OFDM
TOWARDS FIXED AND MOBILE BROADBAND WIRELESS ACCESS
OFDM Towards Fixed and Mobile Broadband Wireless Access
For a complete listing of the
Artech House Universal Personal Communications Series,
turn to the back of this book.
OFDM Towards Fixed and Mobile Broadband Wireless Access

Uma Shanker Jha
Ramjee Prasad
To my wife Mamta and our sons Abhisek and Sachin
—Uma Shanker Jha

To my wife Jyoti, our daughter Neeli, our sons Anand and Rajeev, our granddaughters, Sneha and Ruchika, and our grandson Akash
—Ramjee Prasad
## Contents

**Preface**  
$x_i$

Acknowledgments  
$x_{iii}$

1  
**Introduction**  
1  
1.1 Wireless Network Classifications  
1.1.1 Range  
1.1.2 Signaling  
1.1.3 Infrastructure  
1.2 WiMAX  
1.3 Wireless Broadband (WiBro)  
1.4 Comparative Analysis of New High–Data Rate Wireless Communication Technologies with WiMAX  
1.5 Preview of the Book  
References  
25
## OFDM Systems and Issues  

2.1 Introduction  
2.2 OFDM Concept  
2.3 OFDM Model  
2.4 Time-Frequency Interpretation  
2.4.1 Impairment Issues in OFDM Systems  
2.4.2 Frequency Offset  
2.4.3 Timing Offset  
2.4.4 Carrier Phase Noise  
2.4.5 Multipath Issues  
2.4.6 ISI Issues  
2.4.7 PAPR  
2.5 OFDMA  
2.5.1 Frequency-Hopping OFDMA  
2.5.2 OFDMA System Description  

## References

## Broadband Wireless Access Fundamentals

3.1 Introduction  
3.2 Basics of BWA  
3.2.1 BWA Considerations  
3.2.2 Frequency Band Allocation for BWA  
3.2.3 Will Fixed WiMAX Die?  
3.3 Wireless Broadband Landscape  
3.3.1 WWANs  
3.4 Global Deployment and Interoperability  
3.4.1 Air Interface and PHY Considerations  
3.4.2 Coverage  
3.4.3 QoS  
3.5 Deployment Considerations
4 Fixed Broadband Wireless Access

4.1 Introduction

4.1.1 10- to 66-GHz Licensed Band

4.1.2 Frequencies Below 11 GHz

4.1.3 License-Exempt Frequencies Below 11 GHz (Primarily 5 to 6 GHz)

4.1.4 Reference Model

4.2 Driving Factors of FBWA

4.2.1 Needs

4.2.2 Advantages

4.2.3 Market Segments for FBWA

4.2.4 Applications

4.3 MAC

4.3.1 Service-Specific CS

4.3.2 MAC CPS

4.3.3 Security Sublayer

4.4 PHY Layer

4.4.1 WirelessMAN-SC PHY Specification

4.4.2 WirelessMAN-SCa PHY

4.4.3 WirelessMAN-OFDM PHY

4.4.4 WirelessMAN-OFDMA PHY

4.5 FBWA Deployment Issues

4.6 Conclusions

References

5 Mobile Broadband Wireless Access

5.1 Introduction

5.2 IEEE 802.16e Standard
5.3 IEEE 802.16e Enhancements for Mobility 162
5.4 IEEE 802.16e MAC Enhancements 165
5.5 IEEE 802.16e MAC 167
5.5.1 PMP 167
5.5.2 MAC PDU Formats 168
5.5.3 Data Delivery Services for Mobile Networks 172
5.5.4 Sleep-Mode Support for Mobile Stations 173
5.5.5 MAC Layer Handover Procedures 175
5.5.6 Security Sublayer 178
5.6 Physical Layer Description 182
5.6.1 TDD Frame Structure 184
5.7 Conclusions 186
References 186

About the Authors 189

Index 193
Preface

niyatam sanga-rahitam araga-dvesatah kritam
aphala-prepsuna karma yat tat sattvikam ucyate

“That action which is regulated and which is performed without attachment, without love or hatred, and without desire for fruítive results is said to be in the mode of goodness.”

—The Bhagavad-Gita (18.23)

Broadband wireless access (BWA) requirements are driving the next generation wireless systems and gaining a lot momentum in the industry and academia alike. The next generation of wireless systems will be built to provide mobile Internet access. Although users and practitioners may have differing views about its capabilities and features, the majority of them nonetheless agree that orthogonal frequency division multiplexing (OFDM) will be the air interface of choice for next generation broadband wireless systems.
This book tackles both OFDM system fundamentals and issues including the essential features of the IEEE 802.16 family of standards. BWA technologies are increasingly coming into existence and thus knowledge about this topic is of utmost importance to the wireless community. We have realized that the standards bodies that set the standards for these systems generally produce documents that consist of hundreds and hundreds of pages, which are time consuming to read and to understand to say the least. The purpose of this book is to provide information about the topic in a simple manner, all at one point, by summarizing the key aspects of the BWA standard specified by IEEE 802.16 standards organization.

Figure P.1 details the organization of this book. This book provides a great deal of insight into the IEEE 802.16 standard. Although the term worldwide interoperability for microwave access (WiMAX) has become
synonymous with the IEEE 802.16 standard, in fact WiMAX only looks into the end-to-end interoperability aspects and certification of products built on their specific profiles. The IEEE 802.16 committee specifies the physical and media access control layers but does not deal with the end-to-end systems’ requirements and interoperability criteria of systems built on these requirements. The WiMAX consortium was organized to fill this void and to address two connectivity modes, namely, fixed broadband wireless access (FBWA) and mobile broadband wireless access (MBWA) for interoperability and certification purposes. These two modes are dealt with separately in this book. The OFDM technique is the fundamental building block of the IEEE 802.16 standards. Therefore, a separate chapter is devoted to OFDM and its variants. This book is the first of its kind to provide a simple physical layer and medium access control layer delineation of the standard. It is not our intent to provide substantial details about the standard, but to instead cover the salient features and to provide a basic understanding of the standard.

Completing this book gives us a sense of immense pleasure. We have tried our level best to make each chapter quite complete in itself. The purpose of this book is to provide supplemental reading material to young research students, engineers, undergraduate, graduate, and postgraduate students or anyone else who is interested in the development and deployment of next generation broadband wireless access systems.

As is often said, “Nothing is perfect”—which is true for this book as well in that we cannot claim that this book is error free. Any feedback to improve the content and correctness of the material would be highly appreciated.

Acknowledgments

We would like to convey our heartfelt appreciation to Junko and Shradha without whom this book would have never been completed. They gave their support in preparing the typewritten version of the book.
Introduction

Since the day Guglielmo Marconi demonstrated the ability of radio to provide instant communication, new wireless communication methods have been evolving [1]. People throughout the world are passionately accepting the new wireless communication methods and services. There has been rapid growth in the field of wireless communications in the past two decades, fueled by the need to be always connected, anywhere and anytime. Large-scale deployment of affordable, easy-to-use radio communication networks have given consumers the ability to be in continuous contact. Mobile communication has gone through generations of evolution to bring enhanced and value-added features and services to consumers. Second generation (2G), 2.5G, and third generation (3G) standards of mobile systems are being deployed while efforts are ongoing toward the development and standardization of beyond 3G (B3G) systems and, ultimately, to the much talked about fourth generation (4G) [2]. Figure 1.1 illustrates how the progress toward the next generation in communication technology, 4G, can be perceived as a tree with many branches.

2G services have been used predominantly for voice communications. Although 3G provides data services efficiently at lower cost, it lacks the capabilities to provide broadband real-time services with the required
quality of service (QoS) to support simultaneous voice, data, and multi-
media services to a large group of subscribers. The global demand for
multimedia data services has grown at a remarkable pace, which has led to
the expansion of system capacity in terms of the number of subscribers
supported, higher data rate, and ubiquitous coverage with high mobility.
Thus, it is an important consideration for both equipment manufacturers
and service providers [4] to attract customers and collect healthy return
on investments. Figure 1.2 shows how the technology has progressed
from 2G cellular systems toward existing ones and how this in a natural
way leads toward fulfilling the ever-increasing demands of the consumers
and service providers and, thus, to next generation [5].

Broadband wireless access systems can provide multimedia services
to large numbers of customers and thus have evolved as the solution for
the persistent demand for enhancement in multimedia data services.
Broadband is defined as having instantaneous bandwidths greater than around 1 MHz and supporting data rates greater than about 1.5 Mbps [6]. Intel defines it as a continuum of co-existing, overlapping technologies that enable high-speed communications [7].

1.1 Wireless Network Classifications

Various types of wireless networks can be broadly classified into three categories [8]:

- Range;
- Signaling;
- Infrastructure.
1.1.1 Range

Range depends upon the amount of power a transmitter can deliver. The transmitted power varies from country to country, whose regulatory bodies determine the maximum amount of power in each frequency band. Wireless networks can be classified according to their range. The four types of networks are as follows:

- Wireless personal area network (WPAN) ~ 10m;
- Wireless local area network (WLAN) ~ few hundreds of meters;
- Wireless metropolitan area network (WMAN) ~ few kilometers;
- Wireless wide area network (WWAN) ~ few tens of kilometers.

1.1.1.1 WPAN

With the growth of wireless technologies, the electronics manufacturers have realized that consumers are interested in having freedom from cumbersome connection of cords. Wireless Personal Area Network provides connectivity among different electronic devices utilizing low power short-range wireless connection, thus removing the need of connecting one device to the other through wires. This provides flexibility and ability to move around in a small area, for example in an office or home.

A personal area network (PAN) provides networking of various personal and wearable devices within the space surrounding an entity (such as a person), thus providing the communication capabilities within that space and with the outside world. In Figure 1.3, it can be seen that PAN is a network solution that enhances one’s personal environment by allowing the person to communicate with his or her personal devices in the vicinity and to establish wireless connection with the outside world. PAN can interconnect pocket PCs, personal digital assistants (PDAs), cell phones, webpads, head-mounted displays, and other appliances [9–14].

“The PAN is a network for you, for you and me, and for you and the outer world.” It is based on a layered architecture in which different layers cover the specific types of connectivity. This connectivity is enabled through the incorporation of different networking functionalities into the different devices. So, for the stand-alone PAN, the person is able to
address the devices within his personal space independent of the surrounding networks. For direct communication between two people (i.e., their PANs), the bridging functionality is incorporated into each PAN. For communication through external networks, a PAN implements routing and/or gateway functionalities.

PAN is a dynamic network concept and uses various access technologies for acquisition, access, and maintenance of a session. Moreover, according to the applications, PAN systems provide automatic service and resource discovery, offer QoS (i.e., for multimedia applications), and are scalable in terms of network size. Figure 1.4 presents the general PAN network model.

There are a number of existing concepts of PAN, but the most popular technical solution is Bluetooth [15], named after the Viking king, Herald Bluetooth, who unified parts of Sweden, Denmark, and Norway in the tenth century [16, 17].

The Bluetooth concept originated from an Ericsson project in 1994, and its initial idea was merely replacement of wires [17]. The standardization activity of Bluetooth is done by the Institute of Electrical and Electronics Engineers (IEEE) standards committee that was formed to provide an international forum for the development of Bluetooth and
other PANs. Bluetooth is standardized under the name IEEE 802.15.1, and some of its ideas are incorporated in the ongoing IEEE 802.15 standards concerning PANs [16, 18].

Bluetooth is designed to be used in a short-range radio link between two or more mobile stations supporting point-to-point or point-to-multipoint connection. Two or more units sharing the same medium create a piconet. In a piconet, there can be one master communicating with up to seven slaves. A station can act either as a master or as a slave when required. Any Bluetooth device that initiates a connection assumes the role of master. Multiple piconets constitute a scatternet, in which a station that is master in one piconet can be a slave in another one.

The main characteristics of the Bluetooth system are presented in Table 1.1. Bluetooth uses a frequency-hopping time division duplexing (TDD) for each radio channel and operates in the 2.4-GHz industrial, scientific, and medical (ISM) band. Each Bluetooth radio channel has a bandwidth of 1 MHz and the hopping rate is approximately 1,600 hops.

### Table 1.1
Bluetooth System Characteristics

<table>
<thead>
<tr>
<th>Item</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spectrum</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>Maximum physical rate (symbol rate)</td>
<td>1 Mbps</td>
</tr>
<tr>
<td>Access method</td>
<td>TDMA/FDMA-TDD</td>
</tr>
</tbody>
</table>

*Source: [9].
Note: TDMA = time division multiple access; FDMA = frequency division multiple access.*
per second. It provides an ad hoc approach for communication between various devices [8].

A few more technologies, such as ultra-wideband (UWB) and ZigBee, have also been developed as WPAN standards. PAN-oriented applications mostly use unlicensed frequency bands. For higher data rates, the 5-GHz frequency band, and possibly 60 GHz, can be used, but the advent of UWB access techniques already offers data rates of up to 1 Gbps for very short ranges. Works are ongoing for higher data rates, leading the path toward broadband WPANs. It is envisaged that all the mobile terminals will have WPANs in the near future [1, 9, 17].

The extension of WPAN in creating personal networks (PNs) is envisioned to influence the evolution of the 4G [3, 19] standard. The European Commission Sixth Framework Integrated Project, “My Personal Adaptive Global Net (MAGNET),” is leading WPAN in the direction where people can exchange their digital intelligence in a seamless way. The MAGNET vision is that PNs will support the users’ professional and private activities, without being obtrusive, while safeguarding their privacy and security [20].

PNs consist of communicating clusters of native and alien devices, possibly shared with others and connected through various suitable communication means [17]. In a PN, a user is able to connect to personal devices and services using whatever infrastructure is available for communication. PNs are dynamic in the sense that they are created, maintained, and destructed in an ad hoc manner; for example, when a user moves around a building, nodes become a part of the ad hoc network and may also leave the network when out of range or for any other reasons (such as no longer of use to the user). In fact, a PN can be defined as [19]:

*A dynamic overlay network of interconnected local and remote personal devices organized in clusters, which are connected to each other via some interconnecting structure.*

An “interconnecting structure” includes Internet, intranet, WPAN, WLAN, WMAN, WWAN (cellular systems), public switched telephone network (PSTN), and ad hoc networks. Figure 1.5 illustrates the concept of a PN, showing its heterogeneous collection of networks.
Figure 1.5 Conceptual illustration of PNs. *(From: [21]. © 2004 MAGNET. Reprinted with permission.)*
The realization of PNs will be an important step in the unpredictable path of 4G. In the authors’ view, 4G can be defined by the following equation [17]:

\[
B3G + \text{Pers} = 4G
\]

where \(B3G\) stands for beyond third generation, defined as the integration of existing systems to interwork with each other and with the new interface, and \(\text{Pers}\) stands for personalization, which is the key issue in PNs.

Mobile ad hoc networks (MANETs) also have an important link with WPANs. In the late 1990s, the Internet Engineering Task Force (IETF) created its MANET group [22, 23], which works mainly on the routing aspects of mobile ad hoc networks. WPANs were originally designed as a simple cable replacement, but now they are evolving toward more complex networks of various mobile devices with very different capabilities. Since the global WPAN system acts as an autonomous system of mobile routers, which are free to move and are capable of organizing themselves, MANETs are an important concept for PANs.

A typical person’s day requires interaction with more than just applications and services. In fact, most people have family to interact with, have jobs, friends, or other contacts with whom they might eventually need to share information, resources, services, or applications. To ensure a maximum utilization of PNs, the components in a PN must support the user’s wishes to share services, resources, and information with friends, family, coworkers, and so on. For these situations, a PN needs to be federated with the groups with which the user wishes to interact. The interaction can then provide for various roles in the communication; for example, a person may wish to share more, or private, information with his wife than with a coworker, and so on. Figure 1.6 illustrates the basic principle of federated networks.

For federated PNs security and privacy become even more important issues than for PNs, since now users will be able to interact and share services, resources, information, and so on that are susceptible to malicious persons. Trust relations and authentication of invited users will become an even more important issue since the number of possible combinations of interaction between users in the world is extremely high, and
not all users one is interacting with may be as nice as we would like to believe. The Information Society Technologies (IST) project MAGNET Beyond [24] takes up the challenge of moving PNs this step farther, toward a federation of PNs.

1.1.1.2 WLAN

This section provides a short introduction to the WLANs [9, 17, 25, 26]. WLAN plays as important role as a complement to the existing or planned cellular networks. The market penetration of WLAN has been extensive due to its easy and low cost deployment, wide interoperability, and inherent flexibility.

WLAN provides both infrastructure as well as an ad hoc mode of connectivity to the network. IEEE 802.11–based WLANs work in both modes. WLANs provide network connectivity in areas where wiring/cabling is neither cost effective nor feasible. They provide connectivity for slow mobility with high throughput for both indoor and outdoor

Figure 1.6 Federation of PNs. (From: [19]. © 2006 TELEKTRONIKK. Reprinted with permission.)
environments. Network extension and changes can also be made. WLAN technologies may support higher throughput and longer range at the expense of cost and power consumption. Typically, WLANs provide links from portable laptops to a wired LAN via access points.

WLAN technologies are mainly used for datacentric communication using Internet Protocol (IP) packets. The majority of these devices are capable of transmitting information up to several 100s of meters in an outdoor environment. The components of WLANs consist of a wireless network interface card, known as station (STA), and a wireless router/bridge, referred to as an access point (AP). The AP interfaces the wireless network with the wired network. The most widely used WLANs use the ISM frequency band around 2.4 GHz. This band supports nonline-of-sight connectivity but suffers from interference with equipment working at the same frequency. WLAN standards employ frequency-hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), and orthogonal frequency division multiplexing (OFDM). In the first two techniques, signal power is spread over a wide band of frequencies, which makes the data much less susceptible to electrical noise than conventional radio modulation techniques [27].

In 1990, the IEEE formed a committee to develop a standard for wireless LANs, operating at 1 and 2 Mbps. The IEEE 802.11 system was approved in 1997. The 802.11 standard provides medium access control (MAC) and physical (PHY) functionality for wireless connectivity for fixed, portable, and moving terminals, at portable and vehicular speeds within a local area [28–36]. IEEE 802.11–based WLAN [37–39] was the first and is the most prominent among the several WLAN standards that have come into being in recent years. In 1999, the Wireless Ethernet Compatibility Alliance (WECA) was formed to allow for interoperability among IEEE 802.11 products from various vendors. A Wireless Fidelity (Wi-Fi) interoperability test was developed by the alliance and the logos were provided as product certification. Today, Wi-Fi has become a synonym for IEEE 802.11, and the alliance is now named the Wi-Fi Alliance. There are many groups in the Wi-Fi Alliance [7, 26]:

- IEEE 802.11 was the first standard of the series in frequency-hopping spread spectrum, with a theoretical data rate of
2 Mbps utilizing carrier sense multiple access with collision avoidance (CSMA/CA).

- Subsequent standard IEEE 802.11b provided a theoretical data rate of 11 Mbps with a range of 100m to a maximum of a few hundreds of meters. It operates in the 2.4-GHz unlicensed band.
- The newest IEEE 802.11a standard has a theoretical data rate of 54 Mbps, but it decreases with the distance more quickly than in 802.11b due to its operating frequency of 5 GHz. It operates in the 5-GHz band and has a range of more than 100m.
- IEEE 802.11e includes MAC enlacements for QoS extension.
- IEEE 802.11f is an extension for managing handover.
- Ratified in 2003, IEEE 802.11g has a theoretical data rate of 54 Mbps, but it operates in the 2.4-GHz unlicensed band.
- IEEE 802.11h addresses European Radio Communications Committee requirements at 5 GHz with the addition of transmission power control (TPC) and dynamic channel selection (DCS).
- IEEE 802.11i provides a security extension.
- IEEE 802.11j provides enhancement of the 802.11 standard and amendments and adds channel selection for 4.9 and 5 GHz in Japan.
- IEEE 802.11k defines radio resource measurement enhancements to provide mechanisms to higher layers for radio and network measurements.
- IEEE 802.11n has a theoretical data rate of 320 Mbps utilizing multiple input multiple output (MIMO) and receiver techniques to boost the peak data rate and throughput. It operates in the 2.4- and 5-GHz bands. The provisioning of QoS is included in the standard.
- IEEE 802.11r is working on fast roaming, mainly for Voice over IP (VoIP) service.
- IEEE 802.11s is working on AP-based mesh networks.
- IEEE 802.11t focuses on wireless performance prediction.
Other LAN standards such as High Performance LAN (HIPERLAN) and Multimedia Mobile Access Communication (MMAC) have either absorbed the IEEE 802.11 family of standards or have faded away. The HIPERLAN standard is being developed by the Broadband Radio Access Network (BRAN) Working Group of the European Telecommunication Standards Institute (ETSI). In Japan, equipment manufacturers, service providers, and the Ministry of Post and Telecommunication are cooperating on MMAC project.

The exponential growth of the Internet and wireless has brought about tremendous change in LAN technology in recent years. WLAN technology is still ripening and the market has just started opening. WLANs are to be used in several environments such as the home, office, and public hot spots, to name a few [17].

1.1.1.3 WMAN

WMAN is a wireless network for providing operating coverage in a wider area, tailored for covering dense urban and remote unserved areas. Just as IEEE 802.11, the standard for WLANs, was developed to provide cost-effective coverage in offices, homes, and airports, similarly in IEEE 802.16, the WMAN standards are envisioned to provide cost-effective spectrally efficient connectivity for neighborhoods, villages, and cities. WiMAX, which stands for Worldwide Interoperability for Microwave Access, is a WMAN technology. WiMAX, an industrial working group, was formed to promote deployment of broadband wireless access networks by using global standards and to provide the means for certifying interoperability of products and technologies from various vendors and OEMs. WiMAX provides broadband connectivity over a much wider area than Wi-Fi and may or may not require a line-of-sight path between the subscriber terminal and the access points. It claims to provide a theoretical data rate of up to 70 Mbps with a range of up to a maximum of 50 km. Also, a QoS feature has been added to ensure high performance for voice and video [40]. WiMAX addresses two usage models [41]:

- IEEE 802.16-2004 is a standard designed for fixed-access usage models.
IEEE 802.16e is an amendment to the IEEE 802.16-2004 base specification and targets the mobile market by adding portability and the ability for mobile clients to connect directly to the WiMAX network.

WMAN provides nonline-of-sight fixed broadband wireless access in the unlicensed as well as licensed 2- to 11-GHz frequency band, along with the line-of-sight communication in the 10- to 66-GHz band. The licensed and license-exempt spectra between 2 and 11 GHz are well suited for residential and small business applications using nonline-of-sight links. The IEEE 802.16 standard includes optional mesh architecture and supports multimedia services such as videoconferencing, voice, and gaming. Poor line quality of the installed copper base, the large distances to the central office or cabinets, or the low population density, high cost, and delay in availing services have limited the digital subscriber line (DSL), cable, and fiber optics markets in providing wireline broadband access equally in urban as well as remote areas.

In last-mile markets, where traditional cable or copper infrastructures are either saturated, outdated, or simply out of reach, the WMAN, with its quick deployment and reasonable cost structure, provides an attractive solution.

The WiMAX family of standards is covered thoroughly in this book. Within the 802 framework currently there is an ongoing activity to standardize a true mobile broadband wireless access (MBWA) standard in the form of IEEE 802.20, which is built from the ground up keeping mobility in mind. This group is developing a solution that starts from a clean slate, without the need for backward compatibility [2].

1.1.1.4 WWAN

Wide-area wireless access can be provided through satellites. Satellites allow cells the size of several countries and facilitate access to the Internet in nonaccessible rural zones [8]:

- Geostationary (GEO) satellites are located at 35,800 km above the ground, and they remain in the same position in the sky.
• Low-orbit (LEO) satellites require a “constellation” of satellites in order to have complete coverage of the ground surface. They provide commercial services such as telephony, broadcasting, and global positioning.

• Satellites in medium orbit (MEO) in the long term could constitute a good compromise between the need for a reduced number of satellites and the proximity of the ground, which allows less power consumption and reduced latency times.

WWANs can be commonly termed mobile communications. The growth in the field of mobile communications in the past decade has been tremendous. Now mobile communications are moving toward the next generation—4G—which is seen as the convergence of disparate technologies.

Existing 2G systems are mainly for voice, but 2.5G and 3G systems provide possibilities for data services with varying QoS requirements. At present, the main application for data services over mobile communication systems is Internet access. The future is toward a full-multimedia-type application providing various levels of QoS using an IP-based backbone [2].

1.1.2 Signaling

Wireless networks can be classified as with or without signaling protocol networks [8]:

• A cellular network is an example of a signaling protocol network. Networks with signaling protocol have been implemented by telecommunications operators for telephony. These types of networks ensure fixed bandwidth for a circuit-switched mechanism in which connection is fully dedicated for exchanges between the source and the receiver and provide fixed QoS for packet transmission.

