiar Features of Underwater Acoustic Channels	234
9.2.1	Long and Changing Propagation Delays	234
9.2.2	Primary Characteristics	237
9.2.3	Technological and Operational Limitations	241
9.3	Summary	243
	References	243
10	MAC for UWANs	245
10.1	Overview	245
10.2	Challenges and Categories	246
10.2.1	Medium Utilization	246
10.2.2	Energy Efficiency	246
10.2.3	Quality of Service (QoS)	247
10.2.4	Mobility	247
10.2.5	Fairness	247
10.2.6	Protocol Validation	247
10.2.7	Classification of UWAN MAC Protocols	248
10.3	UWAN MAC Based on RWN Protocols	248
10.3.1	Multiplexing Access Protocols	249
10.3.2	MAC Protocols Without Multiplexing	256
10.4	Newly Designed UWAN MAC Protocols	261
10.4.1	Reservation-Based MAC Protocols	262
10.4.2	Scheduling-Based MAC Protocols	267
10.4.3	Cross-Layer Designed Protocols	274

10.5	Discussion	280
10.6	Summary	281
	References	282
11	Routing in UWANs	287
11.1	Overview	287
11.1.1	Primary Challenges	287
11.1.2	Protocol Category	288
11.2	Stationary Sinks	292
11.2.1	Relative Position-Based Routing	292
11.2.2	Priority Routing	295
11.2.3	Asymmetric Link Connectivity	296
11.2.4	Multipath Routing	297
11.2.5	Cross-Layer Design	298
11.3	Mobile Sinks	300
11.3.1	Routing in 3D UWANs	300
11.3.2	Sector-Based Routing	301
11.3.3	Multiple Mobile Sinks	302
11.4	No Specified Sinks	303
11.4.1	Non Line-of-Sight (NLOS)	303
11.4.2	Routing for Wave Gliders	304
11.4.3	Season-Adaptive Routing	305
11.4.4	Smart Routing Protocols	306
11.5	Discussion	309
11.6	Summary	311
	References	311
12	Transfer Reliability Control in UWANs	315
12.1	Overview	315
12.2	Reliable Transfer Architecture	316
12.2.1	Link-Level Functions	317
12.2.2	Path-Level Functions	317
12.2.3	Typical Error Control Schemes	317
12.3	Data Link Layer	318
12.3.1	Enhanced SW-ARQ	319
12.3.2	Enabling of SR-ARQ	320
12.3.3	Hybrid-ARQ (HARQ)	321
12.4	Network Layer	323
12.4.1	Fountain Codes	323
12.4.2	Network Coding	325
12.4.3	Cooperative Transmissions	328
12.4.4	Reliable Broadcast	329
12.5	Transport Layer	331

12.6	Discussion	332
12.7	Summary	333
	References	333
13	Security in UWANs	337
13.1	Cryptographic Primitives for UWANs	337
13.1.1	Challenges to Popular Cryptographic Primitives	338
13.1.2	Symmetric Key for Reciprocal Channels	339
13.1.3	Public Key with Elliptic Curve Cryptography (ECC).	342
13.1.4	Digital Signature	342
13.1.5	Reputation-Based Authentication	343
13.2	Security Threats in UWANs	345
13.2.1	Environmental Factors	346
13.2.2	Physical Layer Attacks	347
13.2.3	Link Layer Attacks	348
13.2.4	Network Layer Attacks	352
13.2.5	Transport Layer Attacks	353
13.3	Countermeasures Against Typical Threats	353
13.3.1	Against Signal Eavesdropping	354
13.3.2	Countermeasures Against Wormhole Attack.	356
13.3.3	Attack-Resilient Routing	358
13.3.4	A Cryptographic Suite	360
13.4	Discussion	362
13.5	Summary	363
	References	364
	Appendix A: Formulas for Some Queueing Systems	369
	Appendix B: RSA Cryptosystem	375
	Index	377

