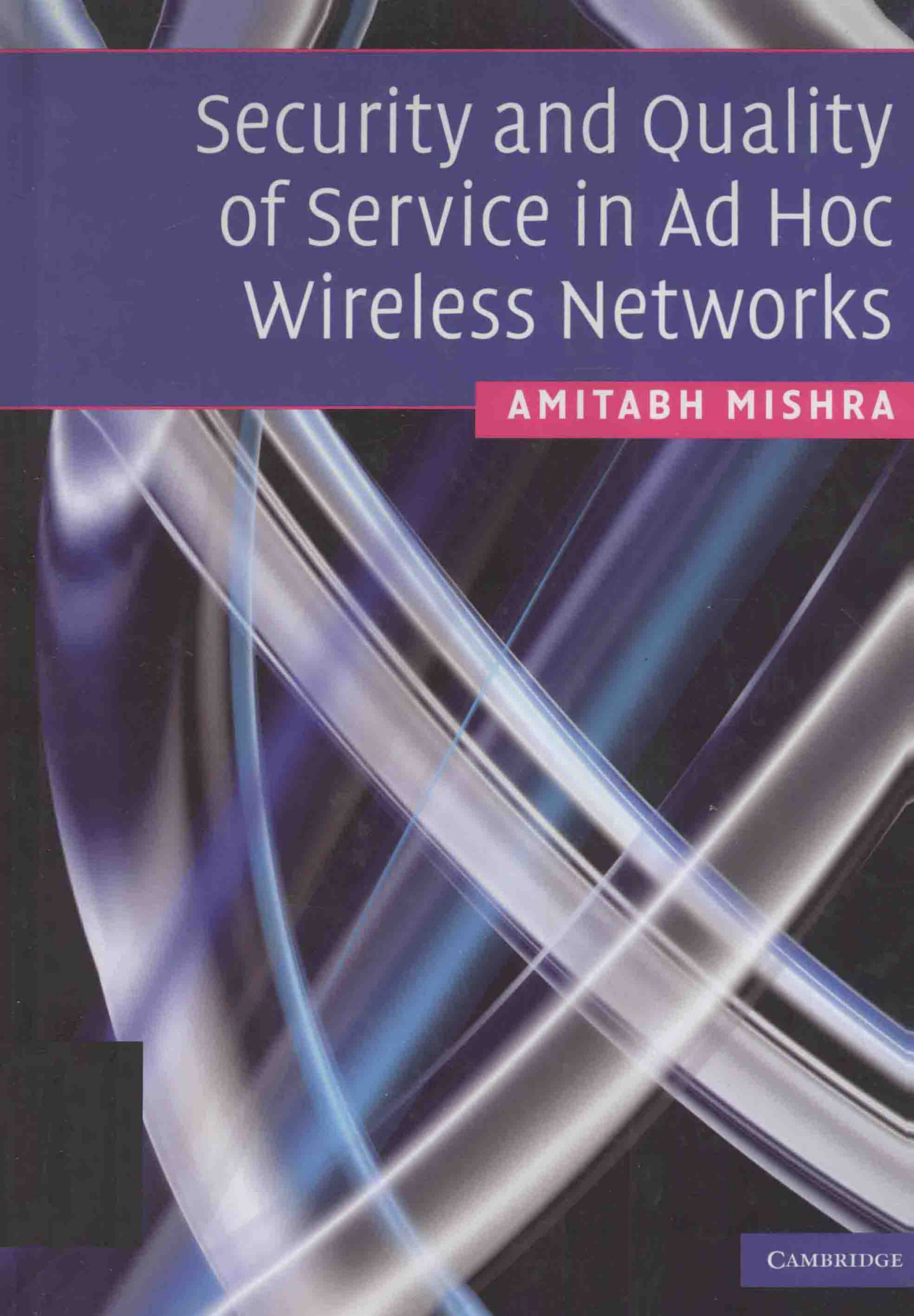
Security and Quality of Service in Ad Hoc Wireless Networks

AMITABH MISHRA



CAMBRIDGE

SECURITY AND QUALITY OF SERVICE IN AD HOC WIRELESS NETWORKS

AMITABH MISHRA
Johns Hopkins University

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo, Delhi

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org

First published 2008

Printed in the United Kingdom at the University Press, Cambridge

A catalog record for this publication is available from the British Library

ISBN 978-0-521-87824-1 hardback

SECURITY AND QUALITY OF SERVICE IN AD HOC WIRELESS NETWORKS

Ensuring secure transmission and good quality of service (QoS) are key commercial concerns in ad hoc wireless networks as their application in short range devices, sensor networks, control systems, and other areas continues to develop. Focusing on practical potential solutions, this text covers security and quality of service in ad hoc wireless networks.