• Local area networks, such as Ethernet, are called networks without signaling. The Internet is the perfect example of the utilization of
this kind of network. These networks are simple and easy to deploy and implement.

1.1.3 Infrastructure

Based on the infrastructure, there can be three cell interconnection methods [8]:

- Networks with infrastructure require another technology (often wired) to interconnect each access point for each cell. This makes it possible to constitute a wider network. These are the conventional point-to-point networks, which use a single link between the subscriber and the destination.

- In the “mesh” networks, the access points are sufficiently close to be “seen” and can communicate with one another without requiring additional infrastructure. Wireless mesh networks are multihop systems in which devices assist each other in transmitting packets through the network, especially in adverse conditions. In wireless mesh networks nodes are composed of mesh routers and mesh clients. Each node operates not only as a host but also as a router, forwarding packets on the behalf of other nodes that may not be within direct wireless transmission range of their destinations. These networks are dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves [42].

- In “ad hoc” networks each piece of equipment constitutes its own cell, which communicates with the others. Rather than the centralized approach of conventional wireless communications, where communications use a central node (base station, access point, or such) to access the network, an ad hoc network can be seen as a distributed approach, where the signal can hop through several nodes (terminals) to reach the destination. Routing protocols, user and service discovery procedures, and security issues are the main research items.
1.2 WiMAX

WiMAX is a nonprofit corporation formed by equipment and component suppliers to promote the adoption of IEEE 802.16–compliant equipment by operators of broadband wireless access systems. The organization is working to facilitate the deployment of broadband wireless networks based on the IEEE 802.16 family of standards by helping to ensure the compatibility and interoperability of broadband wireless access equipment [40, 41, 43, 44]. Table 1.2 shows the steps of development of broadband wireless technologies and the evolution of standard solutions [45].

WiMAX is the common name associated with the IEEE 802.16 standards. Initially, the specification was limited to the 10- to 66-GHz frequency band, but now it has been extended below 11 GHz in licensed as well as unlicensed bands [43, 46]:

- In April 2002, the IEEE 802.16-2001 standard was published, defining a point-to-multipoint fixed wireless access system operating in the 10- to 66-GHz frequency range.

- In January 2003, the IEEE approved 802.16a as an amendment to 802.16-2001, defining line-of-sight capability (see Table 1.3) [43].

<table>
<thead>
<tr>
<th>Year</th>
<th>Parameter</th>
<th>Chip Sets</th>
<th>Air Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000–2001</td>
<td>2 to 11 Mbps peak</td>
<td>Use 802.11 RF and PHY or proprietary</td>
<td>Frequency hopping and direct sequence</td>
</tr>
<tr>
<td>2002–2003</td>
<td>6 to 54 Mbps peak</td>
<td>OEMs forced to develop their own silicon—some use 802.11a RF and PHY</td>
<td>OFDM and S-CDMA approaches</td>
</tr>
<tr>
<td>2004–2005</td>
<td>Up to 72 Mbps peak</td>
<td>Volume silicon supplier</td>
<td>256 FFT OFDM and OFDMA</td>
</tr>
</tbody>
</table>
IEEE 802.16a-2003, published in April 2003, enables 2- to 11-GHz operation. It also introduces a mesh mode, enabling nodes to forward traffic to adjacent nodes.

In July 2004, a revision standard, IEEE 802.16d, now known as IEEE 802.16-2004, was published (see Table 1.3). This standard defines fixed broadband wireless access (FBWA) for bands 10 to 66 GHz and both licensed and unlicensed bands in the 2- to 11-GHz range.

Amendment IEEE 802.16e adds mobility support to IEEE 802.16. In February 2006, IEEE 802.16e-2005 was published that simultaneously supports both fixed and mobile services (see Table 1.3).

WiMAX can provide a wireless alternative to cable and DSL for the last-mile broadband access. It can connect Wi-Fi hot spots with each other and to other parts of the Internet. WiMAX provides the following [43]:

<table>
<thead>
<tr>
<th>Standard</th>
<th>Parameter</th>
<th>Customer Premises Equipment</th>
<th>Mobility</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.16a</td>
<td>E1/T1 service for enterprises Backhaul for hot spots Limited residential Broadband access</td>
<td>External box connected to PC with outside antenna</td>
<td>Fixed outdoor</td>
</tr>
<tr>
<td>802.16d</td>
<td>Indoor broadband access for residential users (high-speed Internet, VoIP, and others)</td>
<td>External box connected to PC with built-in antenna</td>
<td>Fixed outdoor</td>
</tr>
<tr>
<td>802.16e</td>
<td>“Portable” broadband access for consumers Always best connected</td>
<td>PC card</td>
<td>Limited mobility</td>
</tr>
</tbody>
</table>
• Expands the currently limited coverage of public WLAN (hot spots) to citywide coverage (hot zones).

• Blankets metropolitan areas for mobile datacentric service delivery.

• Offers fixed broadband access in urban and suburban areas where copper quality is poor or unbundling difficult.

• Bridges the “digital divide” in low-density areas where technical and economic factors make broadband deployment very challenging. Digital divide is the term associated with the difference in broadband accessibility between urban and remote, rural areas.

The 802.16 standard uses 256-point fast Fourier transform (FFT) OFDM or orthogonal frequency division multiple-access (OFDMA) with 2,048-point transform, depending upon the band being operated in. These access techniques can improve performance in situations where there is no line-of-sight path between the transmitter and the subscriber station. In these situations multipath interference and delay spread are significant. When operating in unpaired frequency bands, WiMAX equipment will use time division duplexing (TDD), while in licensed frequency bands either TDD or half-duplex frequency division multiplexing (FDD) will be used [47].

The WiMAX standard is developed to connect every link in the broadband wireless access chain. Operators, consumers, and manufacturers as well as equipment vendors all will benefit.

1.3 Wireless Broadband (WiBro)

In Korea, HPi, which means High-Speed Portable Internet, was first conceived as a Korean technology standard to provide better data handling than that of the 3G cellular system before 4G systems arrive, but it was renamed WiBro [48]. It has been developed to enable users to access the Internet anywhere, any time with high speed and good quality using portable equipment such as laptops, PDAs, and smart phones. The WiBro network is based on IEEE 802.16e broadband wireless access [49].
WiBro is a South Korean version of WiMAX [41, 50, 51]. Due to the lack of global appeal, WiBro has joined WiMAX and agreed to harmonize with the 802.16e OFDMA system with a 1,024 FFT size [41, 48]. It has adopted OFDMA/TDD for multiple-access and duplex schemes. It has several functions in addition to the IEEE 802.16 specification, such as handoff, sleeping mode, periodic ranging, and bandwidth stealing [52].

WiBro is designed to provide all-IP-based packet services, such as streaming video and music, video and music on demand, on-line gaming, and broadcasting over the 2.3-GHz spectrum at ground speeds up to about 60 km/h but over a relatively smaller area than with other mobile technologies [48]. WiBro promises an initial data rate as high as 1 to 3 Mbps. The WiBro download rate may eventually get up to about 18 Mbps. WiBro handles strictly data. It can carry voice traffic, but only by chopping it up into data packets and using VoIP [51]. The main characteristics of WiBro are the following [53]:

- Frequency, 2.3 GHz;
- Duplex/multiconnection, TDD/OFDMA;
- Channel bandwidth, 10 MHz;
- Modulation, quadrature phase shift keying (QPSK), 8PSK, 16QAM, 64QAM;
- Mobility, 60 km/h;
- Cell coverage
  - Pico, 100m;
  - Micro, 40m;
  - Macro, 1 km;
- Transmission rate per subscriber
  - Uplink, 128k–1 Mbps;
  - Downlink, 512k–3 Mbps;
- Handoff, below 150 ms [between cells in the radio access system (RAS) and inter-RAS]
- Frequency reuse factor, 1.
Services supported by WiBro can be classified into four categories owing to the QoS requirements. They are best effort (BE) service, real-time polling service (rtPS), nonreal-time polling service (nrtPS), and unsolicited grant service (UGS). WiBro incorporates mobile IP (MIP) registration, call admission control (CAC), L2/L3 mobility, and DiffServ mapping to support differentiated QoS. The MIP registration occurs at the request of L3 mobility to home agent (HA) for WiBro service. The CAC method decides to either accept or reject a request. The CAC mechanism has such parameters as bandwidth allocation, maximum/minimum traffic bandwidth, traffic priority, maximum delay, and tolerated jitters. These parameters are applied in the WiBro network depending upon the four service classes mentioned above. The L2 mobility is the provision of seamless mobility from one RAS to another RAS. The L3 mobility is the provision of seamless mobility from one network to another network by using MIP techniques. The DiffServ mapping method provides signaling transmission with hop by hop by using differentiated service code point (DSCP).

Figure 1.7 shows the current architecture of WiBro. There are four main components in the architecture: the portable subscriber station (PSS), RASs, the access control routers (ACRs), and the WiBro core network. The PSS communicates with RAS using WiBro wireless access technology. The PSS also provides the functions of MAC processing, MIP, authentication, packet retransmission, and handoff. The RAS provides wireless interfaces for the PSS and takes care of wireless resource management, QoS support, and handoff control. The ACR plays a key role in IP-based data services, including IP packet routing, security, QoS and handoff control, and foreign agent (FA) in the MIP. The ACR also interacts with the authentication, authorization, and accounting (AAA) server for user authentication and billing. To provide mobility for the PSS, the ACR supports handoff between the RASs while the MIP provides handoff between the ACRs.

In August 2006, Samsung successfully demonstrated 4G services based on Mobile WiMAX technology, which supported 1-Gbps data transmission speed while stationary and 100 Mbps while on the move. It clearly showed that Mobile WiMAX is the most advanced commercial technology that will open the future of the 4G era. As a result of all those
successful activities, major operators home and abroad have highly praised and showed a lot of interest in Mobile WiMAX. Some companies have done extensive feasibility testing for WiBro and WiBro services and they are providing infrastructure and terminals to Korean operators. The Korean government has even set license fees and issued guidelines for commercial WiBro services [51].

1.4 Comparative Analysis of New High–Data Rate Wireless Communication Technologies with WiMAX

It is commonly believed that WiMAX will compete with current 3G wideband code division multiple access (WCDMA) and CDMA2000 and their evolution systems [56]. The “super 3G” standard based on an upgrade for WCDMA is reported to support speeds 10 times faster than the Universal Mobile Telecommunications Services (UMTS) and is also
expected to compete with WiMAX. But mobile WiMAX, with an initial implementation data rate of 1 to 2 Mbps, will eventually provide a data rate of about 20 Mbps and will overtake all the similar technologies.

Table 1.4 provides a comparison between different technologies [57]. It is clearly seen that the mobile version of WiMAX reportedly supports high data rates, and it promises to provide mobile support for speeds up to 150 km/h.

### 1.5 Preview of the Book

This book focuses on the broadband wireless access technologies and mainly provides good insight to WiMAX standards. WiMAX addresses

<table>
<thead>
<tr>
<th>Technology</th>
<th>Bandwidth</th>
<th>Maximum Speed to Deliver Data</th>
<th>Number of Channels in 10 MHz</th>
<th>Total Maximum Speed to Deliver Video and Streaming Audio</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCDMA HSDPA</td>
<td>5 MHz</td>
<td>14.4 Mbps (fixed and mobile)</td>
<td>2</td>
<td>28.8 Mbps</td>
</tr>
<tr>
<td>CDMA2000 1xEV-DO RA</td>
<td>1.25 MHz</td>
<td>3.2 Mbps (fixed and mobile)</td>
<td>7</td>
<td>31.1 Mbps</td>
</tr>
<tr>
<td>IP wireless (UMTS TDD)</td>
<td>5 MHz</td>
<td>7.5 Mbps (fixed and mobile)</td>
<td>2</td>
<td>15.0 Mbps</td>
</tr>
<tr>
<td>Flarion</td>
<td>1.25 MHz</td>
<td>3.1 Mbps (fixed and mobile)</td>
<td>7</td>
<td>22.4 Mbps</td>
</tr>
<tr>
<td>WiMAX</td>
<td>20 MHz</td>
<td>75 Mbps (fixed/nomadic)</td>
<td>2</td>
<td>8 to 46 Mbps</td>
</tr>
<tr>
<td></td>
<td>5 MHz</td>
<td>4 to 18 Mbps (fixed/nomadic)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile WiMAX</td>
<td>5 MHz</td>
<td>Up to 15 Mbps (mobile)</td>
<td>2</td>
<td>Up to 30 Mbps</td>
</tr>
</tbody>
</table>

*Note: HSDPA = high-speed downlink packet access; 1xEV-DO = single-carrier evolution data optimized.*
two connectivity models for broadband wireless access systems, one fixed and the other mobile. Both models are dealt with in detail in this book.

Chapter 2 discusses OFDM, the access technique used by the WiMAX standards. The chapter starts by providing the background of OFDM and the mathematics associated with it. The concept and OFDM model are described in detail. The issues regarding multipath, intersymbol interference (ISI), and intercarrier interference (ICI) are dealt with separately and mathematical analysis is also provided where appropriate. The techniques for mitigation of multipath, ISI, and ICI are described. Issues associated with peak-to-average power ratio (PAPR) are also taken into account. OFDM is also used as a part of the multiple-access technique, by applying a spreading code in the frequency domain. The chapter also discusses OFDMA, which is a variation of OFDM.

Chapter 3 focuses on the fundamentals of broadband wireless access (BWA). Different considerations of BWA and its global deployment and interoperability are described in detail. Important features such as coverage, scalability, and QoS are also covered. Broadband connectivity has been available to some people for a number of years but is still limited to urban and densely populated areas. The numbers of issues that accompany BWA are also described here.

Chapter 4 discusses the WiMAX FBWA part of the IEEE 802.16 standard. The IEEE 102.16-2004 standard defines FBWA and supports both line-of-sight as well as nonline-of-sight communication between the base station and the subscriber stations. The chapter is mainly based on the IEEE 802.16-2004 standard’s specification. FBWA provides a solution to existing limitations and requirements; these needs and requirements are discussed in detail. The effect of FBWA on different market segments and its applications are also taken into account. The chapter also provides a brief yet complete overview of the technology design issues by describing in detail the MAC and PHY layers.

Chapter 5 depicts the details of MBWA, which is addressed as the second usage model of WiMAX-based IEEE 802.16e profiles. It is an amendment of IEEE 802.16-2004 and will simultaneously support both fixed and mobile wireless services, providing a very high data rate. PHY and MAC for 802.16d and 802.16e are intertwined. The enhancements
over MAC and PHY of 802.16d are summarized to provide the overview of MBWA.

References


[33] Green, E. R., “Call for Proposals for P802.11h—DFS TPC,” IEEE 802.11, IEEE 802.11-00/463r1, February 2001.


[57] Santhi, K. R., and G. S. Kumaran, “Migration to 4G: Mobile IP Based Solutions,” IEEE Advanced Int. Conf. on Telecommunications and Int. Conf. on Internet and Web Applications and Services (AICT-ICITW), 2006.
2

OFDM Systems and Issues

2.1 Introduction

In 1960, Chang [1] postulated the principle of transmitting messages simultaneously through a linear band-limited channel without ICI and ISI. Shortly after, Saltzberg [2] analyzed the performance of such a system and concluded, “The efficient parallel system needs to concentrate more on reducing cross talk between the adjacent channels rather than perfecting the individual channel itself because imperfection due to cross talk tends to dominate.” This was an important observation and was proved in later years in the case of baseband digital signal processing.

The major contribution to the OFDM technique came to fruition when Weinstein and Ebert [3] demonstrated the use of the discrete Fourier transform (DFT) to perform the baseband modulation and demodulation. The use of the DFT immensely increased the efficiency of the modulation and demodulation processing. The use of the guard space and the raised-cosine filtering solve the problems of ISI to a great extent. Although the system envisioned as such did not attain the perfect orthogonality between subcarriers in a time-dispersive channel, nonetheless it was still a major contribution to the evolution of OFDM systems.
In quest of solving the problem of orthogonality over the dispersive channel, Peled and Ruiz [4] introduced the notion of cyclic prefix (CP). They suggested filling the guard space with the cyclic extension of the OFDM symbol, which acts as if it is performing the cyclic convolution by the channel as long as the channel impulse response is shorter than the length of the CP, thus preserving the orthogonality of subcarriers. Although addition of the CP causes a reduction of the data rate, this deficiency was more than compensated by the ease of receiver implementation.

This chapter is divided into five sections. Section 2.2 discusses the basic OFDM concept. The OFDM model is introduced in Section 2.3. Section 2.4 describes time-frequency interpretation by elaborating frequency offset, timing offset, carrier phase noise, multipath issues, ISI issues, and PAPR. Finally, OFDMA is presented in Section 2.5.

2.2 OFDM Concept

The fundamental principle of the OFDM system is to decompose the high rate data stream (bandwidth = $W$) into $N$ lower rate data streams and then to transmit them simultaneously over a large number of subcarriers. A sufficiently high value of $N$ makes the individual bandwidth ($W/N$) of subcarriers narrower than the coherence bandwidth ($B_c$) of the channel. The individual subcarriers as such experience flat fading only, and this can be compensated using a trivial frequency domain single-tap equalizer. The choice of individual subcarrier is such that they are orthogonal to each other, which allows for the overlapping of subcarriers because the orthogonality ensures the separation of subcarriers at the receiver end. This approach results in a better spectral efficiency than that of FDMA systems, where no spectral overlap of carriers is allowed.

The spectral efficiency of an OFDM system is shown pictorially in Figure 2.1, which illustrates the difference between the conventional nonoverlapping multicarrier technique (such as FDMA) and the overlapping multicarrier modulation technique [such as discrete multitone (DMT), OFDM, and the like]. As shown in Figure 2.1 for illustration purpose only (in reality, the multicarrier technique is as shown in Figure 2.3), the overlapping multicarrier modulation technique can achieve superior bandwidth utilization. To realize the benefits of the overlapping
multicarrier scheme, however, requires reduction of cross talk between subcarriers, which translates into preserving orthogonality among the modulated subcarriers.

The word *orthogonal* dictates a precise mathematical relationship between frequencies of subcarriers in the OFDM-based system. In a normal frequency division multiplex system, many carriers are spaced apart in such a way that the signals can be received using conventional filters and demodulators. In such receivers, guard bands are introduced between the different carriers in the frequency domain, which results in a reduction of the spectrum efficiency. It is possible, however, to arrange the carriers in an OFDM system such that the sidebands of the individual subcarriers overlap and the signals are still received without adjacent carrier interference. The OFDM receiver can be constructed as a bank of demodulators, translating each subcarrier down to dc and then integrating over a symbol period to recover the transmitted data. If all subcarriers

![Diagram](image-url)
downconvert to frequencies that, in the time domain, have a whole number of cycles in a symbol period $T$, then the integration process results in zero ICI. These subcarriers can be made linearly independent (i.e., orthogonal) if the carrier spacing is a multiple of $1/T$, which will be proved later to be the case for OFDM-based systems.

Figure 2.2 shows the spectrum of an individual data subcarrier, and Figure 2.3 depicts the spectrum of an OFDM symbol. The OFDM signal multiplexes in the individual spectra with frequency spacing equal to the transmission bandwidth of each subcarrier as shown in Figure 2.2. Figure 2.3 shows that at the center frequency of each subcarrier, there is no cross talk from other channels. Therefore, if a receiver performs correlation with the center frequency of each subcarrier, it can recover the transmitted data without any cross talk. In addition, using the DFT-based multicarrier technique, frequency division multiplexing is achieved by baseband processing rather than the costlier bandpass processing.

The orthogonality of subcarriers is maintained even in the time-dispersive channel by adding the CP. The CP is the last part of an OFDM symbol, which is prefixed at the start of the transmitted OFDM symbol, which aids in mitigating the ICI-related degradation.

![Figure 2.2 Spectra of OFDM individual subcarrier.](image-url)
transmitter and receiver block diagrams of the OFDM system are shown in Figures 2.4 and 2.5, respectively.

2.3 OFDM Model

The OFDM-based communication systems transmit multiple data symbols simultaneously using orthogonal subcarriers, as shown in Figure 2.6. A guard interval is added to mitigate the ISI, which is not shown in the figure for simplicity. The data symbols \( d_{n,k} \) are first assembled into a group of block size \( N \) and then modulated with complex exponential waveform \( \{\phi_k(t)\} \) as shown in (2.1). After modulation they are transmitted simultaneously as transmitter data stream. The modulator as shown in Figure 2.6 can be easily implemented using an inverse fast Fourier transform (IFFT) block described by (2.1):

\[
x(t) = \sum_{n=-\infty}^{\infty} \left[ \sum_{k=0}^{N-1} d_{n,k} \phi_k(t - nT_d) \right]
\]

(2.1)

\[\text{Figure 2.3} \quad \text{Spectra of OFDM symbol.}\]
where

$$\phi_k(t) = \begin{cases} e^{j2\pi f_k t} & t \in [0, T_d] \\ 0 & \text{otherwise} \end{cases}$$

and

$$f_k = f_0 + \frac{k}{T_d}, k = 0, \ldots, N - 1$$
\( d_{n,k} \) = symbol transmitted during \( n \)th timing interval using \( k \)th subcarrier

\( T_d \) = symbol duration

\( N \) = number of OFDM subcarriers

\( f_k \) = \( k \)th subcarrier frequency, with \( f_0 \) being the lowest

The simplified block diagram of an OFDM demodulator is shown in Figure 2.7. The demodulation process is based on the orthogonality of subcarriers \( \{ \phi_k(\tau) \} \), namely,

\[
\int_{\mathbb{R}} \phi_k(t) \phi^*_l(t) dt = T_d \delta(k-l) = \begin{cases} T_0 & k = 1 \\ 0 & \text{otherwise} \end{cases}
\]

Therefore, a demodulator can be implemented digitally by exploiting the orthogonality relationship of subcarriers, yielding in a simple IFFT/FFT modulation/demodulation of the OFDM signal:

\[
d_{n,k} = \frac{1}{T_d} \int_{nT_d}^{(n+1)T_d} x(t) \phi_k^*(t) dt \quad (2.2)
\]
Equation (2.2) can be implemented using the FFT block as shown in Figure 2.7.

2.4 Time-Frequency Interpretation

The specified OFDM model can also be described as a two-dimensional lattice representation in time and frequency plane, and this property can be exploited to compensate for channel-related impairment issues. Looking into modulator implementation of Figure 2.6, a model can be devised to represent an OFDM transmitted signal as shown in (2.3). In addition, this characteristic may also be exploited in pulse shaping of the transmitted signal to combat ISI and multipath delay spread. This interpretation is detailed in Figure 2.8.

\[ x(t) = \sum_{k,l} d_{k,l} \phi_{k,l}(t) \]  

(2.3)
where the operand $\phi_{k,l}(t)$ represents the time- and frequency-displaced replica of basis function $\phi(t)$ by $k\tau_0$ and $l\nu_0$ in two-dimensional time and frequency lattices [5, 6], respectively, as shown in Figure 2.8. Mathematically, it can be shown that operand $\phi_{k,l}(t)$ is related to the basis function as follows:

$$\phi_{k,l}(t) = \phi(t - k\tau_0)e^{j2\pi l\nu_0 t} \quad (2.4)$$

Usually, the basis function $\phi(t)$ is chosen as a rectangular pulse of amplitude $1/\sqrt{\tau_0}$ and duration $\tau_0$ and the frequency separation is set at $\nu_0 = 1/\tau_0$. Each transmitted signal in the lattice structure experiences the same flat fading during reception, which simplifies the channel estimation and equalization process. The channel attenuations are estimated by correlating the received symbols with symbols at the lattice points known a priori. This technique is frequently used in OFDM-based communication systems to provide the pilot-assisted channel estimation.

Figure 2.8 Two-dimensional lattice in time-frequency domain.
2.4.1 Impairment Issues in OFDM Systems

Communication systems based on the OFDM technique have some disadvantages as well due to the environment in which they operate. To build upon the inherent spectral efficiency and simpler transceiver design factors, the impairment issues must be dealt with to garner potential benefits. In a communication system, a receiver needs to synchronize with a transmitter in frequency, phase, and time (or frame/slot/packet boundary) to faithfully reproduce the transmitted signal. This is not a trivial task, particularly in a mobile environment, where operating conditions and surroundings vary so frequently. For example, when a mobile is turned on, it may not have any knowledge of its surroundings, and it must take a few steps (based upon agreed protocol/standards) to establish communication with the base station/access point. This basic process in communication jargon is known as synchronization and acquisition. The task of synchronization and acquisition by itself is complex issue, but impairments make it even harder. Impairment issues are discussed in subsequent sections in detail.