Acronyms

3GPP	Third Generation Partnership Project, 176 ¹
AAA	Authentication, Authorization and Accounting, 208
ABE	Available bandwidth estimator, 156
ABR	Associativity-based routing, 149
ACK	Acknowledgement, 22
ADA	Adaptive delayed acknowledgement, 154
AES	Advanced Encryption Standard, 221
AIFS	Arbitration IFS, 88
AIMD	Additive increase and multiplicative decrease, 141
AKM	Authenticated key management, 226
ANC	Analog network coding, 349
AOA	Angle of arrival, 281
AODV	Ad hoc on-demand distance vector, 114
AP	Access point, 2
ARQ	Automatic Repeat reQuest, 22
ATCP	Ad hoc TCP, 155
ATM	Asynchronous transfer mode, 19
ATP	Ad hoc transport protocol, 155
AVP	Attribute–value pair, 200
AUV	Autonomous underwater vehicle, 12
AUC	Authentication center, 181
BER	Bit error rate, 60
BCH	Bose–Ray–Chaudhuri–Hocquenghem, 34
BO	Backoff, 59
BP	Beacon period, 91
BPSK	Binary phase shift keying, 351
BSC	Base station controller, 172
BSS	Basic service set, 216

¹ It is the number of the page on which the corresponding acronym first appears.

BSS	Base station subsystem, ² 173
BTMA	Busy tone multiple access, 82
BTS	Base transceiver station, 172
BU	Binding update, 185
B-ACK	Block acknowledgement, 93
CA	Certificate authority, 204
CA	Collision avoidance, 72
CA	Congestion avoidance, 140
CAC	Call admission control, 186
CAP	Contention access period, 20
CBP	Call blocking probability, 186
CBR	Constant bit rate, 78
CC	Channel carrying, 186
CCH	Control channel, 78
CCMP	CCM protocol, 224
CCMP	Counter mode with CBC-MAC protocol, 222
CCP	Call completion probability, 186
CD	Collision detection, 73
CDM	Code division multiplexing, 27
CDMA	Code division multiple access, 59
CDP	Call dropping probability, 185
CFP	Contention-free period, 92
CHAP	Challenge plus response pair, 209
CIR	Carrier-to-interference ratio, 169
CL	Connectionless, 19
CO	Connection-oriented, 19
CoA	Care-of-address, 183
COPAS	Contention-based path selection, 154
CR	Communication round, 159
CRC	Cyclic redundancy check, 22
CS	Carrier sensing, 58
CSI	Channel state information, 240
CSMA	Carrier Sensing Multiple Access, 59
CSMA/CD	CSMA with collision detection, 253
CTR	Counter mode, 224
CTS	Ciphertext stealing, 356
CTS	Clear-to-Send, 52
CW	Contention window, 252
cwnd	Congestion window, 138
DAG	Directed acyclic graph, 322
DBF	Distributed Bellman Ford, 103
DCAC	Distributed CAC, 186

² An acronym may refer to different definitions.

DCC	Dedicated control channel, 64
DCCP	Datagram congestion control protocol, 137
DCF	Distributed coordination function, 88
DCH	Data channel, 84
DCA	Dynamic channel allocation, 188
DDoS	Distributed DoS, 204
DIFS	DCF IFS, 89
DoA	Direction of arrival, 356
DoS	Denial of service, 204
DP	Data period, 97
DRP	Distributed reservation protocol, 97
DSDV	Destination-sequenced distance vector, 115
DSN	Destination sequence number, 124
DSR	Dynamic source routing, 117
DSSS	Direct-sequence SS, 60
DTLS	Datagram transport layer security, 212
DTN	Delay- and disruption-tolerant network, 11
EAP	Extensible Authentication Protocol, 215
EAPOL	EAP Over LANs, 216
ECAES	Elliptic curve authenticated encryption scheme, 342
ECC	Elliptic curve cryptography, 342
ECDLP	Elliptic curve discrete logarithm problem, 342
ECDSA	Elliptic curve digital signature algorithm, 342
ECN	Explicit congestion notification, 156
EIFS	Extended IFS, 90
ELFN	Explicit link failure notification, 151
ESP	Encapsulating security payload, 215
ETSI	European Telecommunication Standards Institute, 2
EU	European Union, 92
FAMA	Floor acquisition multiple access, 54
FCA	Fixed channel allocation, 188
FCC	Federal Communications Commission, 96
FCS	Frame check sequence, 38
FDD	Frequency-division duplex, 319
FDM	Frequency-division multiplexing, 60
FDMA	Frequency-division multiple access, 63
FEC	Forward error control, 21
FFD	Full function device, 94
FHSS	Frequency-hopping SS, 60
FIFO	First in, first out, 247
FS	Frame sensing, 62
FTP	File transfer protocol, 137
GC	Guard channel, 188
GEO	Geostationary Earth orbit, 4
GKH	Group key handshake, 226

