Emerging Technologies in Wireless LANs

Wireless LANs have become mainstream over the last few years. What started out as cable replacement for static desktops in indoor networks has been extended to fully mobile broadband applications involving moving vehicles, high-speed trains, and even airplanes. An increasing number of municipal governments around the world and virtually every major city in the United States are financing the deployment of 802.11 mesh networks, with the overall aim of providing ubiquitous Internet access and enhanced public services. This book is designed for a broad audience with different levels of technical background and can be used in a variety of ways: as a first course on wireless LANs, as a graduate-level textbook, or simply as a professional reference guide. It describes the key practical considerations when deploying wireless LANs and equips the reader with a solid understanding of the emerging technologies. The book comprises 38 high-quality contributions from prominent practitioners and scientists, and covers a broad range of important topics related to 802.11 networks, including quality of service, security, high-throughput systems, mesh networking, 802.11/cellular interworking, coexistence, cognitive radio resource management, range and capacity evaluation, hardware and antenna design, hotspots, new applications, ultra-wideband, and public wireless broadband.

“Benny Bing has created a masterful, horizon-to-horizon compendium covering the foundations, functionality, implementation, and potential-for-the-future of IEEE 802.11 wireless LAN communications. Whether your interests are in QoS, security, performance and throughput, meshing and internetworking, management and design, or just the latest in Wi-Fi applications, you will find an in-depth discussion inside these covers. Emerging Technologies in Wireless LANs: Theory, Design, and Deployment is an excellent resource for anyone who wants to understand the underpinnings and possibilities of the Wi-Fi offerings we see evolving in the marketplace today.”

– Robert J. Zach, Director, Next Generation Broadband, EarthLink, Inc., USA

“Over the past 20 years, wireless LANs have grown from technical curiosity to a mainstream technology widely installed across residential, enterprise, and even municipal networks. The mobility and convenience of wireless has been augmented by the advanced throughput and range performance available in today’s products, extending the reach of wireless LANs to a broad array of applications. This book explores all aspects of contemporary wireless LANs, from the basics through wireless security, meshes, QoS, high throughput, and interworking with external networks. The broad range of topics and perspective make this the ideal reference for experienced practitioners, as well as those new to the field.”

– Craig J. Mathias, Principal, Farpoint Group, USA

“This book is a wonderful resource for anyone who works with Wi-Fi wireless technologies. It provides an excellent overview for the newcomer and an extensive and up-to-date reference for the expert. This book is a crucial tool for everyone involved in this exciting, fast-paced field. Everyone will learn from it!”

– Professor David F. Kotz, Director, Center for Mobile Computing, Dartmouth College, USA

“The ability of Wi-Fi technology to expand in so many directions while maintaining backwards compatibility has been one key to its success and the technology will certainly continue to evolve. This book has hopefully given you some insights into where we have been and where we may be headed.”

– Greg Ennis, Technical Director, Wi-Fi Alliance

Benny Bing is a research faculty member with the School of Electrical and Computer Engineering, Georgia Institute of Technology. He is an IEEE Communications Society Distinguished Lecturer, IEEE Senior Member, and Editor of the IEEE Wireless Communications magazine.
Emerging Technologies in Wireless LANs

Theory, Design, and Deployment

Edited by

BENNY BING

Georgia Institute of Technology
# Contents

**Authorship by Chapter**  
Foreword  
Preface  

**Part I: Introduction to 802.11**  

### Chapter 1 - Emerging IEEE 802.11 Standards  
1  
1.1 IEEE 802.11n: Enhancements for Higher Throughput  
1.1.1 802.11n PHY  
1.1.1.1 MIMO  
1.1.1.2 40 MHz Channel Binding  
1.1.1.3 Beam Forming  
1.1.1.4 STBC  
1.1.1.5 Other 802.11n PHY Features  
1.1.2 802.11n MAC  
1.1.2.1 High Throughput Support  
1.1.2.2 Legacy Protection, Coexistence, and Interoperability  
1.2 IEEE 802.11k: Radio Resource Measurement  
1.3 802.11p: Wireless Access for the Vehicular Environment  
1.4 802.11r: Fast BSS-Transitions  
1.5 802.11s: Wireless Mesh Networks  
1.6 802.11T: Wireless Performance Prediction  
1.7 802.11u: Wireless Inter-working with External Networks  
1.8 802.11v: Wireless Network Management  
1.9 802.11w: Management Frame Protection  
1.10 802.11y: Contention Based Protocol  
1.11 Conclusions  

### Chapter 2 - Guide to Wireless LAN Analysis  
13  
2.1 Introduction  
2.2 Overview of Wireless LANs  
2.2.1 WLAN Physical-Layer Standards  
2.2.1.1 802.11n  
2.2.2 WLAN Regulation  
2.2.3 WLAN Topologies  
2.2.4 Establishing a wireless connection  
2.2.4.1 Discovery
Contents vi

2.2.4.2 Authentication and deauthentication 18
2.2.4.3 Association, disassociation, and reassociation 18
2.2.4.4 Confidentiality 19
2.2.5 Security 19
  2.2.5.1 Concepts of secure communications 19
  2.2.5.2 Confidentiality and encryption 20
2.2.6 Collision Avoidance and Media Access 22
2.2.7 Physical Layer 24
  2.2.7.1 Radio frequencies and channels 24
  2.2.7.2 Signal and noise measurement 26
  2.2.7.3 Encoding and data rates 27
2.2.8 Packet Structure and Packet Type 28
  2.2.8.1 Data Packet Structure 28
  2.2.8.2 Management and Control Packets 29
2.3 Wireless Network Analysis 29
  2.3.1 Planning and designing a WLAN 30
    2.3.1.1 Predeployment 31
    2.3.1.2 Initial deployment 32
  2.3.2 Managing a WLAN 32
    2.3.2.1 Managing Signals 32
    2.3.2.2 Managing Users 32
  2.3.3 Administering a WLAN 34
    2.3.3.1 Securing the WLAN 34
  2.3.4 Troubleshooting - Analyzing Higher Level Network Protocols 36
    2.3.4.1 Leveraging existing assets with AP Capture Adapters 37
2.4 Conclusion 38