2.4.2 Frequency Offset

Frequency offset in an OFDM system is introduced from two sources: mismatch between transmit and receive sampling clocks and misalignment between the reference frequency of transmit and receive stations. Both impairments and their effects on performance are analyzed.

2.4.2.1 Impairment Due to Sampling Clock Mismatch

The sampling epoch of the received signal is determined by the receiver analog-to-digital (A/D) sampling clock, which will seldom have the exact period matching the transmit sampling clock, causing the receiver sampling instants slowly to drift relative to the transmitter. Many authors [7–10] have analyzed the effect of the sampling clock drift on system performance.

The sampling clock error manifests in two ways: First, a slow variation in the sampling time instant causes rotation of subcarriers and subsequent loss of the signal-to-noise ration (SNR) due to ICI, and second, it causes the loss of orthogonality among subcarriers due to energy spread
among adjacent subcarriers. Let us define the normalized sampling error as

\[ t_\Delta = \frac{T' - T}{T} \]

where \( T \) and \( T' \) are transmit and receive sampling periods, respectively. Then, the overall effect, after DFT, on the received subcarriers \( R_{l,k} \) can be shown [11] as

\[ R_{l,k} = \exp \left[ j2\pi t_\Delta l \frac{T_\text{t}}{T_\text{u}} \right] X_{l,k} \sin \left( \pi t_\Delta \right) H_{l,k} + W_{l,k} + N_{t_\Delta} (l,k) \]

where \( l \) is the OFDM symbol index, \( k \) is the subcarrier index, \( T_\text{t} \) and \( T_\text{u} \) are the duration of the total and the useful duration of the symbol duration, respectively, \( W_{l,k} \) is additive white Gaussian noise, and the final term, \( N_{t_\Delta} \), is the additional interference due to the sampling frequency offset. The power of the final term is approximated [11] by

\[ P_{t_\Delta} \approx \frac{\pi^2}{3} (kt_\Delta)^2 \]

Hence, the degradation grows as the square of the product of offset \( t_\Delta \) and the subcarrier index \( k \). This means that the outermost subcarriers are most severely affected. The degradation can also be expressed as SNR loss in decibels by the following expression [10]:

\[ D_{\text{v}} \approx 10 \log_{10} \left[ 1 + \frac{\pi^2}{3} \frac{E_{\text{v}}}{N_0} (kt_\Delta)^2 \right] \]

The OFDM systems with a small number of subcarriers and quite small sampling error \( t_\Delta \) such that \( kt_\Delta << 1 \), the degradation caused by the sampling frequency error can be ignored. The most significant issue is the different value of rotation experienced by the different subcarriers based on the subcarrier index \( k \) and symbol index \( l \); this is evident from the term
\{\exp( j2\pi kt \Delta T_s / T_s)\}. Hence, the rotation angle is largest for the outermost subcarrier and increases as a function of symbol index \(l\). The term \(t_\Delta\) is controlled by the timing loop and usually is very small, but as \(l\) increases, the rotation eventually becomes so large that the correct demodulation is no longer possible, and this necessitates the tracking of the sampling frequency in the OFDM receiver. The effect of sampling offset on the SNR degradation is shown in Figure 2.9 as a function of the number of subcarriers. From Figure 2.9, it is obvious that as the number of subcarriers in the OFDM symbol increases, so does the degradation; that is, the OFDM system with a large number of subcarriers is very sensitive to the sampling offsets.

### 2.4.2.2 Carrier Frequency Offset

The OFDM systems are more sensitive to frequency error than are the single-carrier frequency systems. The frequency offset is produced at the receiver because of the local oscillator instability and variability of...
operating conditions at transmitter and receiver, Doppler shifts caused by the relative motion between the transmitter and receiver, or the phase noise introduced by other channel impairments. The degradation is caused by the reduction in the signal amplitude of the desired subcarrier and the ICI from the neighboring subcarriers, as shown in Figure 2.10. The amplitude loss occurs because the desired subcarrier is no longer sampled at the peak of the equivalent sinc function of the DFT. Adjacent subcarriers cause interference because they are not sampled at their zero crossings. The overall effect of carrier frequency offset effect on SNR is analyzed by Pollet et al. [10] and for relatively small frequency error; the degradation in decibels is approximated by

\[
SNR_{\text{loss}} (dB) \approx \frac{10}{3 \ln 10} \left( \pi T f_{\Delta} \right)^2 \frac{E_s}{N_0}
\]

where \( f_{\Delta} \) is the frequency offset and is a function of the subcarrier spacing and \( T \) is the sampling period. The performance of the system depends on modulation type. Naturally, the modulation scheme with large constellation points is more susceptible to frequency offset than a small constellation modulation scheme. This is why the SNR requirements for the

**Figure 2.10** Loss of orthogonality due to sampling offset.
higher constellation modulation scheme are much higher for the same bit error rate (BER) performance.

It is assumed that two subcarriers of an OFDM system can be represented using the orthogonal frequency tones at the output of the A/D converter at baseband as

\[ \phi_k(t) = e^{j2\pi ft/T} \]

and

\[ \phi_{k+m}(t) = e^{j2\pi (k+m)t/T} \]

where \( T \) is the sampling period. Let us also assume that due to the frequency drift, the receive station has a frequency offset of \( \delta \) from the \( k \)th tone to the \((k+m)\)th tone; that is,

\[ \phi_{k+m}^\delta(t) = e^{j2\pi (k+m+\delta)t/T} \]

Due to this frequency offset there is an interference between the \( k \)th and \((k+m)\)th channels, given by [12]

\[ I_m(\delta) = \int_0^T e^{j2\pi ft/T} e^{-j(k+m+\delta)2\pi t/T} dt = \frac{T(1 - e^{-j2\pi\delta})}{j2\pi(m + \delta)} \]

and

\[ |I_m(\delta)| = \frac{T|\sin(\pi\delta)|}{\pi|m + \delta|} \]

The aggregate loss (power) due to this interference from all \( N \) subcarriers can be approximated as follows:

\[ \sum_{m} I_m^2(\delta) = (T\delta)^2 \sum_{m=1}^{N-1} \frac{1}{m^2} \approx (T\delta)^2 \frac{23}{14} \quad \text{for} \ N >> 1(N > 5 \text{ enough}) \]
The ICI due to loss of orthogonality caused by the frequency offset is shown in Figure 2.11.

### 2.4.3 Timing Offset

The symbol timing is very important to the receiver for correct demodulation and decoding of the incoming data sequence. The timing synchronization is possible with the introduction of the training sequences in addition to the data symbols in the OFDM systems. The receiver may still not be able to recover the complete timing reference of the transmitted symbol because of the channel impairments that are causing the timing offset between the transmitter and the receiver. A time offset gives rise to the phase rotation of the subcarriers. The effect of the timing offset is negated with the use of a CP. If the channel response due to the timing offset is limited within the length of the CP, the orthogonality across the subcarriers is maintained. The timing offset can be represented by a phase

![Figure 2.11](image_url)  
**Figure 2.11** Total ICI due to loss of orthogonality caused by frequency offset.
shift introduced by the channel and can be estimated from the computation of the channel impulse response. When the receiver is not time synchronized to the incoming data stream, the SNR of the received symbol is degraded. The degradation $\xi$ can be quantized in terms of the output SNR with respect to an optimal sampling time $T_{\text{optimal}}$:

$$\xi = \frac{\Lambda(\tau)}{\Lambda(0)}$$

where $\Lambda(.)$ is the autocorrelation function and $\tau$ is the delay between the optimal sampling instant $T_{\text{optimal}}$ and the received symbol time. The parameter $\tau$ is a random variable since it is estimated in the presence of noise, and it is usually referred to as the \textit{timing jitter}. The two special cases of interest, baseband time-limited signals and band-limited signals, with the normalized autocorrelation functions are \cite{12}:

$$\Lambda(\tau) = \left[ 1 - \frac{|\tau|}{T_{\text{symbol}}} \right]$$

$$\Lambda(\tau) = \frac{1}{N} \left[ \frac{\sin(\pi NW\tau)}{\sin(\pi W\tau)} \right]$$

where $W$ is the bandwidth of the band-limited signal. The single-carrier system is best described as the band-limited signal, whereas the OFDM (multicarrier) system is best described as the time-limited signal. For single-carrier systems, the timing jitter manifests as a noisy phase reference of the bandpass signal. In the case of OFDM systems, pilot tones are transmitted along with the data-bearing carrier to estimate residual phase errors.

2.4.3.1 Loss of Orthogonality Due to Timing Offset

Paez-Borrallo \cite{12} has analyzed the loss of orthogonality due to time shift and the result of the analysis is shown here to quantize its effect on ICI and the resulting loss in orthogonality. Let us denote the timing offset
between the two consecutive symbols as $\tau$. The received stream at the receiver can then be expressed as follows:

$$X_i = c_0 \int_{-T/2}^{-T/2+\tau} \phi_k(t)\phi^*_l(t-\tau)dt + c_1 \int_{-T/2+\tau}^{T/2} \phi_k(t)\phi^*_l(t-\tau)dt$$

where

$$\phi_k(t) = e^{j2\pi kt/T}$$

Substituting $m = k - l$, then the magnitude of the received symbol can be represented as

$$|X_i| = \begin{cases} 
2T \left| \frac{\sin m\pi \tau}{m\pi} \right|, & c_0 \neq c_1 \\
0, & c_0 = c_1
\end{cases}$$

This can be further simplified for simple analysis if $\tau < T$:

$$\frac{|X_i|}{T} \approx \frac{2m\pi \tau}{m\pi} = 2\frac{\tau}{T}$$

This is independent of $m$ for $\tau \ll T$.

We can compute the average interfering power as

$$E\left[\frac{|x_i|^2}{T^2}\right] = 4\left(\frac{\tau}{T}\right)^2 \frac{1}{2} + 0 \cdot \frac{1}{2} = 2\left(\frac{\tau}{T}\right)^2$$

The ICI loss in decibels is computed as follows:
2.4.4 Carrier Phase Noise

The carrier phase impairment is induced due to the imperfection in the transmitter and the receiver oscillators. The phase rotation could be the result of either the timing error or the carrier phase offset [13] for a frequency-selective channel. The analysis of the system performance due to carrier phase noise has been performed by Pollet et al. [14]. The carrier phase noise was modeled as the Wiener process $\theta(t)$ with $E[\theta(t)] = 0$ and $E[(\theta(t_0 + t) - \theta(t_0))^2] = 4\pi \beta |t|$, where $\beta$ (in hertz) denotes the single-sided linewidth of the Lorentzian power spectral density of the free running carrier generator. Degradation in the SNR, that is, the increase in the SNR needed to compensate for the error, can be approximated by

$$D(dB) \approx \frac{11}{6 \ln 10} \left( \frac{4\pi N \beta}{W} \right) \frac{E_s}{N_0}$$

where $W$ is the bandwidth and $E_s/N_0$ is the SNR of the symbol. Note that the degradation increases with the increase in the number of subcarriers.

2.4.5 Multipath Issues

In mobile wireless communication, a receiver collects transmitted signals through various paths, some arriving directly, some from neighboring objects because of reflection, and some even because of diffraction from nearby obstacles. These various paths arriving at the receiver may interfere with each other and cause distortion to the information-bearing signal. The impairments caused by multipaths include delay spread, loss of signal strength, and widening of the frequency spectrum. The random nature of the time variation of the channel may be modeled as a narrowband statistical process [15]. For a large number of signal reflections impinging on the receive antenna, the distribution of the arriving signal can be modeled as a complex-valued Gaussian random process.

$$\text{ICI}_{dB} = 10 \log_{10} \left[ 2 \left( \frac{\tau}{T} \right)^2 \right]$$
based on central limit theory. The envelope of the received signal can be decomposed into quickly varying fluctuations superimposed onto slowly varying ones. When the average amplitude of the envelope suffers a drastic degradation from the interfering phase from the individual path, the signal is regarded as fading. *Multipath* is a term used to describe the reception of multiple copies of the information-bearing signal by the receive antenna. Such a channel can be described statistically and can be characterized by the channel correlation function. The baseband-transmitted signal can be accurately modeled as a narrowband process as follows:

\[ S(t) = x(t)e^{-2\pi f_D t} \]

Assuming the multipath propagation as Gaussian scatterers, the channel can be characterized by time-varying propagation delays, loss factors, and Doppler shifts. The time-varying impulse response of the channel is given by [15]

\[ c(\tau_n, t) = \sum_n \alpha_n(\tau_n, t)e^{-j2\pi f_D \tau_n(t)} \delta[t - \tau_n(t)] \]

where

- \( c(\tau_n, t) = \) response of the channel at time \( t \) due to an impulse applied at time \( t - \tau_n(t) \)
- \( \alpha_n(t) = \) attenuation factor for the signal received on the \( n \)th path
- \( \tau_n(t) = \) propagation delay for the \( n \)th path
- \( f_D = \) Doppler shift for the signal received on the \( n \)th path

The Doppler shift is introduced because of the relative motion between the transmitter and the receiver and can be expressed as

\[ f_D = \frac{v \cos(\theta_n)}{\lambda} \]

where \( v \) is the relative velocity between transmitter and receiver, \( \lambda \) is the wavelength of the carrier, and \( \theta_n \) is the phase angle between the transmitter and the receiver.
The output of the transmitted signal propagating through the channel is given as

\[ z(t) = c(\tau_n, t) * s(t) \]

\[ z(t) = \sum_n \alpha_n [\tau_n(t)] e^{-j2\pi(f_c+f_{D_n})\tau_n(t)} x(t-\tau(t)) e^{-j2\pi f_{z,t}} \]

where

\[ \delta(t-\tau_n(t)) * x(t) = x(t-\tau_n(t)) \]

\[ \delta(t-\tau_n(t)) * e^{-j2\pi f_{z,t}} = e^{-j2\pi f_{z,(t-\tau_n(t))}} \]

\[ \beta_n = \alpha_n [\tau_n(t)] e^{-j2\pi(f_c+f_{D_n})\tau_n(t)} \]

Alternatively, \( z(t) \) can be written as

\[ z(t) = \sum_n \beta_n x(t-\tau_n(t)) e^{-j2\pi f_{z,t}} \]

\( \beta_n \) is Gaussian random process. The envelope of the channel response function \( c(\tau_n, t) \) has a Rayleigh distribution function because the channel response is the ensemble of the Gaussian random process. The density function of a Rayleigh faded channel is given by

\[ f_z(z) = \frac{z}{\alpha^2} \exp \left[ -\left( \frac{z^2}{2\sigma^2} \right) \right] \]

A channel without a direct line-of-sight (LOS) path is typically termed a Rayleigh fading channel. The channel with a direct LOS path to the receiver is generally characterized by a Rician density function and is given by

\[ f_z(z) = \frac{z}{\sigma^2} I_0 \left( \frac{2\eta}{\sigma^2} \right) \exp \left[ -\left( \frac{z^2 + \eta^2}{2\sigma^2} \right) \right] \]
where $I_0$ is the modified Bessel function of the zeroth order and $\eta$ and $\sigma^2$ are the mean and the variance of the direct LOS path, respectively. Proakis [15] has shown that the autocorrelation function of $c(\tau, t)$ is as follows:

$$\Lambda_c(\tau, \Delta t) = E[c(\tau, t)c^*(\tau, t + \Delta t)]$$

In addition, it can be measured by transmitting very narrow pulses and cross correlating the received signal with a conjugate delayed version of itself. The average power of the channel can be found by setting the $\Delta t = 0$; that is, $\Lambda_c(\tau, 0) = \Lambda_c(\tau)$. The quantity is known as the power delay profile or the multipath intensity profile. The range of values of $\tau$ over which the $\Lambda_c(\tau)$ is essentially nonzero is called the multipath delay spread of the channel, denoted by $\tau_m$. The reciprocal of the multipath delay spread is a measure of the coherence bandwidth of the channel; that is,

$$B_m \approx \frac{1}{\tau_m}$$

The coherence bandwidth of a channel plays a prominent role in communication systems. If the desired signal bandwidth of a communication system is small compared to the coherence bandwidth of the channel, the system experiences flat fading (or frequency nonselective fading), and this eases signal processing requirements of the receiver system because the flat fading can be overcome by adding the extra margin in the system link budget. Conversely, if the desired signal bandwidth is large compare to the coherence bandwidth of the channel, the system experiences the frequency-selective fading, and this impairs the ability of the receiver to make the correct decision about the desired signal. The channels, whose statistics remain constant over the several symbol intervals, are considered slow fading channels compared to the channels whose statistics change rapidly during a symbol interval. In general, the indoor wireless channels are characterized by slow frequency-selective fading.
2.4.6 ISI Issues

The output of the modulator as shown in (2.1) is repeated here for reference:

\[ x(t) = \sum_{n=-\infty}^{\infty} \left[ \sum_{k=0}^{N-1} d_{n,k} \phi_k (t - nT_d) \right] \]

Equation (2.1) can be rewritten in discrete form for the \( n \)th OFDM symbol as follows:

\[ x_n(k) = \sum_{k=0}^{N-1} d_{n,k} \phi_k (t - nT_d) \]

where

\[ \phi_k(t) = e^{j2\pi \frac{kt}{T}} \]

For the \( n \)th block of channel symbols \( d_{nP} \), \( d_{nP+1} \), \ldots, \( d_{nP+P-1} \), the \( i \)th subcarrier signal can be expressed as follows:

\[ x_n^i(k) = \sum_{k=0}^{N-1} d_{nP+i,k} \exp \left( j \frac{2\pi}{N} l_i k \right) \text{ for } i = 0, 1, 2 \ldots P-1 \]

where \( P \) is the number of subcarriers and \( l_i \) is the index of the time complex exponential of length \( N \), that is, \( 0 \leq l_i \leq N-1 \).

These are summed to form the \( n \)th OFDM symbol, given as

\[ x_n(k) \equiv \sum_{i=0}^{P-1} x_n^i = \sum_{i=0}^{P-1} d_{nP+i} \exp \left( j \frac{2\pi}{N} l_i k \right) \quad (2.5) \]

The transmitted signal at the output of the digital-to-analog (D/A) converter can be represented as follows:
where \( L \) is the length of data symbol larger than \( N \) (the number of subchannels). Since the sequence length \( L \) is longer than \( N \), only a subset of the OFDM received symbols is needed at the receiver to demodulate the subcarriers. The additional \( Q = L - N \) symbols are not needed, and we will later show that it could be used as a guard interval to add the CP to mitigate the ICI problem in OFDM systems. In multipath and additive noise environment, the received OFDM signal is given by [16]

\[
 r_n(k) = \sum_{i=0}^{L-1} x_n(i) h(k-i) + \sum_{i=0}^{L-1} x_{n-1}(i) h(k+L-i) + v_n(k) \quad (2.6)
\]

The first term in (2.6) represents the desired information-bearing signal in a multipath environment, whereas the second part represents the interference from the preceding symbols. The length of the multipath channel, \( L_h \), is assumed to be much smaller than that of the OFDM symbol, \( L \). This assumption, plus the assumption about the causality of the channel, implies that the ISI is only from the preceding symbol. If we assume that the multipath channel is as long as the guard interval, that is, \( L_h \leq Q \), then the received signal in (2.6) can be divided into two time intervals. The first time interval contains the desired symbol plus the ISI from the preceding symbol. The second interval contains only the desired information-bearing symbol. Mathematically, it can be written as follows:

\[
 r_n(k) = \begin{cases} 
 \sum_{i=0}^{L-1} x_n(i) h(k-i) + \sum_{i=0}^{L-1} x_{n-1}(i) h(k+L-i) + v_n(k) & 0 \leq k \leq Q - 1 \\
 \sum_{i=0}^{L-1} x_n(i) h(k-i) + v_n(k) & Q \leq k \leq L - 1 
\end{cases} \quad (2.7)
\]
2.4.6.1 Performance Degradation Due to ISI

ISI is the effect of the time dispersion of the information-bearing pulses, which causes symbols to spread out so that they disperse energy into the adjacent symbol slots. The Nyquist criterion spells out clearly the way to achieve the ISI-free transmission in a band-limited environment. However, to achieve the ISI-free transmission, the channel must be equalized. The complexity of the equalizer depends on the severity of the channel distortion. Degradation occurs due to the receiver’s inability to perfectly equalize the channel and from the noise enhancement of the modified receiver structure in the process. The effect of smearing of energy into the neighboring symbol slots is represented by the second term in (2.7). The effect of the ISI in the time domain and the frequency domain is shown in Figures 2.12 and 2.13, respectively. The rms delay spread imposes the limit on the achievable data rate [17], which is shown in Table 2.1. Figure 2.13 shows that if the signal bandwidth \((BW = 1/Symbol\ period)\) is smaller than the coherence bandwidth of the channel, the signal incurs the flat fading, which can be mitigated by using a larger dynamic range, but if the signal bandwidth is larger than the coherence bandwidth of the channel, then signal goes through frequency-selective fading.

![Figure 2.12](image_url)  
**Figure 2.12** Time domain interpretation of delay spread.
One of the most important properties of the OFDM system is its robustness against multipath delay spread. This is achieved by using a long symbol period, which minimizes the ISI. The level of robustness against the multipath delay spread can be increased even further by addition of the guard period between transmitted symbols. The guard period allows enough time for multipath signals from the previous symbol to die away before the information from the current symbol is gathered. The most effective use of the guard period is the cyclic extension of the symbol. As shown in Figure 2.14, the end part of the symbol is appended at the start of the symbol inside the guard period (GP) to effectively maintain the orthogonality among subcarriers. Using the cyclically extended symbol, the samples required for performing the FFT (to decode the symbol) can
be obtained anywhere over the length of the symbol. This provides multipath immunity as well as symbol time synchronization tolerance.

As long as the multipath delays stay within the duration of the guard period, there is strictly no limitation regarding the signal level of the multipath—it may even exceed the signal level of the shorter path. The signal energy from all paths just adds at the input of the receiver, and since the FFT is energy conservative, the total available power from all multipaths feeds the decoder. When the delay spread is larger then the guard interval, it causes the ISI. However, if the delayed path energies are sufficiently small, they may not cause any significant problems. This is true most of the time, since path delays longer than the guard period would have been reflected off very distant objects and thus would have been diminished quite a lot before impinging on the receive antenna.

2.4.6.3 ICI

The ICI in the OFDM system is introduced due to the loss of the orthogonality of subcarriers. The loss of orthogonality may be due to the frequency offset, the phase mismatch, or excessive multipath dispersion. The effect of this is illustrated in Figure 2.15, where subcarrier 1 is aligned to the symbol integration boundary, whereas subcarrier 2 is delayed. In this case, the receiver will encounter interference because the number of cycles for the FFT duration is not an exact multiple of the cycles of subcarrier 2. Fortunately, the ICI can be mitigated with intelligent exploitation of the guard period, which is required to combat the ISI. The frequency offset between the transmitter and the receiver generates residual frequency error in the received signal. The effect of the frequency offset can be analyzed analytically from expanding (2.7) as
\[
    r_n(k) = \begin{cases}
    \sum_{i=0}^{L-1} x_n(i) b(k-i) + \sum_{i=0}^{L-1} x_{n-1}(i) b(k + L - i) & 0 \leq k \leq Q - 1 \\
    \sum_{i=0}^{L-1} x_n(i) b(k-i) + v_n(k) & Q \leq k \leq L - 1
    \end{cases}
\]  

(2.8)

At the receiver the guard period is discarded and the remaining signal is defined for \( k = 0, 1, \ldots, N-1 \) as

\[
    r_n'(k) \equiv r_n(k + Q)
\]  

(2.9)

Substituting (2.5) into (2.9) and simplifying yields the following:

\[
    r_n'(k) = \sum_{\alpha} b(\alpha) \sum_i d_{np+i} \exp\left( j \frac{2\pi}{N} l_i (k + Q - \alpha) \right) + v_n(k)
\]

or

\[
    r_n'(k) = \sum_i d_{np+i} \exp\left( j \frac{2\pi}{N} l_i k \right) \exp\left( j \frac{2\pi}{N} l_i Q \right) \sum_{\alpha} b(\alpha) \exp\left( - j \frac{2\pi}{N} l_i \alpha \right) + v_n(k)
\]  

(2.10)
Equation (2.10) can be written in simplified form as

\[ r_n(k) = \sum_i d_{nP+i} \phi_i H(l_i) \exp\left( j \frac{2\pi}{N} l_i k \right) + v_n(k) \quad (2.11) \]

where the prime is dropped without loss of generality and

\[ \phi_i = \exp\left( j \frac{2\pi}{N} l_i Q \right) \sim \text{Constant phase multiplier} \]

\[ H(l_i) = \sum_\alpha h(\alpha) \exp\left( -j \frac{2\pi}{N} l_i \alpha \right) \sim \text{Fourier transform of } h(n) \]

The received signal with frequency offset \( \Delta f \) can be plugged into (2.11) to yield the following:

\[ r_n^{\text{off}}(k) \equiv r_n(k) \exp( j 2\pi \Delta f k ) = \sum_i d_{nP+i} \phi_i H(l_i) \cdot \exp\left[ j \frac{2\pi}{N} k(l_i + \Delta f N) \right] + V_n(k) \quad (2.12) \]

2.4.6.4 Performance Degradation Due to ICI

It can be shown from (2.12) that the frequency offset induces the ICI as well as the loss of orthogonality between subcarriers. In other words, the symbol estimate becomes

\[ \hat{d}_{nP+i} = G_i \left\{ \left[ H(l_i) d_{nP+i} I_{\Delta f} (0) \right] + \sum_{j=0}^{p-1} H(l_m) d_{nP+i} I_{\Delta f} (l_m - l_i) \right\} + V_n(I_i) \quad (2.13) \]

where the ICI term is
\[ I_{\Delta f}(l_m - l_i) = \exp \left[ j \frac{2\pi}{N} k(l_m - l_i + \Delta f N) \right] \]  \hspace{1cm} (2.14)

Starting from (2.14), it can be shown that the SNR degradation due to small frequency offset is approximately [7]

\[ SNR_{\text{loss}} (dB) \approx \frac{10}{3 \ln 10} \left( \pi \Delta f NT_s \right)^2 \frac{E_s}{N_0} \]  \hspace{1cm} (2.15)

where \( E/N_0 \) is the SNR in the absence of the frequency offset.

