

---

# WIRELESS AND MOBILE DATA NETWORKS

---

AFTAB AHMAD

 WILEY-  
INTERSCIENCE

A JOHN WILEY & SONS, INC., PUBLICATION



# WIRELESS AND MOBILE DATA NETWORKS



---

# WIRELESS AND MOBILE DATA NETWORKS

---

AFTAB AHMAD

 WILEY-  
INTERSCIENCE

A JOHN WILEY & SONS, INC., PUBLICATION

Copyright © 2005 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.  
Published simultaneously in Canada.

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, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at [www.copyright.com](http://www.copyright.com). Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

**Limit of Liability/Disclaimer of Warranty:** While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at [www.wiley.com](http://www.wiley.com).

***Library of Congress Cataloging-in-Publication Data:***

Ahmad, Aftab, 1961–

Wireless and mobile data networks / Aftab Ahmad.

p. cm.

Includes bibliographical references.

ISBN-13 978-0-471-67075-9 (cloth)

ISBN-10 0-471-67075-8 (cloth)

1. Wireless communication systems. 2. Mobile communication systems. 3. Computer networks. I. Title.

TK5103.2.A43 2005

621.382—dc22

2004025911

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

To Mahmooda





# CONTENTS

---

<b>PREFACE</b>	<b>xxv</b>
<b>ACKNOWLEDGMENTS</b>	<b>xxix</b>
<b>1. WIRELESS DATA—INTRODUCTION</b>	<b>1</b>
1.1. Wireless Voice / 2	
1.1.1. Fixed Minimum Bandwidth / 2	
1.1.2. Vague Definition of Service Quality / 3	
1.1.3. Delay Requirements / 4	
1.2. Wireless Local Area Networks (WLANs) / 5	
1.2.1. Ad Hoc WLAN / 5	
1.2.2. Infrastructure WLAN / 6	
1.3. Wide Area Cellular Networks / 7	
1.4. Fixed Wireless Networks / 8	
1.5. Personal Area Networks / 10	
1.6. Satellite-Based Data Networks / 10	
1.7. Mobile IP / 12	
1.8. The Wireless Spectrum / 13	
1.8.1. Licensed and License-Free Bands / 14	
1.8.2. Low-Power Wireless Data Systems / 14	
1.8.3. Ultra-Wide Band (UWB) / 14	
1.8.4. The ISM Band / 15	

- 1.8.5. U-NII Spectrum / 16
- 1.8.6. Cellular Systems' Spectrum / 16
- 1.8.7. Fixed Wireless Systems / 17
- 1.8.8. Wireless Metropolitan Area Networks (WMAN) / 20
- 1.8.9. Satellite Data Communications / 20
- References / 21

**2. REFERENCE ARCHITECTURES FOR WIRELESS DATA NETWORKS**

- 2.1. Bluetooth™ / 24
  - 2.1.1. Bluetooth Radio / 25
  - 2.1.2. Baseband Layer / 26
  - 2.1.3. Link Management Protocol (LMP) / 26
  - 2.1.4. Logical Link Control and Adaptation Protocol Layer (L2CAP) / 26
  - 2.1.5. Bluetooth Profiles / 26
    - 2.1.5.1. *Generic Access Profile (GAP)* / 26
    - 2.1.5.2. *Service Discovery Application Profile (SDAP)* / 27
- 2.2. IEEE 802.11 / 27
  - 2.2.1. Physical Layer (PHY) / 29
    - 2.2.1.1. *Physical Medium Dependent (PMD) Sublayer* / 29
    - 2.2.1.2. *Physical Layer Convergence Protocol (PLCP)* / 29
  - 2.2.2. Medium Access Control (MAC) Sublayer / 30
    - 2.2.2.1. *Contention Windows* / 30
  - 2.2.3. Layer and Station Management Planes / 31
- 2.3. HIPERLAN/2 / 32
  - 2.3.1. Physical Layer / 32
    - 2.3.1.1. *Link Adaptation* / 33
  - 2.3.2. Data Link Control Layer / 33
    - 2.3.2.1. *MAC* / 33
    - 2.3.2.2. *Radio Link Control (RLC)* / 33
    - 2.3.2.3. *Dynamic Frequency Selection (DFS)* / 33
    - 2.3.2.4. *Error Control (EC)* / 34
  - 2.3.3. Convergence Layer (CL) / 34
- 2.4. Broadband Wireless Access Networks / 35
  - 2.4.1. The User Plane / 36

- 2.4.2. MAC Layer / 36
  - 2.4.2.1. *Convergence Sublayer (CS)* / 37
  - 2.4.2.2. *MAC Common Part Sublayer (CPS)* / 37
  - 2.4.2.3. *Privacy Sublayer* / 37
- 2.4.3. PHY / 37
- 2.4.4. IEEE 802.16a / 37
- 2.4.5. Mobile Broadband Wireless Access (MBWA) Network / 38
- 2.5. Cellular Data Networks / 38
  - 2.5.1. North American and European Cellular Networks / 38
  - 2.5.2. Voice-Grade Modems / 39
  - 2.5.3. Relative Look at Cellular Network Generations / 40
  - 2.5.4. Core Network / 42
- 2.6. Summary / 43
- References / 43

