EMERGING WIRELESS LANs, WIRELESS PANs, AND WIRELESS MANs

IEEE 802.11, IEEE 802.15, 802.16 WIRELESS STANDARD FAMILY

Edited by

Yang Xiao
Yi Pan

WILEY
A JOHN WILEY & SONS, INC., PUBLICATION

EMERGING WIRELESS LANs, WIRELESS PANs, AND WIRELESS MANs

EMERGING WIRELESS LANs, WIRELESS PANs, AND WIRELESS MANs

IEEE 802.11, IEEE 802.15, 802.16 WIRELESS STANDARD FAMILY

Edited by

Yang Xiao
Yi Pan

WILEY
A JOHN WILEY & SONS, INC., PUBLICATION

Published by John Wiley & Sons, Inc., Hoboken, New Jersey
Published simultaneously in Canada

Library of Congress Cataloging-in-Publication Data:

Xiao, Yang, 1966-
Emerging wireless LANs, wireless PANs, and wireless MANs : IEEE 802.11, IEEE 802.15, IEEE 802.16 wireless standard family/Yang Xiao and Yi Pan.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-471-72069-0 (cloth)
1. IEEE 802.11 (Standard) 2. IEEE 802.16 (Standard) 3. Wireless LANs–Standards. 4. Personal communication service systems–Standards. 5. Wireless metropolitan area networks–Standards. I. Pan, Yi, 1960- II. Title.
TK5105.5668. X53 2008
004.6′8–dc22

2008021441

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

CONTENTS

PREFACE ix

CONTRIBUTORS xi

PART I IEEE 802.11 WIRELESS LANs 1

Chapter 1 IEEE 802.11 Medium Access Control and Physical Layers 3
Kaveh Ghaboosi, Matti Latva-aho, and Yang Xiao

Chapter 2 Framework for Decentralized Wireless LAN Resource Management 27
Jiang Xie, Ivan Howitt, and Anita Raja

Chapter 3 Incentive Issues in IEEE 802.11*x* Wireless Networks 65
Yu-Kwong Kwok

Chapter 4 Capacity and Rate Adaptation in IEEE 802.11 Wireless LANs 81
Ming Li and Yang Xiao

PART II IEEE 802.15.1 BLUETOOTH AND IEEE 802.15.2 105

Chapter 5 Overview of IEEE 802.15.1 Medium Access Control and Physical Layers 107
Kaveh Ghaboosi, Yang Xiao, and Jeff J. Robertson

Chapter 6 Overview of IEEE 802.15.2: Coexistence of Wireless Personal Area Networks with Other Unlicensed Frequency Bands Operating Wireless Devices 135
Kaveh Ghaboosi, Yang Xiao, Matti Latva-aho, and Babak H. Khalaj

Chapter 7 Coexistence of Bluetooth Piconets and Wireless LAN 151
Jingli Li and Xiangqian Liu

PART III IEEE 802.15.3 WIRELESS PANs **187**

Chapter 8 Frame Format, Channel Access, and Piconet Operation of IEEE 802.15.3 Wireless PANs **189**
Yang Xiao, Michael J. Plyler, Bo Sun, and Yi Pan

Chapter 9 Power Management and Security of IEEE 802.15.3 Wireless PANs **217**
Yang Xiao, Michael J. Plyler, Bo Sun, and Yi Pan

Chapter 10 Performance Evaluation and Optimization of IEEE 802.15.3 Piconets **239**
Zhanping Yin and Victor C. M. Leung

Chapter 11 Performance Analysis of MB-OFDM UWB Systems **261**
Chris Snow, Lutz Lampe, and Robert Schoberg

Chapter 12 Distributed Solution for Resource Allocation in Ultra-Wideband Wireless PANs **299**
Hai Jiang, Kuang-Hao Liu, Weihua Zhuang, and Xuemin (Sherman) Shen

PART IV IEEE 802.15.4 AND 802.15.5 WIRELESS PANs **319**

Chapter 13 IEEE 802.15.4 Medium Access Control and Physical Layers **321**
Yang Xiao, Michael J. Plyler, Ming Li, and Fei Hu

Chapter 14 Performance Analysis for IEEE 802.15.4 Wireless Personal Area Networks **349**
Hsueh-Wen Tseng, Yu-Kai Huang, and Ai-Chun Pang

Chapter 15 Data Transmission and Beacon Scheduling in Low Rate Wireless Mesh Personal Area Networks **373**
Jianliang Zheng

Chapter 16 Impact of Reliable and Secure Sensing on Cluster Lifetime in IEEE 802.15.4 Networks **389**
Jelena Mišić

Chapter 17 IEEE 802.15.5: Recommended Practice for WPAN Mesh Network (Low Data Rate) **415**
Chunhui Zhu and Myung J. Lee

Chapter 18 Power-Saving Algorithms on IEEE 802.15.4 for Wireless Sensor Networks **439**
Tae Rim Park and Myung J. Lee

PART V IEEE 802.16 WIRELESS MANs 473

Chapter 19 IEEE 802.16 Medium Access Control and Physical Layers 475
Yang Xiao, Michael J. Plyler, Tianji Li, and Fei Hu

Chapter 20 QoS Support for WiMAX 497
Usman A. Ali, Qiang Ni, Yang Xiao, Wenbing Yao, and Dionysios Skordoulis

Chapter 21 Subchannel Allocation and Connection Admission Control in OFDMA-Based IEEE 802.16/ WiMAX-Compliant Infrastructure Wireless Mesh Networks 515
Dusit Niyato and Ekram Hossain

Chapter 22 Universal Authentication and Billing Architecture for Wireless MANs 555
Xiaodong Lin, Haojin Zhu, Minghui Shi, Rongxing Lu, Pin-Han Ho, and Xuemin (Sherman) Shen

Chapter 23 Scheduling Algorithms for WiMAX Networks: Simulator Development and Performance Study 585
Sai Suhas Kolukula, M. Sai Rupak, K. S. Sridharan, and Krishna M. Sivalingam

INDEX 613

ABOUT THE EDITORS 633

PREFACE

The purpose of this book is to introduce current and emerging Institute of Electrical and Electronics Engineers (IEEE) 802 wireless standards to readers, including IEEE 802.11 wireless local area networks (WLANs)—WiFi, wireless personal area networks (WPANs) (IEEE 802.15.1 Bluetooth, IEEE 802.15.2 coexistence of WLANs and WPANs, IEEE 802.15.3 higher data rate WPANs, IEEE 802.15.4 sensor networks—Zigbee, and IEEE 802.15.5), and IEEE 802.16 wireless metropolitan area networks (WMANs)—WiMAX. The book introduces medium access control and physical layer protocols for all these standards as well as some research articles.

