Wireless Mesh Networks

▸▸ Ian F. Akyildiz and Xudong Wang

▸▸ Advanced Texts in Communications and Networking

WILEY

Wireless Mesh Networks

Professor Ian F. Akyildiz

Georgia Institute of Technology, USA

Dr Xudong Wang

TeraNovi Technologies, Inc, USA

WILEY

A John Wiley and Sons, Ltd, Publication

Wireless Mesh Networks

ADVANCED TEXTS IN COMMUNICATIONS AND NETWORKING

The Wiley series on *Advanced Texts in Communications and Networking* offers a comprehensive range of graduate-level text books for use on the major graduate programmes in communications engineering and networking throughout Europe, the USA and Asia. The series provides technically detailed books covering cutting-edge research and new developments in wireless and mobile communications, and networking. Each book in the series contains supporting material for teaching/learning purposes (such as exercises, problems and solutions, objectives and summaries etc), and is accompanied by a website offering further information such as slides, teaching manuals and further reading.

Titles in the series:

Akyildiz and Wang: *Wireless Mesh Networks* 978-0470-03256-5 (January 2009)
Akyildiz and Vuran: *Wireless Sensor Networks* 978-0470-03601-3 (June 2009)

Wireless Mesh Networks

Professor Ian F. Akyildiz

Georgia Institute of Technology, USA

Dr Xudong Wang

TeraNovi Technologies, Inc, USA

WILEY

A John Wiley and Sons, Ltd, Publication

This edition first published 2009

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ,
United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

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

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Library of Congress Cataloging-in-Publication Data

Akyildiz, Ian F.
Wireless mesh networks / Ian Akyildiz, Xudong Wang.
p. cm.
Includes bibliographical reference and index.
ISBN 978-0-470-03256-5 (cloth)
1. Wireless communication systems. I. Wang, X. (Xudong) II. Title.
TK5103.2.A445 2009
621.384–dc22
2008038552

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

ISBN 9780470032565 (H/B)

Set in 10/12pt Times by Sunrise Setting Ltd, Torquay, UK.
Printed in Great Britain by Antony Rowe.

This book is dedicated to:

My father (1914–1976)
My mother (1923–1983)
You always have been and always will be the inspiration in my life.
Ian F. Akyildiz

My parents
for your love, support, and understanding.
Xudong Wang

Contents

About the Series Editor

Ian F. Akyildiz is the Ken Byers Distinguished Chair Professor with the School of Electrical and Computer Engineering, Georgia Institute of Technology; Director of Broadband Wireless Networking Laboratory and Chair of the Telecommunications Group. Since June 2008 he has been an Honorary Professor with the School of Electrical Engineering at the Universitat Politècnica de Catalunya, Barcelona, Spain. He is the Editor-in-Chief of *Computer Networks Journal* (Elsevier), is the founding Editor-in-Chief of the *Ad Hoc Networks Journal* (Elsevier) in 2003 and is the founding Editor-in-Chief of the *Physical Communication (PHYCOM) Journal* (Elsevier) in 2008. He is a past editor for *IEEE/ACM Transactions on Networking* (1996–2001), the *Kluwer Journal of Cluster Computing* (1997–2001), the *ACM-Springer Journal for Multimedia Systems* (1995–2002), *IEEE Transactions on Computers* (1992–1996) as well as the *ACM-Springer Journal of Wireless Networks (ACM WINET)* (1995–2005). Dr Akyildiz was the Technical Program Chair and General Chair of several IEEE and ACM conferences including ACM MobiCom'96, IEEE INFOCOM'98, IEEE ICC'03, ACM MobiCom'02 and ACM SenSys'03, and he serves on the advisory boards of several research centers, journals, conferences and publication companies. He is an IEEE Fellow (1996) and an ACM Fellow (1997), and served as a National Lecturer for ACM from 1989 until 1998. He received the ACM Outstanding Distinguished Lecturer Award for 1994, and has served as an IEEE Distinguished Lecturer for IEEE COMSOC since 2008. Dr Akyildiz has received numerous IEEE and ACM awards including the 1997 IEEE Leonard G. Abraham Prize award (IEEE Communications Society), the 2002 IEEE Harry M. Goode Memorial award (IEEE Computer Society), the 2003 Best Tutorial Paper Award (IEEE Communications Society), the 2003 ACM SIGMOBILE Outstanding Contribution Award, the 2004 Georgia Tech Faculty Research Author Award and the 2005 Distinguished Faculty Achievement Award. Dr Akyildiz is the author of two advanced textbooks entitled *Wireless Mesh Networks* and *Wireless Sensor Networks*, published by John Wiley & Sons in 2009. His current research interests are in Cognitive Radio Networks, Wireless Sensor Networks, Wireless Mesh Networks and Nanonetworks.

Preface

Wireless Mesh Networks (WMNs) are one of the key technologies which will dominate wireless networking in the next decade. They will help to realize the long-lasting dream of network connectivity anywhere anytime with simplicity and low cost. Accordingly they will play a major role within the next generation Internet. Their capability for self-organization significantly reduces the complexity of network deployment and maintenance, and thus, requires minimal upfront investment.

These networks consist of simple mesh routers and mesh clients, where mesh routers have minimal mobility and form the backbone of WMNs. They provide network access for both mesh and conventional clients. The integration of WMNs with other networks such as the Internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor networks, etc., can be accomplished through the gateway and bridging functions in the mesh routers. Mesh clients can be either stationary or mobile, and can form a client mesh network among themselves and with mesh routers. WMNs are anticipated to resolve the limitations and to significantly improve the performance of ad hoc networks, wireless local area networks (WLANs), wireless personal area networks (WPANs), and wireless metropolitan area networks (WMANs). These networks deliver wireless services to a large variety of applications in personal, local, campus, and metropolitan areas.

In the fall of 2003 we started to work on our survey paper "A Survey on Wireless Mesh Networks" which appeared in March 2005 issue of the Computer Networks (Elsevier) journal with a much shorter and more concise version appearing in the IEEE Communication magazine in September 2005. Note that, over the years, both of these papers were among the top ten downloaded papers within Elsevier and IEEE Communication journals. As we were writing the survey paper we realized that the paper could be converted into a textbook because of the future promise of this technology. However, the field was not mature and there was not enough material to create a textbook at that stage. This, of course, has changed over the past five years. These networks have undergone very rapid progress and have inspired numerous deployments. Research has been accelerated all around the world and several companies have already been offering products to the market, while other companies have started to deploy these networks in various application scenarios. Despite several advances in wireless mesh networking in recent years, many research challenges still remain. The research is being conducted in a very speedy way worldwide and a very large number of papers already exist in the literature and the race is still on to advance this technology.

In close interaction with students, researchers, and engineers, we realized that the time had come to publish this book which is targeted at teaching graduate students, stimulating them for new research ideas, and providing academic and industry professionals with a thorough overview and in-depth understanding of the state-of-the-art in wireless mesh networking and to indicate how they can develop new ideas to advance this technology as well as support emerging applications and services. The book will fill the gap for a comprehensive coverage of all research results on this topic published these past few years. The book covers many published research results including the authors' own contributions as well as all the standardization committee decisions in a cohesive and unified form.

The contents of the book follows the TCP/IP protocol stack starting from the physical layer and covering each protocol layer in detail. Functionalities and existing protocols and algorithms for each layer are covered in depth. The aim is to teach the readers what is already available and how these networks can be further improved and advanced by pointing out open research challenges in each chapter.

Chapter 1 gives a comprehensive introduction to WMNs, including network architectures, characteristics, critical design factors, and typical application scenarios. Chapter 2 studies advanced physical techniques for WMNs, such as adaptive modulation and coding, multi-antenna systems, multi-channel systems, multi-radio systems, and software radios. Chapter 3 presents and compares various medium access control (MAC) protocols for WMNs, ranging from carrier-sense multi-access with collision avoidance (CDMA/CA) variants, TDMA based MAC, CDMA based MAC, to multiple multi-channel MAC protocols. Chapter 4 is dedicated to routing protocols for WMNs. Various routing metrics for WMNs are investigated and compared. Different categories of routing protocols are also presented. Chapter 5 introduces the principles of different basic transport protocols and then investigates various transport protocols proposed for multi-hop wireless networks including WMNs. Chapter 6 looks into the security issues. Security mechanisms specified in IEEE 802.11 and 802.16 are first presented, followed by a detailed study of security protocols for ad hoc networks and WMNs. Chapter 7 discusses different protocols that control and manage WMNs, which include topology management, power management, mobility management, and network synchronization. Chapter 8 is focused on capacity analysis. Different analytical methods proposed to derive wireless network capacity are presented, and different capacity bounds are compared. The results and limitations of existing capacity bounds for WMNs are also discussed. Chapter 9 studies cross-design mechanisms across different protocol layers of WMNs. Limitations and strategies for cross-layer design are also pointed out. Chapter 10 surveys standards that have been specified or standards drafts that are being specified for WMNs. In particular, the latest standardization results in IEEE 802.11s, 802.15.5, 802.16 mesh mode, and 802.16 relay mode are presented. In all these chapters, open research problems have been pointed out and some potential solutions have also been discussed.

It is a major task and challenge to produce a textbook. Although the authors usually have the major burden, there are several other key people who help to publish a book. The foremost thanks go to Birgit Gruber from John Wiley and Sons who initiated the entire idea of writing this book. Her incredible persistence, patience and passion helped to achieve our objective. Several other colleagues, Sarah Tilley, Anna Smart, Sarah Hinton, Rowan January, Joanna Toothill, and finally Tiina Ruonamaa at John Wiley and Sons, have been incredibly helpful and patient. Their assistance, ideas, dedication, and support for the creation of this book will always be greatly appreciated. We also thank several individuals who directly or indirectly contributed to our book. In particular, our sincere thanks go to Cagri Gungor, Stefano Avallone, Claudio Cicconetti, Marco di Felice and Guomei Zhou for their help. Our families sacrificed the most during the creation of this book. No words can express our appreciation and love for their enormous support.

1

Introduction

As various wireless networks evolve into the next generation to provide better services, a key technology, wireless mesh networks (WMNs) has emerged recently [7, 8]. In WMNs, nodes are comprised of mesh routers and mesh clients. Each node operates not only as a host but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. A WMN is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (creating, in effect, an ad hoc network). This feature brings many advantages to WMNs such as low up-front costs, easy network maintenance, robustness, and reliable service coverage.

Conventional nodes, e.g., desktops, laptops, PDAs, PocketPCs, phones, equipped with wireless network interface cards (NICs) can be connected directly to wireless mesh routers. Customers without wireless NICs can access WMNs by connecting to wireless mesh routers through, for example, Ethernet. Thus, WMNs will greatly help users to be always-on-line anywhere anytime. Moreover, the gateway/bridge functionalities in mesh routers enable the integration of WMNs with various existing wireless networks such as cellular systems, wireless sensor networks, wireless-fidelity (Wi-Fi) [264] systems, worldwide inter-operability for microwave access (WiMAX) [265], and WiMedia [266] networks. Consequently, through an integrated WMN, users of existing networks are provided with otherwise impossible services of these networks.

Wireless Mesh Networking is a promising wireless technology for numerous applications [189], e.g., broadband home networking, community and neighborhood networks, enterprise networking, building automation, etc. It is gaining significant attention as a possible way for cash-strapped Internet service providers (ISPs), carriers, and others to roll out robust and reliable wireless broadband service access in a way that needs minimal up-front investments. With the capability of self-organization and self-configuration, WMNs can be deployed incrementally, one node at a time, as needed. As more nodes are installed, up goes the reliability, and also the connectivity, that all subscribers will enjoy.

Deploying a WMN is not too difficult, because all the required components are already available in the form of ad hoc routing protocols, IEEE 802.11 MAC protocol, wired equivalent privacy (WEP) security, etc. Several companies have already realized the potential

Wireless Mesh Networks Ian F. Akyildiz and Xudong Wang

of this technology and offer wireless mesh networking products. A few testbeds have been established in university research labs. However, to make a WMN be all it can be, considerable research efforts are still needed. For example, the available MAC and routing protocols applied to WMNs do not have enough scalability; e.g., throughput drops significantly as the number of nodes or hops increases. Existing security schemes may be effective for certain types of attack, but they lack a comprehensive mechanism to prevent attacks from different protocol layers. Similar problems exist in other networking protocols. Thus, existing communication protocols, ranging from application layer to transport, routing, MAC, and physical layers, need to be revisited and enhanced. In some circumstances, new protocols need to be invented.

Researchers have started to revisit the protocol design of existing wireless networks, especially of IEEE 802.11 networks, ad hoc networks, and wireless sensor networks, from the perspective of WMNs. Industrial standards groups are also actively working on new specifications for mesh networking. For example, IEEE 802.11 [113, 138], IEEE 802.15 [124, 147], and IEEE 802.16 [129, 211, 263] all have established subworking-groups to focus on new standards for WMNs.

1.1 Network Architecture

WMNs consist of two types of nodes: mesh routers and mesh clients. Other than the routing capability for gateway/repeater functions as in a conventional wireless router, a wireless mesh router contains additional routing functions to support mesh networking. To further improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. Compared to a conventional wireless router, a wireless mesh router can achieve the same coverage with much lower transmission power through multihop communications. Optionally, the medium access control protocol in a mesh router is enhanced with a better scalability in a multihop mesh environment.

In spite of all these differences, mesh and conventional wireless routers are usually built based on a similar hardware platform. Mesh routers can be built based on dedicated computer systems, e.g., embedded systems, and look compact, as shown in Figure 1.1. They can also be built based on general-purpose computer systems, e.g., laptop/desktop PCs.

Mesh clients also have the necessary functions for mesh networking, and thus can also work as a router in WMN. However, gateway or bridge functions do not exist in these nodes. In addition, mesh clients usually have only one wireless interface. As a consequence, the hardware platform and the software for mesh clients can be much simpler than those for mesh routers. Mesh clients have a greater variety of devices compared to mesh routers. They can be a laptop/desktop PC, pocket PC, PDA, IP phone, RFID reader, BACnet (Building Automation and Control network) controller, and many other devices, as shown in Figure 1.2.

The architecture of WMNs can be classified into three main groups based on the functionality of the nodes.

- **Infrastructure/Backbone WMNs:**

  The architecture is shown in Figure 1.3, where dashed and solid lines indicate wireless and wired links, respectively. This type of WMN includes mesh routers that form an infrastructure for clients that connect to them. The WMN infrastructure/backbone

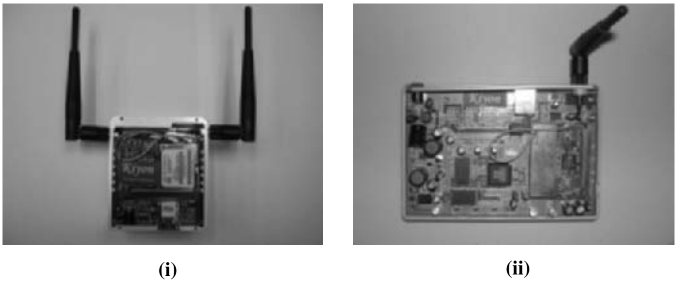

Figure 1.1 Examples of mesh routers based on different embedded systems: (i) PowerPC, (ii) ARM

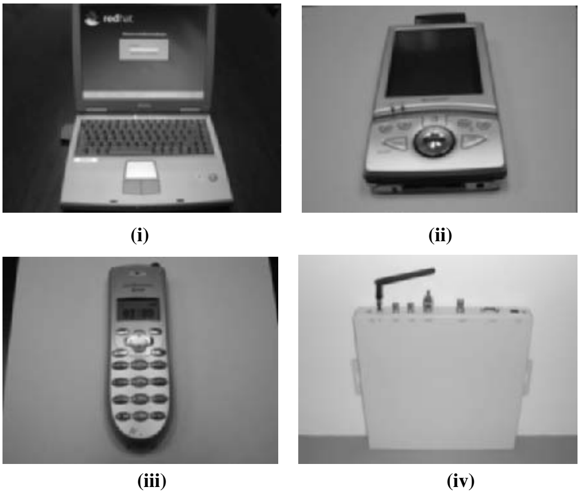

Figure 1.2 Examples of mesh clients: (i) laptop, (ii) PDA, (iii) Wi-Fi IP phone, (iv) Wi-Fi RFID reader

can be built using various types of radio technology, in addition to the heavily used IEEE 802.11 technology. The mesh routers form a mesh of self-configuring, self-healing links among themselves. With gateway functionality, mesh routers can be connected to the Internet. This approach, also referred to as *infrastructure meshing*, provides backbone for conventional clients and enables the integration of WMNs with existing wireless networks, through gateway/bridge functionalities in mesh routers. Conventional clients with Ethernet interface can be connected to mesh routers via Ethernet links. For conventional clients with the same radio technologies as mesh routers, they can directly communicate with mesh routers. If different radio technologies are used, clients must communicate with the base stations that have Ethernet connections to mesh routers.

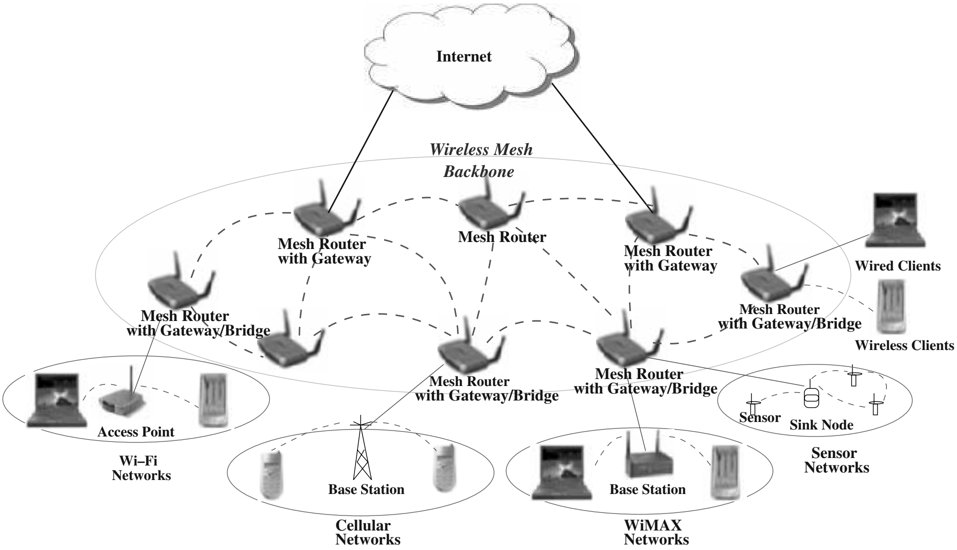

Figure 1.3 Infrastructure/backbone WMNs

Infrastructure/Backbone WMNs are the most commonly used type. For example, community and neighborhood networks can be built using *infrastructure meshing*. The mesh routers are placed on the roofs of houses in a neighborhood, and these can serve as access points for users in homes and along the roads. Typically, two types of radio are used in the routers, i.e., for backbone communication and for user communication. The mesh backbone communication can be established using long-range communication techniques including, for example, directional antennas.

- **Client WMNs:** *Client meshing* provides peer-to-peer networks among client devices. In this type of architecture, client nodes constitute the actual network to perform routing and configuration functionalities as well as providing end-user applications to customers. Hence, a mesh router is not required for this type of network. The basic architecture is shown in Figure 1.4. In *Client WMNs*, a packet destined to a node in the network hops through multiple nodes to reach the destination. *Client WMNs* are usually formed using one type of radio on devices. Moreover, the requirements on end-user devices is increased when compared to *infrastructure meshing*, since, in *Client WMNs*, the end users have to perform additional functions such as routing and self-configuration.

- **Hybrid WMNs:** This architecture is the combination of *infrastructure* and *client meshing* as shown in Figure 1.5. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, WiMAX, cellular, and sensor networks, the routing capabilities of clients provide improved connectivity and coverage inside the WMN. The hybrid architecture will be the most applicable case in our opinion.

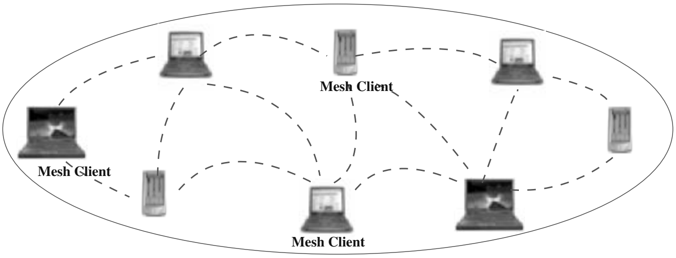

Figure 1.4 Client WMNs

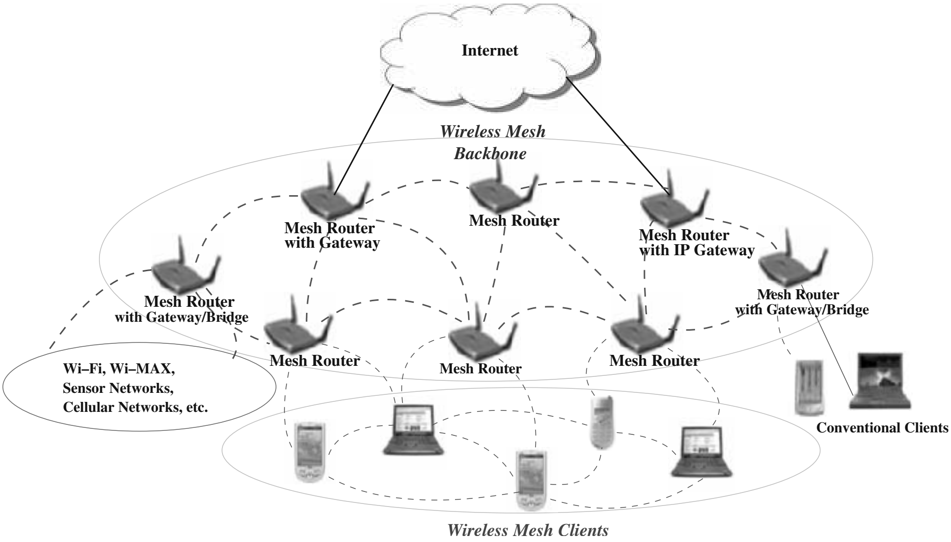

Figure 1.5 Hybrid WMNs

1.2 Characteristics

The characteristics of WMNs are explained in what follows.

- **Multihop wireless network:** One incentive to develop WMNs is to extend the coverage range of current wireless networks without sacrificing the channel capacity. Another major objective of WMNs is to provide nonline-of-sight (NLOS) connectivity among users without direct line-of-sight (LOS) links. To meet these requirements, mesh-style multihopping is indispensable [154], which facilitates higher throughput without sacrificing effective radio range via shorter link distances, less interference between nodes, and more efficient frequency reuse.

- **Support for ad hoc networking, and capability of self-forming, self-healing, and self-organization:** Ad hoc networking enhances network performance, such as flexible network architecture, easy deployment and configuration, fault tolerance, and mesh connectivity, i.e., multipoint-to-multipoint communications. Due to these features, WMNs have low upfront investment requirement, and the network can grow gradually as needed.

- **Mobility dependence on the type of mesh nodes:** Mesh routers usually have minimal mobility, while mesh clients can be stationary or mobile nodes. Thus, the mobility in WMNs varies from node to node, which is different from ad hoc networks.

- **Multiple types of network access:** In WMNs, both backhaul access to the Internet and peer-to-peer (P2P) communications within WMNs are supported [139]. In addition, integration of WMNs with other wireless networks and providing services to end-users of these networks can be accomplished through WMNs. However, an ad hoc network does not require these capabilities.

- **Dependence of power-consumption constraints on the type of mesh nodes:** Mesh routers in WMNs usually do not have strict constraints on power consumption. However, mesh clients may require power efficient protocols. As an example, a mesh-capable sensor requires its communication protocols to be power efficient. Thus, the MAC or routing protocols optimized for mesh routers may not be appropriate for mesh clients, because power efficiency is the primary concern for wireless sensor networks [10, 11].

- **Compatibility and interoperability with existing wireless networks:** For example, WMNs built based on IEEE 802.11 technologies [133] must be compatible with IEEE 802.11 standards in the sense of supporting both mesh-capable and conventional Wi-Fi clients. Such WMNs also need to be interoperable with other wireless networks such as WiMAX, ZigBee [293], and cellular systems.

Based on their characteristics, WMNs are generally considered as a type of ad hoc network owing to the lack of wired infrastructure that exists in cellular or Wi-Fi networks through deployment of base stations or access points. While ad hoc networking techniques are required by WMNs, the additional capabilities necessitate more sophisticated algorithms and design principles for the realization of WMNs. More specifically, instead of being a type of ad hoc networking, WMNs aim to diversify the capabilities of ad hoc networks. Consequently, ad hoc networks can actually be considered as a *subset* of WMNs. To illustrate this point, the differences between WMNs and ad hoc networks are outlined below. In this comparison, the hybrid architecture is considered, since it comprises all the advantages of WMNs.

- **Wireless infrastructure/backbone:** As discussed before, WMNs consist of a wireless backbone with mesh routers. The wireless backbone provides wide coverage, connectivity, and robustness in the wireless domain. However, the connectivity of ad hoc networks depends on the individual contributions of end users which may not be reliable.

- **Integration:** WMNs support conventional clients that use the same radio technologies as a mesh router. This is accomplished through a host-routing function available in mesh routers. WMNs also enable integration of various existing networks such as Wi-Fi, the Internet, cellular and sensor networks through gateway/bridge functionalities in the mesh routers. Consequently, users in one network are provided with services in other networks, through the use of the wireless infrastructure. The integrated wireless networks through WMNs resemble the Internet backbone, since the physical location of network nodes becomes less important than the capacity and network topology.

- **Dedicated routing and configuration:** In ad hoc networks, end-user devices also perform routing and configuration functionalities for all other nodes in the networks. However, WMNs contain mesh routers for these functionalities. Hence, the load on end-user devices is significantly decreased, which provides a lower energy consumption and high-end application capabilities to possibly mobile and energy-constrained end-users. Moreover, the end-user requirements are limited which decreases the cost of devices that can be used in WMNs.

- **Multiple radios:** As discussed before, mesh routers can be equipped with multiple radios to perform routing and access functionalities. This enables separation of two main types of traffic in the wireless domain. While routing and configuration traffic is performed between mesh routers, access to the network from end users can be carried on a different radio. This significantly improves the capacity of the network. On the other hand, these functionalities are performed in the same channel in ad hoc networks constraining the performance.

- **Mobility:** Since ad hoc networks provide routing using the end-user devices, the network topology and connectivity depend on the movement of users. This imposes additional challenges to routing protocols as well as network configuration and deployment. Since mesh routers provide the infrastructure in WMNs, the coverage of the WMN can be engineered easily. While providing continuous connectivity throughout the network, the mobility of end users is still supported, without compromising the performance of the network.

- **Compatibility:** WMNs contain many differences when compared to ad hoc networks. However, as discussed above, ad hoc networks can be considered as a subset of WMNs. More specifically, the existing techniques developed for ad hoc networks are already applicable to WMNs. As an example, through the use of mesh routers and routing-capable end users, multiple ad hoc networks can be supported in WMNs, but with further integration of these networks.

1.3 Application Scenarios

Research and development of WMNs is motivated by several applications which clearly demonstrate the promising market, but, at the same time, these applications cannot be supported directly by other wireless networks such as cellular systems, ad hoc networks, wireless sensor networks, standard IEEE 802.11, etc. In this section, we discuss these applications.

- *Broadband home networking:* Currently broadband home networking is realized through IEEE 802.11 WLANs. An obvious problem is the location of the access points. Without a site survey, a home (even a small one) usually has many dead zones without

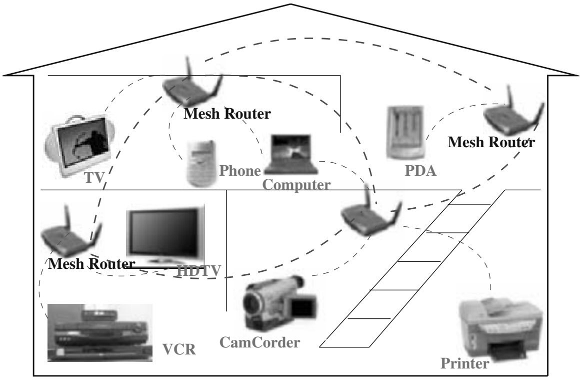

Figure 1.6 WMNs for broadband home networking

service coverage. Solutions based on site survey are expensive and not practical for home networking, while installation of multiple access points is also expensive and not convenient because of Ethernet wiring from access points to backhaul network access modem or hub. Moreover, communications between end nodes under two different access points have to go all the way back to the access hub. This is obviously not an efficient solution, especially for broadband networking. Mesh networking, as shown in Figure 1.6, can resolve all these issues in home networking. The access points must be replaced by wireless mesh routers with mesh connectivity established among them. Therefore, the communication between these nodes becomes much more flexible and more robust to network faults and link failures. Dead zones can be eliminated by adding mesh routers, changing locations of mesh routers, or automatically adjusting power levels of mesh routers. Communication within home networks can be realized through mesh networking without going back to the access hub all the time. Thus, network congestion due to backhaul access can be avoided. In this application, wireless mesh routers have no constraints on power consumptions and mobility. Thus, protocols proposed for mobile ad hoc networks [59] and wireless sensor networks [10,11] are too cumbersome to achieve satisfactory performance in this application. On the other hand, Wi-Fis are not capable of supporting ad hoc multihop networking. As a consequence, WMNs are well suited for broadband home networking.

- *Community and neighborhood networking:* In a community, the common architecture for network access is based on cable or digital subscriber line (DSL) connected to the Internet, and the last hop is wireless by connecting a wireless router to a cable or DSL modem. This type of network access has several drawbacks.

  - Even if the information must be shared within a community or neighborhood, all traffic must flow through the Internet. This significantly reduces network resource utilization.
  - A large percentage of areas in between houses is not covered by wireless services.

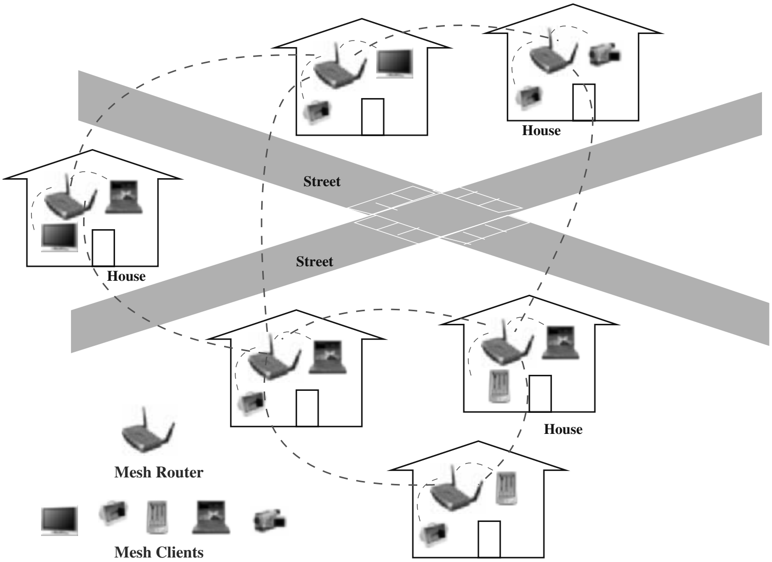

Figure 1.7 WMNs for community networking

- An expensive but high-bandwidth gateway between multiple homes or neighborhoods may not be shared, and wireless services must be set up individually. As a result, network service costs may increase.
- Only a single path may be available for one home to access the Internet or communicate with neighbors.

WMNs mitigate the above disadvantages through flexible mesh connectivities between homes, as shown in Figure 1.7. WMNs can also enable many applications such as distributed file storage, distributed file access, and video streaming.

- *Enterprise networking:* This can be a small network within an office or a medium-size network for all offices in an entire building, or a large-scale network among offices in multiple buildings. Currently standard IEEE 802.11 wireless networks are widely used in various offices. However, these wireless networks are still isolated islands. Connections among them have to be achieved through wired Ethernet connections, which is the key reason for the high cost of enterprise networks. In addition, adding more backhaul access modems only increases capacity locally, but it does not improve robustness to link failures, network congestion, and other problems of the entire enterprise network. If the access points are replaced by mesh routers, as shown in Figure 1.8, Ethernet wires can be eliminated. Multiple backhaul access modems can be shared by all nodes in the entire network, and thus improve the robustness and resource utilization of enterprise networks. WMNs can grow easily as the size of enterprise expands.

  WMNs for enterprise networking are much more complicated than at home because more nodes and more complicated network topologies are involved. The service model

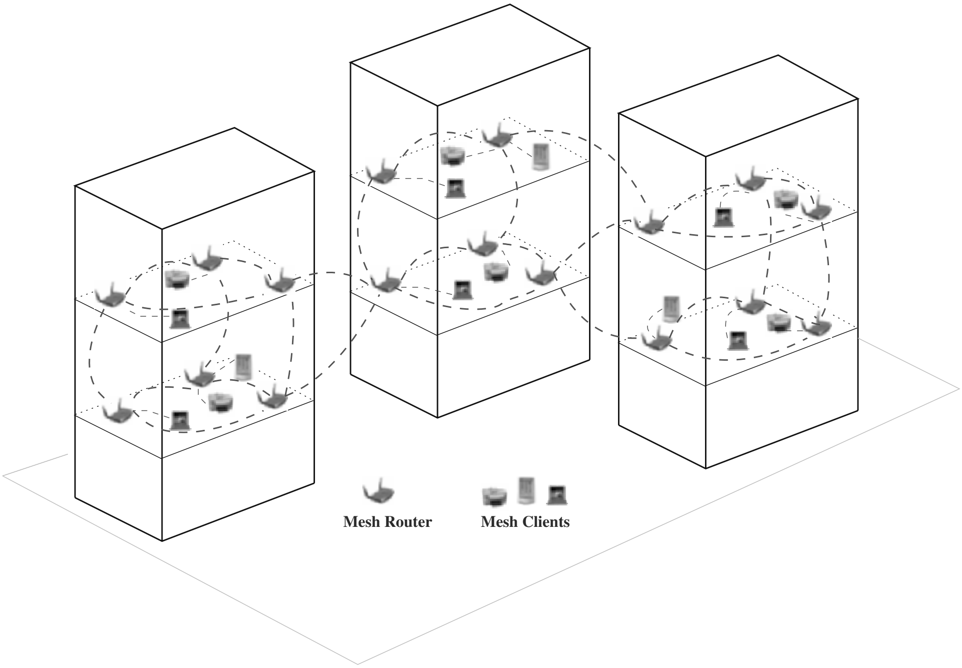

Figure 1.8 WMNs for enterprise networking

of enterprise networking can be applied to many other public and commercial service networking scenarios such as airports, hotels, shopping malls, convention centers, sport centers, etc.

- *Metropolitan area networks (MAN):* WMNs in a metropolitan area have several advantages. The physical-layer transmission rate of a node in WMNs is much higher than that in any cellular systems. For example, an IEEE 802.11g node can transmit at a rate of 54 Mbps. Moreover, the communication between nodes in WMNs does not rely on a wired backbone. Compared to wired networks, e.g., cable or optical networks, wireless mesh MAN is an economic alternative to broadband networking, especially in underdeveloped regions. The wireless mesh MAN covers a potentially much larger area than home, enterprise, building, or community networks, as shown Figure 1.9. Thus, the requirement on the network scalability by wireless mesh MANs is much higher than that by other applications.

- *Transportation systems:* Instead of limiting IEEE 802.11 or 802.16 access to stations and stops, mesh networking technology can extend access into buses, ferries, and trains. Thus, convenient passenger information services, remote monitoring of in-vehicle security video, and driver communications can be supported. To enable such mesh networking for a transportation system, two key techniques are needed: the high-speed mobile backhaul from a vehicle (car, bus, or train) to the Internet, and mobile mesh networks within the vehicle, as shown in Figure 1.10.

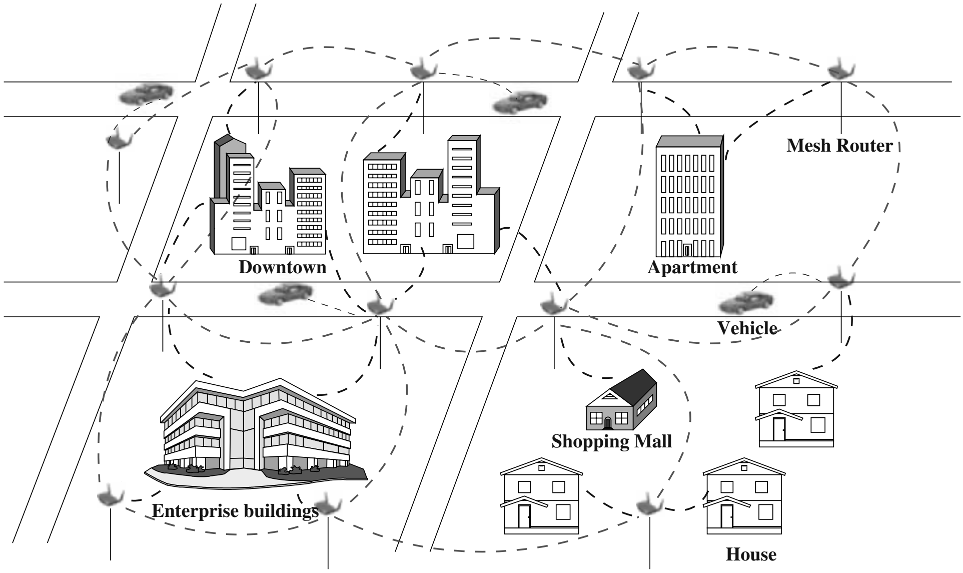

Figure 1.9 WMNs for metropolitan area networks

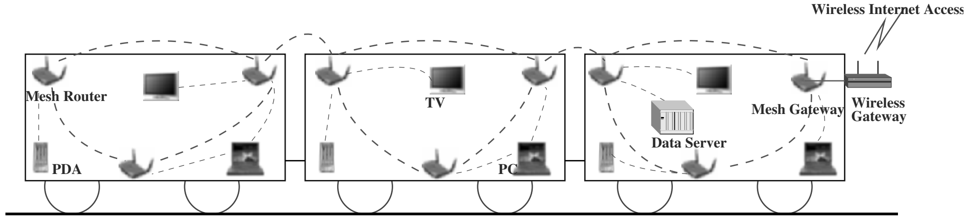

Figure 1.10 WMNs for transportation systems

- *Building automation:* In a building, various electrical devices including power, light, elevator, air conditioner, etc., need to be controlled and monitored. Currently, this task is accomplished through standard wired networks, which is very expensive due to the complexity in deployment and maintenance of a wired network. Recently, Wi-Fi-based networks have been adopted to reduce the cost of such networks. However, this effort has not achieved satisfactory performance yet, because the deployment of Wi-Fi for this application is still rather expensive due to the wiring of Ethernet. If BACnet (Building Automation and Control networks) access points are replaced by mesh routers, as shown in Figure 1.11, the deployment cost will be significantly reduced. The deployment process is also much simpler due to the mesh connectivity among wireless routers.

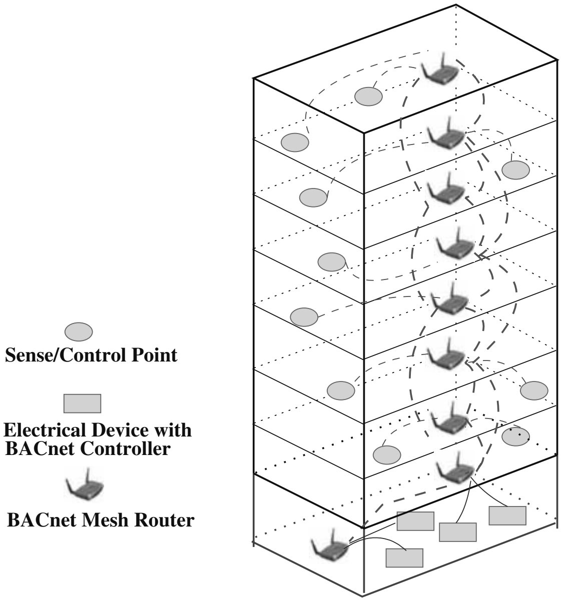

Figure 1.11 WMNs for building automation

- *Health and medical systems:* In a hospital or medical center, monitoring and diagnosis data need to be processed and transmitted from one room to another for various purposes. Data transmission is usually broadband, since high resolution medical images and various periodical monitoring information can easily produce a constant and large volume of data. Traditional wired networks can only provide limited network access to certain fixed medical devices. Wi-Fi-based networks must rely on the existence of Ethernet connections, which may cause high system cost and complexity but without the abilities to eliminate dead spots. However, these issues do not exist in WMNs.

- *Security surveillance systems:* As security is turning out to be a very high concern, security surveillance systems become a necessity for enterprise buildings, shopping malls, grocery stores, etc. In order to deploy such systems at locations as needed, WMNs are a much more viable solution than wired networks to connect all devices. Since still images and videos are the major traffic flowing in the network, this application demands much higher network capacity than other applications.

In addition to the above applications, WMNs can also be applied to *spontaneous (emergency/disaster) networking* and *P2P communications*. For example, wireless networks for an emergency response team and firefighters do not have in-advance knowledge of where the network should be deployed. By simply placing wireless mesh routers in desired locations, a WMN can be quickly established. For a group of people holding devices with wireless networking capability, e.g., laptops and PDAs, P2P communication anytime anywhere is an efficient solution for information sharing. WMNs are able to meet this demand. These applications illustrate that WMNs are a superset of ad hoc networks, and thus, can accomplish all functions provided by ad hoc networking.

1.4 Critical Design Factors

Before a network is designed, deployed, and operated, factors that critically influence its performance need to be considered. For WMNs, the critical factors are summarized as follows.

- *Radio techniques.* Driven by the rapid progress of semiconductor, RF technologies, and communication theory, wireless radios have undergone a significant revolution. Currently many approaches have been proposed to increase capacity and flexibility of wireless systems. Typical examples include directional and smart antennas [219, 240], MIMO systems [245, 272], and multiradio/multichannel systems [4, 236]. To date, MIMO has become one of the key technologies for IEEE 802.11n [113], the high speed extension of Wi-Fi. Multiradio chipsets and their development platforms are available on the market.

  To further improve the performance of a wireless radio and control by higher layer protocols, more advanced radio technologies such as reconfigurable radios, frequency agile/cognitive radios [158, 188], and even software radios [191] have been used in wireless communication.

  Although these radio technologies are still in their infancy, they are expected to be the future platform for wireless networks owing to their capability of dynamically controlling the radios. These advanced wireless radio technologies all require a revolutionary design in higher layer protocols, especially in MAC and routing protocols. For example, when directional antennas are applied to IEEE 802.11 networks, a routing protocol needs to take into account the selection of directional antenna sectors. Directional antennas can reduce exposed nodes, but they also generate more hidden nodes. Thus, MAC protocols need to be redesigned to resolve this issue. As for MIMO systems, new MAC protocols are also necessary [245]. When software radios are considered, much more powerful MAC protocols, such as programmable MAC, are anticipated.

- *Scalability.* Multihop communication is common in WMNs. For multihop networking, it is well known that communication protocols suffer from scalability issues [108, 134], i.e., when the size of network increases, the network performance degrades significantly. Routing protocols may not be able to find a reliable routing path, transport protocols may lose connections, and MAC protocols may experience significant throughput reduction. As a typical example, the current IEEE 802.11 MAC protocol and its derivatives cannot achieve a reasonable throughput as the number of hops increases to four or higher (for 802.11b, the TCP throughput is lower than 1.0 Mbps). The reason for low scalability is that the end-to-end reliability sharply drops as the scale of the network increases. In WMNs, due to their ad hoc architecture, the centralized multiple access schemes such as Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA) are difficult to implement due to their complexities and a general requirement on timing synchronization for TDMA (and code management for CDMA). When a distributed multihop network is considered, accurate timing synchronization within the global network is difficult to achieve [108]. Thus, distributed multiple access schemes such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) are more favorable. However, CSMA/CA has very low frequency spatial-reuse efficiency [3], which significantly limits the scalability of CSMA/CA-based multihop networks. To improve the scalability of WMNs, designing a hybrid multiple access scheme with CSMA/CA and TDMA or CDMA is an interesting and challenging research issue.

- *Mesh connectivity.* Many advantages of WMNs originate from mesh connectivity which is a critical requirement on protocol design, especially for MAC and routing protocols. Network self-organization and topology control algorithms are generally needed. Topology-aware MAC and routing protocols can significantly improve the performance of WMNs.

- *Broadband and QoS.* Different from other ad hoc networks, most applications of WMNs are broadband services with various QoS requirements. Thus, in addition to the end-to-end transmission delay and fairness, more performance metrics such as delay jitter, aggregate and per-node throughput, and packet loss ratios, must be considered by communication protocols.

- *Compatibility and interoperability.* It is a desired feature for WMNs to support network access for both conventional and mesh clients. Thus, WMNs need to be backward compatible with conventional client nodes; otherwise, the motivation of deploying WMNs will be significantly compromised. Integration of WMNs with other wireless networks requires certain mesh routers to have the capability of interoperation among heterogeneous wireless networks.

- *Security.* Without a convincing security solution, WMNs will not be able to succeed due to the lack of incentives by customers to subscribe to reliable services. Although many security schemes have been proposed for wireless LANs, they are still not ready for WMNs. For instance, there is no centralized trusted authority to distribute a public key in a WMN owing to the distributed system architecture. The existing security schemes proposed for ad hoc networks can be adopted for WMNs, but several issues exist.

  - Most security solutions for ad hoc networks are still not mature enough to be practically implemented.
  - The network architecture of WMNs is different from a conventional ad hoc network, which causes differences in security mechanisms.

  As a consequence, new security schemes ranging from encryption algorithms to security key distribution, secure MAC and routing protocols, intrusion detection, and security monitoring need to be developed.

- *Ease of use.* Protocols must be designed to enable the network to be as autonomic as possible, in the sense of automatic power management, self-organization, dynamic topology control, robust to temporary link failure, and fast network-subscription/user-authentication procedure. In addition, network management tools need to be developed to efficiently maintain the operation, monitor the performance, and configure the parameters of WMNs. These tools together with the autonomic mechanisms in protocols enable rapid deployment of WMNs.

2

Physical Layer

Physical layer techniques advance rapidly as communication theories, digital signal processing algorithms, RF technologies, and circuit design for wireless communications quickly evolve. These techniques mainly focus on three directions: increasing transmission rate, improving error resilience capability in a wireless environment, and enhancing reconfigurability and software controllability of radios.

In order to increase the capacity of wireless networks, various high-speed physical techniques have been invented. For example, orthogonal frequency division multiplexing (OFDM) has significantly increased the speed of IEEE 802.11 from 11 Mbps to 54 Mbps. A much higher transmission rate can be achieved through Ultra-Wideband (UWB) techniques. However, UWB is only applicable to short-distance applications such as wireless personal area networks (WPANs). If a transmission speed as high as that of UWB is desired in a wider area network such as WLANs or WMANs, other physical techniques, such as the multiple-input multiple-output (MIMO) mechanism, are needed. In order to further increase capacity and mitigate the impairment by fading, delay-spread, and co-channel interference, multiple-antenna systems [38, 194] have been used for wireless communication. It should be noted that spectrum efficiency must be maintained as high as possible while a new physical layer technique is developed to increase the transmission rate.

To improve error resilience, many channel coding schemes have been developed. Since channel condition varies, a fixed channel coding scheme is not efficient. Thus, an adaptive channel coding scheme is needed. For example, in 3G cellular networks and IEEE 802.11a, coding schemes must be varied as channel condition changes.

In the third direction, physical layer techniques are developed such that they can be controlled by software. Such a capability brings many advantages to wireless communications. For example, physical layer techniques can be optimized adaptively according to the variable conditions in the environment, so that the research and development cycle can be dramatically shortened, radios can be reconfigured, and so on. When cognitive radios are considered, the scarce wireless spectrum can be much better utilized.

In this chapter, advanced techniques along all three directions are discussed. In particular, techniques that have great potential for WMNs are studied. Examples include adaptive modulation and coding, multi-antenna systems, multichannel or multiradios, link adaptation

Wireless Mesh Networks Ian F. Akyildiz and Xudong Wang

Table 2.1 IEEE 802.11a channel coding and modulation

Modulation	Data bits per OFDM symbol	Coded bits per OFDM symbol	Coding rate (Mbps)	Transmission rate
BPSK	24	48	1/2	6
BPSK	36	48	3/4	9
QPSK	48	96	1/2	12
QPSK	72	96	3/4	18
16 QAM	96	192	1/2	24
16 QAM	144	192	3/4	36
64 QAM	192	288	2/3	48
64 QAM	216	288	3/4	54

techniques, software radios, and so on. In order to demonstrate how different physical layer techniques are integrated into the same system, the IEEE 802.11n physical layer [120] is investigated.

Physical layer techniques are usually only concerned with single-hop point-to-point communications. However, when they are applied to WMNs, they will experience new, challenging problems that degrade their performance in a wireless mesh networking environment. Thus, research problems involved in the physical layer of WMNs are pointed out in this chapter. Solutions to these problems are also discussed.

2.1 Adaptive Coding/Modulation and Link Adaptation

In a wireless network, channels usually experience two types of variation.

- *Large scale variations.* These are due to the variable path loss between transmitter and receiver and the variable variance of the mean value of path loss, called shadow fading.

- *Small scale variations.* These are caused by rapid fluctuations of received signal strength over a short time period or travel distance due to multipath propagation. In a broadband network, these rapid variations can cause frequency selective fading.

Because of variations of channel quality, if the same coding and modulation scheme is used all the time, then the bit error rate (BER) in a channel varies significantly, which equivalently reduces the channel capacity and degrades the performance of upper layer protocols.

To resolve this issue, an effective approach is to perform adaptive channel coding and modulation, which has been adopted in many wireless networks such as 3G cellular networks and IEEE 802.11 wireless LANs. For example, in IEEE 802.11a the different channel coding and modulation schemes are as shown in Table 2.1.

With adaptive channel coding and modulation, adaptive error resilience can be provided through link adaptation [55, 94, 214]. As shown in Figure 2.1, the transmission rate of IEEE 802.11a is much higher if link adaptation is adopted. Because of this advantage, link adaptation is widely used for IEEE 802.11 wireless LANs [115, 118].

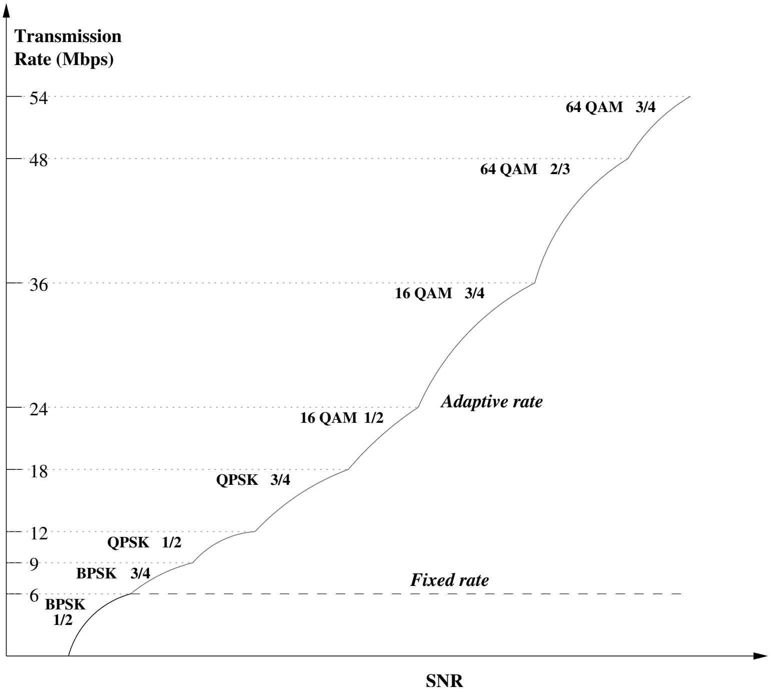

Figure 2.1 Adaptive transmission rate

The basic concept of link adaptation is actually quite simple: adjusting the transmission parameters (e.g. modulation/coding levels) to take advantage of prevailing channel conditions. However, several potential issues need to be considered when link adaptation is desired.

- *Impact on the MAC protocol.* To utilize the capability of adaptive channel coding/modulation in the physical layer, an algorithm must be developed at the MAC layer to take advantage of it. In other words, link adaptation is usually performed at the MAC layer. For example, a rate control algorithm must be implemented in IEEE 802.11 MAC to adaptively select the best transmission rate according to channel conditions. However, link adaptation may impact the design of a MAC protocol. For example, the variable transmission time of a packet makes any mechanisms based on packet count useless. Furthermore, when the performance of a MAC protocol is evaluated, it is also necessary to take into account the variable transmission rate due to link adaptation.

- *Selection of channel state information (CSI) and its availability.* CSI is a type of channel quality indicator. Typical examples of CSI include signal-to-noise ratio (SNR), carrier-to-interference ratio (CIR), and BER at the physical layer, and packet error rate (PER) at the link layer. However, some of them may not be readily measured in a wireless network. On the other hand, one single type of CSI may not be sufficient for link adaptation. For example, under a frequency-selective fading environment, a link adaptation algorithm cannot take signal-to-noise ratio (SNR) or carrier-to-interference ratio (CIR) as a single input from the physical layer, because SNR or CIR alone does not adequately describe the channel quality [157].

- *Dimensions of transmission parameters.* In some wireless networks, the transmission parameters to be adapted are more than just coding or modulation levels. Parameters such as power levels, spreading factors, space, frequency, time, etc., all may need to be adapted. With so many dimensions of transmission parameters, the link adaptation algorithms can be rather complicated. For example, developing link adaptation algorithms for the multiple input multiple output (MIMO) system is still a research challenge. Furthermore, link adaptation with so many parameters is generally a cross-layer optimization problem between physical and MAC layers.

2.2 Directional Antennas and Multi-Antenna Systems

To improve physical layer performance in a wireless environment, a common technology is to consider directional communications or use multiple antennas on the same communication node. It should be noted that a multi-antenna communication system consists of both RF components and baseband processing.

2.2.1 Directional Antenna

Directional antennas enable directional transmission and reception in a wireless network, and thus have several advantages.

- *Better spatial reuse efficiency.* Since transmission and reception are directional, channel reuse does not need to rely on spacial separation, which significantly improves channel spatial reuse efficiency. This feature helps to increase network capacity [240].

- *Lower interference.* Directional transmission and reception reduces the collisions and interference among different nodes. This feature improves the QoS and throughput of a network.

- *Less energy consumption for the same network capacity.* For the same transmission range, less transmit power is needed by a directional antenna than an omni-directional antenna. Thus, for the same transmission rate, less interference will produce by a node to other nodes. In other words, this feature not only improves the energy efficiency [239], but also increases the network capacity.

- *Better security.* Due to directional transmission, eavesdropping becomes much more difficult, and thus enhances security of the network at the physical layer.

Directional antennas can be realized in the following methods.

- *Steerable antenna.* In this case, one antenna is used on each node, pointing in a specific direction. For networking with other nodes, the antenna needs to be mechanically or electronically steerable so that the antenna points to the right direction at the right time [141]. Since the process of changing the direction of a steerable antenna may be slower than ad hoc networking needs, it is not always a good choice for WMNs.

- *Antenna switching.* Each node has multiple antennas each pointing in a different direction. If a node wants to communicate with nodes in different directions, the node must switch antennas from one to another. This process can be quick enough to satisfy the need of ad hoc networking. The drawback of this type of directional antenna is lack of flexibility, because the direction and coverage of a directional antenna are always fixed.

- *Beamforming.* Each node has multiple antennas. However, by applying beamforming techniques, the main beam of antennas points in a direction according to the need of higher layer protocols, while nulls are kept at unwanted directions. Via signal processing algorithms, the direction of the main beam can be controlled to the right direction with a fine granularity.

Thus, a directional-antenna communication system can be built based on a single antenna or a multi-antenna system.

Compared to single-hop networking such as wireless LANs or cellular networks, WMNs can potentially get more benefits from directional antennas. The reason is that the multihop and mesh architecture causes a node in WMNs to experience much higher resource competition with other nodes and thus, directional antennas can significantly reduce this kind of conflict in resource sharing. However, due to the mesh architecture, it is more challenging to control directional antennas in WMNs. To fully take advantages of directional antennas, higher layer protocols, in particular MAC and routing protocols, need to be redesigned. To date, many MAC protocols have proposed considering directional antennas in ad hoc networks [62, 149, 197, 285]. However, few MAC protocols have been proposed specifically for WMNs. Moreover, a single-protocol-layer solution may not work well [220].

In WMNs, it is common to have nodes with multiple radios. When these radios work together with directional antennas, network capacity can be further increased. However, new protocols need to be developed to utilize these benefits.

2.2.2 Antenna Diversity and Smart Antenna

Considering communications between nodes A and B in Figure 2.2, node A is assumed to have M antennas for transmission and N antennas for reception, while in node B there are K antennas for transmission and L antennas for reception. Different values of M, N, K, L result in various multiple-antenna systems.

Single Transmitting Antenna Multiple Receiving Antennas

If multiple antennas are in the receiver but single antenna in the transmitter (i.e., $K = 1$, $M = 1$ and either $L > 1$ or $N > 1$), techniques such as antenna diversity and adaptive/smart antennas can be used for a multi-antenna system. They have been proposed for point-to-multipoint one-hop cellular networks.

Antenna diversity is based on the fact that signals received from uncorrelated antennas have independent fading. Thus, it has high probability that at least one good signal can be received at the receiver. Antenna uncorrelation is usually achieved through different types of diversity.

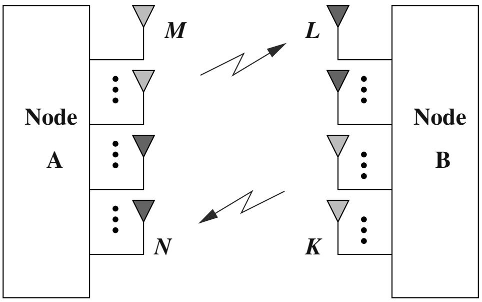

Figure 2.2 Multiple-antenna systems

- *Space diversity.* This is the simplest version of antenna diversity, which is achieved via antenna separation by a certain number of wavelengths. When antennas are at the same location, space diversity will disappear.

- *Polarization diversity.* Since antennas can be at the same location with polarization diversity, it has become a more favorable approach to achieving antenna diversity. However, it is a more complicated technology than space diversity.

- *Pattern diversity.* By adjusting the radiation patterns at different antennas, diversity can be achieved, even if antennas are at the same location. However, pattern diversity also has higher complexity than space diversity.

To utilize diversity, signal processing is needed. The most common techniques are explained as follows [194].

- *Switch diversity.* The antenna with the best signal is selected. The signal quality metrics can be signal strength, BER, etc.

- *Equal gain combining.* To enhance the performance of switch diversity, an equal gain combining technique can be used to co-phase signals and add them together.

- *Maximum ratio combining (MRC).* MRC weights signals by SNRs before combining them. It is the optimum method in the presence of noise.

It should be noted that different signal processing techniques must be employed depending on what type of antenna diversity is used. For example, if polarization or pattern diversity is used, switch diversity may not be effective, and the best choice should be MRC.

When strong interference is present, diversity processing alone is insufficient to receive signals with high quality. To resolve this issue, adaptive antenna array processing or smart antennas are used to shape the antenna beamform in order to enhance the desired signals but nullify the interfering signals. For example, the main antenna beam can be formed to focus on desired signals, and nulls of beam pattern are placed in areas where interference signals arrive.

Adaptive antenna processing usually assumes that part information of the desired signal can be acquired through a training sequence. Then the weights of a space-time receiver is adjusted to minimize the minimum mean square error (MMSE) between the known signals and the received signals. The space-time receiver actually performs the optimum combining of received signals. When no interference exists, it is the same as the MRC technique for antenna diversity. So far, some schemes have been proposed to detect the directions of arrival signals. Based on these directions, the desired signals are combined. These schemes may be useful in theory, but they are not practical in real applications, because there may be too many signal directions for signal arrivals.

The specific approaches of antenna diversity or smart antennas vary a lot for different networks. In a network without training sequence, e.g., IEEE 802.11b or 802.11a/g based wireless networks, it is very difficult to apply smart antenna techniques. In TDMA based networks such as IEEE 802.16 or TDMA cellular networks, optimum combining can be performed based on the training sequence within a time slot. For CDMA networks, since a rake receiver has already provided diversity, the smart antenna will mostly bring performance gain in the sense of reducing co-channel interference (CCI) or multiple access interference (MAI). Moreover, in a CDMA network there are no dominant interferers, and thus it is hard to cancel interfering signals based on the limited degrees of freedom of antenna arrays. As a result, using multiple fixed antenna beams is a much better solution than adaptive antennas. With these fixed antenna beams, no weight calculation or tracking are needed, and thus the multi-antenna system has low complexity.

Antenna diversity and smart antennas are widely accepted in WMNs, since many mesh routers are equipped with these technologies. However, their performance in WMNs needs more evaluation. The first issue is their complexity in a multihop mesh topology. Owing to its complexity and cost, a fully adaptive smart antenna system is only used in base stations of cellular networks, and on-going research and development efforts are still needed to implement fully adaptive smart antenna system in a mobile terminal. In WMNs, this problem becomes worse due to the much more complicated network topology. The second issue is how to keep these techniques effective, or make them more effective, when the traditional point-to-multipoint communications do not exist anymore. Examples of analyzing smart antenna systems for mobile ad hoc networks (MANETs) are reported in [33, 219]. However, other than such preliminary results for MANETs, no work has been done for the scenario of WMNs.

Multiple Transmitting Antennas Single Receiving Antenna

If multiple antennas are in the transmitter and single antenna in the receiver, i.e. $N = 1$, $L = 1$ and either $K > 1$ or $M > 1$, either antenna diversity or smart antenna techniques are difficult to implement. Since the receiver has only one antenna, the transmitter antennas must be designed appropriately so that the arrival signals at the receiver can still keep the performance gain of antenna diversity or smart antenna. To reach this goal, one important requirement is that the channel state information (CSI) must be available at the transmitter. For example, schemes such as [61] assume that CSI is perfectly known.

However, usually only partial information of channel state is available. For a time division duplex (TDD) system, such information can be derived from a reverse link, but is still not accurate to reflect forward link CSI, due to channel variations in time. For a frequency division duplex (FDD) system, CSI of forward and reverse links is independent.

Thus, in a multi-antenna system with multiple antennas at transmitter and single antenna at receiver, antenna diversity or smart antenna must be designed without relying on CSI. This approach may be doable, but its performance is limited.

To achieve diversity under this situation, a commonly used technique is space-time coding (STC) [14]. This scheme actually aims to get the performance gain at the receiver instead of the transmitter. However, to help the receiver to benefit from received signal, the transmitter must apply a coding scheme such that signals on antennas are processed differently in different symbol periods. When the receiver gets such coded signals, it can combine them through an appropriate algorithm such as Maximum Likelihood Detection (MLD). A simple STC scheme discovered by Alamouti [14] is explained as follows. In this scheme, there are two transmitting antennas and one receiving antenna. At symbol period n, the signals at the two antennas are S_1 and S_2, respectively. In the next symbol period $n + 1$, the signals simultaneously transmitted at the two antennas become S_1^* and S_2^*, respectively, where $*$ denotes the complex conjugate operation. When these signals arrive at the receiver, they can be combined and detected via schemes such as MLD. The STC in this example achieves the same diversity gain as MRC with two receiving antennas and one transmitting antenna. However, its drawback is that each antenna loses 3 dB power if the total transmit power is fixed. Nevertheless, STC is a promising technique that achieves second order diversity without bandwidth expansion [194].

To date, it is still very difficult to apply the smart antenna technique to a multi-antenna system with multiple antennas at transmitter and single antenna at receiver. No effective schemes have been proposed yet.

MIMO

If multiple antennas are used at both the transmitter and the receiver, i.e., $M > 1$, $L > 1$ or $K > 1$, $N > 1$, the multiple-antenna system is a MIMO system. Since a MIMO can utilize both diversity and multiplexing of simultaneous data streams, it can potentially increase the system capacity by three times or even more [182]. Currently MIMO has been adopted into IEEE 802.11n [120].

MIMO systems can be built based on spatially separated antennas. For some applications, compact antennas are needed, and thus MIMO systems must be designed based on vector antennas [151]. These vector antennas are built based on co-located elements, e.g., one loop and two dipoles. In fact, vector antennas are examples of pattern diversity. MIMO based on co-located antennas can also increase the capacity by several times. However, its capacity and BER performance is still lower than MIMO systems with spatially separated antennas.

Depending on where MIMO signal processing is performed, a MIMO system can be classified into three types: *receiver processing only*, *transmitter processing only*, and *both transmitter and receiver processing* MIMO systems.

- *Transmitter processing only MIMO.* In this type of MIMO system, the receiver does not need MIMO signal processing but multiple front ends. Thus, the antennas at the receiver are connected to multiple independent front ends with separate data streams. These data streams are then multiplexed into one data stream, providing a much higher data rate than a single antenna system. Since no MIMO processing is needed at the receiver, the transmitter must have an algorithm to perform MIMO processing so that the desired signals have enough Signal-to-Interference-Noise Ratio (SINR). The existing algorithms include the transmit zero forcing *scheme*, transmit MMSE, and the filter bank *scheme*. In the transmit zero-forcing scheme, the transmitter employs an interference pre-eliminating process before signals are sent in different antennas. Thus, when these signals are received at the receiver, their SINR is high enough to be detected. The filter bank scheme tries to maximize the minimum SINR of a subchannel among all subchannels. Transmitting the MMSE optimizes the transmitter weights such that the mean square error between the transmitted symbols and the estimated symbols is minimized. It should be noted that, without MIMO processing at the receiver, no existing algorithm can provide receiver diversity, although multiple receiving antennas are available.

- *Receiver processing only MIMO*. The transmitter is simple in this scenario, where each transmitter for each antenna can be just an ordinary transmitter. Before being transmitted, a single data stream is demultiplexed into multiple substreams that will be modulated and transmitted at different transmitters. It should be noted that the symbols for each transmitter must be drawn from the constellation in a special way, such that total radiated power from all transmitters is constant. When signals from different antennas arrive at the receiver, MIMO signal processing must be performed. So far there are three schemes that can be used: *space-time coding*, *vertical Bell Lab Layered Space-Time* (*V-BLAST*) [93], and *maximum likelihood detection* (*MLD*) [292].

  – *Space-time coding*. In this scheme, the data stream is encoded across all transmitting antennas via a certain coding algorithm, which is a relatively simple process. However, at the receiver, in order to decode the received signals, complicated decoding schemes are needed. Thus, most of the MIMO processing complexity lies in the receiver. When the number of antennas is only 2, simple decoding algorithm such as the Alamouti [19] scheme can be used. However, in general, no simple and effective decoding algorithms are available so far. Thus, it is necessary to develop space-time codes that have low decoding complexity but still achieve satisfactory performance.

  – *V-BLAST*. Only conventional receivers are needed in V-BLAST. Thus, its key task is to remove interference experienced by a specific data substream from other data substreams. V-BLAST simply achieves this via an iterative optimum combining and interference cancellation scheme. First, optimum combining is performed on all received data substreams. When the best substream is found, its signal is canceled from the signals of all other substreams. In the next step, the optimum combining is performed on the remaining substreams to find the best substream. This process is repeated until all substreams are retrieved and output for detection.

  – *MLD*. MLD for MIMO is actually an optimum receiver that detects multiple data streams simultaneously. It has higher complexity than V-BLAST. However, when the same numbers of receiving antennas and transmitting antennas are considered, MLD for MIMO can always achieve better performance – e.g., BER – than V-BLAST can. Moreover, when the number of antennas is small, it is practical to implement MLD in a realistic system. As a result, when the number of antennas is small (e.g., <3), MLD is advantageous over V-BLAST.

- *Both transmitter and receiver MIMO processing.* Since both transmitter and receiver MIMO processing is applied, it is reasonable to expect that such MIMO systems will be able to provide much better performance than the previous two MIMO systems. However, it is also true that these MIMO systems are very complicated. For mobile terminals or mesh clients, they are not an appropriate choice. So far, the most popular scheme to perform both transmitter and receiver MIMO processing is singular value decomposition (SVD) [20]. It diagonalizes the MIMO channels to form independent channels, and then water filling schemes can be applied to these channels to maximize the overall system capacity.

The above MIMO systems are favored by different application scenarios due to different complexity requirements on transmitter and receiver. In a cellular network, transmitter-processing-only MIMO systems are preferred in the downlink, while receiver-processing-only MIMO is a favored in the uplink, because we want to leave the most complicated processing to base stations rather than mobile terminals. In a mobile ad hoc network, we do not have such a choice, because all nodes are equipped with similar processing capability. However, in WMNs the situation is better than that in either cellular networks and mobile ad hoc networks. For communications between mesh routers, all types of MIMO systems can be applied, thanks to the high processing capability of mesh routers. For communications between mesh routers and mesh clients, we can apply transmitter-processing-only MIMO at links from mesh routers to mesh clients, and receiver-processing-only MIMO at links from mesh clients to mesh routers. This illustrates the advantage of WMNs over other wireless networks. However, it is necessary to figure out a scheme to let mesh routers and mesh clients run different MIMO schemes in the same network. This looks straightforward for mesh clients, but for mesh routers it is rather complicated, because a mesh router needs to support communications with both mesh clients and other mesh routers. Suppose that different radios are used for mesh backbone communications and mesh client communications, and each radio is equipped with a separate MIMO system, the problem is simpler. When only single radio is available at mesh routers, novel MIMO systems need to be designed such that: a) the downlink to mesh clients is transmitter-processing-only MIMO; b) the uplink from mesh clients is receiver-processing-only MIMO; and c) uplink and downlink between mesh routers can be any type of MIMO system.

MIMO has been researched for many years, and there are some chipsets available on the market. To further improve transmission rate and reliability, developing new MIMO schemes is an ever-increasing demand. Moreover, new algorithms are also needed to improve performance of existing MIMO technologies, e.g., lower signal processing complexity and less dependence on channel state information.

2.3 Cooperative Diversity and Cooperative Communications

In many application scenarios, multi-antenna systems are not applicable due to unavailability of multiple antennas. There are several reasons for using only a single antenna in a network node.

- *Cost and size of a node.* In some networking devices such as handsets, cost and size must be kept small [202]. If multi-antenna systems are adopted, it is hard to reach this goal.

- *Not enough separation on the same node.* To have an effective multi-antenna system, antennas on the same node must be separated by a distance of more than half a wavelength [171]. If a frequency of 5.0 GHz, as used in IEEE 802.11a, is considered, several centimeters are needed for separation. If a frequency of IEEE 802.11g is considered, the separation distance is much larger. Such a requirement cannot be easily satisfied in a mobile terminal, mesh client, or even a mesh router.

In order to explore the diversity gain in wireless networks without multi-antenna systems, user cooperative diversity has been proposed [160, 231, 232].

The basic concept of user cooperative diversity is simple: when Node A sends a signal to Node B, another node, e.g., Node C that overhears this signal also gets this signal and relays it to node B; as a result, the signal received at Node B is the sum of signals from two different but independent fading paths, i.e., spatial diversity has been achieved via the cooperative communications among different nodes. Thus, in order to achieve diversity by network nodes with single antenna, each node must play two roles: transmit data and work as a cooperative agent to relay data for other nodes.

From this basic concept of getting user cooperative diversity, we can see several challenging problems in this mechanism.

- *Tradeoff of power.* Since one signal needs to be sent to at least two different nodes, more power is needed to send data from source to destination. On the other hand, with diversity, the transmit power at each node can be smaller than in the noncooperative mode. Thus, it is necessary to develop a power allocation algorithm such that minimum transmit power is used to maintain the user cooperative diversity.

- *Tradeoff of transmission rate.* In cooperative communication, a node needs to relay other nodes' data and also transmit its own data. Thus, its transmission rate is reduced. However, due to diversity, channel coding rates can be higher, which increases the transmission rate. Thus, the actual transmission rate may not be reduced. In order to keep the transmission rate as high as possible, we need to consider tradeoff between diversity and reduced chance of transmission.

- *Interference.* With cooperative diversity, interference may also be increased, because the same signal is sent more than once in the network. However, diversity may reduce the transmit power level, which can compensate for the increased interference.

- *Cooperation assignment scheme.* This is concerned with finding other cooperative nodes for each node so that diversity can be achieved. In a one-hop infrastructure based network, cooperation assignment may be just a simple task. However, in a multihop distributed network such as WMNs, cooperation assignment is rather complicated, because it has to take into account many factors such as diversity gain, power, interference, and even fairness among nodes.

- *New requirements on network nodes.* Although diversity can be achieved through cooperative communications, algorithms are still needed to retrieve original data from multiplexed signals. This requires additional processing power on either transmitter or receiver. The functionality of cooperative communications may also need change of hardware in each node.

Therefore, in order to have user cooperative diversity, three algorithms are needed. The first algorithm aims at optimal assignment of cooperative nodes to each node such that the best tradeoff between diversity and power, transmission, and interference is achieved. Given an optimal assignment algorithm, the second algorithm gives a method of how to relay signals in cooperative nodes. The third algorithm focuses on detecting original data from the multiplexed data of originally transmitted signals and relayed signals.

So far, several schemes have been proposed for relaying signals in cooperative nodes [160, 202].

- *Amplify and forward scheme.* In this scheme [159], the partner node amplifies the received signal together with noise and forwards the amplified signal. The drawback of this scheme is that amplifying and forwarding analog signals is a nontrivial requirement for hardware. The advantage of this scheme is that no inter-user channel state information is needed, and conventional channel estimation can be used.

- *Decode and forward scheme.* In this scheme, a node decodes the signal and then retransmits it. An example of this scheme is presented in [231]. The drawback of this scheme is that a node may not be able to correctly detect its partner's signal. In this case, relaying signals will propagate errors. Another drawback of this scheme is that inter-user channel information is needed at the receiver.

- *Coded cooperation.* Each node's data stream is encoded via a channel coding scheme into blocks [110]. The codeword is partitioned into two segments with N_1 and N_2 bits, respectively. When a node transmits data, it first sends N_1 bits in the codeword, and also decodes data from its partner node. If decoding is successful, the node will calculate the second segment of its partner node and then transmits the N_2 bits. Otherwise, it will transmit its own second segment. This scheme does not need inter-user channel information. However, since cooperation is conditional, the receiver needs to know whether transmit nodes have cooperated or not. Other coded cooperation schemes are also discussed in [241].

- *Selection relay.* In order to avoid error propagation, a threshold test must be performed before relaying signals. When it is satisfied, the relay is done. Otherwise, a node needs to enter noncooperative mode. In this sense, coded cooperation is also a type of selection relay scheme.

Several schemes have proposed to detect original signals from multiplexed signals. The simplest scheme is to let relayed signals and original signals arrive at different time intervals. However, such a TDMA scheme may not be efficient, and also has difficulty in time slot allocation. We can also use CDMA to multiplex relayed and original signals. In addition, frequency division multiple access is possible. Whatever multiple access scheme is used, algorithms need to be developed to detect original signals with as good performance as possible.

To date, user cooperative communications have been proved effective in wireless networks. However, the research is still in its preliminary stage, for three reasons. First, most of the existing schemes have only considered the problem of how to effectively forward data by cooperative nodes. How to assign cooperative nodes so as to optimize power, transmission rate, and interference requires new algorithms. Second, no practical solution has been proposed yet. For example, most existing algorithms assume central control is available, simple network topology has been considered, and only simple multiple access is considered in these algorithms. Such constraints render the existing algorithms unsuitable for WMNs. Third, many existing schemes rely on the knowledge of inter-user channel station information, which may not be available. New algorithms that do not or only partially rely on such information need to be developed. Nevertheless, user cooperative diversity is a promising technology, because: a) it potentially enables low-cost network nodes to have antenna diversity and thus increase overall network capacity; b) it can work together with multi-antenna systems to further increase network performance [242]; c) it can help to resolve collision without using reservation based MAC protocol [171] or collision avoidance procedures.

2.4 Multichannel Systems

In WMNs, multiple channels are usually available in the frequency band of a wireless radio. For example, if WMNs are based on IEEE 802.11g, more than three nonoverlapping channels are available. If IEEE 802.11a is considered, this number is larger. When multiple channels are used for simultaneous communication, the network capacity and performance can be significantly increased. A multichannel system can be built in different ways.

- *Single transceiver on single radio.* In this case, a wireless radio is able to work on different channels, but can only work on one channel at a time. Thus, the radio must switch channels on the time axis according to the needs of higher layer protocols such as MAC or routing schemes. A multichannel system based on such radios has low cost, but can still significantly reduce interference and thus increases capacity. The challenges are twofold. First, channel switching speed needs to be fast; otherwise, the overhead due to channel switching is too high. Second, the MAC protocol needs to determine the best time for channel switching and the best channel that can be switched into.

- *Multiple transceivers on single radio.* For a multiple transceiver radio, simultaneous transmissions in different channels can be supported. Multiple transceiver has been implemented in a base station of cellular networks. However, with the concerns of cost and system complexity, a wireless radio with multiple transceivers has not become a mature technique yet for WMNs. Although IEEE 802.11 chipsets with multiple transceivers are already available, their cost is still very high. Since multiple transceivers are on the same radio, the network can potentially have higher capacity than a network with only single transceiver radios. However, due to multiple transceivers, channel allocation algorithms in the MAC or routing protocol need to determine multiple channels at a time. Although channel switching is not always required, it is still necessary because the needed channels for a node may change for the purpose of reducing overall interference in the network. As a result, in many cases, fast channel switching speed is desired. In some simple application scenarios such as a home network, if a radio can have three transceivers, it can satisfy multichannel communications without channel switching.

- *Multiple radios each with single transceiver.* When radio with multiple transceivers is not available but a node needs simultaneous transmissions, we can build the node with multiple radios. Since each radio contains both MAC and physical layers, it is not necessary to develop another MAC protocol for a node. However, schemes, which are called virtual MAC residing in-between MAC and routing layers, are needed to coordinate communications in all radios and among all nodes [4]. In this type of multichannel network, each radio can use fixed channels that are determined in advance, and thus, no channel switching is needed. However, in order to best utilize each radio in an arbitrary network topology, the channel on a radio may change. Thus, channel switching is still needed in this case. More importantly, we need an additional algorithm at the virtual MAC layer to dynamically determine the channels for all radios on each network node.

- *Multiple radios each with multiple transceivers.* This case represents a multichannel system with highest degrees of freedom for channel allocation on a network node. Thus, both cost and network capacity can be highest too.

It is also possible that all the above four types of node or several types of them, coexist in the same WMN. To adapt to this generic case, the MAC protocol and even the routing protocol need to be flexible enough to adapt to all scenarios. For example, the algorithms that assume fixed channel on a node are not applicable.

In a multichannel WMN, other physical layer technologies can be adopted too. For example, each radio can be a multi-antenna system, and link adaptation can be applied too. However, we should realize that the algorithms or protocols to utilize these technologies in a multichannel WMN need to be modified or enhanced. For example, adaptive rate control in a multichannel WMN must determine rates for different channels instead of one channel. In the case of user cooperative communications, the existing schemes may not work anymore, because they have not considered how to achieve user diversity when different channels are used on different paths to the destination.

2.5 Advanced Radio Technologies

Advanced radio technologies including reconfigurable radios, cognitive radios, and software radios, bring many advantages to the research and development of WMNs. For example, in some cases, with reconfigurable radios or software radios, the development cycle of a new protocol can be much shorter. Protocols can also be directly built over reconfigurable radios for a realistic product without need of changing the design of chipsets. In addition, networking protocols can also reconfigure wireless radios in order to achieve optimum performance. In other cases, radios need to be dynamically changed for the purpose of realizing radios such as frequency agile radios or cognitive radios. Thus, building WMNs with advanced radio technologies is indispensable.

2.5.1 Frequency Agile Radios and Cognitive Radios

For a wireless network, frequency bandwidth is a very precious resource. However, many of existing allocated frequency bands (both licensed and unlicensed) have not been utilized efficiently. Measurements by the FCC show that around 70% of the allocated spectrum is not utilized [79, 158]. In addition, the timescale of spectrum occupancy can vary from milliseconds to hours [79]. Therefore, abundant spectrum is still available for wireless communication. Furthermore, in a large scale ad hoc network, the complexity is beyond human planning, and thus, conventional static frequency planning becomes impossible [185]. To achieve much better spectrum utilization and viable frequency planning, frequency agile [188] or cognitive radios [158] are being developed to dynamically capture the unoccupied spectrum. The FCC has recognized the promising future of this technique and pushes to enable it to a full realization.

2.5.2 Reconfigurable Radios and Software Radios

Reconfigurable radios have existed for many years. Currently many wireless radios are more or less capable of being reconfigured. For example, some commercially available IEEE 802.11 radios can be reprogrammed by changing the configurations of the registers for MAC and physical layers. By reconfiguring these registers, the radios can work in a certain style as needed by higher layer protocols. The ultimate goal of reconfigurable radio is software radio, in which programmability exists in all components of a radio such as programmable RF bands, channel access modes, and channel modulations [191].

Software radio is not a mature technique yet, although testbeds are available now [272]. However, for the long term, software radios will be a key technique for wireless communications. They can be one of the most convenient platforms for cognitive radios [80]. Software radios reduce the difficulty of implementing advanced physical techniques such as adaptive modulation and coding, MIMO system [272], controllers for smart and directional antennas, multichannel radios, and so on. They also provide reconfigurability to MAC and even higher layer protocols, so that these protocols can be better designed together with physical layer. Frequency agile or cognitive radios can also be built based on software radios.

2.6 Integrating Different Advanced Techniques: IEEE 802.11n

The advanced physical layer techniques explained in previous sections have been applied to real systems such as IEEE 802.11, 802.15, and 802.16 wireless networks. In this section, the high throughput (HT) physical layer of 802.11, i.e., IEEE 802.11n, is presented to show how different advanced techniques are integrated in the same physical layer of 802.11. More specifically, the advanced functions of adaptive modulation and coding, MIMO, and multichannel operations are explained together with OFDM. Techniques of cooperative communications are not covered in this example, as 802.11n does not include this feature for two reasons: 1) 802.11n is focused on one-hop communications; 2) while 802.11n is being specified, the techniques of cooperative communications have not been mature yet for practical use.

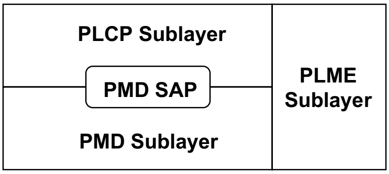

Figure 2.3 Protocol reference model of IEEE 802.11n physical layer

2.6.1 Protocol Reference Model of the Physical Layer

The protocol architecture of the 802.11n physical layer follows a generic model as shown in Figure 2.3.

The physical layer consists of two sublayers in the data plane: the upper sublayer is the physical layer convergence procedure (PLCP), and the lower one is the physical medium dependent (PMD) sublayer. These sublayers are managed by the physical layer management entity (PLME) in the management plane.

2.6.2 PLCP Sublayer

The PLCP sublayer allows the MAC layer to have minimum dependence on the PMD sublayer. Its major functionality is to convert the physical layer service data unit (PSDU) into a PLCP protocol data unit (PPDU) or vice versa. Most 802.11n physical layer functions are embedded in this process.

Different PPDU Frame Formats and PLCP Preambles

In the PLCP layer there are three types of PPDU frame formats, indicating three modes that can be supported in an IEEE 802.11 device.

- Nonhigh-throughput (Non-HT) format: This is needed to support backward compatibility with other 802.11 devices that do not have IEEE 802.11n functionalities.
- High-throughput (HT) greenfield format: When a PPDU follows this format, communications can only be carried out among pure IEEE 802.11n devices.
- HT mixed format: When an IEEE 802.11 device employs such a PPDU format, it can communicate with another IEEE 802.11 device with or without the IEEE 802.11n capability.

Selection of different PPDU formats is controlled by the parameters specified in the MAC/Physical (PHY) service access point (SAP).

As the physical layer of 802.11n is built on top of OFDM, different formats of a PPDU frame indicates a different design of OFDM preamble. As shown in Figure 2.4, the non-HT PPDU preamble consists of three fields: non-HT short training field (L-STF), non-HT long training field (L-LTF), and non-HT signal (L-SIG) field. These fields are exactly the same as that in a PPDU generated in a non-802.11n node. In a L-STF, there exist 10 short training symbols each having a length of 0.8 μs. Between L-LTF and L-STF, there is a guard interval

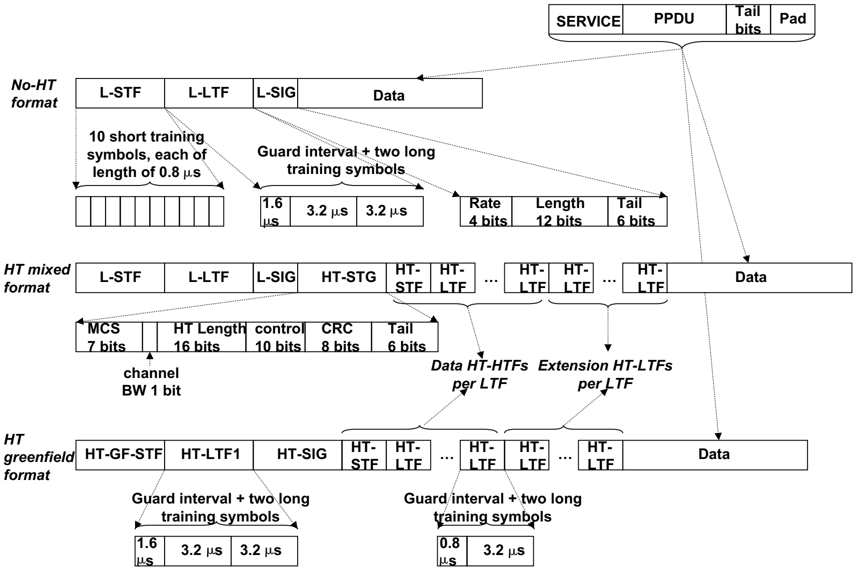

Figure 2.4 Preambles in PPDUs with different frame formats

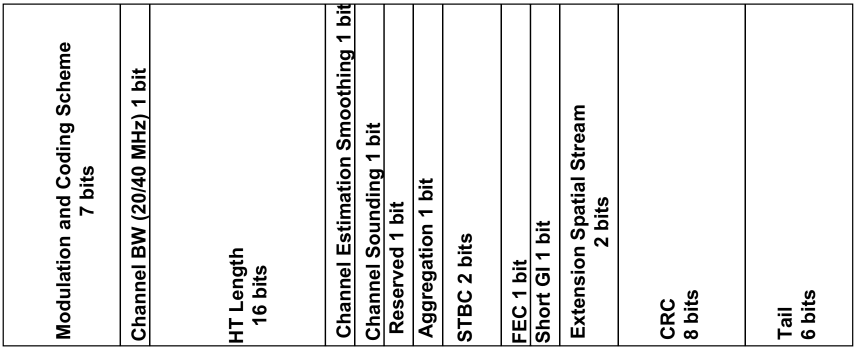
Modulation and Coding Scheme 7 bits
Channel BW (20/40 MHz) 1 bit
HT Length 16 bits
Channel Estimation Smoothing 1 bit
Channel Sounding 1 bit
Reserved 1 bit
Aggregation 1 bit
STBC 2 bits
FEC 1 bit
Short GI 1 bit
Extension Spatial Stream 2 bits
CRC 8 bits
Tail 6 bits

Figure 2.5 The different fields of HT-SIG

of 1.6 µs, which is followed by two long training symbols, each having a length of 3.2 µs, in the L-STF. For the HT greenfield format, the preamble consists of three fields.

- HT greenfield short training field (HT-GF-STF): This aims for automatic gain control (AGC) convergence, timing acquisition, and coarse frequency acquisition.
- HT signal field (HT-SIG): It contains all the information needed for interpreting the HT packet format. Its details can be found in Figure 2.5. An HT-SIG consists of six bytes; except for one bit being reserved, all other bits are for indication or control of

802.11n physical layer functions. It starts with the seven-bit *modulation and coding scheme (MCS)* field, followed by one bit for indicating/selecting channel bandwidth between 20 MHz and 40 MHz. The next field is the *HT-length* indicating the length of an HT PPDU. The one-bit *smoothing* field is to control whether channel estimation smoothing is needed, the *channel sounding* field indicates whether a PPDU performs channel sounding, and the *aggregation* field indicates whether the PPDU contains an aggregated MPDU. The two-bit *space-time block coding (STBC)* field indicates the difference between the number of space-time streams and the number of spatial streams, which is an important parameter for STBC. The *STBC* field is followed by several other fields: the *forward error correction (FEC) coding* field indicates whether binary convolutional code (BCC) or low-density parity check (LDPC) coding is used, *short GI* is to indicate that the short guard interval is used after the HT training symbols, and the field for *extension spatial streams* contains the information as to how many extension spatial streams are needed. The last two fields of HT-SIG are *Cyclic Redundancy Check* (*CRC*) and *tail.*

- HT long training field (HT-LTF): This provides a way of channel estimation. There may be multiple HT-LTFs categorized into two classes: the data HT-LTFs for demodulation of the HT data portion, and the optional HT-LTFs for sounding extra spatial dimensions of the MIMO channel. It should be noted that the first LTF, i.e., HT-LTF1, has the same structure as that of L-LTF. However, all other HT-LTFs are only a half of L-LTF, i.e., each of such HT-LTFs consists of a guard interval of 0.8 μs and one long training symbol of 3.2 μs.

For the HT mixed format, the first three fields are designed for compatibility with non-HT operation. As in the greenfield format, the HT-SIG and HT-LTFs are also contained in the HT mixed format. In addition, following HT-SIG is the HT-STF field, which has similar functionalities to HT-GF-STF and LT-SIF, but is shorter in length.

Function Blocks of Transmitter

In a different portion of PPDUs, the transmitter in the IEEE 802.11n physical layer requires two different sets of function blocks. Such differences ensure compatibility with non-HT devices. More specifically, in a non-HT PPDU or non-HT portion of an HT mixed PPDU, no space-time processing is needed, as shown in Figure 2.6. For the HT signal field in an HT mixed PPDU, space-time processing is not used either, so that a non-HT device knows whether or not the remaining portion of the PPDU is for HT transmission. In the HT portions of an HT mixed PPDU and in the entire HT greenfield PPDU, the transmitter includes all the functions needed for MIMO operation, as depicted in Figure 2.7.

For HT transmission, each function block is explained as follows.

- Scrambler: When bit streams go through this function block, the probability of having long sequences of zeros or ones is significantly reduced. The scrambler ensures proper operation in certain functions, e.g., timing recovery unit, in a receiver's circuit, and also eliminates the dependence of the power spectrum on the actual transmitted data.

- Encoder parser: This is needed only when the number of FEC encoders is more than 1. It splits the scrambled bits among several FEC encoders in a round-robin fashion.

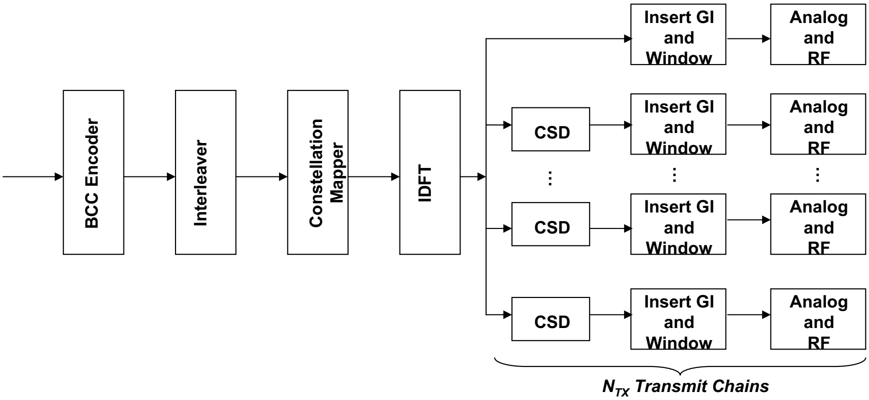

Figure 2.6 Block diagram for non-HT transmission

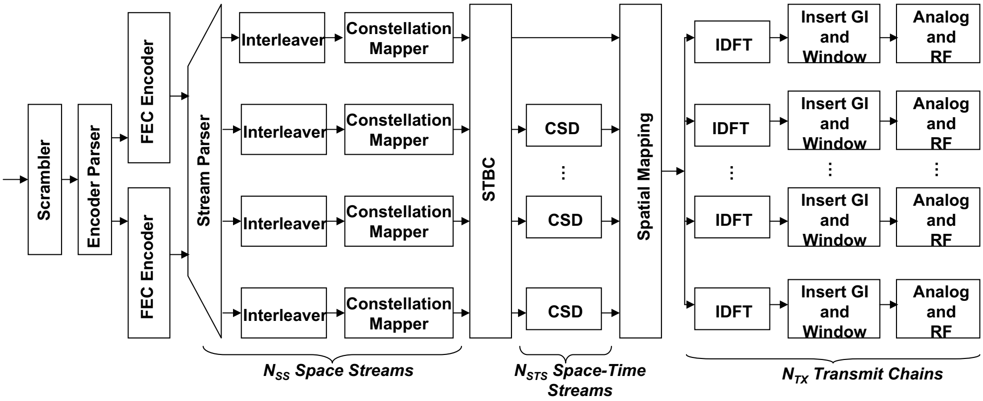

Figure 2.7 Block diagram for HT transmission

- FEC encoder: The bit stream is encoded for error correction. It is possible to have multiple FEC encoders using binary convolutional coding (BCC) or low density parity check (LDPC).

- Stream parser: This gets the bit streams from the FEC encoders and divides them into several spatial streams for parallel processing such as interleaving and constellation mapping.

- Interleaver: For BCC, the interleaver is applied to change the order of the bits in order to avoid adjacent noisy bits. For LDPC, the interleaving operation is not required.

- Constellation mapper: This maps bits in each spatial stream into constellation points that are actually complex numbers.

- Space-time block coding (STBC): This function block is optional. When it exists, the number of spatial streams must be smaller than the number of space-time streams.
- Spatial mapper: This maps space-time streams into transmit chains. When direct mapping is applied, the number of space-time streams is the same as the number of transmit chains. If spatial expansion is used, the number of space-time streams is larger than the number of transmit chains, which can be done by applying matrix multiplication to the space-time streams. If the matrix consists of steering vectors for antenna beams, then beamforming can be achieved.
- Inverse discrete Fourier transform (IDFT): This function converts a block of constellation points into a time domain block. It is a key component of OFDM.
- Inserting guard interval (GI) and windowing: GI or cyclic prefix is inserted by prepending a circular extension of a symbol to itself. Windowing smooths the edges of a symbol in order to increase spectral decay.
- Cyclic shift diversity (CSD) insertion: This function avoids unintentional beamforming. CSD can be done before IDFT, after IDFT, or inside the spatial mapper.
- Analog processing and RF front end: The encoded PPDUs are converted into analog signals and further into RF signals.

