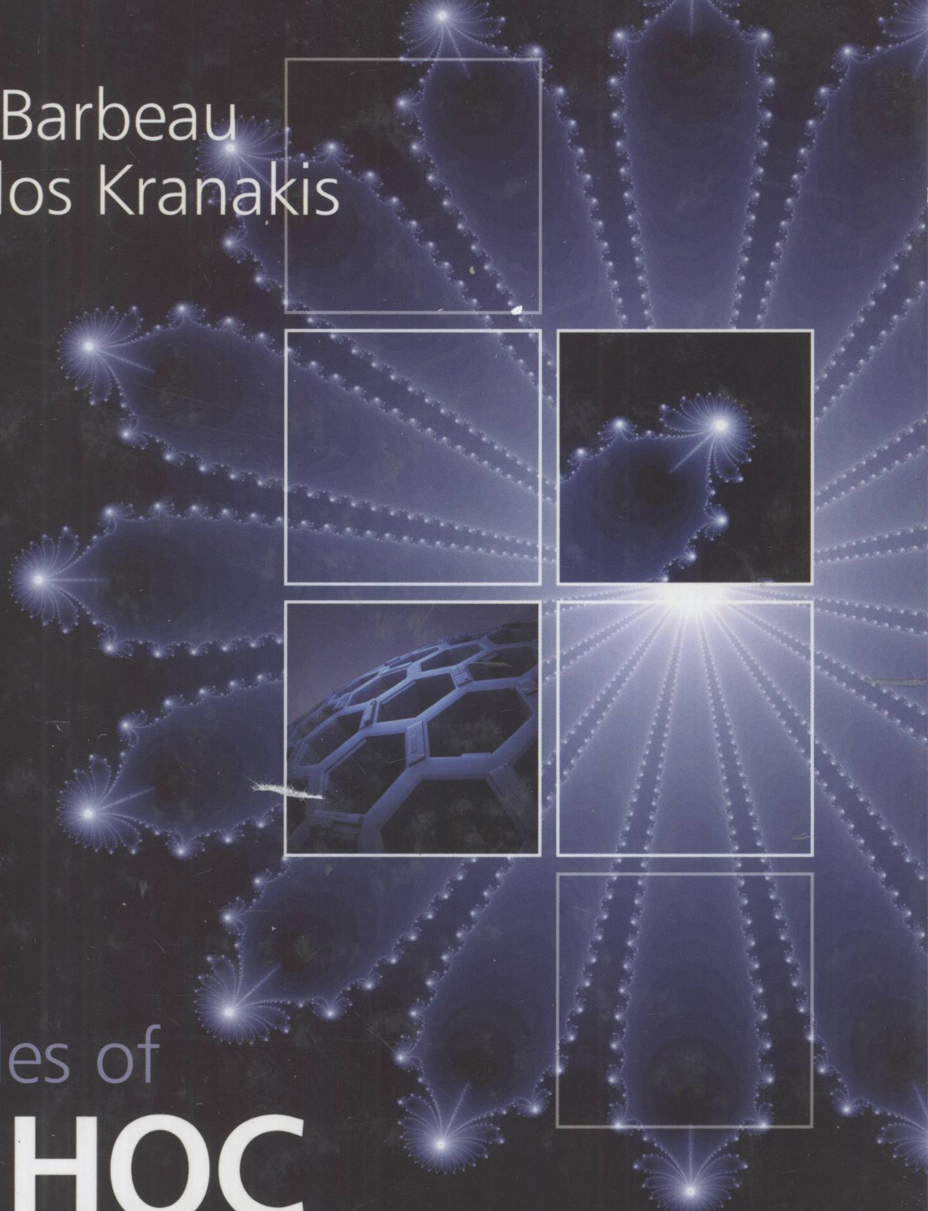
Michel Barbeau
Evangelos Kranakis



Principles of AD HOC NETWORKING

Companion Website

WILEY

Principles of Ad Hoc Networking

Michel Barbeau and Evangelos Kranakis
Carleton University, Canada

BICENTENNIAL 1807 WILEY 2007 BICENTENNIAL

John Wiley & Sons, Ltd

Telephone (+44) 1243 779777

Email (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on www.wileyeurope.com or www.wiley.com

Other Wiley Editorial Offices

John Wiley & Sons Inc., 111 River Street, Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street, San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr. 12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 42 McDougall Street, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 6045 Freemont Blvd, Mississauga, Ontario, L5R 4J3, Canada

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Anniversary Logo Design: Richard J. Pacifico

British Library Cataloguing in Publication Data

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

ISBN: 978-0-470-03290-9

Typeset in 10/12pt Times by Laserwords Private Limited, Chennai, India
Printed and bound in Great Britain by Antony Rowe Ltd, Chippenham, Wiltshire
This book is printed on acid-free paper responsibly manufactured from sustainable forestry in which at least two trees are planted for each one used for paper production.