Starting with a review of the basic principles of ad hoc wireless networking, coverage progresses to the vulnerabilities these networks face and the requirements and solutions necessary to tackle them. QoS in relation to ad hoc networks is covered in detail, with specific attention to routing, and the basic concepts of QoS support in unicast communication, as well as recent developments in the area. There are also chapters devoted to secure routing, intrusion detection, security in WiMax networks, and trust management, the latter of which is based on principles and practice of key management in distributed networks and authentication.

This book represents the state of the art in ad hoc wireless network security and is a valuable resource for graduate students and researchers in electrical and computer engineering, as well as for practitioners in the wireless communications industry.

AMITABH MISHRA worked at Lucent Technologies (formerly Bell Labs) for 13 years before moving to Virginia Tech. He is currently with the Center for Networks and Distributed Systems, Department of Computer Science, Johns Hopkins University. He was awarded his Ph.D. in Electrical Engineering in 1985 from McGill University. A senior member of the IEEE, he has chaired the IEEE Communications Software committee, and holds several patents in the field of wireless communications.

To my parents:
Shrimati Deomani and Shri Brij Mohan Lal Mishra

Preface

Security and quality of service in ad hoc wireless networks have recently become very important and actively researched topics because of a growing demand to support live streaming audio and video in civilian as well as military applications. While a couple of books have appeared recently that deal with ad hoc networks, a comprehensive book that deals with security and QoS has not yet appeared. I am confident that this book will fill that void.

The book grew out of a need to provide reading material in the form of book chapters to graduate students taking an advanced wireless networking course that I was teaching at the Virginia Polytechnic Institute and State University. Some of these book chapters then subsequently appeared as chapters in handbooks and survey papers in journals.

This book contains eight chapters in total, of which five chapters deal with various aspects of security for wireless networks. I have devoted only one chapter to the quality of service issue. Chapter 1 introduces basic concepts related to an ad hoc network, sets the scene for the entire book by discussing the vulnerabilities such networks face, and then produces a set of security requirements that these networks need to satisfy to live up to the challenges imposed by the vulnerabilities. Chapter 1 also introduces basic concepts regarding quality of service as it relates to ad hoc networks. In my presentation in this book, I have assumed that the reader is familiar with basic computer security mechanisms as well as the well known routing protocols of ad hoc networks.

Chapter 2 presents an overview of the wireless security for infrastructure-based wireless LANs that are based on the IEEE 802.11b standard, wireless cellular networks such as GSM, GPRS, and UMTS, and wireless personal area networks such as Bluetooth and IEEE 802.15.4 standard-based networks.

Various possible threats and attacks on ad hoc networks are discussed in Chapter 3. Possible security solutions against such attacks are then presented in various chapters of the book.

The security schemes that govern trust among communicating entities are collectively known as trust management. Chapter 4 presents various trust management schemes that are based on the principles and practice of key management in distributed networks and authentication. Chapter 5 addresses the issue of intrusion detection in ad hoc networks. It includes a discussion on both types of intrusion detection schemes, namely *anomaly* and *misuse* detection, and presents most of the prominent intrusion detection schemes available in the literature.

The topic of quality of service for ad hoc networks is covered in Chapter 6. Supporting appropriate quality of service for mobile ad hoc networks is a complex and difficult issue because of the dynamic nature of the network topology, and generally imprecise network state information. This chapter presents the basic concepts of quality of service support in ad hoc networks for unicast communication, reviews the major areas of current research and results, and addresses some new issues. Secure routing is the theme for Chapter 7, in which I describe the various algorithms that have been proposed to make the ad hoc routing more secure.