### **3. COMPONENTS OF A WIRELESS LAN**

47

- 3.1. Local Area Networks (LANs) / 48
  - 3.1.1. LAN Interconnection (Topology) / 49
  - 3.1.2. Addressing Mechanisms / 50
  - 3.1.3. Medium Specification / 50
  - 3.1.4. Physical Layer Mechanisms / 51
  - 3.1.5. Data Link Control Layer / 51
  - 3.1.6. Traffic Differentiation / 51
  - 3.1.7. WAN/LAN Connection / 51
- 3.2. Wireless LAN Components / 52
  - 3.2.1. Physical Layer Components / 52
    - 3.2.1.1. *Station Types* / 52
    - 3.2.1.2. *Channel Media* / 53
    - 3.2.1.3. *Physical Link* / 53
    - 3.2.1.4. *Signal Conditioning* / 53
    - 3.2.1.5. *Interference-Reduction Mechanisms* / 54
    - 3.2.1.6. *Modulation of Signals* / 56
    - 3.2.1.7. *Data Transmission* / 56
    - 3.2.1.8. *Convergence Procedures* / 56
    - 3.2.1.9. *Rate Selection Capability* / 56
    - 3.2.1.10. *Synchronization, Flow and Error-Control Capabilities* / 57
    - 3.2.1.11. *Physical Layer Management* / 57

- 3.2.2. Medium Access Control (MAC) Layer Components / 58
  - 3.2.2.1. *Network Configurations* / 58
  - 3.2.2.2. *Channel Access* / 58
  - 3.2.2.3. *Multiple Access* / 59
  - 3.2.2.4. *User and Data Privacy* / 62
  - 3.2.2.5. *Power-Management Mechanisms* / 63
  - 3.2.2.6. *Fragmentation* / 63
  - 3.2.2.7. *Multimedia Service* / 64
  - 3.2.2.8. *Packet Forwarding* / 64
  - 3.2.2.9. *Mobility Support* / 64
  - 3.2.2.10. *MAC Layer Management* / 65
  - 3.2.2.11. *MAC Frames* / 65
  - 3.2.2.12. *Teleconferencing Capability* / 65
- 3.2.3. Logical Link Control (LLC) Layer / 66
- References / 66

**4. WLANs: THE PHYSICAL LAYER**

- 4.1. IEEE 802.11 Standards Suite / 68
  - 4.1.1. Station Types / 68
  - 4.1.2. Channel Media / 69
  - 4.1.3. Physical Links / 69
  - 4.1.4. Signal Conditioning / 70
  - 4.1.5. IEEE 802.11g PHY / 70
- 4.2. Interference Rejection Using Barker Sequence, OFDM and CCK / 72
  - 4.2.1. 11-Bit Barker Sequence / 73
  - 4.2.2. Orthogonal Frequency Division Multiplexing (OFDM) / 75
  - 4.2.3. Complementary Code Keying (CCK) / 76
  - 4.2.4. PHY Data Transmission / 77
    - 4.2.4.1. *PLCP Frame Format for 802.11 Series* / 78
    - 4.2.4.2. *Meanings of Frame Fields* / 78
- 4.3. HIPERLAN PHY / 79
  - 4.3.1. Station Types / 81
  - 4.3.2. Channel Media / 81
  - 4.3.3. Signal Conditioning / 81
  - 4.3.4. Modulation and Coding / 81

- 4.3.5. Data Transmission, Convergence and Rate Selectivity / 82
- 4.3.6. PHY Management / 82
- 4.4. Summary / 83
- References / 83

## 5. WLANs: MEDIUM ACCESS CONTROL

85

- 5.1. IEEE 802.11 Medium Access Control / 86
  - 5.1.1. Network Configurations / 86
  - 5.1.2. Channel Access in IEEE 802.11 / 86
  - 5.1.3. Channel Sensing / 87
  - 5.1.4. Collision Avoidance / 88
    - 5.1.4.1. *Prioritizing IFS* / 88
    - 5.1.4.2. *Random Backoff* / 88
    - 5.1.4.3. *Discouraging Multiple Transmissions* / 89
    - 5.1.4.4. *Binary Exponential Backoff* / 89
    - 5.1.4.5. *Contention Window* / 89
  - 5.1.5. Multiple Access in IEEE 802.11 / 89
  - 5.1.6. DCF Transmission / 91
  - 5.1.7. PCF Transmission / 92
  - 5.1.8. User and Data Privacy / 92
    - 5.1.8.1. *User Authentication* / 92
    - 5.1.8.2. *Data Encryption* / 93
  - 5.1.9. Power Management / 94
  - 5.1.10. Fragmentation / 95
  - 5.1.11. Multimedia Support / 95
- 5.2. IEEE 802.11e factor / 95
  - 5.2.1. Enhanced Station / 96
  - 5.2.2. Hybrid Coordinator / 96
  - 5.2.3. Enhanced DCF (EDCF) / 96
  - 5.2.4. Hybrid Coordination Function (HCF) / 97
    - 5.2.4.1. *TXOP* / 97
- 5.3. Routing and Mobility Support / 98
  - 5.3.1. No Transition / 98
  - 5.3.2. BSS Transition / 98
  - 5.3.3. ESS Transition / 98
- 5.4. MAC Layer Management / 99
- 5.5. MAC Frames / 99

- 5.6. Multicasting Capability / 100
- 5.7. HIPERLAN MAC / 100
  - 5.7.1. Network Configuration / 100
  - 5.7.2. Channel Access / 101
    - 5.7.2.1. Contention / 101
    - 5.7.2.2. Yield / 101
  - 5.7.3. Multiple Access / 102
- 5.8. HIPERLAN 2 / 103
  - 5.8.1. Channel Access / 103
  - 5.8.2. Multiple Access / 103
  - 5.8.3. Broadcast Phase / 103
  - 5.8.4. Downlink Phase / 104
  - 5.8.5. Uplink Phase / 104
  - 5.8.6. Direct Link / 104
  - 5.8.7. Random Access Phases / 104
- 5.9. User and Data Privacy / 104
- 5.10. Power Management / 105
- 5.11. Multimedia Services / 105
- 5.12. Routing / 106
- 5.13. Mobility Support / 107
- 5.14. MAC Frame / 107
- 5.15. Teleconferencing Capability / 108
- 5.16. Data Link Control (DLC) Layer / 109
- References / 109

