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

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 Omniaccess 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 secutity 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 Spinger for all his support in helping us through this process.

Bristol, UK — Alan Holt
Hamilton, New Zealand — Chi-Yu Huang

Contents

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	Cata 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 kncryption 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

List of Tables