GoS	Grade of service, 187
GSM	Global system for mobile communication, 20
GTK	Group temporal key, 226
GTS	Guaranteed time slot, 94
HARQ	Hybrid ARQ, 321
HiperLAN	High-performance radio local area network, 2
HLR	Home location register, 175
HMAC	Keyed-Hashing for Message Authentication, 214
HS	Handshaking, 62
ICI	Interchannel interference, 275
ICV	Integrity check value, 223
ID	Identity, 105
IETF	Internet Engineering Task Force, 117
IFS	Interframe space, 89
IP	Internet Protocol, 80
IPN	Interplanetary Internet, 11
IPSec	IP security, 187
IPv4	IP version 4, 23
IRTF	Internet Research Task Force, 117
ISDN	Integrated service data network, 27
ISI	Intersymbol interference, 239
ISM	Industrial, scientific, medical, 30
ISO	International Organization for Standardization, 16
ITCP	Indirect TCP, 148
ITS	Intelligent transportation system, 9
IV	Initialization vector, 220
JTCP	Jitter-based TCP, 149
KCK	Key confirmation key, 227
KEK	Key encryption key, 227
L3MP	Layer 3 or higher mobility protocol, 181
LAN	Local area network, 54
LBL	Long baseline, 239
LDPC	Low-density parity-check code, 38
LED	Light-emitting diode, 14
LEO	Low Earth orbit, 4
LLC	Logical link control, 61
LOS	Line-of-sight, 14
LT	Luby transform code, 324
LTE	Long-term evolution, 3
MAC	Medium access control, 17
MACA	Multiple access collision avoidance, 54
MACsec	IEEE 802.1AE MAC security protocol, 217
MAHO	Mobile-assisted handoff, 175
MAI	Multiple access interference, 252
MANET	Mobile ad hoc network, 5

MAS	Medium access slot, 96
MAU	Medium access unit, 57
MCHO	Mobile-controlled handoff, 175
ME	Messaging, 62
MEO	Medium Earth orbit, 4
MF	MAC frame, 58
MFSK	Multi-frequency shift keying, 253
MIC	Message integrity code, 225
MIH	Media-independent handover, 180
MIHF	MIH function, 180
MIMO	Multi-input–multi-output, 275
MM	MAC mechanism, 58
MPDU	MAC protocol data unit, 224
MPR	Multipoint relay, 125
MS	Mini-slot, 58
MSC	Mobile switching center, 175
MSDU	MAC service data unit, 224
MSR	Mobility support router, 148
MSS	Maximum segment size, 142
NAS	Network access server, 211
NAV	Network allocation vector, 91
NCC	Non-channel-carrying, 190
NCHO	Network-controlled handoff, 175
NDP	Neighbor discovery protocol, 187
NF	Notification packet, 263
NH	Next hop, 109
NIC	Network interface card, 216
NLOS	Non-line-of-sight, 303
NSS	Network and switching subsystem, 175
OC	Operation cycle, 57
OFDM	Orthogonal FDM, 60
OFDMA	Orthogonal FDMA, 252
OLSR	Optimized link state routing, 125
OSI	Open system interconnection, 316
OSS	Operation subsystem, 175
PAN	Personal area network, 93
PAP	Password pair, 212
PCA	Prioritized contention access, 97
PCF	Point coordination function, 88
PCS	Personal communication system, 176
PDA	Personal digital assistant, 3
PIFS	PCF IFS, 89
PKI	Public key infrastructure, 207
PMK	Pairwise master key, 226
PO	Polling, 62