**6. MOBILITY AND INTERNET PROTOCOLS**

- 6.1. Mobility in Internet Applications / 114
  - 6.1.1. Reconnectivity / 114
  - 6.1.2. Portability / 114
  - 6.1.3. Micromobility / 115
- 6.2. Internet Protocols for Mobility / 117
- 6.3. Session Initiation Protocol (SIP) / 117
  - 6.3.1. SIP versus H.323 and HTTP / 117
  - 6.3.2. SIP Provisions / 118
  - 6.3.3. SIP Request Types / 118
  - 6.3.4. SIP Response Types / 120
  - 6.3.5. SIP Operation / 120
  - 6.3.6. SIP and Cellular Networks / 121
  - 6.3.7. SIP and 3GPP, 3GPP2 / 123

- 6.4. Mobile IP / 123
  - 6.4.1. Mobile IP Components / 124
    - 6.4.1.1. *Mobile Host (MH)* / 124
    - 6.4.1.2. *Home Address* / 124
    - 6.4.1.3. *Correspondent Host (CH)* / 124
    - 6.4.1.4. *Mobile Home Agent (HA)* / 124
    - 6.4.1.5. *Mobile Foreign Agent (FA)* / 124
    - 6.4.1.6. *Mobility Agent (MA)* / 124
    - 6.4.1.7. *Mobility Detection* / 124
  - 6.4.2. Agent Discovery / 125
  - 6.4.3. Registration / 125
  - 6.4.4. De-registration / 125
  - 6.4.5. Care-of Address (CoA) / 126
  - 6.4.6. Tunneling / 126
  - 6.4.7. Mobile IP Usage Scenario / 127
  - 6.4.8. Security Measures in Mobile IP / 129
  - 6.4.9. Limitations of Mobile IP / 129
  - 6.4.10. Mobile IP Messages / 132
  - 6.4.11. Internet Standards for Cellular Networks / 132
- 6.5. Mobility Management in an Access Network / 133
  - 6.5.1. Address Allocation / 133
  - 6.5.2. Data Communications / 133
  - 6.5.3. Mobility / 134
- 6.6. Cellular IP / 134
  - 6.6.1. Components of a Cellular IP System / 135
    - 6.6.1.1. *Active and Passive Mobile Hosts* / 135
    - 6.6.1.2. *Base Station* / 135
    - 6.6.1.3. *Gateway Router* / 135
    - 6.6.1.4. *Base Station Routing Cache* / 135
    - 6.6.1.5. *Route Update Packet* / 136
    - 6.6.1.6. *Uplink/Downlink Packet* / 136
    - 6.6.1.7. *Semisoft Handoff* / 136
    - 6.6.1.8. *Paging Area* / 136
    - 6.6.1.9. *Paging Update Packet* / 136
    - 6.6.1.10. *Paging Cache* / 136
  - 6.6.2. cIP Usage Scenario / 136
    - 6.6.2.1. *Hard Handoff* / 138
    - 6.6.2.2. *Semisoft Handoff* / 138
  - 6.6.3. cIP and Mobile IP / 138

- 6.7. IPv6 and Mobility Management / 139
  - 6.7.1. Expanded Address Space / 139
  - 6.7.2. Efficient HA Registration / 139
  - 6.7.3. Autoconfiguration of IP Addresses / 139
  - 6.7.4. Mobility Detection / 140
  - 6.7.5. Optimized Routing / 140
    - 6.7.5.1. *Higher Layer Bindings* / 140
  - 6.7.6. Security / 140
  - 6.7.7. Micromobility / 141
  - 6.7.8. Network Support for Application-Level Mobile IPv6 / 141
  - 6.7.9. Internet and Cellular Networking / 141
- References / 142

**7. DATA COMMUNICATIONS IN CELLULAR NETWORKS: CDMA2000 145**

- 7.1. Business Wireless Data Networks / 146
  - 7.1.1. Cellular Digital Packet Data (CDPD) Network / 147
  - 7.1.2. ARDIS / 147
  - 7.1.3. RAM Data Networks / 147
- 7.2. Cellular Data Networks / 148
  - 7.2.1. Cooperation Explosion / 148
  - 7.2.2. 3G Air Interfaces / 149
  - 7.2.3. UMTS Terrestrial Radio Access (UTRA) / 151
- 7.3. Release D for cdma2000 Based Access / 151
  - 7.3.1. Fast Call Setup (FCS) / 152
  - 7.3.2. Mobile Equipment Identifier (MEID) / 152
  - 7.3.3. Broadcast and Multicast Services (BCMCS) / 153
- 7.4. cdma2000 Standard / 153
  - 7.4.1. CDMA Timescale / 155
  - 7.4.2. Physical Layer (PHY) / 155
    - 7.4.2.1. *Radio Configuration (RC)* / 155
    - 7.4.2.2. *Access Channel* / 155
    - 7.4.2.3. *Reverse Packet Data Channel (R-PDCH)—10 ms (19.2 kbps–1.84 Mbps)* / 155
    - 7.4.2.4. *Transmission* / 158
    - 7.4.2.5. *Forwards Packet Data Channel* / 160
- 7.5. cdma2000 Medium Access Control / 160
  - 7.5.1. Mux and QoS (MaQ) Sublayer / 162
  - 7.5.2. Access Channel Procedures / 162