2.4.6.5 Mitigation of ICI

The ISI is eliminated by introducing a guard period for each OFDM symbol. The guard period is chosen larger than the expected delay spread such that multipath components from one symbol do not interfere with adjacent symbols. This guard period could be no signal at all, but the problem of ICI would still exist. To eliminate the ICI, the OFDM symbol is cyclically extended in the guard period as shown in Figure 2.16. This ensures that the delayed replicas of the OFDM symbols due to multipath will always have the integer number of cycles within the FFT interval, as long as the delay is smaller than the guard period. As a result, multipath signals with delays smaller than the guard period do not cause ICI. The typical cyclic usage of extension as a guard period is shown in Figure 2.17.

![Figure 2.16 OFDM symbol with cyclic extension.](image-url)
Mathematically, it can be shown that the cyclic extension of the OFDM symbol in the guard period makes the OFDM symbol appear to be periodic at the receiver end even though there might be a delay because of the multipath environment.

In an OFDM system the \( N \) complex-valued frequency domain symbols \( X(n) \), \( 0 < n < N-1 \), modulate \( N \) orthogonal carriers using the inverse DFT (IDFT)–producing time-domain signal as follows:

\[
x(k) = \sum_{n=0}^{N-1} X(n) \exp\left(j2\pi \frac{n}{N}\right) = \text{IDFT}[X(n)]
\] (2.16)

As is well known, the basis functions of the IDFT are orthogonal. By adding a CP, the transmitted signal appears periodic:

\[
s(k) = \begin{cases} 
x(k + N) & 0 \leq k < Q \\
x(k) & Q \leq k < L 
\end{cases}
\]

where \( Q \) is the length of the guard period.

The received signal now can be written as

\[
y(k) = s(k) * b(k) + w(k) \quad 0 \leq k < L
\] (2.17)

where the asterisk denotes convolution.

If the CP added is longer than the impulse response of the channel, the linear convolution with the channel will appear as a circular convolution from the receiver’s point of view. This is shown next for any subcarrier \( l \), \( 0 \leq l < L \):
\[ Y(n) = DFT(y(k)) = DFT\left(\text{IDFT}\left(X(n)\right) \otimes h(k) + w(k)\right) = \]
\[ X(n)DFT(h(k)) + DFT(w(k)) = X(n)H(n) + W(n), \quad (2.18) \]
\[ 0 \leq k < N \]

where the symbol \( \otimes \) denotes circular convolution and \( W(n) = \text{DFT}(w(k)) \). Examining (2.18) shows that there is no interference between subcarriers; that is, the ICI is zero. Hence, by adding the CP, the orthogonality is maintained through transmission. The obvious drawback of using the CP is that the amount of data that has to be transmitted increases, thus reducing the usable throughput.

### 2.4.7 PAPR

Another challenge that OFDM systems face is the accommodation of the large dynamic range of a signal. This large dynamic range, often described in terms of PAPR, means that the OFDM signal has a large variation between the average signal power and the maximum signal power.

A large dynamic range is inherent to multicarrier modulations since each subcarrier is essentially independent. As a result, subcarriers can add constructively or destructively, which may contribute to large variation in signal power. In other words, it is possible for the data sequence to align all subcarriers constructively and accrue to a very large signal. It is also possible for the data sequence to make all subcarriers align destructively and diminish to a very small signal. This large variation creates problems for transmitter and receiver design, requiring both to accommodate a large range of signal power with minimum distortion.

The large dynamic range of the OFDM systems presents, in particular, a challenge for the power amplifier (PA) and the low-noise amplifier (LNA) design. The large output drives the PA to nonlinear regions (i.e., near saturation), which causes distortion. To minimize the amount of distortion and to reduce the amount of out-of-band energy radiation by the transmitter, the OFDM and other modulations alike need to ensure that the operation of a PA is limited as much as possible in the linear amplification region. With inherently large dynamic range, this means that the
OFDM must keep its average power well below the nonlinear region of the PA to accommodate the signal power fluctuations.

However, lowering the average power hurts the efficiency and subsequently the range since it corresponds to a lower output power for the majority of the signal in order to accommodate the infrequent peaks. As a result, the OFDM designers must make careful trade-offs between allowable distortion and output power. That is, they must choose an average input level that generates sufficient output power and yet does not introduce too much interference or violate any spectral constraints.

To examine this trade-off further, consider the IEEE 802.11a version of OFDM system that uses 52 subcarriers. In theory, all 52 subcarriers could add constructively, and this would yield a peak power of $20 \times \log(52) = 34.4$ dB above the average power. However, this is an extremely rare event.

Instead, most simulations show that for real PAs, accommodating a peak that is 3 to 6 dB above average is sufficient. The exact value is highly dependent on the PA characteristics and other distortions in the transmitter chain. In other words, the distortions caused by peaks above this range are infrequent enough to allow for low average error rates.

2.4.7.1 Mitigation of PAPR

A simple method of handling PAPR is to limit the peak signals either by clipping or by replacing peaks with a smooth but lower-amplitude pulse. Since this modifies the signal artificially, it does increase the distortion to some degree. However, if it is done in a controlled fashion, it generally limits the PA-induced distortion. As a result, it can in many cases improve the overall output power efficiency.

For packet-based networks the receiver can request a retransmission of any packet with error. A simple but effective technique may be to rely on a scramble sequence to control PAPR on retransmission. In other words, the data is scrambled prior to modulating the subcarriers for retransmission. This alone does not prevent large peaks, and there may still be occasions when the transmitter introduces significant distortion due to a large peak power in the packet. However, when the distortion is severe, the receiver will not correctly decode the packet and will request a retransmission.
When the data is retransmitted, however, the scramble sequence is changed. If the first scramble sequence caused a large PAPR, the second sequence is extremely unlikely to do the same despite the fact that it contains the same data sequence. Since IEEE 802.11a/g/n networks use packet retransmissions already, this technique is used to mitigate some of the problems with PAPR. The downside to this technique is that it does impact the network throughput because some of the data sequences must be transmitted more than once.

To minimize the OFDM system performance degradation due to PAPR, several techniques has been explored, each with varying degrees of complexity and performance enhancements. These schemes can be divided into three general categories:

- Signal distortion techniques:
  - Signal clipping;
  - Peak windowing;
  - Peak cancellation;
- Coding technique;
- Symbol-scrambling technique.

**Signal Distortion Technique**

**Signal Clipping.** The simplest way to mitigate the PAPR problem is to limit (clip) the signal such that the peak level of the signal is always below the desired maximum level [18]. Figure 2.18 shows a pictorial view of clipping.

However, this causes out-of-band radiation and signal distortion. The effect of this clipping is analogous to the rectangular windowing of the sample, which is equivalent to the spectrum of the desired signal being convolved by the sinc function (spectrum of the rectangular window), causing spectrum regrowth in the sidebands, thus causing interference to the neighboring channels.

**Peak Windowing.** Simple clipping gives rise to the spectral growth in sidebands. Therefore, to tame the spectral growth in adjacent bands, other
windowing functions with narrow bandwidth (such as Gaussian, Kaiser, Hamming, and root raised cosine) have been applied and examined, the result of which is shown in Figure 2.19.

Peak Cancellation Technique. The goal of the signal distortion techniques is to reduce the amplitude of the data samples whose magnitude exceeds a certain threshold. The undesirable effect of signal distortion due to these can be avoided by using the peak cancellation technique. In this method, a time-shifted and scaled reference is subtracted from the signal such that each subtracted reference function reduces the peak power of at least one signal sample. A sinc function could be used as a possible reference, but this needs to be spectrally limited. The sinc function can be spectrally limited by applying the raised cosine window function. Figure 2.20 shows an example of the signal envelopes of an arbitrary waveform and the corresponding cancellation signal. After the subtraction of the reference signal, the peak amplitude is reduced to a maximum of 3 dB above the rms value, as shown in Figure 2.21.
Figure 2.19  Frequency spectrum of an OFDM signal with 32 carriers with clipping and windowing.

Figure 2.20  (a) OFDM symbol envelope, and (b) constellation signal envelope.
Coding Technique

Several authors [19–22] have looked into the applicability of coding techniques to mitigate the PAPR issue. To achieve a smaller PAP level, the achievable code rate also becomes smaller. Although a large number of code words are available, their implementation and properties for use as forward error correction (FEC) codes (such as minimum distance) may not be suitable for implementation. However, Wilkinson and Jones [19] observed that a large portion of the codes were Golay complementary sequences, which has a structured way of implementing the PAPR reduction codes. The Golay complementary sequences are sequence pairs for which the sum of the autocorrelation function is zero for all delay shifts other than zero [23–25]. Figure 2.22 shows a typical example of an OFDM signal envelope using a complementary sequence coding.

Symbol-Scrambling Technique

The basic idea of the symbol-scrambling technique is that for each OFDM symbol, the input sequence is scrambled by a certain number of scrambling sequences. The output signal with the smallest PAPR is

![Figure 2.21](image-url) (a) OFDM symbol envelope, and (b) signal envelope after peak cancellation.
transmitted. This technique is very resource intensive, so use of it is limited where cost, size, and power are the overwhelming requirements.

2.5 OFDMA

This section describes the OFDMA technique for wireless communication [26–33]. In earlier sections we discussed the OFDM as a multiplexing scheme that provides better spectral efficiency and immunity to multipath fading, especially in the wireless environment. The OFDM also lends itself to a simple implementation scheme based on a highly optimized FFT/IFFT block. These advantages can also be extended for multiple-access schemes by assigning a subset of tones (subcarriers) of OFDM to individual users. The allocation of subsets of tones to various users allows for simultaneous transmission of data from multiple users, allowing for sharing the medium. In this way, it is equal to ordinary FDMA; however, OFDMA avoids the relatively large guard bands that are necessary in FDMA to separate different users.
An example of an OFDMA time-frequency grid is shown in Figure 2.23, where seven users a to g each use a certain fraction—which may be different for each user—of the available subcarriers. This particular example in fact is a mixture of OFDMA and TDMA, because each user transmits only in one out of every four time slots, which may contain one or several OFDM symbols.

### 2.5.1 Frequency-Hopping OFDMA

In the previous example of OFDMA, every user had a fixed set of subcarriers. It is a relatively easy change to allow hopping of the subcarriers per time slot, as depicted in Figure 2.24. Allowing hopping with different hopping patterns for each user actually transforms the OFDMA system into a frequency-hopping CDMA system. This has the benefit of increased frequency diversity, because each user uses all of the available bandwidth, as well as the interference averaging benefit that is common for all CDMA variants. By using forward error correction coding over multiple hops, the system can correct for subcarriers in deep fades or subcarriers that are interfered by other users. Because the interference and fading characteristics change for every hop, the system

<table>
<thead>
<tr>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
</tr>
<tr>
<td>b</td>
</tr>
<tr>
<td>c</td>
</tr>
<tr>
<td>d</td>
</tr>
<tr>
<td>e</td>
</tr>
<tr>
<td>f</td>
</tr>
<tr>
<td>g</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
</tr>
<tr>
<td>a</td>
</tr>
<tr>
<td>a</td>
</tr>
<tr>
<td>a</td>
</tr>
<tr>
<td>b</td>
</tr>
<tr>
<td>b</td>
</tr>
<tr>
<td>b</td>
</tr>
</tbody>
</table>

**Figure 2.23** Example of a time-frequency grid, with seven OFDMA users, a to g, which all have a fixed set of subcarriers every four timeslots.
performance depends on the average received signal power and interference, rather than on the worst-case fading and interference power.

A major advantage of frequency-hopping CDMA systems over direct sequence or multicarrier CDMA systems is that it is relatively easy to eliminate intracell interference by using orthogonal hopping patterns within a cell. An example of such an orthogonal hopping set is depicted in Figure 2.25. For \( N \) subcarriers, it is always possible to construct \( N \) orthogonal hopping patterns. Some useful construction rules for generating hopping patterns can be found in [26].

### 2.5.2 OFDMA System Description

As an example of an OFDMA system, this section gives a description of a system that was proposed for the European UMTS [27, 28]. Table 2.2 summarizes the parameters and key technical characteristics of this OFDMA air interface.

Figure 2.26 illustrates the time-frequency grid of the OFDMA system. The resources (time and frequency) are allocated based on the type of services and operational environment. The number of time slots and band slots per user is variable to realize variable data rates. The smallest

![Figure 2.24](image-url)
data rate is obtained for one band slot of 24 subcarriers per time slot of 288.46 µs.

The following summary shows some of the advantages of the proposed OFDMA system:

- Use of frequency-hopping OFDMA for interference averaging and frequency diversity;

---

**Figure 2.25** Example of six orthogonal hopping patterns with six different hopping frequencies.

**Table 2.2** Parameters of the Proposed OFDMA System

<table>
<thead>
<tr>
<th>Number</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Subcarrier spacing</td>
<td>4.1666 kHz</td>
</tr>
<tr>
<td>2</td>
<td>Symbol time</td>
<td>288.46 µs</td>
</tr>
<tr>
<td>3</td>
<td>Number of subcarriers per band slot of 100 kHz</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>Pre–guard time</td>
<td>38 µs</td>
</tr>
<tr>
<td>5</td>
<td>Post–guard time</td>
<td>8 µs</td>
</tr>
<tr>
<td>6</td>
<td>Modulation unit</td>
<td>1 band slot and 1 time slot (= 1 symbol)</td>
</tr>
<tr>
<td>7</td>
<td>Modulation block</td>
<td>4 time slots and 1 band slot</td>
</tr>
</tbody>
</table>
- Time division duplex MAC with dynamic channel allocation used for unpaired spectrum allocations, asymmetrical services, and unlicensed usage;
- Straightforward and efficient high–bit rate support by allocating more subcarriers and/or time slots;
- Small guard band requirements at approximately 100 kHz;
- No frequency planning option available; effective reuse factor of 1;
- GSM backward compatibility;
- Minimum bandwidth requirements for system deployment only 1.6 MHz (or less) and deployment possible in steps of 100 kHz.

Figure 2.27 shows the TDMA frame structure. Each frame is of length 4.615 ms, which is divided into 4 subframes of length 1.1534 ms. A subframe contains 4 time slots of duration 288.46 μs. The time slot
4.615 ms frame

4 frames (18.46 ms) Interleave

4 frames (18.46 ms) Interleave

1.1534 ms subframe

288.46 µs time slot

Guard period  Power control  User data

Rx burst

Time alignment

Tx burst

Figure 2.27 Frame (TDMA) structure.
contains a guard period, power control information, and data. Every OFDM symbol is mapped onto one time slot. The structure of an OFDMA symbol is depicted in Figure 2.28.

The whole system frequency band is divided into small blocks (band slots) with a fixed number of subcarriers. To maintain compatibility with GSM, a 100-kHz band slot is chosen that consists of 24 subcarriers. Therefore, the subcarrier spacing is \( \frac{100}{24} = 4.167 \) kHz. Figure 2.29 shows the OFDMA frequency structure.

In each band slot, the two subcarriers at the edge of the band slot are left unmodulated to relax receiver blocking requirements. In addition, the interference of two adjacent blocks of subcarriers is reduced, which may occur when their orthogonality is compromised because of nonlinear PA effects. Adjacent band slots can be concatenated to allow transmission of wideband services.

2.5.2.1 Channel Coding
Convolutional encoding and soft-decision Viterbi decoding is used for the basic data transmission. The objective of this coding is to achieve good quality in the tough mobile radio channel. A constraint length of seven is used, together with variable code rates in the range of 1/4 to 3/4. To achieve very low bit error rates (e.g., \( 10^{-6} \)) for video encoding or data transmission, a concatenated coding scheme is used with an inner convolutional code and an outer Reed-Solomon code.

2.5.2.2 Modulation
The modulation schemes of the OFDMA proposal are QPSK and 8PSK with differential encoding in the frequency domain. An optional coherent
Figure 2.29 OFDMA frequency structure.
mode with 16QAM is available, which uses pilot subcarriers to obtain a channel estimate at the receiver. For differential encoding, each band slot contains one known reference subcarrier value, as depicted in Figure 2.30.

2.5.2.3 Time and Frequency Synchronization

Synchronization is an essential issue for the OFDMA system. The following aspects are considered for uplink and downlink: initial modulation timing synchronization, modulation timing tracking, initial frequency offset synchronization, and frequency tracking.

2.5.2.4 Initial Modulation Timing Synchronization

Initial timing synchronization is required to adjust the mobile station’s internal timing to the base station’s time frame. After switching on, the mobile station monitors the initial acquisition channel (IACH) and the broadcast channel (BCCH).

![Figure 2.30](image-url)  
Figure 2.30 Reference subcarrier allocation.
After the mobile has detected the base station’s timing, it sends a random access channel (RACH) packet to the base station. The base station measures the time offset for the received RACH packet and sends back the necessary timing advance to the mobile (similar to GSM). In the frame structure of the OFDMA system, reserved slots for reception of RACH packets exist.

Because of the time and frequency structure of the OFDMA system, the timing tracking is less critical than with other OFDM systems, where users are interleaved in the frequency domain. The base station can measure the position of the received OFDM burst within the allocated slot for each mobile station individually and send the according timing alignment information back to the mobile station. In addition, timing information can be refined and tracked after the transformation in the subcarrier domain, where a time shift is observed as a phase rotation.

In the mobile station, the timing information is obtained and adjusted by the above-mentioned correlation algorithm. Accurate timing information is required to determine the position of the useful data samples within each burst so that the FFT window can be placed correctly. The guard samples relax the requirement for accurate timing because the position of the FFT window can be shifted within the guard time without performance degradation. Additional timing offset correction can be performed to cope with the FFT window misplacements.

2.5.2.5 Initial Frequency Offset Synchronization

After initial timing synchronization of the mobile station, the frequency offset can be measured by phase comparison of the (ideally) equal time samples within each burst. Equal samples are placed in the guard interval of the OFDM burst. A phase rotation indicates a frequency offset. Using this technique, a frequency error up to one-half the subcarrier spacing can be detected. The initial offset, however, can be larger, so it has to be detected using the specially designed symbols in the IACH channel.

2.5.2.6 Synchronization Accuracy

The proposed synchronization, acquisition, and tracking algorithm is independent of the modulation scheme (coherent or noncoherent). For coherent 16QAM reception, further processing in the frequency
(subcarrier) domain is possible to improve the performance. Frequency domain time tracking (or combined time domain/frequency domain tracking) algorithms can be based on observing phase shifts of the known pilots within the time-frequency grid on the subcarrier domain.

In the downlink, only an IACH is multiplexed to allow fast and precise initial timing and frequency synchronization. In the actual communication mode, timing and frequency tracking can be performed using a correlation-based synchronization algorithm. In the uplink, the rough timing offset is detected by the base station by measuring the arrival time of the RACH burst. This gives an initial time-advance value that is reported back to the mobile. During communication, the arrival time of the burst is detected by the base station using the proposed tracking algorithm (the same as in the downlink) or a tracking algorithm in the frequency (subcarrier) domain, based on the detected constellation rotation.

Both algorithms can also be combined. The alignment values are calculated regularly and reported to the mobile station. Accuracy requirements are relaxed because the design of the burst allows some overlapping arrival (another advancing feature of the raised cosine pulse shaping besides the reduction of out-of-band emission). In addition, the guard time helps to compensate timing misalignments. The OFDMA burst design provides a guard interval at the front and an additional guard interval at the back of the OFDM symbol (see Figure 2.31), which provides robustness against a timing inaccuracy of ±10 µs.

2.5.2.7 Power Control

Power control in the uplink removes the unevenness of received signal strength at the base station side and decreases the total power to the minimum level required to support the specified quality of service (e.g., BER). The accuracy is less critical than with CDMA because with OFDMA, orthogonality is always provided within one cell. A precise power control, however, not only improves the transmission performance but also minimizes the interference to other cells and therefore increases overall capacity.

The OFDMA concept uses both closed-loop and open-loop power control. Based on quality parameters, measured on a slot-by-slot basis, the power is adjusted in the mobile as well as in the base station transmitter.
Each receiver measures the quality of the received burst ($C/I$ ratio) and transmits in the next burst a request to the opposite transmitter to increase, maintain, or decrease the power level, in steps of 1 dB. For the fastest power control mode, one subcarrier is dedicated to carry power control information, and the power is then adjusted on a frame-by-frame basis (each 1.152 ms). Figure 2.32 depicts the power control operation.

### 2.5.2.8 Random Frequency-Hopping Operation

Frequency hopping is very effective to achieve frequency diversity and interference diversity. Frequency diversity is useful to average the frequency-selective channel properties (fading dips). Interference diversity is one of the important techniques used in the OFDMA proposal and has been shown to improve capacity in slow frequency-hopping TDMA systems [29].

The random hopping pattern is designed to be orthogonal within one cell (no collisions in the time-frequency grid) and random between cells (this causes cochannel interference).

The frequency hopping pattern has to fulfill certain requirements:

---

![Figure 2.31](image_url) **OFDMA burst and synchronization requirements.**

Each receiver measures the quality of the received burst ($C/I$ ratio) and transmits in the next burst a request to the opposite transmitter to increase, maintain, or decrease the power level, in steps of 1 dB. For the fastest power control mode, one subcarrier is dedicated to carry power control information, and the power is then adjusted on a frame-by-frame basis (each 1.152 ms). Figure 2.32 depicts the power control operation.

### 2.5.2.8 Random Frequency-Hopping Operation

Frequency hopping is very effective to achieve frequency diversity and interference diversity. Frequency diversity is useful to average the frequency-selective channel properties (fading dips). Interference diversity is one of the important techniques used in the OFDMA proposal and has been shown to improve capacity in slow frequency-hopping TDMA systems [29].

The random hopping pattern is designed to be orthogonal within one cell (no collisions in the time-frequency grid) and random between cells (this causes cochannel interference).

The frequency hopping pattern has to fulfill certain requirements:
• Orthogonality within one cell;
• Support of a variety of services by assigning different bandwidths (number of band slots);
• Support of a variety of services by assigning time slots (number of time slots);
• Support of a couple of time slot structures (4-TDMA, 8-TDMA, 16-TDMA) within the pattern.

The hopping pattern is generated at the base station according to the expected service and traffic requirement and is assigned to the cell. This assignment can be modified because of changes in the traffic characteristics. The base station can then support a set of services and a certain number of users for each service.

2.5.2.9 Dynamic Channel Allocation (Fast DCA)
Besides the frequency-hopping mode, the system can also be operated in TDD mode. Unlike in the frequency-hopping mode, the TDD mode does not separate the spectrum in an uplink and a downlink. Instead, it assigns band slots individually to uplink or downlink connections. In
TDD mode, a dynamic channel allocation algorithm is employed to avoid (rather than to average) excessive interference. The TDD mode is intended for picocellular, indoor use. The indoor environment is characterized by the following:

- Short radio propagation delays (100m is traversed in 0.3 µs, or 0.1% of the symbol duration);
- Greater demand for high-rate services, reducing the interference averaging advantage of frequency-hopping mode;
- Often asymmetric high-speed data traffic, prompting flexible division of bandwidth between uplink and downlink;
- Less severe propagation conditions than those outdoors; lower mobility-induced Doppler spread and delay spread.