PPK	Per-packet key, 222
PPP	Point-to-point protocol, 212
PR	Prioritization, 64
PRMA	Packet reservation multiple access, 60
PRoPHET	Probabilistic Routing Protocol using History of Encounters and Transitivity, 121
PSK	Pre-shared key, 222
PTK	Pairwise transient key, 226
PTSP	Partial tree-sharing protocol, 128
QoS	Quality of Service, 26
RA	Registration authority, 207
RADIUS	Remote Access Dial-in-User Service, 211
RC4	Rivest cipher 4, 220
RD	Route discovery, 122
RE	Reservation, 62
RED	Random early dropping, 25
RERR	Route error, 125
RFC	Request for comments, 117
RFD	Reduced function device, 94
RFN	Route failure notification, 152
RI-BTMA	Receiver-initiated BTMA, 84
RL	Reinforcement learning, 306
RM	Route maintenance, 122
RN	Reported node set, 129
RREP	Route reply, 123
RREQ	Route request, 123
RRN	Route re-establishment notification, 152
RRP	Route request packet, 122
RS	Reed–Solomon, 38
RSA	Ron Rivest, Adi Shamir and Leonard Adleman, 375
RSNA	Robust Security Network Association, 223
RSS	Received signal strength, 171
RSS	Radio subsystem, 175
RT	Reported subtree, 130
RTT	Round-trip time, 79
RTO	Retransmission timeout, 138
RTS	Request-to-Send, 54
rwin	Receiver window, 141
RWN	Radio wireless network, 337
RWN	RF wireless network, 29
SA	Slot access, 61
SACK	Selective ACK, 157
SAK	Secure association key, 217
SAP	Service access point, 181
SC	Scheduling, 62

SC	Shadow cluster, 188
SCTP	Stream control transmission protocol, 134
SI	Signaling, 59
SIC	Successive interference cancellation, 273
SIFS	Short IFS, 83
SIR	Signal-to-interference ratio, 189
SISO	Single-input–single-output, 174
SL	Slot, 56
SN	Sequence number, 113
SNIR	Signal-to-noise-plus-interference noise ratio, 341
SNR	Signal-to-noise ratio, 14
SS	Slow start, 140
SS	Spread spectrum, 54
SSH	Secure shell, 134
SSID	Service set identifier, 216
SSL	Secure socket layer, 211
ST-CG	Spatiotemporal conflict graph, 264
S-FAMA	Slotted FAMA, 255
TBRPF	Topology dissemination based on reverse path forwarding, 118
TC	Topology control, 123
TCP	Transmission control protocol, 18
TCP-AP	TCP with adaptive pace, 153
TCP-DCR	Delayed congestion response TCP, 146
TCP-F	TCP with feedback, 149
TDD	Time-division duplex, 314
TDM	Time-division multiplexing, 54
TDMA	Time-division multiple access, 59
TKIP	Temporal key integrity protocol, 219
TLS	Transport layer security, 210
TS	Time slot, 53
TSC	TKIP sequence counter, 222
TTL	Time-to-live, 120
UDP	User datagram protocol, 134
ULB	Underwater locator beacon, 234
URI	Uniform resource identifier, 116
UUV	Unmanned underwater vehicle, 12
UWAN	Underwater wireless acoustic network, 25
UWB	Ultra-wideband, 6
UWSN	Underwater wireless sensor network, 12
VANET	Vehicular ad hoc network, 10
VLR	Visitor location register, 272
VoIP	Voice over IP, 176
VPN	Virtual private network, 184
WAP	Wireless access protocol, 213
WBAN	Wireless body area network, 6

WEP	Wired equivalent privacy, 216
WiMAX	Worldwide Interoperability for Microwave Access, 4
WLAN	Wireless local area network, 2
WMAN	Wireless metropolitan area network, 3
WMN	Wireless mesh network, 8
WPA	Wi-fi Protected Access, 216
WPAN	Wireless personal area network, 6
WSN	Wireless sensor network, 8
WTLS	Wireless transport layer security, 213
WWAN	Wireless wide area network, 176

