

Computer Communications and Networks

For other titles published in this series, go to
www.springer.com/series/4198

The **Computer Communications and Networks** series is a range of textbooks, monographs and handbooks. It sets out to provide students, researchers and non-specialists alike with a sure grounding in current knowledge, together with comprehensible access to the latest developments in computer communications and networking.

Emphasis is placed on clear and explanatory styles that support a tutorial approach, so that even the most complex of topics is presented in a lucid and intelligible manner.

Alan Holt • Chi-Yu Huang

802.11 Wireless Networks

Security and Analysis

 Springer

Dr. Alan Holt
IP Performance
1-3 Merietts Court
Long Ashton Business Park
Long Ashton
Bristol BS41 9LW
UK

Dr. Chi-Yu Huang
Tata Technologies Ltd
6 Monarch Court
Emerald Park
Emersons Green
Bristol BS16 7FH
UK

Series Editor

Professor A.J. Sammes, BSc, MPhil, PhD, FBCS, CEng
Centre for Forensic Computing
Cranfield University
DCMT, Shrivenham
Swindon SN6 8LA
UK

ISSN 1617-7975

ISBN 978-1-84996-274-2

e-ISBN 978-1-84996-275-9

DOI 10.1007/978-1-84996-275-9

Springer London Dordrecht Heidelberg New York

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2010930228

© Springer-Verlag London Limited 2010

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licenses issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

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

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Cover design: VTEX, Vilnius

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Auntie Kath

Preface

This book is about wireless local area networks (WLANs) based upon the IEEE 802.11 standards. It has three primary objectives:

- To introduce the principles of 802.11 wireless networks and show how to configure equipment in order to implement various network solutions.
- To provide an understanding of the security implications of wireless networks and demonstrate how vulnerabilities can be mitigated.
- To introduce the underlying 802.11 protocols and build mathematical models in order to analyse performance in a WLAN environment.

The book is aimed at industry professionals as well as undergraduate and graduate level students. It is intended as a companion for a university course on wireless networking.

A practical approach is adopted in this book; examples are provided throughout, supported by detailed instructions. We cover a number of wireless vendors; namely, Cisco's Aironet, Alactel-Lucent's Omnicaccess and Meru Networks. While separate vendors, all three systems have a Cisco IOS-like command-line interface.

The GNU/Linux operating system is used extensively throughout this book. GNU/Linux systems have gained considerable popularity in the server and embedded system market (indeed, both Alcatel-Lucent and Meru Network's wireless equipment are based upon GNU/Linux). As well as the core GNU/Linux software we also use a number of open source applications. Wireless equipment does not operate in isolation. There are times when other network services are required, such as RADIUS. FreeRADIUS, in conjunction with a MySQL database server, is used to demonstrate an enterprise security WLAN. For convenience, the Xen virtualisation application is employed to emulate a multi-server environment. We show how to build and configure these systems.

There are many GNU/Linux *distributions* available. In this book, we use Debian and its derivative, Ubuntu. Debian and Debian like distributions have APT, a powerful package management application that greatly simplifies software installation and maintenance. Other distributions will have their advocates and supporters and if you wish to replicate the examples in this book we suggest you use the distribution with

which you are most familiar. However, you will have to *translate* the instructions to suit your distribution where they differ from Ubuntu/Debian.

We present a number of mathematical models in this book for analysing the performance of 802.11. We show how to build these models using the commercial application computer algebra, Maple. The examples presented in this book were developed on Maple version 11, but all the examples should work on older versions.

Acknowledgments

The authors would like to thank the following people for the valuable contribution they made to this book: Dr Adrian Davies, Dr Sue Casson (Leeds University), Michael Dewsnip (DL Consulting), Wayne Look (IP Performance), and Damien Parker (IP Performance).

Thanks also to Simon Rees of Springer for all his support in helping us through this process.

Bristol, UK
Hamilton, New Zealand

Alan Holt
Chi-Yu Huang

Contents

- 1 Introduction 1**
 - 1.1 IEEE 802 2
 - 1.2 Wireless LANs 3
 - 1.3 A Brief History of 802.11 7
 - 1.4 The RF Environment 8
 - 1.5 Book Outline 12
 - 1.6 Summary 13

- 2 Radio Frequencies 15**
 - 2.1 The Electromagnetic Spectrum 15
 - 2.2 Radio Waves 17
 - 2.2.1 Direct Path 19
 - 2.2.2 Absorption 22
 - 2.2.3 Reflection 22
 - 2.2.4 Diffraction 24
 - 2.2.5 Refraction 25
 - 2.2.6 Scattering 25
 - 2.2.7 Multi-path 25
 - 2.3 Radio Frequency Regulation 27
 - 2.4 Spectrum Management 32
 - 2.5 Summary 34