- 7.5.3. Packet Data Channel Control Functions (PDCHCF) / 163
  - 7.5.3.1. *Forward PDCHCF (FPDCHCF)* / 164
  - 7.5.3.2. *Reverse PDCHCF (RPDCHCF)* / 164
- 7.6. All-IP Architecture / 164
  - 7.6.1. Networking Elements / 164
    - 7.6.1.1. *Access Gateway (AGW)* / 164
    - 7.6.1.2. *Authentication Center (AC)* / 164
    - 7.6.1.3. *Base Station (BS)* / 164
    - 7.6.1.4. *Call Session Control Function (CSCF)* / 164
    - 7.6.1.5. *Databases* / 165
    - 7.6.1.6. *Equipment Identity Register (EIR)* / 165
    - 7.6.1.7. *Home Agent (HA)* / 165
    - 7.6.1.8. *Home Location Register (HLR)* / 165
    - 7.6.1.9. *Interworking Function (IWF)* / 165
    - 7.6.1.10. *Media Gateway (MGW)* / 165
    - 7.6.1.11. *Media Resource Function Processor (MRFP)* / 165
    - 7.6.1.12. *Mobile Station (MS)* / 165
    - 7.6.1.13. *Mobility Management (MM)* / 166
    - 7.6.1.14. *Mobile Switching Center (MSC)* / 166
    - 7.6.1.15. *Message Center (MC)* / 166
    - 7.6.1.16. *OSA-Service Capability Server (OSA-SCS)* / 166
    - 7.6.1.17. *Packet Control Function (PCF)* / 166
    - 7.6.1.18. *Policy Decision Function (PDF)* / 166
    - 7.6.1.20. *Visitor Location Register (VLR)* / 166
  - 7.6.2. Planar Architecture / 166
    - 7.6.2.1. *Access Plane* / 167
    - 7.6.2.2. *Network Plane* / 167
    - 7.6.2.3. *Multimedia Bearer Plane* / 169
    - 7.6.2.4. *Multimedia Application Server Control Plane* / 169
- 7.7. Summary / 169
- References / 170

## **8. DATA COMMUNICATIONS IN CELLULAR NETWORKS: W-CDMA**

**173**

- 8.1. Components of the UMTS Network / 174
- 8.2. UMTS Network Domains / 175

- 8.2.1. UE Domain / 176
- 8.2.2. Infrastructure Domain / 176
- 8.3. Strata / 177
- 8.4. Radio Access Network (RAN) / 177
  - 8.4.1. Transport and Logical Channels / 178
  - 8.4.2. Physical Layer (PHY) / 178
- 8.5. UMTS Services / 179
- 8.6. Improvements Over Release 99 / 179
- 8.7. IMS System Concepts / 185
  - 8.7.1. Internet Multimedia Core Network (IM-CN) / 186
  - 8.7.2. IP Connectivity Access Network (IP-CAN) / 186
  - 8.7.3. Terminals / 186
- 8.8. Session Layer Architecture / 186
  - 8.8.1. Interrogation CSCF (I-CSCF) / 186
  - 8.8.2. Proxy CSCF (P-CSCF) / 187
  - 8.8.3. Server CSCF (S-CSCF) / 187
  - 8.8.4. Home Subscriber Server (HSS) / 187
  - 8.8.5. Media Gateways and Associated Control Functions (MGW, MGCF, SGW, BGCF) / 187
  - 8.8.6. Media Resource Functions (MRF) / 188
- 8.9. Open Service Access (OSA) / 188
  - 8.9.1. OSA Interfaces / 188
  - 8.9.2. OSA Functions / 190
    - 8.9.2.1. *Framework (FW) Functions of OSA / 190*
    - 8.9.2.2. *Network Function of OSA / 190*
    - 8.9.2.3. *User Data Related Functions of OSA / 190*
- 8.10. Parlay / 191
  - 8.10.1. Parlay Background / 191
- 8.11. IPv4/IPv6 Scenarios Towards All-IP Infrastructure / 192
  - 8.11.1. GPRS Scenarios / 192
  - 8.11.2. IMS Scenarios / 194
- 8.12. 3GPP Release 6 Objectives / 194
- 8.13. Summary / 194
- References / 195

**9. SECURITY IN WIRELESS DATA NETWORKS**

- 9.1. Ascribing Security to a Network / 198
  - 9.1.1. Why Are Wireless Network Devices a Bigger Challenge? / 199