Experience has shown that reading the standards can be tedious and sometimes confusing since they are normally written in a way that is very detailed. Engineers and researchers in both industry and academia spend huge amounts of time trying to understand them. A good book can help them save this time and help them understand the standards and we hope this book does that.

About 10 standards are presented in this book. The actual text for each standard comprises about 300–600 pages. In our book all 10 standards are discussed in about 600 pages. The main purpose is to help readers understand the standards as well as related research issues.

The book is primarily written for scientists, researchers, engineers, developers, educators, and administrators of universities, industries, research institutes and laboratories, and government agencies working in the area of wireless networks. They will find this book a unique source of information on recent advances and future directions of WLANs, WPANs, and WMANs. We expect that the book will be an informative and useful reference in this new and fast-growing research area.

This book was made possible by the great efforts of our publishers and contributors. First, we are indebted to the contributors, who have sacrificed many days and nights to put together these excellent chapters for our readers. Second, we owe our special thanks to our publishers and staff members. Without their encouragement and quality work this book would not have been possible. Finally, we would like to thank our families for their support.

YANG XIAO
YI PAN

Tuscaloosa, Alabama
Atlanta, Georgia
January 2009

CONTRIBUTORS

Usman A. Ali, Brunel University, West London, United Kingdom

Kaveh Ghaboosi, University of Oulu, Finland

Pin-Han Ho, University of Waterloo, Waterloo, Ontario, Canada

Ekram Hossain, University of Manitoba, Winnipeg, Manitoba, Canada

Ivan Howitt, University of North Caroling, Charlotte, North Carolina

Fei Hu, The University of Alabama, Tuscaloosa, Alabama

Yu-Kai Huang, National Taiwan University, Taipei, Taiwan, China

Hai Jiang, University of Alberta, Alberta, Canada

Babak H. Khalaj, Sharif University of Technology, Tehran, Iran

Sai Suhas Kolukula, Honeywell, Bangalore, India

Yu-Kwong Kwok, Colorado State University, Fort Collins, Colorado

Lutz Lampe, Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, British Columbia, Canada

Matti Latva-aho, Department of Electrical Engineering, University of Oulu, Finland

Myung J. Lee, Department of Electrical Engineering, City University of New York, New York

Victor C. M. Leung, Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, British Columbia, Canada

Jingli Li, University of Louisville, Louisville, Kentucky

Ming Li, California State University, Fresno, California

Tianji Li, Hamilton Institute, The National University of Ireland, Maynooth, County Kildare, Ireland

Xiaodong Lin, University of Ontario Institute of Technology, Ontario, Canada

Xiangqian Liu, University of Louisville, Louisville, Kentucky

Kuang-Hao Liu, University of Waterloo, Waterloo, Ontario, Canada

Rongxing Lu, University of Waterloo, Waterloo, Ontario, Canada

Jelena Mišić, University of Manitoba, Winnipeg, Manitoba, Canada

Qiang Ni, Brunel University, West London, United Kingdom

Dusit Niyato, University of Manitoba, Winnipeg, Manitoba, Canada

Yi Pan, Department of Computer Science, Georgia State University, Atlanta, Georgia

Ai-Chun Pang, National Taiwan University, Taipei, Taiwan, China

Tae Rim Park, Department of Electrical Engineering, City University of New York, New York

Michael J. Plyler, Freed-Hardeman University, Henderson, Tennessee

Anita Raja, University of North Carolina, Charlotte, North Carolina

Jeff J. Robertson, Department of Computer Science, The University of Memphis, Memphis, Tennessee

M. Sai Rupak, IBM, Bangalore, India

Robert Schoberg, Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, British Columbia, Canada

Xuemin (Sherman) Shen, University of Waterloo, Waterloo, Ontario, Canada

Minghui Shi, University of Waterloo, Waterloo, Ontario, Canada

Krishna M. Sivalingam, University of Maryland, College Park, Maryland

Dionysios Skordoulis, Brunel University, West London, United Kingdom

Chris Snow, Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, British Columbia, Canada

K. S. Sridharan, DMACS, Sri Sathya Sai University, Bangalore, India

Bo Sun, Lamar University, Beaumont, Texas

Hsueh-Wen Tseng, National Taiwan University, Taipei, Taiwan, China

Yang Xiao, Department of Computer Science, University of Alabama, Tuscaloosa, Alabama

Jiang Xie, University of North Caroling, Charlotte, North Carolina

Wenbing Yao, Brunel University, West London, United Kingdom

Zhanping Yin, Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, British Columbia, Canada

Jianliang Zheng, Department of Electrical Engineering, City University of New York, New York