Principles of
Ad Hoc Networking

*To Eda and Esther for their love,
compassion and understanding (EK, MB)*

PREFACE

...The shore of the morning sea and the cloudless sky brilliant blue and yellow all illuminated lovely and large. Let me stand here. Let me delude myself that I see these things...
Cavafy (1976)[Morning Sea, page 54]

Exchanging and sharing information has been a vital human activity since ancient times. Communication, in its simplest form, involves a sender who wants to communicate messages to an intended receiver. The word *communication* is derived from Latin and refers to the social need for direct contact, sharing information and promoting mutual understanding. The word *telecommunication* adds the prefix *tele* (meaning distance) and was first used by Edouard Estaunié in his 1904 book *Traité Pratique de Télecommunication Electrique* (see Huurdeman (2003)[page 3]). It is a technology that eliminates distance in communication.

Networks are formed by a collection of interconnected entities that can exchange information with each other. Simple systems consisting of a combination of runners, calling posts, mirrors, smoke and fire, pigeons, heliographs and flags have been used since ancient times. Efficiency in communication (i.e. the amount of information transmitted per time unit) has always been a driving force in developing new technologies. This led to the creation of permanent networked systems that could maintain consistent communication capability over large geographic areas. This gave rise to Claude Chappe's semaphore system in France (1791) and Abraham Edelcrantz' beacon system in Sweden (1794). The successful implementation of the telegraph with Samuel Morse's code (1832) and Alexander Graham Bell's telephone (1876) in the United States (see Holzmann and Pehrson (1995)) created the seeds of a telecommunication revolution that has continued with ever-increasing intensity till the present day.

The growing popularity of time-sharing systems created the need for combining communication lines and computers. Ever since the development of ARPANET that led to the invention of packet switching networks in the early 1960s, there has been no shortage of paradigms in computer networking. Ad hoc networking, which is the subject of the current book, is the latest. Despite the fact that it is less than a decade old, it is already becoming the foremost communication paradigm in wireless systems. According to "The New Dictionary of Cultural Literacy", *ad hoc* comes from Latin and means *toward this (matter).* It is a phrase describing something created especially for a particular occasion. It may be improvised and often impromptu but it is meant to address a situation at hand.

Networks have been around for sometime. They have been the object of numerous, sophisticated graph theoretic studies by mathematicians ever since Euler proposed the celebrated *Königsberg bridge* problem in 1736. Starting with ARPANET, engineers have continued to provide a plethora of inventions that enable dynamic networking solutions. So one may wonder why we need the new term ad hoc networks. An ad hoc network is an assembly of wireless devices that can quickly self-configure to form a networked topology. In traditional networking, nodes had specific, well-defined roles, usually as routers, switches, clients, servers, and so on. In contrast, nodes in ad hoc networks have no preassigned roles and quick deployment makes them suitable for monitoring in emergency situations.

In a way, the design of ad hoc networks needs to abstract simplicity from the midst of a meaningless complexity since topology formation has to take advantage of the physical connectivity characteristics of the environment. Often, studies are interdisciplinary and bring forth a paradigm shift in that they encompass a research approach to networking problems that combines ideas from many diverse disciplines like communication, control, geometry, graph theory and networking, probability, and protocol design that have given rise to many interesting new ideas. Nothing could describe more graphically the vitality of computer science than Alan Perlis' exuberant statement quoted from his 1966 Turing award lecture on "The Synthesis of Algorithmic Systems" (see Perlis (1987)[page 15]).

> Computer science is a restless infant and its progress depends as much on shifts in point of view as on the orderly development of our current concepts.

Computer science is often inspired by combining the sophistication of mathematical abstractions with the practicality of engineering design. In the sequel, we provide a discussion of some of the important developments of ad hoc networks with applications and provide a road map to the contents of the book.

