



universal personal communications

Anand R. Prasad
Neeli R. Prasad

802.11 WLANs *and* IP Networking

security, QoS, and mobility



802.11 WLANs and IP Networking

Security, QoS, and Mobility

For a listing of recent titles in the *Artech House Universal Personal Communications Series*, turn to the back of this book.

802.11 WLANs and IP Networking

Security, QoS, and Mobility

Anand R. Prasad
Neeli R. Prasad



**ARTECH
HOUSE**

BOSTON | LONDON
artechhouse.com

Library of Congress Cataloging-in-Publication Data

Prasad, Anand R., Neeli R. Prasad

A catalog record for this book is available from the Library of Congress.

British Library Cataloguing in Publication Data

Prasad, Anand

802.11 WLANs and IP networking: security, QoS, and mobility.—(Artech House mobile communications library)

1. Wireless LANs 2. Local area networks (Computer networks)

I. Title II. Prasad, Neeli

621.3'821

ISBN 1-58053-789-8

Cover design by Yekaterina Ratner

© 2005 Anand R. Prasad and Neeli R. Prasad

All rights reserved. Printed and bound in the United States of America. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher. All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Artech House cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

International Standard Book Number: 1-58053-789-8

10 9 8 7 6 5 4 3 2 1

*To our parents Jyoti and Ramjee Prasad,
our brother Rajeev,
and our families Akash, Ruchika and Sneha and Jami*

Contents

Preface	xix
Acknowledgments	xxi
Chapter 1 Introduction	1
1.1 Basic Concept of WLANs	1
1.2 Benefits of WLANs	4
1.2.1 Mobility	4
1.2.2 Short-Term Usage	5
1.2.3 Speed of Deployment	5
1.2.4 Difficult Wiring Environment	5
1.2.5 Scalability	6
1.3 Basic Concept of Wireless IP	6
1.4 Market Trend	7
1.5 Requirements of WLANs	9
1.6 Issues	10
1.6.1 General Issues	11
1.6.2 Attenuation	12
1.6.3 Multipath	13
1.6.4 UHF Narrowband	15

1.6.5	Infrared	15
1.6.6	Health Consideration	15
1.7	Future Directions	17
1.7.1	WLANs	17
1.7.2	WWANs	18
1.7.3	WPANs	19
1.8	The Next Generation	21
1.9	Overview of the book	23
	References	24
	Appendix 1A: Comparison of WLAN and WPAN Technologies	31
Chapter 2	Market and Business Cases	33
2.1	Introduction	33
2.2	Market Development	34
2.2.1	WLAN Target Market	36
2.2.2	WLAN Providers	37
2.2.3	Billing	39
2.3	Forces in Motion	42
2.4	Business Case	44
2.4.1	Business Assessment of Various Hotspot Scenarios	45
2.5	Future Growth Areas and Factors	46
	References	47
Chapter 3	IEEE 802.11	49
3.1	IEEE 802 Standardization Process	49
3.2	Overview of IEEE 802 Activities	50

3.3	IEEE 802 Current Activities	51
3.3.1	802.15	51
3.3.2	802.16	53
3.3.3	802.18	53
3.3.4	802.19	54
3.3.5	802.20	54
3.3.6	802.21	54
3.4	Basic IEEE 802.11	54
3.4.1	IEEE 802.11 Features	55
3.4.2	IEEE 802.11 Topology	56
3.4.3	IEEE 802.11 Logical Architecture.....	59
3.5	Medium Access Control Layer	60
3.5.1	Inter Frame Spacing.....	61
3.5.2	Distributed Coordination Function	62
3.5.3	RTS/CTS.....	65
3.5.4	Fragmentation	66
3.5.5	Point Coordination Function.....	67
3.5.6	Scanning.....	69
3.5.7	Association.....	70
3.5.8	Authentication.....	70
3.5.9	Encryption.....	71
3.5.10	Roaming.....	72
3.5.11	Synchronization	72
3.5.12	Power Management	73
3.6	IEEE 802.11 Physical Layers	74
3.6.1	DSSS.....	74
3.6.2	802.11 DSSS at 1 and 2 Mbps	74
3.7	IEEE 802.11b	76

3.7.1	IEEE 802.11b Channels	79
3.8	IEEE 802.11a	80
3.8.1	802.11a OFDM Parameters	81
3.8.2	802.11a Channelization.....	82
3.8.3	802.11a OFDM Signal Processing.....	82
3.8.4	Training.....	83
3.9	New PHY: IEEE 802.11g	85
3.10	Security: IEEE 802.11i	87
3.11	QoS: IEEE 802.11e	87
3.12	IAPP: IEEE 802.11f	88
3.13	Other IEEE 802.11 Activities	88
3.13.1	IEEE 802.11h.....	89
3.13.2	IEEE 802.11j.....	89
3.13.3	IEEE 802.11k.....	89
3.13.4	IEEE 802.11n.....	89
3.13.5	Upcoming Activities	89
	References	90
	Selected Bibliography	92
Chapter 4	Security	95
4.1	Security Threats and Goals	95
4.1.1	Threats	95
4.1.2	Goals	97
4.1.3	Mapping Security Threats to Goals	98
4.2	Related Information	98
4.2.1	IPSec	99
4.2.2	Network Address Translation	104
4.2.3	IPSec and NAT	105
4.2.4	Secure Socket Layer	105