As compared with an HT transmitter, a non-HT transmitter is much simpler. Basically, it does not have MIMO-related function blocks such as parallel processing for spatial streams, STBC, and spatial mapping. In order to support transmissions on multiple antennas, both the HT transmitter and the non-HT transmitter contain multiple transmit chains.

PPDU Encoding Process and Formation of OFDM Symbols

Given a PPDU, the PLCP preamble and data fields are prepared separately.

Preamble Field In the first step of encoding PLCP preamble, the MAC/PHY SAP parameters are used to determine its PLCP format. With the format selected, an appropriate transmitting process (i.e., the mechanism for HT transmission or non-HT) is applied to construct the PLCP preamble. For example, a greenfield PLCP preamble must be transmitted according to the function blocks shown in Figure 2.7. In a mixed PLCP preamble, the HT portions, except for HT-SIG, also follow the same transmitting process. However, for either a non-HT PLCP preamble or the non-HT portions and HT-SIG in the mixed PLCP preamble, it is necessary to apply the transmitting process in Figure 2.6.

When a non-HT transmitting block is used, the OFDM symbols for different fields of the PLCP preamble are the same as those for 802.11a/g. These OFDM symbols are formed according to the specific design of L-STF, L-LTF, L-SIG, and HT-SIG. For example, in the L-STF there are 10 short training symbols, each consisting of 12 subcarriers, and the L-LTF has two long training symbols, each consisting of 53 subcarriers. Compared to a non-MIMO system like 802.11a, the non-HT transmitting block for 802.11n needs to consider multiple transmit chains after OFDM symbols are formed at the output of IDFT. Thus, the same copy of OFDM symbols needs to be sent to different transmit chains, but each can have different CSD or guard interval.

When an HT transmitting block is used to form OFDM symbols for the PLCP HT portions, each OFDM symbol needs to be formed for each transmit chain. Firstly, the specific structure of HT-STF or HT-LTF is considered, to generate the bit streams of each field of HT-STF or HT-LTF. Secondly, these bit streams are mapped onto multiple spatial streams according to STF or LTF mapping matrix. By the end of this step, the HT portions of the PLCP preamble are mapped to multiple spatial streams. Then CSD, spatial mapping, and IDFT are applied in sequence to finally form OFDM symbols at each transmit chain.

Data Field The data field follows the PLCP preamble and consists of the service field for scrambler initialization and a PLCP service data unit (PSDU). How to form OFDM symbols for the data field depends on many parameters, among which the most critical are the number of spatial streams (N_{SS}), the number of transmit chains (N_{TX}), selection of HT or non-HT transmission, MCS, and channel bandwidth.

MCS and channel bandwidth determine the number of data bits in each OFDM symbol, coding rate, the number of coded bits in each OFDM subcarrier (N_{BPSC}), where *BPSC* represents bits per subcarrier, and the number of coded bits in each OFDM symbol (N_{CBPS}), where *CBPS* represents bits per symbol. Depending on such information, the data bits on each spatial stream are encoded. The coded bits are then divided into groups of N_{CBPSS} bits, where N_{CBPSS} denotes the number of coded bits per symbol per spatial-stream (CBPSS). Each group of coded bits is interleaved and then further divided into groups of N_{BPSCS} bits, where *BPSCS* represents bits per subcarrier per stream, i.e., the number of coded bits in each OFDM subcarrier per spatial-stream. Such groups of coded bits of a single subcarrier are then fed into to the constellation mapper to perform a certain modulation. After this step, the coded bits of each subcarrier is converted into a complex number. In other words, in each spatial stream, coded bits are converted into a sequence of complex numbers.

How such complex numbers are filled into subcarriers and form an OFDM symbol depends on another parameter, the number of data subcarriers N_{SD} in each OFDM symbol. N_{SD}, where *SD* represents data subcarriers, is derived from channel bandwidth and channel offset parameters specified in MAC/PHY SAP. As a result, the sequence of complex numbers after the constellation mapper is then divided into groups of N_{SD} complex numbers indexed from 0 to N_{SD}, where N_i corresponds to the ith data subcarrier.

In all the N_{SS} spatial streams, after complex numbers are indexed to subcarriers, STBC and spatial mapping are then applied accordingly for each subcarrier. Cyclic shift diversity may be applied too. After spatial mapping, the data streams become N_{TX} streams of complex numbers, where *TX* represents transmit. If an upper or lower 20 MHz channel is used in 40 MHz, certain groups of complex numbers need to be moved and then associated with other subcarriers. For example, if an upper channel is considered, the complex numbers associated with subcarriers -28 to $+28$ in each transmit chain need to be moved and reassociated with subcarriers 4 to 60. Considering 64 subcarriers in total within the 20 MHz bandwidth, the subcarrier frequency spacing is 312.5 kHz. Thus, such a move of subcarriers is equivalent to shifting the center frequency upper range for 32×312.5 kHz, i.e., 10 MHz.

In each transmit chain, each group of N_{SD} data subcarriers along with pilot subcarriers is converted into time domain using IDFT. A circular extension of the Fourier-transformed waveform is then prepended to itself as a cyclic prefix to form GI. Time domain windowing is necessary to truncate the waveform to a single OFDM symbol. After this step, we can see that a sequence of OFDM symbols is generated one after another in each transmit chain, with the PLCP preamble starting first.

RF Signals Once the complex baseband waveforms corresponding to the OFDM symbols of both the preamble field and the data field are generated, they are up-converted to RF signals according to the specified center frequency. After this step, a PPDU is completely encoded and then sent out.

Modulation and Coding Scheme

In 802.11n, rate adaptation can be performed by dynamically adjusting the MCS. In other 802.11 networks such as 802.11a or 802.11g, rate adaptation is controlled by selecting different modulation and coding schemes. For 802.11n, modulation and coding schemes need to be associated with other parameters.

- Channel bandwidth: Whether the channel is 20 MHz or 40 MHz determines the number of subcarriers in each OFDM symbol.
- The number of spatial streams: Considering two different MCSs, the number of spatial streams can be different.
- The number of pilot subcarriers: Such subcarriers are needed for channel measurement and synchronization. A different number of pilot subcarriers also means a different number of data subcarriers.
- The GI used between OFDM symbols: In 802.11n, there are two options for GI: 400 ns for short GI and 800 ns for normal GI.
- The number of spatial streams.
- Unequal modulation: On different spatial streams, modulation schemes can be different. Unequal modulation is usually used when STBC or transmit beamforming is applied.
- The number of BCC encoders: The number of BCC encoders also impacts the transmission rate. In the current draft of the 802.11n standard, this number is always 1.

With the above parameters, different transmission rates in the physical layer can result, and each rate is represented by an MCS index. For a 20 MHz channel, the transmission rate is indexed from 0 to 31 using equal modulation and then from 33 to 76 using unequal modulation. MCS 32 does not exist for the 20 MHz channel. For 40 MHz channel bandwidth, there are 77 MCS indexes: from 0 to 31, equal modulation is used, while unequal modulation is applied for MCS indexes from 33 to 76. MCS 32 is defined in the 40 MHz channel to achieve the lowest transmission rate by using one spatial stream, a small number of subcarriers, and a low coding rate. A detailed list of these MCS indexes and their corresponding parameters and transmission rates can be found in the IEEE 802.11n standard. An example of MCS indexes using unequal modulation in two spatial streams is shown in Table 2.2, where channel bandwidth is 40 MHz, the number of pilot subcarrier is four, and there are 52 data subcarriers.

Table 2.2 An example of physical layer parameters and the corresponding rates for different MCS indexes

MCS index	Modulation stream 1	Modulation stream 2	Coding rate	Bits per subcarrier	Rate (Mbps) (normal GI)	Rate (Mbps) (short GI)
33	16 QAM	QPSK	1/2	6	39	43.3
34	64 QAM	QPSK	1/2	8	52	57.8
35	64 QAM	16 QAM	1/2	10	65	72.2
36	16 QAM	QPSK	3/4	6	58.5	65.0
37	64 QAM	QPSK	3/4	8	78	86.7
38	64 QAM	16 QAM	3/4	10	97.5	108.3

In IEEE 802.11n standard released in January 2008, the highest data rate that is specified is 600 Mbps, where the channel bandwidth is 40 MHz, short GI is used, there are four spatial streams, modulation is 64 QAM, and coding rate is 5/6. Moreover, there are 108 data subcarriers each holds six bits and six pilot subcarriers.

It should be noted that, although the transmission rate has a one-to-one relationship with an MCS index, the actual transmission rate depends on the performance of several MIMO function blocks such as STBC, transmit beamforming, spatial mapping, and so on. If such function blocks work well in an environment, a high-rate coding and modulation scheme can be selected. However, since the working environment of an 802.11n device varies from time to time, a rate adaptation scheme is needed to dynamically choose the best MCS index. In the simplest case, rate adaptation can be done by just selecting an MCS index according to the profiles of transmission rate, packet retransmission, packet loss, and so on. Such schemes are packet-level adaptation algorithms and show a loose cross-layer design between MAC and physical layers. More sophisticated schemes can be developed to directly determine the best modulation and coding scheme, the best number of spatial streams, and the length of GIs under a certain configuration of channel bandwidth, on the basis of physical layer measurements such as BER, SNR, etc. These schemes are bit-level algorithms and represent the tight cross-layer design between MAC and physical layers.

Mathematical Description of Signals

Given a PLCP protocol data unit (PPDU), the transmitted signal in the baseband of a transmit chain i_{TX}, denoted by $r^{i_{TX}}(t)$ is described as a complex variable, and is related to the RF signal, $r_{RF}^{i_{TX}}$, by the following equation:

$$r_{RF}^{i_{TX}}(t) = \mathrm{Re}\{r^{i_{TX}}(t)\exp(j2\pi f_c t)\}, \tag{2.1}$$

where Re represents the real part of a complex variable, and f_c is the center frequency of the carrier of RF signals.

As depicted in the structure of a PLCP preamble and the format of a PPDU, the transmitted signal of a PPDU consists of multiple fields, including a number of fields in the PLCP preamble and the data field. Thus, the overall baseband transmitted signal of a PPDU depends on the format of the PLCP preamble. Considering the HT mixed format preamble, the baseband signal of a PPDU on a transmit chain can be described as a sum of the baseband

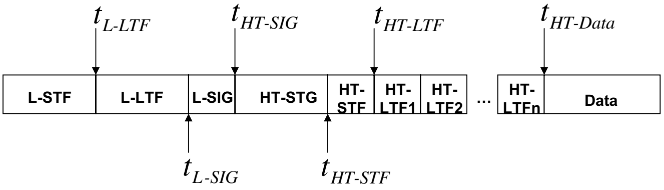

Figure 2.8 The timing relationship of different fields in a PPDU

signals of different fields, as shown below:

$$\begin{aligned} r^{i_{TX}}(t) &= r^{i_{TX}}_{L\text{-}STF}(t) + r^{i_{TX}}_{L\text{-}LTF}(t - t_{L\text{-}LTF}) + r^{i_{TX}}_{L\text{-}SIG}(t - t_{L\text{-}SIG}) + r^{i_{TX}}_{HT\text{-}SIG}(t - t_{HT\text{-}SIG}) \\ &+ r^{i_{TX}}_{HT\text{-}STF}(t - t_{HT\text{-}STF}) + \sum_{i_{LTF}}^{N_{LTF}} r^{(i_{TX},i_{LTF})}_{HT\text{-}LTF}(t - t_{HT\text{-}LTF} - (i_{LTF} - 1)T_{HT\text{-}LTF}) \\ &+ r^{i_{TX}}_{HT\text{-}DATA}(t - t_{HT\text{-}DATA}). \end{aligned} \tag{2.2}$$

In the right-hand side of the above equation, the timing in each field has a one-to-one relationship to the structure of the preamble shown in Figure 2.8. In addition, t_{field} is the time offset that specifies the starting time of each field. For example, L-LTF is the second field and its time offset is $t_{L\text{-}LTF}$, so its baseband signal is $r^{i_{TX}}_{L\text{-}LTF}(t - t_{L\text{-}LTF})$. The length of each field is denoted by T_{field}, e.g., $T_{HT\text{-}LTF}$ is the length of an HT-LTF field.

Given a field, its baseband signal waveform, denoted by $r^{i_{TX}}_{field}$, can be described as follows:

$$r^{i_{TX}}_{field} = \frac{1}{\sqrt{N^{tone}_{field} N_{TX}}} w_{field}(t) \sum_{k} \Upsilon_k X^{i_{TX}}_k \exp(j2\pi k \Delta_F t). \tag{2.3}$$

This waveform combines all signals from all subcarriers of each field in the transmit chain i_{TX}, which is actually performed through discrete Fourier transform (DFT). $X^{i_{TX}}_k$ represents frequency-domain symbols and is the output of spatial processing in subcarrier k of a transmit chain. $w_{field}(t)$ is a windowing function. The scale factor $(1/\sqrt{N^{tone}_{field} N_{TX}})$ ensures that the overall transmit power of the time-domain signal summed over all transmit chains is less than or equal to 1. Another critical parameter in this waveform is Υ_k. Giving an appropriate value to this parameter makes the peak-to-average power ratio (PAPR) of a 40 MHz channel comparable to that of a 20 MHz channel. In IEEE 802.11n, the assigned values of Υ_k are given as

$$\Upsilon_k = 1, \text{ in a 20 MHz channel } \Upsilon_k = \begin{cases} 1, & \text{if } k \le 0 \text{ in a 40 MHz channel,} \\ j, & \text{if } k > 0 \text{ in a 40 MHz channel.} \end{cases} \tag{2.4}$$

As shown in the above equation, the upper tones in a 40 channel are rotated by 90, which is helpful to reduce PAPR.

Table 2.3 One example of STBC

STS index i	$\tilde{d}_{k,i,2m}$	$\tilde{d}_{k,i,2m+1}$
1	$d_{k,1,2m}$	$d_{k,1,2m+1}$
2	$-d^*_{k,1,2m+1}$	$d^*_{k,1,2m}$
3	$d_{k,2,2m}$	$d_{k,2,2m+1}$
4	$d_{k,3,2m}$	$d_{k,3,2m+1}$

Space-time Block Code (STBC) and Beamforming

STBC STBC is performed after constellation mapping. It is optional for IEEE 802.11n and only valid when the number of spatial streams, N_{SS}, is less than the number of spatial time streams, N_{STS}.

The inputs to STBC are the outputs from the constellation mapper, so they can be described as a stream of complex numbers

$$d_{k,i,n};\ k = 0, \ldots, N_{SD} - 1;\ i = 1, \ldots, N_{SS};\ n = 0, \ldots, N_{SYM} - 1,$$

where N_{SD} is the number of data subcarriers and N_{SYM} is the number of OFDM symbols. After STBC operation, the outputs become

$$\tilde{d}_{k,i,n};\ k = 0, \ldots, N_{SD} - 1;\ i = 1, \ldots, N_{STS};\ n = 0, \ldots, N_{SYM} - 1.$$

The actual operation of STBC is reflected in the mapping from $d_{k,i,n}$ to $\tilde{d}_{k,i,n}$. Moreover, the STBC is always performed over one pair of consecutive OFDM symbols in each spatial stream, e.g., $d_{k,i,2m}$ and $d_{k,i,2m+1}$. For example, if $N_{STS} = 4$, $N_{SS} = 3$, then the STBC can be performed as shown in Table 2.3.

Beamforming Considering two nodes using IEEE 802.11n, Node A is the transmitter and Node B the receiver. The channel matrix from Node A to Node B is assumed to be H_k. The transmitted signal of subcarrier k is $\mathbf{x_k} = [x_1, x_2, \ldots, x_{N_{TX}}]^T$, and the corresponding received signal is $\mathbf{y_k} = [y_1, y_2, \ldots, y_{N_{RX}}]^T$, where N_{TX} and N_{RX} are the number of transmitting antennas and receiving antennas, respectively. Thus, $\mathbf{y_k} = H_k\mathbf{x_k}$.

In order to improve the power or signal-to-noise ratio at the receiver in a MIMO system, beamforming can be used. If the beamforming matrix is Q_k, the transmitted signal will become $Q_k\mathbf{x_k}$, and the received the signal is $\mathbf{y_k} = H_k Q_k\mathbf{x_k}$. Thus, the design goal of beamforming is to find the matrix Q_k such that the receiving performance at the receiver is improved. To achieve this goal, channel status information (CSI) must be measured or estimated. Depending on different methods of measuring channel information, beamforming schemes can be classified into two types: implicit feedback beamforming and CSI matrices feedback beamforming.

Implicit feedback beamforming In the implicit feedback beamforming, the channel from the transmitter to its receiver is estimated by the transmitter based on the information of the channel from the receiver to the transmitter. Thus, the channel estimation depends on the channel reciprocity in the forward link and the reverse link. Given the estimated channel H_k and the required performance at the receiver, the transmitter can calculate the set of beamforming matrices, Q_k, one for each subcarrier.

The assumption for channel reciprocity is usually only true for a time division duplex (TDD) system. Thus, implicit feedback beamforming is used in a TDD system. It should be noted that, even if a TDD system is considered, the channel reciprocity may not always be held due to the impact of antennas at the transmitter and also at the receiver. In a TDD system, the over-the-air channel is reciprocal, but the basedband-to-basedband channel between two nodes is not necessarily reciprocal; different nodes have different amplitude and phase characteristics in antennas associated with transmit and receive chains, which degrades the reciprocity of the over-the-air channel. Assume that the amplitude and phase responses of Node A's transmit and receive chains are $A_{TX,k}$ and $A_{RX,k}$, respectively, for subcarrier k. The amplitude and phase responses for Node B's transmit and receive chains are $B_{TX,k}$ and $B_{RX,k}$, respectively. Thus, from Node A to Node B, the baseband-to-baseband channel is $\tilde{H}_{AB,k} = A_{TX,k}H_{AB,k}B_{RX,k}$, where $H_{AB,k}$ is the over-the-air channel from Node A to Node B. Similarly, the baseband-to-baseband channel from Node B to Node A is $\tilde{H}_{BA,k} = B_{TX,k}H_{BA,k}A_{RX,k}$. Thus, even if $H_{AB,k} = H^T_{BA,k}$, it is possible that $\tilde{H}_{AB,k} \neq \tilde{H}_{BA,k}$.

In order to avoid the above issue, a channel calibration procedure is needed to achieve the reciprocity of the baseband-to-baseband channel. The key idea in calibration is to find correction matrices in the transmit chains of both Node A and Node B such that the channel is reciprocal. If the correction matrices in Node A and Node B are $K_{A,k}$ and $K_{B,k}$, respectively, then the baseband-to-baseband channels become $\tilde{H}_{AB,k} = K_{A,k}A_{TX,k}H_{AB,k}B_{RX,k}$ from Node A to Node B and $\tilde{H}_{AB,k} = K_{B,k}B_{TX,k}H_{BA,k}A_{RX,k}$ from Node B to Node A. When $K_{A,k} = \alpha_{A,k}[A_{TX,k}]^{-1}A_{RX,k}$ and $K_{B,k} = \alpha_{B,k}[B_{TX,k}]^{-1}B_{RX,k}$, where $\alpha_{A,K}$ and $\alpha_{B,k}$ are complex-valued scaling factors, then $\tilde{H}_{AB,k} = \alpha_{A,k}A_{RX,k}H_{AB,k}B_{RX,k}$ and $\tilde{H}_{AB,k} = \alpha_{B,k}B_{RX,k}H_{BA,k}A_{RX,k}$. Considering that the amplitude and phase responses of a node's transmit or receive chains can be expressed as diagonal matrices, $\tilde{H}_{AB,k} = (\alpha_{A,k}/\alpha_{B,k})[\tilde{H}_{AB,k}]^T$. Thus, if Node A and Node B can determine proper values for $K_{A,k}$ and $K_{B,k}$, respectively, then the baseband-to-baseband channel reciprocity can be achieved.

CSI matrices feedback beamforming This type of beamforming is used when channel reciprocity does not hold. In this case, the beamformee needs to estimate the channel matrix and send such information back to the beamformer. Since the CSI matrices for each subcarrier, denoted by $H_{eff,k}$, need to be sent back to the beamformer, overhead can be high. To reduce the overhead, the CSI matrices are encoded before being sent from the beamformee to the beamformer. The encoding and decoding procedures ensure that the beamforming feedback information can be sent efficiently and reconstructed correctly. There are two methods of sending such CSI matrices.

- *Noncompressed beamforming matrix feedback:* In this option, the real part and the imaginary part of each element of the matrix are encoded, sent, and decoded.

- *Compressed beamforming matrix feedback:* The matrix is compressed in the form of angles instead of real and imaginary parts. Thus, the information that needs to be sent is compressed.

Based on the CSI feedback information, the transmitter can then determine the spatial mapping matrix Q_k for beamforming.

Channel Sounding

The MIMO channel status information can be estimated from data HT-LTFs in a PLCP preamble. However, when the number of space-time streams, N_{STS} is less than the number of transmit antennas N_{TX} or the number of receiving antennas N_{RX}, the full characterization of the MIMO channel cannot be derived from data HT-LTFs. On the other hand, in some scenarios, it is necessary to get a full characterization of the MIMO channel. For example, the steering matrix for spatial mapping needs to be calculated, the MCS needs to be recommended by a receiver, and channels may need to be calibrated for beamforming.

In order to get the full MIMO channel characterization when N_{STS} is less than N_{TX} or N_{RX}, channel sounding is needed to find out the channel information that cannot be derived from data HT-LTFs. There are two methods of channel sounding: using extension HT-LTFs in a data packet or sending a null data packet (NDP). The former method is applied when channel sounding is performed together with a data packet. In this case, since all data HT-LTFs have been used in the preamble, extension HT-LTFs must be used. However, when an NDP is sent for channel sounding, data HT-LTFs are not used and thus can be used for channel sounding. In such a scenario, no extension HT-LTFs are needed. In both cases, the *channel sounding* field in the HT-SIG is set to zero to indicate that the current PPDU is also a channel sounding packet.

2.6.3 PMD Sublayer

PMD sublayer includes specifications for PMD receiver and transmitter and also defines the service primitives for the service access point (SAP) between PLCP and PMD sublayers.

For a PMD receiver, the following parameters are specified.

- *Receiver minimum input sensitivity.* This sensitivity is specified according to a packet error rate (PER) of less than 10% for a packet service data unit (PSDU) of 4096 bytes. Since the modulation and coding scheme varies with the rate, the receiver minimum input sensitivity is also rate dependent. In a MIMO system, multiple antennas may be used, so this sensitivity is specified per receive antenna.

- *Adjacent channel rejection.* Adjacent channel rejection is measured by setting the desired signal level 3 dB above the receiver minimum input sensitivity and then raising the interfering signal until a PER of 10% is reached; the power difference between the interfering signal and the desired signal is called adjacent channel rejection. The center frequencies of the interfering and desired signals are separate by 20 MHz in the 5 GHz band and by 25 MHz when operating in the 2.4 GHz band. For 40 MHz channels in 802.11n, the center frequencies of the interfering and the desired signals are separated by 40 MHz.

- *Non-adjacent channel rejection.* A similar scheme as that for adjacent channel rejection is used for non-adjacent channel rejection measurement. The center frequencies of the interfering and the desired signals need to be separated by 40 MHz or more for 20 MHz channels and by 80 MHz or more for 40 MHz channels.

- *Receiver maximum input level.* For any basedband modulation, the receiver maximum input level (e.g., −30 dBm) is specified such that PER does not exceed 10%.

- *Clear channel assessment (CCA) sensitivity.* CCA sensitivity specifies a signal level at which a receiver is in the busy state. For a valid 802.11n signal, as long as it exceeds the smallest receiver minimum input sensitivity among all coding and modulation schemes, the receiver will enter the busy state. For any other signals, as long as it is 20 dB above the smallest receiver minimum sensitivity, CCA must hold the receiver busy. From CCA specifications, we know that interference may still exist even if the node detects that the channel is clear according to the CCA threshold. However, it is not a viable approach to lower the CCA threshold, because this can prevent a node from transmitting packets even if only low-level interference exists.

- *Received channel power indicator.* Given a channel, this indicator measures the received RF power over the data portion of the received frame.

The PMD receiver is also required to decode a packet transmitted with a reduced interframe space (RIFS) separation from the previous packet. RIFS aims to improve efficiency by separating back-to-back transmissions from the same transmitter with a very short interframe space. It is only 2 μs in the 802.11n MIMO physical layer, while the slot time and short interframe space (SIFS) are 9 μs and 16 μs, respectively.

In order to ensure appropriate operation, a PMD transmitter must conform to the following specifications.

- *Transmit spectrum mask.* Given a frequency offset from the center frequency, the spectrum mask specifies the power spectrum density (PSD) that a PMD transmitter must satisfy when using a certain channel. Since 802.11n can use either a 20 or 40 MHz channel, two different spectrum masks are defined. For a 20 MHz channel, the spectrum mask is as illustrated in Figure 2.9, where the PSD of each frequency is defined with respect to the maximum PSD of the signal and the unit is dBr. It is critical for a PMD transmitter to conform to the spectrum mask. At a given frequency, if the PSD is lower than that specified in the mask, then it means transmit power in the PMD transmitter is lower than allowed and can result in smaller coverage or lower transmission rate. On the other hand, if the PSD is higher than the specified value in the mask, then it means that there are unwanted emissions that can cause unnecessary interference.

- *Maximum transmit power.* In addition to the spectrum mask, the maximum transmit power from a PMD transmitter must satisfy the requirements in different regulatory domains.

- *Spectral flatness.* Since the 802.11n physical layer is built on top of OFDM, the average energy of the constellations must be specified for a subcarrier. In order to ensure spectral flatness, the average energy needs to be within a small deviation, e.g., the average energy deviation for the constellations in subcarriers -16 to -1 and $+1$ to $+16$ must be within ±2 dB.

- *Center frequency and symbol clock frequency tolerance.* The PMD transmitter must tolerate a certain range (e.g., ±20 ppm) of frequency oscillation.

- *Packet alignment.* At the end of the last symbol of a packet, the transmitter must emit a physical layer transmission end (PHY-TXEND) confirm primitive to let the MAC layer know that the entire packet has been transmitted on the air.

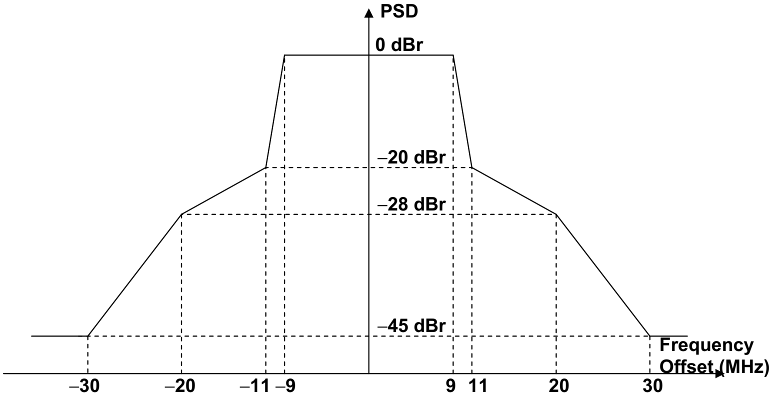

Figure 2.9 Transmit spectrum mask for a 20 MHz channel of 802.11n

- *Modulation accuracy.* A modulation accuracy test procedure specified in the 802.11n standard must be followed to measure the modulation accuracy of the 802.11 physical layer. An important index for modulation accuracy is the transmitter constellation error. This is a root mean square (RMS) error averaged over subcarriers, OFDM frames, and spatial streams. The modulation accuracy is rate-dependent as different modulation schemes are adopted for different transmission rates.

In the SAP between PLCP and PMD sublayers, service primitives are also specified to define the interactions between sublayers and those between peer nodes.

2.6.4 PLME Sublayer

PLME maintains a list of management information base (MIB) attributes that may be accessed by physical layer entities. The MIB attributes cover all the physical characteristics ranging from OFDM parameters, power levels, to all parameters related to MIMO operation. A full list of MIB attributes can be found in the 802.11n draft standard [120].

2.7 Open Research Issues

Research challenges in the physical layer are twofold. First, it is necessary to further improve the transmission rate and the performance of physical layer techniques.

- *New wideband transmission technologies.* New wideband transmission schemes other than OFDM or UWB are needed in order to achieve higher transmission rates in a larger area network.

- *Better beamforming for directional antennas.* New signal processing algorithms are needed for more accurate beamforming.

- *Practical and inexpensive multi-antenna systems.* Multiple-antenna systems have been researched for years. However, their complexity and cost are still too high to be widely accepted for WMNs. If simpler multi-antenna systems are used, diversity performance is not good enough. Thus, both hardware design and signal processing algorithms need to be enhanced.

- *User cooperative communications.* New signal processing algorithms need to be developed to further improve the performance of user cooperative diversity. Another important issue is to develop new algorithms and hardware to build practical user cooperative communication systems.
- *Advanced multichannel systems.* So far wireless radio with multiple transceivers are available. However, its cost is still very high. Thus, it is necessary to optimize the hardware design so as to reduce the cost. The same requirement is needed for a multiradio system. Moreover, multichannel systems with directional antennas are also desired.
- *Advanced radios.* Frequency agile techniques are still in the early phase. Many challenging issues need to be resolved before they can be accepted for commercial use [158]. Software radios are facing the same situation. However, both frequency agile radios and software radios are key technologies for next generation wireless networks.

Second, to best utilize the advanced features provided by physical layer, higher layer protocols, especially MAC protocols, need to be carefully designed. Otherwise, the advantages brought by such physical layer techniques will be significantly compromised.

- *Link adaptation.* To date, most link adaptation schemes focus on adaptive rate control for physical layers with variable channel coding and modulation in the same channel. New link adaptation schemes are needed for a multichannel system. If a MIMO system is considered, different link adaptation algorithms have to be developed too. Thus, whenever a new physical layer technique with multirate support is adopted, a new link adaptation scheme is required.
- *MAC protocol.* For directional and smart antennas, many MAC protocols have been proposed for ad hoc networks [62, 149, 197, 285]. A MAC protocol for MIMO systems is studied in [245]. However, for multi-antenna systems, an efficient MAC protocol to achieve significant throughput improvement is still needed, communication protocols for cognitive radios remain an open issue, and tremendous research efforts are needed to make cognitive-radio-based WMNs practical. For user-cooperative communications, cross-layer design between MAC and physical layers is desired in order to achieve better diversity gain.

It should be noted that all the above issues become much more challenging in WMNs, because:

- Cross-layer design algorithms or cooperative communication algorithms conducted over advanced physical layer techniques involve many nodes within multiple hops.
- The protocols and algorithms to resolve the above issues need to consider the tradeoff between centralized and distributed schemes. Centralized schemes are impractical to implement in a WMN, while distributed algorithms cannot achieve optimal performance.

As far as WMNs are concerned, development of advanced physical layer techniques and design of MAC protocols or cross-layer design are two closely interactive processes. Thus, the traditional sequential design pattern (i.e., the physical layer is designed first and then the MAC layer) may not be a viable solution; a wiser strategy would be to keep the support of mesh networking capability in mind while a new physical layer technique is designed.

3

Medium Access Control Layer

When a network node is equipped with physical layer techniques for signal transmission and reception, it basically has the point-to-point communication capability. However, this is insufficient for networking among multiple nodes, for several reasons.

First of all, an interface is needed between physical and higher layer protocols in order to interpret bit streams and convert them into packets or vice versa. Secondly, operation mechanisms and algorithms are required to coordinate transmission and reception of packets among many nodes with the objective of improving network performance. This type of function is called medium access control (MAC). Thirdly, errors can still occur in bits or packets even though the most advanced channel coding algorithms are applied. This is particularly true for wireless networks because of variations of link quality, interference, and many other factors. As a result, additional error control is usually desired on top of physical layer.

As we pointed out in the previous chapters about the differences between WMNs and mobile ad hoc networks (MANETs), existing MAC and error control schemes proposed for MANETs are not necessarily applicable to WMNs, due to different network characteristics and design features.

The key task of a MAC protocol is to coordinate the process of sharing the same medium among multiple users with the objective of achieving certain performance goals. Typical performance metrics include throughput and QoS, e.g., delay, delay jitter, and packet loss ratio, etc.

Depending on which network node takes care of the coordination of medium access, MAC can be classified into two major types: *centralized MAC* and *distributed MAC*.

In a centralized MAC protocol, the entire process is controlled and coordinated by a centralized node, and all other nodes must rely on this node to access the network. Many wireless networks lie in this category. For example, cellular networks, infrastructure mode wireless LANs, satellite networks, etc. However, in multihop wireless networks, distributed MAC is preferred, because the network itself is distributed in essence. If a centralized MAC is used for these networks, it lacks enough efficiency owing to the need for maintaining the centralized control among multiple nodes. This also inhibits the scalability of the

Wireless Mesh Networks Ian F. Akyildiz and Xudong Wang

MAC protocol. As a result, distributed MAC is extremely necessary for MANETs, and also for WMNs. However, it is obvious that designing a distributed MAC is a much more challenging task than designing a centralized MAC.

In general, there is no transparency between MAC and physical layer, because the lower part of the MAC is built directly upon the physical layer techniques. For example, in the physical layer some basic multiple access schemes such as TDMA, CDMA, or OFDM have been considered. A MAC protocol does not replace these basic multiple access schemes. Instead, it must consider them as a starting point for the design of a MAC protocol.

A MAC protocol usually consists of several major components.

1. *Packet processing and queuing for both transmission and reception.* This is an interface between the MAC and upper layer protocols. When packets arrive from upper layer protocols such as the IP layer, packets are processed by adding MAC headers and some error control fields such as CRC. When security is needed, the contents of a packet needs to be ciphered according to a certain encryption algorithm. After all such processing is completed, packets are queued in the transmission, and wait for resources (e.g., time slots, channels, codes, etc.) to start transmission. In the receiving part, the entire process is performed in the reverse way so that packets are correctly received in the MAC layer and sent to the upper layer.

2. *Coordination of medium access.* This is the key component of a MAC protocol, which involves many different tasks depending on what type of MAC protocols need to be designed.

    - For a reservation based MAC protocol, the key task is to assign resources such as codes, time slots, subcarriers or channels, to users such that the network throughput is maximized, but their QoS is also satisfied. To this end, many other algorithms in the physical layer need to be considered, for example, power control, adaptive coding and modulation, etc. In addition, functions in the network and transport layers also need to be considered. For example, a TDMA MAC may impact slow start performance of TCP owing to the significant differences of round trip time (RTT) before and after resource allocation [257]. These demands imply that cross-layer design between MAC and other protocol layers are important.
    - For a random access MAC protocol such as CSMA/CA, the key issue is to find out the best solution for minimizing collision and fast recovery from collision in case it still happens. Since no reservation is available, collision becomes severe when the number of users increases, and thus significantly degrades the throughput performance. As a result, no QoS can be guaranteed. However, random access MAC protocols have two main advantages. First is their simplicity. No separate signaling and reservation schemes are needed in the protocol. Second is the compatibility with Connectionless (datagram) networks such as the Internet. On the contrary, a reservation-based MAC protocol always has the problem of how to do integration with a connectionless network. For example, if a TDMA MAC is used, whenever a TCP session starts, it has to wait for the allocation to be done. Such a delay is not TCP-friendly, because TCP assumes that the network is congested before even resource allocation is completed. Another

example is when video traffic is sent through a TDMA MAC into the Internet, the MAC has no way of knowing its bandwidth and QoS requirements. Without such information, reservation cannot be correctly done, unless adaptive resource estimation and dynamic time slot allocation are designed interactively. However, a random access MAC protocol does not have any of these problems, because a packet starts its transmission process as it arrives.

3. *Adaptive rate control.* The physical layer of many current wireless networks has the capability of adaptive coding and modulations. To better utilize such a capability, the MAC protocol must consider adaptive rate control for packet transmissions. Owing to the variance of transmission rate, the transmission time of packets also changes as the channel condition varies.

4. *Network formation and association.* This component is actually the network management part for a MAC protocol. It takes care of network formation and association/disassociation of a node to/from the network when a node joins/leaves the network. This is particularly important for WMNs. Without network formation and association, network nodes cannot recognize each other and accordingly start their MAC protocol.

A MAC protocol can be implemented in two types of architecture. In the classical implementation architecture, a MAC protocol is implemented in software (MAC driver), firmware, and hardware. Usually, packet queuing, network formation, node association, and so on, are done in the driver. Timing critical functions, e.g., time slot generation, backoff procedures, etc., are performed in the firmware. The actual real-time operation of the MAC protocol is done in the hardware. For example, when a backoff counter is determined, the exact decrement of this counter is done in the hardware in order to achieve high accuracy. Thus far, many companies have tried to pull more functions in the firmware into the driver level so that the driver has more freedom to control/modify the MAC protocol. This type of method is usually called a “softMAC” implementation. However, since many key functions are still located in firmware, the timing critical part of the MAC protocol is hard to modify. This problem has been solved in the second implementation architecture, which is called *software defined radio* (*SDR*) *MAC architecture*. In this new architecture, no firmware is available. All timing critical functions are implemented in the hardware, but almost all of them can be controlled or modified by the driver. Thus, such an architecture provides a powerful approach to research and development of new MAC protocols.

Owing to the mesh networking topology, the design of a MAC protocol for WMNs is more challenging than that for a single-hop wireless network such as cellular networks or infrastructure based wireless LANs. Thus, a lot of research has been carried out to develop new MAC protocols for WMNs. In parallel with these efforts, several standards groups, in particular, IEEE 802 standard committees, are driving the standardization of the technologies for WMNs in all areas ranging from personal area networks, local area networks, and metropolitan area networks, to even larger scale networks.

The MAC protocols for WMNs can be classified into two categories: single-channel and multichannel MAC protocols which we will cover in the next sections.

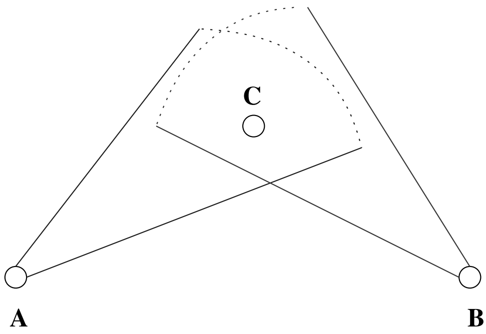

Figure 3.1 Hidden nodes when using directional antenna

3.1 Single-Channel Single-Radio MAC Protocols

3.1.1 CSMA/CA Improvements

The most well-known single-channel MAC protocol is CSMA/CA, which can be used in the ad hoc mode of IEEE 802.11 to form a meshed wireless LAN. Many schemes have been proposed to fine-tune CSMA/CA in order to improve its performance for WMNs. These schemes can be classified into the following categories.

- *Adjust physical carrier sense.* Physical carrier sense can cause both hidden node or exposed node issues: when the sensitivity is high, many nodes become exposed nodes; when the sensitivity is low, many nodes become hidden from each other. Thus, some proposals for using dynamic carrier sense range have been discussed in [155]. However, how to develop a scheduling scheme for all nodes in the network to fine-tune the range in a dynamic way is still a research problem. In actual implementation of an IEEE 802.11 wireless LAN card, the sensing range threshold used in CSMA/CA is configured with such a value that a node can sense the transmission of other nodes at a distance of more than two hops away. In order to reduce the number of exposed nodes, the physical carrier sense must be modified to be directional. A widely accepted scheme is to use directional antenna on nodes [62]. Thus, Node A being out of the directional coverage of Node B can transmit packets at the same time during Node B's transmission. Directional antenna has three shortcomings. Firstly, for nodes in the coverage of each other, exposed nodes still exist. Secondly, when nodes are out of each other's coverage, the network is partitioned, and thus requires dynamic tuning of the antenna beam, which increases the complexity and cost. Finally, hidden nodes will appear. For example, in Figure 3.1, Node C is in the coverage of Node A and Node B, but Node A and Node B do not cover each other. Thus, Node A and Node B become hidden nodes to each other and can cause collisions at Node C.

  Another scheme for reducing exposed nodes is to perform directional backoff [256]. When a node detects a busy channel, it does not always defer its transmission. Instead, it checks if its destination will also detect a busy channel. If not and the backoff counter is zero, then transmission can be started from this node, since the destination node will still be able to receive a packet correctly.

- *Improve virtual carrier sense.* Virtual carrier sense can effectively reduce hidden nodes, but also cause more exposed nodes. In order to reduce the number of exposed nodes, directional virtual carrier sense is needed. A directional virtual carrier sense is proposed in [247] to ensure that the operation of virtual carrier sense based on request to send/clear to send (RTS/CTS) matches the scenarios when both directional and omni-antennas exist in the same network. However, when all nodes use omni-directional antennas, directional virtual carrier sense schemes similar to directional backoff needed to be developed. Such schemes rely on the availability of topology information, and cooperation between neighboring nodes.
- *Dynamic tuning of backoff procedure.* The backoff procedure can be modified in different ways. First of all, a different backoff instead of binary exponential backoff can be used. However, it is not preferred, since it is not compatible with CSMA/CA specified in IEEE 802.11. Another scheme is to assign different minimum and maximum contention windows for different nodes in the network. However, how effective this scheme can be to improve throughput performance is questionable. A scheme that dynamically tunes the contention window is proposed in [43]. In this scheme, the backoff is approximated by p-persistent backoff. Based on this model and also the estimated number of active stations in the network, the optimal persistence factor p_{min} is determined. With p_{min}, the contention window is computed as $2/p_{min} - 1$. Simulations showed that this scheme could effectively improve throughput performance of CSMA/CA. However, it is based on several assumptions. In this scheme, each node is assumed to have packets to send following the Poisson process. In addition, the active stations can be estimated. Moreover, the optimal persistent factor can be calculated based on the estimated number of active stations, estimated collisions, estimated idle periods, and so on. All these assumptions do not really match a real network, in particular in a WMN environment.

The performance of CSMA/CA can be improved by the above schemes. However, no matter what fine-tuning strategy is taken, the scalability issue of CSMA/CA cannot be resolved, because the MAC protocol in these schemes is essentially still a type of CSMA/CA protocol.

3.1.2 IEEE 802.11e

IEEE 802.11e aims to improve the performance of CSMA/CA so that a certain level of QoS can be supported. The key function specified in IEEE 802.11e is the hybrid coordination function (HCF). HCF combines two functionalities: enhanced distributed channel access (EDCA) and HCF controlled channel access (HCCA).

EDCA improves the distributed coordination function (DCF) function by providing prioritized access to different traffic types. In EDCA, the same traffic marking scheme proposed in IEEE 802.1D is adopted. Thus, traffic from the upper layer has eight different priorities. In IEEE 802.11e, these eight priorities are further mapped into four access categories (ACs) each assigned with a different set of parameters such as arbitrary inter-frame space (AIFS), CW_{min}, and CW_{max}. For example, for voice traffic, it has the highest priority, and thus its AIFS is smallest and so are CW_{min}, and CW_{max}. In addition, the maximum contention window of a higher-priority access category (AC) should not be smaller than the minimum contention window of a lower-priority AC. Based on these priorities in different ACs, both internal contentions and extend contentions exist. For internal contentions, different ACs of the same node have to compete with each other to determine which AC is the next to start communications. Once this is determined, ACs from different nodes must contend with each other. The node winning the contention process is allocated with an enhanced distributed channel access (EDCA) transmission opportunity (TXOP). The length of an EDCA TXOP is defined in the beacon. During this period, the number of packets to be transmitted by the node depends on the length of both TXOP and a packet. If the packet is larger than the TXOP, fragmentation is needed. Otherwise, multiple packets are sent in this TXOP.

It should be noted that a legacy node with IEEE 802.11e just tries to access the channel according to DCF.

In Hybrid coordination function Controlled Channel Access (HCCA), QoS access point (QAP) assigns a TXOP to a QoS station (QSTA) by sending a QoS polling message, QoS CF_Poll, to this QSTA. Such a TXOP is called polled TXOP and can occur in both *contention period* (*CP*) and *contention free period* (*CFP*) in each beacon interval. The length of a polled TXOP is granted by the QAP in the QoS CF_Poll message. Along with traffic specifications (TSPEC) and scheduling schemes, polled TXOP can provide QoS guarantees to multimedia traffic.

EDCA and HCCA can provide QoS support to nodes in an infrastructure mode. In a WMN environment, IEEE 802.11e is not applicable due to the following issues.

- EDCA does not really provide true QoS support. EDCA relies on AIFS and contention widow to prioritize channel access. For the ACs on the same node, this is perfect. However, considering different nodes, the backoff counter of a node with a lower-priority AC may reach zero earlier than that of a node with a higher-priority AC. The reason is that the contention window and AIFS on different nodes are not synchronized.

- EDCA is just a per-hop mechanism for QoS support. Even when it works perfectly, it does not provide any support for end-to-end QoS.

- HCCA can provide harder QoS than EDCA, but it depends on the availability of QAP. In WMNs, such kinds of central controller may not be available. Moreover, HCCA also relies on TSPEC and end-to-end scheduling schemes in order to support end-to-end QoS. Such complicated mechanisms are out of the scope of IEEE 802.11e. Thus, whether HCCA can be applied to WMNs is still unknown and needs future research efforts. Another challenging issue to HCCA is how to get TSPEC from high layer protocols, in particular when resource-reservation protocol (RSVP) is not supported in IP networks.

3.1.3 WMN MAC Based on IEEE 802.11s

As explained earlier, CSMA/CA adopted in IEEE 802.11 can be directly applied to WMNs. This kind of scheme may raise many challenges. First of all, a routing protocol is needed on top of CSMA/CA. However, most routing protocols are proposed for mobile ad hoc networks

(MANETs), which can be cumbersome for WMNs. In addition, different routing protocols cannot inter-operate with each other. Secondly, protocols are needed to form and maintain the topology of WMNs, which is much different from a traditional wireless LAN. Proprietary solutions will end up with interworking difficulty. Finally, WMNs based on CSMA/CA are not scalable with the number of nodes and the number of hops. In order to avoid such issues, many companies, including Intel, Motorola and Cisco, established an IEEE 802.11 subworking group for mesh networks, i.e., IEEE 802.11s.

IEEE 802.11s specifies both routing and MAC layer functions. The network architecture, end-to-end protocol stack reference mode, potential routing protocols, topology formation, optimal multichannel operation, and so on, are specified in the first draft of the IEEE 802.11s standard. However, many functions are still out of scope of IEEE 802.11s. For example, how a mesh point supports access for legacy IEEE 802.11 clients is not specified in IEEE 802.11s. In another example, the detailed algorithm of channel allocation in the multichannel mode will not be specified in IEEE 802.11s. On the other hand, many functions that will be specified in the final version of the standard are still being developed and waiting for future discussions.

After reviewing the entire draft of IEEE 802.11s, several potential issues can be found.

- The cross-layer is poorly supported in the current draft, although routing protocol is directly moved to the MAC layer and is specified in IEEE 802.11s. The functions of MAC and routing layers still work transparently to each other as that in a traditional setup of IEEE 802.11 WMNs. Such a solution may solve the inter-working problem, but it is not so evident that such a design can really improve the network performance.
- The scalability problem of CSMA/CA in WMNs has not been solved, and many IEEE 802.11s contributors are still submitting proposals to fine tune the CSMA/CA protocol in a WMN environment. However, fine-tuning parameters does not really resolve the scalability issue. Multichannel operation can be a potential solution for improving scalability. However, the detailed mechanism of interacting between CSMA/CA and multichannel operation is out of the scope of IEEE 802.11s.
- QoS has not been considered in IEEE 802.11s. Considering that IEEE 802.11e is not applicable to WMNs, IEEE 802.11s lacks a solution to QoS support of multimedia traffic.

The details of the IEEE 802.11s standard will be discussed in Chapter 10.

3.1.4 TDMA Over CSMA/CA

Instead of just fine-tuning the parameters of CSMA/CA to improve its performance, a new system architecture is proposed in [256] to integrate TDMA together with CSMA/CA. This new MAC protocol consists of the following major functions.

- Node synchronization based on enhanced time synchronization function (TSF) of 802.11 MAC.
- Software retransmission is proposed to disable the hardware level retransmission in an 802.11 MAC. Based on software retransmission, packet transmission and reception can be limited to a particular time slot, and thus crossing slot-boundary is avoided.

- A distributed scheduling scheme is developed to coordinate packet transmissions in different nodes in WMNs. QoS is considered in time slot allocation of this scheduling scheme.
- The scheduling scheme and TDMA frame structure are designed to support network access of legacy CSMA/CA nodes.

To further improve the performance of TDMA over CSMA/CA, a multichannel mode has been proposed in [257] and contains the following additional major functions.

- Channel switching needs to be improved to reduce the overhead due to channel switching. Although the physical-layer operation of a channel switch can as quick as less than 100 μs, the procedures involved in MAC can take a much longer time. Thus, the channel switching procedure in the MAC needs to be optimized.
- A time slot and channel allocation algorithm [258] is needed to allocate time slots and channels at the same time by considering the traffic demands, QoS, and network topology.

In order to implement the above TDMA MAC protocols based on CSMA/CA, the system architecture of CSMA/CA MAC needs to be software programmable. However, as the chipset design has advanced, such a system architecture has become general practice for MAC protocol design.

TDMA over CSMA/CA holds many advantages.

- It does not have the well-known problems of a CSMA/CA protocol. Thus, throughput, QoS, and fairness of WMNs based on such a MAC protocol are much improved as compared to CSMA/CA.
- It is still compatible with CSMA/CA.
- It can potentially benefit many other protocols such as routing, mobility management, transport, etc., because of its TDMA mechanism.
- Its multichannel mode achieves much more efficient multichannel operation than other existing multichannel MAC protocols, because channel selection and switching are coordinated in a TDMA fashion.

3.1.5 IEEE 802.16 MAC in Mesh Mode

The MAC protocol in IEEE 802.16 was originally designed for fixed point-to-multipoint (PMP) wireless metropolitan area networks (wirelessMAN). The IEEE 802.16a approved in 2003 takes into account the support of mesh mode. In 2004, both mesh mode and PMP mode were consolidated into one standard. In this chapter, our discussions on IEEE 802.16 MAC are focused on the 2004 version of the standard. It should be noted that this version has been enhanced to support both fixed and mobile operation in IEEE 802.16e approved in 2005.

The IEEE 802.16 protocol reference mode is shown in Figure 3.2.

The MAC layer of IEEE 802.16 consists of MAC common part sublayer (CPS) and security sublayer. On top of the MAC CPS, is a service-specific convergence sublayer (CS) that performs the following functions.

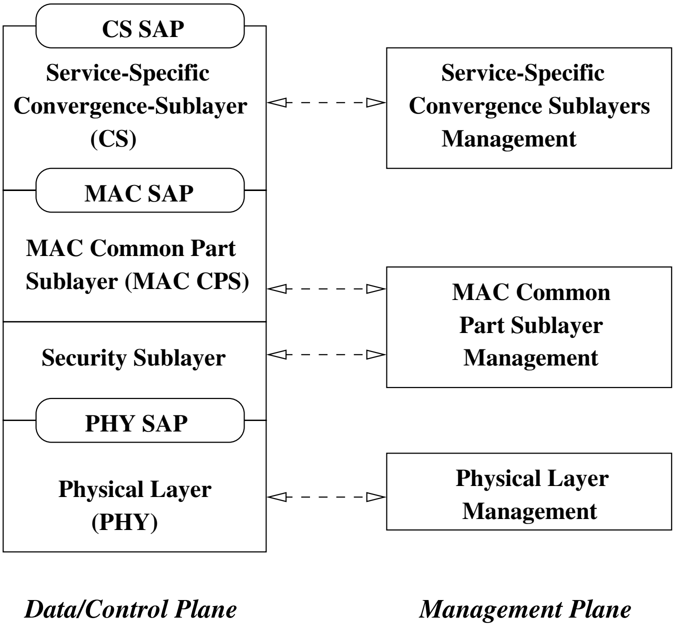
CS SAP
Service-Specific Convergence-Sublayer (CS)
MAC SAP
MAC Common Part Sublayer (MAC CPS)
Security Sublayer
PHY SAP
Physical Layer (PHY)
Service-Specific Convergence Sublayers Management
MAC Common Part Sublayer Management
Physical Layer Management
Data/Control Plane
Management Plane

Figure 3.2 IEEE 802.16 protocol stack

- accept higher-layer protocol data units (PDUs)
- classify and process higher-layer PDUs
- deliver CS PDUs to the appropriate MAC SAP
- receive CS PDUs from the peer entity

So far, two CSs are specified in IEEE 802.16: the asynchronous transfer mode (ATM) CS and the packet CS. Thus, both ATM services and packet-oriented services can be supported over IEEE 802.16 wireless networks.

In the physical layer, several air interfaces are specified, but only one of them currently supports mesh mode: *WirelessMAN-OFDM*, based on OFDM modulation technology and design for non-line-of-sight (NLOS) operation in the licensed frequency bands below 11 GHz.

IEEE 802.16 Mesh Mode and Mesh Networking Architecture

In 802.16 MAC, two networking modes are supported: PMP mode and mesh mode. In PMP mode, a subscriber station (SS) is controlled by a base station (BS) and communicates with another SS through the BS. Communication from a BS to its SS is called a downlink, while those from an SS to the BS is called an uplink. In mesh mode, there is no concept of uplink or downlink since all SSs can be connected to each other via a multihop mesh topology. A typical mesh networking architecture of an IEEE 802.16 mesh network is compared with the PMP mode based networking architecture in Figure 3.3.

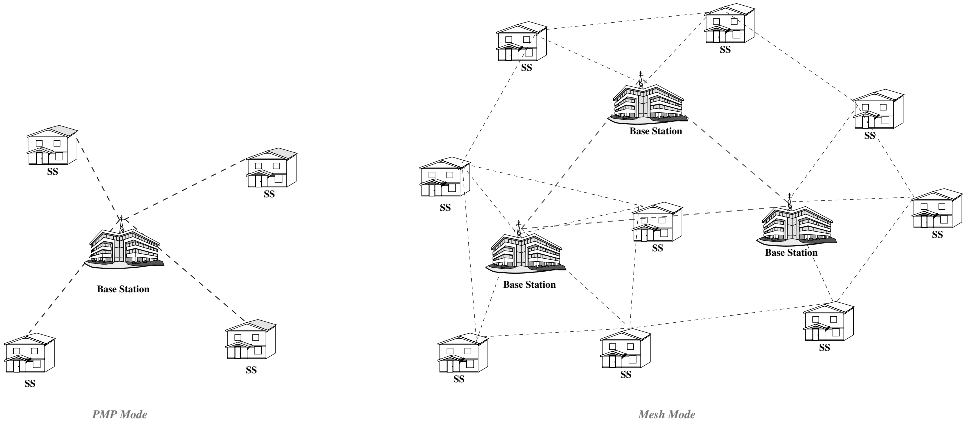

Figure 3.3 Networking architecture of IEEE 802.16: mesh mode versus PMP mode

There are two scheduling modes defined in the standard: *centralized* and *distributed*. In the *centralized* mode, the base station (BS) is responsible for defining the schedule of transmissions in the entire network. In the *distributed* mode, transmissions are scheduled in a fully distributed fashion without requiring any interaction with the BS. Transmissions in the distributed mode can be either *coordinated* or *uncoordinated*, as detailed below. Centralized and distributed scheduling modes can coexist within the same IEEE 802.16 mesh network. In this case, they use dedicated slots in the control subframe, as shown in Figure 3.3.

MAC Support for Physical Layer Options

The time is partitioned into frames of fixed duration. Each frame consists of a control subframe and a data subframe, as illustrated in Figure 3.4. Control subframes are partitioned into slots of fixed duration, which are accessed by nodes based on the distributed election procedure specified by the standard. This ensures that, in a steady state, each node gets the opportunity to transmit control messages in a regular, though not periodic, manner, which was modeled in [46]. A control slot consists of seven OFDM symbols, two of which are used as a physical preamble to synchronize the receiver, and one is used as a guard symbol. Up to 16 control slots can be specified per frame. Data subframes consist of a fixed number of data mini-slots, up to 256. The number of bytes conveyed by a slot depends on the modulation and coding scheme (MCS) used by the sender to transmit data to the receiver. Every node dynamically adapts the MCS from neighbor to neighbor, based on measurements of the received signal quality at the physical layer. However, control messages are transmitted using the most robust modulation and coding scheme, i.e., quadrature phase-shift keying (QPSK) with code rate 1/2. An IEEE 802.16 mesh network can employ up to 16 non-interfering channels for data transmission to increase the available transmission capacity for nearby nodes which cannot exploit spatial reuse. However, control messages are transmitted by all nodes in the network in the same channel.

The following messages can be transmitted during the control slots.

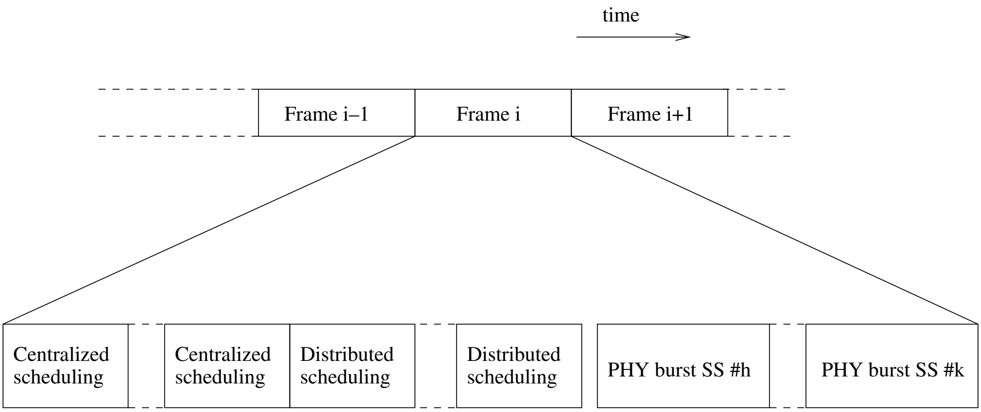

Figure 3.4 Frame structure in mesh mode

- *MSH-NCFG*: Mesh network configuration, used for network configuration and maintenance. MSH-NCFG messages are transmitted in a regular manner by every node in the network at long timescales, much larger than that of frames. For instance, they are used to establish and maintain logical links between neighboring nodes in the transmission range of each other.

- *MSH-NENT*: Mesh network entry, used for performing network entry, as described below.

- *MSH-DSCH*: Mesh distributed schedule, used to coordinate channel access with the distributed scheduling mode.

- *MSH-CSCH*: Mesh centralized schedule, used by the BS to advertise channel reservations with the centralized scheduling mode. Furthermore, nodes can use MSH-CSCH messages to request bandwidth from the BS. Intermediate nodes relay MSH-CSCH messages directed to, or transmitted by, nodes that cannot communicate directly with the BS.

- *MSH-CSCF*: Mesh centralized schedule configuration, used by the BS for network configuration with the centralized scheduling mode.

Network Entry Process

Before a SS becomes part of an IEEE 802.16 network, it must go through the network entry process to join the network. In mesh mode, the network entry process of a new node includes the following sequential functions.

- *Scan for an active network and establish coarse synchronization with the network.* The network time is acquired from the timestamp field of an MSH-NCFG message. The valid network is found by continuously scanning the possible channels.

- *Obtain network parameters from MSH-NCFG messages.* The new node accumulates MSH-NCFG messages until it has received such a message twice from the same node and until it has received a *MSH-NCFG:Network Descriptor* with the network operator ID matching its own. The node also needs to build a physical neighbor list from the acquired information.

- *Open sponsor channel.* The new node selects a sponsoring node from all nodes that have the same logical network ID as that in the node with the matching network operator ID, and synchronizes its time with the sponsoring node. Then a *MSH-NCFG:Network Entry* message should be sent by the new node to the sponsoring node to get a unique node ID and a sponsor channel. From now on, all the remaining procedures between the new node and the sponsoring node are carried out via the sponsor channel.

- *Obtain basic capabilities.* Via the found sponsor channel, the node obtains its basic capabilities from the sponsor node. After this step, the new node becomes an SS.

- *Perform node authorization.* The authorization information and request are sent to the sponsor node through which such messages are tunneled to the authorization node, i.e., the BS in the network. The BS authorizes the new node and sends back an authorization result to the new node.

- *Perform registration.* The new node sends a registration request to the sponsoring node through which the request is further tunneled to the registration node. Upon registration, a unique node ID will be assigned to the new node.

- *Establish IP connectivity.* The new node acquires an IP address using dynamic host configuration protocol (DHCP).

- *Obtain time of day.* The time of day is retrieved from the network.

- *Transfer operational parameters.* The new node must download a parameter file through trivial file transfer protocol (TFTP).

Scheduling and Bandwidth Allocation

Bandwidth allocation depends on whether centralized or distributed scheduling is employed.

In the centralized scheduling, the BS controls the bandwidth allocation in all direct links. Thus, requests from SSs to the BS may go through multiple hops and the same with the grants from the BS to the SSs. Such a multihop request/grant reservation scheme can be quite complicated, and can introduce a large overhead in the network, in terms of both wireless resources consumed by the signaling messages and computational complexity of the algorithms implemented at the MAC layer of the BS. In addition, the network performance totally relies on the performance of the BS. Owing to such shortcomings in the centralized scheduling, distributed scheduling is a more promising option.

Distributed scheduling can be performed in a coordinated or uncoordinated scheme. In coordinated distributed scheduling, a SS's schedule and its proposed schedule change are sent to its neighbors on a PMP basis. Within a given channel of sending such information, all neighbors receive the same schedule and also use the same channel to transmit their schedule information. Coordinated distributed scheduling must ensure that transmissions are scheduled in a manner that does not rely on the operation of a BS and that the transmissions are not necessary from or to the BS.

Within the constraints of coordinated scheduling, uncoordinated distributed scheduling can be performed. Uncoordinated distributed scheduling is applied for fast ad hoc setup of transmission schedules on a link-by-link basis by directed requests and grants by two nodes. Since the coordinated scheduling can be centralized scheduling or coordinated distributed scheduling, the transmissions in coordinated distributed scheduling must be scheduled to ensure that the resulting data transmissions (and the request and grant packets themselves) do not cause collisions with the data and control traffic scheduled by either the coordinated distributed or the centralized scheduling methods.

In both coordinated and uncoordinated scheduling schemes, requests and grants are exchanged in a three-way handshake manner: (i) a node, namely the *requester*, asks a neighbor node, namely the *granter*, to allocate some bandwidth; (ii) the granter advertises a set of slots as ‘granted’ to the requester; (iii) the requester confirms that it will actually use that set of slots (or part thereof) to transmit data. This is carried out by means of MSH-DSCH messages, which contain a list of information elements (IEs), classified by the IEEE 802.16 standard into the following four types. A *request IE* indicates that the requester has data addressed to the granter awaiting transmission, i.e., backlog. The granter reserves bandwidth for the requester using *grant IEs*, each containing a range of slots over a range of frames in a given channel. The same set of parameters is also used in *confirmation IEs*, which are used by the requester to complete the three-way handshake procedure. Finally, *availability IEs* can be used to report slots that cannot be used by the requester to transmit or receive data. The difference between coordinated and uncoordinated mechanisms lies in whether the signaling messages such as requests and grants have collisions. In the uncoordinated mechanism, collision is possible. Thus, an SS responding to a request must wait for a sufficient number of minislots before it sends out a grant, such that other SSs that sent requests earlier have an opportunity to respond with a grant.

Fair End-to-End Bandwidth Allocation

The bandwidth allocation problem in the distributed mode is left unsolved by the IEEE 802.16 standard, except for providing some control messages that may be used for this purpose, such as bandwidth requests and grants. To solve this problem, a fair end-to-end bandwidth allocation (FEBA) algorithm has been proposed [60], which can be used by IEEE 802.16 nodes to dynamically negotiate bandwidth in a distributed manner.

The basic idea of FEBA is that each node assigns bandwidth requests and grants in a round-robin manner where the amount of allocated bandwidth, in bytes, is proportional to the number of traffic flows weighted on their priorities. By keeping separate queues at each node for each traversing traffic flow, this tackles effectively the “spatial bias” problem found in other types of WMN, such as those based on IEEE 802.11 devices. Differentiated service is also provided by serving traffic flows proportionally to their priority. Furthermore, FEBA is able to react promptly to short-term variations of the traffic load in the network, because it is implemented in a fully distributed manner, and thus, it does not incur the overhead of signaling towards/from a centralized node.

With FEBA each node X maintains two virtual queues towards any of its neighbors, say Y: the *requesting* queue and the *granting* queue. The occupancy of the former, i.e., the requesting queue, is the total amount of backlogged bytes directed to Y. On the other hand, the total amount of data enqueued at node Y directed to node X is the occupancy of the granting queue. A granting queue is said to be active if there are *pending* requests, i.e., the receiver node has not granted the entire amount of bytes requested by the sender. Each active queue, both requesting and granting, is assigned a *weight* (ϕ) which is used by the bandwidth request/grant procedure below. The weight ϕ_i of any queue i is computed so that the amount of service is proportional to the number of traffic flows under service, weighted based on their priorities:

$$\phi_i = \frac{\sum_{j \in \mathcal{A}} w_j \cdot I_i(j)}{\sum_{j \in \mathcal{A}} w_j}, \tag{3.1}$$

where $\mathcal{A}$ is the set of all active traffic flows served by this node, j is an active flow with priority w_j, and $I_i(j)$ is an indicator function which equals 1 if j is under service at queue i, 0 otherwise. Since each traffic flow is under service at exactly one queue, $\sum_i \phi_i = 1$.

Requesting and granting active queues are then served in a round-robin fashion: at each round, queue i is entitled to serve $\phi_i F_{RR}$ bytes, where F_{RR} is a system parameter, called *target round duration*. If queue i is not eligible for service, the number of bytes that it could not consume is stored in a local variable. This *lag* will be consumed by queue i in subsequent rounds as compensation.

After a grant has been confirmed, its slots can be used by the requester for transmitting data, because FEBA uses the Deficit Round Robin (DRR) algorithm to select which packets are transmitted in the reserved slots, because it achieves fair queueing for variable length packets, can operate at $\mathcal{O}(1)$ complexity, and its implementation is easy.

3.1.6 MAC for Ultra-Wideband (UWB) WMNs

High speed wireless personal area networks (WPANs) can connect many consumer electronic devices in a small office home office (SOHO) environment. For example, high speed transmission of videos, HDTV signals, images, and large volumes of data are needed between camcorder, HDTV, video player, PC and so on. To support high speed communications in such an environment, UWB is the most promising technology, because it provides a high transmission rate and also demands low power consumption.

The MAC and physical layer technologies were standardized by IEEE 802.15.3. The first version of the standard was approved in 2003 [126]. In this standard, the MAC is still based on the piconet concept. However, the proposal from the WiMedia Alliance, approved by ECMA (European Computer Manufacturers' Association) has a different specification on the MAC protocol for UWB high speed WPAN. The MAC in the ECMA-368 standard [75] mainly consists of prioritized contention access (PCA) based on CSMA and distributed TDMA. Comparing the MAC between the ECMA-368 standard and IEEE 802.15.3, we can see that the superframe follows the same structure: a beacon period, contention access period (CAP), and contention free period (CFP). The differences lie in how the CAP and CFP are controlled and managed.

Neither IEEE 802.15.3 nor ECMA-368 has specified the mesh networking capability. However, there is an increasing demand that UWB-based WPANs need this capability for many reasons. One major reason is to increase network coverage without reducing transmission rate or increasing transmit power. Other reasons include improving reliability, avoiding single point of failure, and so on. Currently, the mesh networking capability is being specified in IEEE 802.15.5 [128]. However, the detailed proposal has not been finalized yet.

3.1.7 CDMA MAC

CDMA has been successfully applied to cellular networks, but few examples can be seen for WMNs. One of the most important reasons is that the CDMA transmitter and receiver will become complicated if a distributed multihop network is concerned. However, as the technology of advanced signal processing develops, CDMA will become an attractive multiple access scheme for WMNs because of several advantages in a WMN environment:

- Less sensitive to hidden node or exposed node issues [34]
- Higher network capacity
- More flexible in frequency spatial reuse
- The interference range can be smaller than the communication range [281]

CDMA is built based on spread spectrum technologies. There are two options: frequency hopping CDMA (FH-CDMA) or direct sequence CDMA (DS-CDMA). In FH-CDMA, interference between different users is avoided or reduced through different frequency hopping sequences. In DS-CDMA, orthogonal codes are used to mitigate the interference between users. To date, researchers have been more interested in DS-CDMA than in FH-CDMA, due to the different performance of DS spread spectrum (DSSS) and FH spread spectrum (FHSS). For moderate levels of interference within the spreading band, DSSS can tolerate and totally reject it, while FHSS may be completely jammed [187], although, for high level interference or interference out of the spreading band, FHSS has better performance. In many applications such as IEEE 802.11 wireless LANs, the concern is in-band interference due to the same industrial, scientific, and medical (ISM) band can be used by different devices. Such different performance also explains why FHSS in IEEE 802.11 was finally abandoned.

Although DSSS is an important multiple access scheme for IEEE 802.11b, and also IEEE 802.11g, it is not actually DS-CDMA, since all transmitters in these networks use the common pseudo-random noise (PN) code. Thus, it is infeasible to use a CDMA-based MAC protocol for DSSS-based IEEE 802.11 WMNs.

DS-CDMA MAC for WMNs

The design of a DS-CDMA MAC for WMNs includes the following challenges.

- *Distributed code assignment.* The PN codes allocated to nodes in the same neighbor must be distinct. Moreover, since the number of distinct codes is limited due to the constraints by the available spectrum and the required transmission rate, spatial reuse of these codes is necessary in WMNs.
- *Spreading-code selection for transmission and reception.* When signals are sent from a transmitter, the issue of whether the receiver's or the transmitter's spreading code is

used needs to be considered. If the receiver's code is used, collisions may happen due to the receiver receiving signals from two nodes hidden from each other and using the same receiver's code. Another issue is that broadcast must be performed by replicating unicast signals to different receivers. On the other hand, if the transmitter's code is used, broadcast is straightforward and no collisions exist that are due to hidden nodes. However, the receiver becomes complicated and expensive, because it has to monitor the activity of all PN codes.

- *Reducing multiple access interference (MAI).* PN codes generated by shift registers are nonorthogonal and orthogonal codes such as Walsh Hadamard codes become nonorthogonal due to multipath or partial-sequence cross-correlation. Nonorthogonal codes cause MAI, so the MAC must be designed to reduce MAI. One severe consequence of MAI is the well-known near-far problem in a CDMA network.

Distributed code assignment has been well researched [34], while spreading-code selection does not have too many options. Thus, the most challenging issue in the design of a DS-CDMA MAC is, given a scheme of distributed code assignment and spreading-code, to develop a method of reducing MAI.

In WMNs reducing MAI is much more difficult than in a cellular network. First, there is no central controller available to carry out joint scheduling and power control [76]. Distributed joint power control and scheduling is rather challenging. Second, the MAI mitigation schemes proposed for cellular networks may not work in WMNs, because it is hard to get accurate position or timing information needed by these schemes.

In [193], a controlled access CDMA (CA-CDMA) MAC protocol is proposed to reduce MAI. CA-CDMA considers two issues in the same protocol. One issue is that, in a multihop ad hoc network, two transmissions using different spreading codes may still not be able to occur simultaneously, no matter what power levels are used in these transmissions. This is an issue to be resolved by proper medium access. The other issue is that, when two transmissions can occur simultaneously, their power levels need to be controlled so that their interference to other users does not destroy reception. This is an issue to be resolved by both power control and medium access.

The CA-CDMA MAC performs joint power control and medium access based on an extended RTS/CTS procedure. Two frequency channels are assumed to be available: one for the control channel sending RTS/CTS messages, and the other for data transmissions. In CA-CDMA, a data packet cannot be sent as it arrives. Instead, it needs an admission control by checking if the transmission can start without disturbing ongoing receptions in other users. This is performed through RTS/CTS in the control channel. Firstly, an RTS message is used at the receiver to estimate the channel gains between transmitter and receiver pairs. Based on channel gains, the receiver calculates the needed transmit power level at the transmitter and the additional noise power that each of its neighbors can add to it. Then, a CTS message is sent by the receiver to notify its neighbors of the additional noise power level, and the transmitter of the transmit power level. Finally, each user keeps listening to the control channel to keep track of the average number of active users in the neighborhood. Since this RTS/CTS process can occur simultaneously at different users, the maximum level of additional noise power level indicated in CTS messages may not be satisfied, and thus still results in MAI. In [193], interference margin is used on each user to mitigate this problem.

Simulation results prove that the CA-CDMA MAC achieves much better performance than an IEEE 802.11 MAC in an ad hoc network. However, it also contains several drawbacks. The CA-CDMA MAC requires two frequency channels, which wastes bandwidth, unless the control channel is allocated with a much narrower bandwidth than the data channel. In addition, the channel characteristics of the control channel are assumed to be the same as those in the data channel. Since the same common PN code is used for all users, the contention probability in RTS messages can be high. More importantly, the CA-CDMA MAC is still an uncoordinated protocol. Without any coordination, the admission control of transmissions in different users can occur during the same time period. Considering a distributed scheme, such time-overlapping usually causes one transmitter–receiver pair's admission is in conflict with another pair's admission, and thus results in high MAI and failure in reception. Thus, design coordinated and controlled access CDMA MAC is an interesting research topic.

Another scheme proposed in [281] reduces MAI by inducing spatial clustering of contending nodes. This scheme is proposed based on the observation that receivers with simultaneous transmissions tend to be clustered if an ideal contention algorithm is applied to support parallel transmission in transmitter–receiver pairs. Theoretically, the spatial clustering algorithm is effective to reduce MAI. However, the way that the algorithm is implemented practically remains a question. If it is implemented following RTS/CTS procedures, it will have the same problems as observed in the CA-CDMA MAC protocol.

FH-CDMA MAC for WMNs

As explained above, DS-CDMA was favored by many applications owing to its quality in rejecting interference in spreading band. However, in distributed networks such as WMNs, FH-CDMA has several advantages over DS-CDMA [63, 260].

- FH-CDMA relaxes the dependence on power control and reduces the timing requirements. However, DS-CDMA needs more accurate synchronization among different users in order to reduce MAI.

- Upper layer protocols can be simpler for FH-CDMA. For example, there is no need to control orthogonal codes in different users and to ensure that the spreading-code does not result in collisions. However, all such work has to be done in DS-CDMA.

- In DS-CDMA, owing to difficulty in achieving high accuracy in synchronization in a distributed CDMA network, the interference can significantly reduce the network capacity. Thus, FH-CDMA can potentially achieve higher network capacity than DS-CDMA. DS-CDMA can achieve high capacity only if guard-zone [100, 193] or interference cancellation is applied.

However, to the best of our knowledge, no results have been reported on the design of FH-CDMA MAC for WMNs. Considering the advantages of FH-CDMA, developing FH-CDMA MAC becomes a promising research topic.

3.2 Multi-Channel Single-Radio MAC protocols

In the single-channel MAC protocol, since the interference range is much larger than the communication range, the time-spatial-reuse efficiency of a channel is low, and thus causes a significant drop of network capacity as the number of hops or as the number of nodes increases. In order to resolve the capacity limitation by interference, multiple channels can be used in the same network. In fact, many radios today can operate in different channels. For example, IEEE 802.11b/g radios can have three nonoverlapping channels, and the number of nonoverlapping channels in IEEE 802.11a is much larger.

In order to utilize multiple channels in the same network, there can be two options depending on the number of channels that work simultaneously on the same node. If a node has only one radio with a single transceiver, then the same node can only use one channel at a time, but different nodes in the same network can use different channels simultaneously. When a node has multiple radios, the same node can use multiple channels at the same time and different nodes in the same network can do the same. It should be noted that multiple radios on the same node can be implemented as multiple NICs or one NIC on which multiple radios reside via system-on-chip (SoC) or radio-on-chip (RoC) technique.

For either single-radio or multiple-radio nodes, a multichannel MAC protocol needs to be developed to efficiently utilize the available channels in the network.

When nodes have a single radio, different sender–receiver pairs need to use different channels at the same time. However, the channel associated to a sender–receiver pair cannot be fixed, because the traffic load on different sender–receiver pairs is time-varying. Thus, channels for these sender–receiver pairs need to be updated dynamically. Such a dynamical update demands an efficient MAC protocol, and also channel switching is needed on each radio.

Since single radio is employed, a single-radio MAC has the advantages of low cost and low complexity, as compared to a multiradio MAC protocol.

To date, several single-radio multichannel MAC protocols have been proposed [24, 236, 257]. However, none of them except the multichannel TDMA over CSMA/CA MAC protocol [257] has actually been implemented and applied in mesh networks.

3.2.1 Multichannel MAC (MMAC Protocol)

MMAC was proposed in [236] for ad hoc networks. However, since mobility was not a concern in the design, MMAC was actually more appropriate for WMNs.

MMAC assumes that the underlying techniques of a wireless node are based on IEEE 802.11 CSMA/CA protocol with RTS/CTS enabled. The target of MMAC is to solve the multichannel hidden node problem when the IEEE 802.11 MAC is applied for multichannel operation. Thus, before explaining the procedures of MMAC, we need to analyze the multichannel hidden node problem.

Multichannel Hidden Node Problem In the multichannel operation, any two nodes must negotiate for a channel. Such a negotiation process must make sure that the neighboring nodes are not using the same channel, in order to avoid collisions. However, a negotiation process, even one based on RTS/CTS, cannot achieve this goal. As shown in Figure 3.5, there are four nodes in a line topology: Nodes A, B, C, and D. In the beginning, Node A and Node B are

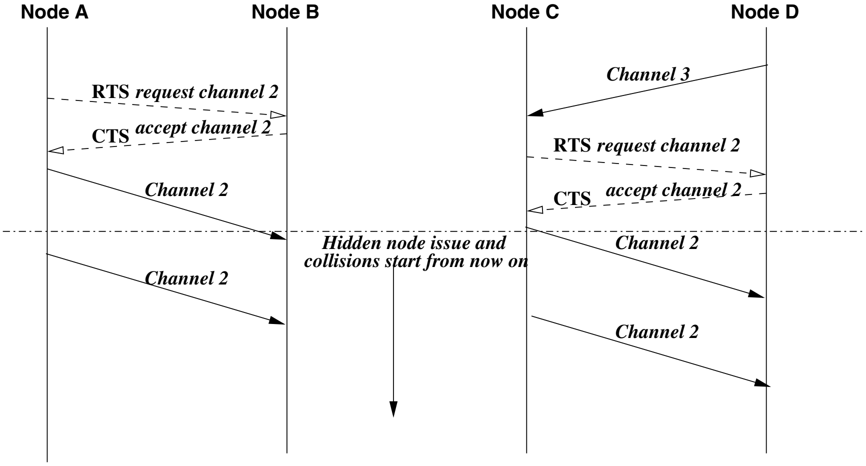

Figure 3.5 An example of multichannel hidden nodes

idle, while Node C receives packets from Node D in Channel 3. After some time, Node A has a packet for Node B, and thus needs to set up a channel to Node B. Node A does so by sending an RTS to Node B in the control channel, say, Channel 1. When Node B gets the RTS, it can select Channel 2, since it is not used by any other nodes. As a result, Node B sends back a CTS to tell Node A that Channel 2 can be used. Such a CTS is unknown to Node C, since C is in Channel 3. After RTS/CTS is done, Node A can start to send packets to Node B in Channel 2. At this time, Node C also has some packets for Node D, and thus, it also starts the RTS/CTS process to find the best channel. However, Node C also finds that Channel 2 can be used, because it does not know Node A is sending packets to B using Channel 2. Consequently, if Node D agrees that Channel 2 can be used, then Node C and Node D will also start to use channel 2 to send packets. Starting from this point, collisions will easily occur and no benefits of multichannel operation can be obtained, because all four nodes will use the same channel to communicate.

As we can see from the multichannel RTS/CTS channel negotiation process, the hidden nodes exist because of two problems: (1) Single transceiver limits the capability of a node in listening different channels; (2) Different channels in different pairs of nodes are not synchronized. Solutions to either problem can eliminate hidden nodes. However, when proposing a MAC protocol for single-transceiver nodes, we have no way of avoiding the first problem, and thus a solution must be proposed to solve the second problem. MMAC is one such solution.

Procedures of MMAC MMAC solves the multichannel hidden node problem based on a simple mechanism: the RTS/CTS based channel negotiation process is sure to be synchronized among all nodes. In such a way, channels for different pairs of communicating nodes will not interfere with each other.

MMAC adopts the synchronization mechanism of IEEE 802.11 to achieve the synchronization process of channel negotiation. Such a mechanism was initially proposed for power

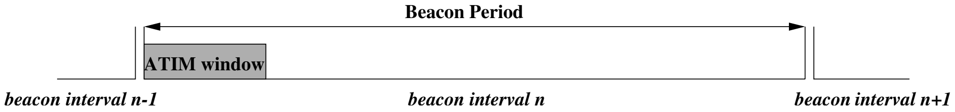

Figure 3.6 IEEE 802.11 beacon interval with ATIM window

management and also for ad hoc networking in the basic service set (BSS) of IEEE 802.11 networks. According to this mechanism, an announcement traffic indication message (ATIM) window in each beacon interval excludes the transmission of regular data packets. Other than beacons and other IEEE 802.11 related control and management frames, the ATIM window is reserved for control messages for the channel negotiation process. The ATIM window, time period for regular data transmission, and the beacon interval are illustrated in Figure 3.6. Since the start and end points of the ATIM window in all nodes can be synchronized through the time synchronization function (TSF) and beaconing procedures, the channel negotiation process in all nodes is thus synchronized. In Figure 3.5, if Nodes A and B perform the RTS/CTS procedures in the ATIM using the same channel as that used by Nodes C and D for RTS/CTS, then the channel negotiated by Nodes C and D will be different from that by Nodes A and B, and thus the multichannel hidden node issue is resolved.

Without the hidden node issue in multichannel operation, the next key step of MMAC is to develop a scheme to select the best channel. Two factors are taken into account to select a channel:

- **Preferable channel list.** Each node maintains a list of channels that are categorized into three different levels of preference.

  1. *High preference.* A channel that has been selected by a node in the current beacon interval has high preference. For each node, only one channel can be in the state of high preference.
  2. *Medium preference.* A channel with medium preference means that it has not been taken by the current node or other nodes in the transmission range of the current node.
  3. *Low preference.* When a channel has been taken by at least one neighbor of the current node, it is in the state of low preference.

- **Traffic load in a channel.** This parameter is used to evaluate which channel is the best to use. The objective is to balance the traffic load in different channels so that the channel with least traffic load is selected, and thus, there is a low chance of interference or collisions in the selected channel. In the original design of MMAC, the traffic load of a channel is represented by the count of source–destination pairs that have selected the channel.

Based on the preferable channel list and traffic load of a channel, the channel selection between source node S and destination node D is operated as follows.

- *Node S sends ATIM request to Node D.* In this ATIM message, the preferable channel list of Node S is attached. When Node D receives this message, it selects the channel based its own preferable channel list node's preferable channel list.

- *Node D selects a channel.* The channel selection process works as follows.

  - If there is a *high preference* channel in Node D's preferable channel list, this channel is selected. Otherwise, if a high preference channel exists in Node S's preferable channel list, it is selected.
  - When no *high preference* channel is available, *medium preference* channel is considered. If there is a channel in either Node S or Node D, such a channel is selected. When multiple such channels are available, an arbitrary one is selected.
  - If no channel is selected in previous steps, a *low preference* channel needs to be selected. In this case, the traffic load in each channel must be taken into account. The channel with the smallest number of source–destination pairs is selected.

- *Node D sends ATIM-ACK to inform S of the selected channel.* When Node D finds the best channel, it sends an ATIM-ACK messages with the selected channel attached. All D's neighbors can receive such a message and thus know that the selected channel will be used by Nodes D and S.

- *Node S channel conflict of selection.* Node S needs to make sure that the channel selected by Node D has not been taken by Node S. If Node S has taken this channel, the entire process of channel negotiation stops.

- *Node S sends an ATIM-RES message to Node D to reserve the channel for Nodes S and D.* If no conflict is found in the selected channel, Node S sends an ATIM-RES message to Node D. In this way, all A's neighbors will know that the selected channels will be used by Nodes S and D. Thus, via ATIM-ACK and ATIM-RES, all neighbors of both Node S and Node D will know that the selected channel will be used.

After a channel has been successfully selected between Node S and Node D, both nodes can be switched to the selected channel and can start transmissions using conventional CSMA/CA protocol.

Simulation results in [236] showed that the MMAC achieved higher throughput than both IEEE 802.11 MAC and dynamic channel assignment scheme in [270]. The average packet delay is also much lower than the other two MAC protocols. However, the overall design of MMAC is far from a practical MAC protocol that can be applied to WMNs. Several issues exist in this protocol, as explained next.

Issues in MMAC Several issues exist in MMAC. First of all, some assumptions are not necessarily valid.

- The actual channel switching speed is not 224 μs. This speed defined by IEEE 802.11 standard only counts the time of the physical channel switching. The overall channel switching time can be much larger, as time is needed for resetting and reconfiguration of different hardware registers and also for related MAC-layer processing of packets.

- Nodes may not be accurately synchronized for two reasons. First, time drifting is possible in some scenarios when TSF, as defined in IEEE 802.11 standard, is applied. Second, even though TSF works, time differences still exist between nodes. The inaccuracy of synchronization implies that the multichannel hidden node issue may still occur if no remedy is available.

Even if certain schemes are applied to solve the problems in the above assumptions, MMAC still has the following major issues.

- *Channel negotiation is inefficient and can be very slow.* Since ATIM, ATIM-ACK, and ATIM-RES are all sent in the ATIM window using the same channel for all nodes, collisions exist and become severe when the number of nodes increases. Once one of these messages is lost, the entire process fails, and thus another round will start after one beacon interval. Such a slow and uncoordinated process results in a long time for selecting a channel between two nodes, and thus cannot quickly capture the variable network dynamics such as variable traffic pattern or loads in the network. In other words, when network dynamics demand changes of channels between nodes, this process will always take a long time and thus results in very low performance in terms of throughput and packet delay.

- *The resource granularity is too large.* Once a channel is selected for two nodes, it will be used for the entire beacon interval. When the same node has packets for more than one destination, the destinations will have difficulty in sharing the resource. Once one destination uses a channel, all others have to be starved for at least one beacon interval. A simple solution is discussed in [236]. It allows a node to switch channels for different destinations within one beacon interval. However, this scheme does not match the channel negotiation procedure of MMAC. Moreover, even if channel switching can be done at the source node within the beacon interval, the destination does not know when a channel shall be switched.

- *The channel preference list may not be correct in priority.* The *high preference* category in the channel list may cause some nodes to be stuck in interfering channels. Suppose a network is busy because all nodes are sending packets to each other. Thus, some nodes in the same interference range have to choose the same channel. After a while, not all nodes send packets in the network. Thus, nodes should have a chance to use different channels for parallel transmission. However, since the channel selection process always selects the channel that was used before (i.e., the *high preference* channel) with the highest priority. Thus, the nodes using the same channel when the network was busy will continue to select the same channel with very high probability, since the negotiation messages are sent using a regular CSMA/CA protocol. As a result, nodes will be stuck in the same channel experiencing collisions for a long time until the CSMA/CA finally finds different channels for each source–destination pair.

- *Traffic load in each channel needs a better metric.* The count of source–destination pairs does not reflect the actual traffic load in each channel, since different pairs of connections can send packets with different traffic rates. A better metric is needed to factor in the traffic load for MMAC channel selection.

3.2.2 Slotted Seeded Channel Hopping (SSCH) MAC

SSCH [24] also works directly on top of the standard IEEE 802.11 protocol, for the benefit of easier deployment of this technology on existing IEEE 802.11 wireless networks.

SSCH consists of the following basic ideas.

- Different channel hopping schedules are used on different nodes so that: (1) interference between these nodes is as low as possible; (2) no logical partition exists in the network.
- In order to coordinate different channel hopping schedules on different nodes, channel hopping is performed slot by slot. Thus, nodes in the network need to be synchronized.
- The channel hopping schedule needs to be determined in a distributed way, since no central controller is available in WMNs.

With these ideas in mind, the critical component of SSCH is the distributed scheduling scheme for slotted channel hopping for mesh nodes.

Distributed slotted channel hopping In SSCH, each node is assumed to be capable of hopping from one channel to another slot by slot. Considering any time slot, if the channels of all source–destination pairs in the interference range are different, then no interference will occur, which is the best case for multichannel operation. To approach the best case, a scheduling scheme is needed to determine the channel hopping schedule that is as optimal as possible. Without a central controller in WMNs, SSCH relies on random process with a unique seed to generate independent channel hopping schedules. The details of the scheduling scheme are explained below.

In SSCH [24], each node maintains four time slots with different channel hopping sequences. However, for the purpose of generality, here we consider m time slots. Thus, the channel hopping schedule of each node is represented by m pairs of (channel, seed) and a rule for updating the channel in each (channel, seed) pair. Suppose the (channel, seed) pair of time slot i is (x_i, a_i), where x_i is updated as follows:

$$x_i \leftarrow (x_i + a_i) \mod n, \tag{3.2}$$

where n is the total number of nonoverlapping channels, x_i is the channel in the range of $[0, n-1]$, a_i is the seed in range of $[1, n-1]$, and i ranges from 0 to $m-1$. According to this rule, each of the n channels must have visited time slot i once after n updates. Thus, the same channel sequence will repeat after $m \times n$ time slots, and each node will have m such channel hopping sequences.

To have a better explanation of the channel updating scheme, an example is given in Figure 3.7, where $m = 2$, $n = 3$.

In SSCH, each node will follow the same rule given in 3.2. In order to have an effective MAC, the channel updating scheme must satisfy three requirements.

1. In order to avoid collisions, neighboring nodes need to have different channels in the same time slot. Thus, the channel hopping schedule must make sure that nodes that do not have data for each other reduce the frequency of channel overlapping as far as possible.

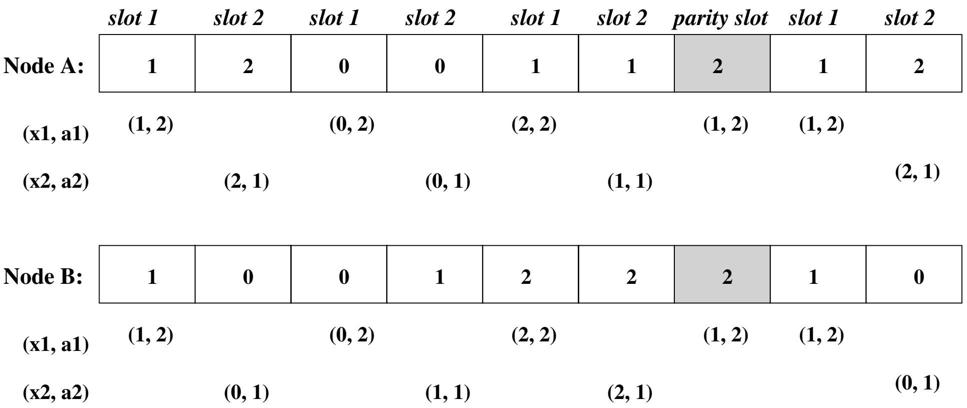

Figure 3.7 An example of channel updating in SSCH

2. Nodes that have data for each other must be guaranteed to have some channels overlapping in some time slots.

3. For any of two neighboring nodes, they must have a channel in common for some time. Otherwise, logical partition will occur in the network.

To evaluate the effectiveness of the channel updating scheme in 3.2, we consider three different scenarios of two nodes.

- *Seeds and channels associated with seeds are the same.* In this case, channels between two nodes are always the same. Thus, requirements 2 and 3 can always be guaranteed. However, requirement 1 will be violated if the two nodes do not have data for each other.

- *Seeds of these two nodes are different.* It can be proved that there is one channel overlapping between these two nodes after n channel updates. Thus, requirements 1, 2, and 3 can be satisfied. However, if the two nodes need to have more channels in common in order to send more data to each other, it cannot be satisfied.

- *Seeds are the same, but channels associated with seeds are different.* Thus, two nodes will never have a channel in common all the time. By simple calculation, the probability of having such a situation is extremely low. However, whenever there is such a case, these two nodes will not be able to communicate with each other, and this results in logical partition in the network. In order to avoid this problem, an additional time slot is added every other $m \times n$ time slots, and the channel in this time slot is always a_1. In this way, all nodes are guaranteed to have one overlapping channel within $m \times n + 1$ time slots. This additional slot is called a *parity slot.*

As explained above, with the parity slot, there is no logical partition in the network and the nodes are guaranteed to have an overlapping channel. However, the channel updating scheme provided in 3.2 cannot capture the network dynamics because of the variable traffic load between nodes. As a result, either collisions between nodes are high or nodes cannot get enough time slots with overlapping channels to send their packets.

In order to capture the network dynamics, a scheme is needed to carefully select (channel, seed) pairs in each time slot for each node. Unfortunately, no scheme was proposed in [24] to fulfill this task; only a simple approach was discussed. In this approach, a node examines the packet queue and selects (channel, seed) pairs such that the node has the best opportunity to send packets to the destination nodes. This approach is quite straightforward, but contains the following two issues.

1. The interest in receiving packets of this node is not considered.
2. Channel congestion is not taken into account.

In order to resolve the first issue, SSCH maintains a counter for each of the m slots, to measure the number of packets received in this slot during the period of one channel update iteration. If more than 10 packets are received, this slot is considered as a *receiving slot*. When selecting (channel, seed) pairs, only those in nonreceiving slots are allowed to change.

For the second issue, SSCH compares the (channel, seed) pairs of nodes sending packets to this node to the (channel, seed) pairs of other nodes. Given one (channel, seed) pair in a particular slot, if the number of other nodes is more than twice as many as the number of nodes sending packets to this node, we need to desynchronize these nodes. This can be simply done by changing the (channel, seed) pair of this node in the given slot.

Simulation results in [24] illustrated that SSCH achieved much better performance than an IEEE 802.11 MAC. However, it contains several issues that limit the performance in WMNs, as explained next.

Issues in SSCH Although SSCH improves the IEEE 802.11 MAC performance in WMNs, several issues still remain.

- *Assumption on channel switching delay is not realistic.* An 80 μs channel switching delay is assumed. However, this is impossible to achieve in any of the current IEEE 802.11 wireless cards. Channel switching delay is usually much larger due to different processing tasks involved in both MAC and physical layers. With a larger channel switching delay, the proposed mechanisms in SSCH may not be able to achieve the performance improvement, as shown in [24].
- *No scheme is available for selecting (channel, seed) pair.* In SSCH, only a simple approach is proposed to select a (channel, seed) pair for a node. However, this approach does not coordinate different (channel, seed) pairs between different nodes. Thus, the selected (channel, seed) on one node can easily conflict with that on another node, which will lose the advantage of multichannel communications. Although conditions of receiving slots and congested channels are considered in SSCH, the proposed scheme again does not have any coordination between different nodes. There is no guarantee that such a scheme can really ensure that the selected (channel, seed) pairs can satisfy the dynamic traffic load on all nodes.
- *The channel updating scheme may not be effective when the traffic load on a node changes quickly.* In order to capture network dynamics due to traffic load, (channel,

seed) pairs must be reselected dynamically. However, as explained in the channel updating scheme, one iteration of the channel hopping schedule needs $m \times n + 1$ time slots, which is a rather long period. When traffic load changes quickly, (channel, seed) pair will have been re-selected much earlier before one iteration of channel hopping schedule is completed. On the other hand, the effectiveness of the channel hopping scheme of SSCH totally depends on the stable and complete iterations of channel updates in each slot. Therefore, when traffic load changes quickly, SSCH does not really follow the required channel hopping schedule and the performance becomes unpredictable.