In the TDD mode, the transmissions of mobile users are scheduled by the base station, which regularly transmits a frame map containing the following:

- Band slot allocations for the next frame. Band slots can be allocated to:
  - The base station for downlink transmission to a single terminal;
  - The base station for downlink transmission to all terminals (broadcast);
  - A single terminal for an uplink transmission;
  - All (or a group of) terminals for contention-based access.
- Transmit power assignments for MTs;
- Acknowledgments for contention traffic received in the previous frame;
- Allocation of slots on a connection basis, so that connection-dependent QoS can be provisioned (a mobile can have one or more connections);
- Transmission of control data and user data on different connections.
Terminals can transmit requests for band slots in contention slots designated by the base station in the FM. They can also piggyback requests onto uplink transmissions, which provides contention-free access, particularly in heavy traffic conditions. The base station performs interference measurements in all band slots, except at the time slots in which it is transmitting. This information is used by the band slot allocation algorithm to assign uplink transmissions to slots with minimal interference. Note that an uplink transmission in an interference-free slot (as measured by the base station) may interfere with a simultaneous uplink transmission at a neighboring base station. No simultaneous uplink and downlink transmissions may be scheduled within a cell. Therefore, the inability of the base station to measure interference in slots in which it is transmitting does not reduce capacity.

The frame layout is entirely decided by the DCA algorithm. Like the frequency-hopping algorithm, the DCA algorithm is distributed and does not rely on communication by way of the infrastructure. Also, as with the frequency-hopping algorithm, it is not part of the system specification; the algorithm may be vendor specific, allowing competitive positioning within a standardized system.

An example of a frame layout is shown in Figure 2.33. The figure is purely illustrative. The frame duration and system bandwidth have unrealistically small values. Also, the packets, such as the frame map—which

![Figure 2.33 Example of frame layout.](image-url)
is transmitted in the beacon—and user data packets, occupy more than one band slot in practice.

In general, the applied DCA algorithm must strive to reduce intracell and intercell interference. Constant bit rate traffic causes long-term interference that is highly predictive of the interference in the next slot. If traffic is bursty, the predictive value of interference measurements is limited. Because a base station is not aware whether band slots in neighboring cells are allocated to circuit mode or packet mode connections, base stations and mobiles average measurements over longer periods of time. As a rule, busy slots (high average interference level) are avoided for any transmission. Quiet slots (low average interference) are assigned to constant bit rate connections or to the guaranteed part of a variable bit rate connection. Slots with medium average interference are assigned to connections with bursty traffic, which use contention mode access.

Initial association does not differ from the procedure in the frequency-hopping mode. When joining the base station, a mobile station first detects the location of the initial acquisition channel and the broadcast channel. The broadcast channel is used to convey the location of the frame map in the current frame to the mobile station. Once the frame map is located, it can be tracked because it advertises when it is moved to a different location.

2.5.2.10 Simple Dynamic Channel Allocation
A simple DCA assigns a fixed resource (band slots and time slots) to a communication during setup. This assignment is kept for the duration of the communication. This scheme is very simple but cannot react to varying interference or channel conditions as can a fast DCA, where the “actual best” channel (= time slot and band slot combination) is used for transmission. This scheme has a lower performance than the fast DCA operation but can be used for simple (uncoordinated) applications such as cordless telephony.

2.5.2.11 OFDMA Capacity
System-level simulations were conducted for various types of services and environments. The simulations were conducted in accordance with [30]. Table 2.3 lists the simulated capacities.
Table 2.3  
Capacities for Various Services and Environments

<table>
<thead>
<tr>
<th>Environment</th>
<th>Cell Capacity (Number of users/MHz/cell) (uplink/downlink)</th>
<th>Spectrum Efficiency (Kbps/MHz/cell) (uplink/downlink)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data 384 Kbps</td>
<td>Outdoor to indoor and pedestrian A — 440/465</td>
<td></td>
</tr>
<tr>
<td>Data 2,048 Kbps</td>
<td>Indoor — 240/240</td>
<td></td>
</tr>
<tr>
<td>Speech 8 Kbps</td>
<td>Indoor office A 33.0/31.0</td>
<td>132/124</td>
</tr>
<tr>
<td>Speech 8 Kbps</td>
<td>Outdoor to indoor and pedestrian A 30.75/32.25</td>
<td>123/129</td>
</tr>
<tr>
<td>Speech 8 Kbps</td>
<td>Vehicular A 27.0/30.5</td>
<td>108/122</td>
</tr>
</tbody>
</table>

References


3

Broadband Wireless Access Fundamentals

3.1 Introduction

IEEE 802 is a working group dedicated to the development of wireless network standards at different levels. The standards being developed under the IEEE 802 family are personal area networks (PANs), local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs) [1]. Figure 3.1 shows the IEEE 802 family. Different task groups within the 802 committee are:

- Ethernet (IEEE 802.3);
- Wireless LANs (IEEE 802.11);
- Wireless PANs (IEEE 802.15);
- Broadband wireless networks (IEEE 802.16);
- Mobile broadband wireless networks (IEEE 802.20).

The basic focus of this book is on broadband wireless access (BWA) techniques. Having developed in steps, IEEE 802.16 is committed to
providing optimized solutions for BWA in fixed, nomadic, portable, and mobile conditions. The WiMAX Forum, an industry-led, nonprofit organization created in 2003 and made up of equipment manufacturers, component suppliers, and service providers, promotes industry-wide adoption of IEEE 802.16. It is a global organization, with member companies based in the countries listed in Table 3.1 [2].

As an industry-led working group, WiMAX Forum boasts to have as its partners such giants in the field of wireless communications as Alcatel, Alvarion, AT&T, Intel, Ericsson, Fujitsu, Hotsip, Lucent, ITM-Group, Getronics, and Siemens.

The chapter includes an introduction to broadband wireless access systems in Section 3.2, which also lists the spectrum options for BWA. Section 3.3 depicts the broadband wireless landscape. Deployment and interoperability are dealt with in Section 3.4, while the deployment considerations are provided in Section 3.5. Issues related to WiMAX are given in Section 3.6.
3.2 Basics of BWA

The ubiquitous access to voice and data networks has been the quintessential driving factor for last-mile connectivity through wireless technology. Wireless technology provides a cost-effective solution that allows for rapid deployment in a logistics-friendly manner. It provides straightforward scalability and extensibility to support growth and expansion of the user base. Wireless local loop (WLL) has already established itself as the primary alternative to the twisted-pair copper wire (local loop) in providing central office (backhaul) connectivity to homes and small offices on “the edge.” The successful deployment of WLL in rural and congested metropolitan areas is enticing BWA technology to address both point-to-point and point-to-multipoint metropolitan coverage, especially

<table>
<thead>
<tr>
<th>Argentina</th>
<th>Hong Kong</th>
<th>Portugal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>India</td>
<td>Russia</td>
</tr>
<tr>
<td>Austria</td>
<td>Indonesia</td>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>Iran</td>
<td>Singapore</td>
</tr>
<tr>
<td>Belgium</td>
<td>Ireland</td>
<td>South Africa</td>
</tr>
<tr>
<td>Bermuda</td>
<td>Israel</td>
<td>South Korea</td>
</tr>
<tr>
<td>Brazil</td>
<td>Italy</td>
<td>Spain</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Ivory Coast</td>
<td>Sweden</td>
</tr>
<tr>
<td>Canada</td>
<td>Japan</td>
<td>Switzerland</td>
</tr>
<tr>
<td>Chile</td>
<td>Kuwait</td>
<td>Syria</td>
</tr>
<tr>
<td>China</td>
<td>Latvia</td>
<td>Taiwan</td>
</tr>
<tr>
<td>Colombia</td>
<td>Lebanon</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>Denmark</td>
<td>Lithuania</td>
<td>Turkey</td>
</tr>
<tr>
<td>Egypt</td>
<td>Malaysia</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Finland</td>
<td>Mexico</td>
<td>United States</td>
</tr>
<tr>
<td>France</td>
<td>Nigeria</td>
<td>Vietnam</td>
</tr>
<tr>
<td>Germany</td>
<td>Norway</td>
<td></td>
</tr>
<tr>
<td>Greece</td>
<td>Papua New Guinea</td>
<td></td>
</tr>
</tbody>
</table>
in areas where the cost and logistics of laying down the copper is prohibitive. The BWA technology also provides an affordable broadband access to consumers who live far from the central office or reside in a rural area with low population density and need T1/E1 connectivity in small office and home environments. Additionally, it provides an alternative to a single-vendor monopoly and coverage to foster competition and to reduce the cost of ownership.

3.2.1 BWA Considerations

The definition of broadband has been debated for many years, but the requirements and expectations differ widely from one user to another. Fueled by the phenomenal growth of broadband Internet access and web browsing demands, the users’ quest for broadband links on the move has been escalating steadily toward pervasive broadband connectivity irrespective of locality, mobility, and type of connectivity. Although BWA does not fulfill the requirements of pervasive communication fully, nonetheless it tackles the growing metropolitan and rural connectivity gap (digital divide). The potential business case for BWA technology is still being debated—only time will tell the real story.

The considerations for BWA are being driven primarily by large corporate enterprises, small businesses, and residential households as a cost-effective and logistics-friendly alternative to point-to-point and point-to-multipoint connectivity. The requirements for BWA have been evolving for a while and have started to converge. The International Telecommunication Union (ITU) [3] has defined the transmission capability of 1.5 to 2.0 Mbps, considerably higher than for a primary Integrated Services Digital Network (ISDN), as the broadband data rate requirement. In many contexts any transmission rate higher than 256 Kbps is considered to be broadband. In early considerations BWA was envisioned as the cost-effective alternative to backhaul connectivity between metropolitan networks, but the mobility aspect was later added as an alternative for mobile users.

The IEEE Standards Association (IEEE-SA) has recently standardized a suite of 802.16 standards to cover LOS and non-LOS (NLOS) connectivity encompassing the 2- to 10-GHz and 10- to 60-GHz
frequency bands, respectively. In the beginning the 802.16 standards family had only a fixed BWA component, but later the mobility aspects were added in the 802.16e version of the standard. It is speculated that 802.16e would offer a competitive landscape to the 3G cellular market. It is also expected that BWA would be a complementary standard, filling the gap between local area and wide area connectivity, as shown in Figure 3.2. Currently, the IEEE 802.21 standard is being developed to work out the coexistence aspects of the ubiquitous wireless connectivity landscape.

The IEEE 802.16 standards incorporate innumerable frequency bands, bandwidth, coverage, and connectivity options to allow for flexible deployment schemes and growth potential. Two versions of 802.16, namely, 802.16-2004, also designated 802.16d (fixed BWA), and 802.16e (mobile BWA) have been defined to meet the requirements for different types of access. IEEE 802.16-2004 is optimized for fixed and nomadic access. The IEEE 802.16e amendment to the standard is designed to support portability and mobility. Different types of access supported by WiMAX and their requirements are shown in Table 3.2.

IEEE 802.16-2004 was ratified in July 2004 and includes all the previous versions (802.16-2001, 802.16c in 2002, and 802.16a in 2003), and it covers both LOS and NLOS applications in the 2- to 66-GHz frequencies. The changes introduced in 802.16-2004 include the NLOS applications in 2- to 11-GHz licensed as well as license-exempt frequency bands. It supports the OFDM modulation technique with 256 and 2,048 carriers for the license-exempt and licensed bands, respectively. The

![Figure 3.2](image-url)  Complementary wireless landscape with coexistence.
enhanced version of the fixed broadband wireless system, IEEE 802.16e, supports portability as well as mobility. It supports scalable OFDMA (SOFDMA) as well as the previously discussed OFDM and OFDMA modes. SOFDMA is a variation of OFDMA that allows a variable number of carriers. MIMO, adaptive antenna systems (AASs), hard and soft handoff, improved power-saving capabilities, and improved security features are some of the enhancements incorporated in the mobile version of 802.16. Table 3.3 shows the features of the fixed and mobile BWA systems.

Tables 3.4 and 3.5 show the roadmap of WiMAX. Table 3.4 shows the timeline of the WiMAX Forum for product certification. It plans to open the certification laboratory for products based on 802.16e in the late months of 2006, and the first 802.16e products certified with WiMAX Forum certification are expected to be out in the first few months of

---

**Table 3.2**

Two Versions of IEEE 802.16

<table>
<thead>
<tr>
<th>Definition</th>
<th>Devices</th>
<th>Locations/ Speed</th>
<th>Handoffs</th>
<th>802.16-2004</th>
<th>802.16e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed access</td>
<td>Outdoor and indoor CPE</td>
<td>Single/stationary</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Nomadic access</td>
<td>Indoor CPE, PCMCIA cards</td>
<td>Multiple/stationary</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Portability</td>
<td>Laptop PCMCIA or minicards</td>
<td>Multiple/walking speed</td>
<td>Hard</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Simple mobility</td>
<td>Laptop PCMCIA or minicards</td>
<td>Multiple/low vehicular speed</td>
<td>Hard</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Full mobility</td>
<td>Laptop PCMCIA or minicards, PDAs or smartphones</td>
<td>Multiple/high vehicular speed</td>
<td>Soft</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Source: [4].

Note: CPE = customer premises equipment; PCMCIA = Personal Computer Memory Card International Association.
Table 3.3
Salient Features of the IEEE 802.16 Standards Family

<table>
<thead>
<tr>
<th>Feature</th>
<th>802.16</th>
<th>802.16-2004 (8021.6d)</th>
<th>802.16e</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency band</td>
<td>10 to 66 GHz</td>
<td>2 to 10 GHz</td>
<td>&lt; 6 GHz</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>20, 25, and 28 MHz</td>
<td>1.25 to –20 MHz</td>
<td>1.25 to 20 MHz</td>
</tr>
<tr>
<td>Typical data rate (maximum)</td>
<td>32 to 134 Mbps</td>
<td>75 Mbps (20 MHz)</td>
<td>5 Mbps (5 MHz)</td>
</tr>
<tr>
<td>Connectivity</td>
<td>LOS</td>
<td>NLOS</td>
<td>NLOS with mobility</td>
</tr>
<tr>
<td>Coverage</td>
<td>&lt; 3 km</td>
<td>Typical &lt; 5 km</td>
<td>&lt; 3 km</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum 30 km (LOS)</td>
<td></td>
</tr>
<tr>
<td>Modulation technique</td>
<td>OFDM</td>
<td>OFDM</td>
<td>OFDM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFDMA</td>
<td>OFDMA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SOFDMA</td>
<td></td>
</tr>
<tr>
<td>Typical application</td>
<td>Fixed</td>
<td>Portable</td>
<td>Mobile</td>
</tr>
</tbody>
</table>

Table 3.4
WiMAX Forum Timeline for Product Certification

<table>
<thead>
<tr>
<th></th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.16-2004 lab opens</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Air protocol certification—outdoor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service certification—outdoor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indoor certification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.16 lab opens</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.16e first certification</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Source: [4].*

2007. Table 3.5 shows the road map to the commercial availability of WiMAX user device equipment.

Other global trends are emerging as well toward the utilization of the 2.3-, 2.5-, 3.5-, and 5.8-GHz frequency bands for BWA, mostly influenced by experimental WiMAX and WiBro deployments. The World Radio Conference (WRC) is also looking into the availability of additional frequency spectrum across the globe to allow for worldwide BWA deployment. Although the frequency spectrum under
consideration by WRC is already being used for proprietary BWA and multichannel multipoint distribution service (MMDS) deployment, as shown in Figure 3.3, nonetheless standardization by WRC provides

<table>
<thead>
<tr>
<th>Year</th>
<th>802.16-2004 WiMAX</th>
<th>802.16e WiMAX</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>First certified products Outdoor CPE Indoor, self-installable CPE PCMCIA card for laptops</td>
<td>—</td>
</tr>
<tr>
<td>2007</td>
<td>—</td>
<td>First certified products PCMCIA card for laptops, indoor self-installable CPE</td>
</tr>
<tr>
<td>2008</td>
<td>—</td>
<td>Mini-PCMCIA card for laptops PDA, smartphone</td>
</tr>
<tr>
<td>2009</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

*Source: [4].*

---

**Figure 3.3** Spectrum under consideration for BWA deployment worldwide.
a landscape for a global frequency spectrum allocation strategy, interoperability, and overwhelming economy of scale considerations.

3.2.2 Frequency Band Allocation for BWA

Figure 3.3 shows the various bands available for BWA in the 2- to 6-GHz range. This range includes licensed as well as unlicensed bands. Licensed bands are those that are owned by carriers that have paid for the use of these bands. Unlicensed bands are those that are freely available for any experimental or enterprise application. Distinct bands for the BWA market are as follows [5, 6].

3.2.2.1 3.5-GHz Band

This is a licensed band that is available for BWA applications in many European as well as Asian countries but not in the United States. It is the most heavily allocated band, representing the largest global BWA market. This band has a bandwidth of 300 MHz, from 3.3 to 3.6 GHz, thus offering great flexibility for large-pipeline backhauling to WAN services.

3.2.2.2 5-GHz Unlicensed National Information Infrastructure and WRC Bands

The Unlicensed National Information Infrastructure (UNII) bands are in three major frequency groups:

- Low and middle UNII bands—5,150 to 5,350 MHz;
- WRC—5,470 to 5,725 MHz;
- Upper UNII/ISM bands—5,725 to 5,850 MHz.

Strong WiMAX growth is expected in these unlicensed bands. Many WiMAX activities are taking place in the upper UNII band because there are few competing services and less interference.

3.2.2.3 WRC

There are two 15-MHz Wireless Communications Service (WCS) bands:
• 2,305 to 2,320 MHz;
• 2,345 to 2,360 MHz.

WiMAX uses OFDM technology, which has exceptional spectral efficiency and thus can be successfully deployed in these bands.

3.2.2.4 2.4-GHz ISM
This ISM band is unlicensed and offers around 80 MHz of bandwidth for BWA deployment.

3.2.2.5 MMDS
The MMDS spectrum provides 31 channels of 6-MHz spacing in the 2,500- to 2,690-MHz range and includes the Instructional Television Fixed Service (ITFS). Significant BWA growth is expected in this band since it is largely underutilized.

3.2.3 Will Fixed WiMAX Die?
The tremendous interest in IEEE 802.16e is threatening the growth of WiMAX fixed applications. It is envisaged that mobile WiMAX will take the lion’s share of the wireless broadband market [7, 8]. The common question that arises is, why invest in two technologies separately when 802.16e supports both fixed as well as mobile applications of WMAN? The undercurrent within the broadband wireless sectors is that fixed WiMAX is nice, but 802.16e is far better and worth waiting for. So, is it the end of fixed WiMAX? Has fixed WiMAX died before even coming into the consumer market? The fixed WiMAX proponents have better answers to these questions. Backhaul is a huge fixed WiMAX market opportunity that will continue to grow, irrespective of the existing broadband technologies.

Fixed and mobile deployments have very different requirements and target very different market segments, with different usage patterns and locations, throughput needs, user device form factors, and service level agreements (SLAs). Two versions of WiMAX have been defined to cater to the needs to two completely different markets with varying
requirements of different applications. In the fixed deployment with basic functionality, both mobile and fixed versions of WiMAX are based on OFDM(A) and are similar in nature. Single-sector maximum throughput for both versions of WiMAX is about 15 Mbps for a 5-MHz channel or 35 Mbps for a 10-MHz channel. But their performance changes with the specific applications since both are optimized for different accesses. IEEE 802.16d is optimized for fixed access and 802.16e for mobile access. Benefits [4] of fixed networks are as follows:

- **Less complex modulation.** As compared to SOFDMA, OFDM is a simpler modulation technique. For markets where mobility is not to be supported, OFDM is a less complex option, making the fixed network quickly deployable at a lower cost.

- **License-exempt bands.** Fixed deployments successfully use license-exempt bands in areas where interference levels are acceptable, in comparison to mobile services, which require a licensed spectrum to provide coverage in wide areas. Thus, 802.16-2004 includes most of the profiles targeting license-exempt bands.

- **Higher throughput.** Higher-spectrum bands selected for 802.16-2004 profiles have an advantage of higher throughput.

- **Better time to market.** Earlier commercial availability of 802.16-2004 products has enabled operators to meet the pent-up demand for broadband connectivity in underserved areas and to start gaining market share ahead of competitors.

Mobile WiMAX of course has its own added advantages, but there is a clear picture of survivability of fixed networks. Most of the companies are bringing to market dual-band products that enable deployment of both mobile and fixed WiMAX environments.

The choice between 802.16-2004 and 802.16e products largely depends on the type of services provided and the business model of the operator. A mobile operator building an overlay network to complement a 3G network will head straight for 802.16e. A wireless Internet service
provider (WISP) supplying wireless access to a rural community will typically choose the less complex, OFDM-based, 802.16-2004 WiMAX products.

### 3.3 Wireless Broadband Landscape

The mobility aspect of wireless connectivity especially is becoming extremely competitive, as shown in Figure 3.4. In particular, the 802.16e and 802.20 (under development) standards would compete for erstwhile cellular systems to gain their user base. Ultimately, survivability of BWA systems would depend on spectral efficiency, cost, superior user experience, and ubiquitous connectivity. Other considerations depend on its adaptation by service providers, its quick deployment in dense metropolitan areas, and proof of its reliability and high availability. Introduction of mobility to the 802.16 standard poses a direct threat to existing 3G cellular systems and shows its potential to compete with cellular networks and to be a strong candidate for 4G [9].

![Figure 3.4](image)

**Figure 3.4** Broadband wireless connectivity landscape.
Advantages that allow 802.16e to stand in competition with 3G cellular networks and that lead 802.16e to migrate toward 4G [9] are as follows:

- **Technology.** 802.16e is based on OFDMA technology paired with MIMO smart antenna technology, which is best suited for 4G.
- **Coverage.** WiMAX has a coverage range of 4 to 6 miles (30 miles maximum).
- **Spectrum.** 802.16 can work in both the licensed as well as the unlicensed frequency bands.
- **Interference.** OFDM, which is supported by 802.16, utilizes multiple channels to send and receive data, which results in less interference.
- **IP connectivity.** 802.16e supports asynchronous transfer mode (ATM), IP versions 4 (IPv4) and 6 (IPv6), Ethernet, and virtual local area network (VLAN) services, which provide a rich choice of service possibilities to voice and data network service providers.
- **Interoperability.** Interfaces are IP based, which permits reuse of mobile client software across operator domains.
- **Backhaul.** 802.16 provides backhaul connections to cellular services.
- **Standardization and economies of scale.** The WiMAX Forum works on standardization, which will provide the ability for mass production of WiMAX-enabled products, lowering the service, development, and deployment costs.

### 3.3.1 WWANs

It seems that the cellular system providers may have a distinct advantage at this early stage because of their existing footprint, amortized research and development costs, and user experience considerations. In addition, the capabilities of 3G systems [10] are rapidly evolving, as shown in Figure 3.5, to match landline capabilities and would compete very favorably with BWA offerings. The CDMA2000 Single-Carrier (1.25-MHz) Evolution Data Optimized (1xEV-DO) Release 0 provides higher
**3G Technologies**

<table>
<thead>
<tr>
<th>Designed for In-Band Migration</th>
<th>CDMA2000 1xEV-DO</th>
<th>Enhanced EV-DO</th>
<th>Scalable Bandwidth EV-DO</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>1.25 MHz</em> Data + IP Voice</td>
<td>IS-856 Release 0</td>
<td>Revision A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dedicated for packet data</td>
<td>3.1 Mbps f/wd link</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.1 Mbps peak rate (fwd link)</td>
<td>1.8 Mbps reverse link</td>
<td>VoIP, lower latency</td>
</tr>
<tr>
<td></td>
<td>300 – 700 kbps average and end user rates</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Designed for New Spectrum</th>
<th>CDMA2000 1X</th>
<th>1xEV-DV?</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>1.25 MHz</em> Voice &amp; Data</td>
<td>IS-2000 Release 0</td>
<td>Rev. C</td>
</tr>
<tr>
<td></td>
<td>Revision A</td>
<td>Rev. D</td>
</tr>
<tr>
<td></td>
<td>Double voice capacity</td>
<td>3.1 Mbps fwd link</td>
</tr>
<tr>
<td></td>
<td>155.6 kbps packet data</td>
<td>Up to 15 carriers aggregated</td>
</tr>
<tr>
<td></td>
<td>50 – 80 kbps average and end user rates</td>
<td>Up to 40 Mbps fwd link</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Designed for New Spectrum</th>
<th>WCDMA (UMTS)</th>
<th>HSDPA</th>
<th>HSUPA</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>5 MHz</em> Voice &amp; Data</td>
<td>3GPP Release 99</td>
<td>Rel. 5</td>
<td>Rel. 6</td>
</tr>
<tr>
<td></td>
<td>64/584 kbps circuit switched/packet data</td>
<td>1.8 to 11.4 Mbps f/wd link</td>
<td>High rate reverse link (EUL), IMS, MBMS</td>
</tr>
<tr>
<td></td>
<td>Soft handoff: 84 – 250 kbps average and end user rates</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008/9</th>
</tr>
</thead>
</table>

**Figure 3.5** 3G evolution timeline.
spectral efficiency with low latency, for a downlink peak data rate of 2.4 Mbps and an uplink peak data rate of 153 Kbps, and supports asymmetric real-time applications. It also has provisioning for downlink per flow QoS to support a mix of applications. The 1xEV-DO Revision A standard and evolving systems continue to enhance the spectral efficiency, peak- to-average data rate per sector, QoS with use of adaptive coding and modulation, hybrid automatic repeat request (HARQ), MIMO, and low-latency packet sizes. A WCDMA system has an equivalent evolution path and achieves higher spectral efficiency, data rate, throughput, and QoS to support symmetric/asymmetric real-time applications.