Chunhui Zhu, Samsung Electronics Corporation, San Jose, California

Haojin Zhu, University of Waterloo, Waterloo, Ontario, Canada

Weihua Zhuang, University of Waterloo, Waterloo, Ontario, Canada

PART I

IEEE 802.11 WIRELESS LANs

CHAPTER 1

IEEE 802.11 MEDIUM ACCESS CONTROL AND PHYSICAL LAYERS

KAVEH GHABOOSI, MATTI LATVA-AHO, and YANG XIAO

1.1 INTRODUCTION

A wireless local area network (WLAN) is an information system[1] intended to offer diverse location-independent network service access to portable wireless devices using radio waves instead of wired infrastructure. In corporate enterprises, WLANs are typically deployed as the ultimate connection between an existing cable infrastructure network and a cluster of mobile clients, giving them wireless access to the shared resources of the corporate network across a building or campus setting. Fundamentally, WLANs liberate customers from reliance on hard-wired access to the network backbone, giving them anywhere, anytime network services access. The pervasive approval of WLANs depends upon industry standardization to ensure product compatibility and reliability among various brands and manufacturers. Among existing system architectures, the IEEE 802.11 family is the most popular and accepted standard concerning medium access control (MAC) and physical (PHY) layers in WLANs; therefore, in this chapter, we briefly overview its basic features in both aforementioned layers. We start our investigation with the MAC layer and its fundamental components. Supported network types, different network services, and media access schemes are covered, accordingly. Subsequently, the physical layer and its basic characteristics are discussed. Different technologies,

[1] In telecommunications, an information system is any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment that are used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data and includes software, firmware, and hardware (Federal Standard 1037C, MIL-STD-188, and National Information Systems Security Glossary).

Emerging Wireless LANs, Wireless PANs, and Wireless MANs. Edited by Y. Xiao and Y. Pan

including frequency hopping (FH), direct-sequence spread spectrum (DSSS) and its high rate (HR) counterpart (i.e., HR/DSSS), and orthogonal frequency division multiplexing (OFDM), recommended for the IEEE 802.11 physical layer are then explored. As a result, this chapter can be assumed as a comprehensive overview of the IEEE 802.11 standard.

1.2 IEEE 802.11 MAC PROTOCOL

In 1997, the IEEE 802.11 working group (WG) proposed the IEEE 802.11 WLAN standard and, subsequently, a revised version was released in 1999. The primary medium access scheme in IEEE 802.11 MAC is the distributed coordination function (DCF), a contention-based protocol which is based on the carrier sense multiple-access/collision avoidance (CSMA/CA) protocol. In the DCF, mobile terminals should contend for the shared wireless channel, and as a result, the medium access delay for each station (STA) cannot be bounded in heavy-traffic-load circumstances. Thus, the DCF is capable of offering only asynchronous data transmission on a best effort (BE) basis. In order to support real-time traffic such as voice and video, the point coordination function (PCF) scheme has been advised as a noncompulsory option. Basically, the PCF is based on a centralized polling scheme for which a point coordinator (PC) residing in an access point (AP) provides contention-free services to the associated stations in a polling list. In addition to the IEEE 802.11 standard [1], there is a well-known book by Gast [2] which is considered as a complete scientific review of 802.11 families. Due to the popularity of the aforementioned book, we will use it frequently throughout the section to refer the reader to more technical issues and discussions.

Recently, considerable interest in wireless networks supporting quality of service (QoS) has grown noticeably. The PCF is already available in IEEE 802.11 to offer QoS but has not yet been implemented in reality due to its numerous technical limitations and performance drawbacks. For that reason, the 802.11 WG initiated IEEE 802.11e activity to develop the existing 802.11 MAC to facilitate support of QoS. Regarding the 802.11e amendment, not only the IEEE 802.11e standard [3] but also recognized introductory and survey papers [4, 5] will be used repeatedly as key references. We cite many technical issues from these works and the references therein to more appropriately explain 802.11/802.11e-based system features.

1.2.1 Categories of 802.11 Networks

The key constructing component of an 802.11 network is the basic service set (BSS), a group of wireless terminals that communicate with each other over a common radio channel [1, 2]. Data transmission is accomplished within a *basic*

service area, defined by radio propagation characteristics of wireless channel. BSSs come in two categories, as illustrated in Fig. 1.1.

The *infrastructure BSS* networks are primary for mobile stations to access the Internet via an AP so that, in most of cases, communications between two stations within the same service set do not happen. In communications between mobile stations in the same service set, the AP deployment acts as an intermediate node for all information exchanges comprising communications. In other words, any data communication between two wireless clients should take two successive hops, i.e., source STA to AP and AP to destination STA. Obviously, the exploitation of APs in infrastructure networks brings two major advantages. On the one hand, no restriction is placed on the physical distance between mobile stations. On the other hand, allowing straight communication between wireless terminals would apparently preserve system capacity[2] but at the cost of increased physical and MAC layer complexity. The most important functions of an AP are to assist stations in accessing the Internet and help save battery power in associated wireless stations. If a mobile terminal is in the power-saving (PS) mode, the AP buffers those frames destined to reach the station during the period it will be in PS status. When the terminal exits the PS mode, the AP forwards the cached data frames to the station one by one. Hence, APs evidently play a key role in infrastructure networks to make implementation of PS mechanisms possible [1].

In the independent BSS (IBSS), mobile stations are allowed to communicate directly. Characteristically, IBSSs are composed of a few stations configured

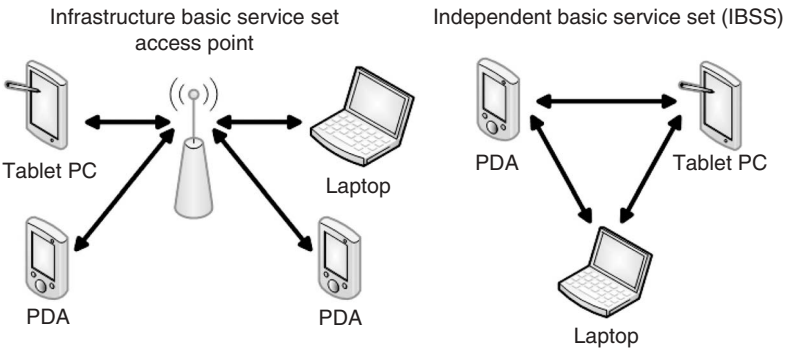

FIGURE 1.1 Infrastructure and independent basic service sets.