Part II: 802.11 Quality of Service

Chapter 3 - WLAN QoS 39
3.1 Introduction 39
  3.1.1 Terminology and Abbreviations 40
3.2 Channel Access 41
  3.2.1 Legacy Channel Access Methods 42
    3.2.1.1 Legacy Contention-Based Channel Access 42
    3.2.1.2 Legacy Pollled Access Protocol 42
  3.2.2 802.11e Contention-Based Channel Access 43
    3.2.2.1 TCMA MAC Protocol 45
  3.2.3 802.11e Pollled Channel Access 46
  3.2.4 Illustrative Examples 48
3.3 Admission Control 49
  3.3.1 Admission Control for Contention-Based Channel Access 50
  3.3.2 Admission Control for Pollled Channel Access 51
3.4 Power Management 51
  3.4.1 Legacy Power-Save Mechanism 52
3.4.2 Automatic Power Save Delivery
   3.4.2.1 Scheduled APSD 53
   3.4.2.2 Full Unscheduled APSD 54
   3.4.2.3 Hybrid Unscheduled APSD 55
   3.4.2.4 Illustrative Examples 56
3.5 QoS in Wireless Mesh Networks 57
3.6 Summary 59
3.7 End Note 59
3.7 References 61

Chapter 4 - Performance Understanding of IEEE 802.11 DCF and IEEE 802.11e EDCA 63
4.1 Introduction 63
4.2 IEEE 802.11 MAC Protocol 64
   4.2.1 DCF Overhead 67
4.3 Performance evaluation of the IEEE 802.11 DCF 69
   4.3.1 The Concept of Saturation Throughput 69
   4.3.2 Maximum Saturation Throughput 71
       4.3.2.1 Performance Bounds for 802.11b DCF 74
   4.3.3 Saturation Throughput Analysis 76
       4.3.3.1 Throughput Performance 80
       4.3.3.2 Delay Performance 82
4.4 MAC Enhancements for QoS Support 86
   4.4.1 IEEE 802.11e EDCA 86
   4.4.2 Further QoS Enhancement for Ad-Hoc Networks 89
4.5 Performance understanding of IEEE 802.11e EDCA 89
   4.5.1 CWmin Differentiation 91
   4.5.2 AIFS Differentiation 92
   4.5.3 Coexistence of EDCA AC_BE and legacy DCF stations 95
       4.5.3.1 Backoff Counter Decrement Rules 96
       4.5.3.2 Analysis of AC_BE Default Settings 98
       4.5.3.3 AIFSN=2 and Legacy DCF Stations 99
4.6 Conclusion 101
4.7 References 101

Chapter 5 - Cross-layer Optimized Video Streaming over Wireless Multi-hop Mesh Networks 105
5.1 Introduction 105
5.2 Proposed integrated cross-layer video streaming 107
   5.2.1 Wireless Multi-hop Mesh Topology Specification 109
   5.2.2 Link and Path Parameter Specification 110
   5.2.3 Application and Network-layer Parameter Specification 111
5.3 Problem Formulation 112
5.4 Video Streaming Optimization in the Multi-hop Mesh Network 114
   5.4.1 End-to-End Optimization 114
viii Contents

5.4.2 Optimization under a certain Horizon of Network Information 115
5.5 Complexity and Information Requirements of the Different Alternatives 119
5.6 Experimental Results 121
5.7 Further Reading 124
5.8 Conclusions 125
5.9 Appendix 126
5.10 References 127

Part III: 802.11 Security

Chapter 6 - Understanding and Achieving Next-Generation Wireless Security 131
6.1 Overview 131
6.2 Risks of Wireless Insecurity 132
6.3 Understanding Wi-Fi Protected Access (WPA) 132
6.3.1 WPA TKIP 133
6.3.2 802.1X - User Authentication and Network Access 134
6.3.3 WPA Cracking Tools 134
6.3.4 WPA Summary 135
6.4 The Way Forward: Wi-Fi Protected Access 2 (WPA2) and 802.11i 135
6.4.1 Increased Density of Access Points 136
6.4.2 Roaming Wireless Clients 136
6.4.3 Failover Requirements 136
6.5 WPA2: Under the Covers 137
6.5.1 WPA2 and 802.1X 137
6.5.2 WPA2 and TKIP 139
6.5.3 WPA2 and CCMP 139
6.5.4 WPA2 and Fast Roaming 140
6.5.4.1 PMK Caching 140
6.5.4.2 Pre-Authentication 141
6.6 Opportunistic PMK Caching: Fast Roaming at Its Fastest 141
6.7 Summary 143

Chapter 7 - Wireless Local Area Network Security 145
7.1 Introduction 145
7.2 Current Application Solutions 146
7.3 MAC-Level Encryption Enhancements 147
7.3.1 The TKIP Per-Packet Hash Function 147
7.3.2 TKIP Temporal Key Derivation 148
7.3.3 Message Integrity Code 149
7.3.4 AES Based Encryption and Data Authentication 149
7.4 Secret Key Distribution and Generation 150
7.5 Authentication 151
7.5.1 802.1x EAP Authentication 151
7.5.2 EAP-MD5 152
7.5.3 EAP-TTLS 153
Contents ix