Development of Ad Hoc Networking

An ad hoc network consists of nodes that may be mobile and have wireless communications capability without the benefit of a mediating infrastructure. Every node can become aware of the presence of other nodes within its range. Such nodes are called *neighbors* because direct wireless communications links can be established with them. Links established in the ad hoc mode do not rely on the use of an access point or base station. Neighbors can communicate directly with each other. The nodes and links form a graph. Any pair of nodes, not directly connected, can communicate if there is a path, consisting of individual links, connecting them. Data units are routed through the path from the origin to the destination. Routing in the ad hoc mode means that there is no need for an address configuration server such as DHCP or routers. Every node autonomously configures its network address and can resolve the way to reach a destination, using help from other nodes. Every node also plays an active role in forwarding data units for other nodes.

Ad hoc network applications

Here are three kinds of applications of the ad hoc concept: ad hoc linking, ad hoc networking and ad hoc association. Ad hoc linking is a feature present in a number of infrastructure-based systems. The D-STAR system is illustrative of an application using the ad hoc linking mode. The developer of the D-STAR protocols is the Japan Amateur Radio League (2005). D-STAR provides digital voice and digital data capability for fixed users, pedestrians and vehicles. It is intended mainly for emergency communications and is TCP/IP based. The data rate is 128 kbps (with a 130 kHz bandwidth). A D-STAR radio may have an Ethernet port for interfacing a computer to the radio. D-STAR radios can communicate directly without any access point, base station or repeater. They do, however, have backbone and Internet interconnection capability. D-STAR radios are currently available. There are a number of other technologies available with ad hoc linking capability such as Bluetooth, WiFi/802.11 and WiMAX/802.16 (mesh topology).

Ad hoc networking refers to the capability that the members of a network have to build routing information and forward data units from one location to another in the network. The Dedicated Short Range Communications (DSRC) is a radio service allocated in the 5.850 GHz-5.925 GHz range for vehicular ad hoc networks developed by the IEEE (2005). Such networks support roadside-to-vehicle and vehicle-to-vehicle communications. Envisioned applications include safety and traffic information dissemination and collision avoidance.

An ad hoc association is a relation established between two applications that find each other. Clients and servers of location-based services are examples of such applications. The goal of location-based services is to link a node's location to other useful information, resource or service. Applications include location of health services and goods. Discovery protocols with awareness of location are required to support location-based services. Protocols have been defined for the purpose of service discovery such as the Bluetooth Service Discovery Protocol and IETF Service Discovery Protocol. They can be combined with location information attributes. Location-based services are also envisioned in the context of DSRC.

Impact on protocol architecture

As depicted in Figure 1, operation in the ad hoc mode has an impact on a network architecture at all levels of the layered hierarchy. The physical layer is responsible for the transmission and reception of frames of bits as radio signals, also known as *framing*. Nodes in the ad hoc mode need their own mechanism to synchronize the start and end of their physical layer frames. Multiple access modes are preferred over modes relying on the use of the signal of a base station to synchronize physical layer frames, such as in time division multiplexing. The roles of the link layer are the control of the access to radio channels, hardware addressing and error control of frames. The link layer in the ad hoc mode needs to address neighbor discovery and the establishment of links, which may be unidirectional or asymmetric. The task of the network layer is to build routing information and forward data units from their origin node to their destination node using available paths. The network layer needs to deal with address configuration, address conflict detection and routing. The purpose of the transport layer is to provide to processes, on a node, process-to-process communication channels. Higher error rates and long interruptions characterize the network level service. These issues need to be addressed by the transport layer. The application layer consists of protocols for supporting the needs of applications. Over ad hoc networks, protocols are required to dynamically discover resources and services.