[2] In computer science, *channel capacity* is the amount of discrete information that can be reliably transmitted over a channel. By the noisy-channel coding theorem, the channel capacity of a given channel is the limiting information transport rate (in units of information per unit time) that can be achieved with vanishingly small error probability.

for a particular goal and for a short period of time. IBSSs are sometimes referred to as ad hoc BSSs or simply ad hoc networks.

IEEE 802.11 allows wireless networks of arbitrary size to be installed and utilized by introducing the extended service set (ESS) concept. Basically, the ESS is constructed by chaining neighboring BSSs and requires a backbone system that provides a particular set of services. Figure 1.2 illustrates an ESS as a combination of three neighboring BSSs. Switching between adjacent BSSs while being connected to the system is called a handoff.[3] Stations with the same ESS are able to communicate with each other even if they are not in the same BSS or are moving from one point to another. For associated stations within an ESS, a wireless network should behave as if it were a single layer 2 local area network (LAN). In such an architecture, APs are similar to layer 2 bridges; consequently, the backbone network should be a layer 2 network as well (e.g., Ethernet). Several APs in a single area may be connected to a single switch or can even use virtual LANs (VLANs) if the link layer connection spans a larger area. 802.11 supplies link layer mobility within an ESS, but only if the backbone network is a single link layer domain, such as a shared Ethernet or a VLAN [2].

Theoretically, extended service areas are the highestlevel abstraction supported by 802.11 wireless networks. In order to let non-802.11 network devices use the same MAC address to exchange data traffic with an associated station somewhere within the ESS, APs should mimic an absolute cooperative system. In Fig. 1.2, the illustrated gateway uses a single MAC address to deliver data frames to the targeted mobile stations in different BSSs. This is the MAC address of an AP with which the intended wireless station has been already associated. As a result, the gateway is unaware of the actual location of a tagged wireless terminal and relies only on the corresponding AP to forward data traffic [1, 2]. The backbone network to which APs are connected is called the distribution system (DS) since it makes delivery of information to and from the outside world possible.

It should be noted that technically different types of 802.11 networks may coexist at the same time. For instance, IBSSs might be constructed within the basic service area of an AP. Coexisting infrastructure BSSs and IBSSs should share the same radio channel capacity and, as a result, there may be adverse performance implications from colocated BSSs as well [2].

[3] In cellular telecommunications, the term *handoff* refers to the process of transferring an ongoing call or data session from one channel connected to the core network to another. In satellite communications, it is the process of transferring satellite control responsibility from one earth station to another without loss or interruption of service. The British term for transferring a cellular call is *handover*, which is the terminology standardized within European-originated technologies such as Global System for Mobile (GSM) communications and Universal Mobile Telecommunications System (UMTS). In telecommunications, there are two reasons why a handoff (handover) might be conducted: if the mobile terminal has moved out of range from one cell site, i.e., base transceiver station (BTS) or AP, and can get a better radio link from a stronger transmitter or, if one BTS/AP is full, the connection can be transferred to another nearby BTS/AP.

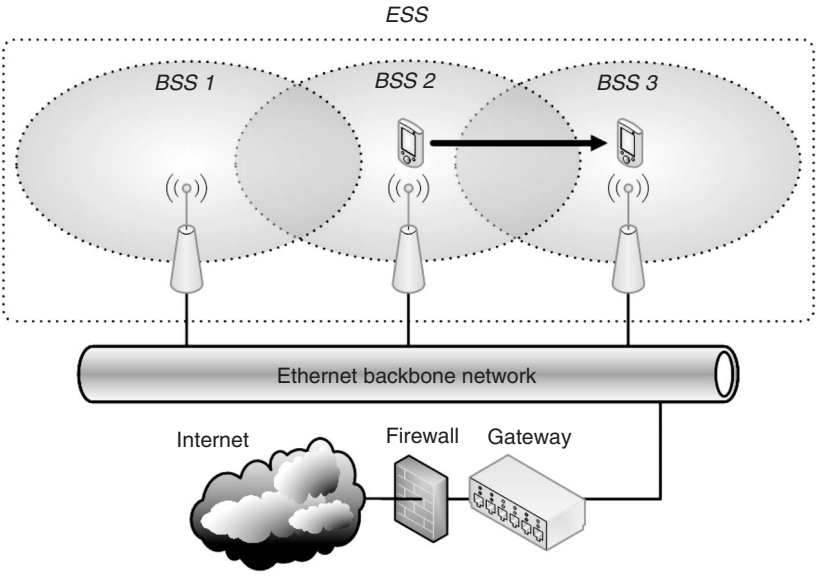

FIGURE 1.2 Extended service set.

1.2.2 IEEE 802.11 Networks Services

Generally the IEEE 802.11 standard provides nine dependent services: Three of these services are dedicated distinctively to data transfer purposes while the remaining ones are explicitly devoted to management operations enabling network systems to keep track of mobile stations and react in different circumstances accordingly.

The *distribution* service is exploited in infrastructure networks to exchange data frames. Principally, the AP, upon receiving a MAC protocol data unit (MPDU), uses this service to forward it to the intended destination station. Therefore, any communication with an AP should use a distribution service to be possible. *Integration* is a specific service provided by the distribution system that makes connection with a non-802.11 network possible. The integration function is not expressed technically by the standard, except in terms of the services it should offer.

MAC frame delivery to the associated terminals will not be possible unless the *association* service ensures that the AP and connected stations can work together and use the network services. Consequently, the distribution system is able to use the registration information to determine the AP with which a specific mobile station has been associated. In other words, unassociated wireless terminals are not permitted to obtain *any* service from the whole system. In an ESS, when a mobile station moves between different BSSs, there should be a set of handoffs to be accomplished in order to keep the station connected to the system. *Reassociation* is generally initiated by a wireless

terminal once the signal strength indicates that a different association is necessary. This means that handoff and reassociation requests are never commenced by APs. Upon completion of reassociation, the distribution system renews its location records to reflect the latest information about reachability of the mobile station. To terminate an existing association, wireless stations may possibly use the so-called *disassociation* service. Upon invocation of disassociation, any mobility information stored in the distribution system corresponding to the requesting station is removed at once.