7.5.4 IEEE 802.11 and RADIUS MAC Authentication 153
7.6 Evolution, Standards, and Industry Efforts 154
  7.6.1 Security-related changes in the TGn High Throughput Amendment 154
  7.6.2 Security-related changes in the TGr Fast BSS Transition Amendment 154
  7.6.3 Security in the TGs Mesh Amendment 154
  7.6.4 Security in the TGw Protected Management Frames Amendment 157
7.7 Wireless and Software Vulnerabilities 157
  7.7.1 Exploiting Wireless Device Drivers 157
  7.7.2 Discovering Driver Vulnerabilities 159
  7.7.3 Exploiting Driver Vulnerabilities 163
  7.7.4 Mitigating Driver Vulnerabilities 164
7.8 Wireless Intrusion Detection 166
  7.8.1 Deployment Models 167
    7.8.1.1 WIDS Overlay Deployment Model 167
    7.8.1.2 WIDS Integrated Deployment Model 167
  7.8.2 Analysis Techniques 168
    7.8.2.1 Signature Analysis 168
    7.8.2.2 Trend Analysis 170
    7.8.2.3 Anomaly Analysis 171
  7.8.3 Upper-Layer Analysis Mechanisms 172
  7.8.4 Wireless Countermeasures 174
    7.8.4.1 Adversary Denial of Service 174
    7.8.4.2 Role-Based Access Control Measures 175
7.9 References 176

Part IV: High Throughput 802.11

Chapter 8 - The 802.11n Standard 179
  8.1 Introduction 179
  8.2 IEEE 802.11n 180
  8.3 Preambles 180
  8.4 802.11n Transmitter 185
  8.5 LDPC Coding 186
  8.6 Space Time Block Coding 187
  8.7 Beamforming 188
  8.8 MAC Enhancements 188
  8.9 Use of 40 MHz Channels 189
  8.10 MIMO-OFDM Performance Results 189
  8.11 References 192

Chapter 9 - MIMO Spatial Processing for 802.11n WLAN 193
  9.1 Introduction 193
  9.2 MIMO OFDM System Overview 193
  9.3 Spatial Spreading 196
  9.4 Transmit Beamforming 197
Contents

9.4.1 Eigenvector Beamforming 197
9.4.2 Channel Sounding and Calibration 198
9.5 Receiver Structures 201
  9.5.1 Near-Optimal Iterative Receiver 201
  9.5.2 List Sphere Decoding 203
  9.5.3 Linear Receivers 203
9.6 Comparison of Spatial Spreading and Transmit Beamforming 204
  9.6.1 Simulation Setup 205
  9.6.2 Throughput vs Range Performance 206
  9.6.3 Packet Error Rate Performance 206
9.7 Complexity Analysis 207
  9.7.1 MMSE Processing 211
  9.7.2 Cholesky Decomposition 211
  9.7.3 LSD Search 211
  9.7.4 LSD Max-log-MAP 212
  9.7.5 Per-Stream LLR Computation 212
  9.7.6 Viterbi Decoding 212
  9.7.7 Examples 213
9.8 Conclusions 214
9.9 References 215

Part V: 802.11 Mesh Networks

Chapter 10 - Capacity of Wireless Mesh Networks 217
10.1 Introduction 217
10.2 Terminology 219
10.3 Single-radio Shared Wireless Mesh 219
10.4 Dual-Radio Shared Wireless Mesh 223
10.5 Multi-Radio Switched Wireless Mesh 225
10.6 Conclusion 229
10.7 Appendix: Capacity analysis for single, dual, multi-radio meshes 230
  10.7.1 String of pearls, mesh portal on one end 230
    10.7.1.1 Single-radio 230
    10.7.1.1.1 Lower bound 231
    10.7.1.1.2 Upper bound 231
    10.7.1.2 Dual-radio 231
    10.7.1.2.1 Lower bound 232
    10.7.1.2.2 Upper bound 232
    10.7.1.3 Multi-Radio 232
  10.7.2 String of pearls, mesh portal in middle 232
    10.7.2.1 Single-radio 232
    10.7.2.1.1 Lower bound 233
    10.7.2.1.2 Upper bound 233
    10.7.2.2 Dual-radio 233
    10.7.2.2.1 Lower bound 233
Contents xi

10.7.2.2.2 Upper bound 234
10.7.2.3 Multi-Radios 234
10.7.3 Full mesh on rectilinear grid 234
10.7.3.1 Single-radio 236
10.7.3.1.1 Lower bound 236
10.7.3.1.2 Upper bound 236
10.7.3.2 Dual-radio 236
10.7.3.2.1 Lower bound 236
10.7.3.2.2 Upper bound 237
10.7.3.3 Multi-Radio 237

Chapter 11 - Autonomous Mobile Mesh Networks and their Design Challenges 239
11.1 Introduction 239
11.2 Evolution of mobile mesh networks 240
11.3 Usage Scenarios for Mobile Mesh Networks 242
11.3.1 Mobile Mesh Networks for Public Safety Services 242
11.3.2 Disaster Relief Operations 243
11.3.3 Defense Network-centric Operations 244
11.3.4 Enterprise Applications 244
11.3.5 Logistics 244
11.3.6 Consumer/Home Networking 245
11.3.7 Transportation Applications 245
11.3.8 Video Surveillance 245
11.4 Performance Requirements for Mobile Mesh and Applications 246
11.4.1 General Performance Metrics for the Internet 246
11.4.2 Performance Metrics for Mobile Ad hoc Networks 246
11.5 Design Challenges for Mobile Mesh Networks 247
11.5.1 Physical Radio Channels 249
11.5.2 Medium and Mesh Network Access 249
11.5.3 Routing and Multicasting 250
11.5.4 Security 251
11.5.5 IP addressing 252
11.5.6 Roaming 253
11.5.7 Data Transfer Reliability 254
11.5.8 Quality of Service (QoS) 254
11.5.9 Network Management 255
11.5.10 Distributed Services in a Mobile Mesh 256
11.5.11 Applications 256
11.6 Conclusions 257
11.7 References 257