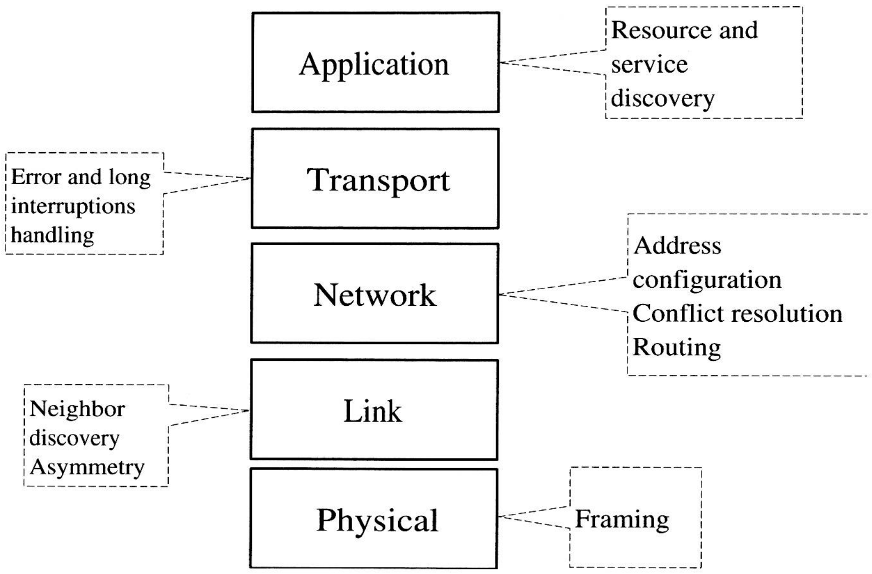


Figure 1 Impact of the ad hoc mode on a protocol architecture.

Roadmap and Style of Presentation

This book grew out of courses that each of us taught over the past few years at both the senior undergraduate level and junior graduate level. We have tried to present issues and topics in as orderly a manner as possible. Generally, chapters are relatively independent of each other and if you are already familiar with the subject you can read it in any order. Figure 2 provides a simple chart of dependencies that the reader may want to follow. Following is a brief outline of the contents of the chapters.

Chapter 1, on *Wireless Data Communications*, looks at the physical layer characteristics of ad hoc networks. Highlights of this chapter include signal representation, analog to digital conversion and digital to analog conversion, architecture of an SDR application, quadrature modulation and demodulation, spread spectrum, antennas and signal propagation.

Chapter 2, on *Medium Access Control*, addresses how wireless media are shared with distributed access. Control mechanisms are discussed, which insure non interfering access. After introducing the fundamentals of probability and statistics, this chapter presents some of the medium access protocols used in ad hoc networks. Highlights of this chapter include traffic modeling, multiple (uncoordinated, contention based, and demand assigned) access, CSMA/CD and CSMA/CA.

Chapter 3, on *Ad Hoc Wireless Access*, goes into the deeper details of a particular technology and discusses the principles of Bluetooth network formation. Highlights of this chapter include architecture of Bluetooth, access control, protocols for node discovery and topology formation, and mesh mode of WiMAX/802.16.

Chapter 4, on *Wireless Network Programming*, describes how to use the packet socket API in order to access the WiFi/802.11 wireless interface in a Linux system and communicate

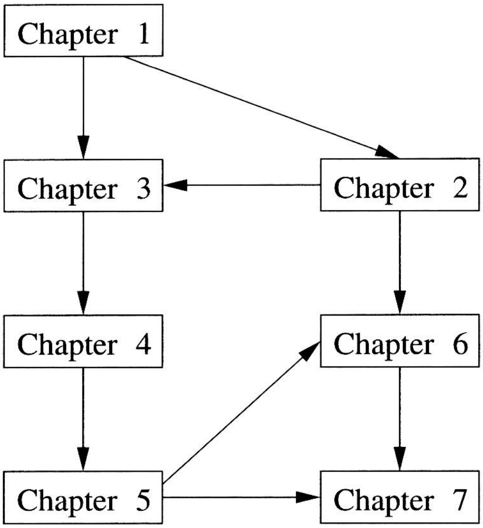


Figure 2 Dependency of chapters.

with other nodes in the ad hoc mode. Highlights of this chapter include ad hoc linking in WiFi/802.11, sockets, parameters and control and receiving/sending frames.

Chapter 5, discusses *Ad Hoc Network Protocols* thus focusing on the network layer. In particular, it addresses the issue of how packets should be forwarded and routed to their destination. Highlights of this chapter include reactive, proactive and hybrid approaches, clustering, ad hoc network model and cluster formation, quality of service, and sensor network protocols (flat routing, hierarchical routing and ZigBee).