Authentication is an obligatory prerequisite to association due to the fact that only authenticated users are authorized to use the network resources. If the APs of a distribution system have been configured in such a way as to authenticate any station, then the system is called an "open system" or an "open network." These kinds of wireless networks can be found, for instance, at university campuses. *Deauthentication* terminates an authenticated relationship between an AP and a wireless station. Since authentication is required before system resources utilization, a side effect of deauthentication is termination of any existing association.

IEEE 802.11 offers a noncompulsory *privacy* service called wired equivalent privacy (WEP). WEP is not iron-clad security; in fact, it can be easily disabled. In response, the IEEE 802.11i task group (TG) is seeking an enhanced and stronger security scheme to be included in the next generation of 802.11 equipments. IEEE 802.11i, known as WiFi-protected access version 2 (WPA2), is an amendment to the 802.11 standard specifying security mechanisms for wireless networks. It makes use of the advanced encryption standard (AES) block cipher, while WEP and WPA (an earlier version) use the RC4 stream cipher. The 802.11i architecture contains the following components: 802.1X for authentication [entailing the use of extensible authentication protocol (EAP) and an authentication server], the robust security network (RSN) for keeping track of associations, and the AES-based counter mode with cipher block-chaining message authentication code protocol (CCMP) to provide confidentiality, integrity, and origin authentication. Another important element of the authentication process is an innovative four-way handshake.

The MPDU is a fancy name for 802.11 MAC frames. The MPDU does not, however, include PHY layer convergence procedure (PLCP) headers. On the other hand, the MAC service data units (MSDUs) are only composed of higher level data units [e.g., Internet protocol (IP) layer]. For instance, an 802.11 management frame does not contain an MSDU. Wireless stations provide the *MSDU delivery* service, which is responsible for getting the data to the actual recipient.

1.2.3 IEEE 802.11 Media Access Schemes

In what follows, we discuss the medium access rules defined in the 802.11 standard and its corresponding amendments. We begin the discussion with the contention-based *802.11 DCF* access scheme. Subsequently, a few paragraphs

are dedicated to the *802.11 PCF*, which is a contention-free channel acquisition technique. Finally, the supplementary QoS-aware amendment of the IEEE 802.11 standard, i.e., the *802.11e hybrid coordination* function (*HCF*), is explored [1–3].

1.2.3.1 IEEE 802.11 DCF. The fundamental IEEE 802.11 access scheme is referred to as the DCF and operates based upon a listen-before-talk (LBT) approach and CSMA/CA.

As indicated, MSDUs are transmitted using MPDUs. If the wireless station chooses to fragment a long MSDU into a number of MPDUs, then it should send the long MSDU through more than one MPDU over the radio system. 802.11 stations deliver MSDUs following a media detection procedure dealing with an idle wireless channel that can be acquired for data transmission. If more than one station senses the communication channel as being idle at the same time, they might commence their frame transmissions simultaneously, and inevitably a collision occurs subsequently. To minimize the collision risk, the DCF uses carrier sense functions and a binary exponential backoff (BEB) mechanism. In particular, two carrier sense schemes, namely physical and virtual carrier sense functions, are employed to simultaneously resolve the state of the radio channel. The former is offered by the physical layer and the latter by the MAC layer, called network allocation vector (NAV). The NAV records the duration that the medium will be busy based upon information announced before the control/data frames are captured over the air interface. If either function indicates a busy medium, the medium is considered busy (i.e., reserved or occupied); if not, it is considered idle. Subsequent to detection of wireless medium as *idle*, for a so-called DCF interframe space (DIFS) time duration, stations continue sensing the channel for an extra random time period called a *backoff period*. The wireless station begins traffic delivery whenever the shared medium remains idle over this further random time interval. The backoff time is determined by each station as a multiple of a pre defined slot time chosen in a stochastic fashion. This means that a fresh independent random value is selected for every new transmission. In the BEB algorithm, each station chooses a random backoff timer uniformly distributed in an interval [0, CW – 1], where CW is the current *contention window* size. It decreases the backoff timer by 1 for every idle time slot. Transmission is started whenever the backoff timer reaches zero. When frame transmission fails due to any reason, the station doubles the CW until it reaches the maximum value CW_{max}. Afterward, the tagged station restarts the backoff procedure and retransmits the MAC frame when the backoff counter reaches zero. If the maximum transmission retry limit is reached, the retransmission should be stopped, the CW should be reset to the initial value CW_{min}, and the MAC frame is simply discarded. At the same time as a wireless station is counting down its backoff counter, if the radio channel becomes busy, it suspends its backoff counter decrement and defers from the media acquisition until the medium again becomes idle for a DIFS [1, 2, 4, 5].

Each MPDU requires the reception of an acknowledgment (ACK) frame to confirm its correct transmission over the wireless channel. If for any reason the intended ACK frame is not received right after the MPDU transmission, the source station concludes that the MPDU was not delivered successfully and may reiterate the transmission. Basically, the CW size of a contending station increases when the transmission fails. After an unsuccessful effort, the backoff procedure is restarted with a double-sized CW, up to a maximum value defined by CW_{max}. Alternatively, subsequent to a successful transmission, the tagged station exploits another random backoff, even if there is no further queued MSDU to be delivered over the air interface. In the literature, this extra backoff is referred to as *post-backoff* given that it is executed subsequent to the data frame departure. There is an exception to the above-mentioned rule: If an MSDU arrives from layer 3 when (1) the transmission queue is vacant, (2) the latest post-backoff has finished, and (3) the medium has been idle for at least one DIFS, then it may be delivered at once with no further backoff procedure [4].