3.3 Multiradio MAC Protocols

With the multiple radios available, the MAC protocol has more freedom in resource allocation, and thus has two advantages over a single-radio MAC protocol. First, it does not always need to switch channels on a wireless radio, which will simplify the protocol design and also reduce the protocol overhead. Second, the multiradio MAC can potentially achieve higher network capacity than a single-radio MAC, since the same node can have simultaneous communications on different radios.

A multiradio system can be built following different architectures.

- *Multiple hardware platforms.* In this case, one radio is attached to each hardware platforms. For example, two single-radio mesh routers can be wired together using Ethernet to form one multiradio mesh router.

- *Single hardware platform.* Multiple radios are attached on the same hardware platform. For example, a mesh router with two wireless LAN card slots can be enhanced into a dual-radio mesh router.

- *Single-chip multitransceiver.* Multiple radios are integrated into one wireless chipset. Thus, only a single hardware platform and only a single wireless LAN card slot are needed.

Given a different architecture, the implementation details of a MAC protocol can be very different. However, the MAC protocol design can be the same no matter what architecture is used.

Although many research results have been reported on multiradio communications in WMNs, most of them are focused on how the channels are assigned on different radios rather than on how the MAC protocol is designed. The research work in the former case will be discussed separately in Section 3.4. In this section, we focus on the latter case. In particular, two protocols are studied: the *multichannel unification protocol* (*MUP*) [4] and the multiradio two-phase protocol [217, 218].

3.3.1 Multichannel Unification Protocol (MUP)

MUP [4] is a virtual MAC protocol that runs on top of multiple wireless interface cards (NICs). MUP assumes fixed channel assignment on each NIC, and the channels on the SAME NIC must be orthogonal. With such a channel assignment, the key task of the MUP on a node becomes selecting the best NIC for each neighbor of this node. In order to determine the best NIC, certain performance metrics must be measured in the network. Thus, MUP includes the following major functions.

- discover neighbors and identify node MUP-capability
- measure the channel quality on each NIC
- select the NIC with the best channel quality
- switch NICs based on variable channel quality on NICs

Neighbor discovery and classification The address resolution protocol (ARP) is used to record the MAC addresses of all neighboring nodes. ARP is one-layer higher than the MUP layer, and thus an ARP request can be captured by MUP, and broadcast on all NICs. A node, whether or not MUP-enabled, will send back an ARP response when it receives the ARP request. In order to find MAC addresses on multiple neighbors and also on multiple NICs on each neighbor, the ARP request needs to be sent for multiple times until timeout occurs.

After the MAC addresses of all possible NICs in each neighbor are resolved, a MUP discovery process is started to find out if a neighbor is a MUP-enabled node. This is done by sending a channel select (CS) message. A MUP-enabled node will respond with a CS-ACK message, while a legacy node will not. When this process is completed, a MUP neighbor table is maintained in each MUP-enabled node. Typically, one entry of a neighbor in the MUP neighbor table contains the following information.

- IP address of the neighbor
- MUP-capability of the neighbor
- this neighbor's MAC addresses that can be resolved by the current node
- the channel quality corresponding to each MAC address
- the last time that a channel selection was made
- the last time that a packet was sent from a NIC of the neighbor
- the list of times for unacknowledged probe messages

The first three items are learned when neighbor discovery and classification is done. All other items will be collected and used in other functions of MUP.

Channel Quality Measurement and Selection of NICs for Communications MUP selects the NIC with the best quality by sending a probe message and measuring the RTT after receiving a response from neighboring nodes.

RTT measurement provides the overall quality estimation on both transmitting channels and receiving channels. It is based on the round trip time from sending a CS message to receiving a carrier sense (CS)-ACK message with the same sequence number of the CS message. This measurement is done by sending CS/CS-ACK messages periodically. In order to let probe messages be sent out first, a priority queue is formed. Thus, MUP relies on IEEE 802.11e to make it work. To smooth the measurement, RTT is updated according to a simple weighted averaging scheme:

$$SRTT_n = \alpha * RTT_n + (1 - \alpha) * SRTT_{n+1}, \tag{3.3}$$

where $SRTT_n$ is the smoothed RTT based on RTT_n, the current measurement of RTT, and the last smoothed RTT.

The probe messages CS or CS-ACK can be lost, so MUP needs a scheme to detect packet loss in these messages. Two schemes are used in MUP. One is based on the sequence number of CS and CS-ACK. If out-of-sequence occurs, MUP knows a probe message is lost. In case the sender has not received CS-ACK within a certain period, e.g., three times the current SRTT, it assumes that packet loss has occurred in probe messages.

Loss of probe messages increases RTT. To take this factor into account, if packet loss of probe messages is detected, the SRTT is increased by three times.

Switch Channels Once a channel is selected, MUP needs to stick with it for a long time period. This period is determined by a random process and is of the order of 10–20 seconds. After the random time period, all channels are measured again through probe messages. If a channel has a certain amount of quality improvement (e.g., $>10\%$) over the existing channel, then that channel is selected as the new one for sending packets. Reordering of packets may happen when packets in the old channel have not been finished. MUP does not include a solution to this problem.

Issues in MUP According to the procedures of MUP, we notice that several issues remain unresolved.

- *Hidden node issue is not solved.* The channel quality measurement is based on one-hop RTT. However, measurements based on shortest RTT do not guarantee that there are no hidden nodes. For example, suppose Nodes A and C are hidden from each other and Node B is a neighbor of both A and C. When Node *A* measures channels, it sends a CS message to neighbors, and Node C cannot hear it, but Node B can receive it and sends back a CS-ACK message. When Node A receives the CS-ACK message, it selects channel 1 (as an example) to send packets. By this time, CS-ACK should have been received by Node C. However, MUP does not have a procedure for Node C to process the CS-ACK message for Node A. Thus, Node C has a very high probability of selecting channel 1 and send packets to Node B. As a result, collisions occur at Node B. Although RTS/CTS can be used to reduce collisions, it causes a large percentage overhead. In order to eliminate this problem, the channel selection procedure needs to be revised.

- *RTT measurement does not reflect traffic load.* Thus, a NIC with good link quality but congested traffic load may be always selected for communications.

- *Channel switching mechanism is not justified.* MUP allocates a random time period for each selected channel. Performance of this scheme cannot be guaranteed, because the time of having the best quality in a channel is definitely not randomized. The time is related to the wireless channel characteristics and interference from nodes using the same channel.

- *Packet reordering is needed when channels are switched.* MUP relies on TCP to handle this issue. This may not be appropriate for a multihop network, because it will cause low end-to-end throughput.

- *Channel allocation on each NIC is not optimal.* Without a global algorithm, the orthogonal channels allocated in NICs of different neighboring nodes can easily cause conflict, which results in severe interference when neighbors select NICs with the same channel.

- *The MAC addresses of a neighbor may not be always detected.* When different orthogonal channels are assigned in two neighboring nodes, some MAC addresses of a node cannot be detected by another. This means that nodes will lose the advantage of multiradio operation.

3.3.2 Multiradio Two-Phase Protocol

The multiradio two-phase protocol is designed specifically for WMNs with long-distance point-to-point links. Thus, directional antennas are used on each radio of a node. The initial design of the multiradio two-phase protocol did not intend to use multiple channels [217]. Instead, the multiple radios on a node use the same channel to send packets to, or receive packets from, different nodes simultaneously on directional antennas.

Although directional antennas are used, side lobes of directional transmission prevent simultaneous transmission and reception on antennas of the same node. However, simultaneous transmissions or simultaneous receptions on all antennas are feasible if the power level on each antenna is carefully controlled. Thus, to efficiently utilize multiple radios with directional antennas, the MAC must be designed so that all antennas on each node are either in transmission phase or reception phase. Thus, in the multiradio two-phase protocol, all nodes repeat operations in two phases: SynTx and SynRx. When a node is in the SynTx state, all neighbors of this node must be in SynRx state. As shown in Figure 3.8, all nodes must be synchronized and operate in a TDMA mode. In the first time slot, when A sends packets to C and B, D also sends packets to C and B. In the second time slot, B sends packets to A and D, and C must also send packets to A and D. In all following time slots, the same operation must be followed, and no other scenarios are allowed.

This example illustrates that the successful operation of the protocol depends on three factors.

1. Nodes need to be synchronized to allow repeated SynTx and SynRx operations.

2. The network topology needs to be bipartite.

3. The power level on each antenna is carefully controlled to ensure correct receptions at the highest rate.

Synchronization The synchronization in the multiradio two-phase protocol is needed for simultaneous packet transmissions and receptions on different interfaces of all nodes.

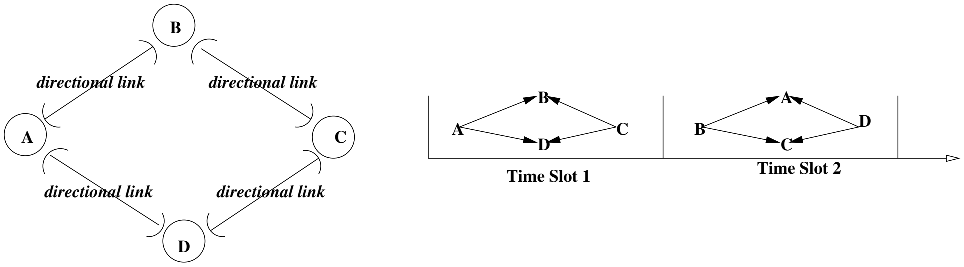

Figure 3.8 An example of SynTx and SynRx operations in the multiradio two-phase protocol

Since the underlying radio is based on IEEE 802.11, certain control over the operation of IEEE 802.11 is needed in order to ensure synchronization.

The first control to be taken is to disable the ACKs in the MAC layer. The multiradio two-phase protocol achieves this by converting all unicast packets from the higher layer into broadcast packets. When ACK is needed, it is implemented in the multiradio two-phase protocol rather than the default function done by IEEE 802.11 hardware.

The second control over the legacy IEEE 802.11 radio is to disable carrier sense based backoff. In the multiradio two-phase protocol, this is achieved by controlling different operations on the two antennas on the same interface. Suppose one antenna is called *antenna 1*, and the other one is called *antenna 2*. Moreover, *antenna 1* is connected, and *antenna 2* is disconnected. In the SynTx state, *antenna 2* is selected, while *antenna 1* is selected in the SynRx state. Thus, when packets are sent on a radio, it does not experience any interference except for some noise, since *antenna 2* is disconnected. In this way, carrier sense is disabled in SynTx, and thus no backoff will occur.

It should be noted that synchronization in the multiradio two-phase protocol is in the sense of packet level instead of clock level, and thus only loose rather than strict synchronization is acceptable. The loose synchronization is achieved by passing a special packet called a "marker packet" between nodes when the period of SynTx is over. When a neighbor in the SynRx state receives the special packet, it switches into the SynTx state.

When the "marker packet" is lost, nodes will be out of synchronization, and thus a timeout mechanism is needed to resume synchronization. The scheme works as follows. A node in the SynRx state starts a timer when it enters this state. If a "marker packet" is not received before the timer expires, it will generate such a special packet by itself and start its SynTx state. Via this simple mechanism, the out-of-synchronization issue due to loss of the special packet can be resolved. To avoid repeated timeouts, however, some random delay can be added after the timer expires before sending a "marker packet" [217].

Bipartite Topology In the multiradio two-phase protocol, if a node is in the SynTx state, all its neighbors must be in the SynRx state. This requirement can be satisfied if and only if the graph of the formed topology is bipartite. A graph is called bipartite when its vertices can be decomposed into two disjoint sets such that no two vertices within the same set is adjacent.

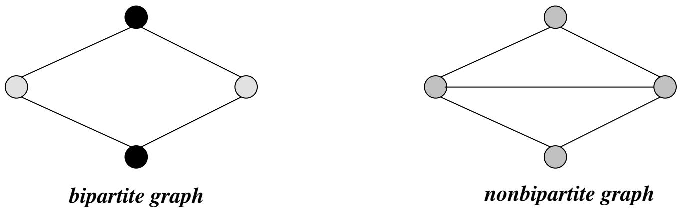

Figure 3.9 Bipartite topology versus nonbipartite topology

As shown in Figure 3.9, the network in the first scenario is a bipartite graph, while that in the second scenario is not. In other words, if a WMN has a topology as shown in the second scenario, then the multiradio two-phase protocol will not work.

To achieve a bipartite topology, the multiradio two-phase protocol depends on a careful topology formation scheme [217].

Power Constraint In the multiradio two-phase protocol, the transmit power level on each interface must be determined so that two conditions are satisfied.

- The received signal at a receiver must be above the level that supports the highest transmission rate.
- In case of loss of synchronization, the interference experienced by a receiver must be higher than the required signal-to-interference-noise ratio (SINR) for a given bit error rate (BER).

For the first condition, the received power level of each interface is calculated by an equation considering the antenna gain, path loss from a transmitter to a receiver, and the transmit power level and satisfying the highest transmission rate. Since the transmit power level is a variable to be determined only one variable is involved in this equation. Since the entire WMN is modeled as a bipartite graph, only two sets of nodes are considered and a node in one set does not transmit to another node in the same set. Thus, the number of equations for meeting the requirement of the first condition is twice as large as the total number of links between the two sets of nodes.

For the second condition, the received power level of each interface on a node is interfered with by the signals from nodes in the other set that lose synchronization. Due to the bipartite topology, the total number of equations for this condition is the same as that for the first condition. However, each equation for this condition is much more difficult, because transmit power levels in different radio interfaces are involved in the same equation.

By solving the above equations, the transmit power levels of each interface on each node are determined. However, if such a power level cannot be found, it means the bipartite topology is not feasible.

Multichannel Operation The initial design of the multiradio two-phase protocol assumes the network to be bipartite. In addition, the capacity of links between two sets of nodes is symmetrical. These two assumptions do not in fact match many application scenarios.

For example, in general the topology of a WMN is not bipartite. Also, for wireless networks, the traffic on different directions of the same link can be rather different.

In order to relax these two assumptions, multichannel operation is taken into account in the multiradio two-phase protocol [218]. The key idea of the enhanced protocol is to use multiple channels to divide an arbitrary network topology into multiple bipartite subgraphs. In each bipartite subgraph, the same protocol in [217] can be applied. Also, for each subgraph, the ratio of capacity in one direction to the other direction is different from that of another subgraph. Thus, the critical task of the enhanced multiradio two-phase protocol is to select a feasible channel allocation so that: (1) the network topology can be split into bipartite subgraphs; (2) the capacity ratio of two directions in each subgraph matches users' needs. As proved in [218], this is a nondeterministic polynomial-time (NP)-hard problem, and thus heuristic schemes are proposed. However, no matter what heuristics are used, there is no guarantee that a feasible channel allocation can be found given an arbitrary topology of a WMN.

Issues in the Multiradio Two-Phase Protocol The multiradio two-phase protocol takes a different direction in designing a multiradio WMN. Simulation studies show that it is effective for achieving much better performance than an IEEE 802.11 WMN. However, it is only applicable to point-to-point links since directional antennas are used. This is in fact not the case for many application scenarios. Moreover, even in the scenario with point-to-point links, the protocol still has the following issues.

- *Multiple radios are not well utilized.* In a bipartite graph, all radios can only use a single channel. Such a constraint limits the utilization of radios, since different radios can inherently use different channels to improve throughput. Moreover, in order to achieve directional transmission, the number of required radios may be large if a node has many neighbors.

- *The end-to-end delay can be large.* This is due to the requirement for simultaneous transmission or reception on all radios. This is because, when a radio receive packets, it has to buffer the packets before they can be forwarded to other nodes via a different radio.

- *Bipartite is not always possible, even with multiple channels.* For many applications, it is impossible to get such a network topology. The protocol does not include a scheme to adjust power levels on each radio so that a bipartite graph can be achieved.

- *Power control does not work together with topology control.* The power level is determined in order to satisfy the required transmission rate and signal quality. However, if a different power level is used, the topology may be changed too.

- *Locations need to be known for power control.* In reality, this is hard to get unless the network size is small and the network topology is simple.

Some issues such as low utilization of radio and large end-to-end delay have been researched recently involving a new channel allocation scheme in [74]. More specifically, the improvement is made by allowing the same link to have different channels in two directions and making sure that no common channel is used for transmitting and receiving packets.

This scheme is effective in theory, but in many cases it is not effective. In 802.11 wireless networks, two noninterfering channels located on the same node may still interference with each other if transmission and reception are used on each radio respectively, which is a well-known problem.

3.4 Channel Assignment in the MAC Layer

Channel assignment is always a key step to a multichannel MAC protocol. It has been considered in all existing MAC protocols. However, many MAC protocols [24, 236] do not include an algorithm that can optimally allocate channels to nodes on the basis of interference between nodes and network dynamics due to variable traffic load. Thus, better channel allocation is needed to improve the performance of the MAC protocol.

In [216], a channel allocation scheme is proposed based on minimizing the interference among neighboring nodes. A coordinated channel allocation scheme is performed in [258] to determine nonconflict time slot and channel allocation for distributed multichannel TDMA MAC of 802.11 mesh networks. In [270] an on-demand and dynamic channel assignment scheme divides all available channels into a common control channel and multiple data channels and divides the available interfaces into one control interface and several data interfaces. The control interface is assigned to the control channel permanently. Here each node keeps a list of current idle (CUL) and free channels (FCL). When Node A wants to communicate with Node B, it sends an RTS message and its FCL on the common control channel. The receiver node compares its FCL with the sender's FCL, and selects an idle channel (if any) and then includes that information in its CTS message. Then, Nodes A and B switch their data interfaces to the selected channel and begin data transmission.

Some channel allocation algorithms are proposed for a specific type of WMN such as the rural WMN [74,218] or WMNs with a centralized root node [21]. In [21] a channel allocation algorithm is developed based on distance-1 edge coloring (D1EC) for WMNs that have a gateway node as the root of the entire topology, and traffic in the network mostly goes to, or comes from, the gateway. If D1EC exists for a graph, channel assignment for the network will be contention-free. However, for arbitrary network topologies, the D1EC problem may be NP-complete, or D1EC may not exist. Thus, a heuristic scheme is proposed based on D1EC as follows. If D1EC exists, then a heuristic mechanism is used to find the result; otherwise, the algorithm tries to minimize the interfering channels. As a result, in the D1EC channel allocation algorithm some links will get contention-free channels, and remaining links get channels with minimum interference. Moreover, such interference information is helpful for the MAC protocol to contend a channel more efficiently. The D1EC based channel allocation algorithm aims to maximize the aggregate network throughput of single-radio WMNs. It is a static allocation scheme, and thus is not applicable to application scenarios where traffic load varies a lot. For a general type of WMNs, this algorithm is not applicable either.

For multiradio WMNs, channel allocation can be done by using a particular coding scheme such as superimposed code [275]. In this scheme, each node maintains a channel codeword which indicates a set of primary and secondary channels of this node. Based on information of the local node and its neighboring nodes, the channel allocated to this node is determined. The superimposed code based channel allocation scheme contains a few problems. Firstly, it assumes that each node has the same number of radios, which is not the case for a common

WMN. In an extreme case such as single-radio WMNs, it is not applicable either. Secondly, the traffic activity in each radio of a node has to be homogeneous. Otherwise, the channel assignment per radio rather than per link is not an efficient scheme. Thirdly, the number of noninterfering channels is not necessarily much larger than the number of radios. For example, in 802.11n, the number of noninterfering channels is small, as channel bonding needs two regular 11a channels for one 11n channel. Fourthly, it is difficult to know which node is the interfering node and sometimes it is impossible. Thus, channel allocation based on channel codeword information of interfering nodes is not always feasible. Lastly, how this algorithm works together with a MAC protocol is unknown.

Note that the channel assignment is closely related to the routing protocol. On the one hand, the channel assignment affects the selection of a routing path. With a different channel assignment, the capacity on the same link can be very different. Considering this fact, for the same end-to-end traffic flow, a routing protocol may choose a different routing path if the channel assignment is different. On the other hand, the routing protocol affects the traffic load on each link, which then demands the channel assignment scheme to satisfy the bandwidth requirement on each link. Therefore, as part of a MAC protocol, channel assignment can also be a part of a routing protocol. In other words, in order to improve the performance of both MAC and routing protocols, channel assignment in a mesh network demands a cross-layer solution between MAC and routing layers. Some theoretical results of joint optimization between channel assignment and routing have been reported in [16, 249].

Channel assignment is also related to congestion control. In [90] a channel assignment algorithm is proposed by considering congestion control for a multiradio WMN. It is an interactive scheme to gradually decompose the problem into two subproblems: congestion control and channel assignment. In one iteration, after the congestion control subproblem is solved with a convergence, the congestion information is exploited by the channel allocation subproblem. The result of the channel allocation captures new interference, and such information will be used by congestion control in the next iteration. How this congestion control oriented channel assignment is integrated with a MAC protocol is not investigated in [90].

An example of joint channel assignment with routing and MAC protocols can be found in [213]. However, the cross-layer cooperation of routing solutions, MAC protocols and channel assignment algorithms remains an open research issue in multichannel WMNs.

3.5 Dynamic Frequency Selection (DFS) Requirements

When multichannel operation is adopted in a radio, certain regulations must be followed. For example, in IEEE 802.11a, although there are 12 nonoverlapping channels, it does not mean that the MAC protocol can use any of them, because the IEEE 802.11a devices may interfere with radar signals [119], which is not allowed in many countries including European Union, USA, and Japan. In order to use these channels without causing interference to radar signals, DFS requirements specified by different standards must be satisfied.

Although different standards specify different procedures and system parameters for DFS, the requirements follow the same framework, as explained below.

- In a network, the device that can initiate communications must follow DFS. Since any node in a mesh network can do so, DFS must be available in every mesh node.

- The first step of DFS is to check the availability of a channel before the channel can be selected. The time during which a channel is checked is called channel availability check time. Usually, at least 60 seconds are needed to check the channel availability.
- When a channel is available, a node starts to use the channel for communications. However, the node should continuously monitor for radar signals.
- Once radar signals are detected, the node should initiate a move to another channel. This means that the node needs to tell all neighbors using the same channel to close the channel. The time from detecting a radar signal to closing the channel is called the channel move time, which is usually at most 10 seconds. During this period, the total transmission time needs to be controlled too. The total transmission time is called the channel closing transmission time, which is at most 260 milliseconds.
- Once the old channel is closed, the node starts to check another available channel. After the channel availability check time has passed and a new channel is found, the node switches to the new channel. At the same time, the node needs to ensure that the old channel cannot be used within a nonoccupancy period. Usually, the nonoccupancy period is at least 30 minutes.

For a multichannel MAC protocol, when it is adopted in a product, a certain scheme must be proposed to follow DFS. In this sense, all the existing multichannel MACs in the literature need to be re-evaluated by taking into account DFS.

3.6 Open Research Issues

A summary of different categories of MAC protocols for WMNs is given in Table 3.1.

Based on the discussions in the previous sections, the main open research problems are summarized as follows.

- *Scalability:* The scalability issue in multihop ad hoc networks has not been fully resolved yet. Most of the existing MAC protocols based on CSMA/CA solve partial problems of the overall issue, but raise other problems. For example, multichannel or multiradio MAC can improve multihop throughput performance by adding more frequency channels. However, such schemes usually result in higher system complexity and higher cost, and an effective channel allocation is still an open research problem, even though many algorithms have been proposed recently.
- *Cross-layer design:* When advanced techniques such as MIMO and cognitive radios are used in the physical layer, novel MAC protocols considering MAC/physical cross-layer design need to be proposed to utilize the agility provided by the physical layer. Moreover, hybrid ARQ can be added as a MAC/physical cross-layer function to improve error control capability of WMNs. When multichannel operation is considered, MAC and routing become an integral problem rather than a separate one.
- *Heterogeneous access technologies:* Some mesh routers in WMNs are responsible for the integration of various wireless technologies. Thus, advanced bridging functions must be developed in the MAC layer so that different wireless radios such as IEEE

Table 3.1 Comparisons of different MAC protocols for WMNs

Category of MAC protocols	Subcategory (some examples)	References	Features
Single-channel MAC protocols (can be extended to multichannel operation)	CSMA/CA variants	[43, 62, 247]	Improve CSMA/CA for WMNs by fine-tuning parameters such as contention window, carrier sense, backoff procedure, etc.; not a solution to scalability
	802.11s MAC	[123]	Based on 802.11e; not scalable for WMNs
	TDMA over CSMA/CA	[256]	A true TDMA is designed overlaying CSMA/CA, scalable performance needs compatibility solution
	TDMA MAC for UWB mesh	[75, 128]	Distributed MAC for WMNs is not finalized; MAC/routing cross-layer design is expected
	TDMA MAC for 802.16 mesh	[60, 130]	MAC procedures are specified in standard, but distributed resource allocation schemes are expected
	CDMA MAC for WMNs	[34, 193]	High performance in interference rejection, no hidden node issue, high complexity
Multichannel MAC (single- or multiradio)	MMAC	[236]	Single-radio operation, assumes fast channel switching, channel negotiation may be slow in covergence and cause high overhead due to a packet-level algorithm
	Multichannel TDMA over CDMA/CA	[257, 258]	Designed for single-radio, but can be easily extended for multiradio; true multichannel TDMA MAC, scalable performance
	SSCH	[24]	Single-radio operation, assumes synchronization among nodes, conflict in channel allocation, slow in capturing dynamic network parameters
	MUP	[4]	Multiradio operation, virtual MAC protocol, channel assignment is not optimal, hidden node issue is not resolved
	Multiradio two-phase MAC	[217]	Multiradio operation, assume point-to-point links based on directional antennas, synchronized tx/rx on all radios of a node, possible low utilization for a radio, large end-to-end delay

802.11, 802.16, 802.15, etc., can work seamlessly together. Reconfigurable/software radios and the related radio resource management schemes may be the ultimate solution to these bridging functions.

- *QoS support:* Most of the existing research efforts in MAC are focused on capacity, throughput, or fairness. However, many applications need to support broadband multimedia communication in WMNs. Thus, the development of MAC protocols with multiple QoS metrics such as delay, packet loss ratios, and delay jitter is an important topic for WMNs.

- *Reconfigurable MAC:* Reconfigurable MAC enables the freedom of new inventions added to the MAC protocol and the cross-layer design between MAC and other protocol layers such as physical and routing. However, the challenge is that usually both software and firmware are involved in MAC protocol implementation. A promising trend in MAC chipset design is that the architecture becomes more and more reconfigurable. When software radios become mature enough for commercial use, more flexible and powerful MAC protocols can be easily developed.

4

Network Layer

In this section we discuss a group of routing protocols developed for WMNs. Consequently, we will learn how the network topology information can be discovered, what routing metric can be used, and more importantly how such components can be integrated with the routing path selection schemes in various routing protocols. We will also learn what principles need to be followed when designing new routing protocols.

WMNs share many common features with ad hoc networks. Thus, the routing protocols developed for ad hoc networks can usually be applied to WMNs. For example, mesh routers of Firetide Networks [81] which use topology broadcast based on reverse-path forwarding (TBRPF) protocol [203], Microsoft mesh networks [190] which are built based on dynamic source routing (DSR) [137], and many other companies use routing protocols based on ad hoc on-demand distance vector (AODV) algorithm. AODV is also the major building block for the routing framework of IEEE 802.11s [122].

Despite the availability of many routing protocols for multihop wireless networks, especially for mobile ad hoc networks, the design of routing protocols for WMNs is still an active research area for several reasons.

- New routing metrics need to be discovered and utilized to improve the performance of routing protocols. The most frequently used metrics so far for routing protocols include hop count and link quality. However, they are far from satisfying the need of routing for WMNs because finding an optimal route depends on various design objectives and network characteristics of WMNs.

- For mobile ad hoc networks (MANETs), the major concern for routing is high mobility in all nodes; complicated procedures are needed to support such mobility. However, such complexities are not necessary in WMNs, because mesh routers usually have minimal mobility. Thus, efficient and lightweight routing protocols need to be developed to achieve satisfactory performance in WMNs.

- The routing protocols for other multihop wireless networks treat the underlying MAC protocol as a transparent layer to routing. However, the cross-layer interaction must be considered in order to improve the performance of the routing protocols in WMNs.

Wireless Mesh Networks Ian F. Akyildiz and Xudong Wang

- The requirement on power efficiency is much different between WMNs and mobile ad hoc networks. In a WMN, nodes in the backbone have no constraint on power consumption, while client nodes usually desire the support of a power-efficient routing protocol. Such differences imply that the routing protocols designed for mobile ad hoc networks may not be appropriate for WMNs.

Considering the features of WMNs, we believe that a routing protocol for WMNs must take into account the design principles as discussed in Section 4.2. Network layer protocols of WMNs need to be adaptive to variable network topology, traffic load variations, and other uncertainties. Owing to the wireless medium and interference among different nodes in a multihop wireless mesh environment, WMNs experience much more severe uncertainties than a single-hop wireless network. For example, a link can easily be broken, which demands a routing protocol to have an efficient and fast fail-over performance. In general, maintaining stable network topologies and routing paths in WMNs is nontrivial.

To select a routing path in WMNs, the routing algorithm needs to consider possible unreliable network topology due to the multihop wireless environment. In addition, the routing path selection is intertwined with resource allocation, interference avoidance and rate adaptation across multiple hops. Mobility in WMNs is less challenging than in MANETs, which is an advantage for designing protocols for WMNs and makes the performance of a routing protocol tractable in a multihop wireless mesh environment. However, as compared to MANETs, WMNs have other challenges for routing protocol design.

4.1 Routing Challenges

A routing protocol can be formulized as an optimization problem: given any source and destination, finding a routing path that achieves the best performance, subject to a number of constraints such as network topology and interference.

Although the optimization objectives vary from one routing algorithm to another, it must obey the *optimality principle*, i.e., if an intermediate Node R is on the optimal path $p_{X,Y}$ from Node X to Node Y, then the optimal path $p_{R,Y}$ from R to Y must be on the same route of $p_{X,Y}$. Based on this principle, optimal paths from all sources to a destination form a sink tree, rooted at the destination. It should be noted that a sink tree is not necessarily unique, because there exist multiple routing paths from the same source to the same destination, but achieving the same performance. As a result, a routing protocol is equivalent to a process of discovering different sink trees and utilizing such trees to form a routing path for any source and destination.

However, in reality the problem of routing is much more complicated, especially when a multihop wireless network like WMN is concerned. Below is a summary of the factors that make routing a more challenging task than just finding routing paths based on sink trees.

- **The network topology can be variable and inconsistent.** The major reasons include:
    - Links between nodes can be up and down, which is particularly true in a wireless network owing to interference, fading, and so on. Such link variations can cause an inconsistent view of network topology by different nodes in the same network.
    - Similar to link variations, the network topology can also be changed due to node mobility or other node activities such as joining or leaving the network.

- **Depending on the performance goal in routing, it may not be possible to determine a routing path solely based on the network topology.** The typical scenarios include:
  - The routing metric is more than just a topology parameter. For example, if only hop count is considered, routing path selection is only concerned with the network topology. However, as other routing metrics are considered, e.g., the delay, the routing path selection is not only related to the network topology, but is also affected by interference from nodes without being on the selected routing paths. Such routing metrics cause two complications: (1) selection of one routing path is coupled with that of another routing path; (2) determining routing path is coupled with resource allocation mechanisms including channel allocation, medium access control, power control, and so on.
  - Routing path selection has to consider traffic distributions in the network in order to achieve load balancing. However, traffic distribution is also a result of routing. Thus, load balancing and routing are closely coupled with each other. Concerning WMNs this problem is much more complicated, because the traffic load of a link impacts multiple links in the interference range.
- There may not be an optimal solution for a given routing problem. As explained before, routing is coupled with many other functions such as resource allocation schemes. In addition, the selection of one routing path may be dependent on another one. Considering such a complicated optimization problem with potential conflict constraints, an optimal solution may not be available.

When routing is considered under the framework of optimization, it is usually formulized as a global or centralized optimization problem. Such a methodology is not applicable to a practical routing protocol. Thus, there is another challenging issue for routing: how to design a distributed routing algorithm to approximate the optimization solution of a global routing algorithm.

4.2 Design Principles

In order to resolve the above challenging issues, some principles need to be considered in the design of routing protocols.

- *Maintaining a consistent and stable network topology.* There are two options to handle inconsistency in the network topology. One is to design a routing protocol in such a way that it is capable of detecting and also resolving inconsistencies. Considering the distributed network architecture of WMNs, this approach usually increases the complexity of a routing protocol and deviates the performance from the optimal result. Thus, a more effective approach is to rely on a topology discovery scheme to acquire a consistent network topology. This approach is part of a routing protocol, but needs to work together with topology control and management schemes. In WMNs, especially infrastructure WMNs, the mesh routers tend to be static, so links can be reliable within a large timescale. As a result, it is possible to develop a topology discovery scheme to ensure that all nodes have a consistent view of the network topology. In addition to the previous schemes, if location information is available, it must be utilized to compensate the instability of network topology.

- *Performing dynamic and adaptive routing.* A routing protocol for WMNs needs to be adaptive to variable conditions in the network and, thus, routing paths must be dynamic instead of static. The variable conditions can be the changing network topology or traffic distribution. The network topology can be controlled to be stable and consistent within a certain time frame, but may be different in different time frames. A routing protocol needs to be adaptive to capture such changes. For traffic distribution, it is generally determined by the distribution of users, their demands, and the traffic patterns. Thus, the traffic is not necessarily uniformly distributed in the network, so a routing protocol needs to be adaptive to variable traffic conditions. A routing protocol should also be adaptive to unexpected changes in the network topology such as link and node failures, out-of-network interferences, etc.

- *Developing new routing metrics.* In wireless networks, one of the earliest routing metrics being used is the hop-count. It is a simple metric, and a routing protocol based on minimum hop-count can always work for WMNs and has the advantage of simplicity. However, such a routing protocol may leave a huge gap between its actual performance and the expected performance goal. Usually the performance goals of a routing protocol of WMNs include supporting QoS, maximizing resource utilization, and increasing network throughput. A routing protocol based on minimum hop-count tends to counter such goals, because of the following typical problems.

  – Minimum hop-count can lead to congestion, as traffic flows tend to follow the same routing path.

  – Minimum hop-count is not necessarily the best routing path, because links on a routing path with more hops may provide higher transmission rate, experience less interference, etc.

  – Minimum hop-count does not take into account the interactions between different routing paths, but this is always the case for WMNs.

  In spite of these problems, the hop-count is still frequently used in some routing protocols because of its simplicity. In addition, many routing protocols still use hop-count as the basic routing metric but incorporate enhancements to improve the performance. However, it is critical to develop new routing metrics for WMNs in order to truly satisfy the performance goals. It should be noted that such routing metrics do not exclude hop-count as one of the routing metrics, since a routing protocol can integrate multiple routing metrics.

- *Considering tradeoff between cross-layer design and single-layer solution.* In WMNs, resource allocation in the MAC layer and link quality provided by the physical layer closely impact the selection of a routing path. Thus, cross-layer interactions between routing and MAC and physical layers are inevitable. To take into account such interactions, cross-layer design can be employed. Such an approach makes the implementation of protocols more complicated as no transparency exists in the network. Another approach to consider cross-layer interactions is to map the interactions or constraints of other protocol layers onto a routing metric. Thus, routing and MAC or physical layer are decoupled into separate problems, but their interactions are still considered through the routing metric. In this approach, it is critical to design the routing metric in such a way that the dynamic interactions or constraints between different protocol layers can be properly reflected. For example, if a routing metric is developed based on link quality which further takes into account the transmission rate, medium access control mechanism, and interference, routing can use such a link quality based routing metric to determine routing paths without directly working together with a MAC or physical layer scheme.

- *Deriving distributed algorithms for routing.* In WMNs, the selection of one routing path is dependent on, or impacts, the selection of another routing path. Such inter-path coupling demands that the routing paths of the entire network be determined under the same optimization formula. This usually requires a global optimization algorithm. For practical implementation, a centralized routing scheme based on global optimization is not scalable, so a distributed routing algorithm is preferred. To derive such a distributed scheme, theories on distributed algorithms are needed. It is also important to make sure that: (1) the distributed algorithm is an accurate approximation to the centralized solution; (2) the global optimization is not an ill-conditioned problem.

- *Ensuring scalability in routing.* Scalability is always a concern, as a routing protocol is expected to work efficiently in WMNs with various sizes. The routing protocol must keep a minimum overhead. As shown in [44], overhead can have a multiplicative impact on the data traffic and severely degrade the performance of a routing path for data traffic. It is preferred to work in a distributed rather than centralized way. Another effective approach is to employ hierarchical routing to virtually split the network into different sectors: each hierarchy level maintains a separate routing function for its corresponding sector of networks. The challenge of this approach is how to coordinate the inter-routing between different sectors. Nevertheless, hierarchical routing is favored by WMNs, as it allows the size of WMNs to grow without significantly increasing the burden on a routing protocol.

- *Adaptively supporting both mesh routers and mesh clients.* Considering the minimal mobility and lack of constraint on power consumption in mesh routers, a much simpler routing protocol can be developed for mesh routers than existing ad hoc routing protocols. Routing in mesh clients has to consider power efficiency and mobility support, but shall not follow the routing methodology developed for mobile ad hoc networks. Instead, mesh clients should collaborate with mesh routers to reduce the complexity of the routing protocol.

As discussed in the above design principles of a routing protocol in WMNs, we know that the major components of a routing protocol include network topology discovery, routing metrics, and routing algorithms. In the rest of this section, these three components are discussed in three separate subsections.

It should be noted that, in order to integrate the above three components in the same protocol, a routing protocol usually has other supporting components or needs assistance from other protocols. For example, a signaling protocol may be required to manage the network topology formation. Also, certain procedures must be designed to transfer routing-related messages across the network. However, in this section these supporting components are not studied separately. Instead, they are discussed wherever necessary.

4.3 Topology Discovery for Routing

Many factors impact network topology formation. Typical examples include link quality, network node mobility, node availability, network deployment, and so on. Through network topology, these factors impact the design and also performance of a routing protocol. Thus, to properly determine the network topology information is a critical function for a routing protocol.

Topology discovery can be done in a centralized or distributed way. However, the distributed discovery scheme is a better choice for WMNs, because WMNs are inherently a distributed multihop network. Topology discovery provides the network topology knowledge and other related information to a routing protocol.

The focus of topology discovery is to find the up-to-date topology information for mesh nodes. To this end, an efficient information exchange scheme is needed to distribute and collect topology information, and thus the following issues must be considered.

- *Frequency of information exchange.* The frequency must be in a fine granularity so that the topology change due to network dynamics can be captured. However, if the frequency is too high, too much information will flow through the network, and thus waste the precious resources of WMNs.

- *Contents of signaling messages.* When a node exchanges topology information with its neighboring nodes, the information to be included in a signaling message depends on working mechanisms of a routing protocol. In order to reduce protocol overhead, a routing protocol should use as little topology information as possible.

- *Approach for information exchange.* This is concerned with finding the most efficient approach for information exchange. Broadcasting may be a reasonable solution when links are reliable, because information can be sent to all neighbors by one message. However, when link quality is not stable, broadcasting is not an effective approach; without acknowledgement, messages can be lost easily. Although retransmissions can be applied to increase the chance of receiving the same message, there is no way to determine how many retransmissions are really needed to guarantee message reception at all nodes due to the lack of acknowledgement. To resolve this issue, unicasting has to be used to exchange topology information. Whether broadcasting or unicasting is employed, we need to consider the tradeoff between the overhead of messages and the accuracy of topology information.

Topology discovery may be hindered by multichannel or multiradio operations, which are common in WMNs. For example, in a multichannel or multiradio WMN the channel assignment or radio selection may be determined together with a routing algorithm. If the network topology discovery depends on the selected channels or radios for links between mesh nodes, then the network topology is uncertain to a mesh node before the routing algorithm selects routing paths. However, topology information is still needed, because the routing algorithm depends on the topology discovery to learn all possible topologies in a multichannel or multiradio WMN, and then determines the best routing paths along these possible topologies. To avoid such a conflict between topology discovery and channel selection, an effective approach is to collect network topology information without relying on channel or radio selection. For example, neighboring mesh nodes can temporarily switch to a common channel to exchange topology information and then fall back to the original channel once topology information exchange is completed.

For some WMNs, location information of mesh routers, and even mesh clients, may be available. In this case, the location information of each node needs to be efficiently delivered to other nodes. Based on nodes' location information, the inaccurate network topology can be compensated for or even geographic routing protocols can be developed.

4.4 Performance Parameters

The ultimate goal of a routing protocol is to find a routing path for any (source–destination) pair but also to achieve the best performance. The performance parameters are diverse and can be defined at different levels of the networking systems.

- *Per-flow parameters.* Per-flow parameters include QoS parameters such as delay, packet loss ratio, and delay jitter and other parameters such as hop-count, per-flow throughput, and intra-flow interference.

- *Per-node parameters.* The performance required by a node includes computation complexity and power efficiency.

- *Per-link parameters.* For a link between two nodes, performance parameters such as link quality, channel utilization, transmission rate, and congestion need to be considered.

- *Inter-flow parameters.* Inter-flow parameters capture interactions among different traffic flows on different links. Typical examples include inter-flow interference and fairness.

- *Network-wide parameters.* In order to support QoS for each traffic flow, a routing protocol is expected to consider overall network performance, and thus, needs to consider network-wide parameters such as the total throughput of a network.

From the users' perspective, the above performance parameters can be classified into two sets: *direct* and *indirect* performance parameters. The former set includes QoS, throughput, and power efficiency. These parameters are visible to users because they represent the performance that can be directly experienced by users. All other parameters fall into the latter set, as they are invisible to users; their impact is only indirectly reflected in QoS, throughput, or power efficiency.

It should be noted that the above parameters are neither independent nor totally overlapping. Thus, they cannot be processed separately and one parameter cannot substitute another one. Consequently, how to capture these cross-related parameters by one routing metric is a very interesting problem. However, as these parameters are so diverse and reside at different levels of the network hierarchy, it is an extremely difficult research problem to develop a routing metric to capture all such parameters. Basically, theoretical breakthroughs are necessary to achieve this goal. In practice, all routing metrics proposed so far only capture a subset of the above performance parameters. Because of such a limit in routing metrics, all existing routing protocols do not really deliver optimal performance for users and the entire network; only the performance parameters captured by the routing metric are actually optimized. The existing routing metrics proposed for WMNs are discussed next.

4.5 Routing Metrics

A routing protocol has to rely on a particular routing metric to determine the "distance" between any source and destination. Based on such distances, routing paths are then decided by a routing algorithm. The actual meaning of the "distance" varies with different routing metrics. For example, if hop-count is used as a routing metric, then the "distance" between a source and a destination means the number of hops between these two nodes. Depending on different optimization goals, different types of distances must be used in a routing protocol, which leads to the need to develop different routing metrics. For example, if delay is more important than the number of hops, then the routing metric must be able to capture the delay on each link so that the distance of a routing path can be represented by the overall delay on this path.

A routing metric can be developed to capture one performance parameter or multiple performance parameters. In the latter case, the routing metric can be derived in single protocol layer or multiple protocol layers. Thus, routing metrics can be classified into three types: (1) metric for single performance parameter; (2) single-protocol-layer metric for multiple performance parameters; (3) multi-protocol-layer metric for multiple performance parameters.

4.5.1 Hop-Count

Hop count is a simple routing metric, because it only needs to know if a link exists or not. However, because of this on/off feature, the hop count cannot provide helpful information about a link, such as packet loss, link quality, etc. Thus, routing protocols based on hop-count only consider one performance parameter, i.e., the minimum hop-count of each routing path. In a very few cases the minimum hop-count is a reasonable metric to find a good routing path. However, in most cases the minimum hop-count is not enough for a routing protocol to achieve a good performance. Nevertheless, the hop-count is used in some existing routing protocols for WMNs, mainly because of its simplicity. In some application scenarios, if reachability instead of optimized performance is the main concern, the hop-count is a useful routing metric.

4.5.2 Per-Hop Round Trip Time (RTT)

Per-hop RTT can be measured by sending unicast probe packets between neighboring nodes and calculating the time spent on the probe-ack procedure, as discussed in [4]. Usually a weighted moving average is needed to get a smoother measurement, because one sample cannot really reflect the actual link status. Based on per-hop RTT, a routing protocol selects a routing path with the least sum of RTTs of all links on the path. Per-hop RTT is able to capture the packet loss ratio in a link, the traffic load and queuing delay in two nodes on the link, and the contention status in all neighboring nodes. However, its effectiveness is constrained by two problems. One is that per-hop RTT is too much dependent on the traffic load/queuing delay, which interferes with the accuracy of per-hop RTT and thus can easily lead to route instability. If a separate queue is assigned to probe packets, then it can accurately measure the link quality but cannot reflect the traffic load. A solution to this problem is to adopt a link measurement scheme proposed in [146]. Another problem is that the accuracy of per-hop RTT measurement totally relies on the weighted moving average scheme. If the variations in measurements are large, then the per-hop RTT has no way to get a reliable value, no matter what weight is applied in the weighted moving average scheme. The overhead of the probe-ack procedure of per-hop RTT needs to be carefully justified, because a node has to send probe packets to all its neighbors. It should be noted that per-hop RTT captures per-link performance parameters, although measurement is actually carried out at the network layer.

4.5.3 Per-Hop Packet Pair Delay

Per-hop packet pair delay (PPD) is measured by sending two back-to-back probe packets from a node to its neighbor. The first probe is a small packet, while the second one is large. When the neighbor receives these two packets, it finds the delay in between them and then sends such information back to the probing node. This method was proposed for wired networks [144] and reinvestigated in [70] for WMNs. Since relative delay is used to measure the per-hop delay, per-hop PPD measurement is less impacted by queueing delays or traffic load in a node. However, this impact still exists, because whether or not being able to send probe packets in a link of two nodes also depends on the queueing delays of other neighboring nodes. This is especially true for a mesh network. For example, when Node A sends probe packet to B, if A's neighbor C is also sending a very high traffic load to A, then A has to delay its probe to B. Therefore, per-hop PPD still has to capture the route instability issue. Moreover, this measurement scheme causes a larger percentage overhead than per-hop RTT, owing to the need for more probe packets. Its performance is also dependent on the weighted moving average scheme [70], and assumes the variation of measurements is small.

Similar to per-hop RTT, per-hop PPD only captures per-link performance parameters.

4.5.4 Expected Transmission Count (ETX)

The ETX of a link is the expected number of transmissions before a packet is successfully delivered on a link. For a route, the ETX is the sum of the ETXs on all links. The link ETX can capture the link quality and packet loss on both directions of a link. In addition, the route ETX can detect interference among links of the same route; the larger the route ETX, the less self-interference on the route.

ETX is estimated based on probe packets [67]. Every period of τ seconds a node sends a broadcast probe message to all its neighbors. Each neighbor records the number of received probe messages (denoted by n_w) during a period of w seconds, where $w > \tau$. Thus, the delivery ratio of sending a packet from the probing node to its neighbor is $n_w/(w/\tau)$. If a probing node embeds the information of n_w from all its neighbors in the probe packet, then each of its neighbors can derive the packet delivery ratio from the neighbor to the probing node. With the delivery ratio in both forward and reverse directions, denoted by d_f and d_r, respectively, ETX is calculated as ETX $= 1/(d_f \times d_r)$.

ETX has a lower overhead because broadcast rather than unicast is applied to probe messages. ETX does not measure delays, so the measurement based on probe messages is not impacted by queueing delays in a node. However, ETX has several other problems. The first problem is that probe messages in fact experience different packet loss ratios from unicast messages because broadcast messages usually use more robust modulation and coding schemes, and thus have low transmission rates. The second problem is that ETX does not take into account the differences in packet size for different traffic flows and the different capacities for different links. The third problem is that the estimation method in ETX may not be accurate, as it relies on the mean loss ratio; however, wireless links usually experience bursty losses. Moreover, a route based on ETX ensures that packets flow through a high capacity path with a high link quality and low self-interference, but this feature tends to cause bottle-neck routes in the network, unless a load-balancing algorithm is designed and runs in parallel with the routing protocol based on the ETX.

In spite of the above problems, ETX is able to reflect per-link performance and, to some extent, the per-flow performance and, accordingly, the network-wide performance.

4.5.5 Expected Transmission on a Path (ETOP)

When a routing path is selected in many routing protocols, the position of a link is not considered in the routing metric. For example, when ETX is used to determine a routing path, only the value of ETX on each link matters. In other words, considering two routing paths, only cumulative ETX value matters when determining which path will be selected. This is true if the link layer has an infinite number of retransmissions, because a retransmitted packet has the same impact no matter at which link retransmission happens. However, if the link layer has a limited number of retransmissions, end-to-end retransmission has to be carried out. Thus, comparing two links, even if their ETX is the same, the one closer to the destination can result in higher transport layer retransmissions, which means that this link could lead to worse performance if it were selected.

ETOP solves the above problem by taking into account the relative position of a link on a routing path when the routing cost of the path is calculated [135]. Considering a routing path with n links from node v_0 to node v_n, its cost is denoted by T_n. For a packet to be delivered end to end through this routing path, the needed number of end-to-end attempts is assumed to be Y_n. Moreover, in an end-to-end attempt j, the number of links that a packet has traversed before it is dropped by the link layer is denoted by M, and the number of link layer transmissions at node j is assumed to be H_j. The ETOP of a routing path is the expectation of T_n and is given by:

$$\mathbb{E}[T_n] = \left(K + \sum_{j=0}^{n-2}(\mathbb{E}[H_j|H_j < K]\mathbb{P}[M > j|M < n])\right) \times \mathbb{E}[Y_n - 1] + \sum_{j=0}^{n-1}\mathbb{E}[H_j|H_j < K]. \tag{4.1}$$

As shown in the above equation, ETOP captures the total number of link layer transmissions of a given routing path under all possible end-to-end attempts.

Compared to ETX, ETOP can improve transport layer throughput, because a routing path is selected with a least number of overall link-layer retransmissions. However, a certain algorithm is needed to derive ETOP based on other parameters that can be measured in an easy way. In [135], an equation has been derived to calculate ETOP from the expected number of transmissions in the link layer. It is derived based on two assumptions: the link layer transmission is assumed to follow the same random process for different nodes, and the link layer transmission in different attempts is independent and has identical distribution. These two assumptions are not really true in a WMN, because links experience different interference, path loss, fading, etc.

4.5.6 Expected Transmission Time (ETT) and Weighted Cumulative ETT (WCETT)

ETT can be viewed as an extended version of ETX. Based on ETX, ETT considers the impact of both packet size and link quality as follows [71]: ETT $=$ ETX$\frac{S}{B}$, where S is the packet size and B is the link bandwidth. Thus, ETT reflects the expected packet transmission time on a link. For a routing path, the expected transmission time can be the sum of ETTs of all links on the path. However, such a scheme does not take into account the channel diversity in WMNs using multiple radios at some nodes. To resolve this issue, a routing metric called WCETT is proposed in [71]:

$$\text{WCETT} = (1 - \beta) \sum_{i=1}^{n} \text{ETT}_i + \beta \max_{1 \leq j \leq k} X_j, \tag{4.2}$$

where n is the number of hops on a routing path, k is the number of available channels for multiradio operation. In addition, $X_j = \sum_{\text{Hop } i \text{ on channel } j} \text{ETT}_i$, so, $\beta \max_{1 \leq j \leq k} X_j$ finds the bottleneck channel of a given routing path. Thus, in equation (4.2), the first term considers the overall expected transmission time of the routing path, while the second term captures the transmission time on the bottleneck channels. In this way, WCETT takes into account the tradeoff between overall routing delay and channel diversity utilization.

ETT enhances the performance of ETX by mapping packet size and link bandwidth into the transmission time. However, it uses a similar estimation scheme as that of ETX, so it has similar problems as ETX, i.e., inaccurate estimation, bottleneck routes, etc. WCETT is not applicable to WMNs based on single-radio multichannel operation for two reasons: (1) broadcast probe messages cannot be sent on different channels of the same radio simultaneously; (2) the channel switching time can be comparable to the ETT of a link.

4.5.7 Effective Number of Transmissions (ENT)

In order to consider both mean loss ratio and variance of links on a routing path, an expected number of transmissions is proposed in [150] to be $mETX = \exp(\mu + \frac{1}{2}\sigma^2)$, where μ and σ^2 are the mean and variance of the packet loss ratio. Based on this concept, a quality-aware routing metric called ENT is derived. In ENT, the end-to-end packet loss ratio of a route cannot exceed a threshold. To satisfy this QoS requirement, two parameters are derived. The first one is the upper bound of expected transmissions M. The second one is a parameter δ, which needs to be included into *mETX* to get *ENT* as follows: $ENT = \exp(\mu + 2\delta\sigma^2)$. Moreover, if $ENT > \log(M)$, the weight of the corresponding link should be infinity.

ENT improves the estimation accuracy of link quality of ETX and also supports the quality-aware routing. However, it is built on top of ETX, so other shortcomings of ETX still exist in the ENT.

4.5.8 Metric of Interference and Channel-Switching (MIC)

MIC aims to consider both inter-flow and intra-flow interference [282]. For inter-flow interference, an interference-aware resource usage (IRU) is proposed for a link l between node i and node j using channel c as

$$\mathrm{IRU}_i = \mathrm{ETT}_i + N_{ij}(c), \tag{4.3}$$

where $N_{ij}(c)$ is the number of nodes interfered with by node i and node j while they transmit in channel c.

To consider intra-flow interference, a channel switching cost (CSC) metric is proposed as follows. For a node i on a routing path, if its incoming hop and outgoing hop use different channels, then $CSC_i = w_1$; otherwise, $CSC_i = w_2$, and $w_2 > w_1$.

Based on the above two metrics, MIC of a path p is then given by

$$MIC_p = \frac{1}{N \times \min(ETT)} \sum_{\text{link } l \in p} IRU_l + \sum_{\text{node } i \in p} CSC_i, \tag{4.4}$$

where N is the total number of nodes in the network.

Although MIC tries to consider both intra- and inter-flow interference, it has a few problems. Firstly, *ETT* is a parameter that has considered all interference experienced by a link, which questions the accuracy of IRU. Secondly, the intra-flow interference CSC does not really reflect the actual interference, but only differentiates same-channel from different-channel communications in consecutive hops. Link quality is not captured in CSC. Moreover, the actual channel switching time is not represented by CSC.

4.5.9 Bottleneck Link Capacity (BLC)

BLC is derived based on the expected busy time (EBT) of transmitting a packet on a link [177]. EBT can be estimated by considering the packet loss rate (PLR) and transmission mechanism in the MAC layer. For example, if RTS-CTS-Data-Ack handshake is used for packet transmission as in an IEEE 802.11 MAC, then the EBT can be calculated as $T_{\text{handshake}}/(1 - e_p)$, where $T_{\text{handshake}}$ is the total transmission time of one RTS-CTS-Data-Ack, and e_p is the PLR. Based on EBT, the residual capacity of a link is defined as the ratio between the idle time and EBT. Considering a path P, if the residual capacity of link i is LC_i, then BLC is given by

$$\mathrm{BLC} = \frac{\min_{i \in P} \mathrm{LC}_i}{\mu^K}, \tag{4.5}$$

where K is the length of the routing path P and μ is a fine-tuning parameter. Thus, BLC indicates the residual capacity of the bottleneck link of a routing path. Moreover, dividing the minimum residual capacity by a certain number is for penalizing a long routing path.

Because busy time is considered in BLC, load-balancing in links has been taken into account. However, the self-interference of a routing path is not considered, as the minimum residual capacity is considered in BLC. In other words, if two routing paths have different self-interferences, then the bottleneck link can have the same residual capacity. The same problem applies to interference from other routing paths.

4.5.10 Expected Data Rate (EDR)

EDR integrates the expected transmission count and the expected transmission contention degree (TCD) into the same routing metric. The TCD of a link is the time that is spent on retransmitting nonacknowledged packets over a given period. Considering link k on a routing path, if the sum of TCDs of links that interfere with link k is I_k, then the EDR of link k is

$$\mathrm{EDR}_k = \frac{\Gamma}{I_k\ \mathrm{ETX}_k}, \tag{4.6}$$

where Γ is the maximum transmission rate of link k.

For the EDR of a routing path, it is defined as the EDR of the bottleneck link.

EDR has some problems. First of all, ETX integrates two closely related parameters: ETX and TCD. In fact, given the same packet length, if ETX is large, TCD is large too. Thus, why ETX and TCD have to be combined as in equation (4.6) remains a question. Secondly, even if the link rate is considered in the metric, it does not consider the fact that multiple rates, instead of only the maximum rate, are available in each link. A third problem with EDR is that the interference range of a given link k is difficult to determine, so I_k is hard to derive. The EDR of a routing path cannot take into account the self-interference, as the EDR of a bottleneck link is used as the EDR of the entire routing path.

4.5.11 Low Overhead Routing Metric

To estimate routing metric, a procedure for sending probing messages or collecting neighbor information is needed. This can cause overhead. Thus, some researchers [142, 183] have proposed using available information in the management information base (MIB) of a MAC layer to derive a routing metric.

In [142], a link quality and congestion aware (LQCA) metric is proposed based on the *ACK Failure Count* (fc_{ACK}) and *RTS Failure Count* (fc_{RTS}) to determine the routing metric. Firstly, the frame transmission efficiency of a node is defined as $FTE = 2/(fc_{ACK} + fc_{RTS})$. The FTE of a path is the multiplications of all nodes on the path. Secondly, the LQCA routing metric is defined to be $FTE_P \times (1 - hop_P/N)$, where FTE_P is the FTE of the routing path P, hop_P is the hop count, and N is the number of nodes in the network. Thus, LQCA captures the link quality and congestion through *ACK failure count* and *RTS failure count*, and it also penalizes long paths through hop-counts. The accuracy of this routing metric totally depends on the performance of the MIB metric. In addition, the failure counts are usually defined per node instead of per link. Thus, the link-related quality is not accurate, as these failure counts are averaged over all links from the same node.

In [183], the network allocation vector (NAV) in MIB is used to derive a routing metric. For each node, an average NAV count (NAVC) is calculated over a certain period. Based on this average NAVC, the congestion status of the network is estimated and mapped to the delay and bandwidth performance. For example, if the average NAVC is over 0.65, the node is considered congested and it contributes the path NAV sum for any routing path involving this node. However, if it is below 0.2, there is no contribution to path NAV sum. Again, the average NAV is a per-node metric instead of per-link, so it does not reflect any link quality. Moreover, how accurate the NAVC can be for representing QoS parameters such as packet loss or delay remains an open issue.

4.5.12 Airtime Cost Routing Metric

To identify an efficient radio-aware path among all the candidate paths, the airtime cost metric is proposed as a default routing metric in IEEE 802.11s draft [122]. It reflects the amount of channel resources consumed for transmitting a frame over a particular link. The path which has the smallest sum of airtime cost is the best path.

The airtime cost C_a for each link is calculated as

$$C_a = \left[O_{ca} + O_p + \frac{B_t}{r}\right]\frac{1}{1 - e_{pt}}, \tag{4.7}$$

where O_{ca}, O_p, and B_t are constants whose values depend on the used transmission technology. O_{ca} is the channel access overhead, O_p is the protocol overhead, and B_t is the number of bits in a test frame. The r and e_{pt} are the bit rate in Mbit/s and the frame error rate for the test frame size B_t, respectively.

The above discussed routing metrics are listed in Table 4.1, where their different characteristics are compared.

As shown in the table, many routing metrics try to capture link-layer performance parameters by using a procedure in the network layer. In fact, these schemes can be enhanced by performing link-quality measurements directly in the link layer and then using such measurements in the network layer. Such a method implies that the routing metrics should involve cross-layer interactions.

4.5.13 Remaining Issues

Although so many routing metrics are available for WMNs, several issues still exist.

- The measurement or estimation method for a routing metric may not be accurate. It may also cause a large overhead, especially for a large scale network.

- Performance comparisons between different routing metrics need further research, although some work has been done for a few routing metrics [70].

- The design of many existing routing metrics is still “ad hoc”. In other words, why the proposed routing metric can improve the network performance is not really justified; usually only simulation results are used to prove the effectiveness of a routing metric. The side-effect of such a design is that the effectiveness of a routing metric may be limited to a certain type of WMN.

- A routing metric may not be able to capture enough network parameters for a routing protocol to optimize the network performance. For example, existing routing metrics are mainly derived based on link qualities to replace hop-count. However, few routing metrics have considered how to capture QoS or throughput parameters in a routing metric, which, however, is critical in WMNs.

Thus, it is necessary to continue to carry out research on routing metrics for WMNs. In particular, new routing metrics that better serve the optimization goal of a routing protocol are needed.

Table 4.1 Comparison of different routing metrics for WMNs

Routing metrics	Perform at what layers	Captured performance parameters	Advantages	Shortcomings
Hop-count	Network	Number of hops	Simple and low overhead	Minimum hop-count is usually not the performance goal
Per-hop RTT	Network	Packet loss, traffic load, queuing delay, contention	Multiple link metrics captured	High overhead in sending probes; estimation accuracy depends on traffic load
Per-hop PPD	Network	Packet loss, transmission delay, contention	Multiple link metrics captured, less impacted by traffic load	High overhead in measuring delay; performance dependent on the measurement accuracy; no load balancing
ETX	Network	Packet loss, retransmission, contention	Captured multiple link metrics, relative lower overhead by using broadcast	Measurement is not accurate due to differences between broadcast and unicast; no load balancing; cannot capture packet loss variations; can have bottleneck link
ETOP	Network, Link	End-to-end attempts, link retransmission	Link position considered in routing	Difficulty in deriving the metric
ETT& WCETT	Network	Same link metrics of ETX and also link bandwidth and packet size	Improve ETX by considering link bandwidth and packet size; channel diversity is considered	Same problems as ETX; not applicable to single-radio multichannel operation
ENT	Network, Link	Packet loss its variance end-to-end packet loss	More accurate estimation of packet loss than ETX; guarantee of end-to-end packet loss	Overhead in collecting packet loss and its variances; other problems of ETX still exist
MIC	Network	Inter-flow and intra-flow interference, other link metrics like ETX	Consider both inter- and intra-flow interference together with ETT; support multichannel operation	The method of integrating ETT and interference level is questionable; hard to estimate interference level; channel switching is not considered
BLC	Network, Link	MAC handshake, time, packet loss rate, hop count	Residual capacity of a link is considered, so load-balancing is performed indirectly	Bottleneck link of a route does not consider self-interference
EDR	Network	Link metrics as that in ETX, contention time	Use contention time of all interfering links to consider interference	Has the same problems as those in ETX; hard to find interfering links

Table 4.1 Continued

Routing metrics	Perform at what layers	Captured performance parameters	Advantages	Shortcomings
LQCA	Network, Link	RTS and ACK failure count, hop count	Only MIB is used, no probing needed, low overhead	There is no per-link metric; MIB information may not be accurate enough for routing
NAVC	Link	Average count of NAV	No probing needed, low overhead	Has the same problems as LQCA
Airtime cost	Link	Resource consumed by a packet on a link	Captures the impact of the dynamic environment to a link	Overhead in probing; airtime cost captured by probe message may be different from a packet

4.6 Categories of Routing Protocols

A routing protocol for WMNs can be *proactive* or *reactive*. For proactive routing, a routing path between two nodes is established before any traffic flow is initiated between them. A reactive routing starts to set up a routing path for two nodes only after traffic is generated between these two nodes.

A routing protocol can be static or dynamic depending whether or not the network experiences variations in topology, link quality, traffic load, and so on. In a wired network, there exist many scenarios where static routing can find many applications. For a multihop wireless network like a WMN, routing usually needs to be dynamic owing to node mobility, link instability, topology change, traffic variations, etc. Two popular dynamic routing schemes are distance vector routing and link state routing [248], which were proposed for wired networks and have become the cornerstone of many dynamic routing protocols of MANETs and WMNs.

Based on its routing algorithm, a routing protocol can be executed in a centralized, distributed, or hybrid manner. For example, in IEEE 802.11s [122] the routing framework includes both modes: AODV-like routing which is distributed and tree-based routing which is centralized. In [169] a hybrid routing scheme is proposed to integrate both modes in the same routing protocol.

To give a finer classification, the existing routing protocols for WMNs can be categorized according to their objectives of performance optimization.

4.6.1 Hop-Count Based Routing

To date many routing protocols developed for WMNs still use hop-count as the routing metric. Although minimizing the number of hop counts is not closely related to performance optimization for WMNs, it has the advantage of simplicity. With a simple routing mechanism, other functionalities can be more easily integrated into a routing protocol. For example, a routing protocol can be designed to efficiently support client mobility [111,261] or to extend the existing protocol for multichannel operation [212]. The simple routing metric also gives researchers an opportunity to try novel routing methodology [29,54]. However, in order to achieve the eventual goal of optimized performance, all such routing protocols are expected to be enhanced to take into account more advanced routing metrics.

4.6.2 Link-Level QoS Routing

In some routing protocols, the routing performance is optimized by minimizing the accumulative or the bottlenecked link-level routing metric of a routing path. However, end-to-end QoS experienced by a user may not be able to be guaranteed. Strictly speaking, QoS is only partly considered in these routing protocols through a hop-by-hop solution at the link level instead of an end-to-end approach.

The quality of link can be impacted by many factors such as channel quality, medium access contentions, interference, network congestion, etc. To measure the quality of a link, we can look into the packet loss rate, retransmission count, and packet transmission time of a link, as discussed in Section 4.5. Many link-quality based routing protocols have been proposed for WMNs [37, 70, 71, 183, 215, 226]. However, the interference (both in-network or out-of-network), the traffic load on different links, and the residual capacity of a link are related to a link quality, but cannot be directly reflected by a link quality. Thus, some link-level QoS based routing protocols have been developed by directly considering interference [271, 282], traffic load balancing [177, 238], and residual link capacity [222, 234] as the performance optimization goal.

4.6.3 End-to-End QoS Routing

In some routing protocols, end-to-end QoS parameters are considered as the performance optimization objective. Thus, these protocols are expected to achieve better QoS performance than the routing protocols based on link-level QoS. So far the end-to-end QoS parameters that are studied most include delay, packet loss, and bandwidth. In [170] a delay-aware routing protocol is developed to support end-to-end delay bound, and a threshold of end-to-end packet loss ratio is guaranteed in [150]. End-to-end bandwidth allocation is considered in [249, 253].

4.6.4 Reliability-Aware Routing

In some application scenarios, reliability is more important than other performance objectives. In this case, multipath routing is a preferred approach, in which multiple routing paths are available to improve the reliability. With multiple routing paths available, they can be used to send traffic simultaneously, or only the best routing path is used and all other paths are for backup only. The former method can achieve better traffic distribution over the entire network, while the latter method is easier for protocol maintenance since only one routing path is used at a time. In [284], multiple copies of a packet are sent to several routing paths from a client to the destination gateway. An integrated routing protocol proposed in [136] to consider two routing paths, one through backbone WMNs and the other through clients, and different routing mechanisms are followed in these two paths. A source routing protocol developed in [195] allows a source to find multiple routing paths to the same destination and then follows a certain mechanism to distribute traffic among these paths.

4.6.5 Stability-Aware Routing

Routing protocols in this category utilize the special system architecture to improve stability. In WMNs, mesh routers are usually stationary and some mesh nodes such as gateways are connected to wired networks. Thus, a routing protocol can select some wired links [19] or more stationary nodes [140] in a routing path to improve routing stability. Only preliminary results have been reported in this category of routing protocols, and more research is needed.

4.6.6 Scalable Routing

For a large scale WMN, it is necessary to develop scalable routing protocols. There can be different approaches to improving scalability of a routing protocol. Among them the hierarchical routing and geographic routing are the most interesting choices as they are totally orthogonal to routing protocols in all previously mentioned categories. In other words, we can incorporate routing protocols from other categories into the framework of hierarchical or geographic routing. Some hierarchical routing protocols have been developed for ad hoc networks [31, 229, 276], but few are available for WMNs, although some preliminary results were reported in [163, 210]. Geographic routing protocols for ad hoc networks are comprehensively studied in [82]. They cannot be directly applied to WMNs unless modifications are made to consider the specific features of WMNs. Geographic routing has the advantage of not relying on the network topology, but it is critical, especially for WMNs, to take into account routing metrics such as link quality rather than just considering hop information [161].

Following the above categorization, we will discuss different routing protocols applicable to WMNs, including multichannel routing protocols. However, as special problems exist in multichannel routing protocols, more discussions are presented in a separate section dedicated to multichannel routing. It should also be noted that some routing protocols can be classified into multiple categories because different performance objectives are considered, but for simplicity of presentation they will be discussed in the category fulfilling the main objective.

4.7 Hop-Count Based Routing Protocols

4.7.1 Light Client Management Routing (LCMR) Protocol

In this case, the end-to-end routing path from a source to a destination client consists of proactive routes among mesh routers and reactive routes between clients and mesh routers [261]. To find the best route from one client to another, hop-count is used as the routing metric. LCMR does not require routing functionality in clients, and the mesh routers supporting clients take care of routing. Thus, mesh routers need to maintain two tables: one for MAC and IP addresses of local clients and the other for the IP addresses of remote clients as well as the IP addresses of remote mesh routers associated with remote clients. Based on these two tables, once a local client needs to set up a routing path to a remote client, its associated mesh router can find out which remote mesh router is responsible for forwarding traffic to the remote client. Based on such information, the mesh routers can then set up a routing path between them using proactive routing and a hop-count metric.

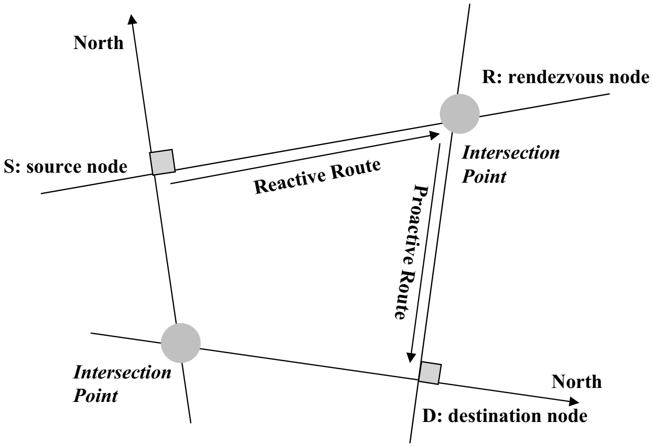

Figure 4.1 A simple setup process of a routing path in ORR

LCMR has a high overhead for maintaining the two tables on each mesh routers, as all clients' IP addresses need to be collected and stored at each mesh router.

4.7.2 Orthogonal Rendezvous Routing (ORR) Protocol

This protocol is proposed for mesh nodes capable of directional communications [54]. Each node can define its neighbors' directions relative to its local *North*. Relying on such information, ORR can reduce the state information for routing, and it does not need flooding for route construction. Compared to geographic routing, ORR does not need the exact location of nodes. It is based on the idea that in the 2-D Euclidean space two orthogonal lines can have at least two intersect points with another group of two orthogonal lines if these two groups of orthogonal lines have different centers. To construct routing paths, a source node sends route discovery in orthogonal directions, while a destination node sends route dissemination in orthogonal directions. Thus, there is at least one intersect point, called the *rendezvous point*, where both route discovery and route dissemination messages are received. In this way a routing path is established between the source and the destination. Moreover, the routing path from the source to the rendezvous point is a reactive route and the remaining path to the destination is a proactive route. The above procedure is depicted in Figure 4.1.

From the mechanism of ORR, we know that it oversimplifies WMNs. Firstly, the direction of a node needs to be configured freely. Secondly, the network is not really a 2-D space. If a 3-D space is considered, the theory for ORR may not be valid. Thirdly, ORR may not work if the node density is high or topology change frequently happens. Finally, the routing path selection procedure is based on hop-count. However, other metrics such as link quality can be adopted to enhance the ORR.

4.7.3 HEAT Protocol

An anycast routing protocol called HEAT is proposed using the idea of temperature field [29]. HEAT considers all nodes in a WMN as a temperature field. The gateways have the highest temperature. The temperature of a nongateway node will be determined by hop-count to the gateways and by the robustness of a routing path from this node to gateways. Once temperatures of all nodes are determined according to this procedure, the packets from any node to the gateways can simply follow the following method: the node forwards the packets to its neighbor with the highest temperature, and this neighbor will repeat the same process until reaching the gateways. Thus, any nongateway node can easily route packets to the gateways without setting up a routing path between a particular (source–destination) pair. However, it should be noted that this anycast scheme totally depends on the assumption that the traffic of WMNs only needs to be routed between gateways and nongateways; for other scenarios anycast routing is not supported. Moreover, how to consider other routing metrics in HEAT remains an open problem.

4.8 Link-Level QoS Based Routing Protocols

Based on the routing metrics derived from link layer parameters, these routing protocols optimize the network performance considering the link quality, interference, load balancing, or link residual capacity.

4.8.1 Link Quality Source Routing (LQSR) Protocol

LQSR [70] is designed based on dynamic source routing (DSR) [137]. It contains all basic DSR functionalities, such as Route Discovery (Route Request and Route Reply messages) and Route Maintenance (Route Error messages). However, LQSR has two major differences from DSR. One is that LQSR is implemented as *layer 2.5* protocol instead of as a network layer protocol. The other is that LQSR supports *link quality metrics*. The *layer 2.5* architecture brings two significant advantages. First, no modification is needed for the higher layer software, i.e., LQSR routing protocol is transparent to higher layer software. Second, no modification is required for link layer software. With different routing metrics and network mobility, the performance of LQSR varies. For stationary nodes in WMNs, the routing metric ETX, achieves the best performance, while the minimum hop-count method outperforms the three link quality metrics, i.e., per-hop RTT, per-hop packet pair delay, and ETX when nodes are mobile. The reason is that, as the sender moves, the ETX metric cannot quickly track the change in the link quality. This result illustrates that the link quality metrics used in [70] are still not enough for WMNs when mobility is concerned. Better routing metrics need to be developed.

4.8.2 Multiradio LQSR (MR-LQSR) Routing Protocol

MR-LQSR is proposed for multiradio WMNs [71]. It is developed based on LQSR, and thus, also based on DSR [137]. To make LQSR perform well in a mesh network with multiple radios per node, WCETT is used as the routing metric in the routing protocol. As explained in Section 4.5.6, WCETT [71] takes into account both link quality metric and the minimum hop-count. It can achieve good tradeoff between delay and throughput because it considers channels with good quality and channel diversity in the same routing protocol. From the functionality of MR-LQSR, we know the major difference from LQSR is WCETT. This again illustrates the importance of developing new performance metrics for WMNs. MR-LQSR assumes that nodes are stationary. This is true for mesh routers, but obviously not applicable to mesh clients. From the experience of LQSR, we know that the performance of MR-LQSR can also be degraded by the mobility of nodes, i.e., mesh clients. In WMNs, multichannel operation over a single radio is another alternative to increase the network capacity. For this type of network, the scheme proposed in [71] is not applicable, because WCETT is limited to multiradio mode.

4.8.3 ExOR Routing Protocol

ExOR is proposed to improve throughput based on cooperative broadcasting packets from source to destination without explicitly setting up a routing path [37]. When a source sends packets to its destination, the following steps are needed. First, packets are buffered in batches, and then the source broadcasts packets batch by batch. Second, the source node selects a set of nodes that have received its packets and lets these nodes decide which node will forward the received packets. This priority of a forwarding node is determined by the cost to the destination, which is evaluated by the accumulative ETX to the destination node. Since ExOR only uses broadcasts, only the forward packet delivery probability is considered in ETX. The set of nodes that are selected for forwarding packets is determined based on the packet loss ratio between the source and these nodes. Although many nodes can receive packets from the source node, only a subset of nodes are selected as forwarding nodes in order to reduce the overhead. Third, the highest priority forwarding node sends its own batch of packets following the same procedure as done by the source node. This process is repeated until 90% of the packets in each batch are received by the destination node. The remaining 10% of the packets will rely on traditional minimum hop-count routing for delivery. The advantage of ExOR is that most of the packets are delivered without setting up routing paths, which is similar to anycast routing. Moreover, ExOR can improve throughput for two reasons. One is that it tries to use the best link to deliver packets through cooperation of forwarding nodes. The other is that the progress of packet forwarding can be continued even if some nodes on a traditional path experience bad link quality or are out of order. On the other hand, ExOR also faces many challenges. In order to achieve agreement among forwarding nodes, the communication overhead can be high. Thus, the selection of a set of nodes may need fine-tuning for different networks. In order to keep delivering packets in sequence and also to reduce duplicate transmissions, a mechanism like *batch map* needs to be maintained, which is another source of overhead.

As explained above, ExOR still needs traditional minimum-hop count routing. A significant drawback of ExOR is that it is difficult to support multiple traffic flows.

4.8.4 AODV-Spanning Tree (AODV-ST) Protocol

AODV-ST is designed for multiradio WMNs [215]. ADOV-ST, as its name indicates, performs hybrid routing, i.e., AODV is used for traffic inside the mesh network and spanning-tree based routing is used for traffic to/from gateways. ETT, as described in Section 4.5.6, is used as the routing metric for this protocol.

The drawback of AODV-ST is that AODV may not be efficient for intra-mesh traffic. Because AODV is a distance vector routing protocol, the WCETT proposed for multiradio WMNs is not applicable.

There are many other protocols that consider link quality. For example in [183] the NAVC metric derived from the MAC layer is incorporated into the AODV protocol. Thus, a routing path is not determined by hop-count but by the NAVC value of that path. Power control is also considered together with routing in [183] in order to improve throughput and reduce power consumption.

4.8.5 Interference Based Routing: IRMA

Although delay or packet loss of a link can reflect the interference or contentions from neighboring nodes, routing protocols based on such metrics cannot directly resolve interference or contentions. Thus, some routing protocols have been designed with a focus on resolving contentions in intra- and inter-traffic flows [271] or reducing interference [282]. Since resolving contentions or interference is closely related to the MAC layer protocol, such routing protocols are usually designed together with a MAC protocol via cross-layer design.

In [271], the medium access mechanism is assumed to be TDMA instead of the popular CSMA/CA of IEEE 802.11 networks. Based on the TDMA framework, an integrated routing and MAC scheduling algorithm (IRMA) is derived to find a routing path for each traffic flow and then to determine slot allocation on each link considering the allocation information, link status, and topology information in the network. The algorithm is a centralized scheme and relies on an existing solution to collect the node, link, and topology related information on the entire network and get specifications of traffic flows. Such signaling can be done in a global control plane (GCP) that can be implemented in a separate dedicated channel or in a dedicated time slot. There are two routing mechanisms defined in IRMA: link-scheduling with minimum-hop routing and link scheduling with bandwidth-aware routing. In the former routing mechanism, a routing path is selected by considering the shortest path using minimum hop-count. Once a path is selected, time slots along this path are determined by the centralized allocation algorithm by considering the latest flow information in the network. This method can result in congested paths or links because the minimum hop-count routing does not consider the available bandwidth. Thus, the second routing mechanism is preferred in most WMNs. In this mechanism, the available bandwidth on each link is factored when a routing path is selected. Based on the bandwidth-aware routing path selection, time slots are then determined for each link on the path. Thus, such a scheme can not only avoid contentions in traffic flows but also avoid bottleneck or congested links.

IRMA has several shortcomings. First of all, it is not scalable with the network size, as it is a centralized scheme. Second, it assumes an efficient scheme for collecting all control information, which in fact is a challenging issue for all routing protocols. Third, the MAC layer is assumed to have TDMA operation, which is not the case for many WMNs.

IRMA is designed for single-channel operation. For multiradio multichannel WMNs, a load and interference balanced routing algorithm (LIBRA) is proposed in [282]. LIBRA assumes the number of nodes in each node's interference range and then relies on such information to calculate the routing metric MIC. LIBRA also constructs a virtual network on top of the real network, and then MIC weights are distributed over the virtual network. Based on such a virtual network and MIC weights, a routing path on the real network can be found via Bellman–Ford or Dijkstra's algorithm. LIBRA reduces interference through MIC and, in theory, its performance is much better than routing protocols that do not consider interference. However, its complexity is high due to the maintenance of a virtual network. In addition, the number of interfering nodes cannot be easily determined in WMNs, which poses a question as to the feasibility of MIC and also LIBRA. Although LIBRA is a multiradio routing protocol, channel allocation is not considered and channels on each radio are assumed to be preconfigured.

4.8.6 Routing with Load Balancing

Routing is directly determined by considering network congestion [238]. Given a source and its destination, a routing path is determined by using the route with the least congestion. If more than one path has the same number of congested nodes, the route with minimum hop-count is selected. The congestion state of a link is determined by the number of retransmissions of RTS and ACK packets. If the congestion exceeds a threshold, the congestion weight on this link increases. Only preliminary results were reported in [238] and further research is needed to fully justify the proposed scheme.

A capacity-aware routing (CAR) protocol is proposed to balance load among links and channels in a multiradio WMN [177]. CAR assumes that channel assignment on radios lasts a long time and can be static. With static channels on each radio in the network, CAR determines the BLC, as described in Section 4.5.9, in a reactive manner for each traffic flow. Transmissions start on a routing path that is determined according to the best BLC metric. However, this path can be switched to a new one if the source finds that the new path has a higher BLC value. Because it considers the bottlenecked link capacity in routing, CAR improves throughput and delay performance. CAR may not achieve optimal performance because the path selections on different flows affect each other but it is not coordinated among such flows.

4.8.7 Routing Based on Residual Link Capacity

Some routing protocols with load-balancing capability have also considered link capacity. For example, in [177] load-balancing is achieved by considering bottlenecked link capacity. An alternative scheme to consider link capacity in routing is to get the information of residual link capacity [222, 234].

In [222] a protocol called Hyacinth is developed to perform routing and channel assignment for a multichannel WMN. *Hyacinth* considers traffic from/to gateways in WMNs and thus uses tree-based routing for such traffic. Each node advertises the costs of its path from/to the gateway. Based on such information, a neighbor that finds a lower value in the cost will leave its old parent node and selects the new node as the new parent node. With such a procedure, all nodes in the network build up routing paths to the gateway like a spanning tree. To reflect the cost of a path, the residual capacity of a link is considered as a routing metric. Thus, when a routing path is available from a node to/from the gateway, it tends to select links that have the largest available capacity. As Hyacinth also involves channel allocation, we will have a more detailed study on this protocol in Chapter 9.

Residual capacity of a link is also considered in [234], where the frame delivery rate (FDR) and traffic load of the link are also considered when the cost of a routing path is calculated.

In other words, the cost of a routing path is the weighted sum of three parameters: residual capacity, FDR, and the traffic load of this path. The residual capacity of a path is the residual capacity of a bottlenecked link, FDR of a path is the product of FDRs of all links on the path, and the traffic load of a path is the maximum load among all links on the path. The routing protocol in [234] follows the routing mechanism of dynamic source routing (DSR) except for the new routing metric that considers residual capacity, FDR, and traffic load to balance load and reduce congestion. However, more research is expected to further evaluate the performance of the new routing metric.

It should be noted that routing protocols considering residual link capacity usually take into account load-balancing.

4.9 End-to-End QoS Routing

End-to-end QoS can be considered in a routing protocol by ensuring end-to-end packet loss rate, delay, or bandwidth.

4.9.1 Quality Aware Routing Protocol

In this protocol, the end-to-end packet loss rate is ensured where both ETX and ENT are used as routing metrics [150]. ENT, as described in Section 4.5.7, is used to determine which routing paths can be used. This is done as follows. Considering a higher layer protocol, the allowed packet loss rate in a link is given. Based on this packet loss threshold and the measurement of the link, a positive number δ used by ENT is derived. With δ and an existing probe scheme, the ENT of each link is determined. The ENT is then compared with the maximum number of transmissions of a packet before it is discarded at the link layer. If the ENT is larger than the link-layer value, the routing cost of the link will become infinity. Otherwise, ETX, as described in Section 4.5.4, is used for the routing cost of the link. As a result, all links that do not satisfy the packet loss requirement will be excluded from routing paths. After this step, routing path selection is performed by just choosing the path with the smallest routing cost. There exists one critical issue in [150]: how to determine the allowed packet loss rate of a link given the threshold of end-to-end packet loss requirement.

4.9.2 RingMesh Routing Protocol

Some initial research results were reported in [170] to consider the end-to-end delay in a RingMesh routing protocol for WMNs. RingMesh is developed based on a token ring protocol proposed for wireless LANs. Different from the wireless token ring protocol [78], RingMesh has to create multiple token rings to support multihop WMNs. These token rings are created and organized from the gateway to all other nodes like a spanning tree scheme, and different channels are used in neighboring rings. The first ring containing the gateway is called the root ring, and the next ring connected to the root ring is a child ring. These two rings share a common node which is called a pseudo gateway. Following this process, other child rings are connected together all the way to the root ring. For a node in the network, which ring it can join depends on the delay from it to the gateway; the node joins a ring that can satisfy the end-to-end delay requirement.

Many problems remain in the RingMesh routing protocol. For example, how to form multiple rings to support multiple gateways to improve the delay performance is not addressed. It is also unknown what can be the solution if no ring can be joined by a node. Also, no mechanism is available to determine the delay from a node to the gateway, which is not a trivial task. Thus, end-to-end delay aware routing is still a challenging research topic.

4.9.3 Bandwidth Reservation Routing Protocol

The end-to-end bandwidth reservation is the performance goal of this routing protocol [253]. As needed by bandwidth reservation, this routing protocol assumes that slots can be allocated and reserved in the MAC layer, like a real-time MAC proposed in [184]. This protocol consists of three phases. In the first phase, routing paths that satisfy the required bandwidth are determined. Then the path with the maximum number of fixed nodes is selected In the second phase, a slot allocation algorithm is used to allocate slots to each link on the selected routing path. In the third phase, the allocated slots are reserved by advertising the allocation information to all related neighbor nodes around this routing path. There is no optimal slot allocation scheme proposed, and only heuristic algorithms are applied to allocate slots in each link. Thus, the performance of the routing protocol is constrained by such heuristic algorithms. Another critical issue is that the real-time MAC [184] cannot really guarantee slot reservation for real-time traffic, because the allocation tables reserved through RTS-CTS procedures may not be readable by neighbors in the interfering range but out of communication range. Such neighbors will not be able to observe the reserved slots and thus can cause contentions.

In [249] theoretical results are derived to ensure end-to-end bandwidth for a new connection admitted into WMNs. If the bandwidth cannot be satisfied, the connection has to be rejected. To check such bandwidth guarantee, both intra-flow interference and inter-flow interference experienced by a potential connection are considered.

4.10 Reliability Aware Routing: Multipath Routing

The main objective of using multipath routing is to improve reliability and provide high fault tolerance [192]. Multipath routing can also enhance load-balancing. In a multipath routing protocol, multiple paths are set up between a source and its destination. Packets can flow in one or more of these selected paths. When link is broken on a path due to a bad link quality or mobility, other paths try to keep transmission progress as smooth as possible. Thus, the end-to-end delay, throughput, and fault tolerance can be much improved.

Multipath routing can be done between a source and its destination or for intermediate nodes particularly on the primary path for the (source–destination) pair. It is shown in [196] that providing multiple paths to intermediate nodes can significantly improve performance rather than just providing multiple paths to the (source–destination) pair: load is more balanced throughout the network, and it is more robust to link failures. However, such a strategy makes the routing protocol much more complicated. To maintain so many paths will also increase the overhead of the routing protocol.

To date just a few multipath routing protocols are available for WMNs.

4.10.1 Resilient Opportunistic Mesh Routing (ROMER) Protocol

Different from traditional disjoint multipath routing, ROMER creates a forwarding mesh, on the fly, for each packet [284]. The procedure of ROMER is explained as follows. First of all, ROMER assumes there is an existing scheme that can find the minimum cost from each mesh router to the gateway. Then the credit is determined while a packet is forwarded on the fly. When a packet is to be delivered from a mesh router, e.g., Node S, to the gateway, the source mesh router needs to set a credit cost. If the minimum cost from the mesh router to the gateway is $C_{min,S}$ and the credit cost is $C_{credit,S}$, then the mesh router S has a budget cost of $C_{min,S} + C_{credit,S}$ to the gateway. When the packet is sent to the next mesh router, e.g., Node A, the budget is reduced by the cost of the traversed link $c_{link_{SA}}$. At mesh router A, the needed credit is computed according to the requirement of $C_{credit,A} + C_{min,A} + C_{link_{SA}} \leq C_{min,S} + C_{credit,S}$, i.e., the remaining credit at mesh router A is $C_{credit,A} = C_{min,S} + C_{credit,S} - C_{min,A} - C_{link_{SA}}$. If the ratio of the remaining credit to the initial credit $C_{credit,S}$ is less than a threshold, e.g., $(C_{min,A}/C_{min,S})^2$, then the packet at mesh router A should be discarded; otherwise, mesh router A forwards the packet according to a randomized opportunistic forwarding scheme. The above process is repeated until the packet is delivered to the gateway. Finally, when multiple intermediate routers receive the same packet from a mesh router and all have enough credit to forward the packet, they need to follow a randomized opportunistic forwarding scheme to forward packets. The probability that each intermediate router can forward a packet depends on the quality of the link to the parent router. The intermediate router with the best link quality forwards the packet with probability 1, while other intermediate routes forward the packet with a probability of R_l/R_{max}, where R_l is the current rate of the considered link and R_{max} is the current rate at the best link. Thus, the same packet can be forwarded by multiple mesh routers. Such multiple copies of packets being sent at different nodes tend to take advantage of the space diversity of the network, and thus can potentially improve the performance. The probabilistic forwarding is to reduce the overhead of duplicate transmissions. Because the same packet flows in different paths of the same network, it is necessary to further suppress duplicate copies of the same packet on the same node.

There exist several problems with ROMER. Packets in ROMER are broadcast rather than unicast. For high rate transmission, broadcasting is much more unreliable than unicasting which compromises the performance of ROMER. ROMER is designed for traffic flows from clients or mesh routers to the gateway; it does not support other traffic scenarios. Lastly, ROMER has to rely on an existing scheme to find out the minimum cost from each mesh router to the gateway. What type of cost is the best for ROMER and how to dynamically update the cost to best serve ROMER remain open questions.

4.10.2 Multipath Mesh (MMESH) Routing Protocol

MMESH is based on source routing and allows the source to find multiple routing paths to the destination [195]. Two phases are needed for this process: route discovery and route maintenance. In the route discovery phase, a set of paths is selected. In the route maintenance phase, these paths are monitored, and if a better path is detected or if a path fails, the routing table needs to be updated. By using multiple routing paths, the reliability is improved, but the protocol needs to pay the price for the complicated procedure of discovering multiple paths and maintaining these paths. The overhead of that kind of operation can be high too. In this sense, MMESH is not comparable to ROMER [284]. MMESH can achieve load balancing in two ways. The first is based on round-robin selection of the next hop for packet forwarding. This can cause a problem with out of order transmissions. In the second approach, the next hop selection can be determined by the congestion status, i.e., the next hop that is least congested is selected to forward packets. However, the effectiveness of both schemes depends on how multiple paths are overlapped. If they are totally disjoint, then the load balancing is not really effective.

It is necessary to pay attention to several issues in multipath routing. First of all, the complexity of a multipath routing is generally much higher than a single-path routing protocol, because a much more complicated procedure is needed for route discovery, routing path selection, and route maintenance. How to design multipath routing without increasing too much complexity remains an important research problem.

Other than the complexity issue, multipath routing may not be always effective. For example, as proven in [88], when a mobile ad hoc network is considered, unless a large number of shortest paths are selected, the load distribution is almost the same as a single shortest path. However, for WMNs this issue may not be so critical, as mesh routers in WMNs have minimal mobility and thus multipath routing tends to be effective in WMNs.

In a multiradio WMN, multipath routing is a much more interesting problem, because more than one physical link is available between any two neighboring nodes, which is very different from a single-radio WMN. Due to the availability of multiple physical links between any two neighbors, more paths are available for a routing protocol to select for a (source–destination) pair. This potentially makes multipath routing more powerful, but also increases the difficulty in developing a scheme to efficiently select the routing path. On the other hand, since channel assignment is also inter-dependent on routing, if multipath selection is considered, the joint design between channel assignment (or topology control) and routing can become a really sophisticated problem.

4.11 Stability Based Routing

In some routing protocols, stability is given a higher priority than other performance goals. In [140] a route with more stationary nodes is preferred over a route with more mobile nodes. Based on such a criterion, the routing paths are formed like a tree from the gateway as the root. Client-to-client communications have to go through the gateway. This indicates that this routing protocol is not a good choice for intra-mesh traffic scenarios.

In [19] another simple scheme is used to improve the stability of a routing protocol. In WMNs, gateways are connected to each other through wired networks. Thus, the routing protocol takes into account the wired links when traffic needs to be routed among these nodes inside a mesh. As for the routing metric, ETX is used for the wireless links and latency is used for wired links. It should be noted that this type of routing protocol is effective only for intra-mesh traffic. When packets go to the Internet through the gateway, it does not make sense to use this routing protocol; when a packet arrives at the wired link, it will just go into the Internet instead of coming back to the WMN and then to the Internet again.

It should be noted that the above routing protocols only consider stability in a qualitative way. In order to consider stability quantitatively, a stability-based routing metric needs to be designed.

4.12 Scalable Routing

For large-scale WMNs, the scalability is a serious problem. Thus, a routing protocol needs to be scalable. In other words, its increased complexity and overhead do not degrade the performance as the network size increases. Two approaches can provide scalable routing: hierarchical routing and geographical routing. The former makes the routing complexity localized into a small region by following a hierarchical routing architecture. The latter relies on the stateless property of geographic routing to avoid complexity and overhead even if the network size is large.

4.12.1 Hierarchical Routing

Numerous hierarchical routing protocols [32, 229, 276] have been proposed for ad hoc networks in recent years. Although they were not developed specifically for WMNs, common design principles can be derived from these routing protocols for a hierarchical routing protocol for WMNs.

In hierarchical routing, a particular self-organization scheme is employed to group network nodes into clusters. Each cluster has one or more cluster heads. Nodes in a cluster can be one or more hops away from the cluster head. Since connectivity between clusters is needed, some nodes can communicate with more than one cluster and work as a gateway. Routing within a cluster and routing between clusters may use different mechanisms. For example, inter-cluster routing can be a proactive protocol, while intra-cluster routing can be on demand [229].