The IEEE 802.16 is a new standard that deals with providing broadband wireless access to residential and business customers and is popularly known as WiMax. This standard has several provisions for ensuring the security of and privacy to applications running on WiMax-enabled networking infrastructure. I discuss the security and privacy features of this standard in Chapter 8.

Acknowledgements

Among the people whose contributions helped me complete this book are Dr. Satyabrata Chakrabarti of Bell Laboratories, who was my guru, and Ketan Nadkarni, who was my graduate student at Virginia Tech. I thank both of them. I would also like to thank Dr. Philip Meyler, Editorial Manager at Cambridge University Press, for persuading me to complete this book. Without his support this book might not have been written at all. The entire Cambridge University Press team, including Anne Littlewood (Assistant Editor), Alison Lees (Copy-editor), and Daniel Dunlavey (Production Editor), has done an outstanding job in shaping this book to the final form, for which I am grateful.

Finally, I would like to thank my wife, Tanuja, and our children, Meghana and Anant, for making this book happen.

Contents

Preface		*page* xi
Acknowledgements		xiii
1	Introduction	1
	1.1 Ad hoc networking	1
	1.2 The ad hoc wireless network: operating principles	3
	1.3 Ad hoc networks: vulnerabilities	8
	1.4 Ad hoc networks: security requirements	11
	1.5 Quality of service	14
	1.6 Further reading	15
	1.7 References	15
2	Wireless security	17
	2.1 Wireless local area networks (IEEE 802.11) security	17
	2.2 Wireless cellular network security	29
	2.3 Bluetooth or IEEE 802.15 security	40
	2.4 Summary and further reading	41
	2.5 References	42
3	Threats and attacks	43
	3.1 Attack classification	43
	3.2 Denial of service (DoS)	44
	3.3 Impersonation	45
	3.4 Disclosure	48
	3.5 Attacks on information in transit	49
	3.6 Attacks against routing or network layer	49
	3.7 Node hijacking	52
	3.8 Further reading	59
	3.9 References	59
4	Trust management	61
	4.1 The resurrecting duckling	61
	4.2 Key management	62

4.3 Authentication 76
4.4 Further reading 79
4.5 References 80
5 Intrusion detection 82
5.1 Introduction 82
5.2 Security vulnerabilities in mobile ad hoc networks (MANETs) 84
5.3 Intrusion detection systems: a brief overview 86
5.4 Requirements for an intrusion detection system for mobile ad hoc networks 88
5.5 Intrusion detection in MANETs 89
5.6 Mobile agents for intrusion detection and response in MANETs 96
5.7 Summary 102
5.8 Further reading 105
5.9 References 106
6 Quality of service 107
6.1 Introduction 107
6.2 Routing in mobile ad hoc networks 110
6.3 Routing with quality of service constraints 112
6.4 Quality of service routing in ad hoc networks 118
6.5 Conclusion and further reading 126
6.6 References 127
7 Secure routing 129
7.1 Security aware routing 129
7.2 Secure distance-vector routing protocols 133
7.3 Mitigating routing misbehavior 136
7.4 Secure packet forwarding – the currency concept 137
7.5 Secure route discovery (SRP) and secure message transmission (SMT) protocols 141
7.6 Summary of security features in routing protocols and further reading 145
7.7 References 146
8 Security in WiMax networks 147
8.1 Introduction 147
8.2 Standardization and certification 148
8.3 Frame structure 151
8.4 Point-to-multipoint (PMP) mode 153
8.5 Mesh 155
8.6 Quality of service 156

8.7 Security features in WiMax 157
8.8 Open issues 169
8.9 Summary and further reading 171
8.10 References 171
Glossary 172
Index 176

1

Introduction

Wireless mobile ad hoc networks consist of mobile nodes interconnected by wireless multi-hop communication paths. Unlike conventional wireless networks, ad hoc networks have no fixed network infrastructure or administrative support. The topology of such networks changes dynamically as mobile nodes join or depart the network or radio links between nodes become unusable. In this chapter, I will introduce wireless ad hoc networks, and discuss their inherent vulnerable nature. Considering the inherent vulnerable nature of ad hoc networks, a set of security requirements is subsequently presented. The chapter also introduces the quality of service issues that are relevant for ad hoc networks.