4.2.5	Kerberos	107
4.2.6	RADIUS and Diameter	109
4.2.7	IEEE 802.1x	110
4.2.8	Extensible Authentication Protocol	112
4.3	IEEE 802.11 Security Issues	117
4.3.1	Authentication	118
4.3.2	Confidentiality	119
4.3.3	Integrity	120
4.3.4	Access Control	120
4.3.5	Other Issues	121
4.3.6	Tools	122
4.3.7	Security Issues in Other Solutions	123
4.4	Countermeasures	123
4.4.1	Personal Firewalls	123
4.4.2	Biometrics	124
4.4.3	Virtual Private Networks	124
4.4.4	Public Key Infrastructure	126
4.4.5	Intrusion Detection System	127
4.5	WPA and IEEE 802.11i RSN	127
4.5.1	IEEE 802.11i Services	128
4.5.2	RSN Information Elements	128
4.5.3	Key Hierarchy	129
4.5.4	Handshake Protocols	132
4.5.5	SAs in RSN Association	132
4.5.6	Discovery Process	134
4.5.7	Pre-Authentication	134
4.5.8	TKIP	134
4.5.9	CCMP	136

4.5.10	IBSS	139
4.6	Comparison	139
	References	140
Chapter 5	Quality of Service	147
5.1	Introduction	147
5.2	Voice Communication Requirement	149
5.2.1	Voice over Wireless Challenges	149
5.2.2	Voice Quality and Characteristics	149
5.3	Limitations of Legacy 802.11 MAC	150
5.3.1	Distributed Coordination Function	150
5.3.2	Point Coordination Function	151
5.4	QoS Support Mechanism of 802.11e	152
5.4.1	Enhanced Distributed Channel Access	153
5.4.2	HCF Controlled Channel Access (HCCA)	155
5.4.3	Coexistence of DCF, PCF and HCF	156
5.4.4	Interpretation of Priority Parameters in MAC Service Primitives	157
5.4.5	Admission Control at the HC	159
5.5	Other QoS-Related IEEE 802.11 Standards	161
5.6	QoS Requirements for Heterogeneous Traffic	161
5.7	Signaling and Control Protocols	162
5.7.1	H.323	163
5.7.2	Session Initiation Protocol	164
5.7.3	Real Time Streaming Protocol	165
5.8	Media Gateway Protocols	165
5.9	Transport Protocols	165
5.9.1	Real Time Protocol (RTP)	166

5.9.2	Real Time Control Protocol (RTCP)	166
5.10	Network-Level QoS	167
5.10.1	Integrated Services (IntServ)	167
5.10.2	Differentiated Services (DiffServ)	171
5.10.3	Drawbacks of DiffServ Mechanism	176
5.10.4	IntServ over DiffServ	177
5.10.5	Policy Management and Billing	177
5.11	QoS Support Across Heterogeneous Access Networks	179
5.11.1	Top-to-Bottom System QoS Model	180
5.11.2	Intra- and Inter-Domain End-to-End QoS for Heterogeneous Access Networks	181
5.12	Voice over WLAN Products	183
	References	184
Chapter 6 Roaming, Handover and Mobility		187
6.1	Handover and Mobility Management	187
6.1.1	Mobility Management	187
6.1.2	Handover	189
6.1.3	Handover Metrics and Initiation Algorithms	190
6.1.4	Handover Protocols (Control)	190
6.1.5	Handover Methodology	191
6.2	IEEE 802.11 Handover Scenarios	191
6.3	IEEE 802.11 Roaming	192
6.3.1	Synchronization	192
6.3.2	IEEE 802.11 Roaming Mechanism	192
6.3.3	General Roaming-Related Functions	193
6.3.4	Initial AP Association	195
6.3.5	Single and Multichannel Roaming	195

6.3.6	IEEE 802.11 Handover Delays	198
6.4	Inter Access Point Protocol: IEEE 802.11f	199
6.4.1	AP Wakeup, ESS Formation, and RADIUS	201
6.4.2	IAPP-ADD Procedure	202
6.4.3	IAPP-Move Procedure	202
6.4.4	IAPP-Cache	203
6.4.5	Neighbor Graph	204
6.5	IEEE 802.11 Handover Delays	205
6.6	IP Mobility	207
6.6.1	Macro Mobility: Mobile IP	207
6.6.2	Mobile IPv6	212
6.6.3	Mobile IP and AAA	213
6.6.4	Mobile IP Security Issues	214
6.6.5	Mobile IP QoS Issues	215
6.6.6	Mobile IP and IPSec	216
6.6.7	MIP and NAT Issues	219
6.6.8	Hierarchical Mobile IP	219
6.6.9	Next Generation All-IP Mobility Management Requirements	221
6.6.10	Seamless Mobility (Seamoby)	222
6.7	Higher Layer Mobility	223
6.7.1	Mobile IP Issues	223
6.7.2	Stream Control Transmission Layer	224
6.7.3	Transport Layer Security	224
6.7.4	Session Initiation Protocol	225
6.8	Roaming in the Public WLAN	226
6.8.1	Inter-WISP Roaming Methods	226
6.8.2	Universal Access Method and WISPr	227