Chapter 6, on *Location Awareness*, brings attention to simple geometric principles that enrich the infrastructureless character of ad hoc networks. It investigates how dynamic communication solutions (e.g. route discovery, geolocation) can be established taking advantage only of geographically local conditions. In addition, the guiding principle is that algorithms must terminate in constant time that is independent of the size of the input network. Highlights of this chapter include geographic proximity, neighborhood graphs, preprocessing the ad hoc network in order to construct spanners, radiolocation techniques and localization algorithms, information dissemination, geometric routing and traversal in (undirected) planar graphs, graph and geometric spanners and properties of random unit graphs, as well as coverage and connectivity in sensor networks.

Chapter 7, on *Ad Hoc Network Security*, discusses a variety of security problems arising in ad hoc networks. These include authentication and signatures, physical layer attacks, security of application protocols (WiFi/802.11, ZigBee), biometrics, routing and broadcast security as well as secure location verification and security of directional antenna systems.

Finally, each chapter concludes with several exercises. Some are rather routine and are meant to complement the text, many others are less so, while the more challenging ones are marked with ($\star$). The reader is advised to attempt them all and may occasionally have to refer to the original published source for additional details.

The book has a companion Web site at http://www.scs.carleton.ca/~barbeau/pahn/index.htm. The companion Web site for the book contains presentation slides and source code for the examples in the book.

Acknowledgements

We would like to thank our students and collaborators for the learning experience that led to this book. We are particularly thankful to Christine Laurendeau who read and commented extensively on portions of the manuscript. Many thanks also to Gustavo Alonso, Paul Boone, Prosenjit Bose, Mathieu Couture, Costis Georgiou, Jen Hall, Danny Krizanc, Pat Morin, Michel Paquette, Tao Wan, and Peter Widmayer for many stimulating conversations. The second author would also like to express his deepest appreciation to Jorge Urrutia for providing a stimulating environment at the Mathematics Institutes in Morelia and Guanajuato and the rest of the routing group Edgar Chavez, Jurek Czyzowicz, Stefan Dobrev, Hernan González-Aguilar, Rasto Kralovic, Jarda Opatrny, Gelasio Salazar, and Laco Stacho for interesting conversations at our annual summer meeting.

During the preparation of the book, the authors were supported in part by grants from MITACS (Mathematics of Information Technology and Complex Systems) and NSERC (Natural Sciences and Engineering Research Council of Canada).

Michel Barbeau and Evangelos Kranakis
Ottawa, Ontario, Canada

Glossary

AP	Answering Protocol, 75
CP	Conditional Protocol, 75
LP	Listening Protocol, 75
RP	Random Protocol, 75
SP	Sleep Protocol, 75
ACL	Asynchronous ConnectionLess, 70
ADC	Analog to Digital Conversion, 5
AES	Advanced Encryption Standard, 204, 205
AOA	Angle Of Arrival, 169
AODV	Ad Hoc On-Demand Distance Vector, 121
API	Application Programming Interface, 103
BASN	Body Area Sensor Network, 207
BER	Bit Error Rate, 20
BFS	Breadth First Search, 149
BiBa	Bins and Balls, 218
BPF	Band Pass Filter, 7
bps	Bit per second, 11
BS	Base Station, 87
CA	Certification Authority, 204
CCK	Complementary Code Keying, 11
CRC	Cyclic Redundancy Code, 89
CSMA	Carrier Sense Multiple Access, 52
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance, 52
CSMA/CD	Carrier Sense Multiple Access/Collision Detection, 58
CTS	Clear to Send, 54
CW	Contention Window, 53
DAC	Digital to Analog Converter, 8
dB	decibel, 17
dBi	dB isotropically, 17
DBPSK	Differential Binary Phase Shift Keying, 11
DCF	Distributed Coordination Function, 52