In recent years the last-mile connectivity problem has been solved with propitiatory technologies in the local multipoint distribution system (LMDS) and MMDS bands. These bands are not uniformly available across the world, which does not allow for economy of scale. In addition, these systems utilize all kinds of waveform access, air interface, and signaling schemes, causing interoperability across systems and equipment. In 1988 the Federal Communications Commission (FCC) allocated and auctioned 1 GHz of spectrum in the 28- to 31-GHz bands for LMDS, intended for backhaul connectivity to CPE for business and residential users. In March 1999, the IEEE 802 LAN/MAN Standards Committee [11] created the IEEE 802.16 Working Group on Broadband Wireless Access. The mission of this body was to “develop standards and recommended practice to support the development and deployment of fixed broadband wireless access systems.” The IEEE 802.16 group has made significant strides toward building a consensus in developing an industry-wide standard for BWA systems.

### 3.4 Global Deployment and Interoperability

The goal [12] of the development of 802.16-related standards was to ensure and fulfill interoperability and global deployment considerations. Establishment of a standard is critical to mass adoption of a given technology; however, standardization by itself is not sufficient—it has to provide a superior user experience. For example, the 802.11b WLAN standard [13] was ratified in 1999; however, it neither reached a profitability margin nor enticed wide adaptation until the introduction of the
Wi-Fi Alliance, and certified, interoperable equipment was available in 2001. Thus, standards need to take into account regulations governing emissions, channel bandwidth, available spectrum and its usage, and the certification process across the globe and be flexible enough to meet local regulatory and consumer requirements. While 802.16 standards have been established for both the licensed and the unlicensed band, the real flexibility needs to be provided in the licensed bands, where service providers would have to pay for the frequency spectrum. Since the spectrum in the licensed bands offers varying degrees of bandwidth, throughput, and cost constraints, it is imperative that the standard address flexibility in bandwidth, throughput, and incremental buildup for worldwide deployment.

3.4.1 Air Interface and PHY Considerations

The air interface and signaling schemes were selected to ensure scalability, ease of implementation, and a technically superior solution with LOS/NLOS coverage constraints. To maintain a high level of spectral efficiency, immunity to multipath impairments and ease of implementation, the OFDM air interface format was selected in preference to competing formats such as TDMA or CDMA. To take advantage of the CDMA technique, a high processing gain is required to provide adequate immunity to interference, requiring RF channel bandwidth one to two orders of magnitude higher than the data rate. This is not feasible for BWA schemes below 11 GHz. For example, data rates up to 70 Mbps would require RF bandwidths exceeding 200 MHz to deliver comparable processing gains and NLOS performance.

Some of the other air interface features of 802.16-related standards are tailored to provide reliable link performance in a broad range of channel environments. These include but are not limited to flexible channel widths, adaptive burst profiles, FEC with concatenated Reed-Solomon and convolutional encoding, optional AASs to improve range/capacity, dynamic frequency selection (DFS) to help minimize interference, and space-time coding (STC) to enhance performance in fading environments through spatial diversity.
At the PHY layer the standard supports flexible RF channel bandwidths and reuse of the channels (frequency reuse) as a way to increase cell capacity as the network grows. The standard also specifies support for automatic transmit power control and channel quality measurements as additional PHY layer tools to support cell planning/deployment and efficient spectrum use. Operators can reallocate spectrum through sectorization and cell splitting as the number of subscribers grows. Also, support for multiple channel bandwidths enables equipment makers to provide a means to address the unique government spectrum use and allocation regulations faced by operators in diverse international markets. The IEEE 802.16 standard specifies channel sizes ranging from 1.75 up to 20 MHz, with many options in between.

In the MAC layer, the CSMA/CA foundation of 802.11, basically a wireless Ethernet protocol, scales about as well as does Ethernet—that is to say, poorly. Just as in an Ethernet LAN, where more users results in a geometric reduction of throughput, so does the CSMA/CA MAC for WLANs. In contrast, the MAC layer in the 802.16 standard has been designed to scale from one and up to hundreds of users within one RF channel, a feat the 802.11 MAC was never designed for and is incapable of supporting.

3.4.2 Coverage

The BWA standard needs to offer optimal coverage and robust links in all kinds of propagation conditions and to deliver reliable performance in rural, urban, and metropolitan environments. The OFDM waveform is capable of offering high spectral efficiency (bits per second per hertz) with the use of spectrally efficient modulation techniques, beam forming, and MIMO antennas over wide ranges, with up to 70 Mbps in a single RF channel. Other advanced techniques [such as low-density parity check codes (LDPC), interference cancellation (IC), spatial diversity techniques, and so forth] can also be used to increase spectral efficiency, capacity, and reuse factor. The OFDM waveform usage in the WLAN in providing connectivity inside an office or a building covering tens and maybe a few hundreds of meters has proved itself worthy of consideration. The 802.16
standard needed to be designed for higher power with an OFDM approach that supports deployments in the tens of kilometers.

### 3.4.3 QoS

The 802.16 standard is designed to provide a superior QoS. The MAC protocol was designed from ground up to keep this in mind. Unlike the 802.11 MAC, which relies on CSMA/CA, 802.16 relies on a grant/request protocol for access to the medium, and it supports differentiated and best effort service levels based on periodic (fast) and aperiodic for scheduling and flow control (e.g., dedicated T1/E1 for business and best effort for residential). The protocol employs link adaptation and automatic repeat request (ARQ) using time division multiplexing (TDM) data streams on the downlink (DL) and TDMA on the uplink (UL). By ensuring collision-free data access to the channel, the 802.16 MAC improves total system throughput and bandwidth efficiency, in comparison with contention-based access techniques such as the CSMA/CA protocol used in WLANs. The 802.16 MAC also ensures bounded delay on the data (CSMA/CA, by contrast, offers no guarantees on delay). The TDM/TDMA access technique also ensures easier support for multicast and broadcast services. With a CSMA/CA approach at its core, 802.11 in its current implementation will never be able to deliver the QoS of a BWA, 802.16 system.

The 802.16 MAC was designed specifically for the point-to-multipoint wireless access environment. Additionally, it was built to be agnostic to physical as well as the upper layer protocols and seamlessly to adapt to ATM, frame relay, Ethernet, or IP, and it must be extensible to evolving and future protocols that have not yet been developed.

It is envisioned that the combination of 802.16a and 802.11 will create a complete wireless solution for delivering high-speed Internet access to businesses, homes, and Wi-Fi hot spots. The 802.16a standard promises to deliver carrier-class performance in terms of robustness and QoS and has been designed from the ground up to deliver a suite of services over a scalable system for long-range, high-capacity, last-mile wireless communications. In BWA, applications include residential broadband access—DSL-level service for small office/home office (SOHO) and small business
establishments and T1/E1-level service for enterprise, all supporting not just data but voice and video as well, wireless backhaul for hot spots, and cellular tower backhaul service, to name a few.

### 3.5 Deployment Considerations

The viability of any new technology depends on a prudent business case and healthy market penetration. The cost of deploying equipment and services, including the maturity of the underlying technology and quick buildup ability, would dictate the success or failure of the venture. Finally, adoption by network operators, service providers, and user communities would be key success criteria.

The operators and service providers must have compelling reasons to invest in BWA technology based on the total cost of ownership, which must include initial deployment, future upgrade capabilities, maintenance, and standardized interface to external entities. It must take into account the cost of CPE, access points, routers, switches, and access terminals (ATs), including the expense of managing the network remotely to minimize the downtime.

The cost of equipment is highly dependent on an available vendor pool. A large vendor pool allows for competition and economy of scale. It accelerates innovation and feature enhancements in a cost-effective manner, including amortization of investments across many suppliers and OEMs. The standardized systems, interfaces, and specifications allow for a level playing field, lowering the barrier of entry to the newcomers and helping to build the large vendor pool.

To survive and prosper in this day and age, any newcomer needs to learn to live in a heterogeneous environment and must strive to coexist with legacy and emerging systems. To attain ubiquitous connectivity, it has to provide a means for seamless roaming and handoff to various other systems without affecting the connectivity or QoS of the link. Inter and intra technology handoff and coexistence issues need to be ironed out and in place before deployment. In the early stages of deployment, this helps in building the confidence of the users because it provides them greater alternatives.
3.6 Issues

The IEEE 802.16 family of standards tackles only the PHY and MAC layers and relies heavily on external bodies to develop standards for higher-layer protocols. This approach has worked well so far, as is evident from the successful deployment and adaptation of Ethernet (802.3) and Wi-Fi (802.11) technologies. The IETF was responsible for developing higher-layer protocols such as TCP/IP, SIP, VoIP, and IPSec to provide the network and transport layers connectivity to the underlying 802.3 and 802.11 families of standards developed by IEEE. In the cellular world, where 802.16e is planning to compete, 3rd Generation Partnership Project (3GPP) and 3GPP2 standards bodies establish not only the air-link interface but a wide range of protocols that allow for intervendor internetwork interoperability, roaming, multivendor network access, and interoperator billing. Since the IEEE 802.16 standard is developed with IP as a core network from the ground up, it certainly gives them some advantage over existing 2G and evolving generations of cellular systems.

References


4

Fixed Broadband Wireless Access

4.1 Introduction

Chapter 3 introduced the fundamentals of BWA. This chapter presents an overview of fixed broadband wireless access (FBWA), whereas MBWA will be discussed in Chapter 5. Broadband access has been available for some time now, but access for most people is still limited. Initially, each BWA vendor built its own proprietary solution for network deployment, which led to increased cost and delay. The expensive, proprietary equipment was not interoperable and was specific to one particular vendor. The lack of interoperability made the usefulness of the technology limited, non-profitable, and non-competitive for BWA providers [1]. Thus, to promote interoperability among vendors, WiMAX came into existence [2]. WiMAX is a technical, industry working group that provides interoperability guidelines and certification criteria to the BWA developers. WiMAX is to 802.16 as Wi-Fi is to 802.11. The standardization will result into affordable, wide-range coverage and dramatic business improvements for BWA. Operators can benefit from interoperability and economies of scale of WiMAX-certified equipment. South Korea is developing its own version of WiMAX, called as WiBro [2, 3].
The IEEE 802.16 Working Group has ongoing activities, and it addresses two usage models. The first is a standard designed for fixed access, IEEE 802.16-2004. The other, IEEE 802.16e, is an amendment to 802.16-2004 that targets the mobile market. This chapter focuses on the IEEE 802.16-2004 standard associated with FBWA. First published in April 2002, the IEEE 802.16 standard defines the specifications for WMANs [4]. This standard was called IEEE 802.16a. A revision standard, IEEE 802.16d, also known as IEEE 802.16-2004, was published in June 2004. The IEEE 802.16-2004 standard defines FBWA for bands 10 to 66 GHz and both licensed and unlicensed bands in the 2- to 11-GHz range. The standard heralds the entry of BWA as an efficient tool to link homes and businesses to core telecommunications networks worldwide. FBWA systems can provide multimedia services to a number of discrete customer sites with IP and offer numerous advantages over wired IP networks [2].

The applications depend on the spectrum to be used. The primary bands of interest are listed in the following subsections.

### 4.1.1 10- to 66-GHz Licensed Band

This band requires LOS. Due to the short wavelength and negligible multipath components, this band is applicable only to the direct LOS mode of operation. Channel bandwidths of 25 or 28 MHz and raw data rates in excess of 120 Mbps are typical for this physical environment. The single-carrier modulation air interface specified in the 10 to 66-GHz band is known as the WirelessMAN-SC air interface.

### 4.1.2 Frequencies Below 11 GHz

Frequency bands below 11 GHz provide a multipath-rich environment, where NLOS signal strengths are significant and thus attractive for cellular types of services. Additional PHY layer functionality and MAC features are introduced by the IEEE 802.16d standard to support near-LOS and NLOS scenarios.
4.1.3 License-Exempt Frequencies Below 11 GHz (Primarily 5 to 6 GHz)

The intrinsic features of this band are the same as those of the licensed band below 11 GHz. However, additional interference and coexistence issues are prevalent in this band due to its license-exempt nature. DFS has been introduced in PHY and MAC by the standard to detect and avoid interference.

4.1.4 Reference Model

The protocol layering model proposed for this standard is as shown in Figure 4.1. The scope of the IEEE 802.16-2004 standard is limited to the data/control plane. This standard covers both the MAC and PHY layers. The MAC comprises three sublayers:
1. Service-specific convergence sublayer (CS);
2. MAC common part sublayer (MAC CPS);

The service-specific CS layer receives external network data through the CS service access point (SAP) and maps this data into MAC service data units (SDUs). The MAC CPS layer receives these SDUs through the MAC SAP. In the process, the SDUs are classified and associated with MAC service flow identifiers (SFIDs) and connection identifiers (CIDs) and may undergo functions such as payload header suppression (PHS).

The MAC CPS provides the core MAC functionality of system access, bandwidth allocation, connection establishment, and connection maintenance. The security sublayer provides authentication, secure key exchange, and encryption. The PHY SAP provides an interface between the MAC and PHY layers. The PHY SAP is implementation specific. Data, PHY control, and statistics are transferred between the MAC CPS and the PHY via the PHY SAP.

This chapter provides an overview of FBWA systems based on the standard reported in [5]. The advent of FBWA is a result of the needs of end users to have good and affordable wireless accessibility within a range of several kilometers at a reasonable cost. Section 4.2 describes the driving factors for the development of the FBWA. The section also lists the advantages, potential market, and applications of FBWA. Section 4.3 explains the MAC in detail, describing its three sublayers. Section 4.4 discusses the four PHY layer specifications. Section 4.5 gives the issues concerned with FBWA deployment, and the chapter is concluded in Section 4.6.

### 4.2 Driving Factors of FBWA

This section deals with the needs and advantages of FBWA and also lists the market segments and applications affected by FBWA.

#### 4.2.1 Needs

Broadband has been benefiting consumers and enterprises for the past few years. The benefit of broadband access has been limited to the people
residing in urban areas with broadband services (via DSL, cable, wireless). Broadband access is not available in most suburban and rural areas. Global integration, need for fast information exchange, and rapidly developing markets in remote areas have fueled the existence of FBWA.

The DSL, cable, and fiber optics markets providing wired broadband access have succeeded in reaching millions of business and private subscribers. But supplying the quick rollout of infrastructure to the last mile has become a difficult and expensive challenge for the carriers, which cannot possibly keep pace with the demand. This has brought about a situation wherein subscribers living in the developed areas with broadband-ready infrastructure can enjoy all the benefits of DSL services while the broadband coverage in remote areas, smaller towns, and rural areas is lagging behind. This is known as the broadband gap or digital divide.

The DSL operators initially focused their deployment in densely populated urban and metropolitan areas but are now required to provide broadband access in suburban and rural areas [6]. The DSL or cable connections are limited for the following reasons: [1, 7]:

- Customers are out of reach of DSL services (too far from the central office).
- Customers are not part of the residential cable infrastructure (a problem for many businesses).
- Customers think it is too expensive (both getting connected and the monthly service fee).

Also, in areas where DSL is available, sometimes it takes too long to get services from the local telephone company. Thus, the hurdles to overcome are poor line quality of the installed copper base, the large distances to the central office or cabinets, or the low population density, and costs and delays in availing services.

In last-mile markets, where traditional cable or copper infrastructures are either saturated, outdated, or simply out of reach, the fast deployment and reasonable cost of fixed wireless broadband provides an attractive solution. The IEEE 802.16 standard with its QoS support, longer reach, and data rates similar to those of DSL naturally becomes a
viable option, offering broadband access to bridge the broadband gap [8]. FBWA as the first phase of WiMAX is a communication system that provides digital two-way voice, data, Internet, and video services.

4.2.2 Advantages

The main business advantages of wireless systems based on IEEE 802.16 can be summarized as follows [9]:

- FBWA provides the ability to overcome the physical limitations that exist with traditional wired infrastructure and still provide residential and business users with comparable throughputs at up to 40 km.
- Broadband service provision can be extended to the areas where the existing plant is not allowing copper-based xDSL-based services.
- It can provide cost efficient service supply in areas where traditional xDSL is not suitable due to low population density.
- Service can be quickly provisioned even in areas that are hard for wired infrastructure to reach, helping operators to overcome the digital divide.

4.2.3 Market Segments for FBWA

Figure 4.2 shows the markets for FBWA systems. As more and more countries enable carriers and service providers to operate in a variety of frequencies, new and lucrative broadband access markets are springing up everywhere [10].

In last-mile markets where traditional (FBWA) cable or copper infrastructures are either saturated, outdated, or simply out of reach, FBWA technology fills the void admirably, providing highly efficient and cost effective access services for millions of subscribers who would otherwise be left out of the loop [6]. The BWA market targets wireless multimedia services to SOHOs, small and medium-sized businesses, and residences. The fixed wireless market for broadband megabit per second transmission rates is growing for providing an easily deployable low-cost...
solution, compared with existing cable and digital subscriber line (xDSL) technologies for dense and suburban environments.

In emerging countries, the main focus of broadband deployment is in urban and suburban areas and will remain so in the near future. The low penetration of plain ordinary telephone system (POTS) and the low quality of the copper pair prevent DSL deployment on a massive scale, fostering the need for alternate broadband technologies [8].

The growth of the market can be seen in Figure 4.3. Understanding the enormous potentials of the fixed wireless networking market, networking equipment makers have shown great interest in WiMAX [6]. Like the Wi-Fi product vendors, the networking equipment makers will have to work with the service providers for deployment [11].

### 4.2.4 Applications

The 802.16 standard can help the industry to provide solutions across multiple broadband segments, namely, (1) cellular backhaul, (2) broadband on demand, (3) residential broadband, and (4) underserved areas [8, 12]. They are briefly discussed in the following paragraphs. The markets
for WiMAX are shown in Figure 4.4. Figure 4.5 illustrates the various needs being served by IEEE 802.16, and Figure 4.6 depicts its NLOS wireless point-to-multipoint connections and LOS backhaul applications.

In the United States, Internet providers are required to lease lines to third-party providers, making wired backhaul relatively affordable. This results in only about 20% of cellular towers being backhauled wirelessly in the United States. It is less common for local exchange carriers to lease their lines to third parties in Europe, and wireless backhaul is used in approximately 80% of European cellular towers. If the leasing requirement by the FCC is removed, U.S. cellular providers will also look into wireless backhaul as a more cost-effective alternative. The robust bandwidth of 802.16 technology makes it a good choice for backhaul for commercial enterprises.

The on-demand connectivity is useful at trade shows and also for businesses such as those that work at construction sites. The deployment of 802.11 hot spots and SOHO wireless LANs in areas not served by cable or DSL will be accelerated by last-mile BWA. For many businesses, the broadband connectivity is important enough that they relocate to areas where service is available. If such service is not available, it may take a local exchange carrier three months or more to provide a T1 line to a

**Figure 4.3** Worldwide broadband market growth.
Figure 4.4 Markets for WiMAX.

Figure 4.5 The IEEE 802.16 standard enables solutions that meet the needs of a variety of broadband access segments.
business customer. IEEE 802.16 wireless technologies allow a service provider to offer speed comparable to wired service at low cost and in a matter of days. The service providers with 802.11 wireless technologies also offer instantly configurable on-demand high-speed connectivity for temporary events, generating hundreds or thousands of users for 802.11 hot spots.

Due to practical limitations, the cable and DSL technologies are incapable of reaching many potential broadband customers. Many older cable networks are not equipped to provide a return channel, and converting them to high-speed broadband can be very expensive. In areas with low subscriber density, the cost of deploying cable is also a significant deterrent to extension of wired broadband. The traditional DSL connections can reach only 18,000 feet from the central office switch,
limiting them to a specific range. For mass deployment, the current generation of wireless systems is relatively expensive since without a standard, few economies of scale are possible. This cost inefficiency will change with the launch of standard-based systems such as 802.16. The limitations of traditional wired and proprietary wireless technologies can be overcome by the absence of the LOS requirement, the high bandwidth, the inherent flexibility, and the range of 802.16 solutions.

For underserved rural and outlying areas with low population density, wireless Internet technology based on IEEE 802.16 is a natural choice. Local utilities and government work together with a local WISP to deliver service in such areas. There currently are more than 2,500 WISPs in the United States that take advantage of the license-exempt spectrum to serve 6,000 markets since the wired infrastructure either does not exist or does not offer the quality to support even reliable voice transmission in these areas. Therefore, most deployments are in the licensed spectrum and are made by local exchange carriers that supply voice services in addition to high-speed data transmission on an international basis. Such applications are designated as WLL since it is a substitute for traditional copper phone wire in the local loop.

4.3 MAC

The MAC is optimized for long-distance links because it is designed to tolerate longer delays and delay variations. The IEEE 802.16 specification accommodates MAC management messages that allow the base station to query the subscriber station, but there is a certain amount of time delay [2].

The IEEE 802.16 MAC protocol was designed for point-to-multipoint (PMP) BWA applications, but to accommodate the more demanding physical environment and different service requirements, MAC also provides ARQ and supports mesh, rather than only PMP network architectures [13]. Mesh networks differ in one main way: In PMP, the traffic is only between the base station (BS) and the subscriber station (SS). In mesh networks, traffic can flow between two SSs or be routed through an SS.
4.3.1 Service-Specific CS

The service-specific CS is the topmost layer among the three sublayers of MAC. This sublayer transforms or maps the external network data into MAC SDUs. That is, it utilizes the services provided by the MAC CPS via the MAC SAP. The functions performed by the CS include accepting, classifying, and processing of higher-layer protocol data units (PDUs). It also delivers CS PDUs to the appropriate MAC SAP and receives CS PDUs from peer entities. The two CS specifications that have been provided currently are as follows:

- ATM CS;
- Packet CS.

4.3.1.1 ATM CS

The ATM CS is a logical interface that associates different ATM services with the MAC CPS SAP. It is specifically defined to support the convergence of PDUs generated by the ATM layer protocol of an ATM network. An ATM connection is either virtual path (VP) switched or virtual channel (VC) switched. An ATM connection is simply identified by a pair of values of virtual path identifier (VPI) and virtual channel identifier (VCI). The VP-switched mode automatically maps all VCIs within one single incoming VPI to that of an outgoing VPI. The VC-switched mode individually maps the VPI/VCI to output VPI/VCI values. The ATM CS performs suppression (PHS) after differentiating the two types of connections. In PHS, a repetitive portion of the payload headers of the CS is suppressed by the sending entity and restored by the receiving entity. On the UL, the sending entity is the SS and the receiving entity is the BS. On the DL, the sending entity is the BS and the receiving entity is the SS.

4.3.1.2 Packet CS

The packet CS resides at the top of the IEEE. 802.16 MAC CPS. It performs all the functions of the CS, utilizing the services of the MAC. The packet CS is used for transport for all packet-based protocols. The implementation of PHS capability is optional.
4.3.2 MAC CPS

This forms the second sublayer of the MAC. Two-way PMP and mesh topologies are wireless networks that utilize a shared medium and provide an efficient sharing mechanism. PMP and mesh topologies are examples for sharing wireless media, where the medium is the space through which the radio wave propagates. The operation of the DL from the BS to the user is based on PMP. The main difference between the PMP mode and the optional mesh mode is that in the PMP mode, traffic flows only between the BS and SSs, while in the mesh mode, traffic can be routed through other SSs and can flow directly between SSs. The systems of the mesh networks are termed as nodes in general. Each node in the mesh network has a 48-bit universal MAC address that uniquely defines it from within the set of all possible vendors and equipment types. Also, each air interface in the SS has a 48-bit universal MAC address that uniquely defines the air interface of the SS. This address is used during the network entry process and as a part of the authentication process by which network systems verify the identity of each other. Figure 4.7 shows the MAC PDU format.

Each PDU consists of a fixed-length generic MAC header, which may be followed by the payload and a cyclic redundancy check (CRC). If present, the payload consists of zero or more subheaders and zero or more MAC SDUs and/or fragments thereof. The payload information may vary in length, so a MAC PDU may represent a variable number of bytes. All reserved fields are set to zero on transmission and ignored on reception.