- 9.2. Security Network Architecture / 199
  - 9.2.1. Securing a Standalone Device / 201
  - 9.2.2. Securing a Networked Device / 201
  - 9.2.3. Securing a Wireless Networked Device / 202
- 9.3. Secure Operating System (SOS) / 203
- 9.4. Components of Security System / 205
  - 9.4.1. Protocols / 206
    - 9.4.1.1. *Authentication* / 206
    - 9.4.1.2. *Association/Registration* / 206
    - 9.4.1.3. *Re-association/Visitor Registration* / 206
    - 9.4.1.4. *Wireline Equivalence Privacy (WEP)* / 206
    - 9.4.1.5. *IPsec* / 207
    - 9.4.1.6. *SSL* / 207
    - 9.4.1.7. *EAP* / 207
  - 9.4.2. Algorithms / 207
    - 9.4.2.1. *Encryption* / 208
    - 9.4.2.2. *Secret-Key Algorithms* / 208
    - 9.4.2.3. *Public-Key Algorithms* / 208
      - 9.4.2.3.1. *How Is Two-Key Cipher Possible?* / 209
    - 9.4.2.4. *Block and Stream Ciphers* / 211
    - 9.4.2.5. *Rounds, Key-Size and Data Block* / 211
  - 9.4.3. Examples of Encryption Algorithms / 211
    - 9.4.3.1. *Advanced Encryption System (AES)* / 211
    - 9.4.3.2. *Data Encryption System (DES) and Triple DES* / 212
    - 9.4.3.3. *f8 Algorithm* / 212
    - 9.4.3.4. *RC4* / 212
  - 9.4.4. Hash Algorithms / 213
    - 9.4.4.1. *Message Digest (MD)* / 213
    - 9.4.4.2. *Message Authentication Code (MAC)* / 213
    - 9.4.4.3. *Digital Signature (DS)* / 214
    - 9.4.4.4. *Digital Certificate (DC)* / 214
  - 9.4.5. Examples of Hash Algorithms / 214
    - 9.4.5.1. *SHA-1* / 214
    - 9.4.5.2. *MD5* / 214
    - 9.4.5.3. *H-MAC* / 214
  - 9.4.5. Key / 215
    - 9.4.5.1. *Key-Generation Algorithms* / 215

- 9.4.5.1.1. *Diffie-Hellman (DH) Algorithm / 217*
- 9.4.5.1.2. *RSA Algorithm / 218*
- 9.4.5.2. *Server-Based Key Management / 218*
- 9.4.5.3. *Public-Key Infrastructure (PKI) / 219*
- 9.4.5.4. *Other Key Infrastructure / 221*
- 9.5. *Wireline Equivalent Privacy (WEP) / 221*
  - 9.5.1. *WEP Architecture / 221*
  - 9.5.2. *WEP Vulnerabilities / 222*
- 9.6. *Wi-Fi Protected Access (WPA) / 223*
  - 9.6.1. *Temporal Key Integrity Protocol (TKIP) / 223*
    - 9.6.1.1. *Michael / 224*
    - 9.6.1.2. *IV Sequence Enforcement / 224*
    - 9.6.1.3. *Key Mixing / 224*
    - 9.6.1.4. *Rekeying / 224*
  - 9.6.2. *TKIP Encapsulation Process / 225*
  - 9.6.3. *WPA Authentication / 226*
    - 9.6.3.1. *RADIUS-Based Authentication / 226*
    - 9.6.3.2. *Pre-Shared Key (PSK) Authentication / 226*
- 9.7. *IEEE 802.11i / 227*
  - 9.7.1. *Master Key (MK) / 227*
  - 9.7.2. *Pairwise Master Key (PMK) / 228*
  - 9.7.3. *Pairwise Transient Key (PTK) / 228*
  - 9.7.4. *IEEE 802.11i and WPA / 229*
- 9.8. *Security in Cellular Networks / 229*
  - 9.8.1. *WCDMA Security Architecture / 230*
    - 9.8.1.1. *User Confidentiality / 231*
    - 9.8.1.2. *Mutual Authentication / 231*
    - 9.8.1.3. *Data Integrity and Encryption / 232*
    - 9.8.1.4. *Flexibility / 232*
  - 9.8.2. *Security in cdma2000 / 232*
    - 9.8.2.1. *Using the A-Key / 232*
    - 9.8.2.2. *Amendments from Earlier Generations / 233*
- 9.9. *Final Word / 233*
  - 9.9.1. *Alternative View / 234*
- References / 235

**10. ROUTING IN WIRELESS LANs**

- 10.1. *Routing in Infrastructure Networks / 240*
- 10.2. *Ad Hoc Wireless Networks / 241*

- 10.2.1. Characteristics of MANETs / 242
- 10.2.2. Goals of the IETF MANET Working Group / 242
- 10.2.3. Sources of Failure in MANETs / 242
  - 10.2.3.1. *Topological Failures* / 242
  - 10.2.3.2. *Channel Failures* / 242
  - 10.2.3.3. *Protocol Failures* / 242
- 10.3. Characteristics of a Good Routing Protocol / 243
  - 10.3.1. Performance Metrics / 243
  - 10.3.2. Networking Context / 243
- 10.4. Classifications of Routing Protocols / 244
  - 10.4.1. Pro-Active and Reactive Routing / 244
  - 10.4.2. Link State Versus Distance Vector / 244
- 10.5. Routing Phases / 245
- 10.6. Routing Mechanisms / 245
  - 10.6.1. Zone Routing Protocol (ZRP) / 245
  - 10.6.2. Dynamic Source Routing (DSR) / 246
  - 10.6.3. Destination Sequenced Distance Vector (DSDV) / 247
  - 10.6.4. Ad Hoc On-Demand Distance Vector Routing (AODV) / 247
  - 10.6.5. Temporally Ordered Routing Algorithm (TORA) / 247
  - 10.6.6. Wireless Routing Protocol (WRP) / 247
  - 10.6.7. Mobile Multimedia Wireless Network (MMWN) / 248
  - 10.6.8. Transmission Power Optimization / 248
    - 10.6.8.1. *Flow Augmentation Routing (FAR)* / 248
    - 10.6.8.2. *Online Max-Min Routing (OMMR)* / 248
    - 10.6.8.3. *Power-Aware Localized Routing (PLR)* / 248
    - 10.6.8.4. *Minimum Energy Routing (MER)* / 248
    - 10.6.8.5. *Retransmission-Energy Aware Routing (RAR)* / 248
    - 10.6.8.6. *Smallest Common Power (COMPOW)* / 248
  - 10.6.9. Load Distribution Protocols / 249
    - 10.6.9.1. *Localized Energy-Aware Routing (LEAR)* / 249
  - 10.6.10. SPAN Protocol / 249
  - 10.6.11. Geographic Adaptive Fidelity (GAF) / 249
  - 10.6.12. Prototype Embedded Network (PEN) / 249
- 10.7. Performance Comparison / 249
- 10.8. Multicasting / 250
  - 10.8.1. Mobility Support Using Multicast IP (MSM-IP) / 250