DDC	Direct Digital Conversion, 5
DDS	Direct Digital Synthesis, 9
DES	Data Encryption Standard, 204
DFS	Depth First Search, 149
DHCP	Dynamic Host Configuration Protocol, 88
DLTR	Distance Left To Right, 179
DMAC	Distributed and Mobility-Adaptive Clustering, 133
DQPSK	Differential Quadrature Phase-Shift Keying, 11
DS	Direct Sequence, 11
DSDV	Destination-Sequenced Distance Vector, 215
DSP	Digital Signal Processing, 1
DSR	Dynamic Source Routing Protocol, 116
DSSS	Direct Sequence Spread Spectrum, 56
DT	Delaunay Triangulation, 150
ECG	Electrocardiogram, 207
EIRP	Effective Isotropic Radiated Power, 24
ESSID	Extended Service Set ID, 104
FER	Frame Error Rate, 20
FH	Frequency Hopping, 11
FS	Frequency Synchronization, 68
FSK	Frequency Shift Keying, 12
GFSK	Gaussian-shape Frequency Shift Keying, 11
GG	Gabriel Graph, 148
GPS	Global Positioning System, 146
HAMA	Hybrid Activation Multiple Access, 57
HMAC	Hash Message Authentication Code, 91
HSP	Half Space Proximal, 155
IARP	Intrazone Routing Protocol, 125
IBSS	Independent Basic Service Set, 52
IERP	Interzone Routing Protocol, 125
IETF	The Internet Engineering Task Force, 121
IF	Intermediate Frequency, 5
IP	Internet Protocol, 70
IPI	InterPule Interval, 208
K	Kilo, 11
L2CAP	Logical Link Control and Adaptation Layer, 70
LAMA	Link Activation Multiple Access, 57
LAN	Local Area Network, 191
LF	Link Formation, 67

LMR	LMR Flexible Low Loss Cable (A trademark of Times Microwave Systems), 21
LocalMST	Local Minimum Spanning Tree, 157
LPF	Low Pass Filter, 5
M	Mega, 11
MAC	Medium Access Control, 46
MAC	Message Authentication Code, 193
MaxDLTR	Max Distance Left To Right, 179
MD	Message Digest, 194
MIC	Message Integrity Code, 205
MidDLTR	Mid Distance Left To Right, 179
MinDLTR	Min Distance Left To Right, 179
MPR	MultiPoint Relay, 122
MS	Mobile Station, 87
MSH-CSCF	Mesh centralized configuration, 93
MSH-CSCH	Mesh centralized scheduling, 92
MSH-DSCH	Mesh distributed scheduling, 92
MSH-NCFG	Mesh network configuration, 90
MSH-NENT	Mesh network entry, 91
MST	Minimum Spanning Tree, 149
MTU	Maximum Transmission Unit, 105
NA	Neighbor Algorithm, 170
NAMA	Node Activation Multiple Access, 56
NCR	Neighbor Aware Contention Resolution, 56
NDP	Neighbor Discovery Protocol, 125
NNG	Nearest Neighbor Graph, 147
ODRP	On-Demand Delay Constrained Unicast Routing Protocol, 136
OFDM	Orthogonal Frequency Division Multiplexing, 11
OLSR	Optimized Link-State Routing, 121
OSI	Open Systems Interconnection, 70
PAMA	Pairwise Link Activation Multiple Access, 57
PCF	Point Coordination Function, 52
PDU	Protocol Data Unit, 89
PER	Packet Error Rate, 20
PKI	Public-Key Infrastructure, 192
PPG	Photoplethysmogram, 207
PSK	Phase Shift Keying, 12
QAM-16	Quadrature Amplitude Modulation-16 states, 11
QPSK	Quadrature Phase shift Keying, 11

r.v.	Random Variable, 30
RB	Random Backed, 68
RC4	Route Coloniale 4, 203
RNG	Relative Neighbor Graph, 148
RoA	Region of Acceptance, 222
RTS	Request to Send, 54
SC	Single Carrier, 11
SCO	Synchronous Connection Oriented, 70
SDP	Service Discovery Protocol, 70
SDR	Software Defined Radio, 1
SEAD	Secure, Efficient, Ad Hoc, Distance vector, 215
SEAL	SElf Authenticating vaLue, 219
SHA	Secure Hash Algorithm, 195
SKKE	Symmetric-Key Key Establishment, 206
SNMP	Simple Network Management Protocol, 88
SS	Spread Spectrum, 11
TC	Topology Control, 124
TCP	Transmission Control Protocol, 23
TDMA	Time Division Multiple Access, 89
TDOA	Time Difference Of Arrival, 168
TKIP	Temporal Key Integrity Protocol, 204
TOA	Time Of Arrival, 168
TTL	Time To Live, 124
UDG	Unit Disk Graph, 146
UDP	User Datagram Protocol, 91
UWB	Ultrawideband, 24
WEP	Wired Equivalent Privacy, 203
WiFi	Wireless Fidelity, 103
WiMAX	Worldwide Interoperability for Microwave Access, 87
WPA	WiFi Protected Access, 204
ZRP	Zone Routing Protocol, 125

Contents