Chapter 12 – Service Provisioning for Wireless Mesh Networks 261
12.1 Introduction 261
12.2 Wireless Mesh Networks 262
12.3 Service Offerings 263
12.3.1 Free Internet Access (Unregistered) 265
Contents

12.3.2 Free Internet Access (Registered) 265
12.3.3 Flat-Rate Fee-Based Public Access 267
12.3.4 Differentiated-Rate Fee-based Public Access 267
12.4 Web Filtering 269
12.5 Wireless Spectrum Preservation 269
12.6 Public Safety 271
12.7 Video Surveillance 272
12.8 Mobile Government Users 273
12.9 Virtual Private Networks (VPN) 274
12.10 Voice over IP (VoIP) 275
12.11 Meter Reading 275
12.12 Government as Anchor Tenant 276
12.13 Dedicated Internet Access 276
12.14 Advanced Network Services 278
12.15 Conclusions 278

Chapter 13 - Metro-Scale Wi-Fi Networks 281
13.1 Introduction 281
13.2 Wireless Broadband Initiatives 282
13.3 Network Use Cases and Performance Requirements 283
13.4 Multi-Tier Network Design Overview 285
13.5 Wi-Fi Tier Design 290
13.6 Mesh Tier Design 293
13.7 Injection Tier Design 297
13.8 Network-wide Seamless Mobility Support 298
13.9 Conclusion 302
13.10 References 303

Chapter 14 - Usage and Performance Comparison of Mobile MetroMesh Networks 307
14.1 MetroMesh Network Architecture 307
14.2 Predictive Wireless Routing Protocol (PWRP) 309
14.2.1 Scalable routing 309
14.2.2 Throughput-optimized routing 309
14.2.3 RF spectrum management 309
14.2.4 Multi-mode routing 310
14.2.5 Seamless session-persistent mobility 310
14.2.6 Dynamic rate-limiting and traffic management 310
14.2.7 Correlated Mesh Data Protocol (CMDP) 311
14.2.8 Patents 311
14.3 Overview of the Networks 311
14.3.1 Client Usage 311
14.3.2 Client Link Performance 312
14.3.3 Mesh Network Performance 312
14.4 Hourly Usage Patterns 314
14.4.1 For-Fee Network 314
Contents

14.4.2 Free Network
14.5 Summary
14.6 References

Chapter 15 - First, Second and Third Generation Mesh Architectures
15.1 Introduction
15.2 Three Generations of Mesh Architectures
15.3 Bandwidth degradation on Single Channel Backhauls
15.4 Latency/Jitter Degradation on Single Channel Backhauls
15.5 Frequency Agility
15.6 Radio Agnostic Mesh
15.7 New Applications Enabled by Third Generation Wireless Mesh
15.8 Conclusions

Chapter 16 - Wireless Mesh Networks
16.1 Introduction
16.1.1 History
16.1.2 The Benefits of Wireless Mesh Networking
16.1.3 Some Typical Deployment Scenarios
16.1.4 Other Wireless Solutions
16.2 Current Issues and Solutions
16.2.1 Network Structure
16.2.2 Intra-mesh Channel Re-use
16.2.3 Medium Access Contention
16.2.4 Mesh Routing and Forwarding
16.2.5 Mesh Security
16.2.6 Congestion Control
16.2.7 Fairness
16.2.8 UDP and TCP Performance
16.2.9 Voice over Mesh
16.2.10 Mesh Network Management
16.3 Mesh Deployment Issues
16.4 IEEE 802.11, Amendment “s”
16.4.1 Overview
16.4.2 The IEEE 802.11s Mesh Network Model
16.4.3 Mesh Discovery
16.4.4 Peer Link Establishment
16.4.5 Mesh Security
16.4.6 Routing Metrics
16.4.7 Routing and Metrics
16.4.8 Forwarding
16.4.9 Interworking
16.4.10 MAC Enhancements
16.5 Conclusion
16.6 References
Part VI: 802.11/Cellular Interworking

Chapter 17 - WLAN Interworking with 2G/3G Systems 351
17.1 Introduction 352
17.2 Standards related activities 353
  17.2.1 3GPP2 353
  17.2.2 3GPP 354
17.3 WLAN Interworking Plumbing 357
  17.3.1 WLAN Association 360
    17.3.1.1 Scanning Process 361
    17.3.1.2 Manual Scan Procedures 362
    17.3.1.3 Automatic Scan Procedures 362
    17.3.1.4 Access Point Sets Definition 362
    17.3.1.5 Iterations in making WLAN system selection 363
    17.3.1.6 Scan Types 363
    17.3.1.7 Candidate Set Selection 365
    17.3.1.8 RSSI Filtering 365
    17.3.1.9 Time delay for subsequent scan event 366
    17.3.1.10 Active Set Selection 366
  17.3.2 WLAN De-Selection 367
    17.3.2.1 In Traffic Operation 368
    17.3.2.2. IP Address Assignment 368
  17.3.3 PDIF Discovery Mechanisms 369
  17.3.4 Tunnel establishment procedures 369
    17.3.4.1 Error Scenario 1 375
    17.3.4.2 Error Scenario 2 375
  17.3.5 UDP encapsulation to support NAT Traversal 376
  17.3.6 Acquiring configuration information 378
  17.3.7 Rekeying Procedures 378
    17.3.7.1 Rekeying of IKE_SA 379
    17.3.7.2 Rekeying of CHILD_SA 380
  17.3.8 Tunnel Disconnect Procedures 381
    17.3.8.1 MS-initiated tunnel disconnection 381
    17.3.8.2 PDIF-initiated tunnel disconnection 382
    17.3.8.3 H-AAA-initiated tunnel disconnection 383
  17.3.9 Application specific Child SA support 384
  17.3.10 NAT Keep Alive and Dead-Peer Detection procedures 385
    17.3.10.1 NAT Keep Alive 385
    17.3.10.2 Dead Peer Detection (DPD) 385
  17.3.11 Voice call establishment procedures 385
    17.3.11.1 Procedures for the packet-switched domain 386
  17.3.12 Supporting mobility without the VCC feature 387
    17.3.12.1 Solutions supporting mobility 388
  17.3.13 Voice Call Continuity 397
  17.3.14 Domain Registration 401
    17.3.14.1 IMS Registration in the IP-CAN domain 401
Chapter 18 - Towards Service Continuity in Emerging Heterogeneous Mobile Networks