When the node density is high, hierarchical routing protocols tend to achieve much better performance because of less overhead, shorter average routing path, and quicker set-up procedure of the routing path. However, the complexity of maintaining the hierarchy may compromise the performance of the routing protocol. In WMNs, in particular client WMNs, hierarchical routing actually may face an implementation difficulty, because a node selected as a cluster head may not necessarily have higher processing capability or channel capacity than the other nodes. Unless intentionally so designed, the cluster head may become a bottleneck. Nevertheless, hierarchical routing will become a attractive choice for WMNs, due to the following factors.

- *Hierarchical network architecture.* There is a trend that more and more WMNs will have a hierarchical network architecture owing to its advantages of organizing and maintaining the network and also its need to backhaul access to the Internet. Usually, mesh routers are in the middle level of the hierarchy, and at the bottom level are the mesh client nodes. Mesh routers can be further split into multiple levels in the hierarchy. For example, an IEEE 802.16 mesh network can run overlaying an IEEE 802.11 mesh network. Although mesh clients can establish direct communications among themselves, the network hierarchy is quite obvious, and must be utilized by many protocols such as network management, mobility management, MAC, routing, and even transport layer protocols. Therefore, maintaining the network hierarchy is not just for the benefits of routing. In other words, the complexity and the overhead of doing so will become acceptable as far as the entire WMN is concerned. Consequently, developing a routing protocol by utilizing the network hierarchy will become a wise strategy.

- *Powerful mesh routers.* With the network hierarchy available, we can always select powerful mesh routers to work as cluster heads for hierarchical routing. These routers can be equipped with powerful processors, multiple radios, enough energy supply, and so on.

Thus, if a WMN is hierarchical in nature, hierarchical routing is an indispensable technique that can greatly enhance the scalability of the routing protocol and also reduce the complexity of routing operations in mesh clients. To better serve this purpose, efficient algorithms need to be developed for self-organization of the network hierarchy, which also involves other protocols, e.g., mobility management and MAC protocols. In this sense, hierarchical routing demands a more comprehensive design.

It should be noted that employing a hierarchical routing method does not exclude other routing schemes. In fact, other routing schemes such as multichannel routing, routing with multiple routing metrics, and geographic routing can be part of the hierarchical routing protocol. For example, in a hierarchical WMN, mesh routers can be cluster heads, and their routing protocol is a multichannel routing protocol due to the existence of multiple radios.

Hierarchical routing for WMNs is not well researched. So far only a few a few preliminary results have been reported. In [210] a hierarchical routing protocol is proposed for load balancing among mesh clients. In this protocol, a mesh router is considered as one cluster head, and mesh clients are associated to a mesh router as members of the cluster. Usually each mesh client is associated with one cluster, but mesh clients that can hear messages from multiple mesh routers can be associated with up to two clusters. In order to support cluster formation, mesh routers need to send periodical announcements. Mesh clients rely on such information to decide which cluster to join. However, the number of mesh clients in different clusters needs to be balanced. This routing protocol improves load balancing, but does not really resolve the scalability issue, as mesh routers are not organized in a hierarchical way. As a result if a WMN has a large number of mesh routers, the routing in the mesh backbone may still not be scalable.

In [163] a Zigbee cluster label (ZiCL) routing protocol is proposed to perform hierarchical routing for Zigbee WMNs. In each cluster, a mesh client or mesh router is connected to the cluster head in one hop. A mesh client without direct connection to the cluster has to be connected to the cluster through a mesh router. Cluster headers are connected through gateways. The communications inside a cluster are based on unicasting, while those between clusters use AODV to set up routing paths between cluster heads and then fulfill end-to-end packet delivery. The hierarchical routing of ZiCL can reduce end-to-end delay and improve scalability. However, it may not be applicable to other types of WMN. Firstly, one-hop unicasting in each cluster means the size of cluster can be very small and can result in many clusters in a large WMN, which again poses problems in scalability. Secondly, the inter-cluster communications need to be improved rather than just using AODV. All the previously mentioned routing protocols can be adopted to improve inter-cluster routing.

4.12.2 Geographic Routing

When position information is available at all nodes in the network, geographic routing is an attractive option. Compared to topology-based routing schemes, geographic routing schemes forward packets by only using the position information of nodes in the vicinity and the destination node [82]. Thus, there is no need to set up a routing path with all the complexities and overhead of doing so. For whatever type of topology change, geographic routing is much less impacted than other routing protocols, because it only depends on position information of the neighbors and of the destination. These two advantages make geographic routing outperform other routing protocols, in particular when a large-scale network is concerned or the network has high mobility. In this sense, geographic routing can be considered as a scalable solution to routing protocols for both infrastructure WMNs and client WMNs.

Early geographic routing algorithms are actually a type of single-path greedy routing scheme in which packet forwarding decisions are based on the location information of the current forwarding node, its neighbors, and the destination node. Various greedy routing algorithms differ in the optimization criterion applied in the forwarding decision. Whatever criterion is used, loop-free packet forwarding must be guaranteed.

To improve power efficiency, a greedy algorithm proposed in [243], determines the routing path based on different energy metrics. However, all greedy routing algorithms have a common problem: *delivery is not guaranteed even if a path exists between source and destination*. Partial flooding and keeping the past routing information can help to guarantee delivery. However, these approaches increase communication overhead and lose the stateless property of single-path greedy routing [82].

In order to keep the stateless property, and guarantee delivery, planar-graph based geographic routing algorithms have been proposed by [40] and [66]. In these algorithms, packets traverse faces on graphs using the well-known right-hand rule. However, open issues still remain in these algorithms [82]. For example, considering the face algorithm proposed in the routing protocol in [40], the communication overhead is much higher than the single-path greedy routing. Thus, planar-graph based geographic routing schemes are mainly used as a recovery scheme when greedy routing fails.

Most greedy and planar-graph based geographic routing algorithms only utilize one-hop position information. They can also be generalized into algorithms using two-hop position information, and thus improve the performance of routing protocols. However, all these routing algorithms neglect a critical design factor for routing in wireless networks, which is link quality. Without considering link quality, packets may be forwarded to a link with bad quality, and thus experience high packet loss. This further causes waste of bandwidth in other links. Thus, the optimization criterion of a geographic routing protocol needs to take into account both position information and link quality. One such routing algorithm is proposed in [161].

A new criterion called normalized advance is defined as $(D(T) - D(n))/Cost(n)$, where $D(T)$, $D(n)$ are the distances from the current node to the destination node and neighbor n, respectively, and $Cost(n)$ is the link cost to represent the link quality between the current node and neighbor n. The link cost can be packet error rate, link delay, energy consumption, and so on. Geographic routing based on normalized advance achieves better performance than other routing protocols, especially when the environment is noisy. However, we believe better link quality metrics and better integration between these link quality metrics and position information are still expected for WMNs.

Geographic routing also has other drawbacks. Firstly, it depends on techniques of getting position information. When GPS is available, getting position information is an easy task, but cost can be much higher unless GPS services become very cheap or free. Otherwise, accurate algorithms need to be developed to determine relative positions between nodes. This problem itself is still a challenging research topic, especially in multihop networks such as WMNs.

Secondly, even if position information is available to each node, such information needs to be sent to all other nodes so that a node can identify a destination node's position. Therefore, when geographic routing is adopted for WMNs, we need to handle these drawbacks properly. Fortunately, for the reason of low mobility in many WMNs, the risk of experiencing such problems is much lower than with a mobile ad hoc network. For example, when mobility is low, it is relatively easy to develop location/position sensing algorithms. Also, position information of nodes does not need to be updated at a high frequency, which greatly reduces the protocol overhead. When mobility is high, as in some client WMNs, in order to avoid frequent exchange of position information among nodes, schemes similar to beaconless routing [101] are needed to reduce signaling overhead by eliminating the periodic *hello* messages.

4.13 Cross-Layer Multichannel Routing Protocols

Multichannel operation is widely adopted in WMNs to improve network capacity. There can be two methods for the design of routing protocols for multichannel WMNs. The first option is to directly apply a single-channel routing protocol to a multichannel WMN. In this case, the multichannel operation is totally taken care of by MAC protocol, and is transparent to routing. This option makes protocol design easier. However, routing determines traffic distributions of the network and thus impacts channel allocation too; if the routing path selection does not consider multichannel operation, the performance may not be good. In order to improve the performance, the second option is to take into account multichannel operation in a routing protocol. There are two schemes in this option: the simpler scheme is to develop a routing metric to consider the impact of multichannel operation such as link quality, interference, packet loss, bandwidth, etc., while a more complicated scheme is to conduct close routing/MAC cross-layer design such as joint channel allocation and routing. So far most multichannel routing protocols [71,177,212,215,282] follow the simpler scheme. However, such routing protocols may not lead to optimized performance. Let us consider MR-LQSR as an example. MR-LQSR assumes that different radios in a node are assigned with noninterfering channels by a separate agency such as MAC protocols. This assumption ignores the close relationship between traffic distribution and channel allocation. Thus, a natural solution to this issue is to carry out routing and channel assignment in the same protocol. MR-LQSR also assumes that the channel assignment changes relatively infrequently. In fact, this is not true in many application scenarios, as traffic load distribution varies a lot from time to time. Thus, channel allocation needs to be dynamic, which requires a dynamic scheme of joint channel allocation and routing.

4.13.1 Joint Channel Assignment and Routing

This protocol is for infrastructure WMNs (IWMNs) in which the aggregated traffic load at mesh routers and channels assigned to each router are assumed to be not changing frequently [16]. However, channels assigned to radios on a node are determined together with routing paths with the objective of obtaining an interference-free link schedule and achieving maximum throughput. Similarly, the routing algorithm studied in [249] assumes that the channel assignment can be static in WMNs. Both [16] and [249] focus on a mathematical formulation of the joint design between channel assignment and routing. However, no actual protocol is proposed. We believe that the theoretical results can provide valuable guidelines to the joint optimization of channel assignment and routing. However, it is still far from being applicable to WMNs for several reasons. First, the assumptions on interference model and transmission power level are not realistic. For example, different radios at a node may experience different interference, and their power level is not necessarily fixed. However, these are differences that make a routing protocol or channel assignment a more challenging problem. Second, no signaling procedure is designed to assist the routing algorithm. In fact, for a routing protocol, one key task is to design an efficient signaling procedure to collect topology information, measure variable routing metric, and so on. Third, the approaches in [16] and [249] have an implicit assumption that the algorithm is executed in a centralized manner. For WMNs, especially in a large-scale WMN, such a scheme significantly limits the scalability of the routing protocols. Thus, it is desired for WMNs to perform joint channel assignment and routing in a distributed way.

In addition, the existing joint channel assignment and routing algorithm has the following problems.

- *Static traffic pattern may not exist.* In an IWMN, this might be a reasonable choice, since mesh routers are almost stationary and there are few activities of frequent adding and removal of mesh routers. However, problems still exist, because the aggregated traffic load at mesh routers can vary a lot depending on where a mesh router is deployed. For example, if a mesh router becomes a hot spot, it definitely needs to carry much higher traffic load than usual. If a hybrid or ad hoc WMN is considered, the aggregated traffic load at different mesh routers also varies a lot. Moreover, due to mobility, traffic patterns change a lot from time to time. All the above scenarios imply that the static channel assignment scheme is not a viable solution for WMNs. As a result, an adaptive channel assignment scheme needs to be performed together with routing by considering dynamic traffic patterns.

  For a multiradio WMN, some research work [65] has been reported to integrate traffic prediction with route optimization. However, the performance of such schemes really depends on the accuracy of prediction, which in general is difficult to achieve.

- *Performance parameters are not really taken into account.* In [16], the goal of routing is to make sure that flows in links are interference free. This objective can definitely avoid interference and thus improve throughput per node. However, this may not necessarily improve the overall network throughput, because performance parameters such as delay, packet loss, etc., are not taken into account, and thus end-to-end transmission of packets will go through a nonoptimal path. The same problem exists in [249], although connection blocking ratio is considered as a QoS parameter in the routing algorithm.

4.13.2 Distributed Joint Channel and Routing Protocol

This protocol takes into account the number of flows that are possible to route on each link [22]. The number of flows is obtained from a solution to the joint channel assignment and routing problem. The objective is to enable every router to utilize each of its links in proportion to their assigned flow rates. To achieve such a goal, the routing protocol only requires a partial knowledge of the network topology and does not make use of a destination-based routing table. Hence, the name Layer-2.5 (L2.5) given to the routing protocol. The operations of the L2.5 routing protocol are as follows. Each router is configured with the flow rate values associated with its links, and records the number of bytes sent to each neighbor in each time interval. Every time a router has to take a forwarding decision, it computes the gap between the desired and the current utilization of its links and selects the neighbor with the biggest gap as the next hop router. Clearly, this strategy might force packets to take extremely long paths to get to the destination. To address this shortcoming, each router needs to know the minimum hop count to every destination, referred to as its hop count vector. Each router also has to know the hop count vector of its neighbors, in order to find out which of them has the same hop count to a given destination. Then, the proposed L2.5 routing protocol provides that every source node includes a *maximum hop count* in each packet it sends. Such a value represents the maximum allowable number of hops to the destination and can be the minimum hop count to the destination multiplied by a constant factor $\alpha > 1$. This value is decremented at each intermediate hop and is used to determine the set of next hop neighbor candidates. Indeed, if the maximum hop count equals the minimum hop count to the destination for the intermediate node, then the packet must be necessarily sent to a neighbor having a smaller hop count to the destination and will thus follow a minimum hop path. Otherwise, the packet may also be sent to neighbors with the same or even greater hop count to the destination. The selected next hop neighbor is the one in the set of neighbor candidates with the largest gap between the desired and the current link utilization. This strategy ensures that packets reach the destination in, at most, the maximum hop count. Also, the L2.5 routing protocol has the potential for a fast recovery from link failures. For instance, if the neighbor selected as the next hop for a packet becomes unreachable and several repeated transmissions fail (no acknowledgment is received), then such a neighbor is removed from the candidate set and a new next hop neighbor is selected (without the need to update the hop count vectors). However, selecting the next hop neighbor on a per-packet basis also has the undesired effect of splitting flows along multiple paths, thus requiring the reordering of packets at the destination. Also, the link quality should be taken into account in the selection of the next hop neighbor by means of, e.g., one of the proposed routing metrics (see Section 4.5).

The joint channel assignment and routing is another example of cross-layer design for routing protocols, as channel assignment is also an essential part of a multichannel MAC. Thus, we believe that the most appropriate layer for doing such a joint design is at the MAC layer, which will make the design more efficient, because inter-layer communication is not needed anymore. Moreover, this methodology will make it much easier to integrate the routing algorithm and other MAC layer functionalities.

4.14 Open Research Issues

A summary of different categories of routing protocol is given in Table 4.2.

Based on the discussions on various routing protocols for WMNs, we know that many research problems still remain open.

- *Performance benchmark.* There are a large number of routing metrics and routing protocols available for WMNs. Considering routing protocols for other multihop

Table 4.2 Comparisons of different routing protocols for WMNs

Category of routing protocols	References of some examples	Features
Hop-count routing	[29, 54, 111, 261]	Simple in routing metric; easy to be integrated with complicated schemes of routing path selection
Link-quality based routing	[37, 70, 71]	A certain metric for link quality is used to select routing path
Interference based routing	[271, 282]	Interference or contention is directly considered in routing
Load-balanced routing	[177, 238]	Congestion or network capacity is explicitly considered
Routing with residual link capacity	[222, 234]	Residual link capacity considered in routing is helpful for load balancing
End-to-end QoS routing	[150, 253]	End-to-end QoS is ensured
Multipath routing	[136, 195, 284]	Multipath for fault tolerance or load balancing
Stability-based routing	[19, 140]	Stability has higher priority
Hierarchical routing	[163, 210]	Scalable performance; maintenance of network hierarchy
Geographic routing	[161]	Scalable performance; routing based on both position information and link quality
Distributed multichannel routing	[22]	Joint channel assignment and routing; distributed approach

wireless networks, the number is much bigger. For both researchers and users of WMNs, they are frequently confused by which routing metric and what type of routing protocols can really provide the best performance. Thus, it is necessary to provide a benchmark to investigate and compare different routing metrics and protocols. In this benchmark, it is expected to include theoretical analysis of performance bound, practical consideration of protocol design, and performance evaluation either through simulations or test beds. In [262], a comparative study is carried out for different routing strategies for WMNs. Some design guidelines are provided in [283] for multihop wireless networks. However, such work is still far from providing a benchmark for selecting routing metrics and protocols.

- *New routing metrics.* In spite of there being so many routing metrics for WMNs, new routing metrics are still desired to further improve the performance of routing protocols. In WMNs, many constraints and performance parameters are cross-related, which makes routing a more challenging problem than cellular or wired networks.

Typical constraints include interference, link retransmission count, link signal strength, packet loss ratio, hop count, link delay, and congestion. Performance parameters may include throughput, load balancing, QoS, etc. To optimize so many performance requirements under heterogeneous constraints is still an unexplored problem. It is highly possible that one routing metric is not enough to capture all constraints and performance parameters. As a consequence, how to integrate multiple routing metrics into the same routing protocol is another challenging issue. It should be noted that the need for routing metrics may be lower if the link quality can be made more predictable. For example, in some rural WMNs [92], the error rate and the received signal quality can be in a good correlation, which indicates that link abstraction is possible. With link abstraction being feasible, routing in WMNs can be much simpler. However, link abstraction is not possible in most application scenarios of WMNs.

- *Scalable routing.* This is a critical requirement for WMNs. So far, few routing protocols have really achieved this goal. Hierarchical routing protocols can only partially solve this problem due to their complexity and the difficulty of management. Geographic routing relies on the existence of GPS or similar positioning technologies, which increases cost and complexity of WMNs. Moreover, inquiry of destination position produces additional traffic load. Lastly, scalability is also related to MAC protocols. Thus, an eventual scalable routing protocol must be closely integrated with the MAC protocol.

- *Cross-layer design and layer-2 routing.* Cross-layer design between routing and MAC protocols is another interesting research topic. Cross-layer design can enhance the efficiency of routing and thus improve the performance of a routing protocol. It also helps to ensure the scalability of WMNs, since scalability depends on collaboration of all protocol layers. So far most research in routing has been focused on network layer functionality only. It has been shown that the performance of a routing protocol may not be satisfactory in this case. Mapping multiple performance parameters from layer-2 into the routing metric of a routing protocol is an example of loose cross-layer design. However, interaction between MAC and routing is so close that merely exchanging parameters between protocol layers is not adequate. Merging major functions of MAC and routing is now becoming a favorable approach.

- *Multichannel routing and dynamic channel assignment.* A multichannel routing protocol not only needs to select a path in between different nodes, but it also needs to select the most appropriate channel or radio on the path. Routing metrics developed for multiradio WMNs may not be applicable to single-radio multichannel WMNs. For a multichannel WMN, MAC/routing cross-layer design is indispensable. A major function of a multichannel MAC protocol is to dynamically assignment channels to links. To avoid conflict channel assignment in routing and eliminate redundant functions, the same dynamic channel assignment must be used at both MAC and routing protocols. Moreover, selecting a routing path involves channel or radio switching in a mesh node. Without considering such overhead through cross-layer design, the switching process may be too slow to degrade the performance of WMNs. An extreme case of MAC/routing cross-layer design is layer-2 routing, in which routing path selection, routing performance metrics, dynamic channel assignment, and efficient medium access are all considered under the same design framework. Such a methodology has been adopted into the IEEE 802.11s standard draft [122].

- *Lightweight but efficient routing protocols for mesh clients.* The existing routing protocols treat all network nodes in the same way. However, such solutions are not efficient for most WMNs, because the differences between mesh routers and clients are not well considered. Mesh routers are much more powerful than mesh clients in processing capability, energy and capacity, while they experience nearly no mobility. Thus, the routing functionality for WMNs must be different for mesh routers and mesh clients. For routing among mesh routers, the focus of design must be on increasing overall throughput, reducing overhead, achieving load balancing, providing QoS, ensuring security, and supporting mesh clients, without being constrained by energy efficiency and processing power. On the other hand, the routing functionality at mesh clients should have low complexity to save energy and react quickly to mobility and topology changes, which is achieved with the support of mesh routers.

- *Network coding and routing.* Network coding can potentially improve the performance of WMNs. Recently some research work has been reported for applying network coding to WMNs [204, 289]. In particular, the benefits of network coding to a multichannel WMN is studied in [289]. However, as network coding is still in an early phase of being applicable to a practical networking protocol, integrating network coding with routing is still a new research direction.

- *Multicast routing.* Routing for multicast applications is another important research topic. Many applications of WMNs need multicasting capability. For example, in a community or a city-wide network, video distribution is a common application. Without multicasting functionality, the network resources will be quickly occupied by video broadcasting or unicasting in WMNs. To date, much research work has been done in multicasting over wired networks, but little research has been carried out on multicasting in a WMN environment.

5

Transport Layer

Similar to the network layer, the transport layer provides two types of service: connection-oriented and connectionless. However, the purpose of having these two types of service is different in this layer. The network services are controlled through routing algorithms or various error control schemes in the link layer. Unfortunately, users have no control over such entities and the network services cannot be flawless. Thus, if a user needs to transport data traffic over a network, they have to rely on a transport layer protocol to satisfy the requirements of a certain application. More specifically, various transport layer QoS parameters must be supported by the transport layer protocol for the application layer. Typical examples include throughput, delay, and packet error ratio.

In WMNs, both real-time and non-real-time traffic will be supported by transport protocols. Real-time traffic is usually tolerant of packet losses but it is delay-sensitive. In contrast, non-real-time traffic is resilient to delay, but demands reliability. Consequently, different transport protocols are needed for non-real-time and real-time traffic in WMNs.

Several transport protocols have been developed for both wired and wireless networks in the past three decades. To the best of our knowledge, only a few transport protocols have been proposed specifically for WMNs. Since there exist many similarities between multihop ad hoc networks and WMNs, existing transport protocols for ad hoc networks are also presented here. We believe that studying such protocols provides good insights and guidelines to design transport protocols for WMNs. Based on the discussions of various transport layer protocols, we finally point out the open research issues that remain to be resolved for WMNs in this chapter.

5.1 Challenges of a Transport Layer Protocol in Wireless Environments

When a transport protocol is applied to wireless networks, many challenging issues emerge.

- *Low bandwidth:* Compared to a wired network, a wireless network usually has much lower bandwidth available. This demands higher efficiency than can be achieved by a transport protocol.

Wireless Mesh Networks Ian F. Akyildiz and Xudong Wang

- *Large bandwidth–delay product (BDP):* Recently the link capacity of some wireless networks such as 802.11n has been significantly increased. However, when they are applied to multihop wireless networks, e.g., WMNs, the large end-to-end delay results in a large bandwidth–delay product (BDP). Large BDP requires a large buffer at both receiver and sender for connectionless transport protocols and also a large congestion window for connection-oriented transport protocols.

  Theoretical results have shown that, under ideal multihop conditions and with packets of identical size, the TCP throughput is maximized for a value of the congestion window set at $n/4$, where n is the number of hops [84]. Another solution is to adopt split-connection protocols [26] such that the BDP in each split connection is small.

- *Frequent blackouts:* Due to wireless environments, network blackouts such as link failures or route failures can easily occur. Packet loss can be caused by unreliable links in addition to congestion. One of the well-known reasons for TCP performance degradation is that the classical TCPs do not differentiate congestion and noncongestion losses [278]. As a result, when noncongestion losses occur, the network throughput quickly drops. Moreover, once wireless channels are back to the normal operation, the classical TCP cannot recover quickly. The protocol in [50] enhances TCP through a feedback mechanism to differentiate between losses caused by congestion or wireless channels. This concept can be adapted to WMNs. Link failure also degrades the TCP performance. Link failure may occur frequently in mobile ad hoc networks since all nodes are mobile. As far as WMNs are concerned, link failure is not as critical as in mobile ad hoc networks, because the WMN infrastructure avoids the issue of single-point-of-failure. However, because of wireless channels and mobility in mesh clients, link failure can still easily occur. To enhance TCP performance, congestion losses and link failure also need to be differentiated. Schemes similar to explicit link failure notification (ELFN) scheme [102] can perform such differentiations.

- *Fluctuating RTT:* The end-to-end packet delay varies a lot from time to time, which can impact the measurement of RTT. However, RTT is critical to most transport protocols, especially TCP. For example, the timeout mechanism in congestion control of TCP is based on RTT.

- *Network asymmetry:* Network asymmetry is defined as the situation where the forward direction of a network is significantly different from the reverse direction in terms of bandwidth, loss rate, and latency [27] In a wireless network, especially multihop networks like WMNs, data and ACK packets of a connection-oriented transport protocol may take different paths, and thus experience different packet loss rate, latency, or bandwidth. Even if the same path is taken by data and ACK packets, they still face network asymmetry problems, because the channel condition and bandwidth on the path varies from time to time and are also different in different directions. The performance of a connection-oriented transport protocol like TCP can be severely impacted by network asymmetry. For example, the loss of an ACK caused by poor link quality in the reverse direction of a connection does not indicate congestion in the forward direction of the same connection. Consequently, TCP has poor performance for wireless multihop ad hoc networks [209, 277]. To solve the network asymmetry problem, schemes [27] such as ACK filtering, ACK congestion control, and so on have been proposed.

- *Heterogeneity:* When a transport protocol manages end-to-end communications across both wired and wireless networks, it experiences different characteristics of these two networks. Thus, the same mechanism or the same set of parameters cannot achieve optimal performance in both networks. To meet the need of heterogeneous networks, one approach that can be adopted is to split one connection into two or more connections so that each of them experiences homogeneous network characteristics. An example is indirect TCP [25] where one end-to-end connection is split into a wired connection and a wireless connection and separate mechanisms are applied for the transport protocol. Another approach that can be applied to TCP is to add a snooping module [26] in the network layer to hide timeout or duplicate acknowledgements (ACKs) from the transport layer. However, this approach was only designed for a one-hop wireless network connecting to wired networks as in the case of cellular networks.

The above issues impact all types of transport layer protocols as they interfere with the process of different control mechanism in the transport layer, such as congestion control in TCP, Stream Control Transmission Protocol (SCTP), and Datagram Congestion Control Protocol (DCCP), flow control in TCP and SCTP, rate control in DCCP. The working mechanism of User Datagram Protocol (UDP) may not be impacted by such issues owing to its simplicity. However, the performance of UDP can still be significantly degraded in a wireless network.

In WMNs, the above-mentioned issues can be more severe because: (1) multiple hops of wireless links result in a higher chance of packet loss, link failure, path asymmetry, and RTT fluctuation; (2) WMNs are generally composed of different wireless networks. Thus, transport protocols proposed for cellular networks or wireless LANs are usually not effective for WMNs. For example, the snooping module proposed for cellular networks [27] cannot be directly applied to WMNs, as it does not consider the situation of a multihop wireless network.

In order to improve the performance of end-to-end communications in WMNs, two approaches can be adopted. The first one is to enhance protocol performance in the lower layers. Typical examples include reliable MAC protocols in the link layer. This option is preferred by UDP as it has no sophisticated mechanisms for reliability in the transport protocol. Of course, reliable lower layer protocols are also beneficial to other transport protocols. The second approach is to enhance existing transport protocols or design new transport protocols for WMNs. These two options are orthogonal and are usually employed simultaneously.

5.2 Transport Layer Protocols for Multihop Ad Hoc Networks

As the core network of a WMN is a multihop ad hoc network in nature, the design guidelines and methodologies in existing transport protocols proposed for multihop ad hoc networks can be adopted for WMNs. Of course, considering the specific features of WMNs, modifications may be necessary.

5.2.1 Protocols for Reliable Data Transport

To date, a large number of reliable transport protocols have been proposed for multihop ad hoc networks. They can be classified into two types: TCP variants and entirely new transport protocols. A TCP variant [50, 68, 102, 176] is developed based on the classical TCP of wired networks, but is enhanced by considering the specific features of multihop ad hoc networks.

TCP Variants

The performance of classical TCPs degrades significantly in multihop ad hoc networks. In this subsection, we discuss various enhanced TCP protocols by addressing the fundamental problems in the classical TCP and the corresponding solutions.

According to different TCP components that are impacted by the environment of a multihop ad hoc network, TCP variants can be classified into several types: (1) differentiation between packet losses and congestions; (2) window optimization; (3) acknowledgement optimization; (4) adaptive control of transmission rates.

Packet Loss Versus Congestion In a multihop ad hoc network, packet loss can be due to either congestion or other errors. In fact, the latter case is even more common than the former case. The packet loss due to errors can be caused by many factors. Typical examples include low link quality, route failure, route change due to mobility, and so on. If such packet loss is considered as congestion, then TCP will frequently invoke congestion control, which severely degrades the performance. To enhance TCP performance, certain schemes are needed to differentiate such packet loss from congestion. The most frequently used method is to detect such events and feed back such information to the TCP sender.

In [50] congestion and packet loss due to route failure are handled separately in TCP. The basic idea is to use a feedback scheme called *TCP-feedback* (TCP-F) to explicitly inform the source of the route failure. Although feedback-based schemes such as explicitly congestion notification (ECN) have been proposed for TCP, no reliability is ensured for sending feedback information, and thus, the congestion notification may not arrive at the source. TCP-F detects the route failure in the networking layer as part of a routing protocol. Once a failure is detected at a node, a route failure notification is sent from this node to the next-hop node until it reaches the source node. When the source node receives such a message, it enters a snooze state, i.e., it stops sending further packets and take the following actions: (1) freeze all timers and windows; (2) start a route failure timer whose value is determined according to the worst case of route re-establishment by the underlying routing protocol. The source stays in this state until a route re-establishment message is received. Once a new route is set up, all unacknowledged packets are flushed out without waiting for acknowledgements. Following this step, the source node falls back to the normal state of a standard TCP protocol.

A method similar to TCP-F is explicit link failure notification (ELFN) studied in [102]. ELFN was designed to differentiate congestion from packet loss due to link failure. ELFN notified link failure to the sender using Internet Control Message Protocol (ICMP) message or routing messages in a similar way to that of TCP-F. Once link failure is detected, the sender disables the transmission timer and enters the *standby* mode. During this mode, the sender periodically sends a probe packet to check if a new route has been established. If the answer is positive, then the sender goes back to the normal state of TCP.

In [73] a sender-based protocol called fixed retransmission timeout (RTO) is proposed. It does not rely on feedback from the lower layers. Rather, a heuristic is employed to distinguish route errors and congestion. Specifically, when RTOs occur consecutively, i.e., an ACK is not received before the second RTO expires, the sender assumes that a route error has occurred. Thus, the unacknowledged packet is retransmitted again without doubling the RTO. Then, RTO remains fixed until the route is re-established and the retransmitted packet is acknowledged.

An end-to-end approach called TCP Detection of Out-of-Order and Response (TCP-DOOR) is presented in [254]. TCP-DOOR attempts to improve TCP performance by detecting and responding to out-of-order (OOO) delivery events. The detection of OOO events is performed at both ends, i.e., the sender detects the OOO ACK packets and the receiver detects the OOO data packets. However, OOO events can be detected only after a route has recovered from failures. Therefore, TCP-DOOR is less accurate and responsive than a feedback-based approach, which can determine whether congestion or route errors occur in a responsive manner.

In WMNs, mobility usually exists in the last hop. Thus, the chance of route failure or link failure is much lower than mobile ad hoc networks. However, such failures are still common. Thus, differentiation between congestion and packet loss due to errors needs to be considered in WMNs. On the other hand, reliability schemes in the link layer or the network layer may be more effective for WMNs than mobile ad hoc networks because of the lower mobility in WMNs. With a more reliable link or network layer, it is possible that feedback-based TCP enhancements can be simpler but more effective.

Window Optimization The TCP window determined by its congestion control scheme is designed for wired networks and cannot achieve optimal performance when a multihop wireless network is considered. For example, in a multihop wireless network employing 802.11 MAC as the link layer protocol, the buffer overflow is rare, and packet loss is usually caused by link-level contention. Based on the investigation in [84], link-layer drops exhibit a graceful behavior: when the TCP window is larger than W^*, the link drop probability gradually increases; it saturates when the TCP window reaches a larger value $\bar{W}$. Thus, in order to get the best TCP throughput, the TCP window must be optimized at W^*. However, the adaptation of TCP window is designed considering the buffer-overflow behavior, which is much different from link-layer drop behavior. As a result, TCP keeps increasing window size until a value much larger than W^*. Such a large TCP window causes a much larger link-layer drop probability, and thus reduces TCP throughput.

Thus, optimizing TCP window is beneficial for maintaining a high throughput for TCP in a multihop wireless network. However, to explicitly calculate such a TCP window is infeasible for a number of reasons. Firstly, the window is closely related to the MAC behavior in a multihop wireless network. Secondly, the optimized window of one flow may be impacted by other flows in the same network. Thirdly, the optimal window size is also related to the number of hops, routing paths, and other factors. Thus, instead of explicitly deriving the optimal TCP window, an indirect solution is proposed in [84] based on random early detection (RED) and adaptive pacing in the link layer. The link RED records the average number of retries in the MAC layer and uses this number to determine whether packets in the buffer need to be dropped or marked. When the average number of retries exceeds a threshold, adaptive pacing is invoked to increase the backoff timer by the transmission time of the previous packet. In this way, better coordination among nodes can be achieved, which in turn fine tunes the TCP window so that it is as close to W^* as possible.

Acknowledgement Optimization In a wireless multihop network that employs a contention-based MAC such as 802.11, the ACKs and data packets are usually not received in a bursty way, as the MAC protocol tries to make sure that each node on the routing path sends one frame at a time. As a result, a sender node may trigger spurious retransmissions and the number of generated ACKs may be large. Recent research points out that nearly 70% of TCP data packet losses occur due to collision with the TCP ACKs, thus motivating the need to limit their number [252].

In order to improve the TCP performance in this type of situation, multiple ACKs can be combined into one using a cumulative ACK scheme, or ACKs can be delayed by using a standard delayed ACK scheme. However, such schemes usually assume a fixed timeout interval, which is not the case for multihop wireless networks. In [68] a dynamic adaptive acknowledgement scheme is proposed where the idea of cumulating a high number of delayed ACKs is combined with the dynamic reaction scheme [17]. The timeout interval is adaptively adjusted by considering packet inter-arrival times. In this way, the receiver delays just enough time for ACKs and avoids spurious retransmissions even if the delay in a multihop wireless network can be variable from time to time.

Adaptive Rate As explained in [68] cumulative ACKs are desired by TCP in a multihop wireless network, and they can also cause problems due to bursty transmissions. This problem may not be severe when adaptive ACK is adopted. However, for cumulative ACKs based on fixed timeout interval, a solution is needed to control the transmission rate; otherwise, the congestion control at the sender can invoke bursty transmissions and cause further contentions in the link layer. One example of such schemes is TCP adaptive pacing (TCP-AP) [77].

TCP-AP adjusts the transmission rate by considering several metrics: congestion window, contention on the end-to-end path, and spatial-reuse constraint. The contention on the routing path is determined based on a coefficient of RTT variations (cov_{RTT}), while the spatial-reuse constraint is calculated based on the four-hop propagation delay (FHD) starting from the sender. With these three parameters, the TCP-AP works as follows. The inter-packet delay (D_{ip}) is computed based on FHD and cov_{RTT} according to $D_{ip} = FHD(1 + 2cov_{RTT})$. This parameter is then used as the timeout value of the pacing timer. Once a timeout occurs, the congestion window is checked to see if it is enough for sending a new packet. If the answer is positive, then a new packet is sent; otherwise, the TCP stays idle.

As shown in the procedure for TCP-AP, the adaptive pacing scheme is a hybrid scheme of sender rate control and congestion control. It has a few advantages: the TCP end-to-end semantics are not impacted and lower layer protocols such as routing and MAC require no change. However, the effectiveness of TCP-AP totally depends on two assumptions: the mechanism of rate control is effective and the estimation of contention and spatial reuse constraint is accurate. Although they are justified through simulations under some specific network topologies in [77], whether or not they are effective to other network topologies remains unknown.

Separate Sublayer for New TCP Functions It should be noted that TCP variants may need more or fewer modifications to the standard TCP/IP protocol suite. In some cases, some modifications are not desired. To improve TCP performance for ad hoc networks without impacting the TCP/IP protocol suite, some solutions have been proposed as an intermediate protocol between TCP and the network layer. An example is the adaptive TCP protocol (ATCP) [176] for mobile ad hoc networks. This protocol is implemented between TCP and IP layers. The objective of ATCP is to make sure that the standard TCP is not impacted by issues such as rerouting timeout, packet loss due to error, out-of-order packet due to multipath routing, and network partitions, which are common in a mobile ad hoc network. To this end, ATCP includes several critical functions: (1) when network partition occurs, the TCP sender is advised into the persistent state instead of invoking timeout; (2) when packet loss due to error instead of congestion happens, the TCP sender retransmit packets without triggering congestion control; (3) if network congestion is truly detected, the regular TCP congestion is invoked. In [176] the differentiation between packet loss due to error and congestion, and the detection of network partition or route failure can be known to ATCP. However, these are not trivial tasks in an mobile ad hoc network.

Entirely New Transport Protocols

As discussed before, many fundamental problems exist in TCP. Therefore, some researchers have started to develop entirely new transport protocols for ad hoc networks.

In [246], the ad hoc transport protocol (ATP) is proposed for ad hoc networks. Transmissions in ATP are rate-based, and quick-start is used for initial rate estimation. The congestion detection is a delay-based approach, and thus ambiguity between congestion losses and noncongestion losses is avoided. Moreover, in ATP, there is no retransmission timeout, and congestion control and reliability are decoupled. By using an entirely new set of mechanisms for reliable data transport, ATP achieves much better performance (e.g., delay, throughput, and fairness) than the TCP variants.

Despite its advantages, an entirely new transport protocol is not favored by WMNs owing to the compatibility issue. ATP assumes that the wireless network can be stand-alone. While this may be true for mobile ad hoc networks, it is invalid for WMNs, since WMNs will be integrated with the Internet and many other wireless networks. Transport protocols for WMNs must be compatible with TCPs in other networks.

5.2.2 Protocols for Real-Time Delivery

To support end-to-end delivery of real-time traffic, UDP instead of TCP is usually applied as a transport protocol. However, the simple mechanism of UDP cannot guarantee real-time delivery and may starve TCP connections in the same network. Thus, additional protocols such as real-time protocol (RTP) and real-time transport protocol (RTCP) are needed to work over UDP. On top of RTP/RTCP, rate control protocol (RCP) is also needed for congestion control.

To date, many RCP protocols have been proposed for wired networks. They can be classified into two types: additive-increase multiplicative-decrease (AIMD)-based or equation-based. However, these protocols are not applicable to wireless networks because of the existence of packet errors and link failures. Thus, differentiation between losses caused by congestion or wireless channels needs to be taken into account with RCP. Various loss differentiation algorithms (LDAs) with congestion control are studied in [49], where only one wireless link is considered on the path between sender and receiver. It is shown in [49] that the hybrid LDA is the most effective. However, this result may not be applicable to WMNs, since multiple wireless links are on the path between receiver and sender.

An analytical rate control scheme is proposed in [5] for end-to-end transmission of real-time traffic over both wired and wireless links. However, whether this scheme is applicable to WMNs needs to be researched further.

To date, few rate control schemes are available for mobile ad hoc networks. Recently, an adaptive detection rate control (ADTFRC) scheme has been proposed for mobile ad hoc networks in [83], where an end-to-end multimetric joint detection approach is developed for TCP-friendly rate control schemes. However, to really support real-time delivery for multimedia traffic, the accuracy of the detection approach is still insufficient. In addition, all noncongestion packet losses due to different problems are processed in the same way [83]. This may degrade the performance of the rate control scheme.

To date, no RCP has been proposed for WMNs. In addition, no effective RCPs for ad hoc networks can be adopted and tailored for WMNs. Thus, RCP for WMNs is a new research area.

5.3 Transport Layer Protocols for WMNs

To date there exist only a few transport layer protocols for WMNs for the following possible reasons. Firstly, when WMNs are deployed, usually more attention is given to other protocols such as routing and MAC, and the standard TCP or UDP protocol is used as the transport layer protocol. This methodology is reasonable in practice, because a new transport protocol or enhancement to a standard transport protocol requires installation of a new software or a software patch to the operating system on a user’s device such as a PC or handset, which is not always preferred. If routing and MAC protocols can provide enough reliability and quality so that standard transport protocols are used, this means a more convenient solution for users and a less complicated system for service providers and system administrators. Unfortunately, because of the challenging issues involved in multihop wireless networks such as WMNs, standard transport protocols cannot always meet the needs of many applications. Secondly, people may think that the transport protocols proposed for mobile ad hoc networks or other multihop networks can be applied to WMNs. However, because of different features between WMNs and other multihop wireless networks, these protocols may not be a good choice for WMNs. For example, many TCP enhancements for ad hoc networks focus on route failure due to mobility. However, such events are rare in WMNs, especially when the routing protocol has been designed considering the special features of WMNs. Moreover, most existing transport protocols for ad hoc networks only consider an isolated multihop wireless network. For WMNs, typically the network is connected to the Internet backbone via some gateways and a large amount of traffic come from, or goes to, the Internet backbone instead of flowing within WMNs. This kind of network architecture leads to two features that need to be considered in a transport protocol for WMNs. The first one is that we may not be able to assume that the transport entity can be modified or changed, because end points may be inside the Internet backbone rather than in WMNs. The other one is that the traffic in WMNs is not uniformly distributed, but tends to be more concentrated at nodes closer to a gateway. Such a traffic pattern makes the interactions between MAC and transport layers significantly different from a general multihop wireless network, as studied in a special case of WMNs i.e., wireless backhaul networks in [87]. As a result, schemes such as TCP-AP [77] or LRED [84] may not be able to deliver good performance in WMNs.

The mesh router generally has a number of mesh clients under it, and must collect the packets from each individual flow for all the connected devices. This results in a significant buffer usage as these packets must traverse in a multihop manner to the gateway, incurring transmission and contention delays at each hop. TCP Vegas and its descendants, such as FAST TCP [268], use buffer occupancy as a congestion metric. This is advantageous as the congestion is detected earlier when the buffer is partially filled, as compared to loss-based TCP variants where packets are dropped due to buffer overflow. However, a single gateway may serve different individual mesh networks, possibly with different TCP flavors. In such cases, the delay-based algorithms suffer from the aggressive transmission rate changes employed by the loss-based algorithms.

With the above issues in mind, we believe that developing transport protocols considering specific features of WMNs is critical to the overall performance of WMNs. In this subsection, several transport protocols that have considered some features of WMNs are discussed. However, as there has not been enough attention paid to the transport layer of WMNs, these protocols are far from addressing all the issues in a transport protocol for WMNs.

5.3.1 Transport Protocols Based on Hop-by-Hop Control

In WMNs, the most frequent cause of packet loss is bit error in packets. This is different from what is seen in a mobile ad hoc network, where route or link failures are the major reason for packet loss. Thus, it is a wise strategy to consider link layer performance enhancement as a functional block of a transport protocol.

On the other hand, considering end-to-end transmission at the transport layer, if a packet is lost at an intermediate node due to bit-error, the end-to-end retransmission not only wastes all the successful transmissions before this node but also needs the packet to traverse the same path again, which can lead to more delay and more waste of resources. Moreover, a large number of ACKs can be generated due to the end-to-end mechanisms, even if delayed-ACK schemes are adopted. These ACKs consume a large percentage of bandwidth.

As a result, it is highly desirable to develop transport protocols based on hop-by-hop control. In what follows, two such types of transport protocols are discussed.

In [223] a “stateful” transport protocol is developed by using hop-by-hop retransmission instead of end-to-end transmission for packets lost due to bit error. Since this protocol requires the routers inside the network to maintain states for transport layer functions, it is called a “stateful” transport protocol. Due to link-layer retransmission for most lost packets instead of end-to-end retransmission, the congestion control scheme in the standard TCP is not applicable. Thus, the congestion control is performed through a rate control scheme at the sender of a connection.

In WMNs, not all nodes can implement proprietary protocols. For example, clients to be connected to WMNs may have to use standard TCP. And nodes residing in the wired network usually use standard TCP too. To support connections to these nodes, a proxy protocol is needed at the ingress/egress nodes to split the end-to-end connections into three subconnections: a subconnection from mobile clients to ingress node of the WMN, a subconnection from the ingress to the egress node of the WMN, and a subconnection from the egress node to the end node in the wired network.

The core function of the stateful transport protocol is applied to the second subconnection and is called a link-aware reliable transport protocol (LRTP). It consists of three key components.

- **Rate control.** In order to carry out rate control at a sender of a flow, an appropriate transmission rate of this flow needs to be calculated. The first step is to measure link capacity based on the service time of link-layer packets. The service time is the time interval from when a packet is scheduled for transmission until a MAC ACK is received. Thus, it takes into account the transmission time, access delay, and contentions. The measured link capacity is then allocated to all flows on the same link using the max-min algorithm. This allocation is a local scheme, so it cannot guarantee conflict between links using the same channel but in the interference range, which can cause hidden node issues and unfairness in channel sharing. To improve the situation, a multihop inter-node coordination scheme is needed to resolve the conflict.

  Once the transmission rate on each flow is calculated, it is embedded in a packet of a flow as a stamp. When the packet sees a lower value on the next link, the stamp will be overwritten by the new value; otherwise, no change is necessary. Once the receiver gets this kind of information, it calculates an average value and then sends it back to the sender via a periodic mechanism. The sender adjusts its transmission rate accordingly.

- **Link-layer retransmission.** When a packet is sent but gets lost, the packet can be retransmitted in the link layer instead of waiting for the receiver to detect the packet loss and then invoke retransmission and control. The process in the latter case is too inefficient. In LRTP, the packet is retransmitted once it is detected as having been lost. However, to avoid head-of-line blocking, a packet to be transmitted cannot be sent again immediately. LRTP maintains a queue for each link and a round-robin scheme is used to schedule packet transmission among all queues. Once a packet is to be transmitted, it is put back into the queue and waits for the scheduling scheme to select it again for transmission. Thus, the LRTP retransmission does not have a head-of-line blocking issue. It should be noted that LRTP retransmission works on top of the MAC-layer retransmission instead of replacing it.

- **NACK and end-to-end retransmission.** Although LRTP handles packet loss due to bit errors, it is possible that buffer overflow or congestion can cause packet loss. In this case, the LRTP retransmission is not helpful in recovering this type of loss. Thus, another mechanism is needed. More specifically, the receiver is relied on to detect this kind of packet loss. Once such an event is detected, it sends negative ACK (NACK) back to the sender. With a NACK, the sender knows which packet needs to be retransmitted. Thus, LRTP integrates both link-layer retransmission and end-to-end retransmission.

Although LRTP can potentially provide better fairness and throughput performance than a standard TCP, it also contains a few critical problems.

- The link capacity estimation scheme may not provide an accurate solution. This scheme claims to be able to capture contention, but in fact contention is not a parameter that is related to the link to be measured but many other links in the same interference range.

- The input rate of a flow, which is measured according to the incoming packets, is used to determine the bandwidth requirement of a flow. However, before an appropriate rate is determined for the sender of a flow, the packets in a flow do not really reflect the bandwidth requirement of this flow. To resolve this issue, LTRP uses another parameter, the current bandwidth share, for the bandwidth requirement. However, the current bandwidth share is not an accurate value either, as the bandwidth requirement of the current flow is not known yet. Thus, whether or not a converged rate can be reached within a reasonable time period remains a question.

- The link-layer retransmission scheme is strongly dependent on the functionality of the MAC protocol. Where different mechanisms are implemented in the MAC layer, this scheme may not be applicable. For example, in IEEE 802.11n, a packet is not simply sent and acknowledged. Instead, multiple packets are aggregated and then sent out according to a frame-aggregation process. The packets in an aggregated packet can be from different flows.

- The inter-node coordination of bandwidth allocation can be a problem too. In fact, for a multihop network, the conflict cannot be really resolved unless the allocation of the entire network is coordinated.

It should be noted that LRTP does not follow any TCP semantics. However, this type of methodology is receiving more and more attention, as it can potentially achieve better performance than the TCP variants. Hop-by-hop control based transport protocols have some shortcomings. For example, all nodes in the network have to maintain states for transport protocols. This is doable for mesh routers, but increases the complexity, and demands higher computational power, in mesh routers. Nevertheless, if a hop-by-hop control scheme can really achieve a good tradeoff between enhanced performance, cost, and feasibility, it is still a promising option for transport protocols of WMNs.

5.3.2 Datagram Congestion Control Protocol (DCCP) for WMNs

To support multimedia applications in WMNs, it is desirable to consider DCCP instead of UDP, because DCCP performs congestions control and is TCP-friendly. Thus, it is very interesting to evaluate the performance of DCCP over WMNs. In [198], some simulation results are presented which demonstrate the performance of DCCP in delivering multimedia traffic over WMNs. It is shown that DCCP can provide smooth throughput for multimedia applications if there are no competing non-DCCP flows. However, if TCP or UDP flows exist, the smoothness drops quickly and may not satisfy the need of multimedia traffic. Thus, how to improve the performance of DCCP over WMNs is still an open research problem.

When hop-by-hop retransmission and rate control are used for a reliable transport protocol, DCCP may experience different impact than that from UDP or TCP. How to make DCCP coexist with this type of new reliable transport protocol is also an important question to answer.

5.4 Open Research Issues

A full summary of all the major transport protocols for multihop wireless networks including WMNs is presented in Table 5.1.

As discussed above, many research issues remain open for both reliable transport protocols and real-time transport protocols.

For reliable transport protocols, TCP variants have the advantages of simplicity and providing easy compatibility with standard TCP protocol suites. Although many TCP variants developed for mobile ad hoc networks can be adopted for WMNs, they tend to be too complicated for WMNs. For example, WMNs may not experience frequent link or route failures. Thus, more efficient schemes for TCP enhancement are expected for WMNs. In particular, a better loss differentiation scheme, congestion detection scheme, retransmission mechanism, and congestion control algorithm are needed for WMNs. Moreover, in order to reduce the impact of network asymmetry on TCP performance, cross-layer optimization is a challenging but effective solution, since all the problems of TCP performance degradation are actually related to protocols in the lower layers. For example, it is the routing protocol that determines the path for both TCP data and ACK packets. To avoid asymmetry between data and ACK packets, it is necessary for a routing protocol to select an optimal path for both data and ACK packets but without increasing the overhead. We also know that the link layer performance directly impacts packet loss ratio and network asymmetry. Thus, in order to reduce the possibility of network asymmetry, the MAC layer may need to treat TCP data and ACK packets differently. As studied in [235], a MAC protocol like CSMA/CA may cause starvation of congestion controlled flows as in TCP, and thus enhancement in the MAC protocol, e.g., contention-window based counter-starvation policy, is needed to improve the transport layer performance.

For non-TCP based reliable transport protocols, cross-layer design has been adopted. In LRTP, retransmission and rate control are mainly executed in the link layer. However, improving the performance of these schemes is still an open problem. Moreover, how to design a better link/transport cross-layer protocol to achieve higher performance and better compatibility to TCP is an interesting topic. As non-TCP reliable transport protocols do not follow TCP semantics but WMNs are usually connected to clients and nodes using standard TCP, it is critical to have a solution to support compatibility with standard TCP.

For real-time delivery, no existing solution from ad hoc networks can be adopted and tailored for the use of WMNs. If UDP is employed as a transport protocol, then brand-new RCPs need to be developed considering the features of WMNs. If DCCP is adopted, it is necessary to improve its performance so that it meets the needs of multimedia applications in WMNs and is also friendly to TCP flows.

Multicasting functionality is demanded by many real-time applications. For example, video streaming or Internet Protocol (IP) TV (IP-TV) may need multicasting to improve the bandwidth efficiency. However, multicasting in WMNs, whether requiring reliability or not, demands new transport protocols. In addition, cross-layer design is important for these protocols as multicasting is closely related to both routing and transport protocols. It should be noted that even for wired networks the reliable multicast transport (RMT) protocol is still being actively developed by researchers, especially the RMT workgroup of the Internet Engineering Task Force (IETF). Some approaches have been released in request for comments (RFCs), but how to extend such protocols to WMNs is an open research problem.

Table 5.1 A comparison of transport protocols for multihop wireless networks

Protocol	Type	Applicability	Features	Drawbacks
Packet loss differentiation schemes [50, 73, 102, 254]	TCP variants	Ad hoc networks	Feedback for detecting congestion; differentiating different packet losses	Notification may be lost; mechanisms of differentiations may not be accurate
Window optimization [84]	TCP variant	Ad hoc networks	Calculate optimal TCP window for wireless networks	Hardness of deriving optimal window
Acknowledgement optimization [68]	TCP variant	Ad hoc networks	Dynamic interval for cumulative ACKs	No mechanism for improving congestion control
Adaptive rate scheme [77]	TCP variant	Ad hoc networks	Adaptive pacing based on hybrid rate and congestion control	Performance limited by accuracy of contention estimation
ATP [246]	Rate control based, reliable	Ad hoc networks	Decoupling reliability and congestion control	Totally incompatible with TCP
ADTFRC [83]	Rate control based	Mobile ad hoc	Multimetric joint detection based rate control	No packet loss differentiation
Analytical rate control [5]	Rate control based	hybrid networks	End-to-end rate control for real-time traffic	Difficulty in deriving rate
LRTP [223]	Based on TCP	WMNs	Hop-by-hop retransmission, rate control for congestion control	Loss of compatibility with TCP; hard to derive rate
DCCP Mesh [198]	Based on DCCP	WMNs with multimedia traffic	Smooth throughput for multimedia traffic	Poor performance when coexisting with non-DCCP flows

Besides the Internet, WMNs will also be integrated with various wireless networks such as IEEE 802.11, 802.16, 802.15, etc. The characteristics of these networks may be significantly heterogeneous due to different network capacity and behaviors of error control, MAC, and routing protocols. Such heterogeneity renders the same transport protocol ineffective for all networks. Applying different transport protocols in these networks will make the integration complicated and costly. As a consequence, proposing an adaptive transport protocol is the most promising solution for WMNs. An adaptive transport protocol is proposed in [6] for an integrated network of wireless LANs, cellular networks, Internet backbone, and satellite networks. However, due to the hybrid ad hoc and infrastructure architecture, which is much different from the integrated network in [6], new adaptive transport protocols need to be proposed for an integrated WMN.

6

Network Security

Security is always a concern to users of wireless networks. Without being comfortable with a satisfactory level of security, users lack motivation to subscribe to wireless services. Therefore, security plays a critical role in wireless networks. In WMNs, security becomes even more critical, for the following reasons.

- **Multihop wireless network security:** Many security schemes for wireless networks are focused on one-hop communications. The multihop architecture renders these schemes insufficient to protect a WMN from being attacked.
- **Multitier security:** In WMNs, security is needed for wireless access from mesh clients to mesh routers and also for wireless connectivity among mesh routers. Mesh routers usually belong to a service provider, while mesh clients can be any users. Such features make the security issue different from that in any other wireless network such as wireless LANs or mobile ad hoc networks. The security mechanism for communications among mesh routers must be different from that in the wireless access part.
- **Multisystem security:** For the benefits of better wireless services, WMNs usually involve interoperation of multiple wireless networks such as IEEE 802.11, IEEE 802.16, IEEE 802.15 based wireless networks. Both security architecture and schemes are much different from one system to another. To make all wireless networks interwork smoothly, the first barrier that needs to be passed is to develop a scheme so that inter-network communications can be provided seamlessly without compromising security in all networks.

6.1 Security Attacks in WMNs

Security attacks occur in all protocol layers ranging from physical layer to transport layer and all protocol planes including both data and management/control planes. Usually attacks in a lower protocol layer are more harmful than those in a higher protocol layer, since the protocol stack is developed bottom up.

Wireless Mesh Networks Ian F. Akyildiz and Xudong Wang

Security of wireless networks can be classified into two types: information security and network security. In WMNs, some attacks target at only information security, while others focus on the network security. It is also possible that some attacks may try to compromise both.

In this section, we explain the most typical security attacks in WMNs.

- **Channel jamming:** Channel jamming directly targets the network security by simply attacking the physical layer. Thus, it is the most brute-force attack. A WMN can easily be brought down by this type of attack. However, traffic jamming can easily be detected, and is also prohibited by law if a licensed band is being used. In a shared frequency band, e.g., ISM band, channel jamming is rather common, simply because the same channel can be selected by different WMNs.

- **Unauthorized access:** In WMNs, before a node starts to use wireless services, it has to join the network, which involves a process of network association and authentication. This normally occurs in the management plane of the MAC protocol. If the authorization and authentication fail in this process, an unauthorized node can access the network. This type of attack does not impact the network security but information security.

- **Eavesdropping:** This is very common when information is not encrypted. As long as a strong enough encryption scheme is employed, eavesdropping can be avoided.

- **Traffic analysis:** This is an attack on information security, and does no harm to the network security. Traffic analysis is usually done in the lower layers such as physical and MAC layers when the information in a traffic flow cannot be accessed. By analyzing the traffic pattern, however, an attacker can retrieve meaningful information for his benefit. Traffic analysis is hard to detect since it is passive and is not involved in the network activities of WMNs.

- **Message forgery:** This attack involves capturing a security hole in a wireless network where message integrity is not ensured. Thus, attackers can inject forged messages into the network to cause malfunction of protocols in different layers. In other words, message forgery is a type of attack to network security and can occur at protocol layers such as MAC and routing.

- **Message replay:** When message integrity is enforced, an attacker can still pose a threat to the network by replaying some authorized messages. Message replay can also occur in MAC and routing layers, and may cause malfunction of these protocols.

- **Man-in-the-middle attack:** In WMNs, an attacker can reside in between a mesh client and a mesh router and try to intercept or manipulate the communication between the mesh client and the mesh router. This kind of attack can also happen between two mesh routers. An example of man-in-the-middle attack is when an attacker sets up a rogue mesh router to make other mesh routers or mesh clients communicate with it. This is really a critical attack, since both network and information security can be compromised, and both mesh routers and mesh clients can be impacted.

6.2 Counter-Attack Measures

In wireless networks including mobile ad hoc networks and WMNs, there are three categories of method that can defend against security attacks.

- **Encryption and cryptographic protocols:** To ensure security, information flowing through the network is encrypted. The security key used in the encryption must be exchanged between senders and receivers. Thus, key management is also an important task. Moreover, cryptographic protocols, which are usually in an application or transport layer, can be designed based on the encrypted information to achieve confidentiality and perform authorization, authentication, and message integrity check (MIC).

- **Secure networking protocols:** Protocols ranging from routing to physical layers should have security counter-attack measures. In mobile ad hoc networks, the most widely researched secure networking protocol is secure routing protocol, and few schemes are proposed for secure MAC protocols. For WMNs, research efforts are needed to change this situation. Secure MAC protocols should be paid more attention, even than secure routing protocols, because routing is built on top of a MAC. In the physical layer, advanced digital signal processing and communication technologies are needed for anti-jamming.

- **Security monitoring and response systems:** Security monitoring and response system are needed to detect security attacks, monitor service disruption, and respond quickly to attacks. There are two motivations for doing so. The first is to take action to stop attacks before security is actually broken. However, no matter what security schemes are adopted to defend against attacks, a wireless network, especially multihop networks like WMNs, are exposed to so many attacks that the line of defense still has a chance to be broken. In this case, certain actions should be taken to prevent attacks from further threatening the security of the network, which is the second objective of the security monitoring and response.

To study the existing security schemes for WMNs, we first investigate the security mechanisms in several wireless networks that are closely related to WMNs, i.e., IEEE 802.11 wireless LANs, IEEE 802.16 wireless Metropolitan Area Networks (MANs), and mobile ad hoc networks. Security technologies for these wireless networks have become building blocks for WMNs. Investigating security schemes of these wireless networks will help us to find out what existing solutions can be used and what are the remaining issues to be resolved for WMNs.

6.3 Security Schemes in Related Wireless Networks

6.3.1 Security of IEEE 802.11 Wireless LANs

The first security protocol defined in the 802.11 standard is called wired equivalent privacy (WEP). It contains several security flaws, but is still being used widely, due to its simplicity. In order to ensure full security of 802.11 wireless LANs, the 802.11 “task group” was working on a new security solution until 2004 when the 802.11i security standard was approved and released.

During the standardization process of 802.11i, WiFi Alliance developed a new specification, called Wi-Fi protected access (WPA), based on a draft version of 802.11i to enhance the security of 802.11 wireless LANs. After the 802.11i standard was finally approved, WiFi Alliance followed mandatory requirements of 802.11i and developed another security specification, called WPA2.

Wired Equivalent Privacy (WEP)

The security mechanism of WEP consists of three major components: confidentiality via Rivest Cipher 4 (RC4) based stream cipher, CRC based integrity check, and pre-shared key (PSK) based challenge-response handshake for authentication.

Given a key R, plaintext X of a packet is encrypted into Y as

$$Y = R \oplus X. \tag{6.1}$$

If two plaintexts X_1 and X_2 are encrypted into Y_1 and Y_2 using the same key K, then there is the following interesting result:

$$Y_1 \oplus Y_2 = X_1 \oplus X_2. \tag{6.2}$$

Such a relationship between encrypted data helps malicious users to easily decipher received messages. Thus, it is necessary to have a unique key for each packet. In WEP, the key generated through a key generation function based on a WEP key and an initialization vector (IV), i.e., $R = RC4(K, IV)$.

Since K is mostly static in WEP, the uniqueness of the RC4 key totally depends on IV. In WEP, IV contains 24 bits, and thus an IV is repeated every 2^{24} packets. Packets with the same IV can also help malicious users decrypt received packets. Thus, to improve confidentiality, either WEP K needs to be changed dynamically or the number of bits for IV needs to be longer.

In WEP, data integrity is achieved by CRC check. However, CRC is effective for detecting bit errors in packets, but not for authentication. Although it is simple, an attacker can change the contents of a packet without a lot of effort. For example, he can flip a bit in the encrypted data and then change the CRC as well. Thus, a better data integrity mechanism is needed in order to improve WEP performance.

WEP authentication between two nodes is achieved through a challenge–response handshake scheme. There are two options of authentication specified in the basic 802.11 standard: open system authentication and shared-key authentication.

Open system authentication is essentially a null authentication algorithm. A node can be authenticated as long as the node receiving the request also uses open system authentication. Thus, authentication can always be accomplished between the two nodes using open system authentication. In other words, no challenge–response mechanism is implemented in open system authentication.

When shared-key authentication is applied, a node initiating the authentication exchange is called the *requester* and the destination of this initial authentication packet is called the *responder*. The requester sends a request to the responder using a shared key. If the responder has authenticated the requester, it generates a challenge text and then sends the encrypted message back to the requester. It should be noted that the generation of a challenge text also follows the WEP encryption procedure, but its key and IV do not need to be sent to the requester, since the requester only needs to copy the challenge text and does not need to know how the challenge text is generated. After copying the challenge text, the requester sends the encrypted data back to the responder. When the responder gets this encrypted message, it needs to decrypt the message and then to compare the received challenge text with the original one. If both challenge texts match, authentication is successful; otherwise, authentication has failed. In fact, authentication can fail due to unsuccessful decryption or integrity check. As a last step, the responder sends the authentication status back to the requester.

WEP authentication can easily be broken due to weak protection of WEP confidentiality and integrity check.

Based on WEP, the basic 802.11 standard specifies authentication and privacy services for 802.11 wireless LANs. Authentication can be open system or shared-key authentication, as explained before. Once nodes are authenticated, the privacy is ensured through WEP encryption and integrity check. A general procedure is described as follows.

- Authentication is carried out via open system or shared-key authentication.
- For an authenticated sending node, once it gets a packet, it first generates CRC for this packet as a integrity check value (ICV).
- The node generates an IV, and then an RC4 key based on the IV and WEP key. The packet together with ICV is finally encrypted using the RC4 key. The next step is to append the IV to the encrypted packet. The final packet is then sent out to a destination node.
- When an authenticated receiving node receives the packet, it first gets the IV and derives the RC4 key. Based on this key, the packet is decrypted and is then checked for integrity. If these steps work correctly, a packet is successfully received; otherwise, the packet is declared as an incorrect packet.

WPA

WEP security is weak in all aspects: encryption can be broken because of static WEP key and high frequency of repeating the same IV; CRC is weak in integrity check; authentication is too simple to be trustworthy.

To improve WEP security, the IEEE 802.11i task group had been working on different solutions. Before a standard was approved, Wi-Fi Alliance also specified interim approaches to improving wireless LAN security based on draft versions of 802.11i. Wi-Fi protected access (WPA) is the first approach developed based on Draft Version 3 of 802.11i.

Compared with WEP, WPA improves encryption by considering two schemes: a larger IV and changing security keys through temporary key integrity protocol (TKIP). In WPA, the totally key size is increased to 128 bits, among which 48 bits are for an IV. TKIP changes working keys based on a master key after a certain number of packets have been sent. TKIP also provides a mechanism of per-packet key mixing. In WPA, a new integrity check scheme called Michael is used. A frame counter is added to Michael to avoid replay or forgery attack. Although TKIP is used in WPA, the ciphering scheme is still the same as WEP. Thus, WPA has the advantage of being compatible with old wireless LAN cards.

In WPA, authentication can be done through a pre-shared key or via 802.1X [112] authentication. The former option is used for application scenarios where 802.1X is considered too expensive. For example, in a home networking scenario, a pre-shared key is preferable, while 802.1X is preferable in enterprise networking.

802.1X is specified by the 802.1 standard working group as a port-based network access control protocol. It can be used for any LAN and provides authentication to devices attached to a LAN port. An 802.1X system consists of three key components: an authentication server, which is usually a remote authentication dial-in user service (RADIUS) server, authenticator, which is an access point (AP) in a wireless LAN, and a supplicant, which is usually a client. 802.1X works according to the following procedures.

- Upon detection of a supplicant, the port on the authenticator will be enabled but will enter the “unauthorized” state where only 802.1X authentication related traffic is allowed on this port.
- The authenticator sends out an extensible authentication protocol (EAP) [1] request entity to the supplicant.
- The supplicant sends an EAP response to the authenticator.
- The authenticator forwards the received EAP response to the authentication server.
- The authentication server can reject or accept the EAP request considering the EAP response. If the EAP request is accepted, the authenticator enables the port so that all traffic is allowed on the given port, i.e., the port is now working in “authorized” state.
- If the supplicant leaves the system, an EAP log-off message will be sent to the authenticator. The port then enters the “unauthorized” state.

During 802.1X authentication, a secure pair-wise master key (PMK) between supplicant and authenticator can be negotiated via EAP. It should be noted that EAP is an authentication framework rather than a specific authentication mechanism. It provides common functions and a negotiation of a desired authentication mechanism. Based on EAP, different authentication mechanisms can be defined [1]. Typical EAP based authentication mechanisms include EAP transport layer security (EAP-TLS) [2] for wireless LAN authentication, EAP-MD5, EAP-PSK, and EAP-TTLS. Since EAP is not a specific protocol, but only defines message formats, an EAP-based authentication protocol needs to encapsulate EAP messages. In 802.1X, this encapsulation is EAP over LANs (EAPOL).

In WPA, whether PMK is derived after 802.1X authentication or from PSK, a four-way handshake is needed to handle secure key management and distribution. The four-way handshake is responsible for confirming the existence of PMK, liveness of peers, and selection of cipher suite. It also generates fresh pairwise transient key (PTK) for each session and group transient key (GTK) for multicast applications. EAPOL-Key frames are used during the four-way handshake as shown in the following procedure.

- *Message 1.* An authenticator sends a cryptographic nonce to a supplicant. This nonce is referred as *ANonce*.
- *Message 2.* When a supplicant receives *message 1*, it creates its own nonce, called *SNonce*. The supplicant then calculates the PTK based on parameters such as *ANonce*,

SNonce, authenticator's MAC address, and supplicant's MAC address. In *message 2*, the supplicant sends SNonce and security parameters used during association to the authenticator. This message gets an authentication check using the key confirmation key (KCK) derived in pairwise key hierarchy.

- *Message 3.* When the authenticator gets message 2, it verifies the validity of this message. If it is valid, the authenticator sends security parameters used in beacons and probe responses in *message 3*. It also sends a GTK encrypted using key encryption key (KEK) derived from pairwise key hierarchy. The entire *message 3* also needs to get an authentication check.
- *Message 4.* When the supplicant gets *message 3*, it performs an authentication check. If the received message is valid, it sends *message 4* to inform the authenticator that all temporary keys are ready for use.

Two key hierarchies are involved in the four-way handshake: pairwise key hierarchy and group key hierarchy. In the pairwise key hierarchy, temporary keys are derived from a PMK. If 802.1X is used, PMK is provided by the authentication server. If a pre-shared key is used, PMK is derived from the password. Starting from PMK, three keys are generated in the pairwise key hierarchy: KCK, KEK, and pairwise temporary key. Thus, a PTK is not just one key but three keys, i.e., KCK, KEK, and pairwise temporary key. In the group key hierarchy, a GTK is created using parameters such as group master key (GMK), group nonce (*GNounce*) and authenticator's MAC address.

Looking at the overall procedure of WPA, three security suites are used: the authentication and key management suite advertises if 802.1X or pre-shared key is used; the group cipher suite defines the data confidentiality protocol for broadcast communications; the pairwise cipher suite contains a list of data confidentiality protocols for unicast traffic.

WPA2

Although WPA significantly increases security of wireless LANs, it can still be broken by related-key attacks. Thus, Wi-Fi Alliance specified a new version of WPA, called WPA2. Compared with WPA, WPA2 replaces the encryption scheme by an advanced encryption standard (AES) called counter mode with cipher block chaining message authentication code protocol (CCMP).

CCMP handles authentication, confidentiality, and integrity. For authentication and integrity, CCMP uses cipher block key chaining message authentication code (CBC-MAC). AES in counter mode (CTR) is used for confidentiality. In WPA2, the CCMP block size and key size are both 128 bits. The detailed procedures of CCMP packet encapsulation are depicted in Figure 6.1. As shown in the encapsulation procedure, an encrypted MAC packet data unit (MPDU) is formed by concatenating four parts: MAC header, encrypted data, MIC, and CCMP header. Encrypted data and MIC are performed through CCM encryption/MIC calculation. Inputs to this step include plain text, constructed nonce, constructed additional authentication data (AAD), and temporary key (TK). AAD protects against a replaying attacker to the MAC header that is not encrypted. The nonce is constructed from packet number (PN), source MAC address, and priority[1] fields. The CCMP header is constructed from PN and key ID.

[1] It is a reserved field set to zero.

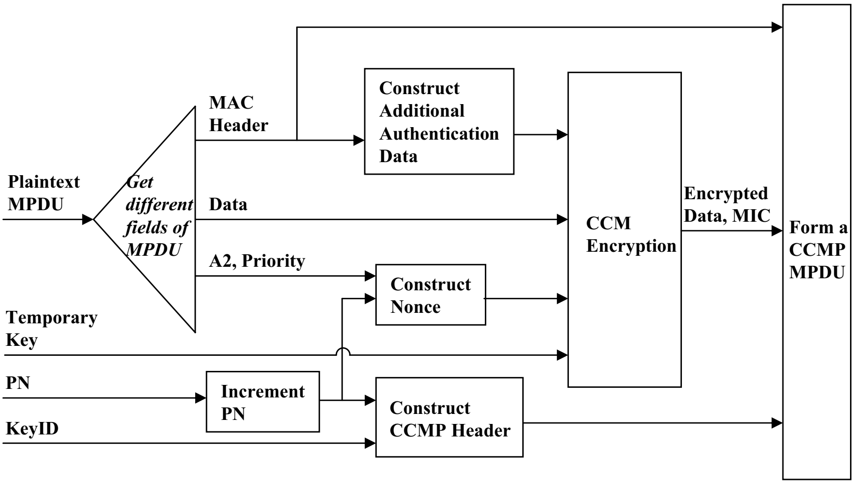

Figure 6.1 Packet encapsulation process of CCMP

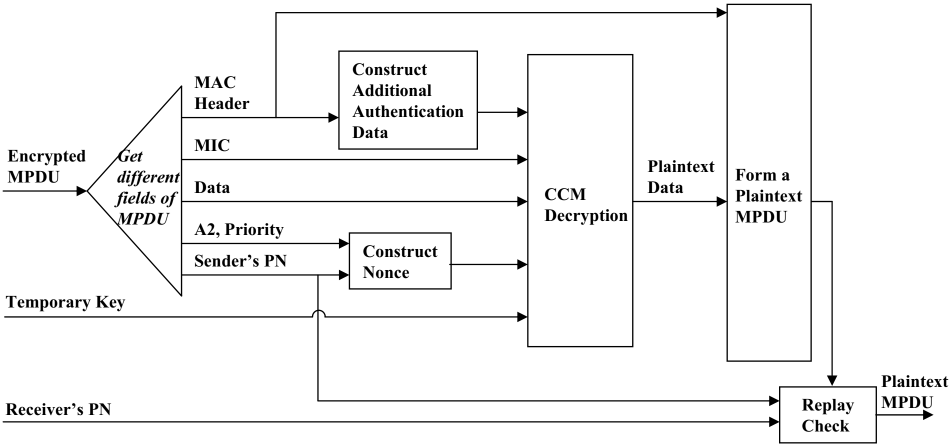

Figure 6.2 Packet decapsulation process of CCMP

The decapsulation process is depicted in Figure 6.2.

WPA2 keeps 802.1X plus the four-way handshake in the authentication mechanism. Since a totally different ciphering scheme is used in WPA2, it is not compatible with old wireless LAN cards.

802.11i

802.11i is a superset of all 802.11 wireless LAN security mechanisms including WEP, WPA, and WPA2.

Two classes of security algorithms are specified in 802.11i security framework. The first class specifies algorithms for creating and using a robust security network association (RSNA), i.e., RSNA algorithms. The second class defines pre-RSNA algorithms. Pre-RSNA security mechanisms include WEP and IEEE 802.11 entity authentication, while RSNA security mechanisms comprise the following components:

- TKIP
- CCMP
- RSNA establishment and termination procedures, including the use of 802.1X authentication
- Key management procedures

The capability of creating an RSNA is indicated in the robust security network (RSN) information element of certain frames such as beacon, probe response, association/reassociation request, message 2/3 of four-way handshake. Pre-RSNA equipment is not capable of creating or supporting RSNA.

According to the 802.11i standard, all pre-RSNA security methods except for open system authentication have been deprecated; implementation of pre-RSNA is only for migration to RSNA security methods.

In RSNA, two data confidentiality and integrity protocols are specified: TKIP and CCMP. A RSNA compliant device is required to support CCMP, but TKIP support is optional. However, a device supporting only WEP is upgradeable to TKIP but not to CCMP. Authentication of RSNA can rely on 802.1X port access entity (PAE) and authentication server, which is not defined in 802.11i or be simply based on PSK. Whether 802.1X or PSK is used for authentication, the key management procedure involves a four-way handshake process.

In 802.11i, when 802.1X authentication is used, the specific EAP method used performs mutual authentication. Thus, it is critical that this EAP method can protect nodes without being exposed to man-in-the-middle attacks. However, many existing EAP schemes, e.g., EAP-MD5, do not meet this requirement. When PSK is used, mutual authentication between any two nodes without being exposed to man-in-the-middle attacks is also a requirement. However, 802.11i assumes that a trustworthy channel exists for nodes to identify a secure extended service set (ESS) or independent basic service set (IBSS). How to set up this trust is not specified in 802.11i.

6.3.2 Security of IEEE 802.16 Wireless MANs

IEEE 802.16 security is specified as a security sublayer at the bottom of the MAC layer. Its focus is on the access control and confidentiality of the data link. The 802.16 security architecture consists of five components.

- **Encryption:** It is performed only for data payloads, and thus CRC and the generic MAC header are not encrypted. The encryption algorithm used in IEEE 802.16 is data encryption standard's cipher block chaining mode (DES-CBC).
- **X.509 certificate profile:** X.509 certificates identify communication parties. Two certificate types are defined in IEEE 802.16: manufacturer certificates and subscriber

station certificates. No base station certificates are defined. Thus, a base station typically uses the public key in the manufacturer certificate to verify the subscriber station certificates.

- **Security associations:** Security association is required to maintain the security state of a connection. There are two security associations in IEEE 802.16: data security association and authorization security association. Data security association protects transport connections between one or more subscriber stations and a base station. Authorization security associations are shared between a base station and a subscriber station. Moreover, a base station uses the authorization security association to configure the data security association on a subscriber station.

- **Privacy and key management (PKM):** A PKM protocol instance establishes a data security association between a base station and a subscriber station. Several message exchanges are needed between a base station and a subscriber station. For example, when a new key or a new data security association is needed, a base station must send a PKM message to the desired subscriber station.

- **PKM authorization:** The PKM authorization protocol aims to distribute an authorization token to an authorized subscriber station. Thus, several message exchanges are also needed for this process between the base station and the authorized subscriber station.

However, all these components contain security flaws. In authorization security association, IEEE 802.16 standards of security lack a specification as that for data association. Thus, authorization secure association can easily be broken. In IEEE 802.16, the BS lacks a certificate. Thus, the security client can be compromised by forgery or replay attacks. Since authorization security association is weak, PKM authorization protocol cannot really serve the purpose of authorization, which also impacts the PKM. The 802.16 standard also fails to specify that the traffic encryption key (TEK) is generated according to uniform probability distribution and a cryptographic-quality random number. Moreover, data encryption standard (DES) used in IEEE 802.16 does not provide strong data confidentiality.

6.3.3 Security of Mobile Ad Hoc Networks

Mobile ad hoc networks lack efficient and scalable security solutions because their security is easier to be compromised [41, 280] due to: vulnerability of channels and nodes in the shared wireless medium, absence of infrastructure, and dynamic change of network topology. The attacks may advertise routing updates [105,286]. Another type of attack is packet forwarding, i.e., the attacker may not change routing tables, but the packets on the routing path may be lead to a different destination that is not consistent with the routing protocol. Moreover, the attacker may sneak into the network, and impersonate a legitimate node and do not follow the required specifications of a routing protocol [230]. Some malicious nodes may create a wormhole and shortcut the normal flows among legitimate nodes [106].

The same types of attack as in routing protocols may also occur in MAC protocols. For example, the backoff procedures and NAV for virtual carrier sense of IEEE 802.11 MAC may be misused by some attacking nodes, which cause the network to be always congested by these malicious nodes [97].

In response to attacks in mobile ad hoc networks, security mechanism at routing layer can be classified into two types: secure routing protocol and secure data forwarding. Secure routing is usually achieved by applying authentication techniques to critical fields of routing messages. The typical authentication techniques include authentication message codes, one-way key chain, and digital signature. Authentication message codes are based on secret keys among a pair of nodes, and thus, are not an appealing option for broadcast messages. In addition, it is difficult to establish pairwise secret keys in ad hoc networks. In a one-way key chain, a one-way function is used to repeatedly generate keys for authentication message codes. Although this technique can be used for broadcast messages [207], it requires time synchronization and a careful schedule of using unreleased keys. Digital signature is based on public-key cryptography. Thus, as long as public keys have been distributed, messages signed by a sender via secret keys can be deciphered and verified. Digital signature is a scalable technique for a large network, even where broadcast messages are considered. However, distribution of public keys needs trustworthy mechanism among nodes, which is also a research challenge for ad hoc networks.

When a routing path is securely established and maintained, the next key step is to keep the security of data forwarding, which includes detection of security attacks and response to them. To date, detection is based on either watchdog [186] or ACK [23]. Once attacks are detected, reaction schemes are employed to prevent attacks from disrupting other parts of the network. Reaction schemes can be network wide [279] and end-host reaction [186]. However, it is more effective to exclude malicious nodes by performing both network wide reaction and end-host reaction.

There is no doubt that security attacks also frequently occur in the link layer of ad hoc networks. Since security mechanisms of IEEE 802.11, IEEE 802.15, and IEEE 802.16 are focused on the MAC layer, they can be applied to the link layer of mobile ad hoc networks. However, owing to the multihop and dynamic network topology, we cannot expect satisfactory performance of these schemes in mobile ad hoc networks. Thus, designing link-layer security mechanisms for mobile ad hoc networks is still subject to future research.

In mobile ad hoc networks, attackers may sneak into the network by misusing the cryptographic primitives [39]. In a cryptographic protocol, the exchange of information among users occurs frequently. The users employ a fair exchange protocol which depends on a trusted third party. However, this trusted party is not available in mobile ad hoc networks due to lack of infrastructure. Thus, another exchange scheme, called *rational exchange*, must be used. Rational exchange ensures that a misbehaving party cannot gain anything from misbehavior, and thus will not have any incentives to misbehave [42].

Key management is one of the most important tasks for network security. However, the key management for mobile ad hoc networks becomes much more difficult, because there is no central authority, trusted third party or server to manage security keys. Key management needs to be performed in a distributed way. A self-organization scheme was proposed in [109] to distribute and manage the security keys. In this self-organizing key management system, certificates are stored and distributed by users themselves. When the public keys of two users need to be verified, they first merge the local certificate repositories and then find the appropriate certificate chains within the merged repositories that can pass this verification.

6.4 Security Mechanisms for WMNs

6.4.1 Features and Challenges of a Secure WMN

The security schemes in other wireless networks are helpful to develop security schemes for WMNs. However, the specific features of WMNs require enhancement to these schemes and also demand new schemes.

Compared with IEEE 802.11 wireless LANs or IEEE 802.16 wireless MANs, WMNs have added the mesh architecture into the network to replace the traditional Ethernet connection between APs or base stations. Such a difference further results in two specific requirements on the security of WMNs: multihop wireless network security and multitier security, as mentioned at the beginning of this chapter. In other words, the security schemes developed for IEEE 802.11 wireless LANs and IEEE 802.16 wireless MANs can be meaningful only for the communications between mesh routers and mesh clients. Both the communications between mesh routers and the end-to-end communications from one mesh client to another mesh client exhibit different security issues from those in the traditional one-hop wireless access scenario in either IEEE 802.11 wireless LANs or IEEE 802.16 wireless MANs. Thus, new security schemes must be developed for mesh networking among mesh routers and mesh clients. The security schemes for network access from mesh clients to a mesh router needs to be improved.

Compared with mobile ad hoc networks, WMNs encounter both challenges and opportunities. WMNs have several advantages over mobile ad hoc networks, especially the mesh backbone with minimal mobility, which can help to realize security in a multihop wireless network with reasonable efforts. However, in mobile ad hoc networks, owing to mobility in all nodes, security is hard to ensure for two reasons. One is that implementation of a security algorithm is sophisticated in such an all-mobile network. The other is that a security algorithm can be easily broken since no trustworthy node can help to enforce the security. Therefore, in theory, a security scheme proposed for mobile ad hoc networks should be able to meet the needs of WMNs. However, two other problems exist, which illustrate the security challenges in WMNs. The first problem is that a security scheme developed is usually too cumbersome for WMNs, since much more complicated mobility and related topology changes need to be considered in such a scheme. If it is applied to WMNs, it causes unnecessary complexity and too much overhead. As a result, the security schemes are useful for WMNs, but improvement is required. The second problem is that mesh routers in the mesh backbone need to communicate with other mesh routers and also provide wireless services to mesh clients. The dual functionality in mesh routers renders the security schemes for mobile ad hoc networks insufficient for WMNs. Either improvement or new schemes need to be developed.

Owing to the limitations of existing security schemes, the security mechanism in IEEE 802.11 mesh mode is still in the process of being developed and specified [122]. Although IEEE 802.16 mesh mode has been specified [130], the security mechanism only considers the scenario of fixed wireless access. The security mechanism of IEEE 802.16 mesh mode is still mainly built on top of the security layer of a PMP mode IEEE 802.16. Moreover, the security issues when mobile nodes are also supported by mesh routers have not been considered.

6.4.2 Security of IEEE 802.11s WMN

To date, existing WMNs still depend on security schemes developed for other wireless networks. For example, currently many IEEE 802.11 based WMNs only adopt WEP as their security mechanism. Some of them have been equipped with WPA or are trying to implement IEEE 802.11i security schemes. However, none of them have implemented a security mechanism that is really effective for WMNs. The IEEE 802.11s task group has worked out a security framework for 802.11s WMNs, but it is still subject to revision and approval. Below, the latest work of 802.11s security is presented and analyzed.

Security Framework of 802.11s WMN

The 802.11s WMN security requires the RSNA functionality to be supported. Thus, pre-RSNA schemes such as WEP cannot be used.

The RSNA in 802.11s WMN is called mesh security association (MSA). Via MSA security functionalities similar to 802.1X are built into a distributed multihop WMN. There are two types of security key holders: mesh key distributor (MKD) and mesh authenticator (MA). A mesh point (MP) can be MKD and MA, MA, or neither. An MP with MA functionality plays the 802.1X authenticator's role, and an MP without MA functionality plays the 802.1X supplicant's role. An MKD and MA can be co-located with MA, and can manage authentication and key distribution for both MA and a supplicant. In an 802.11s WMN, there exists one MKD, multiple MAs, and supplicants. A supplicant can become an MA after it passes security key holder association with the MKD.

It should be noted that the 802.1X in MSA does not mean that 802.11s security needs an extra 802.1X authentication server (AS) in the system. In fact, MSA can operate based on pre-shared key (PSK). In the case of using an extra 802.1X AS to enhance 802.11s WMN security, an MKD works as network access server (NAS) client. Thus, NAS client functionality is required for an MKD in 802.11s WMN. With this functionality, the entire security system actually consists of two 802.1X processes organized hierarchically: 802.1X AS and MKD at the upper level and MKD and MA at the lower level.

Whether using PSK or master session key (MSK) (provided through successful authentication between the AS and the MKD), a security key hierarchy is established after an MP has passed the initial security authentication through an authenticator MP and the MKD of the mesh network. This MP's subsequent secure link setup with other MPs can be done directly, based on this key hierarchy, so steps of authentication and key establishment can be omitted.

The key hierarchy consists of two branches: link security branch and key distribution branch, as shown in Figure 6.3. The former is for generating keys for a secure link and the latter is for generating keys for key distribution. On the link security branch, pairwise master key (PMK) is first derived for MKD based on a pre-shared key (PSK) or a master session key (MSK). PSK is used when 802.1X authentication is not applied; otherwise, an MSK is provided through a successful authentication between the authentication server (AS) and the supplicant MP. Based on PMK-MKD, PMK for MAs, i.e., PMK-MAs, are then derived. Key delivery and key management between the MKD and the MA are handled by mesh key transport and extensible authentication protocol (EAP) message transport protocol. With a PMK-MA, an authenticator MP and its supplicant MP mutually derive a pairwise transient key (PTK). On the key distribution branch, a mesh key distribution key (MKDK) is first

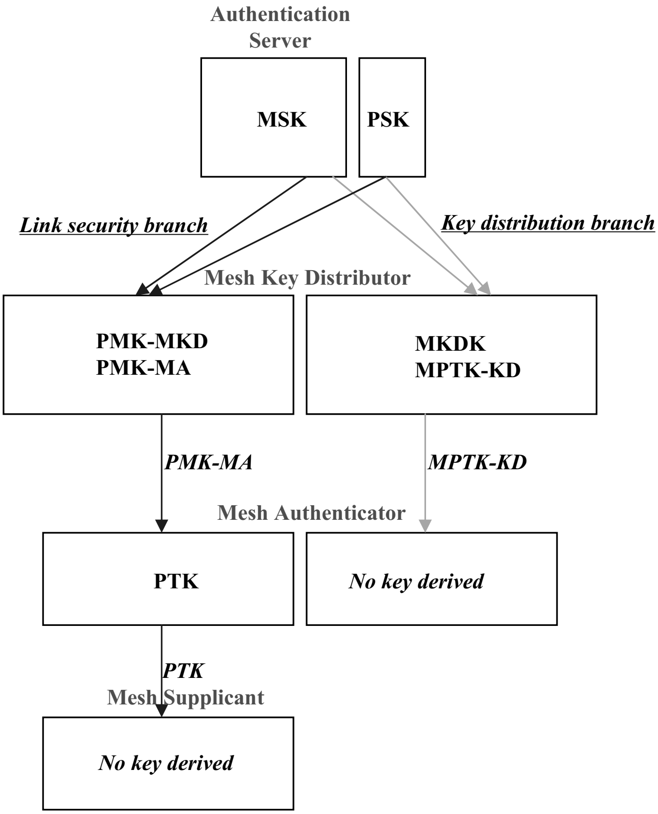

Figure 6.3 Security hierarchy of 802.11s WMN

derived from PSK or MSK, and then a mesh PTK for key distribution (MPTK-KD) is derived mutually by an authenticator MP (after it becomes an MA) and the MKD.

In an 802.11s WMN, the support for MSA is advertised by MPs in the mesh security capability information element (MSCIE) of beacon or probe response frames. The fields of MSCIE are shown in Figure 6.4. In addition to the mesh security capability field identified by the element ID and length field, MSCIE contains two other very important fields: MKD domain ID (MKDD-ID) and mesh security configuration. The MKDD-ID field is set to zero unless the MP implements the MKD function or it has received the MKDD-ID from an MKD during the mesh key holder security handshake.

The mesh security configuration field consists of three subfields and one reserved field.

- *Mesh authenticator bit.* If this bit is set to one, then the MP is configured to play IEEE 802.1X authenticator role during MSA handshake. Otherwise, it works as an 802.1X supplicant.
- *Connected to MKD bit.* If an MP has completed a security association with the MKD and has a valid path to the MKD, then this bit is set to one. Otherwise, it is set to zero.

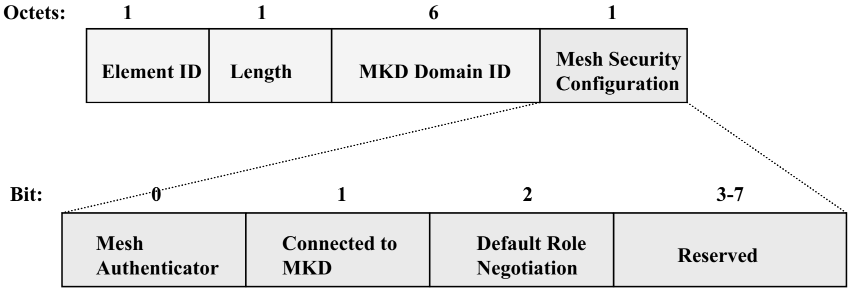

Figure 6.4 Contents of MSCIE

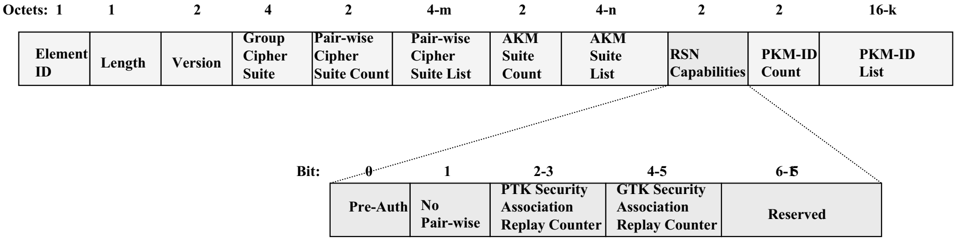

Figure 6.5 Contents of RSNIE

Additionally, if a mesh authenticator bit is set to zero, this bit should be set to zero. For an MP with both MKD and MA functionalities, if the mesh authenticator bit is set to one, then this bit should be one too.

- *Default role negotiation bit.* If this bit is set to one, a default mesh role determination scheme is used. Otherwise, a proprietary scheme is applied.

When the MKDD-ID field is zero, both mesh authenticator bit and connected to MKD bit need to be zero.

MSCIE is also used in mesh key holder security handshake frames.

An MP that wants to authenticate with other MPs using MSA needs to advertise its security policy by inserting an RSN information element (RSNIE) into beacon or probe response frames, since MSA is built on top of RSNA. An RSNIE contains information for the group cipher suite, pair-wise cipher suite, AKM suite, RSN capability, and PMK-ID. As shown in Figure 6.5, the RSNIE is the same as that defined in 802.11i. A group cipher suite is specified in RSNIE for protecting multicast/broadcast frames. A list of the cipher suite supported in the RSN is specified by the cipher suite count and cipher suite list fields. The list of supported AKM suite and valid PMK-IDs are specified in a similar way.

It should be noted that MSCIE and RSNIE also exist in peer link open and peer link confirm messages. Additionally, these two messages include an MSA handshake information element (MSAIE). As shown in Figure 6.6, an MSAIE consists of five major fields for

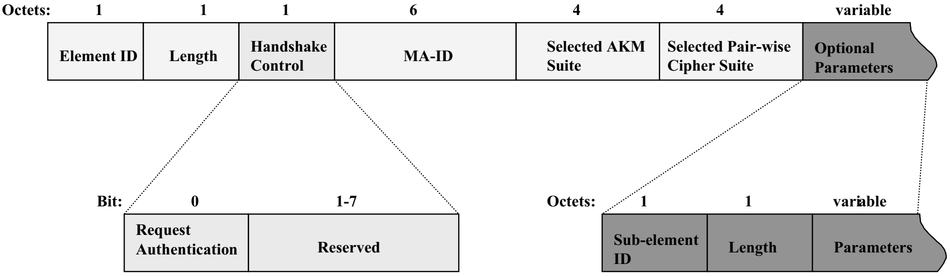

Figure 6.6 Contents of MSAIE

authentication: handshake control, MA-ID, selected authentication and key management (AKM) suite, selected pair-wise cipher suite, and optional parameters. In the handshake control field, if the first bit is set to one, it indicates that the MP requests authentication during the initial MSA authentication procedure. Other bits are reserved for future use. MA-ID is actually the MAC address of the MA that will be used by a supplicant MP to derive the mesh authenticator PMK (PMK-MA). The selected AKM suite contains information on the authentication type and key management type used for link security. For example, whether authentication is based on 802.1X or PSK is indicated in this AKM suite. Whether MSA uses RSNA key management is also specified in AKM suite. The selected pair-wise cipher suite indicates a cipher suite used for securing a link. Whether the ciphering scheme uses WEP, TKIP, or CCMP can be found from the pair-wise cipher suite. If an MP wants to be part of MSA, it needs to select CCMP as the cipher suite, since the default cipher suite of RSNA is CCMP.

The optional parameter contains information of variable length. Different parameters can be sent in this field and are identified through a different subelement ID. For example, MKD-ID and EAP transport mechanisms are two parameters included in this field.

It should be noted that MSCIE, RSNIE, and MSAIE are all contained in the MSA four-way handshake using EAPOL-Key frames, more specifically in four-way handshake message 2 and message 3.

Security Architecture

The entire security architecture of IEEE 802.11s WMN can be captured in Figure 6.7. There are three types of mesh nodes involved in a mesh security system of 802.11s: MKD, MA, and the supplicant. As shown in this architecture, there is only one MKD with which multiple MAs are associated. A supplicant performs security authentication through MAs. The set of MAs, supplicants, and the single MKD form an MKD domain (MKDD). Optionally, the MKD is connected to an AS through which 802.1X authentication is executed.

Considering an MP in an 802.11s secure network, when it needs to establish a secure link with a peer MP, a peer link setup procedure is first executed (step 0 in Figure 6.7). In this initial step, the role of an MP is determined and security policy is selected.