A generic MAC header has one defined DL MAC header, and each MAC PDU begins with either MAC management messages or CS data. There are two defined UL MAC header formats. The first is the generic MAC header that begins each MAC PDU, containing either MAC

![Figure 4.7](image-url)
management messages or CS data. The second is the MAC header format without payload and CRC. The single-bit header type (HT) field distinguishes the two header formats. The HT field is 0 for the former and 1 for the latter. There are six types of subheaders that may be present in a MAC PDU with generic MAC header. The per-PDU subheaders (i.e., extended subheader field, mesh, fragmentation, fast-feedback allocation, and grant management) immediately follow the generic MAC header in MAC PDUs. Among fragmentation and grant management subheaders, the latter comes first. The mesh subheader precedes all other subheaders, except for the extended subheader. In the DL, the fast-feedback allocation subheader always appears as the last per-PDU subheader.

The only per-SDU subheader is the packing subheader, which may be inserted before each MAC SDU. The packing and fragmentation subheaders are mutually exclusive; both cannot appear within the same MAC PDU. Also, a per-SDU subheader always follows per-PDU subheaders. The fragmentation subheaders indicate the fragmentation state of the payload. The grant management subheader is 2 bytes in length and is used by the SS to convey bandwidth management needs to the BS. When the packing subheader is used, the MAC may pack multiple SDUs into a single MAC PDU. In the mesh mode, the mesh subheader always follows the generic MAC header. The extended subheader is not encrypted and always appears immediately after the generic MAC header and before all subheaders.

4.3.2.1 MAC Management Messages
A set of MAC management messages is defined and carried in the payload of the MAC PDU. All MAC management messages consist of a management message type and may be followed by additional fields. The MAC management message format is shown in Figure 4.8.

<table>
<thead>
<tr>
<th>Management message type</th>
<th>Management message payload</th>
</tr>
</thead>
</table>

Figure 4.8 MAC management message format.
4.3.2.2 Construction and Transmission of MAC PDUs

There are certain processes through which transmission of MAC PDUs takes place. IEEE 802.16 takes advantage of incorporating the packing and fragmentation processes with the bandwidth allocation process to maximize the flexibility, efficiency, and effectiveness of both. Fragmentation and packing are allowed to be simultaneously performed for efficient use of the bandwidth [13]. The various steps involved in construction and transmission of MAC PDUs follow.

**Conventions**

Conventions describe the rules in accordance with which data can be transmitted.

**Concatenation**

Multiple PDUs may be concatenated into a single transmission in either the UL or the DL direction.

**Fragmentation**

A MAC SDU or MAC management message can be divided into one or more MAC PDUs by the process of fragmentation. This process allows efficient use of available bandwidth. Fragmentation of traffic takes place when the connection is created by the MAC SAP. The BS initiates fragmentation for DL connections and the SS initiates for UL. The parent SDU is tagged with fragments along with their positions according to the table of fragmentation rules. The capabilities of fragmentation and reassembly are mandatory. Table 4.1 shows the fragmentation rules.

**Packing**

Packing is optional and if active, multiple MAC SDUs are packed into a single MAC PDU. The capability of unpacking is mandatory.

**CRC Calculation**

When a service flow requires the addition of a CRC to each MAC PDU carrying data for that service flow, a CRC is appended to the payload of
the MAC PDU with HT = 0. The CRC protects the generic MAC header and ciphered payload and is calculated after encryption.

*Encryption of MAC PDUs*

Encryption and decryption, along with data authentication of a MAC PDU payload of a mapped MAC PDU to a security association (SA) (described in Section 4.3.3), on a transmitting and receiving connection, respectively, are performed as specified by that SA. The generic MAC header is not encrypted. The header contains all the encryption information [encryption control (EC) field, encryption key sequence (EKS) field, and CID] needed to decrypt a payload at the receiving station. Figure 4.9 shows the encrypted MAC PDU format.

*Padding*

Allocated space within a data burst that is unused can be initialized to a known state.

<table>
<thead>
<tr>
<th>Fragment</th>
<th>Fragmentation Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>First fragment</td>
<td>10</td>
</tr>
<tr>
<td>Continuing fragment</td>
<td>11</td>
</tr>
<tr>
<td>Last fragment</td>
<td>01</td>
</tr>
<tr>
<td>Unfragmented</td>
<td>00</td>
</tr>
</tbody>
</table>

*Source:* [5].

**Table 4.1**

Fragmentation Rules

**Figure 4.9** MAC PDU encryption. (*From:* [5]. © 2004 IEEE. Reprinted with permission.)
4.3.2.3 ARQ Mechanism

ARQ processing is a means of retransmitting MAC SDU blocks that have been dropped or corrupted while being transmitted. The MAC uses the sliding window method. It sends an agreed number of blocks regardless of the acknowledgment received. The receiver transmits an acknowledgment if the blocks arrive and slides the window forward or requests dropped or lost blocks [14].

4.3.2.4 Scheduling Services

Data-handling mechanisms supported by the MAC scheduler for data transport on connection are represented by the scheduling service. Each connection is associated with a single scheduling service. A scheduling service is determined by a set of QoS parameters that quantify aspects of its behavior. Table 4.2 summarizes the scheduling services and the poll/grant options available for each. The UGS is designed to support real-time UL flows that transport fixed-size data packets on a periodic basis, such as T1/E1 and VoIP without license suppression. The rtPS is designed to support variable-size data packets such as Moving Pictures Experts Group (MPEG) video. The nrtPS offers unicast polls on a regular basis, which ensures that the service flow receives request opportunities even during network congestion. The BE service provides efficient service for best-effort traffic in the UL.

<table>
<thead>
<tr>
<th>Scheduling Type</th>
<th>Piggyback Request</th>
<th>Bandwidth Stealing</th>
<th>Polling</th>
</tr>
</thead>
<tbody>
<tr>
<td>UGS</td>
<td>Not allowed</td>
<td>Not allowed</td>
<td>PM bit is used to request a unicast poll for bandwidth needs of non-UGS connections</td>
</tr>
<tr>
<td>rtPS</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Scheduling allows only unicast polling</td>
</tr>
<tr>
<td>nrtPS</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Scheduling may restrict a service flow to unicast polling via the transmission/request policy; otherwise, all forms of polling allowed</td>
</tr>
<tr>
<td>BE</td>
<td>Allowed</td>
<td>Allowed</td>
<td>All forms allowed</td>
</tr>
</tbody>
</table>

Source: [5].
4.3.2.5 Bandwidth Allocation and Request Mechanisms

Increasing (or decreasing) bandwidth requirements is necessary for all the services except incompressible constant bit rate UGS connections. There are numerous methods by which the SS can get a bandwidth request message to the BS.

Requests

Whenever an SS needs UL bandwidth allocation, it uses request mechanisms to indicate that to the BS. A request may be either a stand-alone bandwidth request header or a piggyback request. The piggyback request capability is optional. All requests for bandwidth are made in terms of the number of bytes needed to carry the MAC header and payload but not the PHY overhead. Bandwidth requests are incremental or aggregate. In an incremental bandwidth request, the BS adds the quantity of bandwidth requested to its current perception of the bandwidth needs of the connection. When the BS receives an aggregate bandwidth request, the current perception of bandwidth needs of the connection is replaced by the quantity of bandwidth requested. The type field in the bandwidth request header indicates whether the request is incremental or aggregate.

The capability of incremental bandwidth requests is optional for the SS and mandatory for the BS. The capability of aggregate bandwidth requests is mandatory for the SS and the BS.

Grants

For an SS, each bandwidth grant is addressed to the SS’s basic CID and not to individual CIDs.

Polling

Polling is the process by which the BS allocates to the SSs bandwidth specifically for the purpose of making bandwidth requests. These allocations may be to individual SSs or to groups of SSs.

4.3.2.6 MAC Support for PHY

Several duplexing techniques are supported by the MAC protocol.
**FDD**
In an FDD system, two separate frequencies are allocated for the UL and DL channels. The DL data can be transmitted in bursts. Both UL and DL transmissions use a fixed-duration frame and facilitate the use of different modulation types. Simultaneous use of both full-duplex SSs and optionally half-duplex SSs is allowed. A full-duplex SS is capable of continuously listening to the DL channel, while a half-duplex SS can listen to the DL channel only when it is not transmitting in the UL channel.

**TDD**
In a TDD system, the UL and DL transmissions share the same frequency but occur at different times. A TDD frame has a fixed duration and contains one DL and one UL subframe.

**DL Media Access Profile**
The DL media access profile (DL-MAP) defines the usage of the DL intervals for a burst-mode PHY.

**UL Media Access Profile**
The UL media access profile (UL-MAP) defines the UL usage in terms of the offset of the burst relative to the allocation start position.

**4.3.2.7 QoS**
The various protocol mechanisms may be used to support QoS for both UL and DL traffic through the SS and BS. The principal mechanism for providing QoS is to associate packets traversing the MAC interface into a service flow as identified by the transport CID. A service flow is a unidirectional flow of packets that is provided a particular QoS. The SS and BS provide this QoS according to the QoS parameter set defined for the service flow. Defining transmission ordering and scheduling on the air interface is the primary purpose of the QoS feature.

**Service Flows**
A service flow is a MAC transport service that provides unidirectional transport of packets either to UL packets transmitted by the SS or to DL
packets transmitted by the BS. A service flow is partially characterized by the following attributes:

- **SFID.** A service flow has at least one SFID and an associated direction. The SFID is the principal identifier for the service flow between the SS and a BS.

- **CID.** The CID of the transport connection exists only when a service flow is admitted or active. The SFID and transport CID, when present, are unique from each other.

- **Provision QoS ParamSet.** This is a QoS parameter set that is provision via means outside the standard.

- **Admitted QoS ParamSet.** This is a set of QoS parameters that defines the reserved resources such as the bandwidth of the BS (and the SS).

- **Active QoS ParamSet.** This is a QoS parameter set that defines the service actually being provided to the service flow.

- **Authorization module.** The authorization module is a logical function within the BS. Any change to QoS parameters and classifiers associated with a service flow is approved or denied by the logical function. The possible values of the admitted QoS ParamSet and active QoS ParamSet are limited by the defining of an envelope by the authorization module.

The active QoS ParamSet is always a subset of the admitted QoS ParamSet, which in turn is always a subset of the envelope defined by the authorization module. There are three types of service flows specified by the standard:

- **Provisioned.** This type of service flow is named for the provisioning by, for example, the network management. Both the admitted QoS ParamSet and the active QoS ParamSet are null in this service flow.
• **Admitted.** The active QoS ParamSet of this type of service flow is null, and it has resources reserved by the BS for its admitted QoS ParamSet, but these parameters are not active.

• **Active.** In this type of service flow, the BS has resources committed for a non-null active QoS ParamSet.

**Object Model**

The rectangles in Figure 4.10 represent the major objects of the architecture. Each object has a number of attributes, and underlying attributes uniquely identify the object. The numerical relationships between the objects are marked as \( N, 0, \) or 1 at the ends of the lines connecting the objects. For example, a service flow may be associated with from 0 to \( N \) (many) PDUs, but a PDU is associated with exactly one service flow. The service class is an optional object that may be implemented at the BS and is defined in the BS to have a particular QoS parameter set.

**Service Class**

The service class allows the operators to modify the implementation of a given service to local circumstances without changing the SS

---

**Figure 4.10** Theory of operation object model. *(From: [5]. © 2004 IEEE. Reprinted with permission.)*
provisioning. It also allows higher-layer protocols to create a service flow by its service class name.

Authorization
The authorization module approves any change to the service flow QoS parameters. A new service flow is created and the QoS parameter set of an existing service flow is changed.

Service Flow Creation
The provisioning of service flows is done by means outside the scope of the standard. During provisioning, a service flow is instantiated and gets an SFID and a provision type. The service flow can be dynamically created, initiated by either the BS (mandatory capability) or the SS (optional capability). The SS or BS response indicates acceptance or rejection. Protocols are also defined for modifying and deleting service flows.

Service Flow Management
The series of MAC management messages referred to as dynamic service addition (DSA), dynamic service change (DSC), and dynamic service deletion (DSD) are responsible for creation, modification, and deletion of service flows, respectively (see Figure 4.11). No service flow exists in the null state. In the operational state, a service flow exists and has an assigned SFID. The service flow makes a transition whenever DSx messaging occurs and remains operational. Multiple state machines, one for each service flow, may be active since multiple service flows can exist simultaneously. Only those state machines that match the SFID and/or transaction ID are affected by the DSx messages. The hashed message

![Figure 4.11 Dynamic service flow overview.](image_url)
authentication code (HMAC) digests on all DSx messages are verified by both the SS and the BS before being processed. Any messages that fail are discarded.

### 4.3.2.8 Ranging and Negotiation of SS Capabilities

Upon learning what parameters to use for its initial ranging transmissions, the SS looks for initial ranging opportunities by scanning the UL-MAP messages present in every frame. The SS uses a truncated exponential backoff algorithm to determine which initial ranging slot it will use to send a ranging request message. The SS sends the burst using the minimum power setting and tries again with increasingly higher transmission power if it does not receive a ranging response.

Based on the arrival time of the initial ranging request and the measured power of the signal, the BS commands a timing advance and a power adjustment to the SS in the ranging response. The response also provides the SS with the basic and primary management CIDs. Once the timing advance of the SS transmissions has been correctly determined, the ranging procedure for fine-tuning the power can be performed using invited transmissions. All transmissions up to this point are made using the most robust, and thus least efficient, burst profile. To avoid wasting capacity, the SS next reports its PHY capabilities, including the modulation and coding schemes it supports and whether, in an FDD system, it is half duplex or full duplex. The BS, in its response, can deny the use of any capability reported by the SS [13].

### 4.3.2.9 Network Entry

To enter a network, it is mandatory for the SS to go through the network entry process. Network entry involves the following sequence of actions [14, 15]:

- The SS scans for a suitable BS DL signal, which it uses to establish channel parameters.
- Initial ranging allows the SS to set PHY parameters correctly and establish the primary management channel with the BS. This channel is used for capability negotiation, authorization, and key management.
• The privacy and key management (PKM) protocol authorizes the SS to the BS.

• The SS registers by sending a request message to the BS. The BS response assigns a CID for a secondary management connection.

• The SS and BS create transport connections using a MAC-create-connection request. A request to create a dynamic transport connection indicates whether MAC-level encryption is required.

4.3.3 Security Sublayer

Security is implemented as a privacy sublayer at the bottom of the MAC protocol’s internal layering. The security sublayer provides privacy, authentication of network access, and connection establishment with strong protection from theft of service. This is accomplished by encrypting connections and exchange of keys between the SS and the BS.

4.3.3.1 Architecture

Privacy has two component protocols, as follows:

• An encapsulation protocol for securing packet data across the fixed BWA network:
  • A set of cryptographic suites defined by this protocol, pairing data encryption and authentication algorithms;
  • Rules for applying these algorithms to a MAC PDU payload.

• A PKM protocol providing the secure distribution of keying data from the BS to the SS.

4.3.3.2 Secure Encapsulation of MAC PDUs

The MAC security sublayer contains the encryption services. The generic MAC header format contains the MAC header information specific to encryption. Only the MAC PDU payload is encrypted; the generic MAC header is not encrypted.
4.3.3.3 Key Management Protocol

An SS uses the PKM protocol to obtain authorization and traffic keying material from the BS and to support periodic reauthorization and refresh. The PKM uses X.509 digital certificates (IETF RFC 3280), the RSA\(^1\) public-key encryption algorithm [Pks1], and strong encryption algorithms to perform key changes between the SS and the BS.

**Security Associations**

An SA is the set of security information a BS and one or more of its client SSs can share to support secure communications across IEEE 802.16 networks. Three types of SA are defined: primary, static, and dynamic. During the SS initialization process, each SS establishes a primary security association. Static SAs are provisioned within the BS. Dynamic SAs are established and eliminated, on the fly, in response to the initiation and termination of specific service flows. Both the static and dynamic SAs can be shared by multiple SSs.

SAs are identified using SA identifiers (SAIDs). An SA’s shared information includes the cryptographic suite employed within the SA. It may also include traffic encryption keys (TEKs) and initialization vectors. The exact content of an SA is dependent on the SA’s cryptographic suite.

The SS requests from its BS an SA’s keying material using the PKM protocol, and the BS ensures that each client SS has access only to the SAs it is authorized to access. An SA’s keying material [e.g., Data Encryption Standard (DES) key and cipher block chaining (CBC) initialization vector] has a limited lifetime. The BS provides the SS with the material’s remaining lifetime when it delivers that SA keying material to the SS. The SS becomes responsible for requesting new keying material from the BS before the current keying material expires at the BS. If the current material expires before a new set of keying material is received, the SS performs network entry, with key synchronization between the BS and the SS specified by the PKM protocol.

---

1. The RSA algorithm is named after Ron Rivest, Adi Shamir, and Len Adleman, who invented it in 1977 [16].
SS Authorization and Authorization Key Exchange Overview

SS authorization is the process by which the BS authenticates a client SS’s identity and is controlled by the authorization state machine.

- The BS and the SS establish a shared authorization key (AK) by RSA, from which a key encryption key (KEK) and manage authentication keys are derived.
- The BS provides the authenticated SS with the identities (i.e., SAIDs) and the properties of primary and static SAs for which the SS is authorized to obtain keying information.
- Reauthorization is performed periodically by an SS with the BS after achieving initial authorization and is managed by the SS’s authorization state machine. The TEK state machine manages the refreshing of protected encryption key (TEKs).

TEK Exchange Overview

An SS starts a separate TEK state machine for each of the SAIDs identified in the authorization reply message after achieving authorization. Each TEK state machine manages the keying material associated with its respective SAID and also manages refreshing of keying material for its SAID.

Security Capabilities Selection

An SS support a list of cryptographic suites (pairing of data encryption and data authentication algorithms), and during the authorization exchange, the SS provides the BS this list. The BS selects a single cryptographic suite to employ with the requesting SS’s primary SA, independent of the requesting SS’s cryptographic capabilities. A BS rejects the authorization request if it determines that none of the offered cryptographic suite is satisfactory. The authorization reply sent by the BS includes a primary SA descriptor and an optional static SA descriptor that identify the cryptographic suite employed with the SA. The SS does not start the TEK state machine for static SAs whose cryptographic suites the SS does not support.
4.3.3.4 Cryptographic Methods
All the BSs and SSs support the cryptographic algorithms specified in the standard.

Data Encryption Methods
Data on the connections associated with an SA uses the CBC mode of the U.S. DES or the counter mode encryption (CTR) mode with CBC message authentication code (CBC-MAC) (CCM) mode of the U.S. Advanced Encryption Standard (AES) algorithm to encrypt the MAC PDU payloads, depending on whether the data encryption algorithm identifier in the cryptographic suite of that SA equals 0x01 or 0x02, respectively. The CBC IV is calculated as follows: In the DL, the CBC is initialized with the XOR of the IV parameter included in the TEK keying information and the current frame number. In the UL, the CBC is initialized with the XOR of the IV parameter included in the TEK keying information and the frame number of the frame where the relevant UL-MAP was transmitted.

A 4-bytes packet number (PN) is appended in front of the payload and is not encrypted. The plain text payload is encrypted and authenticated using the active TEK according to the CCM specification. An 8-byte integrity check value (ICV) is appended to the end of the payload and is also encrypted. The PN and cipher text ICV are transmitted least significant bit (LSB) first. The payload after encryption is 12 bytes longer than the plain text payload.

PDU Payload Format
The PN associated with an SA is set to 1 when the SA is established and when a new TEK is installed. The PN is incremented by 1 after each PDU transmission. In the UL the PN is XORed with 0x80000000 prior to encryption and transmission, while it is not modified on DL connections. Any tuple value of (PN, KEY) is used only once for the purpose of transmitting data. Before the PN on either the BS or the SS reaches 0x7FFFFFFF, the SS ensures that a new TEK is requested and transferred, else transport communication on that SA is halted until new TEKs are installed. TEK management in the BS and the SS is depicted in Figure 4.12.
The receiving SS or BS decrypts and authenticates the PDU consistent with the National Institute of Standards and Technology (NIST) CCM specification. Packets found not to be authentic are discarded. The highest value of PN received for each SA is recorded by the receiving BS or SSs, and any packet received having a PN less than the recorded maximum for that SA is discarded.

**Encryption of TEK**

TEK can be encrypted by a number of methods, depending on the TEK encryption algorithm identifier in the cryptographic suite. If the identifier equals 0x01, the encryption method used is 3DES. If the identifier equals 0x02, the RSA method of encrypting the TEK is used. If the identifier equals 0x03 or 0x04, the encryption of TEK-128 with AES and the encryption of TEK-128 with AES key wrap methods are used, respectively.

**Calculation of HMAC Digest**

The HMAC (IETF RFC 2104) has an algorithm that is used for the calculation of the keyed hash in the HMAC digest attribute and the HMAC tuple. HMAC-KEY-D and HMAC-KEY-U authentication keys derived
from the AK are used for authenticating messages in the DL and UL directions, respectively. The HMAC sequence number in the HMAC tuple and the AK sequence number of the AK from which HMAC-KEY-X derives should be equal.

4.4 PHY Layer

IEEE 802.16-2004 defines the PHY layer for the 10- to 66-GHz range of (licensed) spectrum. This band of frequency requires LOS operation, and the effect of multipath is negligible in this physical environment. The standard also supports the 2- to 11-GHz band of licensed and unlicensed spectrum. This frequency range supports NLOS operation and also takes into account the effects of multipath. The PHY layer of 802.16-2004 supports four main modes:

1. WirelessMAN-SC PHY;
2. WirelessMAN-SCa PHY;
3. WirelessMAN-OFDM PHY;
4. WirelessMAN-OFDMA PHY.

The following subsections deal with these PHY air interface specifications in detail.

4.4.1 WirelessMAN-SC PHY Specification

This PHY specification is for operation in the frequency band from 10 to 66 GHz and is designed with a high degree of flexibility, allowing service providers to optimize system deployments with respect to cell planning, cost, radio capabilities, services, and capacity. Both TDD and FDD configurations are supported for flexibility in spectrum usage. Both full-duplex as well as half-duplex SSs are supported by FDD. The UL PHY is based on a combination of TDMA and demand-assigned multiple access (DAMA). The UL channel is divided into a number of time slots. The MAC in the BS controls the number of slots assigned for various uses. The DL channel is based on TDM. A provision is made for a TDMA portion of the DL to support half-duplex FDD SSs.
Operation is performed in a framed format for this specification. There is a DL subframe and an UL subframe in each frame. The DL subframe begins with information necessary for frame synchronization and control. In TDD the DL subframe comes first, followed by the UL subframe, while in FDD UL transmissions occur concurrently with the DL frame. The PHY type parameter is 0 for TDD and 1 for FDD.

4.4.1.1 FDD and TDD Operation

The UL and DL channels are on separate frequencies in FDD operation. The capability of the DL to be transmitted in bursts facilitates the use of different modulation types and allows the system to simultaneously support full-duplex and half-duplex SSs. The DL carrier may be continuous. Figure 4.13 describes the basics of the FDD operation. In the TDD operation, the UL and DL transmissions share the same frequency but are separated in time.

A TDD frame has a fixed duration and contains one DL and one UL subframe. Figure 4.14 shows the TDD frame structure. The transmit/receive transition gap (TTG) is a gap between the DL burst and the subsequent UL that allows time for the BS to switch from transmit to receive mode. After the gap, the BS receiver looks for the first symbols of

![Figure 4.13](image)

**Figure 4.13** Example of FDD bandwidth allocation.
the UL burst. The receive/transmit transition gap (RTG) is a gap between the UL burst and the subsequent DL burst that allows time for the BS to switch from receive to transmit mode. After the gap, the SS receivers look for the first symbols of QPSK-modulated data in the DL burst.

4.4.1.2 DL PHY

A granularity of one physical slot (PS) is defined as the available bandwidth in the DL direction. The available bandwidth in the UL direction is defined with a granularity of one minislot, where the minislot length is $2^m$ PSs ($m$ ranges from 0 through 7). The number of PSs within each frame is a function of the symbol rate. Figure 4.15 illustrates the structure of the DL subframe using TDD. The DL subframe begins with a frame start preamble used by the PHY for synchronization and equalization, which is followed by the frame control section, containing the DL-MAP and UL-MAP stating the PSs at which bursts begin. The following TDM portion carries the data, organized into bursts. The control information of the DL is received and decoded by each SS, and the SS looks for MAC headers indicating data for that SS in the remainder of the DL subframe. Figure 4.16 illustrates the structure of the DL subframe in the FDD case. As in the TDD case, the DL subframe also begins with a frame start preamble followed by a frame control section and a TDM portion organized...
into bursts. The FDD DL subframe continues with a TDMA portion used to transmit data to any half-duplex SSs scheduled to transmit earlier
in the frame than they receive, which allows an individual SS to decode a specific portion of the DL without the need to decode the entire DL subframe. In the TDMA portion, each burst begins with the DL TDMA burst preamble for phase resynchronization. The FDD frame control section includes a map of both the TDM and TDMA bursts.