18.1 Introduction

18.2 Related Work

18.3 Proposed Architecture

18.3.1 Solution Space

18.3.2 Mobility Security Association Bootstrapping

18.3.3 Performance Optimization

18.3.4 Traversing Network Address and Port Translators

18.4 Evaluation

18.4.1 Results

18.4.2 Analysis and Discussion

18.5 Conclusions
Chapter 19 - A Survey of Analytical Modeling for Cellular/WLAN Interworking 441

19.1 Introduction 441
19.2 Cellular/WLAN Interworking Architectures 442
  19.2.1 Loose Coupling Architecture 442
  19.2.2 Tight Coupling Architecture 444
  19.2.3 Hybrid Coupling Architecture 445
  19.2.4 IMS Architecture for 3GPP/3GPP2-WLAN Interworking 446
19.3 Simple Models for Cellular/WLAN Interworking 448
  19.3.1 Cellular/WLAN Model using Birth-Death Processes 448
    19.3.1.1 Model Assumptions 448
    19.3.1.2 Mobility Model 449
    19.3.1.3 Traffic Equations in the Cellular Network 449
    19.3.1.4 Traffic Equations in the WLAN 450
    19.3.1.5 Performance Measures 451
  19.3.2 Cellular/WLAN Model using Multidimensional Markov Chains 452
    19.3.2.1 Model Assumptions 452
    19.3.2.2 Performance Measures 453
19.4 Further Analytical Models for Cellular/WLAN Interworking 454
  19.4.1 WLAN Capacity 454
  19.4.2 Other Mobility Models 456
    19.4.2.1 Non-uniform Mobility within a Single Cell 456
    19.4.2.2 A Cell Residence Time Model for Two-Tier Integrated Wireless Networks 456
  19.4.3 Models with General Distributions 458
    19.4.3.1 Traffic Equations of Handoff Rates 459
    19.4.3.2 Channel Holding Times 461
19.5 Simulation Models 462
19.6 Open Issues 463
19.7 Conclusions 464
19.8 References 465

Part VII: Coexistence

Chapter 20 - Coexistence of Unlicensed Wireless Networks 469

20.1 Introduction 469
20.2 Overview of Unlicensed Frequency Bands 469
  20.2.1 ISM and U-NII Frequency Bands 470
  20.2.2 The 3650 MHz Frequency Band 472
  20.2.3 VHF and UHF Television Frequency Bands 473
20.3 Survey of Unlicensed Wireless Networks 474
  20.3.1 Wireless Local Area Network (WLAN) 474
  20.3.2 Wireless Personal Area Network (WPAN) 476
  20.3.3 Wireless Metropolitan Area Network (WMAN) 477
Contents xviii

23.3.2 Components of a Cognitive WLAN 531
   23.3.2.1 Clustering 531
   23.3.2.2 RF Analysis 531
   23.3.2.3 Integrity Management 532
23.4 Features and Benefits of the Architecture 533
23.5 The Vision for the Future 533

Part IX: 802.11 Range

Chapter 24 - Wi-Fi Range: Impact on Data Rates, Coverage, and Capacity 535
24.1 Introduction 535
24.2 Defining Range and Coverage 535
24.3 Range Basics 536
24.4 Antenna Design 537
24.5 Range and Coverage 539
24.6 Range Limiting Factors 539
   24.6.1 Interference 539
   24.6.2 Multi-Path 540
   24.6.3 Attenuation 541
   24.6.4 Hidden Node 542
24.7 Signal to Noise Ratio 543
24.8 Range versus Capacity 544
24.9 Site Surveys and Dead Spots 546
24.10 Future Technologies 547
24.11 Long Range Wi-Fi Case Study 549
24.12 Summary 550

Part X: 802.11 Hardware Design

Chapter 25 - An 802.11g WLAN System on a Chip 551
25.1 Introduction 551
25.2 Architecture 552
25.3 Implementation 553
   25.3.1 Receiver 553
   25.3.2 Transmitter 554
   25.3.3 Synthesizer 556
25.4 SoC Integration 557
   25.4.1 Calibration 557
   25.4.2 Noise isolation 557
25.5 Experimental Results 558
25.6 Conclusion 561
25.7 References 561
## Chapter 26 - Antenna Design for Portable Computers

26.1 Introduction  
26.1.1 Source of radiation  
26.1.2 Factors Affecting Small Antenna Design  
  26.1.2.1 Conductor Area  
  26.1.2.2 Radiation Resistance  
  26.1.2.3 Radiation Efficiency  
  26.1.2.4 Antenna Q  
26.1.3 Fundamental Limits of Electrically Small Antennas  
  26.1.3.1 Chu-Harrington Limit on Q  
  26.1.3.2 Fundamental Gain Limitation  
  26.1.3.3 Qualification Metrics  
  26.1.3.4 Q-Volume Space  
  26.1.3.5 Q-Volume Space: Example Antennas  
26.1.4 WLAN/WWAN Antenna Requirements  
  26.1.4.1 Secondary Design Considerations  
  26.1.4.2 Antenna Location Selection  
  26.1.4.3 Example Gain and Radiation Patterns  
26.2 Power Statistics of Small Scale Fading in Rayleigh Radio Channels  
26.3 Diversity Architectures  
26.4 Rician Channel Power Statistics  
  26.4.1 Diversity Gain of Omni-Antennas in Rician Channels  
  26.4.2 Diversity Gains of Multiple Antennas under Rician Fading  
26.5 Conclusion  
26.6 References