- 10.8.2. Multicast Routing in MANETs / 251
- 10.9. Dynamic Source Routing (DSR) Protocol / 251
  - 10.9.1. Protocol Operation / 251
    - 10.9.1.1. *Route Caching* / 251
    - 10.9.1.2. *Route Discovery* / 251
    - 10.9.1.3. *Data Transmission Phase* / 253
    - 10.9.1.4. *Route Maintenance* / 254
  - 10.9.2. Flow State Option / 256
  - 10.9.3. DSR Packet / 256
- 10.10. Selecting the Best Route / 256
  - 10.10.1. Topology of Fixed Ad-Hoc Networks / 257
    - 10.10.1.1. *Topology Index* / 258
  - 10.10.2. Effect of Mobility / 258
    - 10.10.2.1. *Mobility and Displacement* / 259
    - 10.10.2.2. *Mobility and Path Loss Models* / 260
  - 10.10.3. Residual Battery / 262
  - 10.10.4. Example of Application of Above Results / 263
  - 10.10.5. Discussion / 265
- 10.11. WLAN Routing Through Cellular Network Infrastructure / 266
  - 10.11.1. Introduction to OWLAN / 266
  - 10.11.2. Design Objectives / 266
  - 10.11.3. OWLAN System Architecture / 267
  - 10.11.4. System Elements / 267
    - 10.11.4.1. *Authentication Server (AS)* / 269
    - 10.11.4.2. *Access Controller (AC)* / 269
    - 10.11.4.3. *Mobile Terminal (MT)* / 269
  - 10.11.5. System Operation / 269
    - 10.11.5.1. *MT (Mobile Terminal)* / 269
    - 10.11.5.2. *AC (Access Controller)* / 270
    - 10.11.5.3. *AS (Authentication Server)* / 270
- 10.12. Routing in Personal Area Networks / 270
- 10.13. Summary / 270
- References / 271

**11. WIRELESS PERSONAL AREA NETWORKS AND  
ULTRAWIDE BAND COMMUNICATIONS**

- 11.1. Wireless Personal Area Networks (WPANs) / 276
- 11.2. Terminology for WPANs / 278

- 11.3. IEEE 802.15.1 Standard / 278
  - 11.3.1. Bluetooth Components / 279
    - 11.3.1.1. *Bluetooth Stations* / 279
    - 11.3.1.2. *Network Configurations* / 279
    - 11.3.1.3. *Channel Media* / 280
    - 11.3.1.4. *Logical Channels* / 281
  - 11.3.2. Bluetooth Network Operation / 282
    - 11.3.2.1. *Access* / 283
    - 11.3.2.2. *Link Establishment* / 283
    - 11.3.2.3. *Synchronous Transmission Scenario* / 284
    - 11.3.2.4. *Asynchronous Connectionless (ACL) Mode* / 284
  - 11.3.3. Bluetooth Summary / 285
- 11.4. Higher Data Rate PANs (IEEE 802.15.3) / 285
  - 11.4.1. High-Data-Rate Piconet (HDR-PN) / 285
    - 11.4.1.1. *Piconet Controller (PNC)* / 286
    - 11.4.1.2. *Piconet Device (DEV)* / 286
    - 11.4.1.3. *Piconet Hierarchy* / 286
  - 11.4.2. Medium Access Control (MAC) Layer / 287
    - 11.4.2.1. *MAC Superframe* / 287
    - 11.4.2.2. *Beacon* / 287
    - 11.4.2.3. *Contention Access Period (CAP)* / 287
    - 11.4.2.4. *Channel Time Allocation Period (CTAP)* / 287
    - 11.4.2.5. *Private CTA* / 288
  - 11.4.3. IEEE 802.15.3 Physical Layer (PHY) / 288
- 11.5. Ultra Wideband (UWB) Spectrum / 290
  - 11.5.1. UWB PHY for IEEE 802.15.3a / 291
  - 11.5.2. DS-UWB (Direct Sequence—Ultra Wideband) / 292
    - 11.5.2.1. *Modulation* / 292
  - 11.5.3. Multi-Band OFDM PHY Proposal / 293
- 11.6. Low Data Rate WPANs (LR-WPANs) and IEEE 802.15.4 / 295
  - 11.6.1. Network Configuration / 297
    - 11.6.1.1. *Star Topology* / 297
    - 11.6.1.2. *Peer-to-Peer Topology* / 298
  - 11.6.2. LR-PAN Physical Layer (PHY) / 298
  - 11.6.3. LR-PAN Medium Access Control (MAC) / 299
    - 11.6.3.1. *MAC Features* / 299
    - 11.6.3.2. *Synchronization and Data Transfer* / 299

- 11.6.3.3. *Beacons / 301*
- 11.6.3.4. *Active and Inactive Portions / 301*
- 11.6.3.5. *Contention Access Period (CAP) and  
Contention-Free Period (CFP) / 301*
- 11.6.4. *Data Transfer Modes / 301*
- 11.6.5. *MAC Frames / 302*
- 11.6.6. *MAC Security / 303*
- 11.7. *Summary / 303*
- References / 303*

