Wireless Networking Principles: From Terrestrial to Underwater Acoustic

Shengming Jiang

Wireless Networking Principles: From Terrestrial to Underwater Acoustic

Springer

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

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 enfant 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 Shengming Jiang
January 2018

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., Yahiha, 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

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-inference 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 graphic, 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 **R**ivest, Adi **S**hamir and Leonard **A**dleman, 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

List of Tables