## Part XI: Wi-Fi Hotspots

### Chapter 27 - Service Control and Service Management of Wi-Fi Hotspots

27.1 Wi-Fi Hotspots Introduction  
27.2 Brief History of Hotspots  
  27.2.1 Overview of Commercial Hotspots  
  27.2.2 Overview of Free Hotspots  
  27.2.3 Wi-Fi Hotspot Signal Range  
  27.2.4 Advantages of Wi-Fi  
27.3 Service Management - Overview  
  27.3.1 Hotspot Service Management  
  27.3.2 Importance of Service Management  
  27.3.3 Network and Data Management Services  
  27.3.4 Obtaining a Network Address  
  27.3.5 Obtaining a Host Address  
  27.3.6 Authentication, Authorization and Accounting for Hotspots  
    27.3.6.1 Authentication  
    27.3.6.2 Authorization  
    27.3.6.3 Accounting  
27.3.6.1 Authentication  
27.3.6.2 Authorization  
27.3.6.3 Accounting
Contents

27.3.7 User Login Page 596
27.4 QoS Services 597
  27.4.1 Per User QoS 598
  27.4.2 Service Level Agreements (SLA) 598
    27.4.2.1 Packages 599
    27.4.2.2 Price Plan 599
    27.4.2.3 Prepaid Cards 599
  27.4.3 Billing and Payment 599
  27.4.4 Network monitoring 599
  27.4.5 Customer Care 600
  27.4.6 Reports 600
  27.4.7 Alerts 600
  27.4.8 Contracts and Tariffs 601
27.5 Wi-Fi Network Designs 601
  27.5.1 Centralized Control over Services for Wi-Fi Networks 601
  27.5.2 Virtual partitioning of wireless network for different types of users 603
  27.5.3 Additional revenue generation opportunities 603
  27.5.4 Session Intercepts and “Hot-Lining” 605
27.6 Lawful Intercept for Communications Assistance for Law Enforcement Act 606
27.7 Security in Wi-Fi 606
  27.7.1 Security Benefits 606
    27.7.1.1 Data privacy 606
    27.7.1.2 Authentication 607
    27.7.1.3 Reliability 607
27.8 Future Technologies 607
  27.8.1 Mobile Hotspots 607
  27.8.2 Managed Services Platform 607
  27.8.3 Wi-Max 607
  27.8.4 Virtual Network Operators 608
27.9 Summary 608

Chapter 28 - Hot Spots: Public Access using 802.11 609
28.1 Introduction 609
28.2 Access Control 610
28.3 New Trends 614
  28.3.1 Trends in Wi-Fi Enabled Devices 614
  28.3.2 Trends Multi-Purpose Access 615
28.4 Architecture 616
28.5 Trends in Municipal Wi-Fi 617
28.6 Trends in Advertising on Wi-Fi Networks 618
28.7 Trends in WiMax 618
28.8 Hotspot dangers and issues 619
  28.8.1 Phishing 619
  28.8.2 Fake hotspots 620
  28.8.3 Worms and Viruses 620
  28.8.4 Snorting 621
### Chapter 28 - Peer-to-Peer File Sharing and DDoS Prevention

28.8.5 Port Isolation
28.8.6 Peer-to-peer file sharing
28.8.7 DMCA
28.8.8 “Whack a mole”
28.8.9 CALEA

28.9 Summary
28.10 References

### Chapter 29 - Strategies for Maximizing Access to Public Commercial Hot Spots

29.1 Retail Service Offerings
- 29.1.1 Day passes
- 29.1.2 Time-based passes
- 29.1.3 Subscriptions
- 29.1.4 PIN-based or Pre-paid Access
- 29.1.5 Private services

29.2 Neutral Host Network Configurations (Roaming)
- 29.2.1 Neutral Host Overview
- 29.2.2 Universal Access Method (UAM) Roaming
- 29.2.3 Smart Client Roaming
- 29.2.4 Smart Client Roaming “Standards” – WISPr and GIS
  - 29.2.4.1 WISPr
  - 29.2.4.2 GIS

29.3 Provisions for Enabling Devices
- 29.3.1 Wi-Fi Enabled Device Overview
- 29.3.2 Laptops
- 29.3.3 PDAs
- 29.3.4 Dual-Mode Mobile Phones and Wi-Fi VoIP Phones
- 29.3.5 Other Mobile Devices (cameras, MP3 players, gaming consoles)

### Part XII: Wi-Fi Applications

#### Chapter 30 - A Discussion of 802.11 for Sensor Networks

30.1 Introduction
30.2 Sensor Network Radio Considerations
- 30.2.1 Sensor Network Specific Radios and Standards
- 30.2.2 Radio Range and Network Scalability
30.3 802.11 Ad-hoc Mode: An Enabler for Sensor Network
30.4 802.11 Power Usage Suitability for Sensor Networks
30.5 A WLAN for a Field of Sonobuoys
- 30.5.1 The Requirements of the NEASW WLAN
- 30.5.2 Radio Range on the Ocean Surface
- 30.5.3 Inter-Buoy Communication Throughput
- 30.5.4 Buoy Energy Availability
- 30.5.5 NEASW Hardware and Software System
- 30.5.6 NEASW Mobile Adhoc Network (MANET)
Contents

30.5.7 NEASW Disruption Tolerant Transport Mechanism 651
30.5.8 NEASW WLAN Demonstration and Results 653
30.6 Conclusion 656
30.7 References 656