To overcome the so-called *hidden terminal* problem, the IEEE 802.11 DCF media access scheme utilizes a request-to-send/clear-to-send (RTS/CTS) mechanism which can be exploited optionally prior to MPDU transmission. As illustrated in Figure 1.3, the source station sends an RTS control frame to its intended destination. Upon reception of the RTS by the receiver, it sends a CTS frame back to the source station. The RTS and CTS frames include information on how long it will take to deliver the upcoming data frame (in the fragmentation case, it indicates the duration of the first fragment) and the corresponding ACK over the radio link. Upon reception of either the RTS or CTS, wireless stations located in the radio range of the transmitting node, in addition to those hidden to the source node and located in the transmission range of the destination station, set their local timer NAV, with the duration announced within the RTS/CTS frames. The RTS and CTS frames protect the MPDU from interferences due to other neighboring wireless nodes. Stations that receive these control frames will not initiate transmission until the above-mentioned NAV timer expires. Between two consecutive frames in the sequence

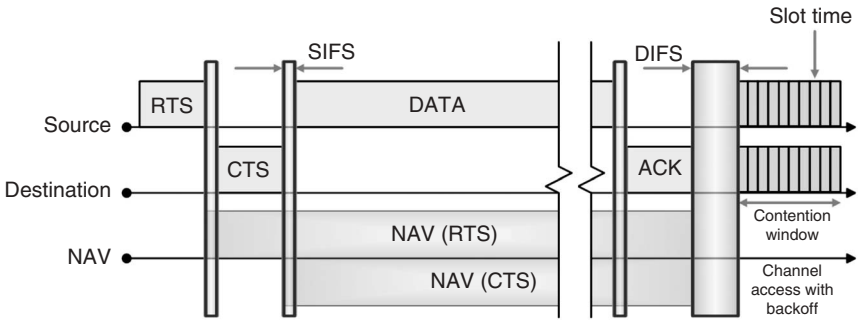

FIGURE 1.3 IEEE 802.11 RTS/CTS access scheme.

of RTS, CTS, MPDU, and ACK frames, a short interframe space (SIFS) gives transceivers time to switch (i.e., between transmitting and receiving modes). It is noteworthy that the SIFS is shorter than the DIFS, which gives the CTS and ACK the highest priority access to the wireless medium [1].

1.2.3.2 IEEE 802.11 PCF. IEEE 802.11 employs an optional PCF to support QoS for time-bound delay-sensitive services. The PCF offers techniques for prioritized access to the shared radio channel and is centrally coordinated by a PC station which is typically an AP. The PCF has higher priority than the DCF scheme. With the PCF, a contention-free period (CFP) and a contention period (CP) alternate periodically over time, where a CFP and the subsequent CP form an 802.11 superframe. The PCF is exploited throughout the CFP, while the DCF is used during the CP access phase. Each superframe is required to comprise a CP of a minimum length that allows at least one MSDU delivery (at least one frame exchange) of maximum size and at the slowest transmission rate under the DCF. A superframe is initiated by a beacon frame generated by the AP. The beacon frame is transmitted irrespective of whether or not the PCF is used. These frames are employed to preserve synchronization of the local timers in the associated stations and to deliver protocol-related parameters. The AP transmits these management frames at regular predefined intervals. Each station knows precisely when the subsequent beacon will arrive. These points in the time domain are referred to as target beacon transmission time (TBTT) and are announced in the previous beacon frame [1, 2].

During the CFP, there is no contention among wireless stations; instead, they are polled periodically by the AP. The PC polls a station requesting delivery of a pending data frame. Whenever the PC has a pending frame destined to an intended station, it utilizes a joint *data* and *poll* frame by piggybacking the CF-Poll frame onto the data frame. Upon reception of the so-called CF-Poll + Data, the polled station acknowledges the successful data reception and piggybacks an MPDU as well if it has any pending data frame targeted to the AP. If the PC does not receive a response from a polled station after waiting for a PCF interframe space (PIFS), it polls the next station or ends the CFP. Thus, no idle period longer than a PIFS occurs during a CFP. Bear in mind that a PIFS is longer than a SIFS but shorter than a DIFS. Since a PIFS is longer than an SIFS, a poll is never issued, e.g., between Data and ACK frames; hence a poll frame does not interrupt an ongoing frame exchange. The PC continues the aforementioned procedure until the CFP expires. A particular control frame, CF-End, is broadcast by the AP as the last frame within a CFP to indicate the end of the CFP (see Fig. 1.4) [1, 2, 4].

The PCF has many problems that have been reported in the literature [4]. Among many others, erratic beacon frame delay and indefinite transmission duration of the polled stations are the most important drawbacks. At the TBTT, the PC schedules the beacon as the next frame to be transmitted, but the beacon can only be transmitted when the medium has been determined to be

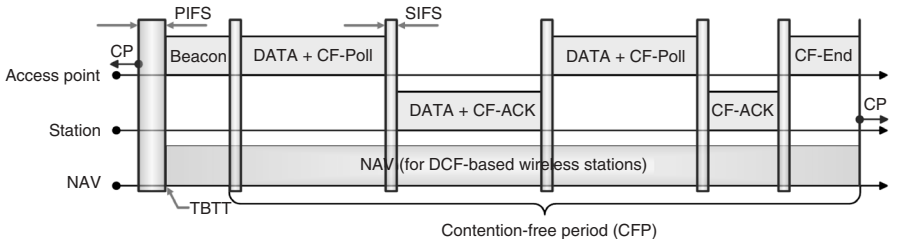

FIGURE 1.4 IEEE 802.11 PCF access scheme and TBTT.

idle for at least one PIFS. In IEEE 802.11, wireless stations are able to start their channel access even if the MSDU delivery is not finished before the upcoming TBTT. Depending upon whether the shared medium is idle or busy at the TBTT, a delay of the beacon frame might take place. The time the beacon frame is delayed from the TBTT determines the delay in a time-bounded MSDU transmission that has to be delivered in the CFP. This may rigorously influence the QoS as it introduces unpredictable time delays in each CFP. A further problem with the PCF is the unknown transmission duration of polled stations. A station that has been polled by the PC is allowed to deliver an MSDU that may be fragmented and of arbitrary length. In addition, different modulation and coding schemes are specified in the IEEE 802.11 family. Therefore, the duration of the MSDU is not under the control of the PC, which degrades the QoS offered to other stations polled during the rest of the CFP.