List of Figures

Fig. 1.1	A wireless local area network (WLAN)	2
Fig. 1.2	A mobile cellular network.	3
Fig. 1.3	A metropolitan area network based on WiMAX.	4
Fig. 1.4	Category of satellites according to earth orbit sizes.	5
Fig. 1.5	A mobile ad hoc network (MANET)	6
Fig. 1.6	An ad hoc wireless network: Bluetooth.	7
Fig. 1.7	A wireless body area network (WBAN)	7
Fig. 1.8	A wireless mesh network (WMN).	8
Fig. 1.9	A wireless sensor network for fire alarm system in forest.	9
Fig. 1.10	An opportunistic network	10
Fig. 1.11	A vehicular ad hoc network (VANET)	10
Fig. 1.12	A conceived interplanetary Internet (IPN).	11
Fig. 1.13	An underwater wireless network	12
Fig. 1.14	Electromagnetic spectrum suitable for wireless communication	13
Fig. 1.15	Infrared and visible light based WLANs.	14
Fig. 1.16	An LED-based optical network.	15
Fig. 1.17	Schematic illustration of a communication network [9].	16
Fig. 1.18	The open system interconnection reference model of ISO [9].	17
Fig. 1.19	Layered networking model: ISO versus TCP/IP [9]	18
Fig. 1.20	Shared-media networks versus switched networks [9].	19
Fig. 1.21	Connectionless networks versus connection-oriented networks [9]	20
Fig. 1.22	Circuit switching versus packet switching [9].	21
Fig. 1.23	Transmission error of physical signals [9].	21
Fig. 1.24	Traffic situation on a crossroad versus MAC.	22
Fig. 1.25	Routing versus switching	23
Fig. 1.26	Flow control: hop-by-hop versus end-to-end [9]	24
Fig. 1.27	Congestion control scenarios [9].	25
Fig. 1.28	End-to-end transmission control [9]	26

Fig. 1.29	Example of network security threats	27
Fig. 1.30	Mobility support	28
Fig. 2.1	Example on polynomial division and checksum calculation.	37
Fig. 2.2	Example of Hamming code and grouping.	40
Fig. 2.3	Example of error correction with Hamming code	41
Fig. 2.4	Construction of the Hamming codeword.	41
Fig. 2.5	Stop-and-Wait protocol	44
Fig. 2.6	Diagram of Stop-and-Wait protocol for analysis	44
Fig. 2.7	Time interval between successive frames positively acknowledged (t_v) with Stop-and-Wait	45
Fig. 2.8	Go-back-N protocol.	46
Fig. 2.9	Time interval between successive frames positively acknowledged (t_v) with Go-back-N.	47
Fig. 2.10	Selective Repeat ARQ protocol.	48
Fig. 3.1	Signal collision	52
Fig. 3.2	Capture effect and spatial reuse.	53
Fig. 3.3	Hidden terminal problem.	54
Fig. 3.4	Exposed terminal problem.	55
Fig. 3.5	Typical network topologies [8]	56
Fig. 3.6	A reference model for MAC protocols [8]	58
Fig. 3.7	Relationship between the MAC protocol components [8]	58
Fig. 3.8	Guard time setting for collision-free reception with TDMA [8].	67
Fig. 3.9	Example of frequency hopping	68
Fig. 3.10	Polling versus token-passing	71
Fig. 4.1	ALOHA versus slotted ALOHA	76
Fig. 4.2	Diagram for ALOHA modeling [1].	77
Fig. 4.3	Condition for a successful frame transmission with ALOHA	78
Fig. 4.4	CSMA variants	80
Fig. 4.5	Principle of CSMA/CA (non-persistent CSMA)	81
Fig. 4.6	Time division of MAC operation for non-persistent CSMA.	82
Fig. 4.7	Time division for slotted non-persistent CSMA	84
Fig. 4.8	Principle of busy tone multiple access (BTMA) protocol	85
Fig. 4.9	Basic operational conditions of MACA.	86
Fig. 4.10	Collision without hidden terminal	86
Fig. 4.11	Collision with hidden terminal	87
Fig. 4.12	CST setting with FAMA [9]	88
Fig. 4.13	Overview of the IEEE 802.11 MAC protocol stack [10].	89
Fig. 4.14	Superframe structure for the co-existing of PCF and DCF modes [10].	89
Fig. 4.15	IFS structure for the IEEE 802.11 MAC protocol [10]	90