Chapter 31 - Wi-Fi based Tracking Systems 661
31.1 “Where’s my stuff?” 661
31.2 Benefits of Tracking 661
31.3 What exactly are RFID and RTLS? 662
    31.3.1 A Review of RFID/RTLS Development 662
    31.3.2 Passive RFID 663
    31.3.3 Active RFID 663
    31.3.4 RTLS System 663
    31.3.5 How RTLS works? 663
31.4 Summary of Timing-based Technologies 664
    31.4.1 The angle of arrival approach (AOA) 664
31.5 Positioning Alternatives 665
    31.5.1 Location estimation 665
    31.5.2 The Cell ID approach 665
    31.5.3 Triangulation-based approaches 666
    31.5.4 Ekahau Estimation Technology 666
    31.5.5 Ekahau Site Calibration 667
    31.5.6 Ekahau Rail Tracking 667
    31.5.7 Normalizing RSSI scales 668
    31.5.8 Configuring Access Points 668
    31.5.9 Adding “dummy” access points 669
    31.5.10 Associating with the Host Network 669
31.6 Conclusion 670

Chapter 32 - Building the Mobile Computing Environment through
    Context-Aware Service Management 671
32.1 Introduction 671
32.2 Trends 672
    32.2.1 Maximizing employee process efficiency and time savings 672
    32.2.2 Mobile users behave fundamentally different from Desktop users 672
    32.2.3 Mobile devices are not Laptops 673
    32.2.4 Mobile devices to adapt to various types of connectivity 674
    32.2.5 Mobile services to have a different life cycle then desktop services 674
32.3 The Basic Components in the Appear Platform 675
    32.3.1 Foundation features 675
32.4 Scientific theories vs. practical implementations 677
32.5 Context-aware Over-the-Air Service Provisioning (OTA) 678
32.6 Context-aware Over-the-Air Service Synchronization 681
32.7 Context-aware Service 682
    32.7.1 Context-aware tracking and dynamic change of application behavior 682
    32.7.2 Context aware Voice over IP 682
Chapter 32 - Implementing context-awareness
32.7.3 Implementing context-awareness 683
32.8 Networking and Appear Products 683
32.8.1 Network Configuration 683
32.8.2 Device Detection and Change Publishing 685
32.9 Some Case Studies 685
32.9.1 Stockholm Metro 685
32.9.1.1 The Solution 686
32.9.1.2 The impact 687
32.9.2 Southwest Florida International Airport (SWFIA) Context-Aware Wireless Emergency Response 689
32.9.2.1 Fast Emergency Response is Critical 689
32.9.2.2 A Context-Aware Wireless Emergency Response Solution 689
32.9.2.3 The Value of Context 690
32.9.3 RATP 691
32.9.3.1 Improving Operations and Customer Service 691
32.9.3.2 A Context-Aware Solution 691
32.9.3.3 The Value of Context 691
32.9.3.4 Return on Investment 691
32.9.4 Dutch Rail (NS) Mobile Frontliners 692
32.9.4.1 Operational and Productivity Gains using Context 692
32.9.4.2 A Context-Aware Solution 693
32.9.4.3 The Value of Context 693
32.10 References 693

Chapter 33 - Experiments Using Small Unmanned Aircraft to Augment a Mobile Ad Hoc Network 695
33.1 Introduction 696
33.2 AUGNet Architecture 698
33.2.1 The Mesh Network Node (MNN) 699
33.2.2 The Test-Bed Monitoring Agent 700
33.2.3 The Ares UA 701
33.3 Test Bed Experiment Plan 702
33.4 Experiment Set 1, Baseline Network Measurements 705
33.4.1 Experiment 1.1, Fixed Ground Nodes 705
33.4.2 Experiment 1.2, Mobile Ground Nodes 706
33.4.3 Experiment 1.3, Fixed Ground Nodes with UA 706
33.4.4 Experiment 1.4, Mobile Ground Nodes with UA 707
33.5 Experiment Set 2, Scenario 1: Improved Connectivity 707
33.5.1 Experiment 2.1, Mobile Node at Edge 707
33.5.2 Experiment 2.2, Mobile Node at Edge with UA 707
33.5.3 Experiment 2.3, Disconnected Groups 707
33.5.4 Experiment 2.4, Disconnected Groups with UA 708
33.6 Experiment Set 3: Scenario 2: Increased UA Range 708
33.6.1 Experiment 3.1, Ground-Ground Range 708
33.6.2 Experiment 3.2, UA-Ground Range 708
33.6.3 Experiment 3.3, UA-UA Range 709
Part XIII: Ultra WideBand (UWB)

Chapter 34 - Ultra-Wideband Wireless Technology

34.1 Introduction 719
34.2 Regulators Weigh in on UWB 720
  34.2.1 Summary of US Rules on UWB 721
  34.2.2 Summary of UWB Rules Specific to Japan 722
  34.2.3 Summary of the EC Decision on UWB 722
  34.2.4 UWB Definitions 724
34.3 UWB Radio Technologies 724
  34.3.1 Continuous-pulse UWB Technology 726
  34.3.2 CWave™ UWB Technology 728
  34.3.3 IEEE802.15.4a UWB Technology 730
  34.3.4 Direct Sequence UWB 731
  34.3.5 TM-UWB Technology 732
  34.3.6 A Multiband OFDM Approach to Utilizing UWB 733
  34.3.7 A Multi-band Approach to UWB 733
  34.3.8 TRD-UWB Technology 734
34.4 UWB Short Pulse Radiation and Reception 735
  34.4.1 Pulse Bandwidth and EIRP 735
  34.4.2 UWB Wavelet Radiation 735
  34.4.3 Radiation of a UWB Elementary Dipole and Loop 736
  34.4.4 Receiving UWB Wavelets 738
34.5 Propagation of UWB Signals 738
  34.5.1 The SBY Propagation Model 739
  34.5.2 Relation to Maximum Rake Gain 739
  34.5.3 An In-Room Ray Tracing Model 739
  34.5.4 Stochastic Propagation models 741
34.6 Recovering UWB Impulse Energy 741
34.7 A UWB Link Performance 742
34.8 Applications and Markets of UWB Systems 742
  34.8.1 Radar and Imaging 742
  34.8.2 High-Rate Wireless Communication 743
  34.8.3 Low-Rate Communications and High-Precision Location and Tracking 743
Chapter 35 - High-rate WPAN