1.2.3.3 IEEE 802.11e: QoS Support in IEEE 802.11 MAC. The HCF, introduced in IEEE 802.11e, consists of two fundamental components: enhanced distributed-channel access (EDCA), an HCF contention-based channel access mechanism, and HCF controlled-channel access (HCCA). EDCA is the primary and mandatory access mechanism of IEEE 802.11e, while HCCA is optional and requires centralized polling and advanced scheduling schemes to distribute shared network resources among associated stations. According to the IEEE 802.11e, there can be two separate phases of operation within a superframe: CP and CFP. EDCA is used in the CP only, while HCCA is used in both phases. The HCF combines access methods of both the PCF and DCF, and this is why it is called *hybrid* [3].

The wireless station that operates as the central coordinator within a QoS-supporting basic service set (QBSS) is called a hybrid coordinator (HC). Similar to the PC, the HC resides within an 802.11e AP (i.e., QoS enabled access point (QAP)). There are *multiple* backoff entities operating in *parallel* within one QoS-aware 802.11e station (QSTA). A QSTA that is granted medium access opportunity should not occupy the radio resources for a time duration longer than a prespecified limit. This important characteristic of the 802.11e MAC protocol is referred to as transmission opportunity (TXOP). A TXOP is the

time interval during which a backoff entity has the right to deliver MSDUs and is defined by its starting time and duration. TXOPs obtained throughout the contention-based phase are referred to as EDCA–TXOPs. Alternatively, a TXOP obtained via a controlled medium access scheme is called an HCCA–TXOP or *polled* TXOP. The duration of an EDCA–TXOP is limited by a QBSS-wide parameter referred to as the *TXOPlimit*. This parameter is distributed regularly by the HC within an information field of the beacon frame. A further enhancement is that backoff entities of QSTAs are totally forbidden from transmitting across the TBTT. That is, a frame transmission is commenced only if it can be completed ahead of the upcoming TBTT. This reduces the expected beacon delay, which gives the HC superior control over the wireless media, especially if the noncompulsory CFP is exploited after the beacon frame. Moreover, an 802.11e backoff entity is allowed to exchange data frames directly with another backoff entity in a QBSS without involving communication with the QAP. Whereas within an 802.11-based infrastructure BSS all data frames are either sent or received by the AP, an 802.11e QSTA can establish a direct link with another 802.11e QSTA using the direct-link protocol (DLP) prior to initiating direct frame transmissions. It should be noted that here the backoff entity deals with the local backoff entity of a tagged QSTA; therefore, they are used interchangeably [3–5].

1.2.3.3.1 IEEE 802.11e: EDCA. In EDCA, QSTAs have up to four distinct and parallel queues for incoming traffic. Each queue is coupled with a specific access category (AC) and contends for the radio channel independent of the others. Collisions among a tagged station's queues are resolved internally, allowing the higher priority queue to commence its transmission while forcing the lower priority queue(s) to perform a collision response.[4] Different levels of service are provided to each AC through a combination of three service differentiation mechanisms: arbitrary interframe space (AIFS), CW size, and TXOPlimit [3].

In contrast to the DCF access rules by which the backoff procedure is started after the DIFS from the end of the last indicated busy medium, EDCA backoff entities start at different intervals according to the corresponding AC of the traffic queue. As already pointed out, these time intervals are called AIFSs. The time duration of the interframe spaceAIFS[AC] is given by

$$\mathrm{AIFS[AC]} = \mathrm{SIFS} + \mathrm{AIFSN[AC]} \times \mathrm{aSlotTime}$$

where AIFSN[AC] $\geq$ 2. Note that AIFSN[AC] should be chosen by the HC such that the earliest access time of 802.11e stations to be the DIFS, equivalent to IEEE 802.11. Note that the parameter aSlotTime defines the duration of a

[4] In the literature, the internal collision between independent backoff entities is called *virtual collision*.

time slot. The smaller AIFSN[AC] corresponds to the higher medium access priority. The minimum size of CW, i.e., $CW_{min}[AC]$, is another parameter which depends upon the AC. The initial value for the backoff counter is a random number taken from an interval defined by CW, which is exactly similar to the DCF case. Again, the smaller $CW_{min}[AC]$ corresponds to a higher priority in acquiring a shared radio channel. An important difference between the DCF and 802.11e EDCA in terms of the backoff countdown rule is as follows: (1) The first backoff countdown takes place at the end of the AIFSN[AC] interval. (2) A frame transmission is initiated after a slot from the moment the backoff counter becomes zero. The CW increases upon unsuccessful frame exchanges but never exceeds the value of $CW_{max}[AC]$. This parameter is defined per the AC as well as part of the EDCA parameter set. Note that the smaller $CW_{max}[AC]$ corresponds to a higher medium access priority. The aforementioned system configurations, in addition to the EDCA parameter set, are illustrated in Fig. 1.5.

As mentioned earlier, in addition to the backoff parameters, the TXOPlimit[AC] is defined per the AC as part of the EDCA parameter set. Apparently, the larger TXOPlimit[AC] is, the larger is the share of capacity for this AC. Once a TXOP is obtained, the backoff entity may keep transmitting more than one MSDU consecutively during the same TXOP up to a duration of TXOPlimit[AC]. This important concept in 802.11e MAC is referred to as *continuation* of an EDCA–TXOP (4).