- 3 Medium Access Control 35**
 - 3.1 802.11 Services 36
 - 3.2 MAC Frame Format 38
 - 3.3 Distributed Coordination Function 39
 - 3.3.1 Carrier Sensing 40
 - 3.3.2 Transmission Methods 40
 - 3.3.3 Inter-frame Spacing 41
 - 3.3.4 Random Back-Off Algorithm 43
 - 3.3.5 Fragmentation 43

3.3.6	Fairness	44
3.4	Point Coordination Function	45
3.5	Hybrid Coordination Function	45
3.5.1	Enhanced Distributed Channel Access	46
3.5.2	HCF Controlled Channel Access	48
3.6	Summary	50
4	Physical Layer	51
4.1	Frequency Hopping Spread Spectrum	51
4.2	Direct Sequence Spread Spectrum	54
4.3	High-Rate Direct Sequence Spread Spectrum	56
4.4	Orthogonal Frequency Division Multiplexing	58
4.5	Extended Rate PHY	60
4.6	MIMO-OFDM	62
4.7	Beamforming	66
4.8	Summary	71
5	Cryptography	73
5.1	Ciphers	73
5.1.1	Symmetric Key Cryptography	74
5.1.2	Asymmetric Key Cryptography	76
5.2	Encryption	78
5.2.1	RC4	79
5.2.2	DES and Triple-DES	80
5.2.3	AES	80
5.3	Message Digests	81
5.4	Digital Signatures	83
5.5	Digital Certificates	84
5.6	Generating Digital Certificates	86
5.6.1	Generating a Certificate Authority	87
5.6.2	Generating Certificates	90
5.6.3	Testing the Certificates	95
5.7	Summary	97
6	Wireless Security	99
6.1	Pre-RSNA	99
6.1.1	Authentication	100
6.1.2	Encryption and Integrity	101
6.2	RSNA	101
6.2.1	Authentication	102
6.2.2	Key Management	105
6.2.3	Encryption and Integrity	105
6.3	Summary	108
7	Configuring Wireless Networks	111
7.1	Ad-hoc Network	112

- 7.2 WEP 114
- 7.3 WPA with Pre-shared Key 115
- 7.4 Multiple SSIDs 119
- 7.5 Wireless Distribution System 121
- 7.6 Wireless Bridge 123
- 7.7 Build an Open Source Access-Point 126
 - 7.7.1 Root Filesystem 126
 - 7.7.2 Administration 127
 - 7.7.3 Configuring the Access-Point 129
 - 7.7.4 Installing Grub 130
 - 7.7.5 Compile the Kernel 130
 - 7.7.6 Install Root Directory Structure onto Compact Flash 132
- 7.8 Summary 134

- 8 Robust Security Network 135**
 - 8.1 Installing FreeRadius 136
 - 8.2 Configuring FreeRadius 138
 - 8.3 Configure FreeRadius to use MySQL 140
 - 8.4 Testing 144
 - 8.5 Configure EAP 146
 - 8.6 Configure TLS 148
 - 8.7 NAS Configuration 149
 - 8.8 Wireless Client 150
 - 8.9 Summary 154

- 9 MAC Layer Performance Analysis 155**
 - 9.1 Fragmentation 155
 - 9.2 Analysis of Multiple Hops 156
 - 9.3 Throughput 158
 - 9.4 Summary 166

- 10 Link Rate Adaptation 167**
 - 10.1 Walffish-Ikegami Model 167
 - 10.2 Berg Model 168
 - 10.3 802.11b Link Rate Adaptation 171
 - 10.4 Link Rate Adaptation in an Urban Area 176
 - 10.5 802.11a Link Rate Adaptation 178
 - 10.6 Link Rate Experiments 182
 - 10.7 Summary 184

- A Build a Xen Server 185**
 - A.1 Install Xen 185
 - A.2 DomU Configuration 187
 - A.2.1 RADIUS Server 187
 - A.2.2 MySQL Server 188
 - A.2.3 DHCP Server 189

- A.2.4 Test Client 190
- B Initial Configuration of Access-Point Controllers 193**
 - B.1 Alcalet-Lucent Omniaccess Controller 193
 - B.2 Meru Controller 194
- References 201**
- Futher Reading 205**
- Index 207**