35.1 Introduction

35.2 Trends and Application Scenarios
   35.2.1 The Increasing Need for Higher Date Rates
   35.2.2 Applications areas
   35.2.3 Regulatory Considerations

35.3 Benefits of Wide-Band Transmission
   35.3.1 From Multipath Performance Perspective
   35.3.2 From Interference Perspective

35.4 Overview of the WiMedia 1.0 MAC

35.5 Overview of the WiMedia 1.0 PHY
   35.5.1 Introduction
   35.5.2 Band Hopping and Time Frequency Codes (TFCs)
   35.5.3 WiMedia OFDM Parameters and Sub-carrier Allocation Scheme
   35.5.4 PLCP Layer
      35.5.4.1 PLCP Preamble
      35.5.4.2 PLCP Header
      35.5.4.3 Encoding of PSDU
      35.5.4.4 Dual Carrier Modulation (DCM)
      35.5.4.5 Frequency Domain and Time Domain Spreading
   35.5.5 OFDM Modulation

35.6 Receiver Algorithms
   35.6.1 Top-level Structure
   35.6.2 Synchronization
      35.6.2.1 Introduction
      35.6.2.2 Auto-correlation
      35.6.2.3 Hierarchical Delayed-correlation
      35.6.2.4 Hierarchical Cross-correlation (H-Xcorr)
      35.6.2.5 Second-stage Correlator
      35.6.2.6 Burst Detection
      35.6.2.7 Frequency Offset Estimation
      35.6.2.8 Timing (Optimum Start of the FFT Window)
      35.6.2.9 DC Offset, Narrow-Band Interference (NBI) and SOP
   35.6.3 AGC
   35.6.4 Timing Error Tracking
   35.6.5 Common-Phase Error Estimation and Tracking
   35.6.6 Zero-padded OFDM Guard Processing
   35.6.7 Channel Estimation and Equalization
      35.6.7.1 Channel Estimation for Different TFCs
      35.6.7.2 Channel Equalization
   35.6.8 In-band Interference Mitigation
   35.6.9 Improved Channel Estimation and Noise Variance Estimation
      35.6.9.1 Generating the reference header symbols from the slicer output
## Contents

35.6.9.2 Generating the reference header symbols from the Viterbi decoder output (iterative decoding) 780  
35.6.10 Multiple Antenna Receiver 780  
35.7 Overview of Next Generation High-speed UWB systems 782  
  35.7.1 Higher-order Constellation 782  
  35.7.2 MIMO 783  
  35.7.3 Wider Bandwidth 783  
  35.7.4 Brute-Force Approach 783  
35.8 Limitations on Capacity/Bit-rate and Next Candidate Technologies 784  
  35.8.1 60 GHz 784  
  35.8.2 Free-space Optics (FSO) and Terra-Hertz (THz) Band 785  
  35.8.3 Cognitive Radios 785  
35.9 References 786  

**Part XIV: Public Wireless Broadband**

### Chapter 36 - Wireless Cities

36.1 Introduction 791  
  36.1.1 What is in it for local authorities? 791  
36.2 The council worker and the resident 792  
36.3 The business traveller and the mobile worker 794  
36.4 Wi-Fi changing the profile of gaming 796  
36.5 The entertainer 797  
36.6 The Wi-Fi tourist 797  
36.7 Wi-Fi art thou Romeo? 798  
36.8 The application challenge 799  
  36.8.1 Enterprise mobility for efficiency and effectiveness 800  
  36.8.2 Creating an agile infrastructure 800  
  36.8.3 Increasing the opportunities for all 801  
  36.8.4 Sharing services 801  
  36.8.5 Examples of applications 801  
36.9 Frequently asked questions answered 802  
  36.9.1 Is Wi-Fi just for larger cities? 802  
  36.9.2 When is the right time for me to roll out a wireless network? 802  
  36.9.3 What’s the difference between an ‘owned’ and ‘operator’ network? 803  
  36.9.4 Paid-for versus free: what’s the best solution? 803  
  36.9.5 What should local authorities advise citizens about wireless security? 803  
  36.9.6 Are there any public health issues with wireless networks? 803  
  36.9.7 How can local authorities avoid restricting competition? 804

### Chapter 37 - The Path to 4G and the Mobilization of the Internet

37.1 Introduction 805  
37.2 Mobilizing traditional and emerging media, communications and commerce business models 806  
37.3 Role of licensed and unlicensed technologies for the mobile Internet 807
Chapter 37 - All Internet is Local: Five Ways Public Ownership Solves the U.S. Broadband Problem

37.1 Introduction 823
37.2 What is Public Ownership? 824
37.3 An Astonishingly Brief History of Telecommunications Regulation 825
  37.3.1 That Was Then 825
  37.3.2 This is Now 826
37.4 Why Public Ownership? 828
37.5 Broadband Access and Competition: Truth and Fiction 837
37.6 Evaluating “Public-Private Partnerships” and Other Private Business Models 838
37.7 The Dollars and Sense of Public Ownership 840
  38.7.1 Risk 842
  38.7.2 A Note About Municipal “Failures” 844

Epilogue 847

Index 849