As already explained, four self-governing backoff entities with different EDCA parameter sets exist inside an 802.11e QSTA. In a tagged QSTA when counters of two or more backoff entities reach zero simultaneously, they

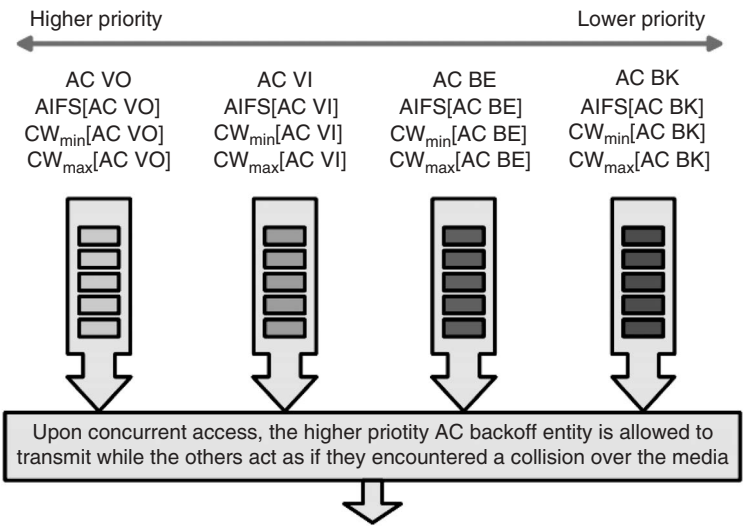

FIGURE 1.5 Four different access categories within a QSTA.

perform channel acquisition in the same time slot and consequently an internal *virtual collision* occurs. It should be noted that virtual collision is an abstract concept and there is no physical collision between contending backoff entities. When internal virtual collision occurs, the AC with the highest priority among collided entities is allowed to transmit, whereas all other backoff entities will act as if a collision has taken place on the shared radio channel.

1.2.3.3.2 IEEE 802.11e: HCCA. HCCA extends the EDCA medium access rules by assigning the uppermost precedence to the HC for the duration of both the CFP and CP. Basically, a TXOP can be attained by the HC through the controlled medium access stage. The HC may apportion TXOPs to itself in order to commence MSDU transactions whenever it requires, subsequent to detection of the shared wireless medium as being idle for PIFS, and without performing any further backoff procedure. To grant the HC a superior priority over legacy DCF and its QoS-aware counterpart, EDCA, AIFSN[AC] should be chosen such that the earliest channel acquisition for all EDCA stations can be the DIFS for any AC. During the CP, each TXOP of a QSTA begins either when the medium is determined to be available under the EDCA rules, i.e., after AIFS[AC] plus the random backoff time, or when a backoff entity receives a polling frame, the QoS CF-Poll, from the HC. The QoS CF-Poll is transmitted by the HC following a PIFS idle period and without any backoff procedure. On the other hand, for the duration of the CFP, the starting time and maximum duration of each TXOP is also specified by the HC, again by the use of QoS CF-Poll frames. In this phase, 802.11e backoff entities will not attempt to acquire the wireless media without being explicitly polled; hence, only the HC can allocate TXOPs by transmitting QoS CF-Poll frames or by immediately transmitting downlink data. Throughout a polled TXOP, the polled candidate mobile station can transmit multiple frames with a SIFS time space between two consecutive frames as long as the entire frame exchange duration does not exceed the dedicated maximum TXOPlimit. The HC controls the maximum duration of EDCA–TXOPs within its QBSS by the beacon frames. Thus, it is able to assign polled TXOPs at any time during the CP and the optional CFP [3].

Two supplementary schemes, namely block acknowledgement (BA) and DLP, which enhance the performance of the MAC protocol, have been taken into consideration in IEEE 802.11e [3, 4]. With the noncompulsory BA, the throughput efficiency of the protocol is improved. BA allows a backoff entity to send a number of MSDUs during one TXOP transmitted without individual ACK frames. The MPDUs delivered during the time of TXOP are referred to as a *block* of MPDUs in the literature and technical documents [4]. At the end of each block or in the next TXOP, all MPDUs are acknowledged at once by a bit pattern transmitted in the BA frame, and consequently the overhead of the control exchange sequences is reduced to a minimum of one ACK frame. On the other hand, each backoff entity is able to directly exchange information with any other backoff entity in the same QBSS without communicating

through the QAP. For IEEE 802.11 and within a BSS, all data frames are sent to the AP and received from the AP. However, it should be obvious that this procedure consumes at least twice the channel capacity in comparison to direct communication. For that reason, DLP is defined to enable pairs of 802.11e backoff entities to establish direct links between each other.

1.3 IEEE 802.11 PHYSICAL LAYER FAMILIES

In this section we first introduce the concepts utilized in radio-based 802.11 physical layers and then present detailed explanations of these physical layers.

The IEEE 802.11 physical layer is divided into two sublayers: the PLCP and the physical medium dependent (PMD). The PLCP receives incoming MSDUs from the MAC layer, adds its own designated header, and then gives them to the PMD. It is mandatory for delivered information to have a *preamble*, which has a pattern that depends on the modulation technique deployed in the physical layer. The PMD is responsible for transmitting every bit it receives from the PLCP over the wireless medium. The physical layer also incorporates a clear-channel assessment (CCA) function to inform the MAC layer when a carrier is detected [2]. Figure 1.6 illustrates the logical structure of the physical layer.

Three different physical layers were standardized in the initial revision of 802.11: frequency-hopping spread spectrum (FHSS), DSSS, and infrared (IR) light. Consequently, supplementary amendments 802.11a, 802.11b, and 802.11 g were developed which are based on OFDM, high rate (HR)/DSSS, and the extended-rate PHY (ERP), respectively. Also, it is noteworthy to mention that 802.11n will be based on multi-input multi-output (MIMO) OFDM [6, 7].

In telecommunications, avoiding interference is a matter of law and the most imperative issue that should be taken into account. Thus, an official authority should impose rules on how the radio frequency (RF) spectrum is to be deployed. In the United States, the Federal Communications Commission (FCC) is responsible for regulating the use of the RF spectrum. European regulation is accomplished by the European Radio-communications Office (ERO) and the European Telecommunications Standards Institute (ETSI). The Ministry of Internal Communications (MIC) regulates radio exploitation in

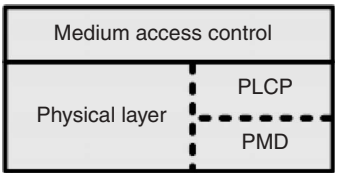

FIGURE 1.6 Physical layer logical structure.