Whether an MP and its peer MP are an 802.1X authenticator or supplicant MP is determined in the peer link management. According to the procedures of peer link management,

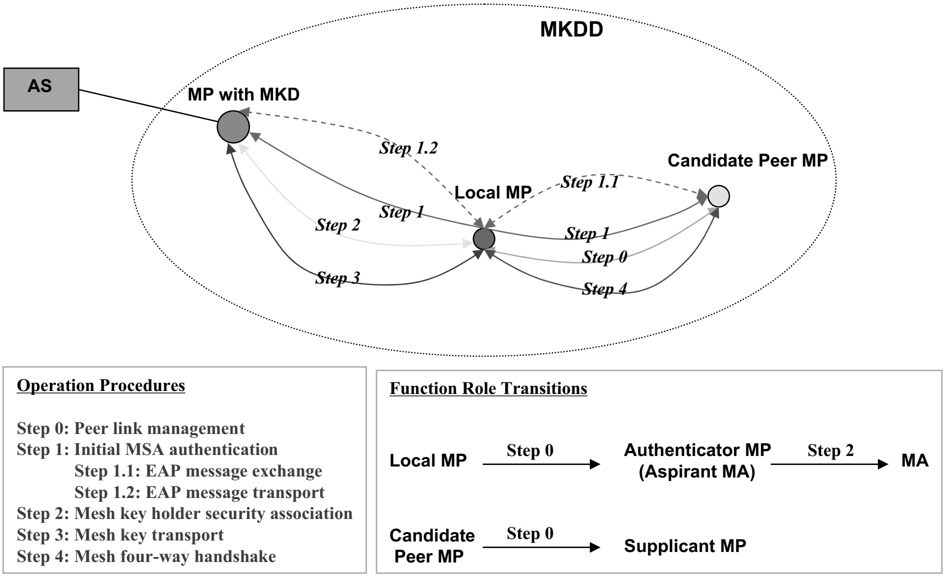
MKDD
AS
MP with MKD
Step 1.2
Candidate Peer MP
Step 1.1
Local MP
Step 1
Step 2
Step 1
Step 0
Step 3
Step 4
Operation Procedures
Step 0: Peer link management
Step 1: Initial MSA authentication
Step 1.1: EAP message exchange
Step 1.2: EAP message transport
Step 2: Mesh key holder security association
Step 3: Mesh key transport
Step 4: Mesh four-way handshake
Function Role Transitions
Local MP
Step 0
Authenticator MP (Aspirant MA)
Step 2
MA
Candidate Peer MP
Step 0
Supplicant MP

Figure 6.7 Architecture and major function blocks of 802.11s mesh security

there are several scenarios for selecting authenticator and supplicant for an MP and its peer MP.

- If only one MP that has already been an MA, i.e., its “Connected to MKD” bit is one, then this MP is usually selected as an 802.1X authenticator, while the other one is an 802.1X supplicant.
- If both MPs have zero in “Connected to MKD” bit, then the MP with a larger MAC address or the selector MP is the 802.1X authenticator.
- If both MPs have one in the “Connected to MKD” bit, then the MP that requests authentication is the supplicant. Otherwise, if both request or neither requests authentication, then the selector MP is the 802.1X authenticator.

With authentication role determined, MSA authentication is carried out in an MKDD. However, depending on whether this MP has established a secure link with a peer MP before, the procedures of MSA authentication are different. If no such a secure link was set up before within the same MKDD, a procedure of initial MSA authentication is needed to set up the mesh key hierarchy. Considering this requirement, and peer link management procedures, we know that usually an 802.1X supplicant needs an initial MSA authentication.

During initial MSA authentication, a mesh key hierarchy is created for the supplicant MP through the interactions among MKD, authenticator MP, and the supplicant MP. If 802.1X authentication is needed, the authenticator MP will initiate the 802.1X authentication with the supplicant MP using EAPOL messages in 802.11 data frames (step 1.1 in Figure 6.7). The 802.1X message may be transported between the MA and the MKD, so an EAP message transport protocol is defined between the MKD and the authenticator MP (step 1.2 in Figure 6.7). Upon successful completion of 802.1X authentication, the MKD receives the MSK and then generates PMK-MKD and PMK-MA. If no 802.1X authentication is needed, PSK is used to generate PMK-MKD and PMK-MA. Thus, steps 1.1 and 1.2 do not exist if PSK instead of 802.1X authentication is adopted in the initial MSA authentication.

For the 802.1X authenticator MP, it can establish a mesh key holder security association with the MKD (step 2 in Figure 6.7). During this step, the authenticator MP is an "aspirant MA". It becomes an MA after this step successfully completes. In this step, encryption keys for security key distribution between MA and MKD are derived. It should be noted that this step may not be necessary if the authenticator MP has already been an MA and established a security association with the MKD.

Finally, the MKD delivers the PMK-MA to the MA using a mesh key transport protocol (step 3 in Figure 6.7).

After the above steps are done, the MSA authentication proceeds with an MSA four-way handshake (step 4 in Figure 6.7) using the existing mesh key hierarchy to set up a PTK between the MA and the supplicant MP. After the four-way handshake, the two MPs can initiate the group key handshake procedure to update their GTK.

Detailed Procedures of Major Function Blocks

Peer Link Setup and Initialization When an MP needs to establish a secure link with a peer MP, a peer link setup procedure is first executed. During this procedure, a lot of security parameters are verified. For example, the security policy, security role, AMK suite, and pairwise cipher suite, and so on, need to be verified. The AKM suite and pairwise cipher suite are selected by a selector MP. The local MP or the peer MP becomes a selector MP if its MAC address is larger.

The peer link management procedure is not designed fully for MSA, but for the general purpose of maintaining a link between an MP and its peer or candidate peer MP. There are two modes of setting up such a link: passive and active. In the passive mode, a local MP listens to the *peer link open* messages from candidate peer MPs. If it can set up a link to a candidate peer MP, it sends a *peer link confirm* message back to the candidate peer MP. In the active mode, the local MP actively sends a *peer link open* message in which the MAC of the candidate peer MP is specified. The local MP receiving such a message sends back a *peer link confirm* message to the candidate peer MP.

Because of the two modes, a local MP needs to both send and receive *peer link open* and *peer link confirm* messages in MSA.

When it sends a *peer link open* message to the candidate peer MP, RSNIE, MSCIE, and MSAIE must be configured and included in this message.

- RSNIE. It is configured in the same way as RSIE in beacon or probe response frames of this MP except that the PMK-ID field needs to be configured to include the PMK-MA name for both sender and receiver, if a previous PMK-MA has been established. For the PMK-MA name of the sender, this field is empty if no PMK-MA exists or the local MP requests initial MSA authentication; otherwise, it contains the PMK-MA of the mesh key hierarchy created during the previous initial MSA authentication. Similarly, for the PMT-MA Name of the receiver, this field contains a valid PMK-MA created by the candidate peer MP during its previous initial MSA authentication.

- MSCIE. This field is set exactly the same as that in beacon or probe response frames.
- MSAIE. Except the following subfields, all other ones must be set to zero.
  - Request Authentication. If the local MP requests initial MSA authentication, it is set to one. Thus, if RSNIE contains PMK-ID entries, this subfield must be set to zero.
  - AKM Suite. If the local MP is a selector MP, this subfield contains the AKM suite selected by the local MP.
  - Pairwise Cipher Suite. If the local MP is a selector MP, this subfield contains pairwise cipher suite selected by the local MP.
  - PMK-MKD Name. This subfield exists if the PMK-MA Name of the sender is present in RSNIE. This name identifies the PMK-MKD created in previous initial MSA authentication by the local MP.

When the local MP receives such a message, it should verify the following information.

- Default Role Negotiation in MSCIE. The local MP checks if this field in MSCIE in the receive message is identical to the one in MSCIE of the local MP's beacons or probe responses.
- Group Cipher Suite in RSNIE. The local MP verifies if this group cipher suite is supported.
- List of AKM Suite and Pairwise Cipher Suite in RSNIE. The local MP check if its supported AKM suite and pairwise cipher suite is included in the list.
- Selected AKM Suite and Pairwise Cipher Suite in MSAIE. If the local MP is not a selector MP, it needs to verify if these suites can be supported.

If the above verification fails, then the local MP shall trigger an event of closing the link. Otherwise, it needs to check if a *peer link confirmation* has been received. If so, then the local MP should make sure all major fields in RSNIE, MSCIE, and MSAIE of these two message match each other.

After this check, additional operations are carried out. For example, the key selection procedure and the 802.1X role selection procedure must be executed [122]. Once the *peer link open* message is successfully processed, the local MP continues the next step according to the finite state machine of peer link management. For example, if the local MP may send a *peer link confirm* message to the candidate peer MP.

When a *peer link confirmation* message is sent, RSNIE, MSCIE, and MSAIE are configured as follows.

- RSNIE. Except for the PMK-ID list, the RSNIE of this message needs to be the same as that of this local MP's *peer link open* message or beacon and probe response frames. If initial MSA authentication will happen after peer link setup, the PMK-ID is empty; otherwise, it includes the PMK-MA name chosen in the key selection procedure.
- MSCIE. This must be the same as that in this local MP's *peer link open* message or beacon and probe response frames.

- MSAIE. Except for the following subfields, all other subfields are set to zero.
  - Request authentication. This is set to one if the local MP requests initial MSA authentication.
  - MA-ID. This contains the MAC address of the 802.1X authenticator.
  - AKM suite and pairwise cipher suite. These have to be the same as those in *peer link open* messages or selected from those supported by both the local MP and the peer MP.
  - Optional parameter list. Three subfields must be set in this list. If the local MP is an 802.1X authenticator, the MKD-NAS-ID needs to be present in the parameter list. If the local MP requests initial MSA authentication and also plays the 802.1X authenticator's role, the MKD-ID in the parameter list will contain the identifier of the MKD with which the local MP has a security association. In addition, the EAP transport list will be specified.

When the local MP receives a *peer link confirmation* message, it follows a different procedure to process this message depending on whether a *peer link open* message has been received.

If a *peer link open* message has been received, the *peer link confirmation* message is processed as follows.

- MSCIE and handshake control in MSAIE. These must be identical to those received in the *peer link open* message.
- RSNIE. The PMKID list must match the local MP's key selection procedure. Other subfields must be the same as those in the RSNIE of the *peer link open* message.
- MA-ID in MSAIE. The role of the 802.1X authenticator needs to match the role selection procedure.
- AKM suite and pairwise cipher suite. These fields must be the same as those in the *peer link open* message.

Otherwise, the selected AKM suite and pairwise cipher suite need to be verified. Such suites need to be supported by the local MP. Additionally, if the local MP is a selector MP, they need to match those selected by this local MP.

After peer link management, the local MP and its peer MP are selected as either an 802.1X authenticator or a supplicant.

Initial MSA Authentication If initial MSA authentication is requested by the supplicant MP during the peer link management procedures, a key hierarchy needs to be created after peer link management is done.

802.1X authentication for creating mesh key hierarchy If 802.1X authentication is required by the negotiated AKM suite, EAPOL messages are exchanged to perform 802.1X authentication. The authenticator MP initiates 802.1X message exchange with the supplicant MP via EAPOL frames being sent in IEEE 802.11 data frames. When it is properly configured, the MA starts the first EAP message. However, if the authenticator MP is not configured to send the first EAP message, it requests the EAP message from the AS. The authenticator MP does so by constructing an EAP encapsulation request message and then sending it to the MKD. Such a message is an EAP encapsulation MSA mesh action frame but does not contain an EAP message subfield.

When the authenticator MP receives an EAP message from the supplicant MP, this message is encapsulated into an EAP encapsulation MSA mesh action frame and sent to the MKD. When the MKD receives an EAP message from the AS with a destination to the supplicant, this message is also encapsulated into an EAP encapsulation MSA mesh action frame and sent to the authenticator MP.

If the AS informs the MKD of accepting or rejecting the supplicant's access, the MKD sends to the authenticator MP the final EAP encapsulation MSA mesh action frame that contains the status of EAP authentication. This final action frame is also called an EAP encapsulation response message. When the authenticator MP receives this message, if EAP authentication succeeds, the supplicant is granted access; otherwise, the authenticator will close the peer link with the supplicant.

PSK for creating mesh key hierarchy If 802.1X authentication is not needed, then the key hierarchy is created directly from PSK. No EAP message transport is involved in this case.

Mesh Key Holder Security Association There are multiple purposes of carrying our mesh key holder security association. Firstly, an MP that is selected as an 802.1X authenticator can begin to operate as an MA after completing a security association with the MKD. Secondly, the message integrity and data origin authenticity can be ensured for all messages exchanged between the MA and the MKD after security association is established. Thirdly, an encryption scheme is provided to protect the derived keys and their contexts delivered from the MKD to the MA.

The mesh key holder security association includes two phases: MKD discovery and mesh key holder security handshake. If the MP is not an MKD, it needs to obtain the MKD-ID from the MSAIE of a peer link confirm message.

With a discovered MKD, the security handshake process is started by the MP that has successfully finished initial MSA authentication. At this stage, the MP is called an "aspirant MA".

The aspirant MA sends handshake message 1 to the MKD. In this message, the EAP transport mechanism selected by the aspirant MA is included. Upon receiving message 1, the MKD verifies whether the EAP transport mechanism can be supported. If it is not supported, the handshake fails. Otherwise, the MKD chooses an MKD-Nonce and derives the mesh pairwise transient key for key distribution (MPTK-KD) based on the MKD-Nonce and the MA-Nonce in message 1. The MKD then sends handshake message 2 to the aspirant MA. After message 2 is received, the aspirant MA derives the MPTK-KD. If no problem is found in received message 2, the aspirant MA sends the handshake message 3 to the MKD and completes the entire mesh key holder security handshake process.

After this process is successfully done, the aspirant MA becomes an MA and assigns one to the "Mesh Authenticator" bit and the "Connected to MKD" bit in MSCIE of beacons or probe responses. The MSCIE shall also contain the MKDD-ID received from MKD in handshake message 2.

The MA will maintain a mesh path to the MKD. If the path is lost, the “Connected to MKD” bit needs to be set to zero, but the MA can still play the 802.1X authenticator role using cached keys.

Upon deriving the MPTK-KD, both the MKD and the MA will reset the replay counter that is used for mesh key transport.

Mesh Key Transport from MKD to MA The mesh key transport protocol completes two tasks: (1) securely deliver the derived PMK-MA and its related information from MKD to MA; (2) request the MA to delete a previously delivered PMK-MA.

For the first task, two mechanisms are specified: pull protocol and push protocol. In the mesh key transport pull protocol is initiated by the MA by sending a request message to the MKD. Upon receiving such a request, the MKD sends back the derived PMK-MA. In the mesh key transport push protocol, the MKD sends the PMK-MA to the MA without solicitation. However, the MKD needs to receive a confirmation message from the MA.

In the mechanism for the second task, the MKD initiates the process by sending a key deletion request to the MA. The MA deletes the key upon receiving this message and will send back a confirmation message to the MKD.

In all three mechanisms, the MKD and the MA maintain different replay counters. The replay counter is incremented by the initiator of each mechanism and is attached in the first message. The recipient verifies that the counter is not used by previous first messages. If it has been used before, then the message is discarded. Since both the MKD and the MA may be an initiator, both maintain a replay counter.

In all messages of the mesh key transport protocol, MIC is included for integrity protection. In addition, in both the pull and push protocols, the PMK-MA is encrypted.

Mesh Four-Way Handshake After peer link management, and initial MSA authentication, if required, the MA starts the MSA four-way handshake. This four-way handshake is similar to that of IEEE 802.11i except for the following.

- *Message 1.* The ANonce here is the MPTKANonce which is obtained by the MA from the MKD during the PMK-MA delivery. As in IEEE 802.11i, the key data field is empty.

- *Message 2.* The SNonce is the MPTKSNonce. The key data field includes encrypted information of RSNIE, MSCIE, MSAIE, and GTK key data encapsulation (KDE). RSNIE may also include PMK-MAName in the PMK-ID list. RSNIE, MSCIE, and MSAIE must be consistent with those in the peer link confirm message sent by the supplicant MP.

- *Message 3.* The message contains an MPTKANonce. Additionally, the key data field includes RSNIE, MSCIE, MSAIE, GTK-KDE, and lifetime KDE. RSNIE, MSCIE, and MSAIE must be consistent with those in peer link confirm message sent by the MA, and PMK-MAName must be in the PMK-ID list in RSNIE. The lifetime KDE contains the lifetime of PMK-MA.

- *Message 4.* This message is the same as that in IEEE 802.11i.

After the MSA four-way handshake completes, both the MA and the supplicant MP open the 802.1X controlled port. Subsequent EAPOL-key frames rely on key replay counter to protect messages from being replayed. The pairwise cipher suite is used to protect messages encrypted with PTK.

Limitations and Challenging Issues

The detailed operation procedures of 802.11 mesh network security have been specified in the IEEE 802.11s standard draft. However, by investigating the entire framework, we can find several major issues in this framework.

- Complexity, overhead, and performance. The procedures, especially the secure peer link management, are so complicated that it is hard to predict the performance for two reasons. First, the more complicated the operation procedures in a security protocol, the higher is the possibility that the security can be compromised, since more components are subject to security attacks. Second, the overhead of the protocol is really unknown. Thus, a full investigation of security performance is needed for the 802.11s security protocol.

- How to determine MKD. Although the functionalities of MKD are specified in 802.11s, there is no method for determining how an MKD is selected. Obviously, randomly picking an MP as an MKD is not a solution. In addition, for scalability reasons, it may need to consider whether only one MKD is enough in a large WMN. If not, then a mechanism needs to be defined to handle the security operations when multiple MKDs coexist.

- Peer link management and role selection procedure. The standard draft has defined a detailed procedure of peer link management of two peer MPs. This procedure also specifies how one of the MPs is selected as an 802.1X authenticator. However, it lacks a mechanism that considers the scenario where a new MP needs to set up a peer link with an MA or a supplicant MP. For example, if the same peer link management and role selection procedure is applied for the peer link setup between the new MP and an MA, it is possible that the new MP is selected as an authenticator but the MA's role becomes a supplicant. Such a conflict should be resolved efficiently; otherwise, frequent flip of function role of an MP can cause unnecessary overhead and also damage the security of 802.11s WMNs. However, no such a procedure is specified in the 802.11s standard draft.

6.4.3 Future Directions

Tremendous efforts are still needed to develop effective security schemes for WMNs, since so far, little work has been done specifically for WMNs. Along this path, three directions can be followed.

- Improve existing security schemes. A security scheme proposed for other wireless networks may not be applicable to WMNs. However, many schemes, with modifications or improvement, can be still applied to WMNs. To illustrate this concept, here are several examples.

  - The security mechanism proposed in IEEE 802.11i can be applied as one component for future IEEE 802.11 WMNs, i.e., for security between mesh clients and mesh routers. For the purpose of backward compatibility, this method is actually a preferred option rather than developing a totally new security.
  - The security mechanism in IEEE 802.16 mesh mode is still not enough to support mobile terminals. However, for the communications among mesh routers, a framework has been specified. Again, in order to be compliant with standards, the framework must be followed by extending the existing security mechanism to support the communications between base stations and mobile terminals and also to further improve the security performance in the IEEE 802.16 mesh backbone.
  - The key management scheme, secure routing protocols, and so on, proposed for mobile ad hoc networks are good examples of security schemes for a distributed multihop wireless networks. Thus, the key idea in these schemes can be borrowed for WMNs. However, modifications are necessary to reduce the complexity of these schemes in handling issues related to frequent topology change and mobility. For example, in WMNs, owing to the existence of mesh backbone, a routing protocol can work without frequent routing message exchange. Fewer routing messages imply that security attacks in the routing path are easier to defend in WMNs than in mobile ad hoc networks. The reduced complexity gives an opportunity for supporting more complicated, but more powerful, algorithms in authentication, MIC, and encryption without increasing cost and complexity in the system.

  In summary, it should be noted that the security algorithms for encryption, authentication, or MIC have been thoroughly researched in various wireless networks. Thus, the remaining work for these algorithms is to modify them to be applicable to WMNs and to evaluate the enhanced version under the WMN environment accordingly.

- *Develop new security protocols.* Besides enhancement of existing security schemes, novel security mechanisms are also desired. In particular, new secure protocols in MAC need to be developed, because the specific features of WMNs make a MAC protocol in WMNs significantly different from that in any other networks. For example, in WMNs, a TDMA MAC can be more easily implemented, while random access based MAC is preferred in mobile ad hoc networks owing to difficulty in timing synchronization. With such a different MAC, security attacks exhibit a lot of differences, and thus demand a different secure mechanism in the MAC protocol.

  A new trend of MAC and routing protocol design is to have cross-layer design. In the ongoing IEEE 802.11s standardization efforts, one option for MAC and routing is to have their major functions merged into one protocol layer, i.e., a layer-2 routing protocol will be specified. Such a methodology totally breaks the traditional layered-design for routing and MAC protocols, and thus makes the existing secure routing or secure MAC protocols not applicable to the final IEEE 802.11 WMNs. The situation is the same for other WMNs. Thus, new secure routing or MAC protocols have to take into account cross-layer design in order to follow this trend, and also, more importantly, to get a more effective security solution. For example, the security of a routing protocol can be better enforced by cooperative operation between MAC and routing protocols than by solely considering routing.

- *Security monitoring and response systems.* Security monitoring can be done directly through other security schemes such as authentication, message integrity check, or secure networking protocols. Once abnormal events are captured by these security schemes, responses should be made to prevent further attacks. For example, a network node that is determined to have been involved in security attacks can be assigned less network resources or even be terminated from network access. In another form of response, the response can just give an alarm and advise a person to check on-site. Whatever form the response action takes, the critical task is to accurately detect attacks in order to reduce the false alarm rate.

  Security monitoring may work independently from any other security schemes, which is a more attractive approach, since it adds one more counter-attack measure to WMNs. For example, a security model can be built based on user profiles of transmission rates, traffic types, mobility, etc. Abnormal behavior of a user can be detected via this model. A similar security model can also be derived based on profiles of a mesh node. The challenging issues of model based security monitoring include accuracy of the model and the availability of meaningful user or node profiles.

  Cross-layer design is also needed for security monitoring and response systems. A framework of intrusion detection in mobile ad hoc networks is proposed in [290]. However, how to design and implement a practical security monitoring system for WMNs has never been researched.

Virtual private networking (VPN) has become an effective scheme for providing a secure network over all public networks. It can also be adopted to establish a secure network over WMNs. However, the mechanism of VPN is independent of the security issues of WMNs, and is thus out of the scope of WMN security. It should be noted that a security attack to WMNs impacts VPN by failing or degrading WMNs; it usually cannot capture the encrypted information in VPN.

6.5 Multilayer Design for WMN Security

Developing security schemes in each protocol layer is necessary. However, this methodology has a limited role in defending attacks, because schemes located in a single protocol layer cannot solve problems in other layers. However, security attacks in a network may come simultaneously from different protocol layers. Thus, a multiprotocol layer security scheme is desired for network protocols.

Multilayer Approach

By looking into the particular features of WMNs and available capabilities of existing security schemes, it is clear that security can be easily compromised without a multilayer design. Thus, here we discuss a new security mechanism for WMNs based on the concept of multilayer design. It should be noted that cross-layer design is inherently embedded in the framework of multilayer design. The major components of the multilayer and cross-layer approach to WMN security are explained as follows.

- **Robust physical layer technique:** The most brute-force and also the most devastating security attack is jamming. Once the security in the physical layer is broken due to jamming, the entire wireless network just does not work anymore, no matter what security schemes are adopted in upper layers. In civil applications, jamming is a rare event, because such intentional actions are prohibited by law. However, jamming is a very common attack in military applications. On the other hand, although intentional jamming does not exist in civil applications, co-channel interference is rather common, especially when a wireless network works in an ISM band. Thus, for security purposes, it is necessary to develop physical layer techniques that are robust to jamming and co-channel interference. For example, a clustered-OFDM based spread spectrum scheme proposed in [288] achieved satisfactory performance in anti-jamming. It was also shown that the clustered-OFDM spread spectrum system working together with channel coding can effectively mitigate both jamming and fading effect.

- **Secure link-layer protocols:** When nodes come on line, they need to be associated with the network before joining the network. Thus, secure association plays a key role in this process. Secure associations are different for clients and mesh routers. Mesh routers are part of the WMN infrastructure, and their security can be better guaranteed, because: (1) more powerful encryption algorithm can be adopted; (2) no security-related information will be released to users. For network association of a mesh client, standard security schemes must be adopted in order to avoid denial of service to clients. For example, for IEEE 802.11 based mesh networks, the security schemes defined by IEEE 802.11i must be followed.

  The same security mechanism for network association must be applied to network access. When a mesh router is considered, it has connectivity to both mesh clients and other mesh routers. Again, security in communications between mesh clients and mesh routers is guaranteed by standard security schemes, while security in communications among mesh routers is achieved through a different but more powerful security algorithm.

- **Secure network-layer protocols:** In the network layer, both routing and data forwarding must be secure. Mobility makes these issues more complicated.

  In the secure routing protocol, integrity must be guaranteed for the messages that establish a routing path. Security schemes in the MAC layer cannot guarantee the integrity of routing messages. Thus, a straightforward solution is to authenticate a routing message hop by hop. This scheme has been adopted by many ad hoc routing protocols. However, it is inefficient due to the per-hop authentication. In WMNs, we propose another secure routing scheme, in which authentication of routing messages is only performed in two sectors: one is between mesh clients and mesh routers, the other is within the mesh backbone consisting of mesh routers. In WMNs, end-to-end communications between two clients may traverse multiple different wireless networks, e.g., IEEE 802.11 and IEEE 802.16. In this case, we can still treat these heterogeneous backbone wireless networks as one sector, and thus, only one authentication is needed. Optionally, we can further split the mesh backbone sector, and different authentication processes are done for different wireless network backbones.

Client mobility will trigger handoff in the link layer and also a change of routing path. Since our proposed scheme significantly reduces the complexity of authenticating routing messages, it supports client mobility more efficiently.

Data forwarding is usually protected by detection of, and reaction to, the malicious behavior of intermediate users. In WMNs, the intermediate nodes are usually mesh routers, and thus, the chance of being attacked by malicious users is low. In other words, if we can raise the security level in mesh routers, security in data forwarding is not a concern at mesh clients, which illustrates the advantage of WMNs. As a consequence, detection and reaction are only needed at the mesh backbone.

- **Secure transport:** In case the security in all lower layers is compromised, the last resort that we rely on is secure transport technology. Today secure sockets layer (SSL) and its successor, transport layer security (TLS), have successfully provided security for end-to-end communications. Thus, no new secure transport protocols are really needed. However, it is necessary to adopt secure transport protocols as an integral part of the overall security solution to WMNs.

6.5.1 Research Issues in the Multilayer Security

As explained before, open research issues for the multilayer security solution are mainly located in the mesh backbone. Such a strategy is advantageous over other schemes, because protocols in mesh clients can just follow standard schemes, and modification to the security module in mesh clients can be minimal.

- **Secure mesh network infrastructure:** Several research issues must be addressed in mesh backbone.

  - *Secure association/authentication among mesh routers:* To increase security performance, more powerful encryption algorithms are employed for network association between mesh routers. Since the same association procedure is used in a mesh router for both mesh clients and other mesh routers, it needs to be modified to take into account the differentiation between clients and routers. Another change to the association procedure is that it needs to support secure association with different wireless networks. For example, an IEEE 802.11 mesh router may need to be associated with another IEEE 802.11 mesh router and an IEEE 802.16 mesh router.

  - *Protection of mesh management and control messages:* To maintain a secure mesh backbone, management messages (e.g. probe/probe-response, beacon, etc.) and control messages need to be protected. Simply using periodic transmission, as usually done in existing mesh networks, can only provide stability but not security. When a malicious node also sends out these messages with different contents, mesh routers will be confused by such messages, and thus, the mesh backbone can be easily partitioned. Thus, encryption is needed to send these messages, and authentication is required for receiving them. The challenge here is that most management and control messages are broadcast in nature, while encryption and authentication usually assume point-to-point communications.

  - *Secure data forwarding:* Detection of malicious behavior needs to be both quick and accurate. Thus, it is necessary to consider the tradeoff between localized detection schemes and end-to-end detection schemes. When necessary, a hybrid detection scheme is needed. In order to expedite the reaction process in the mesh backbone, cooperation among mesh routers is preferred. In case a malicious node is detected, such information can be shared by different mesh routers in the neighborhood. This cooperative scheme increases the speed of reaction and also the accuracy of detection.

  - *Compliance with security standards:* In existing standard mesh networks, in particular IEEE 802.11s, no schemes have been proposed for security in the mesh backbone. However, it is required that the security in the mesh backbone be compliant with security schemes for network access. In the example of IEEE 802.11s, security in the mesh backbone must be compliant with IEEE 802.11i. Thus, when we develop new security schemes for the mesh backbone, we need to follow this guideline. In IEEE 802.16 mesh mode, many security flaws still exist. These problems must be addressed in our link-layer security scheme, but they have to conform with standard guidelines.

- **Secure routing protocol:** The research issues for secure routing are two-fold. One is to design a per-sector authentication scheme for routing messages, i.e., developing a scheme so that authentication is only performed at the first hop, the mesh backbone, and the final hop. No per-hop authentication is needed. The other is to make this per-sector authentication scheme part of the routing protocol.

- **Inter-system authentication:** When multiple mesh backbones from different service providers coexist, inter-system authentication is needed. This research issue is related to mobility management, and thus, must be studied together with mobility management schemes.

7

Network Control and Management

In a traditional wired network, the goal of a network management system is to assist network managers in monitoring and maintaining the network via various tools, applications, and devices. The well-known network management protocols include the simple network management protocol (SNMP) and the common management information protocol (CMIP). In these protocols, network management consists of the following major functions.

- **Performance management:** It aims to maintain the network performance at an acceptable level by monitoring network behavior, measuring various parameters of the network, and taking certain actions when necessary.
- **Configuration management:** Network and system configuration information is monitored so that operation on different versions of network hardware and software can be managed or tracked.
- **Accounting management:** Network utilization is measured in order to appropriately regulate network use by users.
- **Fault management:** This function detects network problems and then logs them or notifies them to users. Moreover, some capabilities of automatically fixing problems are expected.
- **Security management:** This function provides access control in order to avoid network access by unauthorized users.

When a wireless network, especially a WMN, is considered, more functions need to be available in the network management. First of all, a function must exist to handle mobility of network nodes, which demands a mobility management scheme for WMNs. Since the topology in WMNs can be variable because of node mobility, node association/disassociation, and fluctuating signal quality in links, it needs to be controlled so as to stabilize the network and achieve a better performance. Thus, topology control and management are also

Wireless Mesh Networks Ian F. Akyildiz and Xudong Wang

critical for WMNs. The power level of a node in WMNs closely impacts the network topology, the transmission rate of a node, and also the energy efficiency, so power management is another critical function for network management. To assist communication protocols, sometimes timing synchronization is needed among nodes. For example, any protocol based on the concept of TDMA must rely on synchronized timing among different nodes. These additional functions highlight new issues of network management in WMNs. In this chapter, all sections except for the last one are dedicated to additional network management functions required by WMNs. In the last section, traditional functions of network management are briefly discussed by considering the specific features of WMNs.

7.1 Mobility Management

Mobility management consists of two important tasks: location and handoff management [12]. Location management handles location registration and call delivery, while handoff management is responsible for handoff initiation, new connection generation, and data flow control for call handoff.

Several features of WMNs make their mobility management very different from that of both cellular networks and mobile ad hoc networks. In a cellular network, from client to the network there is always one wireless hop. However, there exist multiple wireless hops from mesh client to the Internet. In some mobile ad hoc networks, Internet access is not a concern, so user mobility can be handled by link-layer handoff and routing protocol. In other words, mobility management can be very simple or even not necessary. In a mobile ad hoc network that requires Internet access, the complexity of mobility management increases. However, network nodes do not need to provide network access for other network nodes, which can simplify the mobility management architecture.

The above differences highlight the challenges in mobility management for WMNs. However, compared to mobile ad hoc networks, WMNs have their own advantages such as that mesh routers are usually stationary and do not have a constraint on energy and processing power. Taking advantage of these features is helpful in reducing the complexity of mobility management for WMNs.

7.1.1 Mobility Management in Related Wireless Networks

Mobility management for cellular networks has been researched for many years [12]. In the Internet, to support the mobility of a mobile terminal from one subnet to another subnet, mobile IP has been proposed [206]. Mobile terminals always have one-hop access (either wired or wireless) to home agent (HA) or foreign agent (FA). Many research results have also been obtained for the next generation all-IP based wireless networks, even though there still remain open research problems [13]. The mobility management schemes developed for cellular [12] or mobile IP networks [13] could be useful for WMNs. However, the centralized scheme is usually not applicable to WMNs which are based on distributed and ad hoc architecture. Thus, distributed mobility management is a preferred solution for WMNs.

The most challenging issue of mobility management in mobile ad hoc networks is that the connectivity of a node with other nodes is intermittent and sporadic. Thus, the mobility management schemes proposed for cellular networks are not efficient for mobile ad hoc networks. The preferred approach is distributed mobility management, in which location databases are stored in mobile nodes themselves [99]. Since the network topology and connectivity depend on the mobility of nodes, mobility management in mobile ad hoc networks is a difficult task no matter whether distributed or centralized scheme is employed. In fact, this difficulty discourages users from accepting mobile ad hoc networks. Mobility management schemes of ad hoc networks are mainly comprised of two types: distributed mobility management [99] and hierarchical mobility management [53, 244]. Due to different network architecture and mobility between WMNs and mobile ad hoc networks, these schemes cannot perform well in a wireless mesh networking environment.

7.1.2 Mobility Management in WMNs

Although standards are available for WMNs, mobility management is still a least-specified area. Mobility management of IEEE 802.11 based WMNs is not fully investigated by the 802.11s task group [122] and the interim solution is based on IEEE 802.11f roaming solution [117]. However, this protocol was designed for the roaming from one access point to another, and has the drawback of a very large latency. Therefore, IEEE 802.11f itself is not active now, and roaming of IEEE networks is currently specified in IEEE 802.11r [121]. Neither IEEE 802.11f nor IEEE 802.11r is applicable to IEEE 802.11s due to significant differences in the network architecture.

So far, mobility management of IEEE 802.16 WMNs has not been specified in all available standards and drafts [130–132]. Initially, IEEE 802.16 was designed for fixed wireless access. In order to support mobile clients, an extended version, IEEE 802.16e, was proposed [132]. However, the IEEE 802.16e standard only covers mobility support for the point-to-multipoint (PMP) mode.

The specific features of WMNs make research results of mobility management obtained for other wireless networks not applicable to WMNs. On the other hand, some concepts from cellular, mobile IP, or mobile ad hoc networks can be borrowed for WMNs. So far, among the limited number of research papers on mobility management of WMNs [107, 199, 215, 227], none of them has really investigated the following issues.

- For the system architecture, what are the key differences between mobility management of WMNs and that of cellular networks and mobile IP?
- What is the best system architecture for the mobility management of WMNs?
- What are the challenging issues that are specific to the mobility management of WMNs?

As a result, existing mobility management schemes for WMNs usually follow the same system architecture as that of mobile IP or cellular networks and inherit similar procedures for location management and handoff mechanisms from cellular networks or mobile IP. However, the overall system architecture and operating procedures of a mobility management protocol for WMNs must be developed by following a novel framework because of the specific features pertaining to WMNs [273]. In what follows, we present a new mobility management scheme, called mobile mesh IP [259].

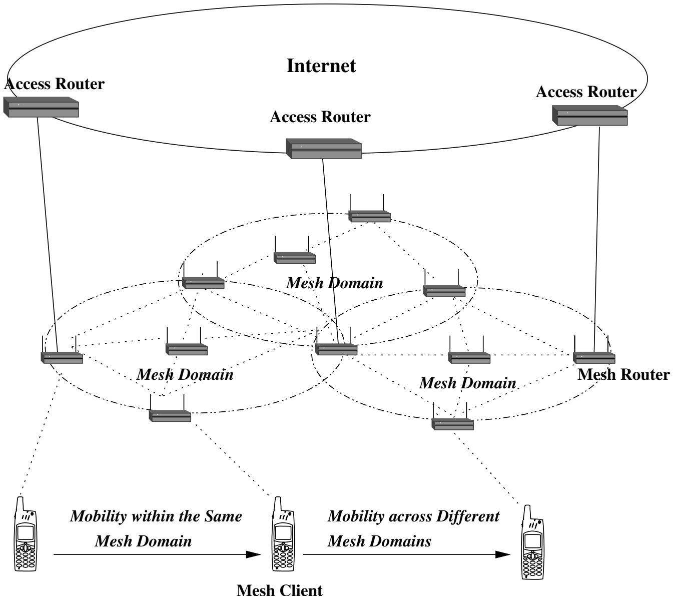

Figure 7.1 Mobility management of WMNs: an example

Architecture of Mobile Mesh IP

In general, mobility exists in either mesh clients or mesh routers. For example, considering a localized mesh network on the train, both mesh routers and mesh clients are mobile relative to the WMN on the ground. However, it is also true that, in most applications, mesh routers in WMNs remain stationary. Thus, in mobile mesh IP, we focus on the mobility management for mesh clients. Moreover, we assume that no ad hoc networking between mesh clients is necessary.

The concept of mobile mesh IP is depicted in Figure 7.1. The mobile mesh IP is compatible with mobile IP since the concepts of HA and FA in mobile IP are adopted. However, because of the WMN environment, the protocol architecture, mechanism, and operation procedures of mobile mesh IP are very different from those of mobile IP. The entire network consists of three hierarchical layers: Internet backbone, mesh backbone, and mesh clients.

The mesh backbone comprises localized mesh networks distributed in different geographical areas. We define such a localized mesh network as a *mesh domain*. Mesh backbone is connected to the Internet via wired links between mesh routers and access routers (AR). A mesh router connected to an AR is usually called a mesh gateway. In general, in one mesh domain only a small number of mesh routers are connected to their ARs. In the simplest case, only one mesh gateway is connected to its corresponding AR. However, if capacity is the concern, then multiple mesh gateways may be needed and are connected to their own ARs.

Similar to mobile IP, mobile mesh IP also needs home agent (HA) and foreign agent (FA) to support mobility management. HA is located at the Internet backbone, and can be distant from WMNs. An FA can be located together with an AR, a mesh gateway, or even a regular mesh router, depending on the design. Accordingly, the care-of-address (CoA) of a mesh client can be handled at an AR, a mesh gateway, or a regular mesh router.

Procedure of Mobile Mesh IP and Remaining Work

The mobile mesh IP is explained below. For simplicity, we assume that the FA is located with the mesh router that has direct connection to the AR. However, the optimal location of the FA is subject to research.

1. **Mesh client moves within the same mesh domain:** If a mesh client does not change its attached mesh router, then nothing needs to be done. When the mesh client detects that its attached mesh router is about to change, layer-2 handoff is invoked. After handoff is done, packets will be routed to the mesh client via the new mesh router. This re-routing process can be handled directly by the mesh routing protocol. However, in order to avoid packet loss and reduce re-routing delay, route rediscovery may need to be done before handoff is complete. It should be noted that route rediscovery only occurs in the same mesh domain, and in all cases no location update is needed.

2. **Mesh client moves from one mesh domain to another:** The change of mesh domain results in the change of CoA. Thus, this scenario is much more complicated than the previous scenario. First of all, layer-2 handoff is needed. Secondly, location update needs to be performed to locate the new FA for the mesh client, update the CoA at the HA, and find a new routing path from the HA to the FA. Thirdly, when location update is done, the mesh routing protocol needs to find a new routing path from the new FA to the mesh client.

Many problems in mobile mesh IP are different from mobile IP and thus require research efforts to solve.

- **Overall architecture design:** The major task in architecture design is to determine where an FA should be located. If it is with an AR or a mesh gateway, then a mesh client will find it difficult to detect the change of CoA, and thus a fast and efficient scheme is needed to detect the change of CoA. On the other hand, if an FA is with a regular mesh router, then it is easy for a mesh client to detect the change of CoA. However, there are several issues. Firstly, it is difficult to maintain an FA because of being separated from the AR by multiple wireless hops. Secondly, a mesh client may experience too frequent change of CoA, unless change of the attached mesh router does not mean a change of CoA. In the latter case, coordination between mesh routers is needed. In either case, signaling messages for updating CoA have to traverse a multihop wireless network, which can experience large delays and cause a large percentage of overhead [273].

- **Fast route rediscovery:** This is required whether or not location update happens. When location update is not needed, route rediscovery only occurs in the mesh routing protocol. Thus, mesh routing protocol needs to be quick in route rediscovery. When location update is needed, additional efforts are needed to quickly find a new routing path from HA to the new FA in the WMN.

- **Fast location update:** In addition to fast route rediscovery, the location update procedure must be designed to quickly locate the new FA for the mesh client.

Since multihop networks exist between the FA and the mesh client, locating a new FA is not obvious, and thus demands an efficient scheme. This task is correlated with the detection of CoA change. When CoA change is detected, the first step in location update is to find the new FA. Once FA is found, the CoA of the mesh client is updated at the HA.

- **Direct mesh routing across different mesh domains:** When a mesh router can be connected to other mesh routers in different mesh domains, it may forward packets from one mesh domain directly to another one for the purpose of load balancing. In this case, the mobility management becomes really challenging, because this mesh router needs to be associated with several gateways with different IP subnets. When a mesh client is associated with this mesh router during roaming, a new scheme is needed for the mesh router to decide which subnet shall be used to allocate an IP address for the mesh client. This issue reflects the conflict between IP routing and mesh routing.

- **Cross-layer design:** Owing the multihop wireless networks in WMNs, cross-layer design between a mobility management protocol and MAC and routing protocols is critical. For example, signaling messages of location management have to traverse a multihop wireless network. To improve the performance of location management, MAC and routing need to be improved to reduce the delay of signaling messages and increase the delivery ratio of such messages.

7.1.3 Open Research Issues

Many research issues still remain unresolved for mobility management of WMNs.

- **New framework of mobility management:** Mobile mesh IP is an example to illustrate the new framework of mobility management of WMNs. However, it still contains many issues to be resolved. Moreover, schemes with better architecture and design than mobile mesh IP also need to be developed.

- **Support of hierarchical mesh backbone:** Mesh backbone may consist of heterogeneous mesh routers organized hierarchically. Under this architecture, mobility management becomes more complicated, since a hierarchical wireless network is involved in all procedures such as handoff, location update, and route rediscovery.

- **Multilayer schemes:** Mobility management is closely related to multiple layers of network protocols, the development of multilayer mobility management schemes as in [72] is an interesting topic.

- **Cross-layer design:** To improve the overall performance of mobility management, cross-layer design plays an important role. For example, many functions such as fast handoff and fast router rediscovery all depend on cooperative work between multiple layers.

- **New location services:** Location service is a desired feature for WMNs. Location information can enhance the performance of MAC and routing protocols. It can help to develop promising location-related applications. Proposing accurate or efficient algorithms for location services is still an open research topic.

7.2 Power Management

Power level is an important parameter that can impact a wireless network in different ways. Thus, control of the power level or dynamic adjustment of the power level is critical to all wireless networks. Usually *power control* aims to determine the transmit power level such that the received power is maintained at a desire level no matter what the channel characteristics are and what the distance is between transmitter and receiver. However, *power management* is concerned with a more generic target. For example, power level needs to be controlled to save energy consumption, improve network stability, adjust the transmission rate, change the network topology, and so on. In this section, we first give a brief discussion of power management in wireless networks that are closely related to WMNs. Then, key aspects of power management in WMNs are presented.

7.2.1 Power Management in Related Wireless Networks

Power management has been a hot research topic for wireless sensor networks. Since sensors are constrained by energy consumption, energy efficiency has been the focus of power management in sensor networks. For mobile ad hoc networks, energy efficiency is again a key requirement. However, it also has another critical requirement: topology control. Owing to node mobility, the network topology is changing quickly, so power management is required to optimize the network topology in response to node mobility.

For IEEE 802.11 wireless networks, both power control and power management have been specified in the base standard [114]. The power control function provides an option for the MAC layer to adjust transmit power for each packet as necessary. Power management defined in IEEE 802.11 aims to reduce power consumption in mobile stations [114]. Mechanisms of power management have been specified for both the infrastructure network and the independent basic service set (IBSS). In the infrastructure network, power management is controlled by the access point. Thus, when a mobile station wants to work in power-save mode, it needs to inform the AP of this by setting the power management bits in the frame control field of a frame. Once the AP is notified of this operation, it cannot just send a packet to the mobile station at any time. Instead, it must buffer packets and send them to the mobile station at designated times when the mobile station is woken from the power save mode. In an IBSS, the principle of power management is similar to that in the infrastructure network. However, the power management process is not totally controlled by access points, but is handled by cooperation between nodes. When a mobile station wants to be in PS mode, it has to inform all other mobile stations of this operation by sending an ad hoc traffic indication message (ATIM). Thus, when another mobile station has packets for this station that is in power-save mode, it has to buffer packets. Different from the infrastructure mode, the mobile station does not have a designated time to send packets to the mobile station in power-save mode. Thus, before it starts to send packets, it has to send an ATIM. Since during the ATIM window, all mobile stations are awake, the mobile station can receive such a message, and then wake up to receive packets.

The operation of IEEE 802.11e [116], the QoS standard for IEEE 802.11, is different from the base IEEE 802.11, so some modifications are made to power management in IEEE 802.11e. For example, they have contention access period (CAP), contention period (CP), contention free period (CFP), and extended distributed channel access (EDCA) transmission opportunities (TXOP) in an IEEE 802.11e frame. Thus, power saving operations need to be changed to adapt to this different frame structure in both the infrastructure network and the IBSS. However, power control of IEEE 802.11e is the same as that defined in the base standard.

In IEEE 802.15, the situation is a little different from IEEE 802.11. In IEEE 802.15.1 [125], power management is defined as a function of the link manager layer. However, no particular scheme is specified. Power control is specified in IEEE 802.15.1 to provide a power controlled link for devices that have such a capability. For IEEE 802.15.4 [127], since it targets at low-rate wireless personal area networks (PANs) such as sensor nodes, power control is not considered as a necessary function. Power management is required according to the standard, but the specification of a detailed scheme is out of the scope of IEEE 802.15.4. In IEEE 802.15.3 [126], both power control and power management have been specified. There are two forms of power control for IEEE 802.15.3: one is maximum transmit power for contention access period (CAP), beacon, and directed management channel time allocations (MCTAs), and the other is adjustable power in channel time allocation (CTA). Maximum transmit power control aims to prevent any device in CAP having better access to the medium. Adjustable transmit power control is intended to reduce both power usage and interference [126]. The goal of power management in IEEE 802.15.3 is to enable longer operation time for battery-powered devices. Three techniques are specified to turn off a device for one or more superframes: device synchronized power save (DSPS) mode, piconet synchronized power save (PSPS) mode, and asynchronous power save (APS) mode. Thus, a device in a piconet can be in four states: ACTIVE mode, DSPS mode, PSPS mode, and APS mode. As usual, IEEE 802.15.3 does not give a detailed scheme for utilizing the three power save modes to reduce power consumption.

In IEEE 802.16 power control is specified to determine transmit power level in both uplink and downlink. Power control can be closed or open loop. However, other functionalities of power management are not specified. For example, how to achieve power efficiency for clients is not defined in IEEE 802.16.

7.2.2 Power Management in WMNs

Power management in most other wireless networks is focused on power control and power saving operations. However, the objective of having power management in WMNs is much broader. Moreover, the goal of power management for WMNs varies, and is also different between mesh routers and mesh clients.

Power Management for Mesh Routers

Since mesh routers do not have a constraint on power consumption, power management usually aims to control connectivity, interference [155], spectrum spatial-reuse, topology [165], and so on. The major functionalities that can be achieved through power management are summarized as follows.

- **Self-organize the network:** When mesh routers are deployed as a backbone network, their locations are an important factor that impacts the network performance, especially for indoor environment. Using a sophisticated RF site survey may help to find satisfactory locations. However, this actually conflicts with the initial motivation of using WMNs, i.e., convenience. Moreover, various deployment factors can impact the performance of WMNs. Although investigating such factors to find out guidelines for deployment of WMNs [224] is helpful to improve network performance, it is not enough for performance optimization considering various contradicting parameters. On the other hand, practically, mesh routers should be able to be deployed by anyone without RF engineering experience. To avoid this dilemma, we can rely on power management to self-organize the network in the following way. First, mesh routers can be deployed by using simple rules. For example, in a home environment, users can put mesh routers in any locations as long as routers have approximately the same distance in between. Owing to different channel fading and attenuation, the received power level at different routers will be different. Thus, the second step is to apply a power management scheme to automatically adjust the power level on each mesh router. By doing so, mesh routers are organized to form a network that will achieve the best performance in terms of throughput.

- **Improve network connectivity and stability:** This functionality can be viewed as an additional task of network self-organization or a new task if self-organization is not available. It aims to ensure that the network is stable in terms of connectivity or topology. In a wireless mesh networking environment, without power management, link quality between nodes varies from time to time. This will cause some nodes to lose connectivity or change their associations with other nodes. Such dynamics will finally result in an unstable network topology, and severely degrade the performance of MAC, routing, and even transport layer protocols. Therefore, power levels on mesh routers need to be adjusted dynamically instead of being set up with a fixed number, so that link quality between nodes is always maintain at an acceptable level.

- **Reduce interference and increase spectrum spatial-reuse:** Spectrum spatial-reuse is a critical factor that impacts the scalability of WMNs. If spectrum spatial-reuse is poor, throughput drops quickly as the number of hops increases, and also the number of users that can be supported is small. When a single channel is used in each network node, interference among nodes greatly impacts the spectrum spatial-reuse factor. When multiple channels are used, this problem is less severe. However, considering one specific channel, its spectrum spatial-reuse is still low. Thus, for both single-channel or multichannel mesh routers, power management is needed to ensure that the received power level at each mesh router does not exceed a desired level. Otherwise, interference will result in a low spatial-reuse efficiency [155]. However, lower received power levels will cause more hidden nodes and thus further cause performance degradation in the MAC protocol. Thus, when the problems of spectrum spatial-reuse efficiency and hidden nodes need to be solved at the same time, power management must be taken into account as an integral part of a MAC protocol.

- **Increase transmission rate:** Currently the physical layer of wireless networks usually supports multiple transmission rates by using different modulation and coding schemes under different channel qualities. The actual transmission rate is selected at the MAC layer according to the statistics of previous transmissions, and such a process is called MAC layer rate control. In WMNs, multiple transmission paths exist. As shown in Figure 7.2, considering end-to-end communications between Node A and Node C,

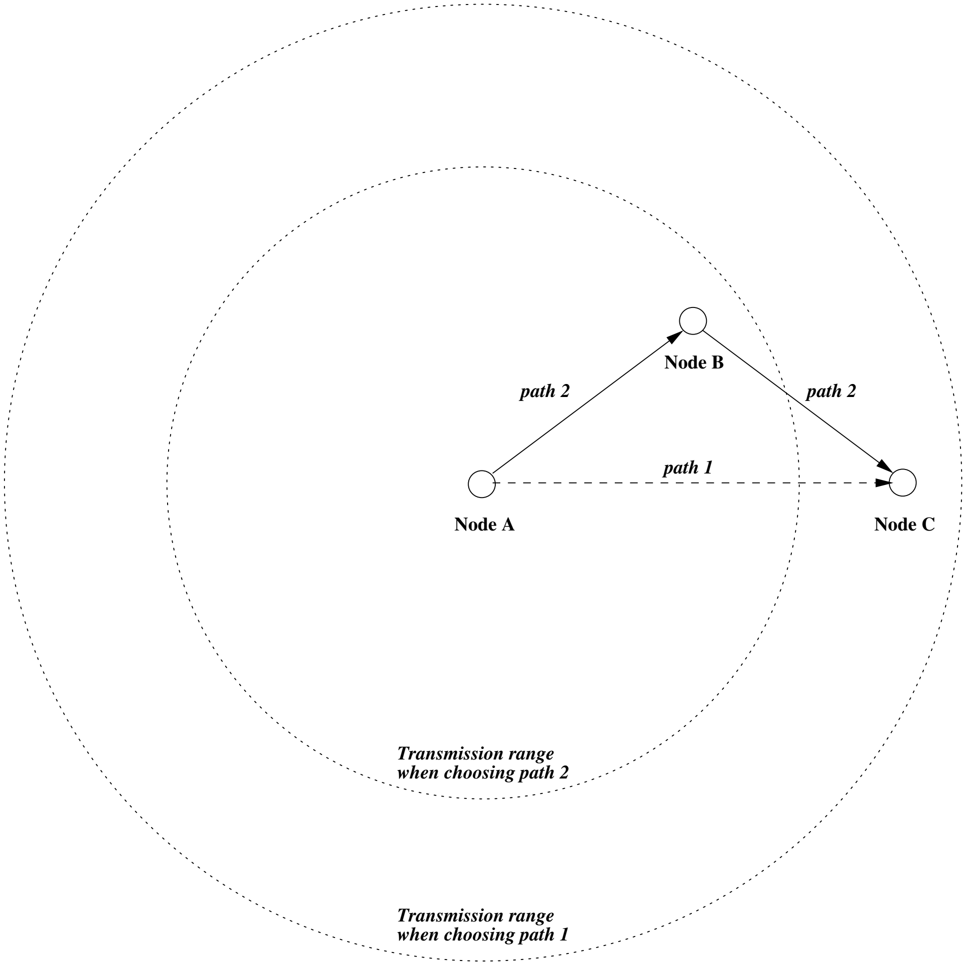

Figure 7.2 An example of interactions among rate control, routing, and power management

the packets from Node A can go directly to Node C (called *path 1*), or go to Node C via Node B (called *path 2*). By using *path 1*, the link quality between Node A and Node C may be poor and thus a low transmission rate has to be adopted. If Node A increases its transmit power level, a higher transmission rate can be used. However, Node A will generate a very large interference range. On the other hand, if *path 2* is adopted, both Node A and Node B can use a lower transmit power level to achieve a high transmission rate. The disadvantage in this scenario is that multihop transmission reduces the capacity of the entire network, because one packet from Node A to Node C simply uses the same channel for a longer time. Thus, a tradeoff is needed to determine whether *path 1* or *path 2* is better. The tradeoff needs to consider the power management, rate control, and routing altogether.

So far, the research on power management for mesh routers is mostly focused on reducing interference. However, other important functionalities have not been investigated. Thus, it is necessary to develop new power management schemes to self-organize networks, increase transmission rate, and improve network connectivity and stability. A more interesting research topic is to develop a power management scheme that will support all the functionalities discussed above.

Power Management for Mesh Clients

In contrast to mesh routers, mesh clients might expect protocols to be power efficient. For example, some mesh clients are IP phones or even sensors; power efficiency is a major concern for them. Thus, it is quite possible that some applications of WMNs require power management to optimize both power efficiency and connectivity, which results in a complicated problem. To avoid this complexity and also to take advantage of the availability of mesh routers, a rule of thumb for protocol design is to make sure that protocols on mesh clients are as simple as possible. For example, for a routing protocol, the major computation and overhead must be kept inside mesh routers.

7.2.3 Open Research Issues

To further improve the performance of WMNs, power management needs to propose solutions to the following research problems.

- Developing a single power management scheme that can self-organize networks, achieve high spectrum spatial-reuse efficiency, maintain stable network connectivity, and transmit packets using high transmission rate.

- Cross-layer design between power management and other protocols, in particular MAC and routing protocols.

- Reducing protocol complexity in mesh clients.

- Implementing protocols on mesh routers to support power saving modes for mesh clients.

7.3 Topology Control and Management

The topology of a wireless network depends on two sets of factors: uncontrollable factors and controllable factors [221]. Uncontrollable factors include node mobility, interference, noise, channel fading, etc. Controllable factors can be transmit power level, antenna direction, and node locations. Topology control is an optimization process of utilizing controllable factors to compensate for uncontrollable factors so that the network topology is formed into a structure that can achieve the desired performance level. The performance metrics include energy efficiency, interference, stability, etc.

7.3.1 Topology Control and Management in Related Wireless Networks

Topology control has been researched for a long time in different networks such as packet radio network (PRN) [104], mobile ad hoc networks, and wireless sensor networks [168].

Based on different performance metrics considered in topology control, existing topology control schemes can be classified into the following major types.

- **Topology control for energy efficiency:** Most of the existing topology control schemes are focused on the problem of reducing energy consumption [47, 166]. This is very meaningful for mobile ad hoc networks and wireless sensor networks, but not for WMNs. Some other schemes consider energy efficiency by switching nodes into power-save mode [91]. Thus, topology control is not only cross-related with power management, but becomes more complicated because of radio on/off directly changing the network topology. Again, this kind of methodology is not necessary for WMNs because there are no constraints in energy.

- **Topology control for low interference:** Interference can be reduced by decreasing transmit power or lowering the network degree. However, to directly control the interference in a topology control scheme, the optimization problem must consider interference as a performance metric. For wireless sensor networks, algorithms are proposed in [168] to solve this problem. Through these algorithms, the maximum link interference of the entire network is minimized. Reducing interference can increase the capacity of an individual node, because its experienced interference becomes lower. However, it does not guarantee that the network capacity also increases, since reducing interference is brought by low transmit power, and this causes a larger number of hops for the same end-to-end communication. Thus, merely relying on interference to optimize topology control may not be sufficient to improve overall network performance.

- **Topology control for fault tolerance:** If topology control is only concerned with energy efficiency or reducing interference, the network topology may become more sensitive to node failure or node departure, for two reasons. First, the network may have few links available for fault tolerance. Second, end-to-end communications between two nodes may have more hops, and thus become more fragile to node failure or node departure. To solve this problem, a fault tolerant topology algorithm is proposed in [167] for wireless ad hoc networks. It should be noted that node failure or node departure is just one source of network instability.

Some topology control schemes [104, 167] need position or location information on each node, while others [91] do not need such information. Generally, topology control schemes independent of position information are preferred to those that need such information. However, sometimes position information can greatly improve the performance of topology control. In this case, tradeoff needs to be made between the accuracy and complexity of a position sensing scheme and the effectiveness of topology control.

Topology impacts the capacity of multihop networks. However, no schemes have really considered capacity as a direct performance metric, because network capacity is determined by several interleaved parameters such as transmit power level, interference, and average hop of a traffic flow, and also by several protocols.

7.3.2 Topology Control and Management in WMNs

Today some WMNs are still using a single channel, while others have started to use multiple channels in order to increase network capacity. Topology control for these two types of WMN are different, since the channel allocation in a multichannel WMN also impacts the topology.

Single-Channel Network

So far little research work on topology control has been specifically done for WMNs, even for single-channel WMNs. The research work on mobile ad hoc networks may not be applicable to WMNs, since mobility is not a concern for topology control of WMNs. Thus, node mobility must be taken out from the optimization problem when a topology control algorithm is designed for WMNs. Energy efficiency is not a constraint in the topology control of WMNs either. Thus, the optimization problem does not need to consider the constraint of energy consumption. In addition, the topology control scheme had no need to handle nodes in sleep or power-save mode. This potentially makes the topology control problem in WMNs easier than that in mobile ad hoc networks, and this motivates us to develop a lightweight or practical topology control scheme for WMNs.

As discussed in the previous subsection, some topology control schemes have been proposed for ad hoc networks or multihop networks without node mobility [167, 168]. These schemes can be applied to WMNs. Recently some schemes have been proposed to construct rural WMNs by minimizing the deployment cost due to antenna towers [205]. In [69] robustness of network topology is considered when building a WMN based on directional antennas. However, all of these schemes consider only one performance metric and take into account the relationship with only one protocol layer. To best take advantage of topology control, a unified scheme that considers multiple performance metrics, and also multiple protocol layers, is needed.

Multichannel Network

For a multichannel WMN, more problems arise in topology control, since network topology is now also impacted by channel selection. In [249], an interference-aware channel allocation scheme is proposed to achieve minimum interference among all K-connected topologies. Other performance metrics such as stability and network capacity have never been investigated in multichannel WMNs.

Multichannel WMNs can be based on a single radio or multiple radios. If it is single-radio based, usually only one transceiver is available on the radio. Thus, channels must be switched on time. In other words, if not carefully designed in topology control, the network can be easily partitioned into different networks from time to time. A simple approach to this problem is to use a common channel at a given time slot for all nodes. Thus, all nodes will have a consistent view of the network topology. A topology control algorithm for a multichannel WMN is usually more complicated than that for a single-channel MAC, even if a single performance metric is considered. When multiple performance metrics are taken in account, the complexity is even higher.

When a WMN consists of multiradio nodes, the network partition issue can be easily resolved, because each node can use different radios at the same time to communicate with its neighbors. For the same reason, the optimization problem of topology control in a multiradio can be simpler; it does not need to consider channel sharing on a time division basis among nodes in the same neighbor.

Open Research Issues

- **Topology control with directional antennas:** So far, most research work on topology control is focused on omnidirectional antennas. Although directional antennas are difficult to use in mobile ad hoc networks, they have a good fit for WMNs, since minimal mobility in mesh nodes makes changing antenna direction become a feasible task. Since different direction of antennas results in different link connectivity, antenna direction control is closely coupled with topology control. Since both MAC and routing are impacted by antenna direction, topology control schemes for WMNs with directional antennas need to take into account the design of MAC protocols and routing protocols.

- **Topology control for WMNs with heterogeneous nodes:** When nodes with single channel and nodes with different numbers of channels coexist in the network, new topology control schemes need to be developed. Moreover, nodes may also be different in maximum transmit power, which gives another constraint on the topology control scheme.

- **Cross-layer design with other protocols:** Since topology is actually used by routing either explicitly or implicitly [221], it is closely related to routing. Moreover, topology also reflects the connectivity between nodes in neighbors, so it also impacts the performance of the MAC. We also know that both routing protocol and MAC protocol are closely related to rate control. In addition, topology control is usually performed through transmit power adjustment, which further impacts power control and management schemes. Therefore, the optimization of topology control must take into account all these constraints, which is a challenging research problem.

- **Topology control for stability:** Fault tolerance to node failure or departure has been considered in [167], and this can definitely improve network stability in the routing layer on a large timescale. However, network stability is also impacted by variations in link quality, which is fast in timescale. Thus, a new scheme is needed in topology control so that fast variable link quality will not produce frequent changes in topology. Otherwise, neither MAC nor routing will work with good performance.

- **Low complexity and practical topology control solutions:** To date, many topology control schemes are proposed without considering the computation complexity or the possibility of being implemented. Although the performance is justified through theoretical analysis, they are difficult to be implemented.

8

Network Capacity

In the past decade, a lot of research work has been carried out to study the capacity of ad hoc networks which can be adopted to investigate the capacity of multihop wireless networks.

For a stationary multihop network, it has been shown that the optimum transmission power level of a node is reached when the node has six neighboring nodes [148]. With this value, an optimum tradeoff between the number of hops between source and destination and the channel spatial-reuse efficiency is achieved. This result is useful for infrastructure WMNs with minimal mobility. When the mobility is a concern, as in hybrid WMNs, no theoretical results are reported so far.

Some experimental studies have been performed in [30], where the simulation results of a stationary network validate the theoretical results of [148].

Asymptotic lower and upper bounds of network capacity are given in [96]. From the analytical results, it follows that the throughput capacity per node reduces significantly when the node density increases. An important implication is derived in [96] as guidelines to improve the capacity of ad hoc networks: *A node should only communicate with nearby nodes.*

The implication given in [96] can also be reflected in [251]. The scheme proposed in [251] increases network capacity of ad hoc networks by utilizing the node mobility. When a node needs to send packets to another node, it will not send until the destination node is close to the source node. Thus, via the node mobility, a node only communicates with its nearby nodes. The scheme has a limitation: the delay may become large and the required buffer for a node may be infinite.

Asymptotic analysis of multihop wireless networks in [96] and [251] has motivated other research work such as [152, 175, 287], where a hybrid network architecture is considered to improve the capacity of ad hoc networks. In the hybrid architecture, nodes only communicate with nearby nodes. If they need to communicate with nodes many hops away, base stations or access points are used to relay packets via wired networks. The hybrid architecture can improve the capacity of ad hoc networks, but it may still not be favored by many applications because wired connections between base stations do not exist in many ad hoc networks or in WMNs. Thus, capacity analysis is carried out for an infrastructure WMN in which the wireless links between mesh routers (i.e., infrastructure nodes) has limited bandwidth in [291].

Wireless Mesh Networks Ian F. Akyildiz and Xudong Wang

In a multihop wireless network, capacity is not the single concern of performance. For example, delay is another performance metric. Networks under a certain scheduling scheme can provide high capacity, but the delay may also be significantly large. Thus, it is necessary to investigate the delay performance while studying the network capacity. In [201], throughput and delay tradeoff is analyzed using an independent and identically distributed (i.i.d.) mobility model. In [85], in addition to the analysis of the throughput-delay tradeoff for both static networks and mobile networks, a scheduling scheme is proposed to achieve throughput-delay optimality.

Most of the existing analytical approaches are based on asymptotic analysis. They have significantly driven the progress in capacity research of multihop wireless networks. However, several research problems are still open. First of all, little research work has been carried out to improve network capacity by considering new technologies such as network coding. More performance metrics need to be taken into account for tradeoff with capacity, i.e., only delay-throughput tradeoff is not sufficient. Moreover, the approaches of asymptotic analysis have limitations. Firstly, the upper or lower capacity bounds derived from these approaches do not reveal the exact capacity of a multihop wireless network with a given number of nodes, in particular when the number is small in the sense of asymptotic analysis but is a typical scale in a practical deployment of WMNs. Secondly, the networking protocols have not been fully captured by the analysis. For example, power control mechanisms, commonly used to improve the network capacity, are not considered in the analysis. As another example, the characteristics of ad hoc routing protocols have not been totally captured in the analysis. In any routing protocol, the route for packets does not necessarily follow the path along the straight-line segment between the source and destination as given in the analysis, because the routing protocol determines a path according to certain metrics such as the hop count, link quality, etc. [70].

An analytical approach is proposed in [139] to study the exact capacity of WMNs. The analysis is simplified by taking advantage of the low mobility feature of WMNs. However, the analytical model is based on assumptions that are not necessarily valid for a WMN.

As a result, the applicability of the theoretical results on practical network architectures still remains unclear. A close match between the theoretical results in [96] and IEEE 802.11 based ad hoc networks is reported in [164]. However, this study relies on the assumption that the traffic pattern in a large ad hoc network tends to be local, and thus, nodes usually communicate with nearby nodes. This assumption is not always valid in a network unless it is intentionally designed so.

8.1 Notations and Terms

In order to help better understand the theoretical results in the following sections, the frequently used asymptotic notations [98] and capacity definitions [96] are explained first. Some terms peculiar to a specific analytical approach will be explained individually as they appear.

$O(\cdot)$: This is a Landau symbol. Given $f = O(\phi(n))$, where $\phi(\cdot)$ is a positive function, there exists a constant c such that $|f| < c\phi$ for all values of n. In other words, the order of f is not higher than that of ϕ.

$o(\cdot)$: This is also a Landau symbol. Given $f = o(\phi(n))$, where $\phi(\cdot)$ is a positive function, $f/\phi \to 0$ as $n \to \infty$. In other words, the order of f is strictly lower than that of ϕ.

$\Omega(\cdot)$: This is the inverse of Landau symbol $O(\cdot)$ and they have the following relationship:

$$f(n) \in O(g(n)) \Leftrightarrow g(n) \in \Omega(f(n)).$$

$\omega(\cdot)$: This is the inverse of Landau symbol $o(\cdot)$.

$$f(n) \in o(g(n)) \Leftrightarrow g(n) \in \omega(f(n)).$$

$\Theta(\cdot)$: Given $g(n) = \Theta(f(n))$, it is not much better than $f(n)$ but also not much worse than $f(n)$, i.e.,

$$\Theta(f(n)) = O(f(n)) \cap \Omega(f(n)).$$

Feasible throughput: A throughput of $\lambda(n)$ is feasible if there exists a spatial and temporal scheme for scheduling transmissions in a multihop wireless network, such that every node can send $\lambda(n)$ bits per second on average to its destination node.

Throughput capacity: A wireless network has a throughput capacity of the order of $\Theta(f(n))$ if there exist deterministic constants $c > 0$ and $c' < \infty$ such that

$$\lim_{n\to\infty} = \Pr(\lambda(n) = cf(n) \text{ is feasible}) = 1$$

and

$$\lim \inf_{n\to\infty} = \Pr(\lambda(n) = c' f(n) \text{ is feasible}) < 1.$$

8.2 Capacity of Ad Hoc Networks without Mobility

To analyze the capacity of wireless networks, the space of the network is scaled into a region of area 1 m^2, in which n nodes are located. In the network, each node can transmit W bits per second over a common wireless channel. The same results will apply to a network with subchannels of capacity of $W_1, W_2, \ldots, W_M$, as long as

$$\sum_{m=1}^{M} W_M = W.$$

Communications between source and destination are carried out in a multihop fashion, and thus packets may wait for transmission at some intermediate nodes.

Since node locations and traffic pattern impact on the analysis, two typical setups of multihop ad hoc networks are defined: *arbitrary networks* and *random networks*. In an arbitrary network, nodes are located arbitrarily in a disk of unit area in the plane, and each node chooses an arbitrary destination to which the traffic is sent at an arbitrary rate. In addition, each node can choose an arbitrary transmission range.

On the other hand, in a random network, nodes are randomly located according to an independent and uniform distribution, either in a unit disk in the plane or on the surface S^2 of a three-dimensional sphere. Each node chooses a node nearest to a randomly located point as the destination to which it sends traffic. The nodes in a random network are homogeneous, i.e., all transmissions use the same transmission range.

8.2.1 Arbitrary Networks

The capacity of a wireless network is constrained by how a packet can be sent successfully in the network. There are many reasons for packet loss, e.g., erroneous packets due to interference among different transmissions from multiple nodes, or dropped packets due to out-of-order transmission or timeout. In this analysis, only interference-related errors are considered. Thus, a packet transmitted from one node to another can be assumed to be successfully received if and only if the received signal level is high enough above the interference. Two models can be used to capture the condition under which a transmission can be successful: the *protocol model* and the *physical model.*

In the protocol model, interference is avoided by allowing only one transmission in the same space region, and thus a transmission from a node with location X_i can be received by a node with location X_j if

$$|X_k - X_j| > (1 + \Delta)|X_i - X_j| \tag{8.1}$$

for every other node X_k with a simultaneous transmission in the same channel. Δ is a guard zone to ensure no interference between neighboring nodes. In the physical model, there is no guard zone but a signal to interference ratio (SIR) is used to prevent interference from neighboring nodes. Assume that a set of nodes, represented by their locations $\{X_k; k \in \mathcal{T}\}$, simultaneously transmit in the same channel using power level P_k for node X_k. In the physical model, a transmission from a node X_i to a receiving node X_j can be received successfully if

$$\frac{P_i/|X_i - X_j|^\alpha}{N + \sum_{\substack{k \in \mathcal{T} \\ k \neq 1}} (P_k/|X_k - X_j|^\alpha)} > \beta \tag{8.2}$$

where β is the minimum SIR for successful reception. Thus, the protocol model contains a more simplified space-reuse model than the physical model.

Upper Bound

Assume that there are n nodes in the network, the network transports $\lambda n T$ bits over T seconds, and the average distance between a source and a destination is $\bar{L}$. Thus, the transport capacity is $\lambda n \bar{L}$ bit-meters per second.

Considering a bit b, $1 \leq b \leq \lambda n T$, it traverses $h(b)$ hops from its source to its destination, and the h_{th} hop has a distance of r_b^h. Thus, for each bit, the average distance from source to destination is $(\sum_{b=1}^{\lambda n T} \sum_{h=1}^{h(b)} r_b^h)/\lambda n T$. Since such an average distance is not less than the average distance $\lambda n \bar{L}$, we have

$$\sum_{b=1}^{\lambda n T} \sum_{h=1}^{h(b)} r_b^h \geq \lambda n T \bar{L}. \tag{8.3}$$

Assume all nodes in the network transmit according to TDMA in M subchannels. Each subchannel has a capacity of W_m bits per second and the overall capacity of all subchannels is W, i.e., $\sum_{m=1}^{M} W_m = W$. Assuming that the time slot is τ seconds, then the number of bits sent in one time slot in subchannel m is less than or equal to $W_m \tau n/2$, since at most $n/2$ nodes can transmit, i.e.,

$$\sum_{b=1}^{\lambda n T} \sum_{h=1}^{h(b)} \delta^h(m, s) \leq \frac{W_m \tau n}{2}, \tag{8.4}$$

where $\delta^h(m, s) = 1$ when the transmission in $h_t h$ hop is using subchannel m and time slot s. Thus, summing over all subchannels and time slots, yields

$$\sum_{b=1}^{\lambda nT} h(b) \leq \frac{WnT}{2}. \tag{8.5}$$

Suppose node X_j is receiving from node X_i at the same time that node X_l is receiving from node X_k. Considering a protocol model and triangle inequality,

$$|X_j - X_l| \geq (1 + \Delta)|X_i - X_j| - |X_l - X_k|. \tag{8.6}$$

Similarly,

$$|X_l - X_j| \geq (1 + \Delta)|X_k - X_l| - |X_j - X_i|. \tag{8.7}$$

Adding the above two inequalities yields

$$|X_l - X_j| \geq \frac{\Delta}{2}(|X_k - X_l| + |X_i - X_j|). \tag{8.8}$$

The above result illustrates that a disk with a radius of $\Delta/2$ times the length of the hop is disjoint with another such disk. Due to the edge effect, such a disk can be on the periphery of the unit disk area (called *domain*). In addition, a transmission range larger than the diameter of the domain is unnecessary. Thus, at least one quarter of such a disk overlaps with the domain. Consequently, the total number of bits received by a receiver from a transmitter in time slot s and subchannel m is $\sum_{b=1}^{\lambda nT} \sum_{h=1}^{h(b)} \delta^h(m, s)(\pi\Delta^2/16)(r_b^h)^2$, which is $\leq W_m\tau$. Considering all subchannels and time slots, we have

$$\sum_{b=1}^{\lambda nT} \sum_{h=1}^{h(b)} \frac{\pi\Delta^2}{16}(r_b^h)^2 \leq WT. \tag{8.9}$$

Define $H = \sum_{b=1}^{\lambda nT} h(b)$ and combine (8.5) and (8.9), and we have

$$\sum_{b=1}^{\lambda nT} \sum_{h=1}^{h(b)} \frac{(r_b^h)^2}{H} \leq \frac{16WT}{\pi\Delta^2 H}. \tag{8.10}$$

Thus,

$$\sum_{b=1}^{\lambda nT} \sum_{h=1}^{h(b)} r_b^h \leq \sqrt{\frac{16WTH}{\pi\Delta^2}}. \tag{8.11}$$

Combining this result with (8.3), we obtain

$$\lambda nT\bar{L} \leq \sqrt{\frac{16WTH}{\pi\Delta^2}}. \tag{8.12}$$

According to the definition of H and (8.5), the transport capacity $\lambda n\bar{L}$ is bounded as follows:

$$\lambda n\bar{L} \leq \frac{\sqrt{8}}{\pi}\frac{1}{\Delta}W\sqrt{n} \tag{8.13}$$

bit-meters per second.

For the physical model, the following result can be derived via the similar approach for the protocol model [96]:

$$\sum_{b=1}^{\lambda nT}\sum_{h=1}^{h(b)}(r_b^h)^\alpha \le 2^\alpha \pi^{-\pi/2}\frac{\beta+1}{\beta}WT. \tag{8.14}$$

Thus, the transport capacity $\lambda n\bar{L}$ is bounded as follows:

$$\lambda n\bar{L} \le \left(\frac{2\beta+2}{\beta}\right)^{1/\alpha}\frac{1}{\sqrt{\pi}}Wn^{(\alpha-1)/\alpha}. \tag{8.15}$$

Consider a special case of the physical model where $P_{max}/P_{min} < \beta$. If node X_i is transmitting to node X_j at the same time that X_k is transmitting to X_l, then from the physical model, we have

$$\frac{P_i/|X_i - X_j|^\alpha}{P_k/|X_k - X_j|^\alpha}.$$

Thus,

$$|X_k - X_j| \ge \left(\frac{\beta P_{min}}{P_{max}}\right)^{1/\alpha}|X_i - X_j|.$$

If we define $\Delta = (\beta P_{min}/P_{max})^{1/\alpha} - 1$, then the physical model is in the same format as the protocol model. This implies that the same upper bound as that for the protocol model can be derived for the physical mode.

Constructive Lower Bound

For arbitrary networks, a certain amount of transport capacity can be actually achieved via properly placing nodes and assigning their traffic patterns.

In the protocol model, if the center of the disk of unit area is located at the origin, and put transmitters at locations $(j(1+2\Delta)r \pm \Delta r, k(1+2\Delta)r)$ and $(j(1+2\Delta)r, k(1+2\Delta)r \pm \Delta r)$ where $|j+k|$ is even. In addition, receivers are placed at locations where $|j+k|$ is odd. Thus each transmitter can send a signal to its nearest receiver that is r away and experiences no interference from another other transmitter–receiver pair. In addition, the total number of such transmitter–receiver pairs is at least $n/2$ and each pair can send a rate of W bits per second. Thus, the transport capacity is $n/2Wr$, i.e.,

$$\frac{W}{1+2\Delta}\frac{n}{\sqrt{n}+\sqrt{8\pi}}.$$

Such a value is a constructive lower bound for the protocol model.

For the physical model, the lower bound can be expressed as

$$\frac{1}{(16\beta(2^{\alpha/2}+(6^{\alpha-2}/\alpha-2)))^{1/\alpha}}\frac{nW}{\sqrt{n}+\sqrt{8\pi}}.$$

Summary of Throughput Capacity for Arbitrary Networks

According to the upper bounds and lower bounds of the transport capacity, the following results can be derived.

For the protocol model, both upper bound and lower bound of the transport capacity is $\Theta(W\sqrt{n})$, so the actual transport capacity of an arbitrary network is $\Theta(W\sqrt{n})$ bit-meters per second. For the physical model, the upper bound of the transport capacity is

$$\left(\frac{2\beta+2}{\beta}\right)^{1/\alpha}\frac{1}{\sqrt{\pi}}Wn^{(\alpha-1)/\alpha}$$

and

$$\frac{1}{(16\beta(2^{\alpha/2}+(6^{\alpha-2}/\alpha-2)))^{1/\alpha}}\frac{nW}{\sqrt{n}+\sqrt{8\pi}}$$

is a feasible lower bound. In other words, for the physical model, the lower bound of the transport capacity is $\Theta(W\sqrt{n})$ and the upper bound is $\Theta(Wn^{(\alpha-1)/\alpha})$. In a special case when $P_{max}/P_{min} < \beta$, it is proved that an upper bound of $\Theta(W\sqrt{n})$ can actually be held. Thus, in this special case, the transport capacity under the physical model is also $\Theta(W\sqrt{n})$.

In an arbitrary network, if each node were treated equally, and each source could have a destination at a distance of 1 meter, then the transport capacity could be transformed into a throughput capacity. Thus, for the protocol model, the throughput capacity is $\Theta(W/\sqrt{n})$ bits per second. For the physical model, the lower bound of throughput capacity is $\Theta(W/\sqrt{n})$, and the upper bound is $\Theta(W/n^{1/n})$.

8.2.2 Random Networks

The interference models in random networks are similar to those in arbitrary networks. Both protocol model and physical model can be used to analyze the capacity of random networks. Usually, the same transmission power P is assumed in all nodes, so the transmission range r is the same for all nodes. Thus, both models need to be modified as follows.

In the protocol model, a transmission from a node at location X_i can be received by a node at location X_j if

$$|X_i - X_j| \le r$$

and

$$|X_k - X_j| > (1+\Delta)r$$

for every other node X_k with a simultaneous transmission in the same channel. In the physical model, a transmission from a node X_i to a receiving node X_j can be received successfully if

$$\frac{P/|X_i - X_j|^\alpha}{N + \sum_{\substack{k\in\mathcal{T}\\ k\neq 1}}(P/|X_k - X_j|^\alpha)} > \beta. \tag{8.16}$$

In order to avoid edge effects, a surface S^2 on a three-dimensional sphere of area of 1 m^2 is studied.

Deriving the capacity of random networks is much more complicated than for arbitrary networks. In order to avoid sophisticated derivations, here we focus on major analytical steps that gradually lead to the results of upper bound and lower bound of throughput capacity of random networks.

Constructive Lower Bound of Throughput Capacity

In order to construct the lower bound of the throughput capacity, the surface S^2 is divided into Voronoi cells, and then the transmission rate in each cell is analyzed. Two important tasks need to be accomplished when the transmission rate in each cell is studied. Firstly, it is necessary to find a feasible schedule so that each cell can get a share of time slots to transmit packets. Based on this schedule, we know the maximum transmission rate in each cell. Secondly, given a transmission rate on each node, we need to determine the transmission rate that needs to be supported in each cell. Based on these two results, the lower bound on the transmission rate for each node can be derived.

Voronoi cells The surface S^2 can be divided into Voronoi cells, and thus the surface becomes a Voronoi tessellation. Given a set of p points $V_p = a_1, a_2, \ldots, a_p$ in surface S^2, the Voronoi cell $V(a_i)$ is the set of all points that are closer to a_i than to any points in set V_p, i.e., a Voronoi cell is defined as $V(a_i) := x \in S^2 : |x - a_i| = \min_{1 \leq j \leq p} |x - a_j|$. For this Voronoi cell, point a_i is called the Voronoi cell generator.

It has been proved in [96] that, for every $\epsilon > 0$, there is a Voronoi tessellation of S^2 such that each cell contains a disk of radius ϵ and is also contained in a disk of radius 2ϵ. From this result, if $\epsilon = \rho(n)$ is the radius of a disk of area $(100 \log n)/n$ in a Voronoi cell ν_n on S^2, then every Voronoi cell will be contained in a disk of radius $2\rho n$.

Therefore, if the transmission range $r(n)$ is assumed to be $8\rho(n)$, then direct communications can be performed between nodes in the same cell or in adjacent cells. In other words, every node in a cell is within a distance of $r(n)$ from every other node in its own cell and adjacent cells. Since the interference range is usually much larger than the communication range, the interfering neighbors are defined as follows: if there is a point in one cell which is within a distance $(2 + \Delta)r(n)$ of another point in the other cell, then these two cells are called *interfering neighbors*. It is interesting to note that this definition of interference range guarantees no hidden nodes in a multihop network.

Given the above defined interference range, it can be proved that every cell in ν_n has no more than c_1 interfering neighbors, where c_1 depends only on Δ and grows no faster than linearly in $(1 + \Delta)^2$ [96].

Maximum transmission rate in each cell Since each cell has no more than c_1 interfering neighbors, when the protocol model is considered, it is easy to show that a schedule must be available such that each cell in ν_n can get a slot from $(1 + c_1)$ slots to transmit packets without experiencing interference.

For the physical model, the same schedule as that in the protocol model can be applied. However, the required SIR, β, must satisfy a certain constraint. If each transmitter is assumed to choose an identical power level, and Δ is large enough, then it is proved that β must satisfy the following constraint [96]:

$$(1 + \Delta)^2 > \left(2\left(c\beta\left(3 + \frac{1}{\alpha - 1} + \frac{2}{\alpha - 2}\right)\right)^{1/\alpha} - 1\right)^2. \tag{8.17}$$

Thus, for both the protocol model and the physical model, the maximum rate that can be transmit on each cell is $W/(1 + c_1)$.

Needed transmission rate by each cell The needed transmission rate carried by each cell depends on how packets are routed from sources to destinations in various Voronoi cells.

Assume Y_i are randomly selected locations, node X_i and location Y_i are assumed to be independently and identically distributed (i.i.d.) and their sequence $(X_i, Y_i)_{i=1}^n$ is also i.i.d. For a source node X_i, its destination node X_j is the node whose location is closest to Y_i. Thus, there exists a straight-line segment L_i, which is a segment of the great circle (that contains X_i and Y_i) on S^2, connecting the source node X_i and the destination node's closest location Y_i. It can be proved that the sequence of straight-line segments ${L_i}_{i=1}^n$ is also i.i.d. [96].

In [267], based on uniform convergence in the weak law of large numbers, each cell is proved to contain at least one node with high probability. More specifically, every cell in ν_n contains at least one node to relay traffic with probability exceeding $(1 - (50 \log n)/n)$.

Thus, for all cells intersecting a straight-line segment L_i, packets can be always relayed from one cell to another. Thus, a routing scheme can be designed by approximating a routing path to a straight-line segment. In this scheme, the last hop can be done by finding the node that is closest to the destination location Y_i.

Given this routing scheme, the mean number of routes served by each cell can be derived from the mean number of straight-line segments that intersects a cell. In [96], the mean value is proved to be no more than $c_5\sqrt{n \log n}$, where c_5 is a constant. With such a mean value of the number of routes passing through each cell, the actual value can be derived utilizing the i.i.d. property of $(X_i, Y_i)_{i=1}^n$. Based on the weak law of large numbers, the following result is derived in [96]: There is a $\delta'(n) \to 0$ such that

$$\Pr\left(\sup_{V \in \nu_n} (\text{Number of straight-line segments intersecting cell } V) \le c_5\sqrt{n \log n}\right) \ge 1 - \delta'(n).$$

When packets have been relayed to Y_i, they will be forwarded to the final destination that is closest to Y_i. This can be done in one hop with high probability. Thus, the traffic to be handled by a cell is proportional to the number of straight-line segments intersecting a cell.

Since each straight-line segment carries a traffic rate of $\lambda(n)$ bits per second, the following result should hold. There is a $\delta'(n) \to 0$ such that

$$\Pr\left(\sup_{V \in \nu_n} (\text{Traffic needing to be carried by cell } V) \le c_5\lambda(n)\sqrt{n \log n}\right) \ge 1 - \delta'(n).$$

Based on this result, we know that the traffic rate that needs to be supported by each cell is less than $c_5\lambda(n)\sqrt{n \log n}$ with high probability.

Lower Bound of Throughput Capacity

From the results of the previous two steps, we know that

$$c_5\lambda(n)\sqrt{n \log n} \le \frac{W}{1 + c_1}. \tag{8.18}$$

Since c_1 grows no faster than $(1 + \Delta)^2$, we can find a deterministic constant $c > 0$ that is independent of n, Δ, and W, such that

$$\lambda(n) = \frac{cW}{(1 + \Delta)^2\sqrt{n \log n}}. \tag{8.19}$$

Such a result is applicable to both the protocol model and the physical model. However, for the physical model, Δ in (8.19) and the required SIR β must satisfy the constraint in (8.17).

Upper Bound of Throughput Capacity

We first study the number of simultaneous transmissions allowed on a subchannel, which depends on the transmission range. However, the transmission range is also related to the connectivity, as the network will be disconnected when the transmission range is so small that isolated nodes appear. Thus, the tradeoff of a transmission range will lead to a result of the maximum transmission rate in a network, i.e., the upper bound of throughput capacity.

Suppose a node X_i transmits to another node X_j in the mth subchannel, and the transmission range is assumed to be $r(n)$. From the protocol model and triangle inequality, we know that the transmission cannot be successfully received unless no other node within a distance of $\Delta r(n)$ of X_j simultaneously receives another transmission. Thus, disks centered at each receiver with a radius of $\Delta r(n)/2$ must be disjoint. Considering the area of such a disk and the disk of a unit area, we know that the maximum number of simultaneous receivers on the mth subchannel is $4/\pi \Delta^2 r^2(n)$. Since the transmission rate in the mth subchannel is W_m bits per second, so the total transmission rate in the entire network considering all subchannels cannot exceed $4/\pi \Delta^2 r^2(n) W$ bits per second.

Assume that the straight-line segment connecting two i.i.d. points on S^2 has a mean length of $\bar{L}$. Thus, as derived in the previous subsection, the mean length of the routing path for packets from the source X_i to the destination X_j is at least $\bar{L} - o(1)$. Thus, the mean number of hops that a packet needs is at least $(\bar{L} - o(1))/r(n)$. Given the transmission rate of $\lambda(n)$ bits per second for each source, the total transmission rates carried by the entire network need to be at least $((\bar{L} - o(1))n\lambda(n))/r(n)$. Such transmission rates must be satisfied by all nodes using all subchannels, so we obtain

$$\frac{(\bar{L} - o(1))n\lambda(n)}{r(n)} \leq \frac{4W}{\pi \Delta^2 r^2(n)}, \tag{8.20}$$

i.e., $\lambda(n) \leq c_{12} W/\Delta^2 n r(n)$, where c_{12} is a constant not depending on Δ, n, or W.

In [96], it has been proved that the necessary condition for ensuring absence of isolated nodes and network disconnectivity with high probability is that $r(n) > \sqrt{(\log n)/n}$. Thus, we have the following upper bound for random networks with the protocol model. For random networks on S^2 under the protocol model, there exists a deterministic constant $c' < +\infty$ and not depending on Δ, n, or W, such that

$$\lim_{n\to\infty} \Pr\left(\lambda(n) = \frac{c' W}{\Delta^2 \sqrt{n} \log n \text{ is feasible}}\right) = 0.$$

For the physical model, there is the following upper bound for throughput capacity: For random networks on S^2 under the physical model, there exists a deterministic sequence $\epsilon(n) \to 0$ and not depending on N, α, β, or W, such that

$$\lim_{n\to\infty} \Pr\left(\lambda(n) = \sqrt{8}\pi \frac{W}{\bar{L}(\beta^{1/\alpha} - 1)} \frac{1 + \epsilon(n)}{\sqrt{(n)}} \text{ is feasible}\right) = 0,$$

where N is the total number of nodes in the entire network.

Table 8.1 Throughput capacity of wireless networks

Interference model	Arbitrary networks	Random networks	Throughput capacity
Protocol	Lower Bound	$\Theta\left(\frac{W}{\sqrt{n}}\right)$	$\Theta\left(\frac{W}{\sqrt{n \log n}}\right)$
	Upper Bound	$\Theta\left(\frac{W}{\sqrt{n}}\right)$	$\Theta\left(\frac{W}{\sqrt{n \log n}}\right)$
	Throughput Capacity	$\Theta\left(\frac{W}{\sqrt{n}}\right)$	$\Theta\left(\frac{W}{\sqrt{n \log n}}\right)$
Physical	Lower Bound	$\Theta\left(\frac{W}{\sqrt{n}}\right)$	$\Theta\left(\frac{W}{\sqrt{n \log n}}\right)$
	Upper Bound	$\Theta\left(\frac{W}{n^{1/n}}\right)$	$\Theta\left(\frac{W}{\sqrt{n}}\right)$
	Throughput Capacity	between lower and upper bounds	between lower and upper bounds

Summary of Throughput Capacity for Random Networks

The above derivation for throughput capacity is carried out on the surface S^2 of a sphere of unit area. It can be proved that the same capacity bounds are held if a planar disk of unit area is considered.

According to the upper bound and lower bound of the throughput capacity of random networks, we have the following results. For random networks under the protocol model, both the upper bound and lower bound of the throughput capacity is $\Theta(W/\sqrt{n \log n})$. Thus, the throughput capacity under the protocol model is $\Theta(W/\sqrt{n \log n})$. For random networks under the physical model, the lower bound of the throughput capacity is $\Theta(W/\sqrt{n \log n})$, but the upper bound is $\Theta(W/\sqrt{n})$.

8.2.3 Implications

The throughput capacities of arbitrary networks and random networks under different interference models are summarized in Table 8.1. From these results, we can see that the throughput capacity of arbitrary networks is usually of a larger order of magnitude than that of random networks. The reason for such a difference is as follows. In the arbitrary networks, the nodes are optimally placed in a disk and the range of each transmission is also optimally selected; however, in a random network, nodes are randomly located in the network and their transmission ranges are the same.

8.3 Capacity of Mobile Ad Hoc Networks

From analytical results in Section 8.2.2, in a random ad hoc network, we know that the per source–destination throughput goes to zero as $W/\sqrt{n \log n}$. Such a quick drop of throughput is due to interference among simultaneous transmissions, but also due to each source–destination having to go through multiple hops in the same network. Thus, in order to improve throughput, the number of hops between source and destination needs to be reduced.

There are two ways of reducing the number of hops between source and destination. One is to increase the power level to expand the communication range. However, this scheme also increases the interference range, which unfortunately causes throughput drop. The other is to ensure that a source only send packets to another node that is within a bounded number of hops. Obviously, for a fixed network, requiring a source to select a destination within a bounded number of hops is not a right answer, since a source is supposed to choose any node as a destination. However, it is possible to reduce the number of hops from source to destination by assuming that packets are not delivered to their destination until the destination is close enough. Such a mechanism depends on mobility of nodes. Thus, for a fixed wireless network, there is no effective solution to reduce the number of hops between source and destination. Even for a mobile wireless network, we need to find answers to the following two questions.

- Given a mobility model, what will be the minimum number of hops that can achieve the highest throughput?
- How should a scheduling scheme be designed so that the required number of hops can be achieved?

In [251], these two questions have been studied assuming a random mobility for all nodes.

Models

When studying the throughput improvement by utilizing mobility, several models need to be specified.

First of all, the network consists of n nodes which are located in a disk of unit area. The location of the ith node is $X_i(t)$ at time t, and $\{X_i(t)\}$ is assumed to be a stationary and ergodic random process with a uniform distribution on the disk. In addition, different nodes move independently as i.i.d. processes. Thus, given two nodes i and j, $\{X_i(t)\}$ and $\{X_j(t)\}$ are i.i.d.

The traffic pattern of the network is assumed as follows. Each node is a source node for one session and also a destination node for another session. The source node i always has data to send to its destination $d(i)$. Moreover, the source–destination association does not change with time even if nodes are mobile.

A physical model is assumed in this analysis. Given that the channel gain from node i to node j is γ_{ij}, the transmit power at node i is $P_i(t)$ at time t, then the received power at node j should be $P_i(t)\gamma_{ij}$. Given the SIR requirement β, node j can successfully receive packets from node i if

$$\frac{P_i(t)\gamma_{ij}(t)}{N_0 + (1/L)\sum_{ki/} P_k(t)\gamma_{kj}(t)} > \beta, \tag{8.21}$$

where N_0 is the background noise power and L is the processing gain of the system. For a narrow band system, $L = 1$. The channel gain is related to nodes' locations as

$$\gamma_{ij}(t) = \frac{1}{|X_i(t) - X_j(t)|^{\alpha}},$$

where α is a parameter greater than 2.

Number of Hops Versus Throughput Improvement

We know that the minimum number of hops in a network is one. For a network with only one hop between source and destination, this means that no nodes in the network will act as a relaying node. Thus, in the following analysis, we consider two scenarios: one is about mobile networks with relaying nodes, and the other is about no relaying nodes.

8.3.1 Mobile Networks without Relaying Nodes

This scenario analyzes the throughput capacity of a mobile network in which only one hop is allowed before source and destination. Thus, when a source node sends to a destination that is more than one hop away, it has to buffer its packets until the destination is within the communication range. Intuitively, we can see problems in this scheme. For example, the delay of buffering packets may be so large that the throughput drops quickly. The following asymptotic throughput result [251] provides a detailed insight into this scenario.