Fig. 4.16	CSMA/CA for the IEEE 802.11 DCF mode [10]	91
Fig. 4.17	RTS/CTS/DATA/ACK process in the IEEE 802.11 DCF mode [10].	92
Fig. 4.18	Principle of the HIPERLAN MAC protocol [11]	93
Fig. 4.19	Network topologies for IEEE 802.15.4 [12]	94
Fig. 4.20	Superframe structure for IEEE 802.15.4 [12]	95
Fig. 4.21	Principle of slotted CSMA/CA in IEEE 802.15.4 [12]	95
Fig. 4.22	Principle of non-slotted CSMA/CA in IEEE 802.15.4 [12].	96
Fig. 4.23	UWB mask defined by FCC of USA [13]	96
Fig. 4.24	Superframe structure defined by ECMA-368 [13].	97
Fig. 4.25	IFS structure defined by ECMA-368 [13].	98
Fig. 4.26	RTS-CTS-frames-ACK handshake defined by ECMA-368 [13].	99
Fig. 5.1	Scenarios for packet forwarding in wireless networks.	102
Fig. 5.2	A routing protocol classification	105
Fig. 5.3	An example of a flooding routing protocol	106
Fig. 5.4	Local adaptive routing in node 4	107
Fig. 5.5	Example of a fixed routing implementation.	108
Fig. 5.6	Routing table and updating process in node 1 with DBF.	110
Fig. 5.7	Spanning trees rooted at nodes 2 (solid line) and 4 (dashed line) with the shortest paths to each node	111
Fig. 5.8	Forwarding of a packet initiated by node 2 with reverse path forwarding.	112
Fig. 5.9	Forwarding of a packet initiated by node 2 with extended reverse path forwarding.	112
Fig. 5.10	An example of routing loop generation with DBF	115
Fig. 5.11	Course of loop generation with DBF and principle of loop avoidance with DSDV	116
Fig. 5.12	Summary on routing protocols for MANETs	117
Fig. 5.13	Example of opportunistic routing [12].	119
Fig. 5.14	Route discovery procedure of DSR.	123
Fig. 5.15	Route discovery procedure of AODV	124
Fig. 5.16	An example for MPR [22]	126
Fig. 5.17	Principle of PTSP and reported node set (RN) computation of TBRPF	130
Fig. 5.18	$P_{encounter}$ as function of time interval (I) between updates [15]	132
Fig. 6.1	Internet protocol stack and typical applications.	138
Fig. 6.2	TCP acknowledgement scheme.	139
Fig. 6.3	Difficult situation for accurate RTT measurement [2]	140
Fig. 6.4	Slide window for flow control in TCP	141

Fig. 6.5	Congestion window manipulation with TCP Tahoe and TCP Reno	143
Fig. 6.6	Fast retransmission with TCP Tahoe.	144
Fig. 6.7	TCP Reno in the case of multiple losses in one cwnd	145
Fig. 6.8	Factors leading to misjudgement on congestion status in multi-hop mobile networks	147
Fig. 6.9	Principle of indirect TCP (ITCP) [10].	148
Fig. 6.10	Protocol stack for the end-to-end TCP connection with ITCP [10]	148
Fig. 6.11	The TCP-F state machine [23]	152
Fig. 6.12	Principle of TCP-AP.	155
Fig. 6.13	Maximum throughput of TCP ($\frac{L}{\tau} = 1$) versus p and n [47].	160
Fig. 6.14	Displacement of congestion control function for a connection consisting of TCP and Semi-TCP [58].	162
Fig. 7.1	Inter-cell handoff versus intra-cell handoff	170
Fig. 7.2	Hard handoff.	170
Fig. 7.3	Seamless handoff.	171
Fig. 7.4	Soft handoff	171
Fig. 7.5	A handoff trigger process based on RSS.	172
Fig. 7.6	Handoff initiation without delay [7]	173
Fig. 7.7	Handoff initiation with delay [7].	173
Fig. 7.8	System structure for mobility support in GSM [6]	175
Fig. 7.9	Vertical handoff scenarios	179
Fig. 7.10	General MIH function (MIHF) reference model and service access points (SAPs) [4]	181
Fig. 7.11	Types of MIHF relationship [4]	182
Fig. 7.12	Roaming effect on user connectivity	184
Fig. 7.13	Assignment of care-of-address (CoA) in mobile IPv4.	185
Fig. 7.14	Packet forwarding with triangle routing and tunnelling.	186
Fig. 7.15	A queuing system for new calls and handoff calls without priority	191
Fig. 7.16	State-transition without priority for handoff calls	192
Fig. 7.17	Queuing handoff calls	193
Fig. 7.18	State-transition for queuing handoff calls	193
Fig. 7.19	Diagram of the guard channel scheme	194
Fig. 7.20	State-transition with guard channels for handoff calls	194
Fig. 7.21	Hypothetical topology of one-dimensional cellular networks	195
Fig. 7.22	2D cellular network: Adjacent Cell (AC), Farthest Interference Cell (FIC), Nearest Non-Interference Cell (NNIC) and Effective Interfering Area (EIA) [41].	197
Fig. 8.1	Wireless and wired environments for network security	206
Fig. 8.2	Example on encryption and decryption	206