**12. BROADBAND WIRELESS ACCESS (BWA) 305**

- 12.1. *Line-of-Site (LoS) and Non-Line-of-Site (NLoS) Systems / 307*
- 12.2. *Effect of Antenna Type / 308*
- 12.3. *BWA Spectrum / 308*
- 12.4. *BRAN versus WirelessMAN™ / 309*
- 12.5. *IEEE WirelessMAN™ / 311*
  - 12.5.1. *WirelessMAN Station Types / 312*
    - 12.5.1.1. *Base Station (BS) / 312*
    - 12.5.1.2. *Subscriber's Station (SS) / 312*
  - 12.5.2. *Network Topologies / 312*
    - 12.5.2.1. *Bandwidth Stealing / 314*
    - 12.5.2.2. *Adaptive Modulation / 314*
    - 12.5.2.3. *Adaptive Antenna System (AAS) / 314*
  - 12.5.3. *WirelessMAN Protocol Architecture / 314*
  - 12.5.4. *MAC Sublayer / 314*
    - 12.5.4.1. *Service Flow / 315*
    - 12.5.4.2. *MAC PDU / 315*
      - 12.5.4.2.1. *MAC Header / 315*
      - 12.5.4.2.2. *CRC / 316*
    - 12.5.4.3. *Transmission of MAC PDU / 317*
    - 12.5.4.4. *QoS Provisioning / 318*
    - 12.5.4.5. *Distributed and Centralized Scheduling in  
eWMAN / 318*
    - 12.5.4.6. *Duplexing Techniques / 318*
    - 12.5.4.7. *Bandwidth Management / 321*
    - 12.5.4.8. *Adaptive Antenna Systems (AAS) / 321*
    - 12.5.4.9. *Dynamic Frequency Selection (DFS) / 321*
    - 12.5.4.10. *Other MAC Sublayers / 322*
  - 12.5.5. *WirelessMAN PHYs / 323*



12.5.6.	WMAN PHY (10–66 GHz) / 323	
12.5.6.1.	<i>PHY Frame</i> / 323	
12.5.6.2.	<i>Downlink Frames</i> / 324	
12.5.6.2.	<i>Uplink PHY Frame</i> / 325	
12.5.6.3.	<i>Physical Medium Dependent (PMD) Sublayer</i> / 327	
12.6.	IEEE 802.20 Mobile Broadband Wireless Access (MBWA) / 328	
12.6.1.	Objectives / 330	
12.7.	Cellular and Satellite Networks as Wireless Local Loops (WLL)s / 330	
	References / 331	

<b>APPENDIX: OVERVIEW AND GUIDE TO THE IEEE 802 LMSC</b>	<b>333</b>
<b>INDEX</b>	<b>343</b>



## PREFACE

---

As broadband access reaches more and more homes and businesses, paradigm changes are occurring in all aspects of data communications. Security in Wireless LANs is becoming an ever more important issue, cellular networks are geared toward a service-oriented design, broadband access does not necessarily imply ‘fixed’ networks and, above all, network architectures with a range of data rates for personal operating space have been specified. Various factors, both international and national, have impacted the interoperability endeavors and we see an unprecedented collaboration among operators, vendors and standardization agencies. A large number of wireless data technologies provide solutions for users of wireless data. Arguably, the ‘secret ingredient’ in all the new and traditional technologies seems to be the Internet Protocol (IP). Without IP, a networking technology, wireless or not, seems to be destined to . . . including IP. However, each of the various network architectures has its own place in the market. Each wireless network relieves its users from some restrictions, such as having a plethora of wires and, many times, provides the freedom to move while connected.

The kind of freedom that wireless networking has promised is not only irreversible, but is also subject to growth, in strides, that is. The depth of knowledge in wireless networking has gone to a point where we talk about changing and choosing modulation schemes from burst to burst, of mobility in excess of 200 kmph, and of license-exempt bandwidth topping 1.5 GHz. Putting it all together in one book is practically impossible without sacrificing one thing or the other. However, it is possible to have a book with a theme, for example, to give enough breadth that the knowledge gained covers sufficient types of networks, and enough depth that the knowledge obtained is not superfluous.

This book tries to meet this general goal of providing a breadth of the technologies in wireless data networks while requiring a respectable background in communications network architecture and some background in fundamental algebra. The emphasis is on data networks.

When we talk about ‘data networks’, we usually imply packet-switched communications, of which voice could be a very important application. Following this logic, we describe only the ‘data’ part of networks, where both voice and data parts exist. Also, ‘multimedia’ in packet-switched networks includes voice communications as well. Therefore, voice, such as in voice over IP (VoIP) is automatically a part of discussing data networks. However, while voice is QoS-intensive, it does not shine as a killer application for high-speed networks, including wireless networks. A killer application would ideally be the one that requires network capability to the fullest and would be in demand to the fullest as well. New architectures for cellular networks seem to have decided to deploy sufficient infrastructure and leave the question of killer application to future, thus providing the scope for third-party service development environment. Nevertheless, the question of a killer application does not really exist in all types of network architectures, specifically, the ones used for access or the ones designed for specific applications. The example of the former are the WLANs and broadband wireless access networks, and the examples for the latter are sensor networks designed specifically for a certain application. We have included a wide range of network architectures, along with chapters to enhance their understanding.