Abbreviations

AAD	Additional authentication data
ADSL	Asynchronous digital subscriber line
AES	Advanced encryption standard
ANSI	American National Standards Institute
AS	Authentication server
BSS	Basic service set
BSSID	Basic service set Identifier
CBC	Cipher-block chaining
CBC-MAC	Cipher-block chaining with message authentication code
CCK	Complimentary code keying
CCM	Counter mode and cipher-block chaining with message authentication code
CCMP	Counter mode and cipher-block chaining with message authentication code protocol
CFB	Cipher feedback
CFP	Contention free period
CP	Contention period
CRC	Cyclic redundancy check.
CSMA/CA	Carrier sense multiple access with collision avoidance
CTR	Counter mode
CTS	Clear-to-send
DAB	Digital audio broadcasting
DES	Data encryption system
DHCP	Dynamic host configuration protocol
DN	Distinguished name
DNS	Domain name system
DPSK	Differentiated phase shift keying
DBPSK	Differentiated binary phase shift keying
DQPSK	Differentiated quadrature phase shift keying
DSA	Digital signature algorithm
DVB	Digital video broadcasting

DSSS	Direct sequence spread spectrum
EAP	Extensible authentication protocol
EAPOL	Extensible authentication protocol over local area network
ECB	Electronic codebook
ERP-OFDM	Extended rate PHY, orthogonal frequency division multiplexing
FHSS	Frequency hopping spread spectrum
FFT	Fast fourier transform
FSK	Frequency shift keying
GI	Guard interval
GMK	Group master key
HCF	Hybrid coordination function
HCCA	HCF controlled channel access
HR/DSSS	High rate direct sequence spread spectrum
IBSS	Independent basic service set
IEEE	Institute of Electrical and Electronics Engineers
ICMP	Internet control message protocol
IFFT	Inverse fast fourier transform
IP	Internet protocol
ISM	Industrial, scientific and medical
IR	Infrared
LAN	Local area network
KCK	EAPOL-key confirmation key
KEK	EAPOL-key encryption key
LEAP	Lightweight EAP
MAC	Medium access control
MAC	Message Authentication Code
MIC	Message integrity code
MD5	Message digest 5
MIMO	Multiple-input multiple-output
MISO	Multiple-input single-output
MRC	Maximum ratio combining
OFB	Output feedback
OFDM	Orthogonal frequency division multiplexing
PBCC	Packet binary convolution coding
PEAP	Protected EAP
PING	Packet internet groper
PLCP	Physical layer convergence procedure
PSK	Pre-shared key
PSK	Phase shift keying
PTK	Pairwise temporal key
PMD	Physical medium dependent
PMK	Pairwise master key
PN	Packet number
PSDU	PLCP service data unit
PPDU	PLCP protocol data unit

QAM	Quadrature amplitude modulation
QPSK	Quadrature phase shift keying
RADIUS	Remote authentication dial in user service
RSA	RSA
RSN	Robust security network
RSNA	Robust security network association
RTS	Request-to-send
SHA	Secure hash algorithm
SISO	Single-input, single-output
SIMO	Single-input, multiple-output
SNMP	Simple network management protocol
SSID	Service set identifier
SSL	Secure socket layer
TCP	Transmission control protocol
TKIP	Temporal key integrity protocol
TLS	Transport layer security
UDP	User datagram protocol
VoIP	Voice over IP
WEP	Wired equivalent privacy
WPA	Wi-Fi protected access

List of Figures

1.1	The IEEE 802 reference model	2
1.2	Performance of Aloha and CSMA schemes	5
1.3	WLANs detected by Kismet Application	9
1.4	Spectrum analysis of 2.4 GHz band	10
1.5	Shannon limit	11
1.6	BER of BPSK modulation	12
2.1	Electric and magnetic field directions	16
2.2	Electric circuit	18
2.3	A half-wavelength Di-pole antenna	18
2.4	Wave components	19
2.5	Refracted radio wave	19
2.6	Free-space loss	22
2.7	Fresnel zone	23
2.8	Diffraction	24
2.9	Diffraction loss	25
2.10	Rayleigh probability density function	27
2.11	Ricean probability density function	28
2.12	802.11 channel allocation in the 2.4 GHz band	30
2.13	U-NII lower and middle	31
2.14	U-NII upper	32
3.1	802.11 reference model	36
3.2	802.11 Infrastructure Network	37
3.3	Authentication/association state machine	37
3.4	MAC header	38
3.5	Frame control field	38
3.6	Channel access with the basic DCF transmission method	41
3.7	Channel access using RTS/CTS and setting the NAV	41
3.8	Fragmentation of a MSDU into MPDUs	44
3.9	MSDU sent as multiple fragments under the RTS/CTS method	44
3.10	PCF access	46