Fig. 8.3	Construction of a hash function [5].	208
Fig. 8.4	Principle of digital signature	209
Fig. 8.5	Principle of digital certificate	210
Fig. 8.6	Tunneling for virtual private network (VPN)	210
Fig. 8.7	Standards for network security [6]	211
Fig. 8.8	Controlled-port network access components and processes [23].	217
Fig. 8.9	Overview of MACsec architecture [25].	218
Fig. 8.10	Encryption and decryption of the WEP frame.	220
Fig. 8.11	Integrity protection with WEP.	221
Fig. 8.12	Parameters for message integrity code (MIC) [29]	224
Fig. 8.13	Key mixing [29]	225
Fig. 8.14	MPDU formats for TKPI [29].	225
Fig. 8.15	Pairwise key architecture [29].	227
Fig. 8.16	Discovery and negotiation diagram [29]	228
Fig. 9.1	Underwater propagation environments for underwater acoustic channels.	234
Fig. 9.2	Example of spatio-temporal uncertainty with slotted access [5]	236
Fig. 9.3	Underwater channel characteristics versus frequency.	238
Fig. 10.1	A classification of the reviewed UWAN MAC protocols	248
Fig. 10.2	Principle of a TDMA-based MAC protocol	250
Fig. 10.3	Tipple hidden terminal problem due to large propagation delay [1, 33]	254
Fig. 10.4	Guard time setting for S-ALOHA in UWANs [1].	257
Fig. 10.5	Principle of CS-MAC and PCAP [20]	258
Fig. 10.6	Collision between RTS and data frames with the original FAMA [1, 24].	259
Fig. 10.7	Principle of S-FAMA [1, 24]	259
Fig. 10.8	A communication round for single hop in COD-TS [1, 53]	263
Fig. 10.9	The 4-way handshaking with multiple node polling in RIPT [59]	264
Fig. 10.10	Synchronous T-Lohi versus asynchronous T-Lohi [1, 34].	266
Fig. 10.11	Conflict relationship in ST-CG for ST-MAC [1, 26].	268
Fig. 10.12	An example on a routing topology and the corresponding ST-CG for ST-MAC [26]	268
Fig. 10.13	Example on coloring operation with TOTA for possible transmissions on the first time slot with a trial carried out for each link (i.e., vertex) corresponding to an ST-CG [61]	270
Fig. 10.14	Concurrent transmission with DOTS: multi-sender to multi-receiver [54]	272
Fig. 10.15	Basic idea of the UAN-MAC protocol [1, 55]	273