In a mobile ad hoc network with n nodes, each node has a transmission rate of R, and none of them is permitted to relay packets. For such a network, the throughput of each source–destination pair must satisfy that, for any constant c larger than $[2^{\alpha}(1+2/\pi)\pi^{-\alpha/2((\beta+L)/\beta)}]^{1/(1+\alpha/2)}$,

$$\Pr\{\lambda(n) = cn^{-1/(1+\alpha/2)}R \text{ is feasible }\} = 0 \tag{8.22}$$

for sufficiently large n.

Such a result implies that the throughput for each source–destination drops to zero at least as fast as $n^{-1/(1+\alpha/2)}$. It can be proved by contradiction [251].

Suppose throughput $\lambda(n) = cn^{-1/(1+\alpha/2)}R$ is feasible. Considering a time period T, $\Lambda_T(i)$ is the set of time instants at which node i is scheduled to make a successful transmission to its destination $d(i)$. Thus, according to the definition of feasible throughput,

$$\liminf\nolimits_{T\to\infty} \frac{\Lambda_T(i)}{T} \geq cn^{-1/(1+\alpha/2)}. \tag{8.23}$$

Considering the random process $D_i(t) = |X_i(t) - X_{d(i)}(t)|$ for $t = 1, 2, \ldots$, it is stationary and ergodic. Thus, (8.23) implies that almost surely the following inequality holds:

$$\liminf\nolimits_{T\to\infty} \sum_{t\in\Lambda_T(i)} D_i(t) \geq \int_0^{F^{-1}(cn^{-(1/(1+\alpha/2))})} zdF(z),$$

where F is the cumulative distribution function (CDF) of the random variable $D_i(t)$. Moreover, this inequality holds for all n nodes, so we obtain

$$\liminf\nolimits_{T\to\infty} \sum_{i=1}^{n} \sum_{t\in\Lambda_T(i)} D_i(t) \geq n \int_0^{F^{-1}(cn^{-(1/(1+\alpha/2))})} zdF(z),$$

which is equivalent to

$$\liminf\nolimits_{T\to\infty} \sum_{t=1}^{T} \sum_{i\in\S(t)} D_i(t) \geq n \int_0^{F^{-1}(cn^{-(1/(1+\alpha/2))})} zdF(z),$$

where $S(t)$ is the set of source nodes that are scheduled to make a successful transmission at time t. This further implies that there must exist a time instant τ such that

$$\sum_{i\in\S(\tau)} D_i(\tau) \geq n \int_0^{F^{-1}(cn^{-(1/(1+\alpha/2))})} zdF(z). \tag{8.24}$$

In the unit disk, the probability that node i is within node $d(i)$'s neighbor of radius z is πz^2. This means that, for destination's location $X_{d(i)}(t) = x$, if $z^{1/\alpha} < |\pi^{1/2} - x|$, then

$$\Pr\{D_i(t) < z|X_{d(i)}(t) = x\} = \pi z^{2/\alpha}.$$

From this, we can derive that $\lim_{z\to 0} F(z)/z^{2/\alpha} = \pi$. Putting this result back into (8.24), we obtain

$$\lim_{n\to\infty} n \int_0^{F^{-1}(cn^{-(1/(1+\alpha/2))})} zdF(z) = \frac{c^{1+\alpha/2}}{\pi^\alpha(1+2/\alpha)}. \tag{8.25}$$

Thus, if

$$c > \left[2^\alpha\left(1+\frac{2}{\pi}\right)\pi^{-\alpha/2}\frac{\beta+L}{\beta}\right]^{1/(1+\alpha/2)},$$

then

$$\sum_{i\in\S(\tau)} D_i(\tau) > B,$$

where $B = 2^\alpha \pi^{-\alpha/2((\beta+L)/\beta)}$. However, from the physical interference model, it can be easily proved that $\sum_{i\in\S(\tau)} D_i(\tau) \leq B$. These two contradictory results prove that throughput $\lambda(n) = cn^{-1/(1+\alpha/2)}R$ is not feasible.

8.3.2 Mobile Networks with Relaying Nodes

It has been proved in the previous section that only using single-hop transmission between source and destination results in a very low throughput. Thus, it is necessary to have at least one relaying node between source and destination. For such a network with relaying nodes, the minimum number of hops that can be achieved is two, i.e., a source node sends packets to a destination directly if it is within each other's communication range; otherwise, the source node just sends packets to a relaying node through which packets are delivered to the destination. Now we need to find out if two-hop transmission between source and destination is good enough for improving the throughput capacity.

Intuitively, if a node simply sends all packets to the same relaying node through which packets are delivered to the destination, then we will definitely be confronted with the same issue as in a mobile network without relaying nodes. More specifically, either from the source node to the relaying node or from the relaying node to the destination node, the packets may have to wait for a long time before the packets can be delivered, which is the same that in Section 8.3.1.

However, given the same source–destination pair, different nodes can be selected to relay packets between the source and the destination. Since more nodes help the source to deliver packets to the destination, it can be expected that a higher throughput can be achieved. The reason can be explained as follows. Owing to nodes location processes $\{X_i(t)\}$, all nodes in the unit disk have the same probability of being scheduled to receive packets from the same source node. Similarly, all nodes have the same probability of being scheduled to send packets to the same destination node. Thus, for packets sent from the same source node, it is sufficient to be relayed once to the destination node; otherwise, the number of hops will be larger than required. Since only two hops are needed to deliver packets for each source–destination pair, the achievable throughput of the network is $\Theta(n)$, i.e., the throughput per source–destination pair is $\Theta(1)$. Next we derive such a result via detailed analysis.

Two-phase scheduling scheme

In order to analyze the throughput improvement in a network with two-hop source–destination transmission, we first describe the detailed scheduling scheme in which only two hops are needed for each source–destination pair.

Assume that the sender density is $\theta \in (0, 1)$, so the number of senders in each time slot is $n_s = n\theta$ and the remaining nodes n_r are potential receivers. Each sender node transmits packets to its nearest neighbor among all nodes in the set of potential receivers using unit transmit power.

Among the n_s sender–receiver pairs, there are N_t sender–receiver pairs whose interference generated by other senders is sufficiently small that transmission is successful. N_t is a random process and it can be proved that the expected number of N_t is $\Theta(n)$, i.e.,

$$\lim_{n\to\infty} \frac{\mathrm{E}[N_t]}{n} = \phi > 0, \tag{8.26}$$

and the probability that nodes i and j are scheduled to act as a send-receiver pair is $\Theta(1/n)$.

The above policy is then applied to scheduling packets for two-phase transmission for all source–destination pairs. The more specific operation procedures are explained below.

In the first phase, n_s nodes are selected as sources. For each source, receivers are identified. If a receiver is the destination, the packets are sent directly from the source to the destination with one-hop transmission. Otherwise, the receiver acts as a relaying node, and thus packets are sent to this receiver and will be relayed to the destination in the second phase.

In the second phase, again n_R nodes are selected as senders. Note that senders can be relaying nodes or sources. For each sender, if a receiver is unidentified, only packets whose final destination is this receiver can be transmitted. For other packets, another receiver should be considered.

Throughput

The phases are executed iteratively. According to the procedure, we know that the two-phase scheduling scheme can be viewed as a queuing system as shown in Figure 8.1. The throughput of each source–destination pair can be derived based on this queuing system.

As shown in the queuing system, a packet to the final destination can have a direct route and $n - 2$ two-hop routes via relaying nodes. Since the locations of the nodes are i.i.d., stationary, and ergodic, the long-term throughput between any two nodes is equal to the probability that these two nodes are selected as a feasible sender–receiver pair, which is $\Theta(1/n)$. Thus, the departure rate at the source node is $\Theta(1/n)$. Consequently, the direct route achieves a throughput of $\Theta(1/n)$. Moreover, for the $n - 2$ two-hop routes, each has an arrival rate of $\Theta(1/n)$ to the queuing system whose server is the relaying node with a service

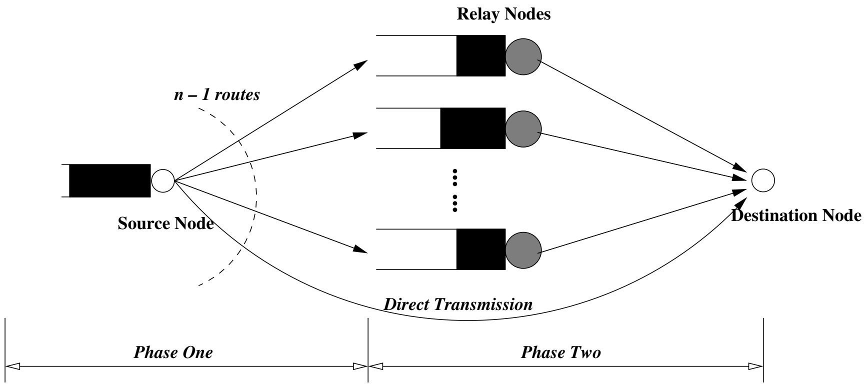

Figure 8.1 The queuing system for the two-phase scheduling scheme

rate of $\Theta(1)$. Thus, the departure rate at each relay node is $\Theta(1/n)$. Looking at the destination node, there are $n - 1$ incoming packets flows each with a rate of $\Theta(1/n)$. Thus, the overall throughput of the $n - 1$ flows is $\Theta(1)$. This proves that the throughput per source–destination pair is $\Theta(1)$.

Discussion

The two critical steps that help to improve the throughput of a mobile ad hoc network include: (1) reduce the number of hops by a two-phase transmission scheme; (2) packets to the same destination are relayed by different nodes in the network. The second step is actually a type of multi-user diversity applied in the scheduling scheme to improve network capacity. If some packets are relayed by nodes that take a long time to reach the destination, we can also expect that other packets will be relayed by nodes that can quickly move close to the destination. Thus, the diversity makes it possible that the throughput capacity scales faster than the delay does. However, the effectiveness of multi-user diversity depends on the mobility model. Suppose that the nodes do not move according to a stationary and ergodic random process, then the throughput of $\Theta(1)$ may not be achievable.

Although multi-user diversity helps to improve the throughput capacity, it may not be effective enough to keep the delay low. In order to further reduce the delay, other scheduling scheme rather than a two-phase transmission scheme must be applied [85]. It can be expected that the throughput will be compromised if we want to achieve a lower delay.

8.4 Capacity of Ad Hoc Networks with Infrastructure Support

Based on the derived results in previous sections, the capacity of a multihop network can be improved by having relaying nodes or clustering nodes in groups so that wireless communications are bounded within a small number of hops.

One practical approach of doing so is to add infrastructure into the ad hoc networks. The infrastructure nodes are connected via wires or wireless links with very large capacity. Thus, there is no capacity bound within the infrastructure itself.

Following the work done in [96], several researchers [152, 175, 287] have derived the capacity bound and the scaling law of ad hoc networks with infrastructure support.

8.4.1 Regularly Placed Infrastructure Nodes and Randomly Located Ad Hoc Nodes

In this scenario, n nodes are placed in random (independent and uniform) locations in a disk of unit area (1 m^2). The m infrastructure nodes are regularly placed into the disk as follows. The disk is divided into a hexagonal tessellation, in which one infrastructure node is placed at the center of each hexagonal cell. The infrastructure nodes are connected by wires and the wired network does not have any bandwidth constraint. Moreover, no power constraint is put on the infrastructure nodes. It should be noted that the infrastructure nodes are deployed for relaying traffic for ad hoc nodes. In other words, they are neither sources nor destinations for any packets in the network.

To analyze the capacity of this kind of network, the protocol model is used to check whether a transmission is successful or not. Also, it is assumed that different subchannels are used for the communication links for ad hoc nodes, uplink transmission from ad hoc nodes to infrastructure nodes, and downlink transmission from infrastructure nodes to ad hoc nodes. Given an ad hoc node with W bits/sec transmission rate, its intra-cell, uplink, and downlink transmission rates are W_1, W_2, W_3, respectively, and $\sum_{i=1}^{3} W_i = W$. In the analysis, it is also assumed that $W_2 = W_3$.

With the presence of infrastructure nodes, the routing scheme between ad hoc nodes becomes different from the scenario studied in [96], since it takes advantage of these infrastructure nodes to improve capacity. Thus, specifying a routing strategy is a necessary step for deriving the capacity of the hybrid network.

Routing Strategy

Two routing strategies are considered in the capacity analysis.

In the first routing protocol, given a source–destination pair, if the destination is located in the same cell as the source, then only ad hoc networking is needed from end to end. However, if the destination is in a different cell, then the source sends the data to the infrastructure node of its cell and then relies on the infrastructure network to forward packets all the way to the destination cell, and finally data arrive at the destination node.

This routing strategy can be generalized by allowing ad hoc networking across multiple cells. For example, given a source–destination pair, if the source and the destination are located within k-nearest neighboring cells, then only ad hoc networking is needed. This is called the k-nearest-cell routing strategy.

The second routing strategy is a probabilistic scheme. For each node, its transmission in infrastructure mode has a probability of p, and the transmission in ad hoc mode has a probability of $1 - p$.

Results

The throughput capacity of the hybrid network varies with the routing strategy and also the ratio of infrastructure nodes over ad hoc nodes.

k-nearest-cell routing

- If $m = o(\sqrt{n})$, the aggregate throughput capacity is $\Theta(\sqrt{(n/\log(n/m^2))}W_1 + mW_2)$. Since $W_2 = W_3$, $W_1 = W - 2W_2$, the aggregate capacity is maximized when $W_2/W \to 0$, and the maximum capacity is $\Theta(\sqrt{(n/\log(n/m^2))}W)$. In other words, the per-node throughput capacity is $\Theta(\sqrt{(1/n\ \log(n/m^2))}W)$.

- If $m = \Omega(\sqrt{n})$, the aggregate throughput capacity is $O(\sqrt{n}W_1) + \Theta(mW_2)$. The maximum capacity is achieved when $W_1/W \to 0$, where the capacity is $\Theta(mW)$. Thus, the per-node capacity becomes $\Theta((m/n)W)$. Suppose $m = n^\alpha$ where $1/2 \leq \alpha \leq 1$, then the per-node capacity is maximized when $\alpha = 1$, i.e., $m = n$, and the capacity becomes $\Theta(W)$.

Probabilistic routing The aggregate throughput capacity of the hybrid network is $\Theta(\sqrt{(np/\log np)}W_1 + mW_2)$, where p is the probability that a node chooses ad hoc mode. As $n \to \infty$, the maximum capacity can be achieved when $p \to 1$, i.e., the capacity becomes $\Theta(\sqrt{(n/\log n)}W_1 + mW_2)$. This indicates that, when the number of ad hoc nodes is large and almost of them choose ad hoc mode, the maximum throughput can be achieved. The reason is that the infrastructure node can be fully utilized as long as there is node communicating with the infrastructure node; adding more nodes in ad hoc mode does not really improve throughput.

As in the case of *k-nearest-cell routing*, the maximum throughput capacity of probabilistic routing is also related to scheduling in the number of ad hoc nodes and infrastructure nodes as well as to the bandwidth allocation in W_1 and W_2.

- If $m = \phi(\sqrt{n/\log n})$, when $W_2/W \to 0$, the maximum aggregate throughput capacity becomes $\Theta((n/\log n)W)$. Thus, the per-node throughput capacity is $\Theta((1/\sqrt{n\ \log n})W)$. Such a result is similar to that of a pure ad hoc network. In fact, $W_2/W \to 0$ implies that almost no communication with infrastructure nodes occurs, which is actually the case of pure ad hoc networking.

- If $m = \omega(\sqrt{n/\log n})$, when $W_1/W \to 0$, the aggregate throughput capacity becomes $\Theta(mW)$. Thus, the per-node throughput capacity is $\Theta((m/n)W)$.

Implications and Discussion

The results derived in the previous section have the following implications.

When a probabilistic routing is selected, if the number of infrastructure nodes scales slower than $\sqrt{n/\log n}$, then the per-node throughput capacity is only $\Theta((1/\sqrt{n\ \log n})W)$. Thus, compared to a pure ad hoc network, the hybrid network has the same capacity as a pure ad hoc network. If the number of infrastructure nodes can scale faster than $\sqrt{n/\log n}$, the per-node throughput capacity, $\Theta(m/nW)$, becomes $\omega((1/\sqrt{n\ \log n})W)$. This implies that the throughput capacity can be higher than the case of pure ad hoc networks, but no significant improvement of throughput capacity can be achieved.

When a k-nearest-cell routing is selected, if the number of infrastructure nodes scales slower than $\sqrt{n}$, where n is the number of ad hoc nodes, then the per-node throughput capacity can only be $\Theta(\sqrt{(1/n \log(n/m^2))}W)$. However, if the number of infrastructure nodes scales not slower than $\sqrt{n}$, then the throughput capacity will be as high as $\Theta(W)$. This result implies that if the number of infrastructure nodes is large enough (i.e., in the same order of magnitude as $\sqrt{n}$), then the per-node throughput capacity can be in the same order of magnitude as the case where all nodes can transmit using a rate of W.

Therefore, in order to really improve the throughput capacity of hybrid networks, two critical factors must be considered. First, the number of infrastructure nodes is large enough. Second, a proper scheduling is needed. It can be seen that neither k-nearest-cell routing nor probabilistic routing is an optimal routing scheme, so the results proposed in [175] do not necessarily give the most appropriate capacity bound.

Moreover, there are some shortcomings in the analytical method. Intuitively, if only the capacity of ad hoc nodes is the concern, then it is optimal for ad hoc nodes to enter and exit the infrastructure once and it is also optimal for them to use the nearest infrastructure node to reach the infrastructure. However, in the analysis, the routing scheme tries to produce some ad hoc networking scenarios. In other words, the constructive scheme has created a nonoptimal result.

8.4.2 Randomly Placed Infrastructure Nodes and Ad Hoc Nodes

In [152], a hybrid network in which both ad hoc nodes and infrastructure nodes are randomly placed is used. As in the case of [175], it is natural to assume that ad hoc nodes can be placed in a random location. However, the assumption of randomly located infrastructure nodes mostly matches the scenario of using wireless LANs as the infrastructure, since the serving area and the locations of the access points are not well determined. For a network architecture similar to cellular networks, this assumption is not necessarily applicable.

The capacity of the hybrid network with randomly place infrastructure nodes and ad hoc node is different under two different conditions: *strong connectivity* and *weak connectivity*. Strong connectivity indicates that ad hoc nodes form a connected topology graph with high probability. Thus, ad hoc nodes can have a stand-alone network for any pair of ad hoc nodes to communicate with each other, with the support of infrastructure. Weak connectivity does not have such a constraint, and ad hoc nodes can have partitions, but they are still connected via infrastructure nodes. Thus, ad hoc nodes stay connected in the overall topology graph, even though they may be partitioned.

Before exploring the detailed capacity result under these two conditions, the models are explained first.

In the hybrid network, both ad hoc and infrastructure nodes are uniformly distributed on a disk of area $A_R = \pi R^2$. The number of ad hoc nodes is N, and that of infrastructure nodes is M. We also assume that the number of ad hoc nodes per infrastructure node is bounded, i.e., $\lim_{N\to\infty}(N/K) = \alpha$, where $\alpha \in (0, \infty)$. For each ad hoc node, its traffic rate to another ad hoc node is $\lambda(N, K)$ bits per second. The total bandwidth is assumed to be W bits per second. The protocol interference model is used, and the guard distance is equal to Δ. Thus, node j can successfully receive a transmission from node i, if and only if $|X_i - X_j| \leq r_T$

and other transmissions around j must be at a distance larger than $(1+\Delta)r_T$ in the same time slot using the same channel.

Throughput Capacity under Strong Connectivity Condition

From results in Section 8.2, we know that the disks of radius $\Delta r_T/2$ centered at ad hoc receivers are disjoint. Thus, the number of simultaneous transmissions without interference is the number of disks of radius $\Delta r_T/2$ that can be packed into the disk of area A_R. Again, from Section 8.2, considering edge effects, the number of simultaneous transmissions is smaller than $16A_R/\pi\Delta^2 r_T^2$. Assuming that the average number of hops within ad hoc networks is $\bar{h}(N, K)$, then we obtain the following inequality:

$$N\lambda(N, K)\bar{h}(N, K) \leq \frac{16A_R W}{\pi\Delta^2 r_T^2}. \tag{8.27}$$

From [95], we know that, in order to have a connected graph, r_T must satisfy $r_T \geq \sqrt{(\log N)/N}$. Thus, (8.27) becomes

$$\lambda(N, K) \leq \frac{16A_R W}{\Delta^2 \log N}. \tag{8.28}$$

Moreover, with the help of Voronoi tessellation, it can be derived the following inequality [152]:

$$\lambda(N, K) \geq \frac{W}{C_1[\log N + \log(1+1/\alpha)]}. \tag{8.29}$$

Combining (8.28) and (8.29), we obtain that the throughput capacity of a random hybrid network is $\Theta(W/\log N)$. Compared to a pure random ad hoc network, this capacity is significantly improved. This result holds as long as the number of ad hoc nodes per infrastructure node is bounded and strong connectivity is ensured.

Throughput Capacity under Weak Connectivity Condition

The strong connectivity does not fully utilize the infrastructure network. In fact, not all ad hoc nodes need to be connected in the topology graph when infrastructure nodes are available. In other words, a weak connectivity can be formed via infrastructure nodes. Under the weak connectivity condition, ad hoc nodes can be partitioned but are all connected in the overall topology graph.

With weak connectivity, the radius r_T is different from the case with strong connectivity. As $N \to \infty$, the radius r_T can be smaller when weak connectivity is concerned. As derived in [152], r_T must satisfy $r_T \geq c_4/\sqrt{\pi N}$, where c_4 is any positive finite number. Combining this result with (8.27), we have

$$\lambda(N, K) < \frac{16A_R W}{c_4^2\Delta^2}. \tag{8.30}$$

Thus, we cannot find a constant $c > 0$ such that

$$\lim_{N\to\infty} \Pr(\lambda(N, K) = cW \text{ is feasible}) = 1.$$

In other words, the per-node throughput capacity of $\Theta(W)$ cannot be achieved with a probability of one.

However, in order to find the achievable upper bound of the throughput capacity, the following steps can be applied. First of all, we assume $r_T \geq \sqrt{A_\epsilon(N)/\pi} = \sqrt{g(N)/\pi N}$. Thus, from (8.27), we have

$$\lambda(N, K) \leq \frac{16 A_R W}{\Delta^2 g(N)}. \tag{8.31}$$

Secondly, in the disk of area A_R, we form Voronoi tessellations such that $\pi\epsilon^2 = A_R g(N)/N$ and $r_T = 6\epsilon$. Thus, each Voronoi cell is confined between two disks of radii ϵ and 3ϵ, respectively. It can be proved that the number of ad hoc nodes is $\Theta(g(N))$ as $N \to \infty$ [152]. Thus, the upper bound shown in (8.31) is achievable.

Furthermore, since $\lim_{N\to\infty} g(N) = \infty$, the achieved throughput capacity in (8.31) goes to zero.

Discussions

Since a different network model is followed in this section, the per-node throughput capacity is different from that derived in Section 8.4.1, which is reasonable. However, in this section it has been proved that under the weak connectivity condition, the throughput capacity of $\Theta(W)$ cannot be achieved. In Section 8.4.1, we have shown that $\Theta(W)$ can be achieved when the number of infrastructure nodes for up-/down-link access and the number of ad hoc nodes are equal. However, these two results do not contradict with each other. The reason is that the two results are derived based on two different network models and, more importantly, are based on different topology requirements. The weak connectivity condition does not cover the scenario where the number of infrastructure nodes is equal to the number of ad hoc nodes. In fact, the latter case not only has better connectivity but also needs smaller transmission range because of the simultaneous growth of ad hoc nodes and infrastructure nodes. Consequently, this case can be expected to achieve higher throughput as the number of nodes increases.

It should be noted that the number of infrastructure nodes scales increases linearly with the number of ad hoc nodes. Thus, no other scaling regimes are considered in [152].

8.4.3 Arbitrarily Placed Infrastructure Nodes and Randomly Located Ad Hoc Nodes

The reason for considering arbitrary location of infrastructure nodes is to allow each infrastructure node to adjust its transmission range for its transmission to ad hoc nodes. Thus, the number of simultaneous transmissions between ad hoc nodes and infrastructure nodes can be increased, which can potentially improve the throughput of the hybrid network.

Before explaining the detailed analytical results about throughput capacity, we first describe what models are adopted.

Model

In a hybrid network, there are n ad hoc nodes and m infrastructure nodes. The ad hoc nodes are uniformly distributed in locations $X_1, X_2, \ldots, X_n$ within a disk of unit area. Infrastructure nodes are arbitrarily placed, but they are connected either via wires or wireless links with infinite capacity. Communications between two ad hoc nodes or between an ad hoc node and an infrastructure node have a capacity of W bits per second. Ad hoc nodes cannot work in both receiving and transmitting modes, while infrastructure nodes can do so.

In the network, only ad hoc nodes can be a source of traffic, and infrastructure nodes only relay traffic. In addition, an ad hoc node selects its random location in the unit disk and another ad hoc node closest to this location is the destination.

In the analysis, only the protocol model is considered as the interference model.

Upper Bounds

From analysis of pure ad hoc networks, it is known that the number of simultaneous transmissions in the network is upper bounded by $c_1/\Delta^2 r^2$, where c_1 is independent of Δ and the number of nodes in the network. Thus, the transmission range r is desired to be as small as possible. However, to avoid network partition, the transmission range needs to be lower-bounded. Using the similar results derived in [95], the connectivity range in the hybrid network, denoted by $r(n, m)$, satisfies

$$r(n,m) = \begin{cases} \Omega\left(\sqrt{\frac{\log n}{n}}\right), & \text{if } m = o\left(\sqrt{\frac{n}{\log n}}\right), \\ \Omega\left(\sqrt{\frac{1}{m}}\right), & \text{if } m = \Omega\left(\sqrt{\frac{n}{\log n}}\right). \end{cases} \tag{8.32}$$

Considering this connectivity range and simultaneous transmissions among the $m + n$ nodes, the per-node throughput $\lambda(n, m)$ is upper bounded as [287]

$$\lambda(n,m) \le c_2 \frac{Wm}{n} + c_3 \frac{W}{\Delta^2 n r(n,m)}, \tag{8.33}$$

where c_2, c_3 are two positive constants. Combining this result with (8.33), we obtain the per-user throughput capacity as

$$\lambda(n,m) = \begin{cases} O\left(\frac{Wm}{n}\right), & \text{if } m = \Omega\left(\sqrt{\frac{n}{\log n}}\right), \\ O\left(\frac{W}{\sqrt{n \log n}}\right), & \text{if } m = O\left(\sqrt{\frac{n}{\log n}}\right). \end{cases} \tag{8.34}$$

It has been proved that, for any m, the upper bound for the per-node throughput capacity is [287]

$$\lambda(n.m) = O\left(\frac{W}{\log n}\right). \tag{8.35}$$

Considering this upper bound and the upper bounds in (8.34), we can get the upper bounds for the per-node throughput capacity in three regimes defined by n and m

- regime (i): $m = O(\sqrt{n/\log n})$;
- regime (ii): $m = \omega(\sqrt{n/\log n})$, but $m = O(n/\log n)$;
- regime (iii): $m = \omega(n/\log n)$.

In each regime, the upper bound is determined by choosing the tightest bound among all derived bounds. Thus, the upper bounds are given as

$$\lambda(n, m) = \begin{cases} O\left(\dfrac{W}{\sqrt{n \log n}}\right) & \text{in regime (i),} \\ O\left(\dfrac{Wm}{n}\right) & \text{in regime (ii),} \\ O\left(\dfrac{W}{\log n}\right) & \text{in regime (iii).} \end{cases} \tag{8.36}$$

Lower Bounds and Per-Node Throughput Capacity

Derivations of lower bounds must consider certain schemes of placing infrastructure nodes, routing packets, and scheduling transmissions.

In regime (i), it is easy to derive that the upper bound is also a lower bound, since a pure ad hoc network is able to achieve a throughput of $\Theta(W/\sqrt{n \log n})$. Thus, in regime (i), the per-node throughput capacity is $\Theta(W/\sqrt{n \log n})$.

In regime (ii), via careful placement of infrastructure nodes based on Voronoi tessellation and finding a scheduling scheme to ensure that each node only communicates with its closest infrastructure nodes, it can be proved that $\lambda(n, m) = \Omega(Wm/n)$ [287]. Combining this result with the upper bound in regime (ii), we know that the per-node throughput capacity is $\Theta(Wm/n)$.

From (8.35), the highest throughput capacity is $\Theta(W/\log n)$ for any number of infrastructure nodes. Moreover, in regime (ii), if $m = \Theta(n/\log n)$, i.e., when the maximum number of infrastructure nodes is used, then the capacity is $\Theta(W/\log n)$. Thus, $\Theta(W/\log n)$ is an achievable capacity in regime (iii). Considering the upper bound in the same regime, we know that the per-node throughput capacity is really $\Theta(W/\log n)$.

Combining results in three regimes, a hybrid network with infrastructure nodes arbitrarily placed has the following per-node throughput capacities:

$$\lambda(n, m) = \begin{cases} \Theta\left(\dfrac{W}{\sqrt{n \log n}}\right) & \text{in regime (i),} \\ \Theta\left(\dfrac{Wm}{n}\right) & \text{in regime (ii),} \\ \Theta\left(\dfrac{W}{\log n}\right) & \text{in regime (iii).} \end{cases} \tag{8.37}$$

Different capacities in different regimes clearly indicate that the number of infrastructure nodes plays an important role. If the number of infrastructure nodes is not big enough, i.e., in regime (i), the capacity result of the hybrid network is the same as that of a pure ad hoc network. In other words, infrastructure nodes do not help improve the capacity of ad hoc networks. If the number of infrastructure nodes is large enough, e.g., in regime (ii), then the capacity of the hybrid network increases as the number of infrastructure nodes. This means that the infrastructure nodes can significantly improve the per-node throughput of ad hoc networks in this scenario. However, if the number of infrastructure nodes is too large, as shown in regime (iii), then the per-node throughput capacity does not really increase even if the number of infrastructure nodes keeps growing. Even though the per-node throughput capacity in this scenario is still higher than that in regime (i), too large a number of infrastructure nodes means waste of investment. Consequently, it is critical to choose an appropriate number of infrastructure nodes in order to trade off the improvement of throughput for ad hoc nodes and the investment costs for the hybrid network.

8.5 Capacity and Delay Tradeoff

In a wireless multihop network, the network capacity, usually represented by throughput, is not the only concern for users. In fact, QoS is equally important. Usually QoS metrics include delay, delay jitter, and packet loss ratio. In all the theoretical analysis, it is assumed that, as long as the constraint defined in the interference model is satisfied, a packet can be sent and received successfully without any packet error. Thus, packet loss has not been taken into account as a key factor when capacity analysis is carried out for wireless networks. Delay jitter has not been considered either in any existing research work. However, delay has already been considered as a key performance metric when the capacity of a wireless multihop network is analyzed.

Throughput of a random network with both static and fixed nodes is analyzed in [28], where a routing algorithm is proposed to optimize throughput. Based on such a framework, delay is studied. In [201], throughput and delay tradeoff are analyzed using the i.i.d. mobility model. In [85], the throughput–delay tradeoff has been analyzed for both static networks and mobile networks. For mobile networks, the random walk (RW) model is assumed in the analysis. Some results of mobile networks derived in [85] are similar to the results in [178] where a Brownian motion model is assumed for node mobility.

In this section, we focus our discussions on the analytical methodology in [85], since it is generic for static networks and mobile networks.

In order to increase the network capacity, two rules can be followed: reducing the number of hops that a packet shall travel and the interference range of a transmission. However, scheduling schemes following these rules usually improve throughput but increase delay. Thus, given a scheduling scheme, it is necessary to investigate whether or not it causes unacceptable delay. It is also interesting to perform a throughput–delay tradeoff when a scheduling scheme is designed for wireless multihop networks.

8.5.1 Analytical Model and Definitions

n nodes are assumed to be uniformly distributed into a unit torus. They are randomly split into $n/2$ source–destination pairs. Time is slotted into unit length for packetized transmission. The unit torus is divided into n square cells, i.e., the unit torus becomes a $\sqrt{n} \times \sqrt{n}$ discrete torus.

In a static network, nodes do not move. In a mobile network, nodes move according to a random walk model. Initially, each node is independently and uniformly distributed into one of the n cells. Then the node walks randomly on the two-dimensional $\sqrt{n} \times \sqrt{n}$ discrete torus. That means that, if a node is cell (i, j), its next location will be in one of the four neighbor cells $(i-1, j)$, $(i, j-1)$, $(i+1, j)$, $(i, j+1)$ with equal probability. Thus, the given random walk model assumes that each node moves $1/\sqrt{n}$ in unit time, i.e., moving velocity scales as $1/\sqrt{n}$. Moreover, all nodes move independently according to a uniform stationary and ergodic distribution.

The random walk is preferred due to its Markovian nature, since the present position of the node determines the distribution of its future position.

The protocol model is applied to determine whether a transmission is successful. When a node can send packets successfully, it uses a transmission rate of W bits per second.

In a time-slotted system, usually packets being transmitted in a time slot need to be scheduled, for one of several reasons. Firstly, a time slot may not be able to accommodate the transmission of all nodes; which node should be selected to send how many packets need to be scheduled. Secondly, a time slot length may not be exactly divisible by the packet length, and thus whether a packet can be sent in a time slot must be checked before it is scheduled in a time slot. All these issues complicate the analysis of capacity and delay in a multihop wireless network.

In order to simplify the problem, a fluid mode is adopted for packet transmission in a time slot. In this model, as long as time remains in a time slot, a fraction of a packet can be sent in the time slot. Thus, a packet may be sent in two different time slots. Similarly, a time slot may be used to send multiple packets.

When the packet size is constant, then the fluid model is not applicable. A different approach must be used to analyze delay and capacity scaling [86].

Given a scheduling scheme $\prod_n$ in a network with n nodes, its throughput $T_\Pi(n)$ can be defined as follows.

Given a source–destination pair i, $1 \leq i \leq n/2$, the number of bits transferred in t time slots is denoted by $B_{\Pi_n}(i, t)$. Given a specific variable $C(n)$, a random variable $A_\Pi(n)$ is defined as the event that the average bit rate for the source–destination pair i is not less than $C(n)$, i.e.,

$$A_\Pi(n) = \left\{ \min_{1\leq i\leq n/2} \lim_{t\to\infty} \inf \frac{1}{t} B_{\Pi_n}(i, t) \geq C(n) \right\}.$$

If $\Pr(A_\Pi(n)) \to 1$ when $n \to \infty$, then the scheme $\Pi = \{\Pi_n\}$ is said to achieve a throughput of $C(n)$, i.e., $T_\Pi(n) = C(n)$.

The delay for the same scheduling scheme is defined in the following way. For the source–destination pair i under the scheduling scheme Π_n, the delay of packet j is denoted as $D^i_{\Pi_n}(j)$. Thus, for the same source–destination pair, the average delay per packet is $(\bar{D})^i_{\Pi_n} = \lim_{k\to\infty} \sup(1/k) \sum_{j=1}^{k} D^i_{\Pi_n}(j)$. Considering all source–destination pairs, the average delay is

$$(\bar{D})_\Pi = \frac{2}{n} \sum_{i=1}^{n/2} (\bar{D})^i_{\Pi_n}.$$

Consequently, the delay for the scheme Π, denoted by $D_\Pi(n)$ is defined as the expectation of the average delay over all source–destination pairs, i.e., $D_\Pi(n) = (2/n) \sum_{i=1}^{n/2} E[\bar{D}^i_{\Pi_n}]$.

With the above defined throughput and delay, the throughput–delay optimality can be specified. Given a throughput–delay pair $(T(n), D(n))$, it is throughput–delay optimal if there exists a scheduling scheme Π such that

$$T_\Pi(n) = \Theta(T(n)) \text{ and } D_{prod}(n) = \Theta(D(n)),$$

but for any other scheme Π',

$$T_{\Pi'}(n) = \Omega(T(n)) \text{ and } D_{prod'}(n) = \Omega(D(n)).$$

It should be noted that, given a network, there could exist multiple pairs of $(T(n), D(n))$ that achieve throughput–delay tradeoff.

8.5.2 Throughput–Delay Tradeoff in Static Networks

Before we give a specific scheduling scheme that can achieve throughput–delay optimality, we first need to consider important properties of a static random network.

Assuming the unit torus is divided into square cells of area $a(n)$, then the number of such cells is $1/a(n)$. Consider these cells in the unit torus, the following properties are held [85].

- *Property 1:* Consider n nodes in the network, if $a(n) \geq 2(\log n)/n$, then each cell has at least one node with high probability.
- *Property 2:* Under the protocol interference model, given any cell, the number of cells that cause interference is bounded above by a constant c_1 that is independent of n. Thus, each cell can start transmission every $(1 + c_1)$ time slots, which is actually an interference-free schedule.
- *Property 3:* If $a(n) = \Omega(\log n/n)$, the number of source–destination lines passing through a cell is $O(n\sqrt{a(n)})$ with high probability.

The scheduling scheme is developed based on these properties, as described below:

- For $1/a(n)$ square cells on the unit torus, two conditions must be checked: 1) no cell is empty; 2) the number of source–destination lines passing through each cell is at most $c_2 n\sqrt{a(n)}$.
- If neither condition is satisfied, then each of the $n/2$ sources just sends packets to its destination directly in a round-robin fashion.
- Otherwise, the following policy is applied by utilizing property 2.
  1. For each source–destination pair, a straight line is used to connect the source and the destination. The packets go through cells that are intersected by the straight line.
  2. Each cell becomes active every $(1 + c_1)$ time slots. Cells that are sufficiently far apart transmit simultaneously in the same time slot.
  3. When a cell becomes active in a time slot, one packet from each source–destination pair whose straight line intersects the cell is sent according to a TDM scheme.

Given the above scheduling scheme, the throughput and delay can be derived as follows.

First of all, the probability that neither condition is satisfied is vanishingly low as $n \to \infty$, because properties 1 and 3 are held by the static random network.

Thus, the throughput and delay results are nearly contributed by the scheduling scheme when both conditions are satisfied, i.e., no cell is empty and the number of source–destination lines passing through each cell is at most $c_2 n\sqrt{a(n)}$. From property 2, each cell can transmit at least a packet every $(1 + c_1)$ time slots, where c_1 is independent of n. Thus, the cell throughput is $\Theta(1)$. According to the scheduling scheme, such a throughput is contributed by all source–destination lines in the cell. From property 3, the number of such lines is $O(n\sqrt{a(n)})$. Thus, each source–destination line has a throughput of $\Theta(1/n\sqrt{a(n)})$.

Given a source–destination pair i, the number of hops for each packet is $\Theta(\sqrt{a(n)}/d_i)$, where d_i is the distance of the straight line for the given source–destination pair. Thus, the average number of hops for a packet averaged over all source–destination pairs is $(1/n)\sum_{i=1}^{n/2} d_i/\sqrt{a(n)}$. When n is large, the average distance of source–destination lines is $\sum_{i=1}^{n/2} d_i/n = \Theta(1)$. Thus, the average number of hops that a packet travels is $\Theta(1/\sqrt{(a(n))})$. For each hop, the delay of a packet is at most c_1 time slots, because this packet should be sent out within the current time slot or the one after the next c_1 time slots are over. Thus, the delay of a packet after all hops is at most c_1 times the number of hops. In other words, the delay is $\Theta(1/\sqrt{a(n)})$.

Thus, for the given scheduling scheme, if $a(n) \geq 2(\log n)/n$, the throughput and delay of the static random network are $T(n) = \Theta(1/\sqrt{na(n)})$ and $D(n) = \Theta(1/\sqrt{a(n)})$, respectively. Thus, for $T(n) = O(1/\sqrt{n}\log n)$, $T(n) = \Theta(D(n)/n)$. It can proved that such a throughput–delay pair is optimal [85], i.e., for any other scheme that can achieve the same throughput, $T(n)$, as that in the given scheduling scheme, the delay $D(n)$ will be $D(n) = \Omega(nT(n))$.

8.5.3 Throughput–Delay Tradeoff in Mobile Networks

It has been proved in [251] that a throughput of $\Theta(1)$ can be achieved if a two-hop scheduling scheme is adopted in a mobile ad hoc network. However, such a scheme can result in a large delay. Here we analyze the delay of such a scheduling scheme, and then present schemes that can achieve a better tradeoff between throughput and delay.

Delay of Mobile Networks with Throughput of $\Theta(1)$

The scheduling scheme for a mobile random network that can achieve throughput of $\Theta(1)$ is similar to that given in [251], i.e., the key concept is that the scheduling scheme must consider two constraints: (1) at most two hops are allowed for a packet from its source to its destination; (2) packets of the same source–destination pair are relayed by different nodes in the network.

With these constraints in mind, the scheduling scheme is described as follows.

- The unit torus is divided into n square cells each with an area of $1/n$. According to the results in Section 8.5.2, each cell can become active once in every $(1 + c_1)$ time slots.
- When a cell becomes active, only nodes in the same cell can have transmissions to each other.
- Given an active cell, its time slot is split into two subslots: subslot A and subslot B
  1. In subslot A, a source node is selected at random. With a probability of p_1, this source node sends a packet to another randomly chosen node, which can be a relay node or a destination. Thus, with probability $1 - p_1$, the source node does nothing.
  2. In subslot B, a destination node is selected at random. Then another node, which can be a relay node or a source node, is selected randomly to send a packet to

this destination node. However, if the selected node for packet transmission has no packets, it does nothing.

Such a scheduling can achieve a throughput of $\Theta(1)$. Its delay performance is analyzed as follows.

Given a packet for a source–destination pair, its delay consists of two components: *hop delay* and *mobile delay*. Hop delay is the time for sending a packet from a source node to a relay node or destination node. Thus, it is independent of n. Mobile delay is the time for a relay node to find the destination so that a packet is delivered. As a result, the delay of a source–destination pair is dominated by the mobile delay.

Upper Bound Given the above scheduling scheme, the transmission of a packet can be modeled as a relay queue, in which each source–destination pair has $n - 2$ queues to relay packets for this pair. Thus, a packet arrives at the relay queue when: (1) a relay node R is in the same cell as the source node S; (2) the cell is active; (3) S and R are selected as a sender–receiver pair; (4) S actually sends a packet. A packet can depart from the relay queue only when: (1) R is in the same cell as the destination node D; (2) the cell is active; (3) R and D are selected as a sender–receiver pair. However, an actual packet departure depends on whether R has packets for D. Thus, without considering available packets in R, the departure is only called a potential departure.

Considering the above relay queue, the inter-arrival times and inter-potential-departure times are not i.i.d. for the following reason. Both processes depend on whether a pair of nodes can be selected as a sender–receiver pair. However, due to the Markovian nature of the mobility model, two nodes being selected as a sender–receiver pair in the current time slot impacts the probability of any other two nodes being selected as a sender–receiver pair. Without i.i.d. for either arrival and departure process, it is difficult to analyze the relay queue. Thus, we need to use different types of queue to approximate the relay queue and then derive the delay.

Consider the first queue, Q_1, in which an arrival is assumed to occur with probability p_1 whenever S and R meet, irrespective of whether S and R are selected as a sender–receiver pair. The departure process is assumed to be the same as that in relay queue. Without requiring S and R to be a sender–receiver pair, the Markovian nature is eliminated from inter-arrival times, and thus it can be proved that the inter-arrival times of Q_1 are i.i.d. and the distribution is that of G independent copies of τ, where τ is the inter-meeting time of S, and R, and G is a geometric random process with $p = p_1$.

Since the inter-arrival times of Q_1 are stochastically dominated by those of the relay queue, the delay of Q_1 provides an upper bound for the delay of the relay queue.

Q_1 can be further approximated by the second queue, Q_2, which is constructed as follows.

The potential departure process in Q_1, which is the same as that in the relay queue, depends on two other processes: R and D are in the same cell and R and D are selected as a sender–receiver pair. Due to the latter process, the inter-potential-departure process is not i.i.d. anymore. However, it can be proved that the probability that a potential departure occurs can be not less than a constant c_2 for large enough n, where c_2 is independent of n. Thus, Q_2 is a queue such that its arrival process is the same as Q_1, but for the departure process, R and D are selected as a potential departure instant with probability c_2. Thus, in Q_2 the inter-potential-departure process is i.i.d. and the distribution is that of the sum of G independent copies of τ, where τ is the inter-meeting time of S and R, and G is a geometric random process with $p = c_6$. Furthermore, the inter-potential-departure time of Q_2 is stochastically dominated by those of Q_1. Considering that Q_1 and Q_2 have the same arrival process, the delay of Q_1 is upper-bounded by that of Q_2.

Q_2 can be further approximated by two queues in tandem, Q_3 and Q_4. The arrival process of Q_3 is the same as that of Q_2, but the departure process is an i.i.d. Bernoulli process with parameter $2/3n$. When Q_3 is not empty, and the arrival to Q_4 is the packet sent from Q_3; otherwise, a dummy packet is fed to Q_4. Thus, the arrival process of Q_4 is the same as the potential-service process of Q_3. It can be proved that the delay of the two queues in tandem provides an upper bound on the delay of Q_2 and it is $O(n \log n)$ [85].

By considering the construction of all the above queues, we know that the delay in the given scheduling scheme is $O(n \log n)$.

Lower Bound Considering a relay node in cell (i, j) and its corresponding destination node in (k, l), the delay of a packet is at least equal to the time for the two nodes walking into the cell. By a difference random walk model, the time is equivalent to the case where the relay node walks from cell (i, j) until it arrives at cell (k, l). It can be proved that the expectation of this time is $\Theta(n \log n)$ [15]. Thus, the delay of the given scheduling scheme is lower bounded by $\Theta(n \log n)$.

Combining the lower bound and the upper bound, we know that the scheduling scheme that achieves a throughput of $\Theta(1)$ has a delay of $\Theta(n \log n)$, i.e., $D(n) = \Theta(n \log n)$.

Scheme for Throughput–Delay Tradeoff

In order to carry out throughput–delay tradeoff, a different scheduling scheme is needed for the same network but with a different throughput range.

In [85], two different regimes are considered: (i) $T(n) = O(1/\sqrt{n \log n})$; (ii) $T(n) = \omega(1/\sqrt{n \log n})$. Thus, the scheduling scheme for throughput–delay tradeoff consists of two parts for these two regimes: subscheme A for the regime of $T(n) = O(1/\sqrt{n \log n})$ and subscheme B for $T(n) = \omega(1/\sqrt{n \log n})$.

Subscheme A In the throughput regime of $T(n) = O(1/\sqrt{n \log n})$, i.e., the low-throughput range, the scheduling scheme works as follows.

- The unit torus is divided into square cells each with a area of $a(n)$. It is known that each cell becomes active once every $(1 + c_1)$ time slots.

- When a cell becomes active, each source node in this cell generates a packet for its destination. These packets from all source nodes are transmitted in the same time slot.

- The packet size scales as $\Theta(1/n\sqrt{a(n)})$. Thus, in each time slot, the number of packets that can be transmitted is $\Theta(n\sqrt{a(n)})$. If in a time slot, the packets in a cell exceed this limit, the excess packets have to be dropped.

- When a packet is being sent from its source S, it chases its destination D for at most $k(n) = \Theta(\log \log n)$ stages as shown below.

- Initially, the packet is generated in cell C^0, and its destination is in cell C^1. The packet is then sent by hopping through the cells on the line connecting C^0 and C^1. The stage number $k = 1$.
- If D is still in C^1, then the packet is delivered; otherwise, the second stage is needed, i.e., $k \leftarrow k + 1$.
- If $k < k(n)$, repeat the stage. Otherwise, drop the packet.
- In each stage, if a packet is sent to a cell with a node, then the packet has to be dropped.

Since each cell becomes active once every $(1 + c_1)$ time slots and each node follows random walk, the fraction of the time that each node can be in an active node is $1/(1 + c_1)$. According to subscheme A, when a cell becomes active, each source generates a packet size of $\Theta(1/n\sqrt{a(n)})$. Thus, the traffic rate generated by each source node is $\Theta(1/n\sqrt{a(n)})$. If the packet dropping ratio is almost zero, then we derive that the throughput under subscheme A is $\Theta(1/n\sqrt{a(n)})$.

According to subscheme A, we know that packets can be dropped in the following scenarios: (1) a packet cannot find its destination before all stages have been exhausted; (2) a packet arrives at a cell without any node; (3) the number of packets in a cell exceeds the limit that is allowed in a time slot.

It can be proved that the fraction of packets that are dropped due to these issues goes to zero as $n \to \infty$ [85]. In other words, the throughput is really $\Theta(1/n\sqrt{a(n)})$.

The delay of subscheme A is dominated by the process that a packet chases its destination. Thus, $D(n) = \sum_{k=1}^{k(n)} l_k$, where l_k is the number of hops from the source to the destination in stage k. According to the mobility model and the chasing strategy, it is proved that $D(n) = O(\sqrt{n/\log n})$. In a static network, we are sure that a packet can always successfully find its destination. Thus, the delay of a static network is a lower bound of subscheme A. We know that the delay of a static network is $\Theta(\sqrt{n/\log n})$. Thus, we derive that the delay of subscheme A is also $\Theta(\sqrt{n/\log n})$.

Combining the results of throughput scaling and delay scaling, and noting that $a(n) = \Theta(\log n/n)$, we know that the throughput–delay tradeoff of subscheme A is

$$T(n) = \Theta\left(\frac{D(n)}{n}\right) \quad \text{for } T(n) = O\left(\frac{1}{\sqrt{n \log n}}\right). \tag{8.38}$$

Therefore, the through scaling, delay scaling, and the throughput–delay tradeoff are exactly the same as a static network. In other words, in the throughput regime of $T(n) = O(1/\sqrt{n \log n})$, the benefit of utilizing mobility to improve throughput performance is discouraged, because that would require a more complicated scheduling scheme but the throughput is not improved even though the delay is comparable to that in the static network.

Subscheme B From subscheme A, we know that it has an obvious shortcoming, i.e., the chasing mechanism is not efficient. To obtain a higher throughput without significantly increasing delay, we can consider a method that combines the scheduling scheme for a random network and the subscheme A. The former scheme can achieve a throughput of $\Theta(1)$, but delay can be $\Theta(n \log n)$, while the latter scheme achieves much lower delay but throughput is low too. Thus, we need to have a careful combination of these two schemes. Such a scheme is subscheme B, as described below.

- The unit torus is divided into square cells of area $a(n) = \Theta(\log n/n)$. In the scheme, $b(n)$ is used as a tradeoff point of combining subscheme A and the scheduling scheme for throughput of $\Theta(1)$, where $\log n/n \leq b(n) \leq 1$. In addition, two additional parameters are defined: $l(n) = c_3\sqrt{na(n)}$ and $c_0(n) = c_4\sqrt{na(n)}$
- Each cell becomes active once in $(1 + c_1)$ time slots. Also, each node in the network has a separate first in first out (FIFO) queue for each of the $n/2$ source–destination pairs.
- Packet size scales as $\Theta(1/\sqrt{n^3 b(n)^3 \log n})$. Thus, in an active time slot, the number of packets that can be transmitted is $\Theta(\sqrt{n^3 b(n)^3 \log n})$. If more packets are waiting to be sent, they have to be dropped.
- In a time slot, source-to-relay and relay-to-destination operate in two separate subslots, i.e., subslot A for source-to-delay phase and subslot B for delay-to-destination phase.
- The source-to-relay phase includes the following steps:
  - Each source maintains a counter and a state variable for every other node. For example, C_{ij}^{SR} and S_{ij}^{SR} are the counter and the state variable maintained by node i for node j. These two parameters are used as follows.
    1. If $C_{ij}^{SR} = 0$ and the step-distance between nodes i and j is larger than $l(n)$, then set $C_{ij}^{SR} = -1$.
    2. If $C_{ij}^{SR} = -1$ and the step-distance between nodes i and j is not larger than $l(n)$, then set $C_{ij}^{SR} = c_0(n)$ and with probability p_0 set $S_{ij}^{SR} = 1$ and otherwise set $S_{ij}^{SR} = 0$.
    3. Once subslot A arrives, the source with such an active slot decreases the counter by one until it reaches zero.

  When a cell becomes active, every source node i in this cell sends a packet to its destination via every other node j for which $C_{ij}^{SR} > 0$ and $S_{ij}^{SR} = 1$. Since multiple hops may exist from the source node to its relay nodes, a chasing scheme similar to subscheme A should be applied here. Since the step-distance between the source node and the relay nodes is limited by $l(n)$, the delay of doing so can be smaller than that in subscheme A.

- The relay-to-destination phase consists of the following steps.
  - A counter also needs to be maintained by a node i for node j, as follows.
    1. If $C_{ij}^{RD} = 0$ and the step-distance between nodes i and j is larger than $l(n)$, then set $C_{ij}^{RD} = -1$.
    2. If $C_{ij}^{RD} = -1$ and the step-distance between nodes i and j is not larger than $l(n)$, then set $C_{ij}^{RD} = c_0(n)$.

3. Once subslot B arrives, the node with such an active slot decreases the counter C_{ij}^{RD} by one until it reaches zero.

- When a cell becomes active, every node i sends a packet to every other destination j for which $C_{ij}^{RD} > 0$. Again, the same chasing scheme as in subscheme A is used to find its destination j for node i. Furthermore, the distance between nodes i and j is upper-bounded by $l(n)$, the delay of finding a destination can be greatly reduced.

- If a packet is sent to a cell without containing any node, then it has to be dropped.

The following results can be derived for throughput and delay scaling of subscheme B:

$$T(n) = \Theta\left(\frac{1}{\sqrt{nb(n)}\,\log n}\right)$$

and

$$D(n) = \Theta\left(n \log\left(\frac{1}{b(n)}\right)\right),$$

where

$$b(n) = \Omega(\log n/n) \text{ and } b(n) = O(1).$$

Thus, the throughput–delay tradeoff is also $T(n) = \Theta(D(n)/n)$ when $T(n) = \omega(1/\sqrt{n \log n})$.

8.5.4 Open Research Issues

There remain several open issues where throughput–delay tradeoff is concerned. First, hybrid networks with infrastructure support can help improve the capacity of multihop wireless networks, which is a typical case in WMN. However, the delay performance in such networks is still unknown and no research work has been carried out to study this problem.

Besides delay, there are other performance metrics that are critical for users. For example, delay jitter, maximum delay, and packet loss ratio are all important parameters for determining whether a network provides enough quality of service to users. Thus, it is meaningful to study the tradeoff between throughput and these parameters. To date, no research result has been reported on this subject.

8.6 Applicability of Asymptotic Capacity Analysis to WMNs

Asymptotic analysis of network capacity provides a good insight into the characteristics of multihop wireless networks, as summarized below.

- It reveals how the capacity scales as the number of nodes in the network.

- It can also help to understand how different factors impact the network capacity. Such factors include mobility model, interference model, scheduling scheme, and so on.

- Asymptotic analysis of network capacity helps identify approaches to increasing throughput capacity. For example, in [251] a two-phase transmission scheme is proposed to significantly increase the network capacity by utilizing mobility of nodes. Such a concept is beneficial to protocol design and can be adopted in a practical MAC protocol for mobile multihop networks.

However, many issues remain unresolved. First of all, the existing work of capacity analysis has not really captured the network architecture of WMNs. Compared with conventional ad hoc networks, WMNs are two-tier hierarchical networks in which there exist different types of communication among various nodes. For instance, communications between two mesh clients are different from those between two mesh routers or between mesh clients and mesh routers. Consequently, the throughput capacity of WMNs must be studied by considering all such different types of communication. Moreover, the capacity is not only depicted as a function of the number of client nodes, but also as a function of the number of backbone nodes such as mesh routers. In comparison with hybrid ad hoc networks, WMNs use wireless links instead of wired lines to connect backbone networks. In the capacity analysis of hybrid ad hoc networks, communication links among backbone nodes are assumed to have unlimited capacity, and such communications do not cause interference on other communications, e.g., communications between two client nodes or communications between client nodes and backbone nodes. However, these assumptions are no longer valid in WMNs. The work of asymptotic analysis on the capacity of WMNs has been initiated in [291]. For infrastructure WMNs in which clients do not have ad hoc networking among themselves, the per-client throughput capacity has been derived. For an infrastructure WMN with N_c randomly distributed mesh clients and N_r regularly placed mesh routers among which N_g routers are gateways, assuming that each mesh router can transmit at W bits per second, the per-client throughput capacity can be described in four regions as follows:

$$C(\lambda_c) = \begin{cases} \Theta\left(\dfrac{W\sqrt{N_r}}{N_c}\right) & \text{if } N_r = O\left(\dfrac{N_c}{\log N_c}\right) \text{ and } N_g = O(\sqrt{N_r}), \\ \Theta\left(\dfrac{WN_g}{N_c}\right) & \text{if } N_r = O\left(\dfrac{N_c}{\log N_c}\right) \text{ and } N_g = \omega(\sqrt{N_r}), \\ \Theta\left(\dfrac{W}{\sqrt{N_r}\log N_c}\right) & \text{if } N_r = \omega\left(\dfrac{N_c}{\log N_c}\right) \text{ and } N_g = O(\sqrt{N_r}), \\ \Theta\left(\dfrac{WN_g}{N_r \log N_c}\right) \text{ and } O\left(\dfrac{WN_g}{N_c}\right) & \text{if } N_r = \omega\left(\dfrac{N_c}{\log N_c}\right) \text{ and } N_g = \omega(\sqrt{N_r}). \end{cases} \tag{8.39}$$

For a generic WMN which allows ad hoc networking among clients, it is still an ongoing research effort to derive its capacity. In addition, the above work can be applied to a multichannel WMN. However, if channel assignment is assumed to be not optimal, then results can be different. Given a random channel assignment, the capacity of a wireless network is analyzed in [35]. How to extend such results to the case of WMNs remains an open problem.

As pointed out in previous sections, the throughput–delay tradeoff for a hybrid network remains unknown. Also, it is necessary to consider more QoS parameters together with delay and throughput scaling. In addition, how network coding can improve the delay performance and increase throughput capacity needs thorough research.

More critically, the existing approaches of asymptotic analysis have two severe failures, which prevent them from really revealing the exact capacity of a multihop network. Firstly, asymptotic results only provide some scaling laws of delay, throughput, and so on. The theoretical bounds are not necessarily valid when the number of nodes is in a small order of magnitude. In a wireless sensor network, such a problem may be avoided when the number of nodes in the network is large enough to approximate the scaling law in asymptotic results. However, in a WMN, the number of nodes in the network is typically much smaller than is assumed in asymptotic analysis.

Secondly, the capacity of WMNs is affected by many factors such as network architecture, network topology, traffic pattern, network node density, number of channels used for each node, transmission power level, and node mobility. A clear understanding of the relationship between network capacity and the above factors provides a guideline for protocol development, architecture design, deployment and operation of the network. However, the simplified assumptions made in asymptotic analysis has no way to capture so many intertwined factors. One may argue that these factors do not impact the scaling law of network capacity. However, we do not agree with such a viewpoint for two reasons. As we have seen in capacity analysis, a small change in mobility model, scheduling scheme, or network architecture can result in a significantly different scaling law in both delay and throughput capacity. Nevertheless, as we discussed above, we believe that asymptotic analysis is a first step for us to explore the true capacity of WMNs.

We noticed that some research work had been done in [139] to analyze the capacity of a WMN without relying on asymptotic analysis. The analysis is simplified by taking advantage of the low mobility feature of WMNs. However, the analytical model contains assumptions that are not necessarily valid for a WMN, as explained below.

- The traffic in all nodes is sent to a single gateway which is not the case for WMNs.
- Each node receives an equal share of the bandwidth to achieve fairness. However, this assumption is not valid if network nodes have different distances between them.
- The unidirectional traffic case is assumed to be easily extended to the bidirectional traffic case. However, the network capacity becomes totally different if bidirectional traffic is considered.
- The network architecture considered is actually still an ad hoc network. Furthermore, only a specific MAC protocol very similar to CSMA/CA with RTS/CTS is considered. However, CSMA/CA is not the only MAC solution for mesh networks. For example, the IEEE 802.11e MAC can achieve higher throughput than the CSMA/CA, because of the existence of contention free periods (CFP). For a TDMA MAC, much higher throughput can be achieved, especially under heavy traffic load.

Thus, the approach is still too vague to cover the important features of WMNs; it does not really reveal the exact capacity of WMNs.

Consequently, exploring the exact capacity of WMNs will continue to be an important but challenging research topic. Recently asymptotic results have been derived to explicitly involve topology and traffic patterns in capacity analysis [145]. Such work can be applied to WMNs too. However, due to the difficulty of deriving the capacity of wireless networks, tremendous efforts are still needed until a theory for exact capacity can be discovered. On the other hand, exploring practical solutions to improving network capacity [18, 225] remains a promising research direction for WMNs. These solutions can be located separately in different protocol layers or across multiple layers as cross-layer design.

9

Cross-Layer Design

The methodology of layered protocol design has been applied for decades in different types of network. Whether it is the well-known open systems interconnection (OSI) architecture, ATM architecture, or today's dominant Internet architecture, protocols are distributed in different layers. In such an architecture, protocols are designed without being constrained by each other. The schemes and algorithms employed in these protocols are transparent to each other, no matter how simple or sophisticated they are. Advantages such as scalability of network size, portability of protocols in different layers, flexibility in protocol design, and so on can be easily obtained.

However, such a protocol design methodology has been challenged for years. There are many reasons behind it, but they can be summarized as follows. First of all, the requirement of service quality is ever-increasing. For example, in addition to connectivity and always-on networking, features such as high speed transmission rate and quality of service (QoS) for time-critical applications are also desired by users. To meet such requirements, the conventional layered protocol design may not be a viable solution. One proof is that today's end-to-end QoS solution for the Internet usually involves multiple protocol layers. Secondly, the network heterogeneity is much higher than before. For example, the Internet is not composed of one single network, but consists of different categories of network such as wired networks, wireless networks, and optical networks, each consisting of many network types. The conventional layered architecture is effective for integrating them into the same network, but the performance is not optimized. For example, when a routing path is set up for two end users through different types of network, the routing protocol can simply find an available path considering metrics such as shortest distance or lowest cost. However, if end users want to find a path with enough bandwidth, then the routing protocol needs to consider the interactions with the MAC layer. For example, in a LAN (wired or wireless), meshed optical networks, and so on, the bandwidth on a certain link is not guaranteed if the MAC layer functionality is not appropriately controlled. Thirdly, many networks today, especially wireless networks, have no dedicated links between nodes. In a wireless network, transmission between two nodes also interferes with other nodes in the neighborhood. Thus, the meaning of "link" pertained to a conventional wired network does not exist anymore. The capacity of a link is variable and can be fully cross-related with other links. Such

Wireless Mesh Networks Ian F. Akyildiz and Xudong Wang

inter-dependence in fact breaks the transparency between different protocol layers. Where a multihop network, such as a WMN, is concerned, this problem becomes much more obvious.

Whether layered protocol design or cross-layer design is a better option for future networks is still an ongoing research topic. Researchers have proposed that protocol layering can be obtained by decomposing the optimization of overall network performance [58]. As long as optimization decomposition is successfully done, protocol in each layer work independently as an optimal module to achieve the best network performance; as a consequence, minimal cross-layer interaction is really needed. However, the methodology of "layering as optimization decomposition" actually cannot avoid cross-layer design, especially where a WMN is concerned. There are two major reasons for this limitation. Firstly, to carry out optimization decomposition, there remain too many unresolved issues. One typical example is the lack of a model that can capture stochastic dynamics in different time scales such as packet, session, connection, and topology levels. This is especially true in a multihop network like WMN. Secondly, the protocol layering by optimization decomposition does not necessarily match the existing protocol stack that is widely adopted in WMNs. Depending on different representation of the optimization problem, different decomposition structure may be derived, which results in a different architecture of protocol layering. However, in WMNs the standard protocol stack is TCP/UDP IP over different link layer and physical layer protocols. The mismatch between the current standard protocol stack and the protocol layering from optimization decomposition actually suggests that cross-layer design is highly desirable if network performance needs to be optimized.

Therefore, it is reasonable to believe that cross-layer optimization will continue to be one of the most important methodologies for protocol design of WMNs. However, certain issues must be considered when carrying out cross-layer protocol design [143]: cross-layer design has risks due to loss of protocol layer abstraction, incompatibility with existing protocols, unforeseen impact on the future design of the network, and difficulty in maintenance and management. Thus, certain guidelines need to be followed [143].

In this chapter we investigate cross-layer design of WMNs [9]. The necessity for cross-layer design is first pointed out, followed by discussing challenging issues involved in WMNs. We then study cross-layer design schemes between different protocol layers.

9.1 Motivations for Cross-Layer Design

Cross-layer design has been widely used to improve the network performance, especially in a wireless network. Many research results have shown that cross-layer design can significantly improve the network performance. In this section we illustrate the need of cross-layer design for WMNs in two aspects. Firstly, we notice that researchers have dedicated efforts to proposing methodologies to decouple cross-layer interactions. The most well-known concept is "layering as optimization decomposition". We fully respect such a methodology and agree that it can be an effective solution for improving network performance with minimal cross-layer design. However, by looking into the mechanism of this methodology, we can find out that this method cannot really eliminate the need of cross-layer design. On the contrary, the optimization decomposition actually provides a systematic framework for cross-layer design.

Secondly, under the circumstances of WMNs, we explain the special features that pertain to WMNs but put a higher demand on cross-layer design.

9.1.1 Layered Design Versus Cross-Layer Design

Layering as Optimization Decomposition

Layered protocol architecture is one of the most important factors that have made networking so successful. However, we have lacked a systematic approach to analyzing whether layering of protocols is optimal. “Layering as optimization decomposition” fills such a gap between theoretical and practical methodologies of protocol design. In this method, various protocol layers are integrated into one single coherent theory, in which asynchronous distributed computation over the network is applied to solve a global optimization problem in the form of generalized network utility maximization (NUM). The key idea of “Layering as optimization decomposition” is to decompose the optimization problem into subproblems each corresponding to a protocol layer and functions of primal or Lagrange dual variables coordinating these subproblems correspond to the interfaces between layers [58]. Since different decompositions result in different layering schemes, conditions under which layering incurs no loss of optimality need to be studied and so does the sensitivity of a layering scheme. These conditions and sensitivity can help to identify the performance differences between different layering schemes.

The basic NUM is usually formulated for protocol layer performance optimization, while generalized NUM needs to capture the entire protocol stack. A possible formulation of a generalized NUM is shown as [58]

$$\begin{array}{ll} \text{maximize} & \sum_s U_s(x_s,\ P_{e,s}) + \sum_j V_j(w_j) \\ \text{subject to} & \mathbf{Rx} \le \mathbf{c}(\mathbf{w}, \mathbf{P}_e) \\ & \mathbf{x} \in \mathcal{C}_1(\mathbf{P}_e),\ \mathbf{x} \in \mathcal{C}_2(\mathbf{F}) \text{ or } x \in \Pi \\ & \mathbf{R} \in \mathcal{R},\ \mathbf{F} \in \mathcal{F},\ \mathbf{w} \in \mathcal{W}. \end{array} \tag{9.1}$$

This NUM tries to maximize the user utility function $U(\cdot)$ and resources $V_j(\cdot)$ on network element j. x_s and w_j denotes the rate for source s and the physical layer resources at network element j, respectively. $\mathbf{R}$ is a routing matrix, and $\mathbf{x}$ denotes the link capacity as a function of physical layer resource $\mathbf{w}$ and the desired error probability $\mathbf{P}_e$ after decoding. All physical layer factors such as interference, power control, etc should be captured in function $\mathbf{c}$. Thus, the first constraint in the above NUM represents the behavior perceived at the routing layer. The coding and error control mechanisms versus the rate are captured in function $\mathcal{C}_1(\cdot)$, while the contention based MAC or scheduling based MAC is captured in $\mathbf{C}_2(\cdot)$ and Π, respectively, where $\mathbf{F}$ is the contention matrix and Π is a schedulability constraint set. Thus, the second line of constraints stands for link layer behavior that has taken into account the effect of the physical layer. From the above generalized NUM, we can see that the network performance is to be optimized at the transport layer subject to the constraints in routing, MAC, and physical layers.

The above formulation is based on a deterministic fluid model, which cannot represent many scenarios, especially in WMNs. Thus, stochastic NUM is a preferred formulation. Stochastic NUM has been an active research area, in which many challenging issues still remain to be resolved.

Whether it is a deterministic or a stochastic generalized NUM, the optimization decomposition is usually carried out following three steps.

- The generalized NUM is formulated independent of layering possibilities.
- A modularized and distributed solution is developed to perform optimization by following a particular decomposition.
- The space of different decompositions is explored such that a choice of layered protocol stack is made.

In a generalized NUM, the objective function is usually composed of two parts: user objective functions and operator objective functions. These two parts can be simply integrated via a weighted sum. Another option is multi-objective optimization that characterizes the Pareto-optimal tradeoff between user objective and the operator objective. Game theory can also be used to formulate the NUM with both user and operator objective functions.

The optimization decomposition for the generalized NUM is composed of both horizontal decomposition and vertical decomposition.

- *Vertical decomposition.* In this type of decomposition, the entire network functionalities are decoupled into different modules such as congestion control, routing, scheduling, MAC, power control, error control, and so on. Different modules can be classified into different layers in the protocol stack.
- *Horizontal decomposition.* Horizontal decomposition aims at devising a distributed computation solution to an individual module. More specifically, this step will work out a specific distributed mechanism and algorithm for protocols such as congestion control, scheduling, MAC, and so on.

Optimization decomposition can help us to better understand existing layered protocols and will provide a systematic design for an optimized layered protocol architecture. However, such methodology does not preclude the need of cross-layer design for the following reasons.

- For the same NUM, different decompositions can achieve the same optimization, but are mapped to different layering schemes.
- Difficulties in modeling can prevent this method from being applied to a realistic protocol design. For example, it is more reasonable to have a stochastic NUM than a deterministic one, but we still lack appropriate models for stochastic NUM capturing network dynamics in different levels such as session, packet, topology, etc. Also, different protocols in the protocol stack may operate in timescales that can be different by several orders of magnitude, which brings challenges to modeling.
- Optimization decomposition, in particular vertical decomposition, separate functionalities into different modules in different layers. However, the decomposition may still keep coupling between layers or modules. Such coupling actually proves the natural need of cross-layer design in a network.
- No matter how optimal a decomposition can be done and how good a layered architecture is achieved, it may not match the existing protocol stack being widely used in reality. For example, the Internet protocol architecture is well recognized as a default standard for both wired and wireless networks in many application scenarios. Architecture mismatch between an optimal decomposition and an existing protocol stack also suggest the need of cross-layer design.

Thus, cross-layer design will undoubtedly continue to be an important approach to improving network performance. However, it should be noted that the research results of optimization decomposition performed on the generalized NUM can benefit cross-layer design. For example, comparing a decomposition result with the existing protocol stack can tell us which layers need cross-layer optimizations and how to optimize the interactions between layers.

Multihopping is Order Optimal

Independent of the work of "layering as optimization decomposition", the scaling laws of transport capacity of wireless multihop networks studied in [274] also suggest that layered design is optimal.

Given a planar network in which two nodes are separated with a distance ρ_{ij}, if node i transmits a signal level of $X_i(t)$, then its received signal level is

$$Y_i(t) = \sum_{j \neq i} \frac{e^{-\gamma \rho_{ij} X_j(t)}}{\rho_{ij}^{\delta}} + Z_i(t),$$

where $Z_i(t)$ is Gaussian noise, and constant δ is the path loss exponent and γ is the absorption constant. In [274], the following results have been proved.

- *The scenario of exponential attenuation.* Suppose absorption exists in the medium (i.e., $\gamma > 0$) or path loss exponent ρ_{ij} is larger than 3, then the transport capacity, defined as the distance-weighted sum of rates, grows as $\Theta(n)$. Furthermore, if traffic load on each node can be balanced, then the multihop forward-and-decode strategy, treating interference as noise, is order-optimal with respect to the transport capacity.

- *The scenario of low attenuation.* If $\gamma = 0$ or the path loss exponent is small (e.g., $\delta < 3/2$), then the attenuation is low. In this scenario, other strategies such as coherent multistage relaying with interference subtraction can be order-optimal with respect to the scaling law of transport capacity. This result suggests that a new protocol architecture rather than a conventional layered structure is probably needed for information transport.

In WMNs, the normal scenario is actually exponential attenuation. In [134], it states that layered design with a decode-and-forward strategy can achieve optimal performance, within a constant, in regard to network capacity. It also points out that a decode-and-forward strategy matches the architecture of layered design. Consequently, it is concluded that the cross-layer design can only improve throughput by at most a constant factor and that unbounded performance improvement cannot be achieved.

However, such a statement can be too strong in many scenarios, especially when we come to actual protocol design rather than asymptotic analysis. As explained below, the results in [143, 274] cannot really prove that cross-layer design is not necessary.

- *The theoretical result is only based on simplistic network models and only meaningful asymptotically.* As far as a realistic WMN is concerned, neither these models nor asymptotic scaling law is really applicable. For example, under the condition that asymptotic capacity bound is achieved, cross-layer design may not be able to achieve even a small improvement of throughput. However, in a realistic WMN, due to constraints of system complexity, reasonable network size (not approaching infinite) and nonideal network models, the network capacity is far below the asymptotic capacity bound. Such a gap motivates the need for cross-layer design.

- *Decode-and-forward strategy does not imply no cross-layer design.* Almost all existing multihop wireless networks are designed based on a decode-and-forward strategy, but we still see many examples of cross-layer design for improving network performance. For example, the existing protocol stack adopted in 802.11 WMNs is definitely a decode-and-forward strategy, but carrying out MAC/physical or MAC/routing cross-layer design is a common technology to improve network performance.

9.1.2 Cross-Layer Design in WMNs

Several characteristics of WMNs make cross-layer design more necessary in WMNs than in other multihop wireless networks such as mobile ad hoc networks or wireless sensor networks. First of all, WMNs lack the luxury of a clean-slate protocol design. The protocol has to follow the well-known standard protocols, especially Internet protocol architecture. Secondly, advanced wireless radio technologies in the physical layer adopted by WMNs and the ever-increasing demand for higher bandwidth and better service by users pushes together so that all protocol layers become potentially interactive with each other. Lastly, the inherent nature of the shared medium by all nodes in WMNs further exacerbates the problem. In particular, a MAC protocol has no way to be so efficient that variance in the physical layer is invisible to protocols above the MAC layer. Detailed explanations on these challenging issues are given below.

- *No clean-slate protocol architecture.* Using optimization decomposition can result in a new protocol architecture that is quite different from the existing standard protocol stack. The well-known Internet protocol architecture has been widely adopted for most applications of WMNs. Thus, how to make the layered protocol architecture derived from optimization decomposition and the Internet protocol stack match with each other is a technical challenge. It is highly possible that in many cases no match can be achieved. Thus, in order to further improve network performance without abandoning the Internet protocol architecture, cross-layer design becomes indispensable.

- *Advanced physical layer technologies.* Compared to other multihop networks, WMNs are more concerned with bandwidth and network capacity. Thus, many advanced physical layer technologies have been adopted into WMNs. These technologies fall into several major categories.

  – *Multirate transmission technology.* This is achieved by having multiple options of modulation, coding, and power control schemes. Different transmission rate usually results in different transmission range and interference range. With multirate transmission technology, the same physical layer can support a different transmission rate depending on the link quality and the environment. In a single-hop wireless network, using link adaptation protocols – which is a type of simple cross-layer design scheme – can satisfy the need for maximizing throughput. In WMNs, however, merely using link adaptation is not enough, since links within multiple hops are related to each other. Thus, in WMNs, link adaptation becomes network wide rather than a one-hop mechanism. So, link adaptation is inevitably cross-related to routing and topology control. Such a cross-relationship between different protocols reflects the necessity of cross-layer design.

  - *Advanced antenna technology.* Directional antennas and the advanced versions such as smart antennas can significantly reduce interference between nodes that are close to each other. Such technologies certainly increases network capacity, but also demands extra algorithms in upper layers to coordinate antenna direction or beamforming. In a single-hop wireless network, a control algorithm located in the MAC layer, i.e., MAC/physical cross-interaction, is enough. However, in WMNs, routing needs to be considered together, since different beamforming or antenna direction impacts the routing path and vice versa. In other words, routing, MAC, and physical layers all need to play together. A more advanced antenna technology is multiple input and multiple output (MIMO). In a node using MIMO, advanced signal processing technology is employed to achieve an optimal balance between link reliability and link capacity. MIMO on a point-to-point or point-to-multipoint setup has been well researched. However, how to take advantage of MIMO in WMNs usually demands a network-wide scheduling scheme.
  - *Multichannel or multiradio technology.* Multichannel operation (either single- or multiple-radio) can significantly reduce the interference between nodes in a multihop network. To utilize such a technology, an extra algorithm, dynamic channel allocation, must be developed in the MAC layer. This algorithm also needs to be aware of interference from outside networks. Since varying channels in different hops potentially impacts the optimal routing path that can be selected, both MAC and routing protocols must work together to take advantage of the multichannel technology.

  It should be noted that the above three classes of physical layer technology are usually integrated, which further intensifies the challenge in protocol design in upper layers. For example, multirate transmission can happen on a physical layer using MIMO and multichannel operation. For a WMN with so many advanced physical layer features, it is more challenging to re-optimize both MAC and routing protocols.

- *Imperfect MAC.* MAC has always been a critical part in wireless networks. Many solutions are available. However, none of them is perfect because of two major factors: (1) the wireless medium is always imperfect in nature; (2) the MAC itself has no guarantee of performance. In the second factor, a typical example is CSMA/CA, which is a best effort protocol and cannot provide any guarantee of delay, collisions, etc. Such unpredictable performance of the MAC can severely limit the performance of a routing protocol. For example, routing messages may not be able to be sent out in a congested CSMA/CA based WMN, which in turn impacts the capability of a routing protocol. This issue is even worse in WMNs because the performance of MAC is not just a matter of single-hop networking but multihop. Research can be carried out to constantly improve the MAC protocols for WMNs. However, as a matter of fact, if routing is not taken into account, optimal performance can only be achieved locally.

Consequently, in order to achieve the ultimate goal of perfect MAC, routing must be considered as an integral part of MAC. In this sense, MAC and routing protocols in WMNs are so closely related that they should be put together as two modules in one layer or even just one module in the same protocol layer. A typical example is the upcoming IEEE 802.11s standard for 802.11 WMNs, in which MAC and routing have been put together into the same MAC layer. However, we have also noticed that optimal interactions between MAC and routing have not been exploited yet in IEEE 802.11s.

- *Mixed traffic types with heterogeneous QoS.* WMNs are expected to support a large variety of services that consist of many traffic types with heterogeneous QoS requirements. In order to deliver such services in WMNs, transport layer, routing, and MAC protocols need to cooperate nicely; otherwise, either service quality is not ensured or the network resources may be wasted. For example, it is always preferable to use separate transport layer protocols for VoIP, video, and data traffic. For VoIP and video traffic, finding a reliable routing path is obviously not the goal, since a path does not guarantee the quality of VoIP or video, no matter how reliable the path is. Thus, finding a routing path must consider bandwidth allocation. This problem has been researched as a QoS routing topic. However, when more advanced physical layer technologies are considered, it becomes more than a QoS routing problem and has to involve tight routing/MAC cross-layer design. For example, variation of bandwidth demand on a given routing path or change of a routing path can trigger reallocation of time slots, channels, antenna directions, etc. on all links related to the given routing path or vice versa.

Based on the above analysis, we know that cross-layer design is imperative for WMNs. However, it should be noted that, given a network that does not have such characteristics of WMNs, a layered protocol design would be promising enough to achieve optimal network performance.

9.2 General Methodology of Cross-Layer Design

Cross-layer design can significantly improve network performance [36, 56, 153]. It can be performed in two ways: loosely coupled cross-layer design and tightly coupled cross-layer design.

In the loosely coupled cross-layer design, the optimization is carried out without crossing layers, but focusing on one protocol layer. In order to improve the performance of this protocol layer, parameters in other protocol layers are taken into account. Thus, information in one layer must be passed to another layer. Typically, parameters in the lower protocol layers are reported to higher layers. For example, the packet loss rate in the MAC layer, or channel condition in the physical layer can be reported to the transport layer so that a TCP protocol is able to differentiate congestion from packet loss. As another example, the physical layer can report the link quality to a routing protocol as an additional performance metric for the routing algorithms.

It should be noted that information from multiple layers can be used on another layer to perform cross-layer design. With such information, there are two different ways of utilizing such information. The first one is the simplest case of cross-layer design, in which the information in other layers works just as one of the parameters needed by the algorithm in a protocol layer. The performance of this algorithm is improved because a better (more accurate or reliable) parameter is used, but the algorithm itself does not need a modification. For example, the physical layer can inform the TCP layer of the channel quality so that TCP can differentiate real congestion from channel quality degradation, and thus carry out congestion control more intelligently. In the second method, based on the information from other layers, the algorithms of a protocol have to be changed. For example, if a MAC protocol can provide a routing protocol information about its performance, the routing can perform multipath routing to utilize spatial diversity. However, the change from single-path routing to multipath routing needs a significant modification to the routing protocol rather than just parameter adaptation.

In the tightly coupled cross-layer design, merely information sharing between layers is not enough. In this scheme, the algorithms in different layers are optimized together as one optimization problem. For example, for MAC and routing protocols in a multichannel TDMA WMN, time slots, channels, and routing path can be determined by one single algorithm. Using optimization across layers, it can be expected that much better performance improvement can be achieved by the tightly coupled cross-layer design than the loosely coupled scheme. However, the advantage of the loosely coupled design is that it does not totally abandon the transparency between protocol layers.

An extreme case of tightly coupled cross-layer design is to merge different protocol layers into one layer. According to the concept of “layering as optimization decomposition”, this kind of design tries to improve network performance by re-layering the existing protocol stack. Merging multiple protocol layers into one layer keeps the advantage of tightly coupled cross-layer design. Furthermore, it can also eliminate the overhead in cross-layer information passing. Interestingly, merging multiple protocol layers is not just a theoretical concept, but has been seriously considered in real practice. For example, in the upcoming 802.11 standards for mesh networks, the routing protocol is being developed as one of the critical modules in the MAC layer. Such a merging between routing and MAC layers provides great potential for carrying out optimization across MAC and routing, based on the same algorithm.

Cross-layer design can be done between multiple layers or just two layers. Given a protocol stack, cross-layer design can be done in any two protocol layers. In the following sections of this chapter, instead of going through all the combinations of cross-layer design, we focus on the ones that are most critical to WMNs. Considering the Internet protocol architecture, the protocol layers that contain most specific features of WMNs include MAC, routing, and physical layer. In some cases, the transport layer needs to be optimized with the physical layer in WMNs. Thus, in the remaining part of this chapter we will investigate the detailed protocols in cross-layer design between MAC and physical, between MAC and routing, and between physical and transport. Optimization algorithms across multiple layers are also discussed.

9.3 MAC/Physical Cross-Layer Design

Cross-layer design between MAC and physical layers is more common than that between any other two layers because MAC and physical layer are so close to each other. In many wireless networks, the lower part of the MAC layer and the baseband of the physical layer are implemented on the same card or even on the same chipset. Real-time interactions between the two layers occur frequently. Thus, in most wireless networks including WMNs, the cross-layer between MAC and physical layer always exists in nature. On top of these natural interactions between the lower part of the MAC and the baseband of physical layer, the advanced physical layer techniques have empowered the physical layer to be able to support more sophisticated cross-layer design for the purpose of enhancing network performance. These techniques include the following typical categories.

- *Multiple coding and modulation schemes.* When a different coding and modulation scheme is used, the transmission rate on a link changes too.

- *Advanced antenna techniques.* The examples include directional antennas and smart antennas.

- *MIMO.* Based on multiple antennas for transmission and reception and advanced signal processing techniques, the transmission rate of a wireless link can be significantly increased by MIMO.

- *Orthogonal frequency division multiplexing (OFDM) technologies.* OFDM can used to build OFDM time division duplex (TDD), OFDM frequency division duplex (FDD), or orthogonal frequency division multiple access (OFDMA) systems as specified in IEEE 802.16. It can also be used as a building block for UWB systems.

- *Ultra wideband (UWB).* Very high transmission rate is achieved using ultra wide bandwidth. UWB can be pulse-based like direct sequence (DS) UWB as specified by the UWB forum or OFDM-based such as multiband-OFDM (MB-OFDM) supported by WiMedia Alliance.

These technologies can be combined into one device. For example, in a WiMedia UWB device, UWB based on MB-OFDM, multirate is supported through variable coding and modulation, and link throughput can be improved through MIMO. The advanced physical layer technologies provide great potential for improved performance of delay, throughput, packet loss, etc. However, the physical layer itself does not determine how to adaptively fine tune the parameters in these advanced technologies. In fact, such fine tuning is a critical task in the upper sublayer of a MAC protocol. Thus, to optimize the performance of these advanced physical layer technologies, the cross-layer design between MAC and physical layer becomes indispensable.

9.3.1 Link Adaptation, Adaptive Rate Control, and Adaptive Framing

In a wireless network, fading, interference, noise, and so on can greatly impact the link capacity, and in turn decreases the network capacity. To maintain a robust link performance, the most well-known technique is link adaptation through adaptive modulation and coding.

Link adaptation is coupled with rate control because different modulation and coding schemes result in different transmission rate and also different link layer performance such as packet error rate. Given a specific link, link adaptation dynamically selects the most appropriate modulation and coding scheme and thus the best transmission rate. Thus, as far as transmission rate is concerned, link adaptation serves the same purpose as rate control. However, there are some differences between rate control and link adaptation. In a rate control scheme the optimization is performed on the link transmission rate, while optimization is done directly on modulation and coding parameters in a link adaptation scheme. Furthermore, link adaptation usually depends on physical layer parameters such as bit error rate (BER) or signal to noise ratio (SNR) to determine the coding and modulation parameters. Thus, implementation of link adaptation is closer to the physical layer. One shortcoming of link adaptation is that the physical layer may lack a mechanism for providing accurate measurement of BER or SIR. On the other hand, in the MAC layer the link quality information can be derived from other easily measurable parameters such as packet loss rate, retransmission rates, etc., since such parameters change as the link quality varies. As a result, a different mechanism, i.e. rate control, is usually applied in the MAC layer to adaptively select the modulation and coding schemes in the physical layer. A rate control scheme usually consists of two major modules: rate selection and mapping between rate and physical layer parameters. Several MAC layer parameters such as packet loss ratio, retransmission rates, and packet error rates, can be used as link quality indexes to determine the best transmission rate. Given a transmission rate, the modulation and coding scheme can be selected based on a mapping table between rate and coding/modulation.

Most existing rate control or link adaptation schemes focus on link-layer performance. However, solely using optimization on link rate or coding/modulation is not enough to guarantee the performance. For example, in either link adaptation or rate control, the link transmission rate needs to be reduced when BER or packet loss rate increases. However, such a simple scheme may not always work, because the BER or packet loss rate may be just due to inside-network interference between different nodes rather than noise or outside-network interference. Thus, if a node's transmission rate is reduced, its transmission time is increased too, and this causes a higher duration of interference to other nodes in the same network. Other nodes performing the same rate control or link adaptation scheme experience the same problem, and then the entire system becomes a positive-feedback closed-loop control system, which means that the system can quickly lose stability and the rate in all nodes becomes very low. To solve this issue, adaptive frame size in the MAC layer must be determined considering the interference between different nodes in the same network. Such an adaptive framing scheme is a more advanced rate-control mechanism, which not only selects the best transmission rate but also determines the most appropriate frame size corresponding to this rate. An example of rate-adaptive framing is proposed in [52], where the size of a MAC layer frame is determined by a receiver and then fed back to the transmitter. Such a scheme can achieve significantly much better performance than other rate control schemes in [103, 228].

It should be noted that simple link adaptation or rate control schemes are commonly used in the many current WMNs. For example, in IEEE 802.11, 802.15, and 802.16 based WMNs, all existing rate control schemes are still based on rate control schemes with optimization on either rate or modulation/coding only. However, as a multihop mesh network, the interactions between different nodes significantly impact the performance of the rate control schemes. Thus, it is highly desirable for schemes such as rate-adaptive framing in [52] to be developed for WMNs.

9.3.2 Adaptive Antenna Direction Control

Compared to omni-direction antenna, directional antennas hold several advantages. With a directional antenna, the same transmit power on a node can make signals reach much longer distance. In other words, for the same distance, a directional antenna can achieve much better link quality than an antenna that is omni-direction. A directional antenna can effectively reduce the number of interfering nodes, which is particularly true in WMNs.

To take these advantages, the physical layer of a wireless node must be able to support the dynamic change of antenna direction. Moreover, the MAC protocol needs to coordinate antenna directions in different nodes. Thus, the cross-layer optimization works as follows. Firstly, the MAC determines the direction of a node. Secondly, the physical layer should be able to tune the antenna to the target direction.

In the physical layer, the simplest form of directional antenna is where the antenna is mechanically directional. However, such an antenna is not scalable in WMNs, since the antenna direction of any node needs to be tuned to a different direction adaptively according to the variations of traffic pattern, link quality, network topology, etc. Another type of directional antenna is the sectored antenna. By using such an antenna, the antenna direction can be tuned to a certain sector. A more sophisticated way of achieving a directional antenna is beam-forming in a smart antenna. Given a target direction, the antenna beam can be formed to such a direction. Beam-forming can achieve a more accurate antenna direction and have a finer granularity in tuning the directions.

In a wireless network with a point-to-point or a point-to-multipoint topology, the adaptive antenna control is straightforward. However, where a WMN is concerned, the antenna direction control becomes complicated, since a node may need to communicate with other nodes in different directions. Adaptive antenna direction control reduces exposed nodes in a WMN and thus has great potential for significantly increasing throughput. However, it also results in more hidden nodes. To avoid performance degradation by these hidden nodes, scheduling becomes a critical task. The simple scheme such as the RTS/CTS mechanism defined in 802.11 is not effective anymore, because the hidden nodes are not due to the distance but due to uncoordinated change of antenna directions on different nodes. Thus, the scheduling scheme does not reside on one node. Instead it resides on different nodes in WMNs and runs as a distributed but cooperative algorithm among all nodes in WMNs. Since antenna change by the scheduling scheme also impacts the routing path, adaptive antenna direction control actually involves a cross-layer design among three layers, i.e., routing, MAC, and physical layers.

9.3.3 Dynamic Subcarrier Allocation and Frame Aggregation for OFDM

OFDM has been used in many existing wireless networks including IEEE 802.11 and 802.16. In many OFDM based wireless networks, the subcarriers in one OFDM symbol are treated as one resource unit. For example, in 802.16 wireless networks, the TDMA FDD and TDMA TDD modes do not allow subcarrier allocation. In 802.11 networks, the subcarrier is not visible to the MAC layer protocol. However, as the physical layer transmission rate becomes higher and higher, subcarrier allocation becomes necessary. Considering a TDMA frame in which a time slot contains one OFDM symbol, if the physical layer transmission rate is high, then one time slot can hold a large packet size. To avoid under-utilization of an OFDM symbol, frame aggregation is needed in the MAC layer. However, the effectiveness of frame aggregation depends on enough traffic load being generated at a node. Also, frame aggregation causes performance degradation such as increased latency of a packet.

To avoid such issues, subcarrier allocation is preferred. With subcarrier allocation, a much finer resource unit can be achieved, and thus, a packet can be accommodated as it arrives.

There is another motivation for subcarrier allocation. In a wireless network, especially in a multihop wireless network, nodes in the same network can experience different amounts of fading. As a result, for the same subcarrier, it may experience bad channel quality on one node but good channel quality on another node. Thus, it is beneficial to allocate different subcarriers to different nodes whose channel quality varies depending on their locations.

In IEEE 802.16, the operation mode OFDMA provides an option of subcarrier allocation. In Qualcomm's Flash OFDM, subcarrier allocation is also supported. In a point-to-multipoint wireless network, subcarrier allocation has been thoroughly researched [237, 255, 269]. However, in a multihop wireless network such as WMNs, few results have been reported on subcarrier allocation. In [162] subcarrier allocation is studied for a WMN with a single mesh router and multiple mesh clients. A two-layer hierarchical fair scheduling scheme is proposed to determine subcarriers and their powers for the mesh router and mesh clients. Slow fading is considered in the proposed scheduling scheme. Thus, such a scheme is not applicable to frequency selective fading channels.

9.3.4 MIMO Control and Scheduling

It is well known that MIMO can significantly improve the link capacity of a wireless network via transmit diversity and spatial multiplexing. Such a technique has been considered as the most important solution to extending physical transmission rate of IEEE 802.11 wireless networks, i.e., in the upcoming 802.11n standards. MIMO in a wireless network can be treated independently from the MAC protocol. This method of protocol design is simple but is definitely a suboptimal solution; the advantageous features of MIMO seen in a point-to-point link may not be maintained in a more complicated network topology as in WMNs. To fully utilize the advantages of MIMO, the MAC protocol must be specially designed considering the cross-layer dependence with the MIMO physical layer techniques.

By using multiple antennas for transmitting and receiving, several performance improvements can be achieved in a MIMO system [294].

- *Transmit diversity.* The same information is sent in different antennas to increases the reliability, which in turns increases throughput in the MAC layer.

- *Spatial multiplexing.* Different streams of packets are sent in different antennas and thus achieve higher transmission rate than a single-antenna system.

- *Beamforming.* Different transmission angles are controlled in different antennas so that a desired beam is formed pointing in a certain direction. With beamforming, better transmission range and higher rate can be achieved.

- *Interference nulling.* Again via control on different antennas, the interference from, or to, certain directions can be reduced. Thus, interference between different nodes can be controlled.

The above improvements are not mutually exclusive, and can be combined to reach even higher performance improvement. How to trigger different functionalities in the physical layer so as to get the best combination of the above improvements is one of the tasks of cross-layer design between MAC and physical layers. In a WMN, other than the above improvements, another improvement is possible. Since each node has multiple antennas and has multiple neighboring nodes to send and receive packets, it can send packets to different nodes using different antennas or it can receive packets from different nodes using different antennas. Such multi-user OFDM puts a more challenging requirement on scheduling of packet transmissions in a MIMO system.

MIMO control and scheduling usually consists of the following critical steps.

- *Get channel state information (CSI).* CSI can be obtained at the receiver from the training sequence in a receive signal. However, there are three difficulties in getting CSI. First, the training data is sent before MIMO control takes effect; otherwise, it would be impossible for a node to get CSI for all its neighbors. However, the dilemma is that the CSI can be very different from the case when MIMO control kicks in. Thus, identifying a right set of reachable neighbors, and the CSI from them with MIMO transmissions, is still an unresolved and challenging research issue. Second, CSI feedback to the transmitter may not always be available, for two reasons. One reason is that the channel may change so quickly that the feedback is too slow to catch up with the change. The second is that there is no mechanism of sending the feedback information from the receiver to the transmitter. Without CSI at the transmitter, an open-loop system needs to be developed to carry out MIMO control. Third, the mobility or topology change makes the previous two problems even more severe, since neighbors of a given node are not stable and thus the CSI from these neighbors must be updated constantly.