The first three chapters have the goal of enhancing the understanding of later chapters. First chapter gives a bird’s eye view of various wireless and mobile network types. It ends with a discussion on the frequency spectra allocated for these networks. Chapter 2, in continuation, discusses the protocol architectures of various network types. Even though we classify networks as personal, local, metropolitan and wide area networks, their real classification is in terms of protocol planes. Chapter 3 discusses various components of wireless LANs. A wireless LAN is much more complex than the wired counterpart and utilizes many concepts that are relatively more advanced. Instead of explaining these concepts as a digression, we have included them in a separate chapter. Following Chapter 3, there are two chapters on WLANs: Chapter 4, on descriptions of the physical layer (PHY) standards, and Chapter 5, an account of the medium access control (MAC) layer standards. The material presented in these chapters is organized in a convenient sequence. Also, the chapter on components of a WLAN (Chapter 3) is kept in view while organizing Chapters 4 and 5. In a way, WLANs are for low-level mobility (link-level). The next step in mobility would be the wide area mobility for wireless data terminals. The next three chapters and Chapter 10 cover this topic.

In Chapter 6 we discuss the two main Internet protocols that bear the responsibility of wide area mobility provision, the mobile IP and the session initiation protocol (SIP). Mobile IP provides what is called macromobility and SIP provides signaling mechanisms for macromobility on a higher protocol

level, so that the mobile user does not lose established associations while on the move. Together, mobile IP and SIP provide the IETF ‘open’ architecture for the next generation of cellular networks, discussed in the next two chapters, that is, Chapter 7 and Chapter 8. Chapter 7 is on the cdma2000 network, that is, the 3G evolution from the North American systems based on CDMA. The cdma2000 is now developed under the partnership project 3GPP2 and has Release D as the latest one. The chapter focuses on the packet data part of the network. Chapter 8 does the same for W-CDMA, which is an evolution from the European Union’s TDMA+FDMA network, that is, the GSM network. W-CDMA is now developed as part of another partnership project, 3GPP. In this chapter, we also take the opportunity to bring to light the open service access (OSA) capability and Internet multimedia service (IMS) that are the service development environments for the open service architectures. The wide area coverage continues in Chapter 10, with a discussion on routing in an ad hoc network. However, after discussing WLANs and cellular networks, we have a look at the security issues in wireless data networks, that is Chapter 9.

The topic of security is heavily influenced by political and trade issues and lacks in enforcement in real life. Perhaps due to the dependence of security technology on trade relations it could not really be a regular part of network architectures. However, the scenario is changing rapidly and the latest encryption standard of the wireless data in the United States (Advanced Encryption System) is actually not designed within the United States. Since it is our view that security was just as complex as the network architecture, if not more, the chapter is a little longer than other chapters. We discuss various concepts relating to wireless data security, from the very basic to what is going on most recently. In terms of the security protocols and architecture standards, we discuss mainly the WLANs, as that is where most vulnerability lies. After discussing security, we continue further network architectures in Chapters 10, 11, and 12.

In Chapter 10 we discuss routing in local area networks. The routing is made complex when there is no infrastructure. Consequently, most of the chapter is on mobile ad hoc networks (MANETs). Due to the numerous idiosyncratic characteristics of such networks, there are a large number of routing protocols proposed. Instead of making the chapter a comparative study of these mechanisms, we take a good look of one mechanism (Dynamic Source Routing), as proposed in a recent Internet-draft, and switch to a serious issue of deciding how to compare routes in order to prioritize them. In this discussion, we go a little higher in level and bring forward an analysis framework that can be developed and worked out to compare and optimize routing protocols for MANETs. More research is needed in this framework, and it is being carried out. Chapter 11 presents a discussion on low area coverage wireless networks, called wireless personal area networks (PAN)s. Even though it may be the Bluetooth standards that brought the word out about PANs, we stick to IEEE standards recommendations on it. In fact, IEEE 802.15.1, which is

Bluetooth v1.1 adopted as such (along with some new interface definitions), is an admission of the fact that Bluetooth has established its recognition, beyond doubt. The Working Group IEEE 802.15, however, did not stop at that, and covered a range of PANs for high-data rates (IEEE 802.15.3 and IEEE 802.15.3a) and low rates (IEEE 802.15.4). These are discussed in this chapter. The ultrawide band (UWB), to be standardized as IEEE 802.15.3a, has a lot more than meets the eye at this time. Research and developments in this band (or set of bands) has to continue for many years before we can truly utilize the bandwidth and properties at this small wavelength and power.

Chapter 12, the last chapter, is on wireless broadband access (WBA). It is our view that actual growth of technology in this area lags behind the possibilities and potential applications. With the WiMAX initiative, however, this might change. The IEEE standards 802.16 and 802.16a, discussed in this chapter, could very well be responsible for future developments. The chapter also includes a few words about a current IEEE initiative about mobile broadband Internet access. The Working Group IEEE 802.20 is considering this initiative and hopes to have a standard in near future.

The book can be used by developers, IT managers in wireless data networks, professors for a graduate level or senior undergraduate level course on wireless data networks, and for professional training. The author does not propose various routes for a single-semester course, as the link among various chapters can be easily identified. Every group of users can develop their own course. The overall presentation is short enough to be used within one semester with appropriate adjustments in coverage. I hope that you find the book useful in enhancing the understanding of wireless data networks. If you are a developer, then it is my advice that you use specifications for actual development, and not this book. In order to assist instructors in textbook adoption for academic and professional training, slides of chapters and quizzes will be made available at the following FTP site: [ftp://ftp.wiley.com/public/sci\\_tech\\_med/wireless\\_networks/](ftp://ftp.wiley.com/public/sci_tech_med/wireless_networks/).

AFTAB AHMAD