1.1 Ad hoc networking

Conventional wireless networks require as prerequisites a fixed network infrastructure with centralized administration for their operation. In contrast, so-called (wireless) mobile ad hoc networks, consisting of a collection of wireless nodes, all of which may be mobile, dynamically create a wireless network amongst themselves without using any such infrastructure or administrative support [1,2]. Ad hoc wireless networks are self-creating, self-organizing, and self-administering. They come into being solely by interactions among their constituent wireless mobile nodes, and it is only such interactions that are used to provide the necessary control and administration functions supporting such networks.

Mobile ad hoc networks offer unique benefits and versatility for certain environments and certain applications. Since no fixed infrastructure, including base stations, is prerequisite, they can be created and used "any time, anywhere." Such networks could be intrinsically fault-resilient, for they do not operate under the limitations of a fixed topology. Indeed, since all nodes are allowed to be mobile, the composition of such networks is necessarily time varying. Addition and deletion of nodes occur only by interactions with other

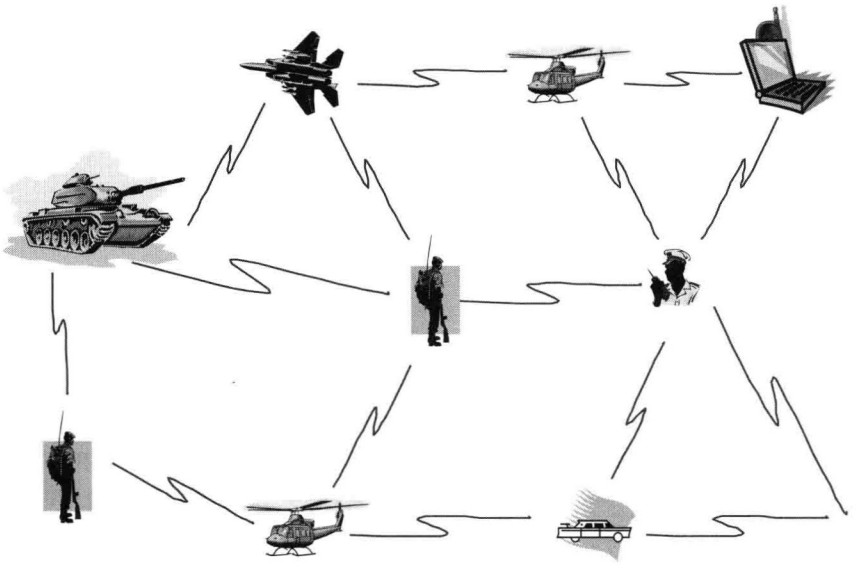


Figure 1.1 Conceptual representation of a mobile ad hoc network

nodes; no other agency is involved. Such perceived advantages elicited immediate interest in the early days among military, police, and rescue agencies in the use of such networks, especially under disorganized or hostile environments, including isolated scenes of natural disaster and armed conflict. See Fig. 1.1 for a conceptual representation. In recent days, home or small-office networking and collaborative computing with laptop computers in a small area (e.g., a conference or classroom, single building, convention center, etc.) have emerged as other major areas of application. These include commercial applications based on progressively developing standards such as Bluetooth [3], as well as other frameworks such as Piconet [4], HomeRF Shared Wireless Access Protocol [5], etc. In addition, people have recognized from the beginning that ad hoc networking has obvious potential use in all the traditional areas of interest for mobile computing.

Mobile ad hoc networks are increasingly being considered for complex multimedia applications, where various quality of service (QoS) attributes for these applications must be satisfied as a set of predetermined service requirements. As a minimum, the QoS issues pertaining to delay and bandwidth management are of paramount interest. In addition, because of the use of the ad hoc networks for military or police use, and of increasingly common commercial applications, various security issues need to be addressed. Cost-effective resolution of these issues at appropriate levels is essential for widespread general use of ad hoc networking.

Mobile ad hoc networking emerged from studies on extending traditional Internet services to the wireless mobile environment. All current works, as well as this presentation, consider the ad hoc networks as a wireless extension to the Internet, based on the ubiquitous IP networking mechanisms and protocols. Today's Internet possesses an essentially static infrastructure where network elements are interconnected over traditional wire-line technology, and these elements, especially the elements providing the routing or switching functions, do not move. In a mobile ad hoc network, by definition, all the network elements move. As a result, numerous more stringent challenges must be overcome to realize the practical benefits of ad hoc networking. These include effective routing, medium (or channel) access, mobility management, power management, and security issues, all of which affect the quality of the service experienced by the user.