- *Determine the tradeoff between transmission rate, range, and reliability.* This is an independent step from the previous one. Usually the network performance metrics such as throughput and QoS are important factors to determine the needed MIMO control such as spatial multiplexing, diversity, beamforming, and interference nulling. The challenge in this step is how to combine as many features as possible so that the best performance can be achieved.

- *Scheduling packet transmissions on different antennas on different nodes using the collected CSI.* Based on the collected CSI and determined MIMO control, scheduling schemes need to be developed for packet transmissions on different nodes. In WMNs, the challenge is how to develop a distributed scheduling scheme such that the global optimal solution can be approached.

A few research results have been reported to investigate optimization of MIMO transmissions [48, 245]. However, these results are derived based on simple assumptions such as perfect synchronization in packet transmission [48] and no physical layer dependencies and channel variations [245]. Furthermore, as with directional antenna control, MIMO control and scheduling may also involve routing protocol as part of cross-layer design. So far, no research has been reported on this topic.

9.4 Routing/MAC Cross-Layer Design

A routing protocol of a multihop wireless network determines a path for any packet from source to destination. In its simplest form, a routing protocol can just consider connectivity between nodes, i.e., as long as a connectivity can be maintained a routing path is set up. However, to enhance performance, other routing metrics and mechanisms must be taken into account. For example, a routing protocol may need to consider minimum hop count, lowest traffic load, etc. However, such layered design approaches are still suboptimal in performance. The reason is that the behavior of the MAC protocol has not been taken into account. Thus, no matter how the routing protocol is optimized, if the underlying MAC does not provide satisfying performance, the overall performance perceived by a routing protocol can be poor.

A MAC protocol aims to provide medium access opportunities to nodes sharing the same medium, given any condition of traffic load, interference, noise, and topology of a network. However, traffic load, interference, and so on are closely related to a routing protocol. Thus, the performance of a MAC protocol can be significantly impacted by a routing protocol.

In order to achieve the best network performance, routing and MAC must be jointly optimized.

9.4.1 Methodology of Routing/MAC Cross-Layer Design

Routing/MAC cross-layer can be done in a simple loosely coupled scheme as follows. A routing protocol collects information in the MAC layer, such as link quality, interference level, or traffic load information, to determine the best routing path. Such a method can only achieve a limited performance gain, since the MAC layer is considered but not optimized accordingly.

In order to optimize the performance of routing and MAC protocols together, the working mechanisms of a MAC protocol must be explored and optimized as part of the tasks of routing/MAC cross-layer design.

It is well known that a MAC protocol can be reservation based or random access based. For a random access based MAC, no mechanism is available to fine tune the MAC layer performance by considering information from the upper layer. Instead, a node just tries its best to access the medium. Such a MAC has the great advantage of simplicity and has another advantage of being decoupled from upper protocol layers. However, the shortcoming is that the MAC itself has low performance and routing protocol can even have worse performance since there is no opportunity for cross-layer optimization. Such a problem reflects one of the many issues of applying a CSMA/CA MAC protocol to WMNs. There are two possible solutions to this problem. One is to modify the random access protocol so that it becomes closer to a reservation protocol. For example, 802.11e hybrid channel access control includes a mechanism for scheduling and reservation, which makes CSMA/CA works similarly to a reservation based protocol. The other solution is to have overlaying protocols. For example, we can develop a TDMA protocol overlaying CSMA/CA [256].

Because of the limited capabilities of MAC/routing joint optimization for a random access network, we start to focus on cross-layer design between a routing protocol and a reservation-based MAC protocol. Although today's WMNs are still mostly based on CSMA/CA-type random access MAC, more and more WMNs are starting to use reservation based MAC. One reason is that many existing multihop wireless networks are being standardized under the framework of TDMA. Typical examples include 802.16 mesh networks and relaying networks, UWB mesh networks, WiMedia mesh networks, etc. Another reason is that the poor performance of CSMA/CA for WMNs has motivated the development of better

MAC protocols overlaying CSMA/CA. With such an enhancement, the overall MAC works approximately as a reservation based MAC.

A reservation based MAC protocol is usually concerned with scheduling packet transmissions with respect to properly assigned resources. Thus, the critical task in such a MAC is resource allocation considering constraints such as QoS, interference, network topology, etc., which are all related to a routing protocol. The network resources can be time slots, CDMA codes, channels, and so on. In order to have optimal resource allocation, the routing path and resource allocation can be determined in the same algorithm. This algorithm can be split into suboptimization problems in both MAC and routing layers or can be merged into one protocol layer: either MAC or routing.

Joint optimization between time slot (or code) allocation and routing has been reported in QoS routing of multihop wireless networks as discussed in Chapter 4. In WMNs, a router is usually powerful enough to operate using multiple channels or even multiple radios. Such a capability adds a new dimension of resource allocation, and thus a new joint optimization scheme is needed between channel allocation and routing path.

9.4.2 Joint Channel Allocation and Routing

Channel allocation depends on how traffic is distributed in the network, which is determined by routing. However, given the same routing paths, different channel allocation will also result in different network performance. Thus, joint optimization between channel allocation and routing protocol is an important topic for WMNs. As of today, some research papers have reported solutions to this optimization problem. While most of them are focused on the optimization algorithm [16, 249], a few other papers have proposed practical protocols [222].

Joint Channel Allocation and Routing Protocol

Hyacinth considers channel assignment together with routing for WMNs. It assumes that traffic aggregated at mesh routers only goes to, or comes from, the gateway nodes. With such an assumption, spanning trees are built up from gateway nodes to all nongateway nodes. For each end-to-end traffic flow, the routing path is found along spanning trees such that load balancing is considered. After a routing path is set up, channels are assigned to NICs on each node via a local channel allocation scheme. Thus, Hyacinth consists of the following major functions: load-balancing routing and distributed load-aware channel assignment.

Load-balancing routing The key step of load-balancing routing is to construct the routing tree. When a tree is being built up, the routing metric takes into account traffic load along the tree. Thus, a routing path based on such a tree will achieve load-balancing.

A node periodically broadcasts its reachability information to the wired network via an *Advertise* packet to its one-hop neighbors. At the beginning, only the gateway nodes can send an *Advertise* packet. However, as a spanning tree is gradually built up, other nongateway nodes can send such a packet. After Node A sends an *Advertise* packet, one of its neighbors, e.g., Node B, that receives such a packet can join Node A in two cases. One is that Node B does not have a path to the wired network. The other is that the cost in Node B's path to the wired network is higher than the new path. To join Node A, Node B sends a *Join* message to Node A. Once Node A gets the *Join* message, it adds Node B in its children list and sends an *Accept* message to Node B with information about channels and the IP address to forward traffic from Node B to Node A. In this case, Node B should inform its old parent, e.g., Node C, that it will leave Node C by sending a *Leave* packet. When Node C gets the *Leave* packet, it will tell all its upstream nodes to the wired network to remove the forwarding entry pointing to Node B and its children. After *Join/Accept/Leave*, Node B also starts to send an *Advertise* packet to continue the tree construction process.

When a tree is built up, the routing metric, i.e., the cost to the wired network, is an important parameter that determines the load-balancing performance of the routing protocol. In Hyacinth, the following metrics are considered.

- *Hop count.* This is the number of hops from a node to the wired network.
- *Gateway link capacity.* This is the residual capacity of the uplink that connects the root gateway of a tree to the wired network.
- *Path capacity.* This is the minimum residual capacity on the path from a node to the wired network.

The gateway link capacity and path capacity are dynamic depending on the interactions of multiple nodes. Thus, route flaps can occur and result in nonconvergent network behavior. In order to avoid such an issue, when a new node joins a tree, the *Join* message should propagate all the way back to the gateway node to check whether the join is acceptable. If not, the new node cannot join the tree. Although this scheme can avoid route flaps, the whole process is complicated and can slow and cause more overhead to the routing protocol.

Distributed load-aware channel assignment Given a routing path, the channels in all nodes along this path need to be assigned. In any multiradio network, channel allocation in a node usually impacts channel allocation on other nodes, which is called the channel dependency issue. In order to resolve such an issue, two sets of NICs are specified for each node: Up-NICs and Down-NICs. Channel allocation at a node is only performed on Down-NICs, and Up-NICs use the same channels as those in the Down-NICs of its parent node.

Based on such an architecture, channel allocation is started from the root of a routing path up to the final node. Given a node on the routing path, before the channels on Down-NICs are allocated, the per-channel load information is collected. For each NIC, the channel with least load is selected. The load of a channel is estimated by summing the traffic load contributed by all interfering neighbors.

In order to give more bandwidth to nodes closer to the root of a tree and also not to impact the channel allocation in parent, nodes, higher priority is given to parents, nodes when channel assignment is performed. Thus, when a node searches for a channel, it is restricted to those channels that are not used by interfering neighbors with a higher priority.

Issues in Hyacinth Simulation study shows that Hyacinth can significantly improve throughput. Experiments based on a prototyping system also illustrate that Hyacinth is fast in routing path recovery. However, the joint routing and channel assignment scheme still contains the following shortcomings.

- *The Hyacinth protocol totally depends on spanning trees.* The validity of such a scheme depends on an assumption that the traffic of all nodes goes to the gateway nodes or comes from gateway nodes. For other traffic patterns, the protocol does not work anymore.

- *Channel dependency problem still exists in all children nodes and nodes in the same level.* When a node's Down-NICs are updated with new channels, the channel allocation in all its children nodes and nodes at the same level of the spanning tree have to be updated too.

- *Channel allocation may not be convergent.* Channel allocation can be started by any nodes owing to the distributed method. Although priority is given to parent nodes, priority for nodes in the same level on the spanning trees is the same. Owing to the uncoordinated allocation of nodes with the same priority, their channel assignment may not be convergent, and thus may cause severe interference among nodes.

- *Channel assignment and load-balancing routing may be inconsistent.* Channel assignment is performed based on a routing path established considering load-balancing. However, when channels are reassigned for different nodes on the routing path, the actual load along this routing path, and also the capacity in other links, will be changed. Thus, although load-balancing routing and channel assignment are decoupled in Hyacinth, it does not mean that the two functions will produce consistent results. In other words, when channel assignment is done, the routing path may have lost the advantage of load-balancing.

- *Traffic load estimation does not necessarily reflect the actual traffic load.* This is because MAC-layer contention cannot be accurately captured by weighted summation.

9.4.3 Advanced Features and Challenges

In a single-channel WMN, resource allocation can be done as it is in the framework of QoS routing. It should be noted that the resource at the MAC layer is not fixed. It can be variable owing to the variation of channel quality and the changing parameters in the physical layer. Such variations result in fluctuations of link capacity, which is usually regulated by a rate control algorithm. Thus, a WMN is usually a multirate system.

Since the transmission rate is not just related to link quality, it also impacts the transmission range (and thus the topology), interference, etc. As a result, rate control is coupled with both resource allocation and routing. How to carry out joint optimization among resource allocation, rate control, and routing is still an open research topic.

When multichannel operation is also considered, the above problem becomes even more sophisticated. Thus, joint optimization among channel allocation, rate control, resource allocation, and routing becomes one of the most difficult problems for routing/MAC cross-layer design.

9.5 Transport/Physical Cross-Layer Design

In a multihop wireless network, the capacity of a link is usually variable owing to factors such as interference, time-varying channel quality, fading, and so on. Without a fixed capacity in these links, an end-to-end transmission mechanism, i.e., a transport layer protocol, needs to be optimized by considering the varying link capacity. This motivates the need of cross-layer design between transport layer protocol and physical layer techniques.

Transport layer protocol can be simple or complicated, depending on what services need to be provided at the transport layer. The two most well-known transport layer protocols are TCP and UDP. For UDP, the mechanism is very straightforward: a source node just sends its desired traffic rate without considering what will happen on the intermediate nodes and links from itself to the destination node. TCP works significantly differently. A source node needs to adaptively adjust its transmission rate according to the congestion condition in the network. The congestion can be real congestion on a certain link or poor quality in a link.

Because of different transport mechanisms in TCP and UDP, their impact on the overall performance of the network is quite different. UDP does not obey any rule for controlling traffic rate at the transport layer. Thus, in order to improve the overall network performance, the source rate has to be regulated by other mechanisms such as connection admission control or end-to-end rate control. Owing to the variable link capacity, these control algorithms must be cross-optimized with the physical layer. Thus, the cross-layer design between UDP and the physical layer becomes a problem of joint optimization between the physical layer and admission control or rate control.

On the other hand, for a TCP protocol, a congestion control algorithm must exist to regulate the source rate. Thus, cross-layer design between TCP and the physical layer is a problem of joint optimization between the congestion control algorithm of TCP and different physical layer parameters.

In the remaining part of this section, we focus on the scenario of TCP and physical layer joint optimization.

Cross-layer design between TCP and the physical layer for a multihop wireless network has been researched for years. Different methods in the literature can be classified into two categories. In the first category, the congestion control algorithm of TCP is optimized by considering the information collected from the physical layer. One example is to use the physical layer information to differentiate packet loss due to congestion from that due to link quality related loss. This kind of optimization can only achieve limited performance improvement, because the interaction between TCP and the physical layer is not considered. However, when a link is congested, the physical layer can adjust its parameters, e.g., transmit power, to avoid congestion, which will also help TCP achieve better performance. Similarly, when a link experiences low quality, the physical layer parameters such as coding rate or transmit power can be adjusted to enhance the link quality. Thus, instead of passively taking action only in TCP, TCP and physical layer control schemes can be jointly optimized. Such schemes belong to the second category of cross-layer design between TCP and the physical layer. By contrast with the first category, this involves more complicated algorithms and also more sophisticated protocols and their implementation. Because of such challenges, many research issues remain unresolved.

Congestion control mechanisms have been analyzed as distributed algorithms that solve the network utility maximization problem [179, 181]. For the physical layer, as more advanced technologies are developed, its control becomes more and more complicated, especially when cross-layer design is involved. Thus, the key tasks of joint optimization between congestion control and the physical layer are twofold: one is to extend the existing congestion control optimization algorithm to embrace the physical layer factors, and the other is to determine what parameters need to be controlled in the physical layer and also to optimize such parameters together with congestion control.

There have been many variants of TCP, such as Tahoe, Reno, Vegas, etc. However, the congestion control mechanisms of all of them follow the same rule: the transmission rate of each source is adjusted based on implicit or explicit feedback of congestion signals generated by active queue management (AQM). Some of them use loss as a congestion signal, while others use delay. Since a delay-based congestion signal relates to good properties of convergence, stability, and fairness [179], it is favored by many existing congestion control algorithms. TCP Vegas is one of the congestion control algorithms that use delay-based congestion signal. If d_s is the propagation delay from a source to its destination and D_s is the delay of both propagation and congestion-induced queuing delay, then the TCP window w_s needs to be updated by considering the difference between these two parameters, more specifically, the difference of the expected rates w_s/d_s and w_s/D_s. D_s is measured based on the timing information in acknowledgment (ACK) packets. Thus, the sliding window of TCP Vegas can be updated as follows:

$$w_s(t+1) = \begin{cases} w_s(t) + \dfrac{1}{D_s(t)}, & \text{if } \dfrac{w_s(t)}{d_s} - \dfrac{w_s(t)}{D_s(t)} < \alpha_s \\ w_s(t) - \dfrac{1}{D_s(t)}, & \text{if } \dfrac{w_s(t)}{d_s} - \dfrac{w_s(t)}{D_s(t)} > \alpha_s \\ w_s(t), & \text{else} \end{cases} \tag{9.2}$$

where α_s is a parameter that controls the congestion level and also impacts the stable transmission rate.

The physical layer has many parameters to be controlled. The most well-known ones include transmit power, coding, and modulation. Other parameters include antenna direction, beam forms, etc. Thus, it is difficult to have one control mechanism that covers the optimization of all such parameters. A more practical scheme is to focus on one or two parameters in the control mechanism and assume others fixed. For example, in [57] power control is considered as the main mechanism for fine-tuning the physical layer performance. Below we discuss how joint optimization between TCP congestion control and physical layer power control can be done [57].

Joint TCP Congestion Control and Power Control

This can be formulated as a problem of optimizing users' utility with respect to the transmit power and users' source rate.

For a source s, suppose its rate is x_s and its utility is $U(x_s)$. Thus, for all sources, the overall utility is $\sum_s U_s(x_s)$.

Looking at a link l, its capacity c_l is determined by its transmit power, the noise, and other users. Suppose the power levels of all nodes are denoted by a vector $\mathbf{P}$, then we have [57]

$$c_l(\mathbf{P}) = \frac{1}{T}\log(1 + K\mathrm{SINR}_l(\mathbf{P})), \tag{9.3}$$

where T is the symbol period, K is a constant depending on BER and modulation, and SINR_l is the signal-to-interference-noise ratio. Usually $K = -\phi_1/\log(\phi_2(BER))$, where ϕ_1, ϕ_2 are constants depending on modulation. Considering a CDMA-like system and denoting G_{lk}

as the path gain from the transmitter of link l to the receiver of link k, then SINR_l can be described as $P_l G_{ll}/(\sum_{k \neq l} P_k G_{lk} + n_l)$, where n_l is the noise at the receiver of link l. Given a link l, all traffic passing through it cannot exceed its capacity $c_l\mathbf{P}$. If the set of links on the routing path of source s to its destination is $L(s)$, then link l is subject to a constraint of $\sum_{s:l \in L(s)} x_s \leq c_l(\mathbf{P})$.

As a result, joint congestion control and power control needs to find an optimal solution of rate $\mathbf{x} = x_1, x_2, \ldots$ and power $\mathbf{P}$ such that the overall utility is maximized, i.e., the cross-layer optimization can be formulated as follows [57]:

$$\begin{aligned} &\text{maximize} \quad \sum_s U_s(x_s) \\ &\text{subject to} \quad \sum_{\substack{s:l \in L(s) \\ (\mathbf{x},\mathbf{P}) \geq 0}} x_s \leq c_l(\mathbf{P}), \forall l. \end{aligned} \tag{9.4}$$

As shown in this optimization problem, the optimization of congestion is performed not only over source rate but also over transmit power level, which is very different from an Internet congestion control algorithm. The above joint optimization scheme makes several assumptions in the network protocol. Firstly, the physical and MAC layers work as a CDMA system. Secondly, the routing path is assumed to be single-path and is predetermined. Lastly, the coding rate and modulation types are also assumed to be fixed.

To derive a concrete solution, in [57] delay-based congestion signal and TCP Vegas sliding window update are considered. More specifically, the utility function can be further described as $U_s(x_s) = \alpha_s d_s \log(x_s)$, where α_s is a parameter used in TCP Vegas sliding window update. The window update procedure has been described in (9.2). With these two specific considerations, the solution to the joint optimization problem in (9.4) can be derived with the following results [57].

- *Update of sliding window and transmission rate.* The window is updated according to (9.2), and transmission of source s at time t is

$$x_s(t+1) = \frac{w_s(t+1)}{D_s(t)}, \tag{9.5}$$

where $D_s(t)$ is the total measured end-to-end delay at time t.

- Update of transmit power. The transmitter of link l updates its power as follows:

$$P_l(t+1) = P_l(t) + \frac{k\lambda_l(t)}{P_l(t)} - k \sum_{j \neq l} G_{lj} m_j(t), \tag{9.6}$$

where $k > 0$ is a constant. $m_j(t)$ is the information sent from transmitter j and is measured locally at j according to

$$m_j(t) = \frac{\lambda_j(t)\text{SINR}_j(t)}{P_j(t)G_{jj}}, \tag{9.7}$$

and $\lambda_j(t)$ is a weighted queuing delay [180] at the transmitter j, i.e.,

$$\lambda_j(t+1) = \left[\lambda_j(t) + \frac{\gamma}{c_j(t)}\left(\sum_{s\ j \in L(s)} x_s(t) - c_j(t)\right)\right]^+, \tag{9.8}$$

where γ is a positive constant.

Discussions on the Algorithm

Based on these results, we know that the proposed cross-layer optimization algorithm can be implemented in a distributed way. However, it should be noted that nodes need to flood the information of $m_j(t)$. Also, the measurement of $m_j(t)$ depends on SINR measurement on each node and the measurement of path gain. Owing to stochastic characteristics, these parameters may not always be measured accurately. Thus, the robustness of the above algorithm to the fluctuations of these measured parameters needs to be studied. It has been proved in [57] that the proposed joint congestion control and power control algorithm is robust to parameter perturbation and the convergence can be achieved at a geometric rate. It also has a nice property of global convergence to the optimal solution $(\mathbf{x}^*, \mathbf{P}^*)$. Graceful tradeoff between algorithm complexity and performance improvement can be achieved too.

However, the joint congestion control and power control optimization algorithm is limited to the scenario where several assumptions must be satisfied.

First of all, coding and modulation are fixed; otherwise, the optimization algorithm needs to determine the optimal selection of coding rates and modulation schemes. For some multihop wireless network, in particular some low rate networks, this assumption is reasonable. However, for WMNs that are usually concerned with high speed transmission, the physical layer is always expected to adaptively adjust coding rate and modulation. Such work is usually performed in a rate control algorithm in the MAC layer. However, because of the change of rate, the parameters such as transmit power and link capacity change too. Thus, joint optimization between TCP and physical layer needs to consider variable coding and modulation.

The function that models the relationship between link capacity and power control may be different in many WMNs. For CDMA-based WMNs, this model works fine. However, many WMNs are not based on CDMA, but TDMA or random-access. For these WMNs, SIR is very small when multiple nodes send packets simultaneously. Although the capture effect helps some nodes receive correct packets even under interference, an interfered node usually cannot send or receive correct packets. Thus, fine-tuning power does not have significant impact on the link capacity. In other words, joint power control and congestion control will not achieve optimal throughput performance. For such WMNs, the more critical task is to carry out joint optimization between congestion control and scheduling in the MAC layer, as will be discussed in the next section.

In the joint congestion control and power control algorithm, the routing path is assumed to be fixed. In fact, when congestion occurs, another well-known mechanism is to find a better routing path so that congestion is avoided. Such a mechanism can be achieved through multipath routing or load-balancing routing. This proves that cross-layer design between transport layer and physical layer is not enough and can inevitably involve routing protocol. Such issues will also be discussed in the following section, but we have noticed that, so far, no effective solutions are available for providing joint optimization across all protocol layers.

9.6 Joint Optimization Algorithms across Multiple Protocol Layers

For a multihop wireless network like WMN, design of the entire protocol stack can be formulated as one optimization problem. We call this approach "full-optimization design".

The solution to this problem can be mapped across different protocol layers in a clean state protocol architecture. Such an approach can achieve a layered design or loosely coupled cross-layer design, since the interactions between layers are small owing to optimization throughout the protocol stack. However, the shortcoming is that the protocol layers derived from optimization may not exactly match an existing protocol stack such as the Internet. In order to avoid such an issue, another approach is to formulate an optimization problem considering the existing protocol architecture. Thus, it is just a "suboptimization design". A solution to this problem provides no help in reducing interactions between protocol layers, but can significantly improve performance by optimizing cross-layer interactions.

Cross-layer optimization can be formulated across different protocol layers ranging from the application layer to the physical layer. For example, the cross-layer design in the previous section illustrates the cross-layer optimization between physical layer and transport layer. However, in WMNs or a multihop wireless network in general, the most typical cross-layer optimization is joint optimization of congestion control and scheduling. In a multihop wireless network, congestion control can be done end to end in transport layer or link by link in the MAC layer, while scheduling involves the close interactions between MAC and physical layer. Scheduling determines parameters for both MAC and physical layers and depends on the congestion control to determine a best transmission rate. The interactions between congestion control and scheduling also involve the routing protocol. Thus, a well-defined joint optimization between congestion control and scheduling can enhance performance optimization in layers including transport, routing, MAC, and physical layers.

9.6.1 Joint Optimization of Congestion Control and Scheduling

A network user usually expects to get as many resources as possible from the network. When multiple users are considered, and if no arbitration is enforced, they can be easily in a situation where none of them can really get satisfactory service quality. A conventional solution to this problem is to use transport layer protocol to perform congestion control, routing protocol to find the best path considering load balancing, and MAC protocol to schedule transmissions with the objective of achieving best one-hop performance. However, such a scheme cannot achieve optimal performance, because the algorithms in the different protocol layers are not optimized altogether. In other words, the network is not really optimized with the objective of satisfying as many users as possible.

To improve the network performance, joint optimization between transport, routing, MAC, and physical layer is needed. Such an optimization should be performed with the aim of maximizing users' interests. Since transport is mostly concerned with congestion control, and MAC/physical layer is concerned with scheduling, algorithms on joint congestion control and scheduling provide a promising approach to optimizing network performance so as to maximize the benefits to networks users.

In a joint congestion control and scheduling algorithm, transport layer protocol is considered in the congestion control part, MAC and physical layers are considered in the scheduling part, and routing is embedded in the interactions between congestion control and scheduling. The optimization target of such an algorithm is to maximize users' benefits as defined by utility functions. With this mind, we will discuss how the algorithm of joint congestion control and scheduling is formulated in the next subsection.

Formulations

To formulate joint optimization between congestion control and scheduling, we need to define two models that capture the behaviors of congestion control and scheduling. The objective of congestion control is to find each user's rate such that the utilities of all users are maximized under the condition that the network system can be stabilized by a particular scheduling scheme. Thus, the objective of scheduling is to design a scheduling policy such that the given rate of each user is satisfied in a stable system.

Assume that there are K users in the network. Given a user k, its traffic originates from source node s_k and d_k has a rate of r_k. We assume the rate r_k is upper-bounded by M_k. The utility of user k is a function of rate, i.e., it is $U_k(r_k)$. Thus, the congestion control and scheduling must achieve the following joint optimization

$$\begin{aligned} \max_{r_k < M_k} \quad & \sum_k U_k(r_k) \\ \text{subject to} \quad & \vec{r} \in \Lambda. \end{aligned} \tag{9.9}$$

where $\vec{r} = [r_k, k = 1, \ldots, K]$ is a vector of all users' rates. Λ stands for the capacity region or the rate region that contains the set of all rate vectors for which a scheduling scheme can be found to stabilize the network. Thus, the congestion control and scheduling are cross-related via this capacity region. For example, given an optimized rate vector, what scheduling scheme can be used is also constrained. On the other hand, the set of all available scheduling schemes also constrains the best rate vector in (9.9). It should be noted that in (9.9) the overall utility of the entire network is considered via summation of all users' utilities. However, more sophisticated methods of integrating different users' utility functions can be considered too.

To solve the optimization problem in (9.9), the first step is to derive the capacity region Λ. Two schemes can be used to define the capacity region: node-centric capacity region and link-centric capacity region.

Node-Centric Capacity Region and Optimal Solution

We consider a network with N nodes, and links between these nodes are represented by the set $\mathcal{L} = \{(i, j), i, j = 1, \ldots, N, i \neq j\}$. The capacity of each link (i, j) is c_{ij}. In order to ensure that users' rates fall into a stable capacity region, the incoming and outgoing traffic rate on each node must be balanced. Based on such a concept, the node-centric capacity region can be derived. Denote c_{ij}^d as the link capacity used by traffic toward destination d on link (i, j). Thus, a user rate vector belongs to the capacity region if and only if the following constraint is satisfied [200, 250]:

$$\sum_{j:(i,j)\in\mathcal{L}} c_{ij}^d - \sum_{j:(j,i)\in\mathcal{L}} c_{ji}^d \geq \sum_{k:s_k=i,d_k=d} r_k \text{ for all } i \text{ and all } d, \text{ and } i \neq d,$$

$$r_{ij}^d \geq 0 \text{ for all } (i, j) \in \mathcal{L} \text{ and for all } d. \tag{9.10}$$

Considering that the capacity set of all links is $\mathcal{C}$, since the capacity of all links $\vec{c}$ cannot lie outside the convex hull of $\mathcal{C}$, we need to consider a second constraint for the capacity region:

$$\left[\sum_d c_{ij}^d \in Co((C))\right] \tag{9.11}$$

To further consider the impact of the physical layer, the capacity of each link is related to a few other factors such as power control, modulation, coding, rate control, and so on. Thus, the capacity of all links is $\vec{c} = \mathcal{F}(\vec{P})$, where $\vec{P}$ is a vector representing all physical layer parameters. If the set of all feasible physical layer parameters is Π, then the capacity set of all links is $\mathcal{C} = \{\mathcal{F}(\vec{P}),\ \vec{P} \in \Pi\}$. Although the function $\mathcal{F}$ is usually nonconvex, the hull of $\mathcal{C}$ is convex and also closed and bounded. Thus, the capacity region Λ is a convex set. The optimization problem of (9.9) can be solved with the help of Lagrange multiplier q_i^d for a constraint for each (i, d) in (9.10). Thus, the joint congestion control and scheduling problem is decomposed into the following two subproblems.

- *Congestion control.* The data rate of each user is

$$r_k(t) = \operatorname*{argmax}_{0 \le r_k \le M_k} [U_k(r_k) - x_k q_{s_k}^{d_k}(t)]. \tag{9.12}$$

- *Scheduling.* The transmission rate on each link is

$$\vec{c}(t) = \operatorname*{argmax}_{\vec{c} = \mathcal{F}(\vec{P}), \vec{P} \in \Pi} \sum_{(i,j) \in \mathcal{L}} c_{ij} \max_d (q_i^d(t) - q_j^d(t)). \tag{9.13}$$

  The relationship between $\vec{c}(t)$ and $\vec{c}^d(t)$ is then established as follows. For each link (i, j), define $d^*(i, j) = \text{argmax}_d (q_i^d - q_j^d)$, then

$$c_{ij}^d(t) = \begin{cases} c_{ij}(t) & \text{if } d = d^*(i, j), \\ 0 & \text{otherwise.} \end{cases} \tag{9.14}$$

  Thus, such a relationship also specifies the links that the traffic toward destination d shall take. This means that the routing mechanism is embedded in the scheduling subproblem. As shown in (9.14), the same source may follow multiple routing paths to its destination. Thus, the above derivation has an implicit assumption of using multipath routing in the joint optimization problem.

To update the user rate and link capacity, the Lagrange multiplier is updated as follows:

$$q_i^d(t+1) = \left\{ q_i^d(t) - h_t \left[c_{ij}^d(t) - \sum_{j:(j,i) \in \mathcal{L}} c_{ji}^d(t) - \sum_{k: s_k = i, d_k = d} r_k(t) \right] \right\}^+, \tag{9.15}$$

where h_t, $t = 1, 2, \ldots$ is a sequence of positive step sizes. It has been proved in [172] that if $h_t \to 0$ as $t \to \infty$ and $\sum_t h_t = \infty$, then a unique optimal solution $\vec{r}^*$ can be found for the joint congestion control and optimization problem.

Link-Centric Capacity Region and Optimal Solution

The link-centric capacity region can be derived by considering the balanced traffic load on each link. In order to know how each user contributes to the traffic on a link, a routing matrix has to be specified for each user on each link. If the traffic of user k passes through link (i, j), then the routing index for this user on this link, denoted by H_k^{ij}, is 1; otherwise, $H_k^{ij} = 0$.

Thus, user rate vector $\vec{r}$ lies in the capacity region Λ if and only if

$$\sum_{k=1}^{K} H_k^{ij} r_k \leq c_{ij} \quad \text{for all } (i,\ j) \in \mathcal{L},\ \vec{c} \in Co(\mathcal{C}). \tag{9.16}$$

To consider the physical layer impact on the link capacity, the same relationship between $\vec{c}$ and physical layer parameters $\vec{P}$ as that for the node-centric capacity region can be used. The solution to the joint congestion control and scheduling optimization problem can be derived in a similar way to the node-centric case, i.e., joint congestion control and scheduling is decomposed into the following two components.

- *Congestion control component.* The data rate of each user is

$$r_k(t) = \text{argmax } 0 \leq r_k \leq M_k \left[U_k(x_k) - x_k \sum_{(i,j)\in\mathcal{L}} H_k^{ij} q_{ij}(t) \right]. \tag{9.17}$$

- *Scheduling component.* The transmission rate on each link is

$$\vec{c}(t) = \underset{\vec{c}=\mathcal{F}(\vec{P}),\vec{P}\in\Pi}{\text{argmax}} \sum_{(i,j)\in\mathcal{L}} c_{ij} q_{ij}(t). \tag{9.18}$$

The Lagrange multiplier is updated as follows:

$$q_{ij}(t+1) = \left[q_{ij}(t) - h_t \left(c_{ij}(t) - \sum_{k=1}^{K} H_k^{ij} r_k \right) \right]^{+}, \tag{9.19}$$

where h_t, $t = 1, 2, \ldots$ is a sequence of positive step sizes.

Comparisons

As shown in derivations, there exist several key differences between node-centric and link-centric joint congestion control and scheduling optimization [173].

The first difference lies in how routing is handled in the joint optimization problem. In the node-centric scheme, the routing protocol, assumed to be multipath routing, is considered in the scheduling component. In the link-centric scheme, the routing path is predetermined, so no routing protocol is actually considered.

The traffic model reflects the second difference. In the link-centric scheme, the balance equation has an implicit assumption that the traffic on different links on the routing path is the same. This is only true when a user's traffic is constant or there is no delay in delivering traffic. However, there is no such assumption in the node-centric scheme. In this sense, the node-centric scheme has a more accurate traffic model.

In addition to the differences, both schemes share some similarities. Both schemes assume a centralized optimization algorithm. However, when we come across a wireless multihop network like WMN, a distributed scheme is needed. How to map these two schemes into a distributed scheme is not self-explained in the derivations and needs further research. In addition, both schemes can take into account various physical layer characteristics such as channel variations in the scheduling component.

9.6.2 Limitations of Cross-Layer Optimization Algorithms

Perfect Versus Imperfect Scheduling

In the scheduling component of the joint congestion control and scheduling optimization problem, the optimal solution may be difficult to derive for two reasons. One is that the function $\mathcal{F}$ for the relationship between link rate and physical layer factors is usually concave. The other is that the Lagrange multiplier changes every time period, which implies that the scheduling must be updated per one time period. These two problems result in a very high complexity in the scheduling scheme and render the optimization algorithms nearly useless in practical implementations. In order to lower the complexity, the following two approaches can be taken.

In the first approach, the optimization algorithm is applied to a simple network model. For example, in an infrastructure network like a typical wireless LAN setup, an optimal schedule can be achieved with polynomial-time complexity. For a node-exclusive interference model where only two nodes can communicate at the same time, an optimal schedule can also be achieved with low complexity. An example of this case is a Bluetooth network. However, this approach is not applicable to WMNs, since the network model is very different from that of WMNs.

In the second approach, we have to relax the optimality requirements of the scheduling problem. The scheduling with such relaxed requirements then becomes an imperfect scheduling scheme. The capacity region that can be achieved is thus smaller than that of perfect scheduling. However, due to relaxed requirement, the complexity of the scheduling scheme is much lower and can be realized in a distributed way. Imperfect scheduling and its impact to cross-layer optimization is studied in detail in [174].

Implementation Issues

Besides complexity, the cross-layer optimization algorithms also have several other critical issues.

When coming to the applicability of cross-layer optimization algorithms, the first question we have to face is how to map the algorithms onto the existing protocol stack. For example, WMNs are usually built based on an Internet protocol architecture, in which a variant of the TCP protocol is applied to control network congestion, the MAC protocol varies as different physical layer technologies are used, and different types of routing protocol can be used. Unless we use a totally clean-slate protocol architecture, we have to consider the necessary modification to formulation of the cross-layer optimization algorithm.

In the joint congestion control and scheduling algorithm, the MAC layer is assumed to be schedulable. In fact, some MAC layer protocols are totally random. A typical example is the CSMA/CA protocol, which is widely accepted as the basic MAC for IEEE 802.11 wireless networks. For such random MAC protocols, scheduling the transmission rate for each link cannot be easily achieved. Thus, to develop a stochastic scheduling scheme so that the optimal rate of each link can be achieved is a challenging problem. Another approach that we can take is to design another better coordinated MAC overlaying the random MAC [256, 257], and then the optimal scheduling is performed on the overlaying MAC protocol.

Between MAC and physical layer, another difficult problem is how to accurately model the relationship function between the two layers. This is even more challenging for WMNs, since the physical layer usually contains many advanced physical layer technologies such as smart antenna, MIMO, adaptive coding/modulation, adaptive power control, multichannel operation, etc.

The existing cross-layer optimization schemes have not taken into account the QoS requirements by users. In the previous subsection, the joint congestion control and scheduling algorithms only achieve the optimal rate for each user. However, the user usually does not care about which user rate they have to obey so that the entire network achieves the best performance. Instead, what they care about is their QoS specifications. For example, they may demand a traffic rate that is not an optimal solution of the cross-layer optimization, but this has to be satisfied in order to guarantee their QoS. In this case, the cross-layer optimization problem needs to have a new formulation.

As shown in the joint congestion control and scheduling algorithms, the routing protocol is not considered in a proper way. More specifically, the connectivity of a routing path is not ensured in these algorithms. No matter how a routing protocol is assumed (either multipath routing or predetermined routing), we need to make sure that the routing path for a given user is connected; otherwise, such a routing mechanism makes no sense. In other words, the optimal solutions derived on the basis of such a routing protocol is not useful in practical implementations.

In view of the above issues, we believe that cross-layer optimization will continue to be a challenging research topic for WMNs.

9.7 Prudent Use of Cross-Layer Design

As shown in previous sections, there is no doubt that cross-layer design can improve network performance. However, issues can come together with such benefits, as explained below.

- *System complexity.* Many cross-layer design schemes can be easily shown to achieve great performance by using simulations or even prototypes. However, when it comes to the actual implementation of these schemes, we will find complexities of modifying protocols in different layers. These modifications can impact the maintainability of the software, stability of the different protocol modules, and flexibility of porting codes to different platforms.

- *Protocol interoperability and compatibility.* With cross-layer design, the standard working mechanism in the protocol stack is broken. Thus, a wireless network with cross-layer design may well be incompatible with other networks, and thus interoperation between different networks is hard to maintain. Consequently, a cross-layer design scheme should have a remedy for standard compatibility. However, it can be imagined that, even if interoperation can be maintained via such a remedy, the benefits of cross-layer design may diminish when networks with and without cross-layer design have to work together.

- *Evolution capability.* In a layered protocol architecture, protocols in one layer can evolve separately without disrupting the functionalities of protocols in another layer. When cross-layer design is adopted, any upgrade or change in protocols must be coordinated among different protocol layers. This requirement significantly limits the capability of product evolution.

It should be noted that such issues usually do not exist in a layered design scheme. To avoid such issues, tradeoff should be made between performance improvement and loss of the advantages of layered design. However, technically it is extremely difficult to carry out a reasonable tradeoff since issues such as system complexity or protocol interoperability are not easy to evaluate quantitatively. Thus, here we suggest several rules that can be followed to avoid blind use of cross-layer design.

- *Achieve enough margin of performance improvement.* Cross-layer design brings network performance improvement with the price of high system complexity. Thus, to compensate the cost, the performance improvement must be sufficiently significant. Multiple performance metrics may need to be considered together to evaluate the overall network performance improvement. In fact, using cross-layer design, we can easily see some performance improvement in throughput, delay, packet loss, etc. However, if the improvement is only a small percent, e.g., 5%, then we may not think it a wise strategy to adopt cross-layer design, since such a performance improvement can easily vanish due to uncertainties in a wireless network such as interference, noise, shadowing, etc.

- *Explore any possible opportunity that can improve network performance using layered protocol design.* For cross-layer design, benefits always come together with issues. Thus, the best strategy is to explore the capability of layered protocol design as much as possible. The theoretical research work on "layering as decomposition optimization" can be used for guidelines in doing so.

- *Carry out cross-layer design without compromising framework specified by standards.* In order to ensure standard compatibility to a large extent and thus to maintain interoperability and evolution capability, it is a good strategy to carry out cross-layer design within the framework of standard specifications.

- *Push standardization of cross-layer design framework and methodology.* To further improve the viability of cross-layer design schemes, standardizing the framework of cross-layer design is necessary.

Moreover, several principles discussed in [143] can be adopted as additional cautionary guidelines for cross-layer design.

- *Take into account dependency graph for the entire protocol stack.* With cross-layer design, protocols become interactive with each other. The interactions can be dependent on each other and cause multiple adaptation loops, which causes performance degradation in protocols not being considered in cross-layer design. To solve this problem, a dependency graph representing interactions between protocols needs to be derived for the entire protocol stack.

- *Timescale separation and stability.* Based on the dependency graph, if a parameter is controlled by two different adaptation loops, timescale separation can be used to avoid conflict. The rationale is that the two entities controlling the same parameter work on a different timescale. Adaptive control theory has proved that stability can be achieved via timescale separation. If they work in a similar timescale, then closed-loop control theory should be used to prove the stability of the given interactions.

- *Avoid unbridled cross-layer design.* If multiple cross-layer interactions are employed, it is easy to get an unstructured spaghetti-like protocol architecture, which is hard to maintain. Also, in this case network performance improvement may be only achievable within a small area of equilibrium state. Away from equilibrium, the network performance can be much worse that would be achieved by a layered protocol design.

These principles can help to avoid unintended consequences of using cross-layer design.

10

Standards on Wireless Mesh Networks

Wireless mesh networks have been envisioned as an important solution to the next generation wireless networking. Currently many standards are being specified for mesh networking technologies in different application areas.

Among the various standards organizations, the IEEE 802 standards committee is the most enthusiastic at promoting wireless mesh networking technology in all its aspects. For example, the IEEE 802 standards committee includes different working groups for personal area network (PAN) based, local area network (LAN) based, or metropolitan area network (MAN) based wireless mesh networks. The standards being specified cover various protocol layers such as MAC, routing, roaming, interworking, advanced physical techniques, and so on. Other standards organizations usually either focus on one protocol layer or do not have a special group dedicated to wireless mesh networking technologies. For example, it is well known that the Internet Engineering Task Force (IETF) has been working on standards for routing protocols for ad hoc networks under the charter of mobile ad hoc networks (MANET). However, it only covers routing protocols for MANET that are not different from WMNs, as we discussed in previous chapters.

In parallel with standards organization, several well-known industry nonprofit organizations are also playing an important role in standardization of wireless LAN/MAN products. For example, the Wireless Fidelity (Wi-Fi) Alliance spends its efforts in certifying wireless LAN products to ensure interoperability between products from different companies. A certified Wi-Fi product should conform to a certain subset of IEEE 802.11 standards.

In this chapter, we focus on standard activities within the IEEE 802 standards committee. Specifications related to WMNs but produced by industry alliances or forums are also presented.

As of today, no standard on WMNs is really available for implementation; finalizing standards is still an ongoing effort. However, drafts of these standards have been released in different working groups and their task groups. In this chapter, we present the latest work on these drafts. However, the process of standardizing WMNs is so complicated that many

Wireless Mesh Networks Ian F. Akyildiz and Xudong Wang

issues in wireless mesh networking have not yet been resolved. Thus, we will also point out potential issues in these standards drafts in this chapter. Suggestions for resolving these issues are also made. It should be noted that our analysis and suggestions only represent our opinions and will not necessarily be considered as a future plan in any standards task groups. However, we hope that our suggestions will provide guidelines to carry out research in WMNs and also stimulate faster progress in the standardization process of WMNs.

10.1 Overview of IEEE 802 Working Groups for Wireless Networks

The IEEE 802 standards committee develops standards for LANs and MANs. Many standards are well known and widely used, for example, Ethernet and wireless LAN. Currently, the active IEEE 802 working groups include 802.1, 802.3, 802.11, 802.15, 802.16, 802.17, 802.18, 802.19, 802.20, 802.21, and 802.22. Except for 802.3 for Ethernet and 802.17 for packet ring, all the other groups are related to wireless networks. More specifically, 802.11, 802.15, 802.16, 802.20, 802.21, 802.22 are different groups with a focus on a separate topic related to wireless LAN/MANs, as explained in Table 10.1. Since the monitoring of, and active participation in, ongoing radio regulatory activities, at both the national and international levels, are so important for the above six working groups for radio based networks, IEEE has a separate technical advisory group, 802.18, with a focus on radio regulation. In addition, coexistence with current and ongoing standards is critical to the success of any standard, there is a separate technical advisory group, 802.19, dedicated to coexistence. Most IEEE 802 standards are focused on MAC and physical layer specifications; issues above these two layers are specified in 802.1. For example, 802 LAN/MAN architecture, internetworking among 802 LANs, MANs and other wide area networks, 802 Security, 802 overall network management, and so on are all specified in 802.1.

As far as WMNs are concerned, only IEEE 802.11, 802.15, 802.16 are actually developing standards for this purpose. Thus, in the following sections, we focus on standards activities on WMNs in these three working groups. Other working groups are only briefly introduced in this chapter.

10.2 Overview of Industry Alliances/Forums for Different Wireless Technologies

There are several well known industry alliances/forums that also critically impact the progress and the future of wireless networking technologies in LAN/MAN areas.

Wi-Fi Alliance certifies products that conform to IEEE 802.11 standards. Products that are manufactured by different companies but have passed certification by Wi-Fi alliance will be capable of interoperating smoothly with each other. Wi-Fi Alliance does not specify standards for wireless LANs, but its efforts at certifying Wi-Fi products strongly support the success of wireless LAN products. Without interoperability, it can be imagined that users would not be willing to use 802.11 products.

Table 10.1 Summary of IEEE 802 standards working groups for radio-based networks

Working group	Objective and focus
802.11	This group is for wireless local area networks. There are more than 24 active task groups for different topics related to wireless LANs. Among them, 802.11s is dedicated to developing standard for meshed wireless LANs
802.15	This group is for wireless personal area networks. There are more than five active task groups for different topics of wireless PANs. Among them, 802.15.5 is dedicated to standardization of mesh PANs
802.16	This groups is for broadband wireless access in a metropolitan area. Several task groups have completed their projects but more than four tasks groups remain active. Mesh mode has been specified in the completed projects and a new task 802.11j is dedicated to mobile multihop relay
802.20	This group specifies physical and MAC layers of an air interface for interoperable mobile broadband wireless access systems, operating in licensed bands below 3.5 GHz, optimized for IP-data transport, with peak data rates per user in excess of 1 Mbps. The supported mobility can be up to 250 km/h in a MAN environment
802.21	This is a media independent handoff working group. It develops standards to support handover and interoperability between 802 heterogeneous networks including both 802 and non-802 networks
802.22	This group targets wireless regional area networks. It is developing a standard for a cognitive radio-based PHY/MAC/air-interface for use by license-exempt devices on a noninterfering basis in the spectrum that is allocated to the TV broadcast service

WiMedia Alliance and the UWB forum are two leading industry organizations that specify radio platforms of high-rate UWB wireless networking. There were efforts in IEEE 802.15.3a to consolidate proposals from these two groups. However, this process has never been successful. Thus, IEEE 802.15.3a is now an inactive task group, and the high rate UWB wireless networking technologies are specified independently in WiMedia Alliance and UWB forum.

The WiMAX Forum promotes and certifies the compatibility and the interoperability of broadband wireless products. Such an effort will support the acceptance of IEEE 802.16 and European Telecommunications Standards Institute (ETSI) HiperMAN wireless MAN standards.

IEEE 802.16 was initially designed for fixed broadband wireless networks. Then the version with mobility, IEEE 802.16e, was developed to extend 802.16 to support mobile users. However, while IEEE 802.16e was being standardized, Korea initiated WiBro, which is somewhat similar to a version of IEEE 802.16e. In product design, WiBro is expected to achieve higher transmission rate and faster mobility than 802.16e, but backward compatibility with IEEE 802.16 products is not its concern. Thus, the issue of interoperability between WiBro and WiMAX cannot be ignored. However, the compelling need of both mobility and broadband wireless access continues to support the acceptance of WiBro by different countries.

There are a few other industry alliances. For example, Bluetooth special interest group (SIG) promotes the Bluetooth technology and ensure compatibility and interoperability of different Bluetooth products. However, we will review all of them here since none of them is closely related to WMNs.

10.3 Standards for Meshed Wireless LANs

802.11 based WMNs have been researched for several years now. Driven by the worldwide acceptance of 802.11 wireless LANs and a huge number of 802.11 nodes deployed in various application scenarios, 802.11 based WMNs are probably the most popular ones. The most common solution to wireless mesh networking using 802.11 is to combine layer-3 ad hoc routing protocol with 802.11 MAC protocol. Many enhancements have been made to both ad hoc routing protocols and the 802.11 MAC protocol so that the performance of WMNs can be as high as possible. However, no standards were specified for 802.11 based wireless mesh network until the establishment of 802.11s standard task group in IEEE.

10.3.1 Overview of IEEE 802.11 Standard Activities

The IEEE 802.11 working groups have been working towards standardization of MAC and physical layer technologies for wireless LANs for many years. Initially, there were two task groups: the MAC task group and the PHY task group. The work of both groups was completed in 1997 and included in IEEE std 802.11, 1997. This version of the standard was updated in 1999. Starting from this initial work, many other topics have been covered since then, for example, QoS, security, management, roaming, dynamic frequency selection, power control, high throughput physical layer technologies, and mesh networking. The IEEE 802.11 working group has established so many task groups that their alphabetical names are almost used up. A complete list of 802.11 task groups, their objectives, and status are shown in Table 10.2 in alphabetical order. The names of 802.11l, 802.11o, 802.11q, and 802.11x are not to be used by IEEE 802.11 working groups for inclusion into the published standard. Currently only 802.11z is left for a future task group. If more task groups are needed, another naming scheme will have to be adopted.

10.3.2 IEEE 802.11s

The traditional setup of 802.11 wireless LANs that the infrastructure of each basic service set (BSS) is connected via Ethernet LANs. Such a fixed network architecture limits the flexibility of network deployment and increases cost. Thus, mobility of BSS and multihop networking are needed.

Starting from the first IEEE 802.11 standard, the ad hoc networking has been specified in the independent basic service set (IBSS) mode. In this mode, stations (STAs) can connect to each other without any central coordinator such as an access point (AP). Moreover, there is no access or connection to the distributed system (DS). Thus, STAs are totally self-contained as an ad hoc network. Such an operating mode has been researched in the field of ad hoc networking. However, it has been realized for a long time, especially in industry, that the

Table 10.2 Summary of IEEE 802.11 task groups and standards

Standards/task groups	Objective and focus	Status
802.11a/TGa	Specify a new physical layer based on OFDM for 5 GHz band to support data rate up to 54 Mbps	Standard approved in September 1999
802.11b/TGb	Specify a higher rate physical layer based on direct sequence spread spectrum for 2.4 GHz band to support data rate up to 11 Mbps	Standard approved in September 1999
802.11c/TGc	Define specific procedures for bridge operation specified in IEEE 802.1D	Completed, part of 802.1D
802.11d/TGd	Define various requirements needed to extend wireless LANs to new regulatory domains	Standard approved in 2001
802.11e/TGe	Enhance 802.11 MAC to improve and manage QoS, provide different service classes, and enhance security and authentication mechanisms	Standard approved in September 2005
802.11f/TGf	Provide recommended practice for inter-AP protocol to ensure interoperability between APs from different vendors	Standard approved in June 2003. Withdrawn
802.11g/TGg	Extend the physical layer capability of 2.4 GHz in 802.11b based on OFDM. In addition to all rates of 802.11b, higher rates up to 54 Mbps are supported.	Standard approved in June 2003
802.11h/TGh	Enhance 802.11 MAC and 802.11a physical layer to support dynamic frequency selection and transmit power control	Standard approved in December 2003
802.11i/TGi	Enhance MAC layer security	Standard approved in June 2004
802.11j/TGj	Enhance 802.11 MAC and 802.11a physical layer to obtain regulatory approval from Japan in 4.9 GHz and 5 GHz bands	Standard approved in 2004
802.11k/TGk	Define radio resource management to provide interfaces to high layers for radio and network measurements	Active, Draft
802.11-Revma/TGm	Maintain 802.11 standards and provide corrections to all 802.11 standards, and consolidate all approved standards	Active, Draft
802.11n/TGn	Improve MAC layer throughput ($>$100 Mbps) based on MIMO technologies. Both MAC and physical layers need to be enhanced	Active, Draft

Table 10.2 Continued

Standards/task groups	Objective and focus	Status
802.11p/TGp	Support communications between vehicles for speed up to 200 km/h for a range of up to 1000 meters in 5 GHz band	Active, Draft
802.11r/TGr	Specify fast BSS transition so that real-time applications, in particular VoIP is supported	Active, Draft
802.11s/TGs	Extend ESS to support meshed wireless LANs. Self-configuration of multihop networking and support of both unicast and multicast are needed	Active, Draft
802.11.2/TGt	Specify a set of performance metrics, measurement methodologies, and test conditions to help measure and predict performance of WLAN devices. Recommended practice standard	Active, Draft
802.11u/TGu	Enhance MAC and physical layers to support interworking with external networks	Active, Draft
802.11v/TGv	Provide wireless network management enhancements to both MAC and physical layers	Active, Draft
802.11w/TGw	Improve security of 802.11 management frames by defining enhancements such as data integrity, data origin authentication replay protection, and data confidentiality	Active, Draft
802.11y/TGy	Standardize mechanisms to allow shared 802.11 operation with other users in 3.65–3.70 GHz band in the USA. 802.11j, 802.11a, 802.11h, will be extended	Active, Draft

IBSS mode is not enough for many interesting application scenarios where ad hoc networking is needed but Internet access and support of client nodes are also necessary. Thus, both infrastructure mode and IBSS mode will be integrated in a new type of multihop network.

To meet the above requirements, wireless mesh networking is needed for 802.11 wireless networks. For years, many companies have developed their proprietary solutions to build up 802.11 based WMNs. Such solutions share several common principles.

- The network usually includes three types of nodes: mesh routers, clients, and gateways.
- An ad hoc routing protocol is implemented in mesh routers to work together with 802.11 MAC. Certain radio aware functions may be included in the routing protocol.
- The 802.11 MAC driver is enhanced in mesh routers to improve multihop performance. Typical examples include fine-tuning CSMA/CA parameters, developing algorithms for multiradio or directional antennas, etc.
- Certain network configurations are needed to support client access, Internet access, roaming, and so on.

In spite of the similarities, the proprietary solutions are usually not interoperable. In order to resolve such an issue and meet the ever-increasing demands of 802.11 mesh networks, it is critical to develop a standard for 802.11 mesh networks. IEEE 802.11s serves just this purpose.

Before the establishment of 802.11s, many companies had started to push a standard for 802.11 mesh networks in 2005. At the beginning, many proposals were submitted to resolve different issues in a 802.11 mesh network. These proposals were finally consolidated and merged into one proposal in early 2006, which provides the basic framework for the current 802.11 task group. Since then, the 802.11 task group has worked on resolving issues in the framework. Draft 1.0 of the 802.11s standard has been generated and is currently going through a letter ballot [123]. Because many issues still exist in the 802.11s draft, when the official 802.11 standard will be released is still unpredictable.

Network Architecture of 802.11s

In order to understand the network architecture of 802.11s, we first need to explain 802.11 ESS and its difference from IBSS.

An 802.11 ESS consists of multiple BSSs connected through a DS and integrated with wired LANs. The DS service (DSS) is provided by the DS for transporting MAC service data units (MSDU) between APs, between APs and portals, and within the same BSS if MSDU is broadcast/multicast or intended to involve DSS. The portal is the logical point for letting MSDUs from a non-802.11 LAN enter the DS. An ESS appears as a single BSS to the logical link control layer at any station associated with one of the BSSs. The 802.11 standard has pointed out the difference between IBSS and ESS. IBSS actually has one BSS and does not contain a portal or an integrated wired LAN since no physical DS is available. Thus, the ESS architecture can meet the needs of client support and Internet access, while IBSS cannot. However, IBSS has the advantage of self-configuration and ad hoc multihop networking. Thus, it is a good strategy for developing schemes to combine the advantages of ESS and IBSS. The solution path being taken by IEEE 802.11s is one such scheme.

In 802.11s, a meshed wireless LAN is formed via ESS mesh networking. In other words, BSSs in the DS do not need to be connected by wired LANs. Instead, they are connected via mesh networking, possibly with multiple hops in between. Portals are still needed to interconnect 802.11 wireless LANs and wired LANs. Based on such a concept, the network architecture of 802.11s is formed as shown in Figure 10.1. There are three new nodes in this architecture. A mesh point (MP) is an 802.11 entity that can support wireless LAN mesh services. A mesh access point is an MP that can also work as an access point. A mesh portal is a logical point where MSDUs enter and exit the mesh network from and to other parts of the DS such as a traditional 802.11 LAN or from and to a non-802.11 network. Mesh portal includes the functionality of MP. It can be co-located with an 802.11 portal.

Because MPs do not have AP functionality but can work as relaying nodes, the meshed wireless LAN is not an ESS anymore. Thus, in a recent 802.11 standard meeting, the suggestion of changing the project authorization request (PAR) of 802.11s was made so that the title of 802.11s will be just "Mesh Networking" rather than "ESS Mesh Networking".

The protocol stacks of these three types of nodes are illustrated in Figure 10.2. The 802.11s MAC is developed based on existing 802.11 MAC for an MP (or the MP module in a Mesh Access Point (MAP) or mesh portal). We can see that the mesh routing protocol of a MP (or the MP module in a MAP or mesh) is located in the MAC layer. In a mesh portal,

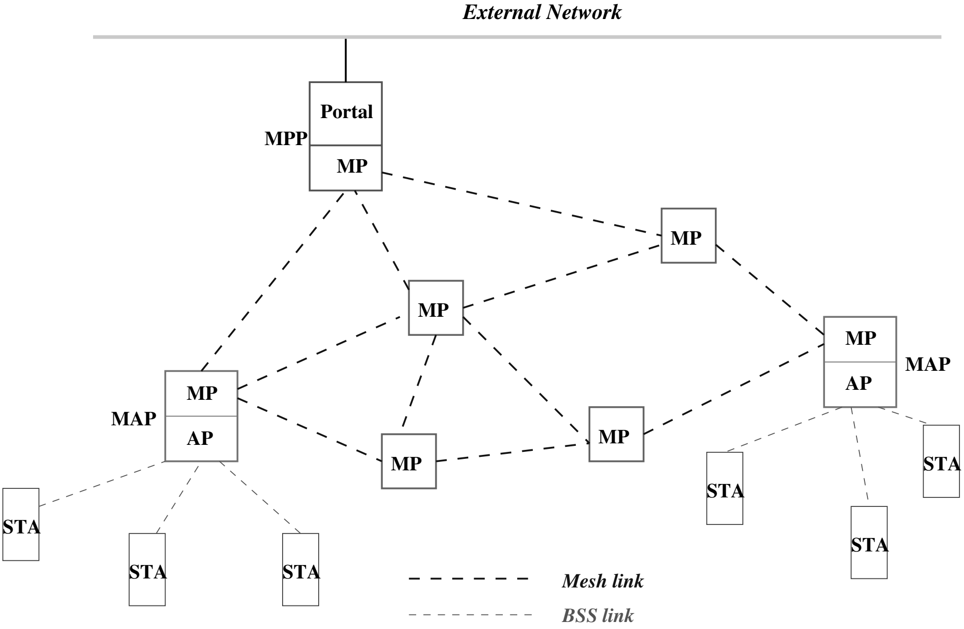

Figure 10.1 Network architecture of 802.11s meshed wireless LANs

a layer-3 routing protocol is also needed for path selection from the mesh network to the external network or vice versa.

Framework Overview of 802.11s

According to the project authorization request (PAR) of 802.11s, the following rules must be followed.

- The standard will be an extension to the IEEE 802.11 MAC.
- The 802.11s defines an architecture and protocols to create an 802.11 wireless distribution system (WDS) for ESS mesh networks.
- The ESS mesh is functionally equivalent to ESS connected by wired networks.
- The mesh network can be self-configured.
- The mesh protocol will utilize 802.11i security and its extension.
- For security, APs in a mesh network are controlled by a single logical administration entity.
- The 802.11s amendment will allow the use of one or more radios on each AP in the mesh network.

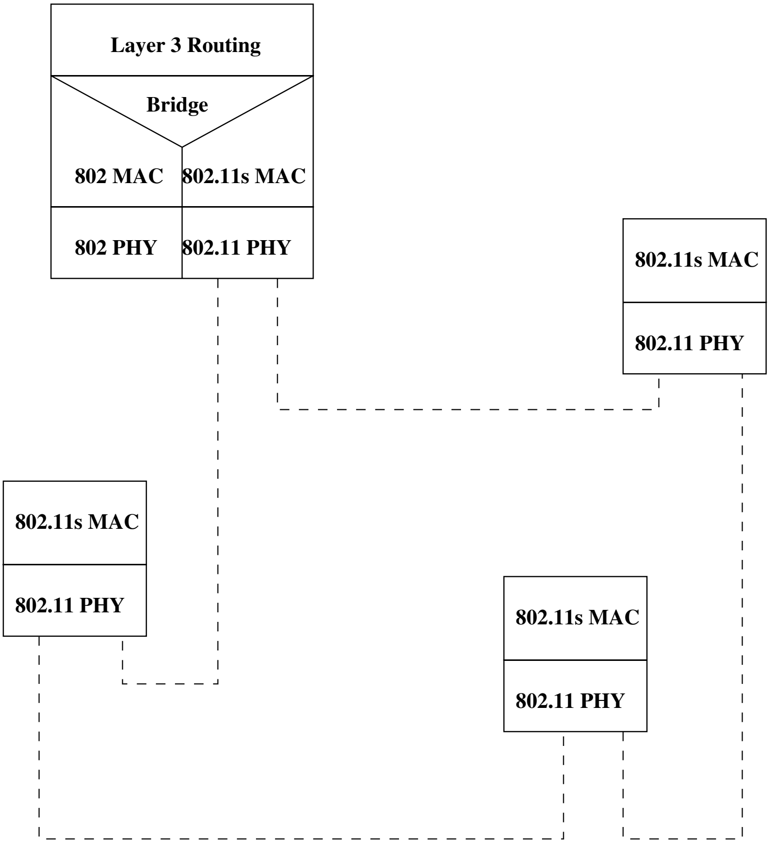

Figure 10.2 Protocol stack of 802.11s

- The target configuration of 802.11s is up to 32 devices participating as mesh points. However, more devices can be supported too.

Accordingly, the upcoming 802.11s standard will include the following critical components.

- *Extension of frame formats for mesh operation.* This includes both adding new information elements (IEs) to the existing frames and defining new frames.

- *Topology formation of a mesh network.* This includes the specifications of how a mesh network is created and how other mesh nodes join or leave the network. Both single channel and multichannel operations will be supported.

- *Interworking.* Mechanisms for interconnecting the mesh network with other wired networks or wireless networks will be specified.

- *MAC.* Many functionalities need to be specified for the MAC protocol, including MAC enhancement, MAC layer congestion control, power management, multichannel operation, synchronization, and so on.
- *Routing in the MAC layer.* Since the routing protocol is specified in the MAC layer, MAC address routing is needed. Also, the routing needs to be radio aware. How legacy nodes are supported needs to be specified in the routing framework.
- *Security.* As always, security is critical for wireless networks.

In the following subsections, we will first present the work that has been done in the current 802.11s draft. We will then point out the problems that still remain in the Section "Open Problems in 802.11s".

Topology Formation/Discovery

Discovery and Formation of Mesh Networks When a new mesh node powers up, it may use passive or active scanning to discover a mesh network. In 802.11s, a new ID, called mesh ID, is used to identify a mesh network. The mesh ID is attached to beacons and probe response frames as a new IEs for passive and active scanning, respectively.

The function of mesh ID is similar to service set identifier (SSID), but SSID cannot be used to identify a mesh network. One of the reasons is that a mesh ID can prevent STAs from being associated with MPs without AP functionality. For the same reason, for a non-AP mesh point, the beacon should not include a valid SSID, so the wildcard value is used for SSID IE in beacons of non-AP MPs.

Before a new mesh node is associated with a mesh network identified by a mesh ID, it needs to check whether its mesh profile matches the established mesh network. In 802.11s, each mesh device must support at least one profile consisting of a mesh ID, a path selection identifier, and a path selection metric identifier. If such mesh capability information in a mesh node matches that in the mesh network, it will start association. Security procedures will be involved in this association process. If a new mesh node cannot find a mesh network, it needs to create a mesh network.

Mesh Peer Link Establishment Once a mesh node has joined a mesh network, and before it can start send packets, it needs to establish peer links with its neighbors. In 802.11s, state machines and detailed procedures have been specified for setting up peer links. Once this step is completed, it is also necessary to establish a measure of link quality for each peer link. This requires a link quality measurement scheme and a procedure for populating such information among neighbors. When necessary, a procedure to ensure symmetrical link quality information has to be available. It should be noted that the link quality information of each peer link will also be one of the routing metrics for the routing protocol.

Multichannel Topology Formation In the single-channel mode, a mesh device just selects one channel during the discovery process. In a multichannel case, a mesh node needs to select multiple channels for its multiple radios or for channel switching if single radio is supported.

In order to manage the topology in a multichannel mesh network, the concept of unified channel graph (UCG) is used. In a UCG, all devices are interconnected using the common channel. Thus, in a single-channel mesh network, the entire network has only one UCG [123]. For a multichannel mesh network, the number of UCGs depends on a self-organization of the network. In the same UCG, the channel precedence value is the same for all devices. Such a value is different in different UCGs, and is used for coalescence or switching the channel in UCGs.

A simple channel unification protocol and a simple channel graph switching protocol are specified in the current 802.11s draft. However, such mechanisms are only applicable to simple scenarios such as when only slow channel switching is needed. If dynamic and fast channel switching is needed, the UCG concept and its supporting procedures in the current 802.11s draft may be insufficient for it to be useable.

Routing

It is a widely accepted concept that it is beneficial to have layer-2 routing for WMNs. However, 802.11s is probably the first standards committee that actually specifies routing in the MAC layer. Among many other reasons, interoperability is the most obvious motivation to do so. Previously many proprietary 802.11 mesh networks were built using different routing protocols, which result in the difficulty of interoperation.

In 802.11s, the framework for routing is extensible, which means that different routing protocols can be supported by following this framework, but the mandatory protocol will be implemented in order to achieve interoperability.

The routing mechanism in 802.11s handles packet forwarding for MPs, MAPs, and associated STAs. Unicast, multicast, and broadcast frames are all supported in the same framework. Since routing is performed in the MAC layer, packet forwarding is carried out via MAC addresses, which requires the MAC header to contain at least four MAC addresses. Compared to the previous MAC protocol, the two additional MAC addresses are for the MAC addresses of the source and the destination of an end-to-end flow.

In a routing protocol, nodes usually need to exchange routing messages for the purpose of finding link status, collecting neighbor information, requesting routing path, and so on. Thus, many control messages are involved. In 802.11s, such messages are sent in various mesh action frames.

In the current draft of 802.11s, one mandatory routing protocol and one optional routing protocol are specified. The mandatory routing protocol is called hybrid wireless mesh protocol (HWMP), which is a hybrid routing protocol of on-demand routing and proactive tree-based routing. The optional routing protocol is based on link state routing and is called radio aware optimized link state routing (RA-OLSR).

HWMP An 802.11 mesh network has several features. The network infrastructure tends to have minimal mobility and most of the traffic is to/from the Internet. However, some nodes in the network can be an MP but still need mobility such as some handset devices, laptops, etc. In order to meet the diverse requirements by making the routing protocol efficient for different scenarios, HWMP is being specified in 802.11s. In HWMP, an on-demand routing protocol is adopted for nodes that experience a changing environment, while a proactive tree-based routing protocol is an efficient choice for nodes in a fixed network topology. In this routing protocol, the mandatory routing metric is airtime, which measures the quality of links. The extensible framework supports other types of metric such as QoS parameters, traffic load, power consumption, and so on. However, in the same mesh, only one metric will be used.

The on-demand routing protocol is specified based on radio-metric AODV. Thus, the basic features of AODV [208] are adopted, but extensions are made for 802.11s. The proactive tree-based routing is applied when there is a root node configured in the mesh. With this root, a distance vector tree can be built up and maintained for other nodes. This type of routing protocol can avoid unnecessary routing overhead for routing path discovery and recovery.

It should be noted that the on-demand routing and tree-based routing can run simultaneously.

Four control messages are specified for HWMP: root announcement (RANN), route request (RREQ), route reply (RREP), and route error (RERR). Except for RERR, all control messages contain three important fields: destination sequence number (DSN), time-to-live (TTL), and metric. DSN and TTL can prevent the *counting to infinity* problem, and this metric helps to find a better routing path rather than just using hop count. The entire routing protocol is built based on these control messages.

In the on-demand routing, RREQ is broadcast by a source MP with the aim of setting up a route to a destination MP. When an intermediate MP receives the message, it creates/updates a route to the source if the sequence number of the RREQ is greater than the previous one or the sequence number is the same but the metric is better. If the intermediate MP has no route to the destination, it just forwards the RREQ message further. Otherwise, there are different cases depending on two flags: destination only (DO) flag and reply and forward (RF) flag. If the DO flag is set to 1, then the intermediate MP does nothing but just forwards the RREQ to the next-hop MPs until it reaches the destination node. Once the destination node gets this message, it sends a unicast RREP back to the source MP. All intermediate MPs create a route to the destination when receiving this RREP message. If the destination-only (DO) flag is set to 0 and the RF flag is set to 0, then the intermediate MP sends a unicast RREP message to the source node and does not forward RREQ. However, if the DO flag is 0 but the RF flag is 1, then the intermediate MP sends a unicast RREP message to the source node; additionally, it needs to set the RF flag to 0 and then forward the RREQ message to the destination node. In this way, the subsequent intermediate MPs will not be able to send RREP messages to the source node. It should be noted that the DO flag is set to 0 and the RF flag is set 1 only when the source node has no valid route and wants to create a new route to the destination node. As we can see, the above procedures have been modified for HWMP as compared to the original AODV protocol.

In the proactive tree-based routing mode, there are two mechanisms. One is based on proactive RREQ and the other is based on proactive RANN. In the proactive RREQ mechanism, the root MP periodically broadcasts the RREQ messages. An MP in the mesh receiving the RREQ creates/updates the path to the root, records the metric and hop count to the root, updates the RREQ with such information, and then forwards RREQ. Thus, the presence of the root and the distance vector to the root can be disseminated to all MPs in the mesh. If the proactive RREP bit in the proactive RREQ message is set to 1, then the receiving MP sends a gratuitous RREP to the root so that a route from the root to this MP is established. On the other hand, if the proactive RREP bit is set to 0, the gratuitous RREP is sent only when there is data to send between the MP and the root with a bidirectional route.

In the proactive RANN mechanism, the root periodically flood an RANN message into the network. When an MP receives the RANN and also needs to create/refresh a route to the root, it sends a unicast RREQ message to the root. When the root receives this unicast RREQ, it replies with an RREP to the MP. Thus, the unicast RREQ forms the reverse route from the root to the originating MP, while the unicast RREP creates the forward route from the originating MP to the root.

RA-OLSR RA-OLSR is a proactive link-state routing protocol that is developed based on OLSR [64]. However, in order to reduce flooding overhead, several extensions are made. Firstly, only a subset of one-hop neighbors of an MP is selected to relay control messages. Such neighbor MPs are called multipoint relays (MPRs). The MPRs are selected such that control messages relayed by them can reach all two-hop neighbors of the selecting MP. The MPR selection is performed through periodic *Hello* messages between MPs. In addition, the message exchange frequency can be controlled based on fisheye scopes as defined in fisheye state routing protocol [89]. Secondly, to provide shortest routes, RA-OLSR requires only partial link state information to be flooded. The minimum set of links are the links between the MPRs and their selectors.

Since RA-OLSR continuously maintains routes to all destinations in the network, it is specially beneficial for source–destination pairs that are very dynamic or where the network is large and dense. RA-OLSR is a distributed protocol, without a requirement for reliable delivery of control messages. It can also support both single-interface and multiple-interface MPs.

The mechanisms for supporting nonmesh STAs are specified for RA-OLSR. However, the overhead of these mechanisms is still extremely high, in particular when the number of STAs is large.

Support of Legacy Nodes For packets transmitting between legacy nodes via the mesh network, the routing protocol inside the mesh may need the source and the destination MAC addresses of a legacy node. Thus, two additional MAC addresses are added into the MAC header. This is the mechanism of the six-address scheme specified in 802.11s.

Other than this mechanism, the routing protocol of the mesh also needs to handle legacy nodes. For example, the association of legacy nodes with an MP will be efficiently handled such that a routing path can be found for legacy node to send packets via the mesh network. In the current draft of 802.11s, this part of the functionality has not been fully specified.

MAC

The basic operation mechanism of 802.11s MAC is the enhanced distributed channel access (EDCA) specified in 802.11e. Other features of 802.11e such as HCCA are not adopted into 802.11s. In this sense, the QoS of 802.11s in its current form is still far from enough for many multimedia services. Moreover, EDCA does not work well for mesh networks, since its prioritization mechanism does not perform well in a multihop mesh environment. Nevertheless, the current 802.11s MAC protocol is built on top of EDCA with various enhancements.

Beaconing and Synchronization Beaconing procedures for unsynchronizing and synchronizing MPs are defined in 802.11s. A mechanism to avoid beacon collisions is also specified in the mesh beacon collision avoidance (MBCA) mechanism. Also, an MP can be designated as a beacon broadcaster for a defined period of time while all other MPs defer their transmission of beacons.

Based on beacons and probe responses, synchronization is carried out for MPs. In 802.11s, the synchronization is similar to the timing synchronization function (TSF) of the original 802.11 standard. The differences are twofold. One is that the MPs are not all synchronized and their beacon intervals are not necessarily the same. The other is that not only a TSF timer but also an offset is needed for synchronization.

Whether or not an MP supports synchronization is identified by synchronization capability field of the WLAN mesh capability IE. When an MP does not need synchronization, it maintains its own TSF timer and does not update it when receiving beacons or probe responses. However, for a synchronizing MP, it needs to maintain a mesh TSF time that is common to all synchronizing MPs. The mesh TSF time is equal to the sum of the TSF timer and the offset on the synchronizing MP. Because of using the offset, the TSF timers of synchronized MPs can be different. On the other hand, when receiving beacons or probe responses that contain the sender's TSF timer and the offset, an MP follows a synchronization procedure similar to that for the IBSS mode of 802.11 networks. More specifically, the MP performs the following calculation.

$$\textit{Calculated time stamp} = \textit{received TSF value} + \textit{received offset} - \textit{the MP's own offset}.$$

If the calculated time stamp is later (or faster) than the MP's local TSF value, then the TSF timer is updated with this calculated time stamp. Otherwise, this step is ignored. Optionally, the MP can update its offset rather than the TSF timer as follows. If the sum of the received TSF value and the received offset is larger than the sum of the MP's TSF value and self offset, then the self offset is updated as follows.

$$\textit{The MP's new offset} = \textit{received TSF value} + \textit{received offset} - \textit{the MP's TSF value};$$

otherwise, no updating is needed.

It should be noted that updating the TSF timer and updating the offset cannot be used at the same time.

Multichannel Operation Multichannel operation is very important to WMNs, but no mechanism has been specified in 802.11s.

At the beginning, there was a proposal called the common channel framework (CCF) which was adopted into earlier versions of the draft (before draft 1.0). However, because of the many problems that were not resolved effectively, the proposal was removed from the draft. Nevertheless we still introduce the mechanism of CCF here.

In CCF, nodes that want to use multichannel operation need to negotiate their channel in the common channel. Thus, the common channel is known to all nodes in the mesh network. A transmitter first sends a request to switch (RTX) message to request a channel. The receiver sends back a clear to switch (CTX) to confirm the requested check. If RTX-CTX is successful, then a channel is selected for these two nodes. Thus, both nodes switch to the selected channel and exchange data following the data/ack procedure. Once this is done, both nodes switch back to the common channel. This mechanism is applied to all nodes that are able to support CCF. In the common channel, in addition to RTX-CTX messages, packets for nodes that do not support CCF can be sent.

The major problems of CCF are discussed in the section "Open Problems in 802.11s".

Mesh Deterministic Access Mesh deterministic access (MDA) allows MPs to access a certain period with lower contention than that in other periods without MDA. Such a period is called an MDA opportunity (MDAOP). Before using MDAOP to access the medium, the owner of this MDAOP, i.e., the transmitter, needs to set up the MDAOP with its receiver.

In a multihop network, the interference between nodes that are more than one hop away should be considered. Thus, in the MDA mechanism, two types of time period are defined. The neighborhood MDAOP times of an MP are the RX-TX times in which the MP and its neighbors are either a transmitter or receiver of these MDAOPs. For a neighbor of this MP, it also has such time periods, but to the MP, these times are called neighbor MDAOP interfering times.

When an intended transmitter wants to set up a new MDAOP to an intended receiver, it needs to check its neighbor MDAOP times, the TX-RX times for other frames, and the neighbor MDAOP interfering times for the intended receiver. If no overlapping occurs and the MDA limit is not reached, then the transmitter sends an MDAOP setup request to the receiver. The receiver will do the same check. If the check is passed, the receiver accepts the MDAOP; otherwise, it rejects it. Once the MDAOP is set up, both the transmitter and the receiver will start to advertise their new MDAOP time in the MDAOP advertisement IE. Both the transmitter and the receiver can initiate the teardown process to release the MDAOP time period. The teardown is complete once the initiator is ACKed by the receiver.

During an MDAOP period, the transmitter and the receiver follow a different procedure. If this period is accessed by the transmitter, i.e., the owner of MDAOP, it attempts to use CSMA/CA but uses new backoff parameters, MDA maximum contention window (MDACWmax), MDA minimum contention window (MDACWmin), and MDA interframe space number (MDAIFSN), to set up an TXOP. However, for a nonowner of TXOP, it has to defer its access by setting its NAV to the end of the MDOAP or by using a carrier sensing scheme.

Intra-Mesh Congestion Control An 802.11 mesh usually has multiple hops. The one-hop transmission may interfere with its previous hop, the next hops, or any links in the neighbors. One problem from such an interaction is that links may be congested, and thus a node with congested links may receive more packets than can be sent out. The transport layer protocol such as TCP can help mitigate this problem, but research has shown that it is not effective enough in a wireless multihop network. On the other hand, contention resolution can also help reduce congestion. However, in a mesh network, the contention level experienced by different nodes is different, which make a contention resolution protocol ineffective. For these reasons, intra-mesh congestion control is specified in 802.11s.

The intra-mesh congestion control is a hop-by-hop scheme. Nodes in the neighborhood need to exchange congestion information and control message in order to resolve congestion in the network. Thus, the scheme consists of three modules: local congestion monitoring, congestion control signaling, and local rate control.

In the current draft of 802.11s, some local congestion monitoring schemes are suggested. For example, congestion can be monitored by comparing the transmitting rate and the receiving rate of packets that need to be forwarded. Queue size can also be used to monitor congestion. Once congestion is detected, the congested node will inform its previous hop nodes by sending a unicast *Congestion Control Request* message in the mesh action frame. The node that receives the message will adjust its transmission rate according to the locate rate control algorithm. The congested node also sends a broadcast message *Neighborhood Congestion Announcement* to all its neighbors so that neighbors can also regulate their transmission rate.

Congestion control signaling can be triggered periodically or nonperiodically. In either case, in order to carry out local rate control, the target rate must be computed by the congested node and sent to the upstream node. The target rate is computed for each traffic category as defined in 802.11e rather than one link. Such information is attached as an IE in the congestion control request message. When the upstream node receives the congestion control message, it controls its transmission rate according to the target rate to the congested node. The upstream node will also send a *Congestion Control Response* message to tell the congested node about its offer traffic load. The locate rate control at a node when receiving the neighborhood congestion announcement has not been discussed in 802.11s.

Although congestion control can help improve the mesh network performance, unfortunately the critical parts of this mechanism such as target rate computation and the local rate control algorithm have not been clearly specified yet; only simple conceptual discussions are available in the draft of 802.11s.

Power Management Many nodes in 802.11s mesh networks always work in an active state since they either need to be an AP or to forward traffic for other nodes. However, there are still other nodes that need to work in power-save mode. Typically these nodes are the lightweight MPs or MPs that do not forward traffic for other nodes. Of course, STAs associated with an MAP may also work in power-save mode, but the mechanism for these nodes is the same as that in the original 802.11 standards.

A lightweight MP needs to check whether its neighbors are also in power-save mode. If the answer is negative, it may choose to enter power-save or communicate with neighbors without entering power-save mode. In the former case, the MP may not be able to communicate with nodes that do not support power-save mode. Thus, whether or not a lightweight MP goes into power-save mode is determined by considering the tradeoff between power and communication constraints. In some cases, a lightweight MP can just operate as an STA, so its power management is carried out through an AP. However, mostly the power management can be done via an announcement traffic indication message (ATIM) based mechanism.

In the ATIM-window based power management scheme, an MP works in two states: doze or wake state. The MP in power-save mode needs to wake up during the ATIM window to receive or send control messages including beacons. The ATIM window repeats every one delivery traffic indication message (DTIM) interval. DTIM is usually equal to multiple beacon intervals. An MP may also wake in a scheduled time period negotiated with other MPs. In power-save mode, packets in an MP need to be buffered and wait to be sent during the wake state.

To initiate the power management in a mesh, the following procedure will be used.

- An unsynchronizing MP will set the values of DTIM, ATIM window, beacon interval, and power management mode. Such information is sent in beacon frames.
- When a synchronizing MP creates a mesh or when it joins a mesh where all neighbors are unsynchronized MPs, the same operation as the previous item is needed.
- When a synchronizing MP joins a mesh where there are synchronizing neighbor MPs, it needs to set the beacon interval and power management mode, and update its ATIM window and DTIM interval according to the values in the received beacons of synchronizing MPs.
- The ATIM window will start from the target beacon transmission time (TBTT) within each beacon interval.

It should be noted that an MP that has established peer links with other MPs cannot change to power-save mode unless (1) it can support power-save mode and (2) all its neighbor MPs can send packets to MPs working in power-save mode. Moreover, the MPs in power save mode will be coordinated with the neighbor discovery mechanism and the route discovery mechanism. Otherwise, these MPs can experience low performance and degrade the performance of the entire mesh.

Interworking

The interworking between mesh networks and other LAN segments is carried out through the bridging function in mesh point portals (MPPs) in a manner compatible with IEEE 802.1D.

In order to tell MPs in the mesh networks of its presence, an MPP needs to send an MPP announcement. An MPP announcement protocol is specified in 802.11s. An MPP sends an announcement IE in management frames. When an MP get a management frame with a valid MPP announcement IE, it checks the destination sequence number in the MPP announcement IE of the current MPP announcement message. If it is smaller than that of a previous MPP announcement message, the current message will be discarded. Otherwise, it needs to forward MPP announcement information to other MPs after the portal propagation delay has expired and also the TTL value is still greater than zero. In addition, it needs to record the MAC address and routing metric to this MPP.

When an MP has packets to send, it first follows the data forwarding procedures as defined in the routing protocol. If an intra-mesh route to the destination MAC address cannot be found, then the MP will forward all packets to the all active MPPs in the mesh.

At an MPP, both egress and ingress messages need to be handled. An egress message is generated by an MP inside the mesh. If the MPP knows that the destination node is inside the mesh, it will forward the message to the destination node. If the destination is outside mesh, it will forward the message to the external network. However, if the destination node is unknown to the MPP, the MPP will forward the message to both the external network and the mesh network. An ingress message is a packet received by the MPP from the external network. If the destination node inside the mesh is known to the MPP, the message is simply forwarded by the MPP. Otherwise, the MPP can have two options: establish a route to the destination or broadcast the message within the mesh network.

Node mobility is also considered in 802.11s. There are four scenarios of node mobility. If a node moves within the mesh, then the routing protocol will take care of the mobility.

If a node moves from the LAN outside the mesh to another LAN, no special action is needed for the mesh network, since 802.1D bridging functionality will handle this scenario. In the third scenario where a node moves from inside the mesh to outside the mesh, then the routing protocol needs to repair the routing path after detecting that the route has changed. When a node moves from outside the mesh to inside the mesh, both MPP functionality and routing protocol cooperate to build the new routing path for the node.

MPP plays a critical role in interworking. From the above procedures, we know that it needs to support 802.1D bridging functionality. Moreover, MPP also needs to support VLAN functionality. In other words, the VLAN tag information defined in IEEE 802.1Q must be carried between MPs and MPPs. 802.1Q defines two header formats: Ethernet-encoded formats and sub-network access protocol (SNAP)-encoded header. If the former is considered, a change to the 802.11 MAC header is needed in order to add the VLAN tag information. The latter does not need such a change.

Security

The security specification in 802.11s is dedicated to protection of transporting packets. The security in routing or forwarding functionality in a mesh network is not specified.

The 802.11s security inherits lots of work from 802.11i and includes 802.1X for initial authentication, as discussed in Section 6.4.2. In order to satisfy the peer-to-peer environment, a role negotiation protocol is added before starting the security protocol exchange. Fast reconnection to the network developed based on the key hierarchy specified in 802.11r, but modification has been done for robust peer-to-peer link establishment.

Open Problems in 802.11s

The 802.11s amendment is still being standardized. Many issues still exist. Instead of discussing detailed problems/errors in the current draft of 802.11s, here we point out just the major issues. If no remedy is found to resolve these issues, they will eventually degrade the performance of the mesh networking protocol and push 802.11s away from success.

Topology for Multirate Operation and Physical Rate Control In order to support routing, MAC, and other functionalities, the network topology needs to be maintained. 802.11s has specified such a framework in which the peer-link setup takes into account link quality measurement. However, this kind of mechanism is not flexible for a mesh network with multirate operation. Currently most physical layer technologies for wireless networks including 802.11 support multiple rates depending on the selection of different modulation and coding schemes. For this kind of multirate network, the topology is very sensitive to the transmission rate that is being used. For example, if a high rate is used, the communication range (and usually the interference range) is reduced too. Normally the physical rate on a node is controlled automatically by a rate control per packet. Mostly the control/signaling messages are sent out using the lowest transmission rate to improve reliability. Thus, the topology being built up based on such messages is not consistent with the network topology that is seen by other packets. Such inconsistency will cause problems to any topology-related protocols such as routing and MAC.

Since the change of rate results in a different communication range and a different interference range, it may be also beneficial to consider tradeoff between the number of hops and the physical rate. For example, in order to connect two nodes, we can use one-hop communication with a very low transmission rate. We can also use multihop communications with a very high transmission rate. The end-to-end throughput for these two cases may be different, and so is the interference to other nodes. Unfortunately, the framework of topology formation in 802.11s is not flexible enough to support optimization between the rate and the number of hops.

Link Quality Measurement and Routing Metrics Link quality is an important parameter for multiple modules of 802.11s, including the routing protocol, as discussed in Chapter 4. In 802.11s, the link quality measurement is based on the current transmission rate and transmission error rate, and thus is called the airtime cost. However, such a scheme lacks two important mechanisms. First, what packets can be sent and how they are sent is not specified. Without careful design, the link quality measurement can be inaccurate. For example, the frequency of measurement packets and their transmission rate impact the result of airtime cost. Second, the packet error rate due to transmission error does not actually reflect the link quality. For example, the packet error rate can be due to collisions, which is totally dynamic depending on the traffic activity and the behavior of routing and MAC protocols. Thus, the airtime cost varies a lot, so it cannot provide a good metric for link quality. Routing based on such a metric may have a stability issue. Consequently, a more reliable and stable metric for link quality measurement and routing protocol is still desired.

Routing Protocol As a routing protocol, either HWMP or RA-OLSR has some shortcomings. First, the scalability of both routing protocols is limited. In HWMP, the proactive tree-based routing is totally centralized and constrained by the root node. When there is a short path between two MPs, the routing protocol still routes the packets via the root, which results in a bottleneck at the root node and wastes precious wireless resources owing to the nonoptimized routing path. For RA-OLSR, the overhead of control messages is too high although Fisheye scope mechanism is adopted.

Second, for both HWMP and RA-OLSR, although they are being specified as a routing module in the MAC layer, their interactions with other MAC functionality, especially the medium access mechanism, are not considered. This strategy actually loses one important advantage of layer-2 routing, i.e., MAC-routing cross-layer design. Radio metric routing in HWMP or radio aware routing in RA-OLSR have been considered as a simple interaction between routing and MAC/PHY layer. However, such interaction is far from sufficient. For example, for both mechanisms, how to use the routing metric based on airtime cost to find a better routing path is not specified. However, such a scheme critically determines the performance of the routing protocol. In another example, if intra-mesh congestion control is used, the routing protocol will cooperate with the congestion control algorithm by a mechanism of considering the target rate; otherwise, the effectiveness of congestion control can be compromised. When multichannel operation comes into the picture, the cross-layer design becomes much more necessary.

Third, supporting legacy nodes is still an ongoing effort. Such a functionality is not specified in the HWMP, while the procedures in RA-OLSR can result in a very high percentage of overhead, which also limits the scalability of the routing protocol.

Finally, in the current framework, although multiple routing metrics can be supported, only one metric is supported in the same mesh. However, in many application scenarios, multiple metrics are needed and integrated into the same mesh. Obviously the current framework is not extensible for supporting such a feature.

QoS Although 802.11s adopted the EDCA mechanism, no QoS can be provided. First of all, EDCA is only a mechanism for achieving soft QoS, i.e., traffic prioritization. Such a mechanism is good for traffic classes with different priorities, that for the nodes with the same traffic class, then no priority is provided. Such a problem is amplified in a multihop environment.

Other mechanisms such as MDA or intra-mesh congestion control at most provide some improvement of QoS locally, and also such mechanisms contain many problems as explained later.

Multichannel Operation In 802.11s, for multiradio MPs, only a simple UCG mechanism is used to unify the network using different channels. So far, there is no MAC mechanism defined for multichannel operation for single-channel radios. The original proposal of CCF has several obvious problems. CCF needs packet-level channel switching, but since the duration of channel switching is larger than the time of sending a regular packet, the channel switching causes a huge percentage overhead. Moreover, the RTX-CTX in the common channel has no way to avoid possible collisions from non-CCF nodes in a new channel that the CCF node wants to switch to. Thus, when CCF node switches to the new channel, its performance is not guaranteed, and may cause some coexistence issues. Since RTX-CTX messages are always sent in the common channel that is shared by other non-CCF nodes, such messages can be congested and result in a slow process of getting a new channel. Moreover, CCF lacks a scheme for determining channel selection.

Although the above problems come from CCF, they must also be considered for multichannel algorithm. To the best of our knowledge, the solution in [257] is the only multichannel MAC protocol that can avoid the above problems, yet also provide QoS support through the TDMA overlaying CSMA/CA.

Congestion Control There are several problems in the proposed intra-mesh congestion control mechanism. There is an effective mechanism for congestion monitoring in the IEEE 802.11s specification. Congestion based on queue size may not work since the queue size is also impacted by higher layer protocols such as TCP. Whenever congestion happens, the congestion monitoring scheme may need to take some time to get a reliable measurement. For example, the time window must be large enough to avoid a false alarm. Such a time window may already cause TCP to take action and adjust the traffic rate. No matter how bad the TCP performance, the status of congestion may have changed, and thus the monitoring scheme may not be able to capture such an event.

In the target rate computation, a node must need traffic load information in all neighbors including one-hop and two-hop ones. Otherwise, the computed target rate can be arbitrary and degrade the performance of congestion control. However, in 802.11s no mechanism is specified to exchange traffic load related information among one-hop and two-hop neighbors. How to determine the target rate based on neighbor information is not specified either. Moreover, there is no scheme specified in 802.11s for the local rate control. Simply adjusting EDCA parameters cannot achieve the goal because EDCA is more effective for traffic prioritization rather than ensuring a certain traffic rate. The above problems render the current framework for congestion control useless in a multihop mesh environment.

MDA MDA aims to reduce the contention in a 802.11s mesh. However, such a mechanism can cause an interoperability issue. In the same 802.11s mesh network, if there are both non-MDA and MDA nodes, the performance of either type of node may be degraded. An MDA node has no way to prevent a non-MDA node from accessing the MDAOP TXOP. However, the non-MDA node may experience difficulty in accessing the medium owing to the existence of MDAOP TXOP.

The MDA mechanism relies on timely information about neighbor MDAOP interfering times and neighborhood MDAOP times to determine an MDAOP. This means that frequent message exchange is needed between MPs. This can cause a large overhead. Moreover, such information may have to be propagated over multiple hops, but no filtering mechanism is specified in MDA. In MDA, when determining a new MDAOP, interfering times must be checked on all neighbors rather than just the intended receiver. Also some procedures in MDA involves HCCA, which is not consistent with the design rule of 802.11s, since HCCA is not part of 802.11s.

Security 802.11s utilizes security work from 802.11i. Thus, any security problems in 802.11i also exist in 802.11s. Moreover, due to the multihop mesh network architecture, security becomes a more challenging issue. For example, the "man-in-middle" security attack can more easily occur in 802.11s mesh network.

Additionally, all security procedures only take care of the potential security attacks in transporting data. How to make sure that the routing protocol is secure is not specified. 802.11s claims that this issue is out of its scope, but this also reminds us about being careful with routing security when an 802.11s network is deployed.

Fast Handoff In 802.11s, non-MP clients are supported through the AP on the MAP. For this kind of node, when they move within the mesh, the handoff delay can be large due to channel scanning, security, authentication, and other necessary operation procedures. For an 802.11 mesh, VoIP is one of the killer applications. However, without a fast roaming scheme, it is impossible to deliver VoIP traffic without service disruption. However, no mechanism is specified for fast handoff. A possible solution to this problem is that 802.11s should consider including work from 802.11k and other necessary mechanisms for fast handoff.

Multiple MPP In the current framework of 802.11s, single MPP is assumed. However, in a relatively large-scale mesh network, e.g., an enterprise network, multiple MPPs are needed in order to provide enough backhaul capacity to the Internet.

When multiple MPPs are available, many functionalities such as interworking and routing protocols in the current 802.11s draft need to be modified accordingly.

10.4 Standards for Meshed Wireless PANs

There are many application scenarios related to wireless PANs. The most well known ones include home networks, office networks, and wireless sensor networks.

Wireless PANs have characteristics such as short distance between nodes and low power consumption. Both MAC and physical layer techniques must take into account such factors. Standard groups such as IEEE 802.15 and other associations such as Bluetooth Special

Table 10.3 Summary of IEEE 802.15 task groups and standards

Standards/task groups	Objective and focus	Status
802.15.1	MAC and physical layer specifications for wireless PANs; corrected and revised in 2005	Completed
802.15.2	Coexistence between 802.15 wireless PANs and other devices in the same unlicensed band	Completed
802.15.3	High rate MAC and physical layer specifications for wireless PANs	Completed
802.15.3a	Higher rate MAC and physical layer specifications based on UWB for wireless PANs	Withdrawn
802.15.3b	Correct and revise 802.15.3	Completed
802.15.4	Low rate MAC and physical layer specifications for wireless PANs	Completed
802.15.4a	New physical layers for more accurate location/range lower power consumptions, and scalable rates	Active
802.15.4b	Correct and revise 802.15.4	Active
802.15.5	Mesh networks for wireless PANs; both low rate and high rate wireless PANs are being considered	Active

Interest Group (SIG), WiMedia Forum, UWB Forum, and so on are working on specifications for the protocols in various scenarios for wireless PANs.