6.9	Fast Handover in WLAN	227
	References	228
Chapter 7 WLAN Deployment and Mobile Integration		231
7.1	Deployment Issues and Requirements	231
7.1.1	General Network Deployment Considerations	231
7.1.2	Wireless Deployment	233
7.1.3	Other Deployment Considerations	235
7.1.4	Wireless Network User Needs and Utilization	235
7.2	System Considerations	236
7.2.1	Automatic Data Rate Control Algorithm	237
7.2.2	Thresholds and System Scalability	238
7.3	WLAN MAC and PHY Layer Deployment	241
7.3.1	Coverage	241
7.3.2	Interference	243
7.3.3	Cell Overlap	244
7.3.4	Frequency Planning	246
7.3.5	Cell Overlay Structure	247
7.4	Corporate WLAN Deployment	248
7.4.1	IEEE 802.1x EAP Deployment	249
7.4.2	IPSec Deployment	249
7.4.3	Static WEP Deployment	251
7.4.4	Selection Criteria Model	251
7.4.5	Corporate WLAN Deployment Issues	251
7.5	Public WLAN Deployment	255
7.6	Operator-Owned PWLAN Solutions	256
7.6.1	SMS Based PWLAN Deployment	258
7.6.2	SIM-Based PWLAN Deployment	259

7.6.3	Mobile and WLAN Roaming	260
7.7	Secure Network Management	261
7.7.1	Secret Key Authentication	263
7.7.2	Privacy Using Conventional Encryption	265
7.8	3GPP - WLAN Deployment Architecture and Standard	265
7.9	Conclusions	267
	References	269
Chapter 8	Future Generation Communications	273
8.1	Introduction	273
8.2	The Need for Future	275
8.2.1	What Will Sell?	275
8.2.2	Is it Common Sense?	275
8.2.3	How to Know What Will Sell	276
8.2.4	Different Perspectives	278
8.3	Defining the Future	279
8.4	Technologies	280
8.4.1	B3G	280
8.4.2	Beyond	281
8.5	A Lesson to Learn	284
8.6	Other Technologies	284
8.7	Future Development	285
8.7.1	MAC	285
8.7.2	IP	286
8.7.3	TCP	288
8.7.4	RRM	288
8.7.5	Source Coding	289
8.7.6	Channel Coding	290

8.7.7 Physical Layer	291
8.7.8 QoS	291
8.7.9 Security	294
8.7.10 Mobility	296
8.8 IEEE 802 Activities Towards the Future	296
8.9 Standardization and Regulations	297
8.10 Conclusions	298
References	298
List of Abbreviations	301
About the Authors	313
Index	315

Preface

□ □

(Not by wealth alone is a human satisfied)

-*Rig Ved*

Even after all the earthly riches are enjoyed there still remains in the heart a longing for knowledge, true knowledge. It is this longing and the desire to bring the knowledge to others that resulted in the revelation of this book.

“How do IEEE 802.11 wireless local area networks (WLANs) work together with the higher layer protocols, particularly with the IP layer? How does it really work with the mobile network? What are its issues? What is the business model of WLANs now and in the future?” were the main questions that led to the writing of this book. These questions were unanswered in our first, edited, book titled *WLAN Systems and Wireless IP for Next Generation Communications*. In this book we try to answer these questions and elaborate on them.

The first chapter introduces IEEE 802.11-based WLAN and its issues; this chapter also gives a brief overview of the complete book. In the second chapter, written by Rajeev R. Prasad, we discuss market and business for WLANs for different service providers including the mobile operator.

With this background of WLANs and market we dive deep into the WLAN standards in Chapter 3, discussing the IEEE 802.11 standard in detail. Both the medium access control (MAC) and physical layer (PHY) are covered in this chapter. The discussion of MAC enhancements for security, quality of service (QoS), and mobility are left for later chapters.

Currently the foremost issue of IEEE 802.11-based WLANs is security. The fourth chapter of the book discusses the current security solution and its issues. In this chapter various solutions being provided in the market to overcome the security issues are also discussed. Technologies discussed include Virtual Private Network (VPN), IP Security (IPSec), and Secure Session Layer (SSL). The chapter also discusses the draft IEEE 802.11i standard together with Extensible Authentication Protocol over LAN (EAP) which is used by IEEE 802.1x.