- 3.11 Prioritisation in EDCA 48
- 3.12 The four access categories (ACs) for ECDA 49
- 4.1 PPDU encapsulation 52
- 4.2 Frequency hopping spread spectrum 52
- 4.3 The PLCP frame format for FHSS 54
- 4.4 Direct sequence spread spectrum 55
- 4.5 Long preamble 56
- 4.6 Polyphase complementary codes 57
- 4.7 PBCC convolutional encoder 58
- 4.8 Short preamble 58
- 4.9 The PLCP frame format for OFDM in 802.11a 59
- 4.10 Cyclic prefix 61
- 4.11 MIMO Communication system 62
- 4.12 Space-time coding 63
- 4.13 Diversity gain for N replica input streams 63
- 4.14 Spatial multiplexing 64
- 4.15 Capacity of a MIMO system 65
- 4.16 Capacity of Tx/Rx diversity 65
- 4.17 Gain of a simple beamformer 67
- 4.18 Gain of a simple beamformer (polarplot) 68
- 4.19 Uniform linear array (ULA) 69
- 4.20 Gain of a beamformer with a boresight of 0° 70
- 4.21 Gain of a beamformer with a boresight of 45° 71
- 4.22 Beamformer for various boresight angles (polar plot) 72
- 5.1 ECB encryption 74
- 5.2 An illustration of the problems related to ECB Encryption 76
- 6.1 Summary of 802.11i security 100
- 6.2 Assembly of a WEP frame 102
- 6.3 802.1X 103
- 6.4 EAP over LAN (EAPOL) 104
- 6.5 802.11i key hierarchy 105
- 6.6 TKIP frame 106
- 6.7 TKIP encapsulation 107
- 6.8 Expanded CCMP frame 108
- 6.9 CCMP header 108
- 6.10 CCMP encapsulation process 109
- 6.11 CCMP decapsulation process 109
- 7.1 An Aironet AP running dual SSIDs 119
- 7.2 Wireless distribution system 121
- 7.3 A wireless bridge topology 124
- 7.4 Output of make menuconfig command 131
- 8.1 RSN architecture 136

9.1	Probability of MSDU transmission failure.	156
9.2	Probability of MSDU transmission failure.	157
9.3	Successful transmission probability for multiple links	157
9.4	File transfer times	166
10.1	Walfish-Ikegami model path loss	169
10.2	Street plan	169
10.3	Signal loss in an urban area (Berg model)	172
10.4	802.11b Link rate adaptation versus SNR (dB)	174
10.5	802.11b Link adaptation $NOISE = -90$ dB.	175
10.6	802.11b Link adaptation $NOISE = -87$ dB.	176
10.7	Link adaptation of 802.11b in an urban area ($\phi = 90^\circ$).	177
10.8	Link adaptation of 802.11b in an urban area ($\phi = 55^\circ$).	178
10.9	Walfish-Ikegami model link rate adaptation for BER 10^{-4}	178
10.10	802.11a link rate adaptation versus SNR	180
10.11	Link rate versus distance for 802.11a	181
10.12	Retransmissions versus link rate	183

List of Tables

- 1.1 Some of the IEEE 802 standards 3
- 2.1 The electromagnetic spectrum 17
- 2.2 Signal losses caused by material 23
- 2.3 ISM bands 29
- 2.4 Channel allocation in the 2.4 GHz band 30
- 2.5 5 GHz unlicensed bands 31

- 3.1 SIFS and aSlotTime values 42
- 3.2 Contention windows values 43
- 3.3 Mapping of user priority to access category 47
- 3.4 Default values of the EDCA parameter set 48

- 4.1 Details of modulation methods in 802.11 52
- 4.2 DBPSK encoding 55
- 4.3 DQPSK encoding 55
- 4.4 Details of modulation methods in 802.11b 57
- 4.5 Details of modulation schemes for the 802.11a PHY 59
- 4.6 802.11g PHYs 61

- 5.1 Performance of AES 80
- 5.2 Performance comparison of RC4, DES and AES 81

- 7.1 Summary of wireless equipment manufacturers 112
- 7.2 Summary of laptops used to form an ad-hoc network 112

- 8.1 IP addresses 136

- 10.1 Modulation techniques supported by 802.11b 172
- 10.2 802.11a Link rate adaptation (empirical data) 179
- 10.3 Retransmissions 183