10.4.1 Overview of IEEE 802.15 Standard Activities

Although the IEEE 802.15 standards group is not the only association that works on specifications for wireless PANs, it contains many task groups that cover almost all scenarios for wireless PANs. Also, it is closely related to Bluetooth SIG, WiMedia Forum, UWB Forum, and so on. Knowing the status in IEEE 802.15 will reveal a big picture of standardization of wireless PANs.

In IEEE 802.16, there are many task groups that have been approved by the IEEE 802 standards committee. A complete list is shown in Table 10.3.

802.15.1 worked on MAC and physical layer specifications for wireless connectivity with fixed, portable, and moving devices within or entering a personal operating space (POS). This is the original focus of 802.15, i.e, PANs. A POS is specified as a space that envelops the person (whether stationary or in motion) and typically extends up to 10 m in all directions.

The first version of the 802.15.1 standard was approved in April 2002, and it was revised in May 2005. Both versions are based on the Bluetooth technology. According to 802.15.1, devices work in the 2.4 GHz ISM band, which is the same as that used by many IEEE 802.11 devices. In order to ensure coexistence, another standard, 802.15.2, approved in June 2003, specified coexistence mechanisms between wireless PANs and 802.11 wireless LANs and other networks working in the same unlicensed band.

Since the transmission rate of 802.15.1 does not meet the requirements of many high rate applications such as digital imaging and multimedia, a new task group, 802.15.3, was established to specify new MAC and physical layers for wireless PANs. In the physical layer of the 802.15.3 standard approved in June 2005, different modulation and code schemes are applied to achieve scalable data rates ranging from 11 Mbps to 55 Mbps. The MAC layer stills employs the piconet concept from Bluetooth and is able to support both isochronous and asynchronous data types. 802.15.3 was revised in a separate project, called 802.15.3b. The revised standard 802.15.3b was approved in December 2005 and the major revisions are located in the MAC layer. To support an even higher transmission rate than that defined in 802.15.3, a task group called 802.15.3a was created in May 2004. The original goal of this group was to develop UWB based wireless PANs so that the transmission rate is high enough to support applications such as high density videos and other high rate multimedia traffic. After many months of effort, the progress of this task group entered in an unresolved deadlock, mainly because the two proposals for the same standard could not be consolidated as one joint proposal in subsequent standards meetings. Thus, unfortunately, the activity of 802.15.3a has been pending since then. Of course, the development of UWB technologies for wireless PANs has never stopped. Basically, companies in both groups continue to work on specifications for UWB wireless PANs in two industrial consortiums called WiMedia Forum and UWB Forum, as announced in January 2006.

IEEE 802.15 also has task groups working on standards for wireless PANs with low transmission rate such as sensor networks. In the 802.15.4 standard approved in October 2003, both MAC and physical layers have been specified for low rate wireless PANs. In the physical layer, two types are specified: 868/915 MHz direct sequence spread spectrum (DSSS) and 2450 MHz DSSS. In the former one, the physical layer rate can be 20/40 kbps, while the latter supports a rate of 250 kbps. CSMA/CA is adopted as one key function of the MAC layer, using both star and peer-to-peer topologies. Superframe structure is also an option and time slots can be allocated by the PAN coordinator to support devices with time critical data. The 802.15.4 standard is being revised in a separate task group called 802.15.4b, and another task group, 802.15.4a, is currently working on new physical layer technologies for low rate wireless PANs with objectives of more scalable rates, high location/range accuracy, and lower power consumption. Two options are being considered: UWB impulse radio in UWB unlicensed spectrum and chirp spread spectrum in 2.4 GHz spectrum.

In all the above standards, the network topologies considered include star, peer-to-peer, and tree. However, mesh topologies are not considered. To utilize the advantages of mesh networking such as better coverage, higher throughput, and lower power consumption, a new task group called 802.15.5 was started in 2004 to work on wireless mesh networking solutions for both high rate and low rate wireless PANs. Currently, the call for proposals for the mesh networking protocols is still open.

10.4.2 IEEE 802.15.5

The IEEE 802.15.5 task group aims to provide a *recommended practice* rather than a mandatory standard for the architectural framework that enables WPAN devices to be interoperable in a stable and scalable wireless mesh topology.

Network Architecture and Protocol Stack

In 802.15.5, the meshed wireless PANs can have a topology of full mesh or partial mesh, as shown in Figure 10.3. There are three types of node in the network: PAN coordinator, coordinator, and end device. End devices are connected to their coordinator as a star topology, which is the exactly the same as that in other 802.15 wireless PANs. Coordinators are connected to each other through a mesh topology (either full mesh or partial mesh), which is different from the topology of other 802.15 wireless PANs. For example, a 802.15.1 scatternet can also form a multihop wireless PAN, but it is actually a tree-based network topology because of the master/slave mechanism. In 802.15.4, a multihop wireless PAN is formed via the concept of the cluster tree network, which is also a type of tree topology. Neither scatternet nor cluster tree topology has the flexibility of mesh topology, although it is simpler and thus demands lightweight protocols in MAC and routing layers. Lack of such flexibility can result in several other issues such as poor network coverage, low reliability due to no redundant path, high power consumption, etc. Thus, the meshed wireless PANs of 802.15.5 are targeted at:

- Extending network coverage without increasing transmit power or receive sensitivity
- Enhancing reliability via route redundancy
- Simplifying network configuration
- Increasing device battery life with better transmissions and fewer retransmissions

Other than the difference in network topology, all other 802.15 wireless PANs have just focused on MAC and physical layers, even for a multihop network. Thus, how to route packets from end to end is not specified. Without a routing protocol this may cause several problems. For example, the routing functionality has to be implemented by vendors, which can cause interoperability issues between products of different vendors. Thus, specifying a routing protocol is one of the most important tasks for the 802.15.5 task group. Thus, in 802.15.5, both MAC and routing protocols need to be specified. The MAC is enhanced based on that of other 802.15 wireless PANs, and new routing function is added on top of the enhanced MAC protocol. Since low rate wireless PANs and high rate wireless PANs have different physical layer and MAC layer specifications, the 802.15.5 task group is currently working on separate specifications for them. However, the protocol stack of these two types of mesh network is the same, as shown in Figure 10.4.

High Rate Mesh

High rate (HR) meshed wireless PANs are being standardized based on 802.15.3b. Typical applications include: (1) multimedia home networking such as HDTV, DVD, interactive gaming in a multiroom environment; (2) interconnection between a PC and its peripherals; (3) interconnection between handheld devices.

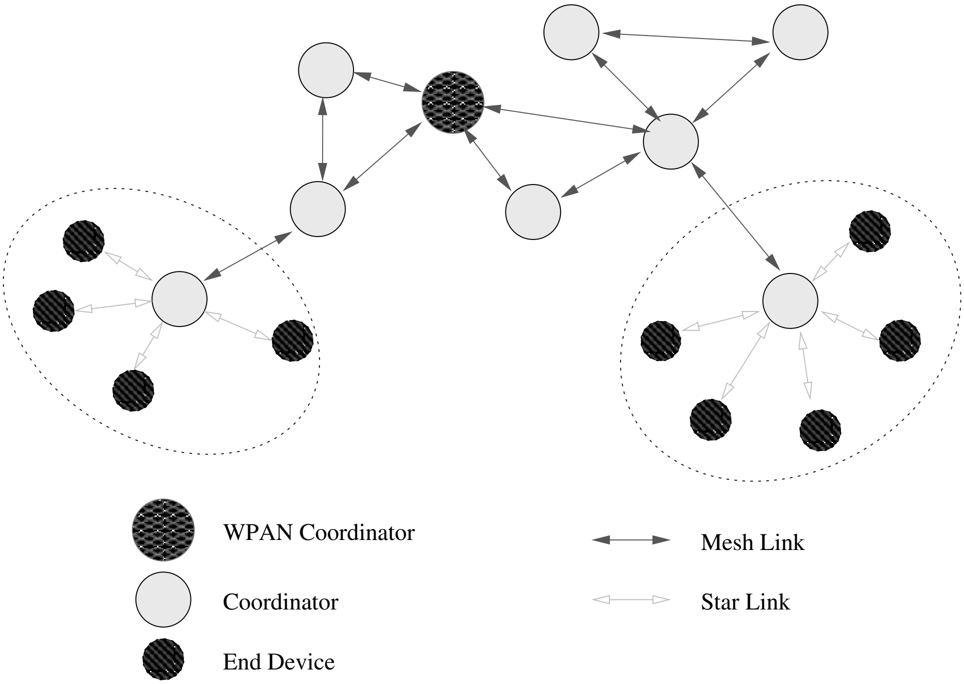

Figure 10.3 802.15.5 meshed wireless PANs

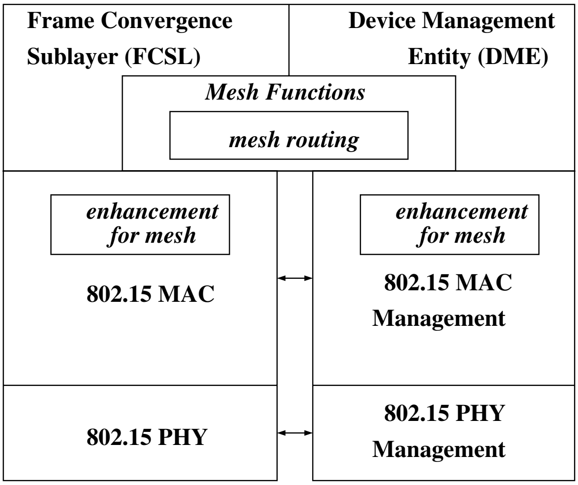

Figure 10.4 Protocol stack of 802.15.5 meshed wireless PANs

The standard for the HR meshed wireless PANs will need to consist of the following enhancements or new components.

- *MAC.* The major change of the MAC protocol is at the coordinator. Because of the mesh topology, a coordinator needs to control end devices and coordinate resource allocation with other coordinators. Other issues such as mobility, QoS, and beacon management also need to considered. Mechanisms such as multiple beacons per superframe, reservation negotiation, and efficient spatial reuse schemes are being developed for the new standard.

- *Routing.* Because of the mesh networking, packet transmission between two devices controlled by two different coordinators may have different paths. Thus, a new routing protocol is needed to select the best path for robustness, reliability, load balancing, etc. Currently, multiple proposals for the routing protocol are being considered in 802.15.5. All such protocols are tree-based routing schemes. Some of them are centralized schemes, while others are distributed. How to efficiently support multicast routing is another task that needs to be done for 802.15.5 routing.

- *Security.* Security in a star network controlled by a single coordinator is simple. However, where a mesh network has different coordinators, security becomes a much more challenging issue. Firstly, a wireless PAN coordinator must be able to ensure that another wireless coordinator being connected as a mesh peer is a trusted node. Secondly, as explained in Chapter 6, various security attacks can occur in a multihop mesh network. Without a fully trusted and central authority, achieving a completely secure meshed wireless PAN is a difficult task for the 802.15.5 task group.

Low Rate Mesh

Low rate (LR) meshed wireless PANs are currently being standardized based on 802.15.4b. Major applications of LR meshed wireless PANs include automation and control, monitoring and sensing, location services, entertainment, and so on.

The challenges of the LR mesh are different from the HR mesh. The critical requirements of an LR mesh are as follows.

- *Reliability.* LR mesh wireless PANs can be used for mission-critical applications in which transmission rate may not be important but end-to-end reliability is a necessity.

- *Power consumption.* The nodes in an LR mesh need extremely power-efficient solutions so that they can run entirely on battery for long periods.

- *Large coverage area.* By contrast with the HR mesh, a LR mesh usually supports applications that need a much larger coverage area of meshed wireless PAN services. Thus, end-to-end communications may go through a large number of hops. Together with the tighter requirement of power consumption, protocols designed for LR mesh demands a higher efficiency.

In the 802.15.5 task group, MAC enhancement is still minimal and the focus so far is still in the routing part. Since MAC plays an important role in a mesh network, we believe that more effort will be put into MAC enhancement once progress on the routing part is on the right track.

In the current proposals for the routing protocol for LR mesh, the focus is still on tree-based schemes. For the purpose of both routing and addressing, a scheme is being specified for building up a meshed adaptive tree. The meshed adaptive tree schemes avoid the problem of running out of addresses. In addition, based on the meshed adaptive tree, routing protocols are developed. For unicast routing, the meshed adaptive tree provides the basic functions of routing. Moreover, optimized routing is achieved through distributed link state routing. For multicast routing, shared multicast trees for different multicast groups are constructed based on the meshed adaptive tree built by the unicast routing.

10.4.3 UWB-Based Meshed Wireless PANs

Since the end of IEEE 802.15.3a, major activities in UWB wireless networking occur in two industrial consortiums: WiMedia Alliance and UWB Forum. The UWB of WiMedia is based on multiband OFDM, while that of UWB Forum is based on direct sequence UWB (DS-UWB). Both consortiums consist of many companies. However, currently, it looks as if WiMedia's UWB has received major wins in competition. WiMedia is backed by the USB forum for certified wireless USB, and has also been picked by Bluetooth SIG to integrate WiMedia UWB technology into future versions of Bluetooth.

WiMedia Alliance Versus UWB Forum

The UWB technologies of WiMedia Alliance and UWB Forum are quite different in the physical layer. There are also significant differences in the MAC layer, as explained below.

- The MAC protocol in UWB Forum is mostly inherited from IEEE 802.15.3, while WiMedia UWB developed its own MAC protocol. Thus, the MAC of UWB Forum still follows the concept of piconet, while WiMedia UWB does not.

- Because of the piconet architecture, the interference between different groups of nodes in various piconets cannot be avoided in a UWB Forum MAC. However, in WiMedia UWB MAC, all nodes are treated equivalently, and the entire network is distributed.

- In the MAC of UWB Forum, each piconet has the same superframe in which only one beacon can be sent in the beacon period. However, in a WiMedia UWB MAC, multiple beacons can be sent in a superframe for the purpose of handling different beacon groups for the nodes in the distributed network. With multiple beacons per superframe, nonconflict beacon transmission can be achieved. Also, a simpler mechanism can be applied to avoid interference between nodes in different beacon groups.

- The MAC of UWB Forum is similar to 802.15.3, and so the 802.15.5 mesh networking standard is applicable. However, it will not be straightforward to apply this standard to WiMedia UWB.

Since the UWB technology of UWB Forum is very close to 802.15.3, we will focus on WiMedia UWB in the next subsection. We will also point out what is still missing from the WiMedia MAC for meshed wireless PANs.

WiMedia UWB

Through the European association for standardizing information and communication systems, i.e., ECMA, WiMedia Alliance published two standards on UWB technology in December 2005. ECMA-368 is a standard on UWB MAC and physical layer technologies, while ECMA-369 is a standard for the interface between the MAC and physical layers specified in ECMA-368.

Overview of WiMedia UWB Physical Layer According to ECMA-368, the UWB physical layer utilizes the 3.1–10.6 GHz unlicensed frequency bands, and can support data rates of 53.3 Mbps, 80 Mbps, 106.7 Mbps, 160 Mbps, 200 Mbps, 320 Mbps, 400 Mbps, and 480 Mbps. The UWB spectrum is divided into 14 bands, each with a bandwidth of 512 MHz. Among the 14 bands, 12 are split into four band groups each consisting of three bands, and the remaining bands form the fifth band group. In each band, one OFDM symbol consists of 110 subcarriers (100 data subcarriers and 10 guard subcarriers) to transmit information and 12 pilot subcarriers for coherent detection. For each data stream, it is firstly coded via convolutional code. The coded data is then spread using a time-frequency code (TFC) within a band group. There are two types of TFC code: one is time-frequency interleaving (TFI) and the other is fixed frequency interleaving (FFI). Via TFI, the coded data is interleaved over three bands, while using FFI, the coded data is only sent in a fixed band. In ECMA-368, several different TFC codes are defined in each of the first four band groups: four using TFI and three using FFI. Thus, several channels are allowed in each of the first four band groups. In the fifth band group, only two FFI TFC codes are defined. Thus, within the 14 bands, there are a total of 30 channels specified.

WiMedia UWB MAC For a WiMedia MAC, the time axis is divided into superframes. Each of them consists of 256 medium access slots for a total length of 65536 µs. It is further divided into three periods: beacon period (BP) and data transmission period. The data transmission period consists of a reservation period and a prioritized contention access (PCA) period.

Each superframe starts with BP, and the starting time is called BPST. A BP is composed of multiple beacon slots. Thus, a node can receive multiple beacons from different nodes. The length of a BP can be extended to support the variable number of nodes in the range. To avoid the same beacon slot being used by nodes within two hops but allowing the reuse by nodes that are more than two hops apart, the occupancy information of these beacon slots needs to be sent as BP occupancy IE (BPOIE) in each beacon. Neighbors can use such information to choose their beacon slot or effectively resolve beacon collisions. Because of a multibeacon BP in the superframe, interference between different beacon groups of nodes can be effectively reduced. For the same reason, 802.15.5 is also trying to adopt the same superframe structure. Based on a multibeacon BP, beacon groups can easily be merged as an extended beacon group.

Based on the superframe and beacon operation, there are two options for data transmission: prioritized contention access (PCA) and reservation via distributed reservation protocol (DRP).

PCA is similar to 802.11e EDCA. The major difference is that clear channel assessment (CCA) is not based on energy level detection, owing to the low power characteristics of UWB.

Instead, CCA is done through preamble sensing. PCA is used for non-real-time traffic, and any medium access slots that are not reserved by DRP can be used for PCA.

There are two mechanisms of DRP: implicit DRP and explicit DRP. In the implicit DRP, the reservation owner and target send reservation information in the DRP IE of a beacon. In the explicit DRP, the reservation owner and target need to use DRP Reservation Request and DRP Reservation Response frames to negotiate the desired reservation. In either mechanism, there are five types of reservations: alien BP, hard, soft, private, and PCA reservations. Alien BP reservation is for reserving medium access slots to protect alien BPs. Hard reservation is for reserving medium access slots for reservation owner and target, and no other nodes can use such slots. As soon as it is not used, it needs to be released for PCA. Soft reservation permits PCA, but the reservation owner has priority to access it. Private reservation consists of access slots for reservation owner and target, but it can be used by other access schemes that are not specified by WiMedia MAC. PCA reservation is used to reserve medium access slots exclusively for PCA. No other access schemes or devices can access a PCA reservation.

As we can see in WiMedia UWB MAC, how to support mesh networking is not specified. In particular, the DRP does not consider the multihop resource allocation. For example, when time slots need to be allocated to all links in a multihop path between two end nodes, DRP needs to be extended such that reservation negotiation can be done for multiple hops. No routing protocol is specified for path selection for a multihop end-to-end transmission. Thus, if an end-to-end reservation is needed for a multihop path, then layer-3 routing protocol is needed to map end-to-end multihop reservation process into the one-hop DRP reservation process. Combining a layer-3 routing protocol and DRP, end-to-end reservation can be accomplished. However, an interface protocol between routing and MAC needs to be developed. More importantly, such a solution results in a low performance mesh network, since the routing path selection and slot allocation are not considered together.

10.4.4 Remaining Issues in Standards for Meshed Wireless PANs

Technologies for meshed wireless PANs evolve quickly, but the standardization process does not seem to keep up with the pace. For both IEEE 802.15.5 and WiMedia, specifications for the MAC protocol for meshed wireless PANs are far from being completed.

For 802.15.5, the standardization process is still in its early phase. Its future is still uncertain for several reasons. First, many key components of the standard have not been defined yet. Second, performance of the existing proposals lacks enough evaluation. For example, for both HR meshed wireless PANs and LR meshed wireless PANs, routing protocols are all tree-based. However, whether such schemes are good for mesh networks is still a question. Lastly, the 802.15.5 will only be a recommended practice rather than a mandatory standard. Thus, there is a possibility that companies will not follow this standard but use other proprietary solutions, which will definitely cause an interoperability issue.

For WiMedia UWB, DRP is a critical module that handles resource allocation in a distributed network. Unfortunately, in the current version, DRP has not considered the operation of a multihop network as in meshed wireless PANs. Thus, resource request messages are not relayed over multiple hops and resource allocation is only optimized for one-hop neighbors. Thus, significant work is needed to extend DRP. However, routing protocol is not specified in the current WiMedia standards. For the purpose of interoperability and performance enhancement, specifying routing protocol in the MAC layer needs to be done for WiMedia MAC.

For both 802.15.5 and WiMedia Alliance, cross-layer design between MAC and routing has not yet been considered. In 802.15.5, the MAC and routing are still being considered as separate modules. In WiMedia standards, since no routing is specified, cross-layer is totally out of the question. However, as explained in Chapter 9, in a TDMA-like mesh network, routing and MAC work together so closely that they need to function as interactively as possible; otherwise, the performance of the meshed PANs could be low.

Another issue that has not been considered in standards is multichannel operation, which can greatly increase the performance of meshed wireless PANs.

10.5 Standards for Meshed Wireless MANs

10.5.1 Overview of IEEE 802.16 Standard Activities

IEEE 802.16 standards are targeted at broadband wireless access in MAN. QoS is always an important concern for any 802.16 standard. Thus, from the beginning, service specific convergence sublayer, QoS mechanism, per-connection traffic flow management, and scheduling schemes for connections are all covered in the IEEE 802.16 standards.

The standardization process in IEEE 802.16 is a little different from that in 802.11 and 802.15 in the sense that standards for different perspectives of wireless MANs are consolidated more efficiently.

The first IEEE 802.16 standard was approved in December 2001 as a result of the 802.16.1 project. In this version, the frequency bands of 10–60 GHz are considered. In the MAC layer only point-to-multipoint (PMP) mode is specified, while the physical layer is only focused on single carrier (SC) technologies including both FDD and TDD. Other than these two layers, other sublayers such as service specific convergence sublayer, MAC common part sublayer, and privacy sublayer are also specified. The system profiles are updated and expanded in the IEEE 802.16c standard released in December 2002. The sets of features and functions to be used in typical implementation cases are listed in such system profiles.

For frequency bands of 2–11 GHz, another standard, IEEE 802.16a, was released in April 2003. As compared to previous versions of the IEEE 802.16 standards, several major differences need to be noted in this version. First of all, owing to the longer wavelength in this frequency band, line of sight (LOS) is not necessary and multipath may be significant. This requires the physical layer to have the ability to support near- or non-line-of-sight (NLOS) environments. Such an ability demands techniques such as advanced power management, interference mitigation/coexistence, and multipath antennas. Also, multicarrier technologies such as OFDM and OFDMA are adopted into IEEE 802.16a. Owing to the lossy wireless medium in this frequency band, the MAC layer also needs per-connection based ARQ. Secondly, the frequency band also covers a license exempt band primarily in 5–6 GHz. Thus, an addition feature such as dynamic frequency selection (DFS) must be supported. Starting from IEEE 802.16a, all IEEE 802.16 standards include the specifications of five types of physical layer, i.e., wirelessMAN-SC for 10–60 GHz, wirelessMAN-SCa for 2–11 GHz licensed bands, wirelessMAN-OFDM for 2–11 GHz licensed bands, wirelessMAN-OFDMA for 2–11 GHz licensed bands, and wirelessHUMAN (high-speed unlicensed MAN) for 2–11 GHz unlicensed bands.

Interestingly, owing to multipath and NLOS, the throughput and coverage of the wireless LAN can be compromised in a traditional PMP mode. Thus, a mesh mode is specified as an optional topology for IEEE 802.16a with wirelessMAN-OFDM or wirelessHUMAN physical layer. We will discuss the mesh mode in detail in Section 10.5.2.

In October 2004, a new version of the IEEE 802.16 standard was released. This version not only corrected errors and inconsistencies in previous versions, but also consolidated 802.16.1, 802.16c, and 802.16a. Thus, all the five types of physical layers, PMP and mesh modes, DFS, and so on are all covered in IEEE 802.16-2004. IEEE 802.16-2004 was completed under the project of IEEE 802.16d and 802.16-REVd. In September 2005, the specifications of management information base (MIB) for the MAC and physical layer and their associated management procedures are approved as a new standard, 802.16f.

However, in all the above IEEE 802.16 standards, only fixed systems are considered. In reality, there are many application scenarios where subscriber stations actually demand mobility support. The first version of the IEEE 802.11 standard that can support mobility was released in December 2005 as IEEE 802.16e. It expands the 2004 version of the IEEE 802.16 standard to allow for mobile subscriber stations.

Currently, there are still several active task groups.

In the network management task group, in addition to the completed work of IEEE 802.16f, three projects remain active. IEEE 802.16k works on amendment to IEEE 802.1D on 802.16 bridging functionality, IEEE 802.16g focuses on management plane procedures and services, and IEEE 802.16i expands the work of 802.16f and provides amendment to the mobile management information base.

For 2–11 GHz unlicensed bands, solution to the coexistence issue is still being specified in the license-exempt task group IEEE 802.16h. Maintenance of all IEEE 802.16 standards and the task of overseeing the standardization process are done by the Maintenance Task Group.

Lastly but also most interestingly to us, a new task group was approved by the IEEE Standards Association in early 2006 to focus on the functionalities of mobile multihop relay in wireless MANs. This new task group is IEEE 802.16j. Its purpose is to enhance the coverage, throughput, and system capacity of 802.16 networks by specifying multihop relay functionalities via relay stations. The relay stations are interoperable with base stations and do not need any change in subscriber stations. IEEE 802.16j enhances the physical layer of OFDMA to support multihop relay. It also needs to enhance MAC layer functionalities. IEEE 802.16j is only concerned with licensed bands. We will study the details of mobile multihop relay of 802.16j in Section 10.5.3.

A summary of all IEEE 802.16 task groups/standards is shown in Table 10.4 in chronicle order.

10.5.2 IEEE 802.16 Mesh Mode

Network Architecture of Mesh Mode

In PMP mode, direct communications links exist only between a base station (BS) and subscriber stations (SSs). However, in mesh mode direct communications among SSs, and between a BS and SSs, are all possible. Thus, BSs and SSs become mesh BSs and mesh SSs in mesh mode. A mesh BS is the BS that has connection to backhaul services. Thus, a generic architecture for mesh mode is as follows. A top tier 802.16 BS node covers a few mesh BSs via the PMP mode, and in the second tier a mesh BS provides backhaul access for many

Table 10.4 Summary of IEEE 802.16 task groups and standards

Standards/task groups	Objective and focus	Status
802.16.1	The first version of the IEEE 802.16 standard. The physical layer is single carrier and only PMP mode is considered in the MAC layer. Frequency bands are in 10–60 GHz. Only fixed systems considered	Approved in December 2001
802.16c	Expand 802.16.1 on system profiles	Approved in December 2002
802.16a	The first IEEE 802.16 standard in 2–11 GHz. Five options of physical layer are specified. Mesh mode is included in this version	Approved in January 2003
802.16-2004	Provide corrections to IEEE 802.16.1 and consolidate 802.16.1, 802.16c, and 802.16a. Only fixed systems are considered. This work was done in task group 802.16d and 802.16-REVd	Approved in June 2004
802.16f	Expand 802.16-2004 on MIB	Approved in September 2005
802.16e	Expand 802.16-2004 to allow for mobility in subscriber stations	Approved in December 2005
802.16g	Part of management task group. Amend 802.16 on management plane procedures and services	Active
802.16i	Part of management task group. Amend 802.16 on mobile MIB	Active
802.16k	Part of management task group. Amend 802.1D for 802.16 bridging functionality	Active
802.16h	Specify coexistence procedures in license-exempt bands	Active
802.16j	Enhance 802.16/2004 and 802.16e to support mobile multihop relay. Enhancements are carried out in wirelessMAN-OFDMA physical layer and MAC layer. Relay stations and base stations need to be interoperable. No change is needed for subscriber stations	Active

mesh SSs. The mesh BS and its mesh SSs form a cluster of mesh nodes. Within the cluster, mesh networking is used to connect the different nodes. Direct communications between mesh nodes in different clusters are not necessary. When a new node joins the network, the network entry process will help the new node find the best mesh BS of a particular cluster. Thus, to investigate the mesh mode of 802.16, we can focus on one mesh cluster that consists of one mesh BS and a number of mesh SSs.

Motivation of Mesh Mode

In PMP mode, 802.16 networks experience several issues. Especially in the 2–10 GHz frequency bands, due to NLOS and multipath fading, there are coverage holes. In addition, the one-hop throughput may be low when the distance between the BS and a SS is large. However, mesh networks can avoid such issues. In the mesh mode, nodes can choose the best link to communicate, which not only avoids coverage holes but also increases the transmission rate. Moreover, for the same end-to-end flow, multihop communications can achieve higher throughput than that of single one-hop communications. This is because the physical layer transmission rate drops quickly as the communication distance increases beyond a certain point.

Consequently, mesh mode can greatly improve coverage and throughput, which potentially enhance the QoS and scalability of 802.16 wireless MANs. However, it also involves several challenges.

- Formation of the mesh network. There need to be efficient and secure procedures to manage the mesh network.
- Synchronization in a multihop mesh network. This is more challenging than in the centralized PMP mode.
- More complicated MAC-routing inter-dependence. In PMP mode, MAC is totally handled by the central node, the BS. Also, routing is simple. However, in mesh mode, mesh routing protocol is needed and the MAC is concerned with more than one hop.
- Tradeoff between power and transmission rate in the physical layer.

These issues have not been addressed in the specifications of mesh mode in 802.16 standards.

Major Protocol Components of Mesh Mode

Network Entry Process When a new node arrives, it follows the network entry process to join the mesh network. The detailed procedure is explained in Chapter 3.

During the network entry process, a mesh node selects a sponsor node, does coarse synchronization, and performs DFS. Then, it works together with the sponsor node to check authentication, perform fine synchronization, and other higher layer functions such as DHCP.

Once the mesh node becomes part of the mesh network, it needs to manage its links and neighbors.

Link and Neighbor Management Once a mesh node joins the mesh network, in addition to the link to the sponsor node, it also needs to establish links to all its neighbors. First of all, the mesh node must determine the link qualities to all its neighbors. Then, it selects the neighbors to which the link qualities are satisfactory. In order to set up a link from the new mesh node its neighbor, a challenge-response security process is followed.

- The mesh node first sends a challenge to its neighbor. This message contains HMAC {Operator Shared Secret, frame number, Node ID of the new mesh node, Node ID of the neighbor node}, where the Operator Shared Secret is a private key obtained from the provider, and the frame number is the last known frame number in which the neighbor node sent a Mesh Network Configuration (MSH-NCFG) message.

- Once the neighbor receives the challenge, it computes the same value as in previous item. If the computed value does not match the received one, it sends back a rejection. Otherwise, it sends a challenge-response, which contains HMAC{Operator Shared Secret, frame number, Node ID of the neighbor node, Node ID of the new mesh node}.

- Upon reception of the response, the new mesh node computes the same value as in the previous item and compares it. If the computed one does not match the received value, then a rejection is returned. Otherwise, the new mesh node sends back an *Accept*, in which a randomly selected but unused link ID is included.

One the challenge-response process is successfully done, a new link is created between the new mesh node and the selected neighbor. From now on, the selected link ID is used to indicate the actual link from the new mesh node to the neighbor.

It should be noted that the numbers of bits in node ID and link ID are 16 and 8, respectively. Moreover, link ID is part of the connection ID for each mesh node.

Connection Management In mesh mode, connections are not explicitly set up; otherwise, the network would be swamped with signaling messages. Instead, the 16-bit connection ID (CID) is formed as follows. The second byte of the CID is for link ID, which actually tells the receiver about this connection. If its value is 0xFF, then the packet in the connection ID is a broadcast message. The first byte conveys information such as priority, reliability, and so on. More specifically, the eight bits consist of the following fields.

- Two bits for message types such as MAC management, IP packets, etc.

- One bit to indicate whether ARQ is enabled or not

- Three bits to set traffic class and priority

- Two bits to indicate the drop precedence

According to this mesh CID structure, we know that once a link is established, 64 connections can be set up for this link. Among them, when the first byte is 0xFF, the second byte should be the network ID. Such a CID means that a broadcast message is being sent to an intended network.

As in the PMP mode, QoS and resource allocation are done based on CID. However, the scheduling schemes in mesh mode are very different from those of PMP mode.

Packet Transmission According to Different Scheduling Options To enable us to understand the different scheduling schemes, the frame structure needs to be studied first. In the mesh mode, only TDD is considered in 802.16 standards. Each frame consists of two subframes: a control subframe and a data subframe. Depending on the different messages sent in the control subframe for various purposes of network operation, two types of control

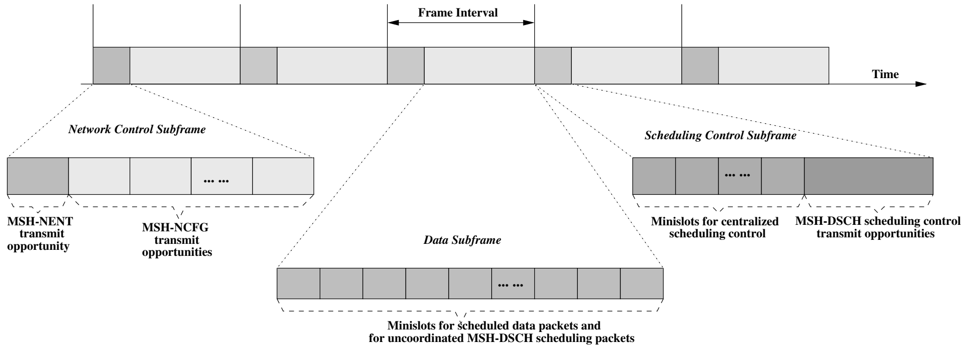
Frame Interval
Time
Network Control Subframe
... ...
MSH-NENT transmit opportunity
MSH-NCFG transmit opportunities
Scheduling Control Subframe
... ...
Minislots for centralized scheduling control
MSH-DSCH scheduling control transmit opportunities
Data Subframe
... ...
Minislots for scheduled data packets and for uncoordinated MSH-DSCH scheduling packets

Figure 10.5 Subframe-scheduler mapping in 802.16 mesh mode

subframe can be identified. In the first type, the control subframe consists of minislots for network entry and network configuration, and is thus called the network control subframe. For the second type, the control subframe is dedicated to sending different scheduling messages, and is thus called the schedule control subframe. The frames with a network control subframe only occur periodically, and the period is a system parameter. All other frames in the time axis have a schedule control subframe.

As presented in Chapter 3, there are three types of scheduling schemes for transmissions of data packets. In addition, scheduling schemes are needed for network control and configuration messages. Thus, in order to design different algorithms for various scheduling schemes, a first step is to map transmissions of different types of schedulers into separate time slots in a TDMA frame of 802.16 mesh networks.

As shown in Figure 10.5, each frame consists of a control subframe and a data subframe. The network control subframe and the schedule control subframe do not exist in the same frame, but occur periodically in different frames. In a network control subframe, one transmission opportunity is allocated to network entry related messages, while other transmission opportunities are allocated to send mesh network configurations. In a schedule control subframe, some minislots are allocated to sending control messages of centralized scheduling (MSH-CSCH) and other transmission opportunities are assigned to control messages of coordinated distributed scheduling (MSH-DSCH). The length of the control subframe (MSH-CTRL-LEN) is fixed and the total number of OFDM symbols is MSH-CTRL-LEN multiplied by seven, where MSH-CTRL-LEN is a parameter specified in the network descriptor. Thus, the size of minislots for data subframes is determined by

$$(\mathit{OFDM\ symbols\ in\ one\ frame} - (\mathit{mesh\ control\ subframe\ length} \times 7))/256.$$

It should be noted that the control messages of uncoordinated distributed scheduling are sent in data subframes.

From Figure 10.5, we know that control subframes provide transmission opportunities for sending the control messages about different scheduling schemes. However, in a mesh network, accessing such opportunities needs to be coordinated in order to ensure protocol efficiency. In a schedule control subframe, this task can be easier, since the minislots for MSH-CSCH and MSG-DSCH are centrally controlled by mesh BS. For a network control subframe, no central control exists, and the limited number of transmission opportunities for different nodes are shared via an election-based method, as specified in the 802.16 standards.

Corresponding to this subframe-scheduler mapping in Figure 10.5, we know that all the scheduled data transmissions occur in the data subframe. For uncoordinated distributed scheduling, before the minisots for sending data packets are determined, the control messages are also sent in the data subframe. This is the major difference between a coordinated and an uncoordinated distributed schedule scheme. Thus, in the data plane, there are flows of scheduled data packets and control messages of uncoordinated distributed scheduling. All other traffic flows, such as network entry related messages, network configuration messages, control messages for centralized scheduling, and coordinated distributed scheduling, all occur in the control plane.

Remaining Issues of Mesh Mode

Although mesh mode has advantages over PMP mode, it still lacks the following features.

- *Mobility.* In 802.16a, mobility in subscriber stations is not considered. However, for more and more application scenarios, mobility is a compelling need. Although 802.16e has considered mobility in SSs, the related issues in mesh mode are not resolved. For example, links or connections can change quickly owing to mobility in a mesh network.

- *Full and extended coverage.* It is true that mesh mode provides a better coverage than PMP mode. However, in certain environments, especially in terrain or city areas, some locations may still have no coverage because of severe multipath fading, reflections, and so on. Thus, simply basing on a mesh BS and SSs is not an efficient scheme to provide full coverage. However, if we want to extend the coverage to some isolated areas, IEEE 802.16 mesh mode is not an effective solution.

- *High capacity.* In 802.16 networks, a large percentage of traffic will go to or come from backbone networks. In mesh mode, such traffic has to go through the mesh BS via other SSs. Such a mechanism has two shortcomings. First, the SSs also have high traffic load, which can impact their performance in forwarding traffic. Second, the number of hops via SSs can be large. When SSs are mobile, these problems become even more severe.

10.5.3 IEEE 802.16j

In order to further improve the performance of 802.16 networks, a new operation mode is being standardized in the 802.16j task group. This operation mode is called mobile multihop relay (MMR). As the name implies, MMR aims to support mobile stations (MSs), improve network capacity, enhance coverage, and extend coverage for 802.16 networks by using relaying stations through multihop networking.

Network Architecture of MMR

A typical architecture of 802.16j MMR is illustrated in Figure 10.6. There are four types of nodes in the network: one BS, multiple relay stations (RSs), and supported SSs or MSs. An RS can be classified into three types: fixed, nomadic, and mobile RS. A fixed RS (FRS) is

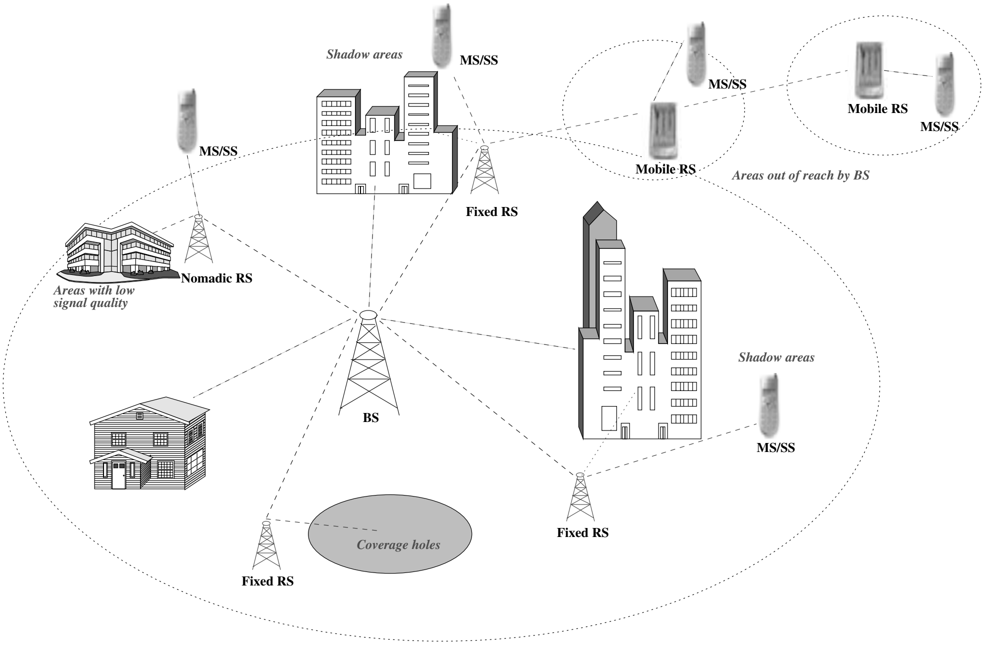

Figure 10.6 The network architecture of 802.16 mobile multihop relay

an RS installed at a permanent location. If the location of an RS can be changed but is fixed for periods comparable to a session of user traffic, then such an RS is called a nomadic RS (NRS). A mobile RS (MRS) can relay traffic while moving. Comparing the mesh mode and MMR, we notice two major differences between them.

- The network topology is not a pure mesh network anymore. Instead, the topology is actually a tree topology. From the BS to relay stations (RSs) and then to SSs or to MSs is a tree-like topology. The BS is a root node.
- Additional nodes, i.e., RSs, are included in the network to improve capacity, enhance mobility support, and extend coverage.

Standardization Status

We are still at an early stage in finalizing the standard of 802.16j. However, to make MMR a viable solution, the scope of this task group must consider the following features.

- In an MMR network, for the purpose of backward compatibility, SSs and MSs must be exactly the same as those in an 802.16 network without MMR. Thus, from RSs or the BS to MSs/BSs must use the same OFDMA PMP links as those in 802.16e.
- Both mobile and fixed subscriber stations should be supported by the BS and RSs. Thus, both the BS and RSs must be 802.16e compatible. In other words, from the BS to RSs, or from one RS to another RS, the link must be OFDMA PMP.

- All three types of RS must work together under the same MMR network architecture. Because of multihop networking on an RS, in addition to the OFDMA PMP link, an MMR link must be added. Also, traffic aggregation must be considered at each RS.
- The BS also needs to work together with all types of RS. Thus, its functionalities need to be extended to support MMR links and traffic aggregation from RSs.
- Security and management functionalities must be added to the BS and RSs to maintain the security and reliability of both MMR and PMP links.
- The complexity of RSs must be much lower than a BS.

Technical Challenges in MMR

In MMR mode, many challenging issues need to be resolved. Most of them are being tackled by participants of the 802.16j task group. However, it is also reasonable to believe that some challenging issues still remain to be resolved even after a version of the 802.16j standard is released. Nevertheless, here we point out the following major challenging issues in different protocol layers where MMR mode is concerned.

- *Routing protocol.* Considering tree topology, multihop wireless networking, coexistence of MMR and PMP links, and mobility, developing an efficient routing protocol is necessary. For example, a conventional tree-based routing protocol or ad hoc routing protocol may not fit well into this framework.
- *MAC protocol.* Multiple issues are involved in the MAC protocol layer.
  - *Resource management.* This includes the tasks of scheduling packet transmission, radio resource management, power control, and so on. Whether centralized, distributed, or hybrid schemes are most effective also needs investigation.
  - *Frequency planning for MMR and PMP links.* Algorithms in the MAC layer are needed to coordinate or spatially reuse frequencies in different links.
  - *Call admission control and traffic shaping.* Efficient mechanisms need to be developed to check if a call can be accepted in a multihop distributed network. For admitted calls, traffic shaping policies need to be selected.
  - *QoS.* Both resource management and admission control are related to QoS. However, more functionalities are needed in order to really guarantee QoS. For example, load-balancing in various links of the MMR network and congestion control or flow control.
- *Cross-layer design between MAC and routing protocols.* Since selecting a routing path is related to load-balancing and scheduling, and vice versa, MAC and routing protocols need to be designed considering cross-layer optimization.
- *Advanced physical layer techniques.* Advanced physical layer techniques need to be enhanced or improved for MMR owing to mobility and multihop networking. The MAC protocol needs to efficiently utilize advanced features such as MIMO and beamforming in the physical layer.

- *Network management and configuration.* RSs are expected to be self-maintained and self-configured. Thus, new network management protocols need to be developed to manage the node entry process, node configuration, handoff/roaming, and so on.

- *Security.* Because of both mobility and multihop networking, security is more difficult to guarantee than in the mesh mode. Thus, potential new security attacks in MMR need to be studied, and corresponding solutions explored.

References

[1] Aboba B, Blunk L, Vollbrecht J, Carlson J and Levkowetz H 2004 Extensible authentication protocol (EAP), *IETF RFC 3748*.

[2] Aboba B and Simon D 1999 PPP EAP TLS authentication protocol, *IETF RFC 2716*.

[3] Acharya A, Misra A and Bansal S 2003 High-performance architectures for IP-based multihop 802.11 networks. *IEEE Wireless Communications* 22–28.

[4] Adya A, Bahl P, Padhye J, Wolman A and Zhou L 2004 A multi-radio unification protocol for IEEE 802.11 wireless networks. In *Proc. Annual International Conferences on Broadband Networks (BroadNets).*

[5] Akan OB and Akyildiz IF 2004a ARC: the analytical rate control scheme for real-time traffic in wireless networks. *IEEE/ACM Transactions on Networking* **12**(4), 634–644.

[6] Akan OB and Akyildiz IF 2004b ATL: an adaptive transport layer suite for next-generation wireless internet. *IEEE Journal on Selected Areas in Communications* **22**(5), 802–817.

[7] Akyildiz IF, Wang X and Wang W 2005 Wireless mesh networks: a survey. *Computer Networks Journal (Elsevier)* **47**(4), 445–487.

[8] Akyildiz IF and Wang X 2005 A survey on wireless mesh networks. *IEEE Communications Magazine* **43**(9), s23–s30.

[9] Akyildiz IF and Wang X 2008 Cross-layer design in wireless mesh networks. *IEEE Transactions on Vehicular Technology 57*2, 1061–1076.

[10] Akyildiz IF, Su W, Sankarasubramaniam Y and Cayirci E 2002 Wireless sensor networks: a survey. *Computer Networks Journal, Elsevier* **38**(4), 393–422.

[11] Akyildiz IF and Kasimoglu IH 2004 Wireless sensor and actor networks: research challenges. *Ad Hoc Networks Journal, Elsevier* **2**, 351–367.

[12] Akyildiz IF, McNair J, Ho JSM, Uzunalioglu H and Wang W 1999 Mobility management in next-generation wireless systems. *IEEE Proceedings Journal* **87**(8), 1347–1385.

[13] Akyildiz IF, Xie J and Mohanty S 2004 A survey of mobility management in next-generation all-IP-based wireless systems. *IEEE Wireless Communications* **11**(4), 16–28.

[14] Alamouti SM 1998 A simple transmit diversity technique for wireless communications. *IEEE Journal on Selected Areas in Communications* **16**(8), 1451–1458.

[15] Aldous D and Fill J 2001 Reversible Markov chains and random walks on graph. In *online link: http://www.stat.berkeley.edu/users/aldous/RWG/book.html*

[16] Alicherry M, Bhatia R and Li L 2005 Joint channel assignment and routing for throughput optimization in multi-radio wireless mesh networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 58–72.

[17] Allman M, Paxson V and Stevens W 1999 TCP congestion control. *IETF RFC 2581*, pp. 66–70.

[18] Alimi R, Li L, Ramjee R, Viswanathan H and Yang Y 2008 iPack: in-network packet mixing for high throughput wireless mesh networks. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM).*

Wireless Mesh Networks Ian F. Akyildiz and Xudong Wang

[19] Amir Y, Danilov C, Musaloiu-Elefteri R and Rivera N 2007 An inter-domain routing protocol for multi-homed wireless mesh networks. In *Proc. IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM),* pp. 1–10.

[20] Andersen JB 2000 Array gain and capacity for known random channels with multiple element arrays at both ends. *IEEE Journal on Selected Areas of Communications* **18**(11), 2172–2178.

[21] Aryafar E, Gurewitz O and Knightly E 2008 Distance-1 constrained channel assignment in single radio wireless mesh networks. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 762–770.

[22] Avallone S and Akyildiz, IF and Ventre G 2008 A channel and rate assignment algorithm and a layer-2.5 forwarding paradigm for multi-radio wireless mesh networks. *IEEE/ACM Transactions on Networking*, 1–14.

[23] Awerbuch B, Holmer D, Nita-Rotaru C and Rubens H 2000 An on-demand secure routing protocol resilient to Byzantine failures. In *Proc. ACM Workshop Wireless Security (WiSE),* pp. 21–30.

[24] Bahl P, Chandra R and Dunagan J 2004 SSCH: slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 216–230.

[25] Bakne A and Badrinath BR 1995 I-TCP: indirect TCP for mobile hosts. In *Proc. 15th IEEE International Conference on Distributed Computing Systems,* pp. 136–143.

[26] Balakrishnan H, Seshan S and Katz RH 1995 Improving reliable transport and handoff performance in cellular wireless networks. *ACM/Kluwer Wireless Networks* **1**(4), 469–481.

[27] Balakrishnan H, Padmanabhan VN and Katz RH 1999 Network asymmetry: the effects of asymmetry on TCP performance. *ACM Kluwer Mobile Networks and Applications (MONET)* **4**, 219–241.

[28] Bansal N and Liu Z 2003 Capacity, mobility and delay in wireless ad hoc networks. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 1553–1563.

[29] Baumann R, Lenders V, Heimlicher S and May M 2007 HEAT: scalable routing in wireless mesh networks using temperature fields. In *Proc. IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM),* pp. 1–9.

[30] Belding-Royer EM, Melliar-Smith PM and Moser LE 2001 An analysis of the optimum node density for ad hoc mobile networks. In *Proc. IEEE International Conference on Communications (ICC)* **3**, pp. 857–861.

[31] Belding-Royer EM 2003 Multi-level hierarchies for scalable ad hoc routing. *ACM/Kluwer Wireless Networks (WINET)* **9**(5), 461–478.

[32] Belding-Royer EM and Perkins CE 2003 Evolution and future directions of the ad hoc on-demand distance vector routing protocol. *Ad hoc Networks Journal* **1**(1), 125–150.

[33] Bellofiore S, Foutz J, Govindaradjula R, Bahceci I, Balanis CA, Spanias AS, Capone JM and Duman TM 2002 Smart antenna system analysis, integration and performance for mobile ad hoc networks (MANETs). *IEEE Transactions on Antennas and Propagation* **50**(5), 571–581.

[34] Bertossi AA and Bonuccelli MA 1995 Code assignment for hidden terminal interference avoidance in multihop packet radio networks. *IEEE/ACM Trans. Networking* **3**(4), 441–449.

[35] Bhandari V and Vaidya N 2007 Capacity of multi-channel wireless networks with random (c, f) assignment. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC)*, pp. 229–238.

[36] Bhatia R and Kodialam M 2004 On power efficient communication over multi-hop wireless networks: joint routing, scheduling, and power control. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 1457–1466.

[37] Biswas S and Morris R 2005 ExOR: opportunistic multihop routing for multi-hop wireless networks. In *Proc. ACM Annual Conference of the Special Interest Group on Data Communication (SIGCOMM),* pp. 133–144.

[38] Blostein SD and Leib H 2003 Multiple antenna systems: their role and impact in future wireless access. *IEEE Communications Mag.* 94–101.

[39] Borisov N, Goldberg I and Wagner D 2002 Intercepting mobile communications: the insecurity of 802.11. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 180–188.

[40] Bose P et al. 1999 Routing with guaranteed delivery in ad hoc wireless networks. In *Proc. 3rd ACM International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications,* pp. 48–55.

[41] Buttyan L and Hubaux J-P 2002 Report on a working session on security in wireless ad hoc networks. *ACM Mobile Computing and Communications Review* **7**(1), 74–94.

[42] Buttyan L and Hubaux J-P 2001 Rational exchange – a formal model based on game theory. In *Lecture Notes in Computer Science*, vol. 2232, pp. 114–126.

[43] Cali F, Conti M, and Gregori E 2000 Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit. *IEEE/ACM Trans. Networking* **8**(6), 785–799.

[44] Camp J, Mancuso V, Gurewitz O and Knightly E 2008 A measurement study of multiplicative overhead effects in wireless networks. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 76–80.

[45] Cao L and Dahlberg T 2006 Path cost metrics for multihop network routing. In *Proc. IEEE International Conference on Performance, Computing, and Communications Conference (IPCCC),* pp. 18–21.

[46] Cao M, Ma W, Zhang Q and Wang X 2007 Analysis of IEEE 802.16 mesh mode scheduler performance. *IEEE Trans. Wireless Commun.* **6**(4), 1455–1464.

[47] Cardei M, Wu J and Yans S 2006 Topology control in ad hoc wireless networks using cooperative communication *IEEE Trans. Mobile Computing* **5**(6), 711–724.

[48] Casari P, Levorato M and Zorzi M 2005 On the implications of layered space-time multiuser detection on the design of MAC protocols for ad hoc networks. In *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communication (PIMRC)*, pp. 1354–1360.

[49] Cen S, Cosman PC and Voelker GM 2003 End-to-end differentiation of congestion and wireless losses. *IEEE/ACM Trans. Networking* **11**(5), 703–717.

[50] Chandran K, Raghunathan S and Prakash R 2001 A feedback-based scheme for improving TCP performance in ad hoc wireless networks. *IEEE Personal Communications* **8**(1), 34–39.

[51] Chatterjee S, Roy S and Bandyopadhyay S 2006 Hop-efficient and power-optimized routing strategy in a decentralized mesh network using directional antenna. In *Proc. Fifth International Symposium on Parallel and Distributed Computing (ISPDC),* pp. 155–160.

[52] Chen C-C, Luo H, Seo E, Vaidya NH, and Wang X 2007 Rate-adaptive framing for interfered wireless networks. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM).*

[53] Chen WT and Chen P-Y 2003 Group mobility management in wireless ad hoc networks. In *Proc. IEEE Vehicular Technology Conference,* pp. 2202–2206.

[54] Cheng B, Yuksel M and Kalyanaraman S 2006 Orthogonal rendezvous routing protocol for wireless mesh networks. In *Proc. IEEE International Conference on Network Protocols (ICNP),* pp. 106–115.

[55] Chevillat P, Jelitto J, Barreto AN and Truong HL 2003 A dynamic link adaptation algorithm for IEEE 802.11a wireless LANs. In *Proc. IEEE International Conference on Communications (ICC),* pp. 1141–1145.

[56] Chiang M 2004 To layer or not to layer: balancing transport and physical layers in wireless multihop networks. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 2525–2536.

[57] Chiang M 2005 Balancing transport and physical layers in wireless multihop networks: jointly optimal congestion control and power control. *IEEE Journal on Selected Areas in Communications* **23**(1), 104–116.

[58] Chiang M, Low SH, Calderbank AR and Doyle JC 2007 Layering as optimization decomposition: a mathematical theory of network architectures. In *Proceedings of IEEE,* **95**(1), 255–312.

[59] Chlamtac I, Conti M and Liu J 2003 Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks Journal, Elsevier* **1**(1), 13–64.

[60] Cicconetti C, Akyildiz IF and Lenzini L 2009 FEBA: a Bandwidth Allocation Algorithm for Service Differentiation in IEEE 802.16 Mesh Networks. *IEEE/ACM Transactions on Networking*.

[61] Choi L-U, Letaief KB and Murch RD 2001 MISO CDMA transmission with simplified receiver for wireless communication handsets. *IEEE Trans. Communications* **49**, 888–898.

[62] Choudhury RR, Yang X, Ramanathan R and Vaidya NH 2002 Using directional antennas for medium access control in ad hoc networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 59–70.

[63] Chuprun S and Bergstrom CS 1998 Comparison of FH/CDMA and DS/CDMA for wireless survivable networks. In *Proc. IEEE Radio and Wireless Conference (RAWCON),* pp. 27–30.

[64] Clausen T and Jacquet P 2003 Optimized link state routing protocol (OLSR). *IETF RFC 3626.*

[65] Dai L, Xue Y, Chang B and Cao Y 2008 Integrated traffic prediction and routing optimization for multi-radio multi-channel wireless mesh networks. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 71–75.

[66] Datta S, Stojmenovic I and Wu J 2001 Internal node and shortcut based routing with guaranteed delivery in wireless networks. In *Proc. IEEE International Conference on Distributed Computing and Systems; Wireless Networks and Mobile Computing Workshop,* pp. 461–466.

[67] De Couto DSJ, Aguayo D, Bicket J and Morris R 2003 A high-throughput path metric for multi-hop wireless routing. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 134–146.

[68] de Oliveira R and Braun T 2005 A dynamic adaptive acknowledgment strategy for TCP over multihop wireless networks. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 1863–1874.

[69] Dong Q and Bejerano Y 2008 Building robust nomadic wireless mesh networks using directional antennas. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 1624–1632.

[70] Draves R, Padhye J and Zill B 2004 Comparisons of routing metrics for static multi-hop wireless Networks. In *Proc. ACM Annual Conference of the Special Interest Group on Data Communication (SIGCOMM),* pp. 133–144.

[71] Draves R, Padhye J and Zill B 2004 Routing in multi-radio, multi-hop wireless mesh networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 114–128.

[72] Dutta A, Wong KD, Burns J, Jain R, McAuley A, Young K and Schulzrinne H 2002 Realization of integrated mobility management protocol for ad hoc networks. In *Proc. IEEE MILCOM,* pp. 448–454.

[73] Dyer T and Boppana R 2001 A comparison of TCP performance over three routing protocols for mobile ad hoc networks. In *Proc. of ACM MOBIHOC*, pp. 56–66.

[74] Dutta P, Jaiswal S, Panigrahiz D and Rastogi R 2008 A new channel assignment mechanism for rural wireless mesh networks. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM).*

[75] ECMA International 2005 High rate ultra wideband PHY and MAC standard. *ECMA Standard 368*, 1st edn.

[76] ElBatt T and Ephremides A 2002 Joint scheduling and power control for wireless ad-hoc networks. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 976–984.

[77] ElRakabawy SM, Klemm A and Lindemann C 2005 TCP with adaptive pacing for multihop wireless networks. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC),* pp. 288–299.

[78] Ergen M, Lee D, Sengupta R and Varaiya P 2004 WTRP – wireless token ring protocol. *IEEE Transactions on Vehicular Technology* **53**(6), pp. 1863–1881.

[79] FCC cognitive radios. *http://www.fcc.gov/oet/cognitiveradio*

[80] Fette B 2003 SDR technology implementation for the cognitive radio. In *Proc. FCC Workshop on Cognitive Radios.*

[81] Firetide networks, *www.firetide.com*

[82] Frey H 2004 Scalable geographic routing algorithms for wireless ad hoc Networks. *IEEE Network Mag.*, 18–22.

[83] Fu Z, Meng X and Lu S 2003 A transport protocol for supporting multimedia streaming in mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications* **21**(10), 1615–1626.

[84] Fu Z, Zerfos P, Luo H, Lu S, Zhang L and Gerla M 2003 The impact of multihop wireless channel on TCP throughput and loss In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 1744–1753.

[85] Gamal AE, Mammen J, Prabhakar B and Shah D 2006a Optimal throughput-delay scaling in wireless networks–part I: the fluid model. *IEEE Transactions on Information Theory* **52**(6), 2568–2592.

[86] Gamal AE, Mammen J, Prabhakar B and Shah D 2006b Optimal throughput-delay scaling in wireless networks–part II: constant-size packets In
online link: http://www.stanford.edu/m̃ammen/papers/it-TDpkt.pdf

[87] Gambiroza V, Sadeghi B and Knightly EW 2004 End-to-end performance and fairness in multihop wireless backhaul networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* 287–310.

[88] Ganjali Y and Keshavarzian A 2004 Load balancing in ad hoc networks: single-path routing vs. multi-path routing. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 1120–1125.

[89] Gerla M, Hong X and Pei G 2002 Fisheye state routing protocol (FSR) for ad hoc networks. In *IETF Internet-Draft.*

[90] Giannoulis A, Salonidis T and Knightly E 2008 Congestion control and channel assignment in multi-radio wireless mesh networks. In *Proc. Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON).*

[91] Godfrey PB and Ratajczak D 2004 Naps: scalable, robust topology management in wireless ad hoc networks. In *Proc. Information Processing in Sensor Networks (IPSN),* pp. 443–451.

[92] Gokhale D, Sen S, Chebrolu K and Raman B 2008 On the feasibility of the link abstraction in (rural) mesh networks. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 61–65.

[93] Golden GD, Foschini CJ, Valenzuela RA and Wolniansky PW 1999 Detection algorithm and initial laboratory results using V-blast space-time communication architecture. *IEE Electronics Letters* **35**(1), 14–16.

[94] Grilo A and Nunes M 2003 Link adaptation and transmit power control for unitcast and multicast in IEEE 802.11a/h/e WLANs. In *Proc. IEEE International Conferences on Local Computer Networks,* pp. 334–345.

[95] Gupta P and Kumar PR 1999 Critical power for asymptotic connectivity in wireless networks. In *Stochastic Analysis, Control, Optimization and Application: A Volume in Honor of W.H. Fleming*. Springer.

[96] Gupta P and Kumar PR 2000 The capacity of wireless networks. *IEEE Trans. Information Theory* **46**(2), 388–404.

[97] Gupta V, Krishnaurthy S and Faloutsos M 2002 Denial of service attacks at the MAC layer in wireless ad hoc networks. In *Proc. IEEE MILCOM,* pp. 1118–1123.

[98] Hardy GH and Wright EM 1979 *An Introduction to the Theory of Numbers,* 5th edn. Clarendon Press.

[99] Haas ZJ and Liang B 1999 Ad hoc mobility management with uniform quorum systems. *IEEE/ACM Trans. Networking* **7**(2), 228–240.

[100] Hasan A and Andrews JG 2007 The guard zone in wireless ad hoc networks *IEEE Transactions on Wireless Communications* **6**(3), 897–906.

[101] Heissenbuttel M and Braun T 2003 BLR: beacon-less routing algorithm for mobile ad hoc networks. *Computer Communications Journal, Elsevier*.

[102] Holland G and Vaidya NH 1999 Analysis of TCP performance over mobile ad hoc networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 219–230.

[103] Holland G, Vaidya NH, and Bahl P 2001 A rate-adaptive MAC protocol for multi-hop wireless networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM)*, pp. 236–251.

[104] Hu L 1993 Topology control for multihop packet radio networks. *IEEE Trans. Communications* **41**(10), 1474–1483.

[105] Hu Y, Perrig A and Johnson D 2002 Ariadne: a secure on-demand routing protocol for ad hoc networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 12–23.

[106] Hu Y, Perrig A and Johnson D 2003 Packet leashes: a defense against wormhole attacks in wireless networks. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 1976–1986.

[107] Huang R, Zhang C and Fang Y 2007 A mobility management scheme for wireless mesh networks In *Proc. IEEE Global Telecommunications Conference (GLOBECOM),* pp. 5092–5096.

[108] Huang L and Lai T 2002 On the scalability of IEEE 802.11 ad hoc networks. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC),* pp. 173–182.

[109] Hubaux J-P, Butttan L and Capkun S 2001 The quest for security in mobile ad hoc networks. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC),* pp. 146–155.

[110] Hunter TE and Nosratinia A 2002 Cooperative diversity through coding. In *Proc. IEEE International Symposium on Information Technology,* p. 220.

[111] Iannone L and Fdida S 2005 Meshdv: a distance vector mobility-tolerant routing protocol for wireless mesh networks. In *Proc. IEEE ICPS Workshop on Multi-hop Ad hoc Networks: From Theory To Reality (REALMAN)*, pp. 1–8.

[112] IEEE 802.1 Working Group 2004 IEEE standard for local and metropolitan area networks: port-based network access, *IEEE Std 802.1X*.

[113] IEEE 802.11 Standard Group web site, *http://www.ieee802.org/11/*

[114] IEEE 802.11 Working Group 1999 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE 802.11 Standard, 1999 Edition*.

[115] IEEE 802.11 Standard Working Group 1999 Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: High-speed physical layer in the 5 GHz band. *IEEE 802.11a Standard*.

[116] IEEE 802.11e Task Group 2005 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. *IEEE 802.11e Standard*.

[117] IEEE 802.11f Task Group 2003 IEEE trial-use recommended practice for multi-vendor access point interoperability via an inter-access point protocol across distribution systems supporting IEEE 802.11 operation. *IEEE Std 802.11f,* 2003.

[118] IEEE 802 Standard Task Group 2003 Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: further higher data rate extension in 2.4 GHz band. *IEEE 802.11g Standard*.

[119] IEEE 802.11h Task Group 2003 Wireless LAN medium access control (MAC) and physical layer (PHY) specifications Amendment 5: spectrum and transmit power management extensions in the 5 GHz band in Europe. *IEEE 802.11h Standard*.

[120] IEEE 802.11n Task Group 2007 Draft amendment to standard for information technology – telecommunications and information exchange between systems – LAN/MAN specific requirements – Part 11: wireless medium access control (MAC) and physical layer (PHY) specifications: Amendment 4: Enhancement for higher throughput. *IEEE P802.11n/D3.01-2007*.

[121] IEEE 802.11r Task Group 2006 Wireless medium access control (MAC) and physical layer (PHY) specifications: Amendment 2: fast BSS transition. *IEEE P802.11r/D2.0*.

[122] IEEE 802.11s Task Group 2006a Joint SEE-Mesh/Wi-Mesh proposal to 802.11 TGs overview, *IEEE Doc: 802.11-05/0567r6*.

[123] IEEE 802.11s Task Group 2006b Draft amendment to standard for information technology – telecommunications and information exchange between systems – LAN/MAN specific requirements – Part 11: wireless medium access control (MAC) and physical layer (PHY) specifications: Amendment: ESS mesh networking. *IEEE P802.11s/D1.00-2006*.

[124] IEEE 802.15 Standard Group web site, *http://www.ieee802.org/15/*

[125] IEEE 802.15.1 Task Group 2002 Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs). *IEEE Std 802.15.1-2002*.

[126] IEEE 802.15.3 Task Group 2003 Wireless medium access control (MAC) and physical layer (PHY) specifications for high rate wireless personal area networks (WPANs). *IEEE Std 802.15.3-2003*.

[127] IEEE 802.15.4 Task Group 2003 Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs). *IEEE Std 802.15.4-2003*.

[128] IEEE 802.15.5 Task Group 2008 Mesh enhancements for IEEE 802.15 WPANs. *IEEE Draft 802.15.5/D3*.

[129] IEEE 802.16 Standard Group web site, *http://www.ieee802.org/16/*

[130] IEEE 802.16 Standards 2004 Air interface for fixed broadband wireless access systems. *IEEE Std 802.16*.

[131] IEEE 802.16a Task Group 2003 Air interface for fixed broadband wireless access systems – Amendment 2: medium access control modifications and additional physical layer specifications for 211 GHz. *IEEE Std 802.16a.*

[132] IEEE 802.16e Task Group 2005 Air interface for fixed and mobile broadband wireless access systems – Amendment 2: physical and medium access control layers for combined fixed and mobile operation in licensed bands. *IEEE Std 802.16e.*

[133] Intel Inc., Multi-hop mesh networks – a new kind of Wi-Fi network.

[134] Jain K, Padhye J, Padmanabhan V and Qiu L 2003 Impact of interference on multi-hop wireless network performance. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 66–80.

[135] Jakllari G, Eidenbenz S, Hengartner N, Krishnamurthy S and Faloutsos M 2008 Link positions matter: a noncommutative routing metric for wireless mesh networks. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM).*

[136] Jseemuddin M, Esmailpour A, Alwan A and Bazan O 2006 Integrated routing system for wireless mesh networks. In *Proc. Canadian Conference on Electrical and Computer Engineering,* pp. 1003–1007.

[137] Johnson DB, Maltz DA and Hu Y-C 2004 The dynamic source routing protocol for mobile ad hoc networks (DSR). *IETF Internet-Draft: work in progress.*

[138] Jou T-S and Eastlake DE 2004 ESS mesh network study group meeting minutes.

[139] Jun J and Sichitiu ML 2003 The nominal capacity of wireless mesh networks. *IEEE Wireless Communications* **10**(5), 8–14.

[140] Jun J and Sichitiu ML 2008 MRP: wireless mesh networks routing protocol. *Elsevier Compute Communications,* **31**, 1413–1435.

[141] Kajiya J 2004 Commodity software steerable antennas for mesh networks. *Microsoft Mesh Networking Summit.*

[142] Karbaschi G and Fladenmuller A 2005 A link quality and congestion-aware cross layer metric for multi-hop wireless routing. In *Proc. of IEEE MASS'05,* pp. 7–11.

[143] Kawadia V and Kumar PR 2005 A cautionary perspective on cross-layer design, *IEEE Wireless Communications,* 3–11.

[144] Keshav S 1995 A control-theoretic approach to flow control. *ACM SIGCOMM Computer Communication Review* **25**(1), 188–201.

[145] Keshavarz-Haddad A and Riedi R 2007 Bounds for the capacity of wireless multihop networks imposed by topology and demand. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC).*

[146] Kim K-H and Shin KG 2006 On accurate measurement of link quality in multi-hop wireless mesh networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 38–49.

[147] Kinney P 2003 IEEE 802.15 general interest in mesh networking. *IEEE 802.15 Request for Information of a Mesh Network Study Group, presentation slides.*

[148] Kleinrock L and Silvester J 1978 Optimum transmission radii for packet radio networks or why six is a magic number. In *Proc. IEEE National Telecommunications Conference,* pp. 4.3.1–4.3.5.

[149] Ko YB, Shankarkumar V and Vaidya NH 2000 Medium access control protocols using directional antennas in ad hoc networks. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 13–21.

[150] Koksal CE and Balakrishnan H 2006 Quality-aware routing metrics for time-varying wireless mesh networks. *IEEE Journal on Selected Areas in Communications* **24**(11), pp. 1984–1994.

[151] Konanur AS, Gosalia K, Krishnamurthy SH, Hughes B and Lazzi G 2005 Increasing wireless channel capacity through MIMO systems employing co-located antennas. *IEEE Transactions on Microwave Theory and Techniques* **53**(6), 1837–1844.

[152] Kozat UC and Tassiulas L 2003 Throughput capacity of random ad hoc networks with infrastructure Support. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 55–65.

[153] Kozat UC, Koutsopoulos I and Tassiulas L 2004 A framework for cross-layer design of energy-efficient communication with QoS provisioning in multi-hop wireless networks. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 1446–1456.

[154] Krishnamurthy L, Conner S, Yarvis M, Chhabra J, Ellison C, Brabenac C and Tsui E 2002 Meeting the demands of the digital home with high-speed multi-hop wireless networks. *Intel Technology Journal* **6**(4), 57–68.

[155] Krishnamurthy L 2004 Making radios more like human ears: alternative MAC techniques and innovative platforms to enable large-scale meshes. *Microsoft Mesh Networking Summit*.

[156] Lai T and Zhou D 2003 Efficient and scalable IEEE 802.11 ad hoc mode timing synchronization function. In *Proc. 17th IEEE International Conferences on Advanced Information Networking and Applications*.

[157] Lampe M, Rohling N and Zirwas W 2002 Misunderstandings about link adaptation for frequency selective fading channels. In *Proc. IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC),* pp. 710–714.

[158] Lane B 2003 Cognitive radio technologies in the commercial arena. In *Proc. FCC Workshop on Cognitive Radios*.

[159] Laneman JN, Wornell GW and Tse DNC 2001 An efficient protocol for realizing cooperative diversity in wireless networks. In *Proc. IEEE International Symposium on Information Technology,* pp. 294.

[160] Laneman JN, Tse DNC and Wornell GW 2004 Cooperative diversity in wireless networks: efficient protocols and outage behavior. *IEEE Transactions on Information Theory* **50**(12), 3062–3080.

[161] Lee S, Bhattacharjee B and Banerjee S 2005 Efficient geographic routing in multihop wireless networks. In *Proc. Sixth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC),* pp. 230–241.

[162] Lee K-D and Leung VCM 2006 Fair allocation of subcarrier and power in an OFDMA wireless mesh network. *IEEE Journal on Selected Areas in Communications* **24**(11), 2051–2060.

[163] Lee KK, Kim SH, Choi SY and Park HS 2006 A mesh routing protocol using cluster label in the ZigBee network. In *Proc. IEEE MASS06,* pp. 801–806.

[164] Li J, Blake C, De Couto DSL, Lee HI and Morris R 2001 Capacity of ad hoc wireless networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 61–69.

[165] Li L, Halpern JY, Bahl P, Wang Y-M and Wattenhofer R A cone-based distributed topology-control algorithm for wireless multi-hop networks. *IEEE/ACM Transactions on Networking* **13**(1), 147–159.

[166] Li L and Halpern JY 2004 A minimum-energy path-preserving topology-control algorithm. *IEEE Trans. Wireless Communications* **3**(3), 910–921.

[167] Li N and Hou JC 2006 Localized fault-tolerant topology control in wireless ad hoc networks *IEEE Trans. Parallel and Distributed Systems* **17**(4), 307–320.

[168] Li X-Y, Moaveni-Nejad K, Song W-Z and Wang W-Z 2005 Interference-aware topology control for wireless sensor networks. In *Proc. Third Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON),* pp. 263–274.

[169] Lim AO, Wang X, Kado Y and Zhang B 2008 A hybrid centralized routing protocol for 802.11s WMNs. *ACM/Kluwer Mobile Networks and Applications (MONET)* **13**(1–2), 117–131.

[170] Lin D, Moh T and Moh M 2006 A delay-bounded multi-channel routing protocol for wireless mesh networks using multiple token rings: extended summary. In *Proc. 31st IEEE Conference on Local Computer Networks (LCN),* pp. 845–847.

[171] Lin R and Petropulu AP 2005 A new wireless network medium access protocol based on cooperation. *IEEE Transactions on Signal Processing* **53**(12), 4675–4684.

[172] Lin X and Shroff NB 2004 Joint rate control and scheduling in multihop wireless networks. In *Proc. IEEE Conf. Decision and Control,* pp. 1484–1489.

[173] Lin X, Shroff NB and Srikant R 2006 A Tutorial on cross-layer optimization in wireless networks. *IEEE Journal on Selected Areas in Communications* **24**(8), 1452–1463.

[174] Lin X and Shroff NB 2006 The impact of imperfect scheduling on cross-layer congestion control in wireless networks. *IEEE/ACM Trans. Netw.* **14**(2), 302–315.

[175] Liu B, Liu Z and Towsley D 2003 On the capacity of hybrid wireless networks. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 1543–1552.

[176] Liu J and Singh S 2001 ATCP: TCP for mobile ad hoc networks. *IEEE Journals on Selected Areas in Communications* **19**(7), 1300–1315.

[177] Liu T and Liao W, 2006 Capacity-aware routing in multi-channel multi-rate wireless mesh networks. In *Proc. IEEE International Conference on Communications (ICC),* pp. 1971–1976.

[178] Liu X, Sharma G, Mazumdar RR and Shroff NB 2005 Degenerate delay-capacity trade-offs in ad hoc networks with Brownian mobility. *IEEE/ACM Transactions on Networking* **14**(SI), 2777–2784. *online link: http://min.ecn.purdue.edu/ĩnx/paper/it05.pdf*

[179] Low SH, Paganini F and Doyle JC 2002a Internet congestion control. *IEEE Control Syst. Mag.* **22**(1), 28–43.

[180] Low SH, Perterson LL and Wang L 2002b Understanding Vegas: a duality model. *J. ACM* **49**(2), 207–235.

[181] Low SH 2003 A duality model of TCP and queue management algorithms. *IEEE/ACM Trans. Networking* **11**(4), 525–536.

[182] Lozano A, Farrokhi FR and Valenzuela RA 2001 Lifting the limits on high-speed wireless data access using antenna arrays. *IEEE Communications Mag.* **39**, 156–162.

[183] Ma L, Zhang Q, Xiong Y and Zhu W 2005 Interference aware metric for dense multi-hop wireless network. In *Proc. of IEEE International Conference on Communications (ICC),* pp. 1261–1265.

[184] Manoj BS and Siva Ram Murthy C 2002 Real-time traffic support for ad hoc wireless networks. In *Proc. IEEE ICON,* pp. 335–340.

[185] Marshall P 2003 Beyond the outer limits: next generation communications. In *Proc. FCC Workshop on Cognitive Radios*.

[186] Marti A, Giuli T, Lai K and Baker M 2000 Mitigating routing misbehavior in mobile ad hoc networks. In *Proc. Int. Conf. Mobile Computing and Networking (MOBICOM),* pp. 255–265.

[187] McCune E 2003 DSSS vs. FHSS narrowband interference performance issues. *RF Design Magazine*, 90–104.

[188] McHenry M 2003 Frequency agile spectrum access technologies. In *Proc. FCC Workshop on Cognitive Radios*.

[189] Mesh Networking Forum 2004 Building the business case for implementation of wireless mesh networks. *Mesh Networking Forum 2004*.

[190] Microsoft Mesh networks. *http://research.microsoft.com/mesh/*

[191] Mitola J 2000 Software radio architecture: object-oriented approaches to wireless system engineering. *Wiley Inter-Science*.

[192] Mueller S and Ghosal D 2004 Multipath routing in mobile ad hoc networks: issues and challenges. *Lecture Notes in Computer Science*, vol. 2965. Springer, pp. 209–234.

[193] Muqattash A and Krunz M 2003 CDMA-based MAC protocol for wireless ad hoc networks. In *Proc. Sixth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC),* pp. 153–164.

[194] Murch RD and Ben Letaief K 2002 Antenna systems for broadband wireless access. *IEEE Communications Mag,* 76–83.

[195] Nandiraju NS, Nandiraju DS, Agrawal DP 2006 Multipath routing in wireless mesh networks. In *Proc. IEEE MASS06,* pp. 741–746.

[196] Nasipuri A and Das SR 1999 On-demand multipath routing for mobile ad hoc networks. In *Proc. IEEE International Conferences on Computer Communications and Networks,* pp. 64–70.

[197] Nasipuri A, Ye S and Hiromoto RE 2000 A MAC protocol for mobile ad hoc networks using directional antennas. In *Proc. IEEE Wireless Communications and Networking Conference (WCNC),* pp. 1214–1219.

[198] Navaratnam P, Akhtar N and Tafazolli R 2006 On the performance of DCCP in wireless mesh networks. In *Proc. International Workshop on Mobility Management and Wireless Access (MOBIWAC),* pp. 144–147.

[199] Navda V, Kashyap A and Das SR 2005 Design and evaluation of iMesh: an infrastructure-mode wireless mesh network. In *Proc. Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM),* pp. 164–170.

[200] Neely MJ, Modiano W and Rohrs CE 2003 Dynamic power allocation and routing for time varying wireless networks. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 745–755.

[201] Neely M and Modiano E 2005 Capacity and delay tradeoff for ad hoc mobile networks. *IEEE Transactions on Information Theory* **51**(6), 1917–1937.

[202] Nosratinia A, Hunter TE and Hedayat A 2004 Cooperative communication in wireless networks. *IEEE Communications Magazine* **42**(10), 74–80.

[203] Ogier R, Templin F and Lewis M 2004 Topology dissemination based on reverse-path forwarding (TBRPF). *IETF RFC 3684*.

[204] Omiwade O, Zheng R and Hua C 2008 Practical localized network coding in wireless mesh networks. In *Proc. Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*.

[205] Panigrahi D, Dutta P, Jaiswal S, Naidu KV and Rastogi R 2008 Minimum cost topology construction for rural wireless mesh networks. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 771–779.

[206] Perkins CE 1998 Mobile networking through mobile IP. *IEEE Internet Computing* **2**(1), 58–69.

[207] Perrig A, Canetti A, Tygar D and Song D 2002 The TESLA broadcast authentication protocol. *RSA CryptoBytes* **5**(2), 2–13.

[208] Perkins C, Belding-Royer E and Das S 2003 Ad hoc on-demand distance vector (AODV) routing. *IETF RFC 3561*.

[209] Petrovic M and Aboelaze M 2003 Performance of TCP/UDP over ad hoc IEEE 802.11. In *Proc. International Conference on Telecommunications,* pp. 700–708.

[210] Pham NT and Hwang W-J 2007 Hierarchical routing in wireless mesh networks. In *Proc. 9th International Conference on Advanced Communication Technology,* pp. 1275–1280.

[211] Piggin P, Lewis B and Whitehead P 2003 Mesh networks in fixed broadband wireless access: multipoint enhancements for the 802.16 standard. *IEEE 802.16 presentation slides*.

[212] Pirzada AA, Portmann M and Indulska J 2006 Evaluation of multi-radio extensions to AODV for wireless mesh networks. In *Proc. 4th ACM International Workshop on Mobility Management and Wireless Access (MOBIWAC),* pp. 45–51.

[213] Pradeep K and Vaidya N 2006 Routing and link-layer protocols for multi-channel multi-interface ad hoc wireless networks. *ACM SIGMOBILE Mobile Computing and Communications Review* **10**(15), 31–43.

[214] Qiao D, Choi S, and Shin KG 2002 Goodput analysis and link adaptation for IEEE 802.11a wireless LANs. *IEEE Trans. Mobile Computing* **1**(4), 278–292.

[215] Ramachandran K, Buddhikot MM, Chandranmenon G, Miller S, Almeroth K and Belding-Royer E 2005 On the design and implementation of infrastructure mesh networks. In *Proc. IEEE Workshop on Wireless Mesh Networks (WIMESH).*

[216] Ramachandran KN, Belding EM, Almeroth KC and Buddhikot MM 2006 Interference-aware channel assignment in multi-radio wireless mesh networks. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 1–12.

[217] Raman B and Chebrolu K 2005 Design and evaluation of a new MAC protocol for long distance 802.11 mesh networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 156–169.

[218] Raman B 2006 Channel allocation in 802.11-based mesh networks. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 1–10.

[219] Ramanathan R 2001 On the performance of ad hoc networks with beamforming antennas. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC),* pp. 95–105.

[220] Ramanathan R, Redi J, Santivanez C, Wiggins D and Polit S 2005 Ad hoc networking with directional antennas: a complete system solution. *IEEE Journal on Selected Areas in Communications* **23**(3), 496–506.

[221] Ramanathan R and Rosales-Hain R 2000 Topology control of multihop wireless networks using transmit power adjustment. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 404–413.

[222] Raniwala A and Chiueh T-C 2005 Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 2223–2234.

[223] Raniwala A, Sharma S, De P, Krishnan R and Chiueh T-C 2007 Evaluation of a stateful transport protocol for multi-channel wireless mesh networks. In *Proc. IEEE International Workshop on Quality of Service,* pp. 74–82.

[224] Robinson J and Knightly E 2007 A performance study of deployment factors in wireless mesh networks. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 2054–2062.

[225] Robinson J, Uysal M, Swaminathan R and Knightly E 2008 Adding capacity points to a wireless mesh network using local search. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 1247–1255.

[226] Rozner E, Seshadri J, Mebta Y and Qiu L 2006 Simple opportunistic routing protocol for wireless mesh networks. In *Proc. of IEEE Workshop on Wireless Mesh Networks (WIMESH)*, pp. 48–54.

[227] Sabeur M, Sukkar GA, Jouaber B and Zeghlache D 2007 Mobile party: a mobility management solution for wireless mesh network. In *Proc. Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).*

[228] Sadeghi B, Kanodia V, Sabharwal A and Knightly E 2002 Opportunistic media access for multirate ad hoc networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM).*

[229] Saha AK and Johnson DB Self-organizing hierarchical routing for scalable ad hoc networking. *Department of Computer Science Technical Report,* TR04-433. Rice University.

[230] Sanzgiri K, Dahill B, Levine BN, Shields C and Belding-Royer EM 2002 A secure protocol for ad hoc networks. In *Proc. IEEE International Conference on Network Protocols (ICNP),* pp. 78–87.

[231] Sendonaris A, Erkip E and Aazhang B 2003a User cooperation diversity – part I: system description. *IEEE Transactions on Communications* **51**(11), 1927–1937.

[232] Sendonaris A, Erkip E and Aazhang B 2003b User cooperation diversity – part II: implementation aspects and performance analysis. *IEEE Transactions on Communications* **51**(11), 1939–1948.

[233] Shen C-C and Srisathapornphat C and Jaikaeo C 2003 An adaptive management architecture for ad hoc networks. *IEEE Communications Mag.*, 108–115.

[234] Shen Q, Fang X and Shan Y 2006 An integrated metrics based extended dynamic source routing protocol for wireless mesh networks. In *Proc. International Conference on Communications, Circuits and Systems,* pp. 1457–1461.

[235] Shi J, Gurewitz O, Mancuso V, Camp J and Knightly E 2008 Measurement and modeling of the origins of starvation in congestion controlled mesh network. In *Proc. of IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 1633–1641.

[236] So J and Vaidya N 2004 Multi-channel MAC for ad hoc networks: handling multi-channel hidden terminals using a single transceiver. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC),* pp. 222–233.

[237] Song G and Li Y 2005 Cross-layer optimization for OFDM wireless networks – part I: theoretical framework. *IEEE Transactions on Wireless Communications* **4**(2), 614–624.

[238] Song W and Fang X 2006 Routing with congestion control and load balancing in wireless mesh networks. In *Proc. International Conference on ITS Telecommunications,* pp. 719–724.

[239] Spyropoulos A and Raghavendra CS 2002 Energy efficient communications in ad hoc networks using directional antenna. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 220–228.

[240] Spyropoulos A and Raghavendra CS 2003 Asymptotic capacity bounds for ad hoc networks revisited: the directional and smart antenna cases. In *Proc. IEEE Global Telecommunications Conference (GLOBECOM),* pp. 1216–1220.

[241] Stefanov A and Erkip E 2004 Cooperative coding for wireless networks. *IEEE Transactions on Communications* **52**(9), 1470–1476.

[242] Stefanov A and Erkip E 2005 Cooperative space-time coding for wireless networks. *IEEE Transactions on Communications* **53**(11), 1804–1809.

[243] Stojmenovic I and Lin X 2001 Power-aware localized routing in wireless networks. *IEEE Transactions on Parallel and Distributed Systems* **12**, 1122–1133.

[244] Sucec J and Marsic I 2002 Location management for hierarchically organized mobile ad hoc networks. In *Proc. IEEE Wireless Communications and Networking Conference (WCNC),* pp. 603–607.

[245] Sundaresan K, Sivakumar R, Ingram MA and Chang T-Y 2003 A fair medium access control protocol for ad hoc networks with MIMO links. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM),* pp. 2559–2570.

[246] Sundaresan K, Anantharaman V, Hsieh H-Y and Sivakumar R 2003 ATP: a reliable transport protocol for ad-hoc networks. In *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC),* pp. 64–75.

[247] Mineo Takai M, Martin J, Aifeng Ren A and Bagrodia R 2002 Directional virtual carrier sensing for directional antennas in mobile ad hoc networks In *Proc. Sixth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC),* pp. 183–193.

[248] Tanenbaum AS 1996 Computer Networks. *Prentice Hall*, Third Edition, 1996.

[249] Tang J, Xue G and Zhang W 2005 Interference-aware topology control and QoS routing in multi-channel wireless mesh networks. In *Proc. Sixth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC),* pp. 68–77.

[250] Tassiulas L and Ephremides A 1992 Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks. *IEEE Trans. Autom. Control* **37**(12), 1936–1948.

[251] Tse DNC and Grossglauser M 2002 Mobility increases the capacity of ad hoc wireless networks. *IEEE/ACM Trans. Networking* **10**(4), 477–486.

[252] Tung L-P, Shih W-K, Cho T-C, Sun, YS and Chen MC 2007 TCP throughput enhancement over wireless mesh networks. *IEEE Communications Magazine* **45**(11), 64–70.

[253] Vidhyashankar V, Manoj BS and Siva Ram Murthy C 2006 Slot allocation schemes for delay sensitive traffic support in asynchronous wireless mesh networks. *Computer Networks* **50**(15), pp. 2595–2613.

[254] Wang F and Zhang Y 2002 Improving TCP Performance over mobile ad hoc networks with out-of-order detection and response. In *Proc. Seventh ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC),* pp. 217–225.

[255] Wang X and Xiang W 2006 An OFDM-TDMA/SA MAC protocol for broadband wireless LANs with QoS constraints. *ACM/Kluwer Wireless Networks* **12**(2), 159–170.

[256] Wang X, Wang W and Nova M 2005 Distributed TDMA for wireless mesh networks. *US Patent Serial Number: 11/076738.*

[257] Wang X, Rollinger V, Patil A, Chao G, Wang W and Nova M 2006 Distributed multichannel wireless communications. *US Patent Serial Number: 11/420668.*

[258] Wang X, Wang W and Nova M 2006 Distributed time slot and channel allocations for wireless mesh networks. *US Patent Serial Number: 11/952948.*

[259] Wang X and Akyildiz IF 2009 Mobile mesh IP for wireless mesh networks. Work in progress.

[260] Weber SP, Yang X, Andrews JG and de Veciana G 2005 Transmission capacity of wireless ad hoc networks with outage constraints. *IEEE Transactions on Information Theory* **51**(12), 4091–4102.

[261] Wehbi B, Mallouli W and Cavalli A 2006 Light client management protocol for wireless mesh networks. In *Proc. 7th International Conference on Mobile Data Management (MDM),* pp. 123–126.

[262] Wellons J, Dai L, Xue Y and Cui Y 2008 Predictive or oblivious: a comparative study of routing strategies for wireless mesh networks under uncertain demand. In *Proc. Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pp. 215–223.

[263] Whitehead P, Piggin P, Lewis B and Lynch S 2003 Mesh extensions to IEEE 802.16 and 16a. *IEEE 802.16 proposal*.

[264] The Wi-Fi Alliance. *http://www.wi-fi.org/*

[265] The WiMAX Forum. *http://www.wimaxforum.org/home*

[266] The WiMedia Alliance. *http://www.wimedia.org/*

[267] Vapnik VN and Chervonenkis A 1971 On the uniform convergence of relative frequencies of events to their probabilities. *Theory of Probability and Its Applications* **16**(2), 264–280.

[268] Wei DX, Jin C, Low SH and Hegde S 2006 FAST TCP: motivation, architecture, algorithms, performance. *IEEE/ACM Transactions on Networking* **14**(6), 1246–1259.

[269] Wong CY, Cheng RS, Letaief KB and Ross D 1999 Multiuser OFDM with adaptive subcarrier, bit, and power allocation. *IEEE J. Select. Areas Commun.* **17**(10), 1747–1757.

[270] Wu S, Lin C-Y, Tseng Y-Y and Sheu J-P 2000 A new multi-channel MAC protocol with on-demand channel assignment for multi-hop mobile ad hoc networks. In *Proc. 5th International Symposium on Parallel Architectures, Algorithms, and Networks (ISPAN)*, pp. 232–237.

[271] Wu Z, Ganu S and Raychaudhuri D 2006 IRMA: integrated routing and MAC scheduling in multihop wireless mesh networks. In *Proc. IEEE Workshop on Wireless Mesh Networks (WIMESH)*, pp. 1–8.

[272] Xiang W, Pratt T and Wang X 2004 A software radio testbed for two-transmitter two-receiver space time coding wireless LAN. *IEEE Communications Mag.*, 520–528.

[273] Xie J and Wang X 2008 Mobility management in hybrid wireless mesh networks. *Revised for IEEE Network Magazine*.

[274] Xie L-L and Kumar PR 2004 A network information theory for wireless communication: scaling laws and optimal operation. *IEEE Trans. Info. Theory* **50**(5), 748–767.

[275] Xing K, Cheng X, Ma L and Liang Q 2007 Superimposed code based channel assignment in multi-radio multi-channel wireless mesh networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM).*

[276] Xu K, Hong X and Gerla M 2002 Landmark routing in ad hoc networks with mobile backbones. *Journal of Parallel and Distributed Computing (JPDC)* Special Issue on Ad Hoc Networks, **63**(2), 110–122.

[277] Xu S and Saadawi T 2001 Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks? *IEEE Communications Mag.* **39**(6), 130–137.

[278] Xylomenos G, Polyzos GC, Mahonen P and Saaranen M 2001 TCP performance issues over wireless links. *IEEE Communications Mag.*, 52–58.

[279] Yang H, Meng X and Lu S 2002 Self-organized network layer security in mobile ad hoc networks. In *Proc. ACM Workshop Wireless Security (WiSE),* pp. 11–20.

[280] Yang H, Luo H, Ye F, Lu S and Zhang L 2004 Security in mobile ad hoc networks: challenges and solutions. *IEEE Wireless Communications*, 38–47.

[281] Yang X and de Veciana G 2004 Inducing spatial clustering in MAC contention for spread spectrum ad hoc networks. In *Proc. Seventh ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC)*, pp. 121–132.

[282] Yang Y, Wang J and Kravets 2005 Interference-aware load balancing for multihop wireless networks. In *Tech. Rep. UIUCDCS-R-2005-2526, Department of Computer Science, University of Illinois at Urbana-Champaign,* 2005.

[283] Yang Y and Wang J 2008 Design guidelines for routing metrics in multihop wireless networks. In *Proc. IEEE Annual Conference on Computer Communications (INFOCOM)*, pp. 1615–1623.

[284] Yuan Y, Yang H, Wong SHY, Lu S and Arbaugh W 2005 ROMER: resilient opportunistic mesh routing for wireless mesh networks. In *Proc. IEEE Workshop on Wireless Mesh Networks (WIMESH).*

[285] Yum T-S and Hung K-W 1992 Design algorithms for multihop packet radio networks with multiple directional antennas stations. *IEEE Trans. Communications* **41**(11), 1716–1724.

[286] Zapata M and Asokan N 2002 Securing ad hoc routing protocols. In *Proc. ACM Workshop on Wireless Security (WiSe),* pp. 1–10.

[287] Zemlianov A and de Veciana G 2005 Capacity of ad hoc wireless networks with infrastructure support. *IEEE Journal on Selected Areas in Communications* **23**(3), 657–667.

[288] Zhang H and Li Y 2003 Anti-jamming property of clustered OFDM for dispersive channels. In *Proc. IEEE Military Communications Conference (MILCOM),* vol. 1, pp. 336–240.

[289] Zhang X and Li B 2008 On the benefits of network coding in multi-channel wireless networks. In *Proc. Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pp. 341–349.

[290] Zhang Y and Lee W 2000 Intrusion detection in wireless ad-hoc networks. In *Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM),* pp. 275–283.

[291] Zhou P, Wang X and Rao R 2008 Capacity of infrastructure wireless mesh networks. *IEEE Transactions on Mobile Computing* **7**(8), 1011–1024.

[292] Zhu X and Murch RD 2002 Performance analysis of maximum likelihood detection in a MIMO antenna system. *IEEE Transactions on Communications* **50**(2), 187–191.

[293] The Zigbee Alliance. *http://www.zigbee.org/*

[294] Zorzi M, Zeidler J, Anderson A, Rao B, Proakis J, Swindlehurst LA, Hensen M and Krishnamurthy S 2006 Cross-layer issues in MAC protocol design for MIMO ad hoc networks. *IEEE Wireless Communications* **13**(4), 62–76.

Index