Fig. 10.16	Principle of Zigzag decoding [1, 66].	276
Fig. 10.17	Basic idea of the FDA protocol [70].	276
Fig. 10.18	The sequence diagram of 1D CT-MAC: solid lines refer to transmitted packets and dash lines represents received packets [27].	277
Fig. 10.19	TFO-MAC: fixed channel assignment with OFDM [28].	278
Fig. 10.20	TFO-MAC: dynamic channel assignment with OFDM [1, 28].	279
Fig. 11.1	Phero-Trail location service protocol for SEA swarm [15]: a As the mobile sink moves, it sends location updates to the mobile nodes on the hull; b A query is forwarded to the node holding the current location of the mobile sink along the trail	290
Fig. 11.2	Principle of vector-based-forwarding (VBF) [11]	293
Fig. 11.3	Depth-based routing (DBR) [16].	294
Fig. 11.4	Void-aware pressure routing (VAPR): recovery mode of the local maximum node [1].	295
Fig. 11.5	An example of priority routing [14]	296
Fig. 11.6	Scenarios for asymmetric link connectivity [22–24]	297
Fig. 11.7	An example of focused beam routing (FBR) [32].	299
Fig. 11.8	3D ZOR (ZOR^3) and 3D ZOF (ZOF^3) for Mobicast protocol [34].	301
Fig. 11.9	Forwarder selection at the sender with SBR-DLP [35]	302
Fig. 11.10	Non line-of-sight routing via surface reflection [38]	303
Fig. 11.11	Regional routing versus point routing [17]	304
Fig. 11.12	Example of a season-adaptive routing [13]	305
Fig. 11.13	Framework of reinforcement learning (RL) [41]	306
Fig. 11.14	An example of Q-learning for routing [39, 42].	308
Fig. 12.1	A general architecture for end-to-end transfer reliability control [7].	316
Fig. 12.2	Typical error control schemes [7]	318
Fig. 12.3	Transmission flow with JSW [16].	320
Fig. 12.4	Principle of the underwater selective repeat (USR) protocol with $M = 4$ ($\tau = 4T_d$, $\delta = 0.5T_d$, $W = 1.5T_d$, $T_a = 0.5T_d$) [20].	321
Fig. 12.5	Type-I HARQ in UWANs for sending window equal to 6 ($M = 6$) [7, 22].	322
Fig. 12.6	Type-II HARQ in UWANs for $M = 6$ [7, 22]	323
Fig. 12.7	Example of LT decoding process [24]	324
Fig. 12.8	Coding versus no coding in the network: an edge can transmit only one packet once [5].	326
Fig. 12.9	Routing pipe for network coding [28].	327
Fig. 12.10	Cooperative regions for one-hop and multi-hop UWANs [34].	329

Fig. 12.11 Principle of reliable broadcast based on SRB 330

Fig. 13.1 Principle of symmetric key generation in reciprocal
channels [11]. 339

Fig. 13.2 Symmetric key generation for reciprocal channels
with OFDM 340

Fig. 13.3 Structure of the ARTMM reputation model 344

Fig. 13.4 A default security threat scenario [11]. 346

Fig. 13.5 Diagram of jamming attacks 348

Fig. 13.6 Diagram of replay attack [38] 349

Fig. 13.7 Diagram of wormhole attack [11, 38] 350

Fig. 13.8 Diagram of Sybil attack [11, 38]. 351

Fig. 13.9 Diagram of man-in-the-middle attacks. 353

Fig. 13.10 System model for J-ANC [8] 355

Fig. 13.11 Wormhole detection with DoA estimation [60]. 357

Fig. 13.12 Key chain for group key management [3, 11]. 361

Fig. 13.13 Key tree for group key management [3] 362

List of Tables

Table 1.1	Comparison between radio, optical and acoustic media for underwater communication	15
Table 1.2	QoS requirements of typical applications [16]	26
Table 1.3	Wired networks versus wireless networks.	29
Table 2.1	Example of FEC using triplet modular redundancy	39
Table 2.2	Parity check group calculation of the Hamming codeword for ASCII code.	42
Table 2.3	Comparison between FEC and ARQ [12].	48
Table 3.1	Characteristics of MAC mechanisms and multiplexing-based access schemes [8]	62
Table 3.2	Decoding of node A's signal from the multiplexing of A and B	70
Table 4.1	Typical MAC protocols in the context of the MAC reference model (Fig. 3.6) [2].	76
Table 5.1	Summary of the RFCs for routing protocols.	133
Table 6.1	Major causes of reception failure in multi-hop mobile networks.	147
Table 7.1	IEEE 802.11 WLANs versus GSM cellular networks.	177
Table 8.1	Wireless networks versus wired networks for network security.	205
Table 9.1	RWNs versus UWANs.	243
Table 10.1	Modified popular RWN MAC protocols.	249
Table 10.2	New UWAN MAC protocols	262
Table 11.1	Typical application scenarios of UWAN routing protocols and proposals	289
Table 12.1	Typical schemes for link-level reliability control	332
Table 12.2	Typical schemes for path-level reliability control	332

Table 13.1 Key lengths (bits) for equivalent security with typical
cipher schemes [11, 24] 342

Table 13.2 Signature size, generation time and authentication
overhead [11, 29] 343

Table 13.3 Network security with the layered network
architecture [11, 37] 346