The absence of a fixed infrastructure for ad hoc networks means that the nodes communicate directly with one another in a peer-to-peer fashion. The mobility of these nodes imposes limitations on their power capacity, and hence, on their transmission range; indeed, these nodes must often satisfy stringent weight limitations for portability. Mobile hosts are no longer just end systems; to relay packets generated by other nodes, each node must be able to function as a router as well. As the nodes move in and out of range with respect to other nodes, including those that are operating as routers, the resulting topology changes must somehow be communicated to all other nodes, as appropriate. In accommodating the communication needs of the user applications, the limited bandwidth of wireless channels and their generally hostile transmission characteristics impose additional constraints on how much administrative and control information may be exchanged, and how often. Ensuring effective routing is one of the great challenges for ad hoc networking.

The lack of fixed base stations in ad hoc networks means that there is no dedicated agency for managing the channel resources for the network nodes. Instead, carefully designed distributed medium access techniques must be used for channel resources, and, hence, mechanisms must be available to recover efficiently from the inevitable packet collisions. Traditional carrier sensing techniques cannot be used, and the hidden terminal problem [6,7] may significantly diminish the transmission efficiency [8]. An effectively designed protocol for medium access control (MAC) is essential to the quest for QoS.

1.2 The ad hoc wireless network: operating principles

I start with a description of the basic operating principles of a mobile ad hoc network. Figure 1.2 depicts the peer-level multi-hop representation of such a

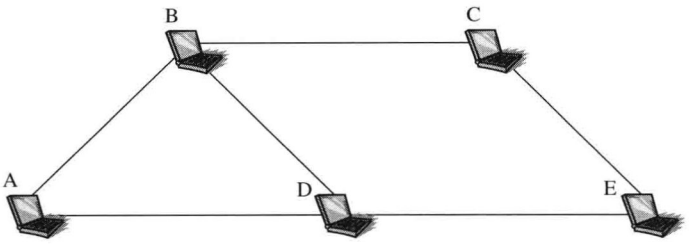


Figure 1.2 Example of an ad hoc network

network. Mobile node A communicates with another such node B directly (single-hop) whenever a radio channel with adequate propagation characteristics is available between them. Otherwise, multi-hop communication is necessary where one or more intermediate nodes must act as a relay (router) between the communicating nodes. For example, there is no direct radio channel (shown by the lines) between A and C or A and E in Fig. 1.2. Nodes B and D must, therefore, serve as intermediate routers for communication between A and C, and A and E, respectively. Indeed, a distinguishing feature of ad hoc networks is that all nodes must be able to function as routers on demand. To prevent packets from traversing infinitely long paths, an obvious essential requirement for choosing a path is that the path must be loop-free. A loop-free path between a pair of nodes is called a route.

An ad hoc network begins with at least two nodes broadcasting their presence (beaconing) with their respective address information. As discussed later, they may also include their location information, obtained, for example, by using a system such as the Global Positioning System (GPS), for more effective routing. If node A is able to establish direct communication with node B in Fig. 1.2, verified by exchanging suitable control messages between them, they both update their routing tables. When a third node, C, joins the network with its beacon signal, two scenarios are possible. The first is where both A and B determine that single-hop communication with C is feasible. In the second scenario, only one of the nodes, say B, recognizes the beacon signal from C and establishes the availability of direct communication with C. The distinct topology updates, consisting of both address and route updates, are made in all three nodes immediately afterwards. In the first case, all routes are direct. For the other, shown in Fig. 1.3, the route update first happens between B and C, then between B and A, and then again between B and C, confirming the mutual reachability between A and C via B.

The mobility of nodes may cause the reachability relations to change in time, requiring route updates. Assume that for some reason, the link between B and

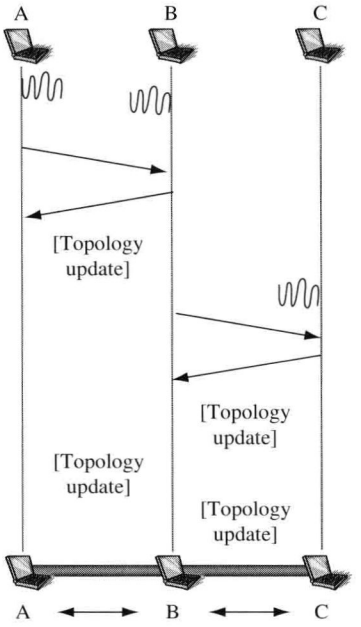


Figure 1.3 Bringing up an ad hoc network

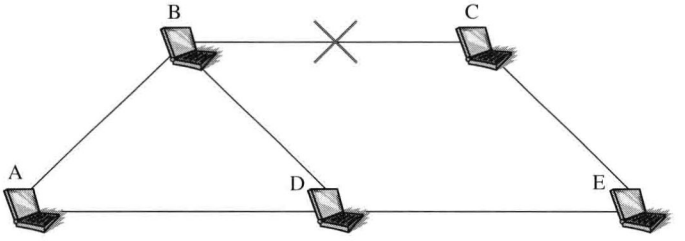


Figure 1.4 Topology update owing to a link failure

C is no longer available, as shown in Fig. 1.4. Nodes A and C can still reach each other, although this time only via nodes D and E. Equivalently, the original loop-free route $\langle A \leftrightarrow B \leftrightarrow C \rangle$ is now replaced by the new loop-free route $\langle A \leftrightarrow D \leftrightarrow E \leftrightarrow C \rangle$. All five nodes in the network are required to update their routing tables appropriately to reflect this topology change, which will be first detected by nodes B and C, then communicated to A and E, and then to D.

The reachability relation among the nodes may also change for other reasons. For example, a node may wander too far out of range, its battery may be depleted, or it may suffer a software or hardware failure. As more nodes join the network or some of the existing nodes leave, the topology

updates become more numerous, complex, and, usually, more frequent, thus diminishing the network resources available for exchanging user information.

Finding a loop-free path as a legitimate route between a source–destination pair may become impossible if the changes in network topology occur too frequently. Here, "too frequently" means that there was not enough time to propagate to all the pertinent nodes all the topology updates arising from the last network topology changes, or worse, before the completion of determining all loop-free paths accommodating the last topology changes. The ability to communicate degrades with accelerating rapidity as the knowledge of the network topology becomes increasingly inconsistent. Given a specific time-window, we call (the behavior of) an ad hoc network combinatorially stable if, and only if, the topology changes occur sufficiently slowly to allow successful propagation of all topology updates as necessary. Clearly, combinatorial stability is determined not only by the connectivity properties of the networks, but also by the complexity of the routing protocol in use and the instantaneous computational capacity of the nodes, among other factors. Combinatorial stability is an essential consideration for attaining QoS objectives in an ad hoc network, as we shall see below. I address the general issue of routing in mobile ad hoc networks separately in the next section.

The shared wireless environment of mobile ad hoc networks requires the use of appropriate medium access control (MAC) protocols to mitigate the medium contention issues, allow efficient use of limited bandwidth, and resolve so-called hidden and exposed terminal problems. These are basic issues, independent of the support of QoS; the QoS requirements add extra complexities for the MAC protocols, mentioned later in Chapter 5. The issues of efficient use of bandwidth and the hidden/exposed terminal problem have been studied exhaustively and are well understood in the context of accessing and using any shared medium. I briefly discuss the "hidden-terminal" problem [6] as an issue especially pertinent for the wireless networks.

Consider the scenario of Fig. 1.5, where a barrier prevents node B from receiving the transmission from D, and vice versa, or, as usually stated, B and D cannot "hear" each other. The "barrier" does not have to be physical; a large enough distance separating two nodes is the most commonly occurring "barrier" in ad hoc networks. Node C can "hear" both B and D. When B is transmitting to C, D, being unable to "hear" B, may transmit to C as well, thus causing a collision and exposing the *hidden-terminal* problem. In this case, B and D are "hidden" from each other. Now consider the case when C is transmitting to D. Since B can "hear" C, B cannot risk initiating a transmission to A for fear of causing a collision at C. Here is an example of the *exposed terminal* problem, where B is "exposed" to C.