**DL Burst Allocation**

The DL data sections are used for transmitting data and control messages to the specific SSs. The data is always FEC coded and is transmitted at the current operating modulation of the individual SS. In the TDM portion, data is transmitted in order of decreasing burst profile robustness, while in the case of a TDMA portion, the data is grouped into separately delineated bursts that need not be in robustness order.

The DL-MAP message contains a map that states at which PS the burst profile changes occur. In the case of TDMA, if the DL data does not fill the entire DL subframe, the transmitter is shut down.

**DL Transmission Convergence Sublayer**

After the CS pointer byte is added, the DL payload is segmented into blocks of data designed to fit into the proper codeword size. The payload length may vary, depending on whether shortening of code words is allowed or not for this burst profile.

**DL Physical Medium Dependent Sublayer**

The DL PHY coding and modulation for the physical medium dependent (PMD) mode is summarized in Figure 4.17. The DL channel supports adaptive burst profiling on the user data portion of the frame. Up to 12 burst profiles can be defined. Since there are optional modulation and FEC schemes that can be implemented at the SS, a method for identifying the capability of the BS is required. Randomization is employed to minimize the possibility of transmission of an unmodulated carrier, and it ensures adequate numbers of bit transitions to support clock recovery. The stream of DL packets is randomized by modulo-2 addition of the data with the output of the pseudo-random binary sequence (PRBS) generator. Selectable FEC code types are presented in Table 4.3.
DL Modulation

The PHY uses a multilevel modulation scheme to maximize the utilization of the air link. The modulation constellation can be selected per subscriber based on the quality of the RF channel. In the DL, the BS supports QPSK and 16QAM modulation and, optionally, 64QAM. In changing from one burst profile to another, the BS uses one of two power adjustment rules: maintaining constant constellation peak power (power adjustment rule = 0), or maintaining constant constellation mean power (power adjustment rule = 1). In the former case, corner points are
transmitted at equal power levels regardless of modulation type, while in
the latter the signal is transmitted at equal mean power levels regardless of
modulation type. The I and Q signals are filtered by square-root raised
cosine filters prior to modulation. The excess bandwidth factor \( \alpha \) is 0.25.

4.4.1.3 UL PHY

The UL transmission CS operation is identical to that of DL.

**UL Subframe**

The structure of the UL subframe used by the SS to transmit to the BS is
shown in Figure 4.18.

During the UL subframe, three classes of bursts may be transmitted
by the SS:

1. Those that are transmitted in contention opportunities reserved for
   initial ranging;
2. Those that are transmitted in contention opportunities defined by
   request intervals reserved for response to multicast and broadcast
   polls.

![Figure 4.18](image-url) UL subframe structure.
3. Those that are transmitted in intervals defined by data grant information element (IEs) specifically allocated to individual SSs.

Each UL burst begins with an UL preamble. This preamble is based upon a repetition of a $+45^\circ$-rotated constant amplitude zero autocorrelation (CAZAC) sequence. Each UL burst profile in the UL channel descriptor (UCD) message includes the following parameters:

- Modulation type;
- FEC code type;
- Last code word length;
- Preamble length;
- Randomizer seed.

**UL PMD Sublayer**

The UL PHY coding and modulation are summarized in the block diagram shown in Figure 4.19. The UL modulator implements a randomized, variable modulation which is set by the BS. QPSK is supported, while 16QAM and 64QAM are optional. In changing from one burst profile to another, the SS uses one of two power adjustment rules:

![Conceptual block diagram of the UL PHY.](image)
maintaining constant constellation peak power (power adjustment rule = 0), or maintaining constant constellation mean power (power adjustment rule = 1). In the former case, corner points are transmitted at equal power levels regardless of modulation type, while in the latter, the signal is transmitted at equal mean power levels regardless of modulation type.

4.4.1.4 Channel Quality Measurements

The receive signal strength indicator (RSSI) and the carrier-to-interference-and-noise ratio (CINR) signal quality measurements and associated statistics can aid in such processes as BS selection/assignment and burst adaptive profile selection. Because channel behavior is time variant, both the mean and the standard deviation are defined. The process by which RSSI measurements are taken does not necessarily require receiver demodulation lock; for this reason, RSSI measurements offer reasonably reliable channel strength assessments even at low signal levels. On the other hand, although CINR measurements require receiver lock, they provide information on the actual operating conditions of the receiver, including interference and noise levels, and signal strength. When collection of RSSI measurements is mandated by the BS, an SS obtains an RSSI measurement from the DL burst preambles. From a succession of RSSI measurements, the SS derives and updates estimates of the mean and the standard deviation of the RSSI. In the case of CINR, the SS obtains CINR measurements.

4.4.2 WirelessMAN-SCa PHY

The WirelessMAN-SCa PHY is based on single-carrier technology and is designed for NLOS operation in frequency bands below 11 GHz. For licensed bands, channel bandwidths allowed are limited to the regulatory provisioned bandwidth divided by any power of 2, but no less than 1.25 MHz. The terms *payload*, *burst*, *burst set*, *burst frame*, and *MAC frame* are used in this specification. Their details are as follows:

- Payload refers to individual units of transmission content that are of interest to some entity at the receiver.
A burst contains payload data and is formed according to the rules specified by the burst profile associated with the burst. The existence of the burst is made known to the receiver through the contents of either the UL or DL maps. For the UL, a burst is a complete unit of transmission that includes a leading preamble, encoded payload, and trailing termination sequence.

A burst set is a self-contained transmission entity consisting of a preamble, one or more concatenated bursts, and a trailing termination sequence. For the UL, burst set is synonymous with burst.

A burst frame contains all information included in a single transmission. It consists of one or more burst sets.

A MAC frame refers to the fixed bandwidth intervals reserved for data exchange. For TDD, a MAC frame consists of one DL and one UL subframe, delimited by the TTG. For FDD, the MAC frame corresponds to the maximum length of the DL subframe. FDD UL subframes operate concurrently with DL subframes but on a separate (frequency) channel. The DL and UL subframes each hold a burst frame.

4.4.2.1 Transmit Processing

Figure 4.20 illustrates the steps involved in transmit processing. Source data are first randomized and then FEC encoded and mapped to QAM symbols. QAM symbols are framed within a burst set, which typically introduces additional framing symbols. Symbols within a burst set are multiplexed into a duplex frame, which may contain multiple bursts. The

![Figure 4.20](image_url)
I and Q symbol components are band-limited using pulse-shaping filters, quadrature modulated up to a carrier frequency, and amplified with power control so that the proper output power is transmitted.

Except where indicated otherwise, transmit processing is the same for both the UL and DL. Source bits, that is, the original information bits prior to FEC encoding, are randomized during transmission. Frame control header (FCH) payloads are encoded. Adaptive modulation and the concatenated FEC are supported for all other payloads.

The modulations supported by this specification are tabulated in Table 4.4. With the exception of spread binary phase shift keying (BPSK), FEC-encoded bits are mapped directly to a modulation constellation using one of the constellation maps. Since multiple mappings are defined for several specified modulation schemes, the appropriate FEC and code rate description are chosen to determine the specific mapping to be used.

Both DL and UL data are formatted into framed burst sets. The DL supports one or more framed TDM burst sets, while the UL supports framed TDMA burst sets. The format used by a burst set is indicated by the burst set frame type burst profile encoding (on UL) and extended IE (on DL). Three formats are defined. The standard format is supported on both the UL and DL. This format is always used for data containing the FCH. Support of at least one of these two duplexing modes (FDD and TDD) is mandatory. FDD SSs may be half-duplex FDD (H-FDD).

### Table 4.4

<table>
<thead>
<tr>
<th>Modulation</th>
<th>UL</th>
<th>DL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spread BPSK</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>BPSK</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>QPSK</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>16QAM</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>64QAM</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>256QAM</td>
<td>Optional</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Source: [5].
4.4.2.2 Channel Quality Measurements

BS selection/assignment and burst adaptive profile selection can be done with aid of RSSI and CINR signal quality measurements and associated statistics.

When collection of RSSI measurements is mandated by the BS, an SS obtains an RSSI measurement from the DL burst set preambles. From a succession of RSSI measurements, the SS derives and update estimates of the mean and the standard deviation of the RSSI and reports them via REP-RSP messages. In the case of CINR, a succession of CINR measurements is taken. The method used to estimate the CINR of a single message is left to individual implementation, but the relative and absolute accuracy of a CINR measurement derived from a single message is ±1 and ±2 dB, respectively, for all input CINRs above 0 dB.

4.4.3 WirelessMAN-OFDM PHY

The WirelessMAN-OFDM PHY is based on OFDM modulation and is designed for NLOS operation in the frequency bands below 11 GHz. It uses a 256-point transform and access is by TDMA. This air interface is mandatory for license-exempt bands [13].

4.4.3.1 OFDM Symbol Description

Inverse Fourier transforming creates the OFDM waveform. This time duration is referred to as the useful symbol time $T_b$. A copy of the last $T_g$ of the useful symbol period, the CP, is used to mitigate multipath while maintaining the orthogonality of the tones. Figure 4.21 illustrates this structure in the time domain.

The frequency domain description includes the basic structure of an OFDM symbol. The OFDM symbol shown in Figure 4.22 is made up from subcarriers, the number of which determines the FFT size used. There are three subcarrier types:

- Data subcarriers for data transmission;
- Pilot subcarriers for various estimation purposes;
Null subcarriers for no transmission at all, for guard bands, nonactive subcarriers, and the DC subcarrier.

The purpose of the guard bands is to enable the signal to naturally decay and create the FFT “brick wall” shaping. Subcarriers are nonactive only in the case of subchannelized transmission by an SS.

4.4.3.2 Channel Coding
Channel coding is composed of three steps:

- Randomization;
- FEC;
- Interleaving.
They are applied in this order at transmission. The complementary operations are applied in reverse order at reception.

**Randomization**

Data randomization is performed on each burst of data on the DL and UL. The randomization is performed on each allocation (DL or UL), which means that for each allocation of a data block (subchannels on the frequency domain and OFDM symbols on the time domain), the randomizer is used independently. If the amount of data to transmit does not fit exactly the amount of data allocated, padding of 0xFF (“1” only) is added to the end of the transmission block for the unused integer bytes.

**FEC**

An FEC, consisting of the concatenation of a Reed-Solomon outer code and a rate-compatible convolutional inner code, is supported on both UL and DL. Support of BTC and convolutional turbo codes (CTCs) is optional.

**Interleaving**

All encoded data bits are interleaved by a block interleaver, with a block size corresponding to the number of coded bits per the allocated subchannels per OFDM symbol, $N_{c/bps}$. The interleaver is defined by a two-step permutation. The first ensures that adjacent coded bits are mapped onto nonadjacent subcarriers. The second permutation ensures that adjacent coded bits are mapped alternately onto less or more significant bits of the constellation, thus avoiding long runs of lowly reliable bits.

After bit interleaving, the data bits are entered serially to the constellation mapper. BPSK, Gray-mapped QPSK, 16QAM, and 64QAM are supported, whereas the support of 64QAM is optional for license-exempt bands. Pilot subcarriers are inserted into each data burst to constitute the symbol, and they are modulated according to their carrier location within the OFDM symbol.
4.4.3.3 Control Mechanism

**Synchronization**

For TDD and FDD realizations, it is recommended (but not required) that all BSs be time synchronized to a common timing signal. In the event of the loss of the network timing signal, BSs may continue to operate and automatically resynchronize to the network timing signal when it is recovered. For both FDD and TDD realizations, frequency references derived from the timing reference may be used to control the frequency accuracy of BSs, provided that they meet the frequency accuracy requirements.

**Ranging**

There are two types of ranging processes: initial ranging and periodic ranging. Initial ranging (coarse synchronization) and power control are performed during two phases of operation: during (re)registration and when synchronization is lost and during transmission on a periodic basis. Initial ranging uses the initial ranging contention-based interval, which requires a long preamble. The periodic ranging uses the regular UL burst. During registration, a new subscriber registers during the random access channel, and, if successful, it is entered into a ranging process under control of the BS. The ranging process is cyclic in nature, with default time and power parameters used to initiate the process, followed by cycles in which (re)calculated parameters are used in succession until parameters meet acceptance criteria for the new subscriber. Ranging on reregistration follows the same process as new registration.

**Band Requesting**

There may be two types of REQ regions in a frame. These two types are REQ region-full and REQ region-focused. In a REQ region-full, when subchannelization is not active, each transmit opportunity consists of a short preamble and one OFDM symbol using the most robust mandatory burst profile. When subchannelization is active, the allocation is partitioned into transmission opportunities (TOs) both in frequency and in time. The width (in subchannels) and length (in OFDM symbols) of each TO is defined in the UCD message defining. The transmission of an SS contains a subchannelized preamble corresponding to the TO chosen,
followed by data OFDM symbols using the most robust mandatory burst profile. In a REQ region-focused, a station sends a short code over a TO that consists of four subcarriers by two OFDM symbols. Each TO within a frame is indexed by consecutive TO indices. The first occurring TO is indexed 0.

**Power Control**

As with frequency control, a power control algorithm is supported for the UL channel with both an initial calibration and a periodic adjustment procedure without loss of data. The objective of the power control algorithm is to bring the received power density from a given subscriber to a desired level. The received power density is defined as total power received from a given subscriber divided by the number of active subcarriers. When subchannelization is not employed, the number of active subcarriers is equal for all the subscribers, and the power control algorithm brings the total received power from a given subscriber to the desired level. The BS should be capable of providing accurate power measurements of the received burst signal. When subchannelization is employed, the SS maintains the same transmitted power density unless the maximum power level is reached.

4.4.3.4 Channel Quality Measurements

As with the previous two PHY specifications, RSSI and CINR are used for signal quality measurement. Implementation of the RSSI and CINR statistics and their reports is mandatory. Here, an SS obtains RSSI and CINR measurements from the OFDM DL preambles and reports them via REP-RSP messages.

4.4.4 WirelessMAN-OFDMA PHY

This uses OFDMA with a 2,048-point transform [11] and is designed for NLOS operation in the frequency bands below 11 GHz. For licensed bands, channel bandwidths allowed are limited to the regulatory provisioned bandwidth divided by any power of 2 but no less than 1.0 MHz. In the OFDMA mode, the active subcarriers are divided into subsets of subcarriers; each subset is termed a subchannel. In the DL, a
subchannel may be intended for different receivers (or groups of receivers); in the UL, a transmitter may be assigned one or more subchannels, and several transmitters may transmit simultaneously. The subcarriers forming one subchannel may be, but need not be, adjacent. The concept is shown in Figure 4.23.

4.4.4.1 OFDMA Ranging

When used with the WirelessMAN-OFDMA PHY, the MAC layer defines a single ranging channel. This ranging channel is composed of one or more groups of six adjacent subchannels, where the groups are defined starting from the first subchannel. Optionally, the ranging channel may be composed of eight adjacent subchannels using the symbol structure. Users are allowed to collide on this ranging channel. To effect a ranging transmission, each user randomly chooses one ranging code from a bank of specified binary codes. These codes are then BPSK modulated onto the subcarriers in the ranging channel, one bit per subcarrier. The initial ranging transmission is used by any SS that wants to synchronize to the system channel for the first time. An initial ranging transmission is performed during two consecutive symbols. The same ranging code is transmitted on the ranging channel during each symbol, with no phase discontinuity between the two symbols. Periodic ranging transmissions are sent periodically for system periodic ranging. Bandwidth request transmissions are for requesting UL allocations from the BS. These

![Figure 4.23 OFDMA frequency description (three-channel schematic example).](image-url)
transmissions are sent only by the SSs that have already synchronized to the system.

4.4.4.2 Channel Coding

Channel coding procedures include randomization, FEC encoding, bit interleaving, and modulation. When repetition code is used, allocation for the transmission always includes an even number of adjacent subchannels. The basic block passes the regular coding chain where the first subchannel set the randomization seed, and the data follow the coding chain up to the mapping. The channel coding process for regular and repetition coding transmission is depicted in Figure 4.24.

The data output from the modulation is mapped onto the block of subchannels allocated for the basic block and then is also mapped onto the allocated subchannels.

Randomization

Data randomization is performed on data transmitted on the DL and UL. The randomization is initialized on each FEC block (using the first subchannel offset and OFDMA symbol offset on which the FEC block is

![Diagram of channel coding process for regular and repetition coding transmission.](image)
mapped; symbol offset, for both UL and DL, is counted from the start of the frame, where the DL preamble is count 0). If the amount of data to transmit does not fit exactly the amount of data allocated, padding of 0xFF (“1” only) is added to the end of the transmission block, up to the amount of data allocated.

**Encoding**

The encoding block size depends on the number of subchannels allocated and the modulation specified for the current transmission. Concatenation of a number of subchannels is performed to make larger blocks of coding where it is possible, with the limitation of not passing the largest block under the same coding rate.

The interleaving and modulation are done as they were in the OFDM specification. Channel quality measurement is implemented by using RSSI and CINR measurements as specified in earlier subsections.

### 4.5 FBWA Deployment Issues

From all the discussions in this chapter it can be said that because of the fast, simple, and less expensive deployment capability, FBWA is known to be a promising alternative technology to existing copper line asymmetric digital subscriber loop (ADSL) or hybrid fiber-coaxial (HFC) cable broadband services. However, efficient system planning and resource allocation policies are warranted for such systems, because in addition to the challenges posed by the dynamic nature of wireless links, interference resulting from aggressive frequency reuse is a major design concern. Therefore, resource allocation strategies will a play major role for the successful evolution of FBWA [17].

WiMAX is all set to supplant Wi-Fi, but for WiMAX to enjoy the level of mass-market deployments experienced by Wi-Fi, the cost of CPE should drop sharply and come under the affordable range of common people. But the experts say that “extra performance comes at the cost of high price” [18]. To reach the target of lower cost, the network must be simple to deploy, the backbone should rely on IP technology, and the network architecture must be simplified compared to current cellular
systems. The first deployment is likely to happen in bands around 3.5 GHz [19].

4.6 Conclusions

The cost and complexity associated with traditional wired cable and telephone infrastructure have resulted in significant broadband coverage holes. The early attempts to use the wireless technology could not provide economy-of-scale coverage due to lack of a standard and interoperability. The introduction of the IEEE 802.16 standard with its flexibility, scalability, QoS, cost effectiveness, and fast deployment facilitates the growth of broadband wireless markets everywhere. Equipment vendors, carriers, and end users will benefit from this. As a result, customers in remote areas will be able to enjoy the broadband wireless coverage. The abolition of the LOS requirement between transmitting and receiving antennas is the key feature of FBWA, and this will enable the introduction of indoor, self-install WiMAX modems [18].

Although FBWA shows great promise to uplift the broadband wireless system connectivity, it still needs some improvements to correct its flaws in order to prevent security threats. The security sublayer at the bottom of the MAC is implemented as the privacy sublayer. Learning from the mistakes of the IEEE 802.11 standard, the working group used a pre-existing standard Data Over Cable Service Interface Specification (DOCSIS) that was designed to solve the last-mile problem in cabled networks. Changes were made in the DOCSIS system design so that it could be used by BWA systems. However, the DOCSIS initially designed for cable modems failed to properly protect the 802.16 link, which is wireless [14, 15]. An SS has a unique certificate that is authenticated by the BS during the authorization process. The BS’s certificate is not defined, so cross and mutual authentication is not possible. This provides threats to the subscriber’s device [15]. Also, only the MAC PDU payload is encrypted, while the generic MAC header and CRC are not encrypted. The encryption algorithm used by 802.16 is relatively weak and is susceptible to threat. The initialization vector used by 802.16 is predictable, which further weakens the confidentiality of the data. The new draft
802.16e that supports MBWA as well tries to address the existing security concerns [20].

References


5 Mobile Broadband Wireless Access

5.1 Introduction

Mobile broadband wireless access (MBWA) is touted as the holy grail of ubiquitous mobile broadband access anywhere, any time, and from any device. Additionally, it is envisioned that MBWA would potentially bridge the coverage gaps of currently deployed cellular systems with broadband data capabilities and guaranteed QoS, including the extension of the limited range and coverage of WLANs [1–11].

The requirements and specifications for MBWA systems continue to be either developed or enhanced by numerous local/global standards bodies [such as the ITU, IEEE, 3GPP and 3GPP2, Association of Radio Industries and Businesses (ARIB), Telecommunication Technology Association (TTA), Telecommunication Technology Committee (TTC), and many others], consortia [WiMAX, WiBro, the Alliance for Telecommunications Industry Solutions (ATIS), and so forth], and other forums around the world. The forerunners among these systems under considerations are IEEE 802.16e–based systems (WiMAX and WiBro). Unfortunately for IEEE 802.16e–based systems, they face numerous hurdles in realizing their potential, that is, in attaining the status of de facto standard for mobile broadband access, for both voice and data. Although the
systems represent technology that has been developed from the ground up to fulfill broadband data needs, service providers still must build infrastructure to support them, and consumers must adopt them to pay for the huge deployment and buildup costs for ubiquitous coverage.

Although this book deals mainly with the specifications of the IEEE 802.16e–based protocols, it is nonetheless important to understand the present landscape of the wireless mobile broadband offerings and contemporary systems, which present a formidable competition to IEEE 802.16e–based systems. The success of systems based on IEEE 802.16e specifications depend on many factors, and only time will script their real potential and success story. Meanwhile, advanced services offerings based on 3GPP2 CDMA2000 1xEV-DO Revision 0 and 3GPP–based HSDPA have been picking up great momentum over the past few years. Each promises average throughputs of 400 to 700 Kbps, allowing service providers to offer VoIP, enhanced data throughput with differentiated QoS, agile web browsing, and location-based services, including real-time video streaming and content delivery.

Additionally, in 3GPP2-based 1xEV-DO Revision 0 and Release A standards, air interfaces are optimized for broadband packet data throughput and incorporate a number of advanced technologies [such as diversity receivers, beam forming (BF), HARQ, MIMO, and adaptive modulation and coding (AMC) schemes] that significantly enhance spectral efficiency and data throughput. The EV-DO is being widely deployed in the United States, but there is already anticipation for Release A, which delivers 3.1 Mbps on the DL and 1.8 Mbps on the UL. Planned enhancements of the air interface in the form of 1xEV-DO Release B will bundle multiple 1.25-MHz channels to provide significant bandwidth gains, which can theoretically attain 70 Mbps with 20 MHz of spectrum. In fact, Release B essentially would place the CDMA2000 3G system at par with WiMAX without the overhead of building a complete new infrastructure, since CDMA2000 cellular operators already have the basic infrastructure deployed. Figure 5.1 depicts the evolution of 3G cellular systems, including their DL and UL capabilities.

The evolution of prominent 2G systems [GSM and Interim Standard 95 (IS-95)] has been consistently enhancing the air interface (PHY and MAC layers) to provide increasingly superior data capability for
Figure 5.1 3G cellular systems evolution.
systems built primarily for voice applications. Tables 5.1 and 5.2 provide a comparative view of these two systems and their evolution toward attaining equality with landline systems (such as T1/E1 connectivity).

It can be inferred from Table 5.2 that 3G systems are constantly evolving toward better data throughput and a differentiated class of service.

This chapter describes the mobile version of the IEEE 802.16 standard. A brief introduction of the standard is provided in Section 5.2. Section 5.3 deals with enhancements for mobility in the IEEE 802.16e standard. The MAC and PHY layer specifications are described in detail in the IEEE 802.16-2004 and IEEE 802.16e standards, so only the salient features are covered here. IEEE 802.16e [1] incorporates MAC enhancements for mobility, and Section 5.4 describes the MAC enhancements. Section 5.5 presents the MAC protocol in detail. Section 5.6 provides the PHY layer description, especially the SOFDMA scheme, which provides the required scalability to support various bandwidths without any change in the upper layer. Finally, conclusions are given in Section 5.7.

### Table 5.1
Evolution of 2G Systems (Voice-Centric) Towards 3G Systems
(Primarily Broadband Data Capabilities)

<table>
<thead>
<tr>
<th></th>
<th>IS-95/CDMA2000</th>
<th>GSM/WCDMA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FL</td>
<td>DO Revision 0</td>
</tr>
<tr>
<td>Peak data rate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS-95</td>
<td>FL</td>
<td>DO Revision 0</td>
</tr>
<tr>
<td>CDMA2000 1x</td>
<td>14.4</td>
<td>2.4 Mbps</td>
</tr>
<tr>
<td>Kbps</td>
<td>153 Kbps</td>
<td>9.6 Kbps</td>
</tr>
<tr>
<td></td>
<td>153 Kbps</td>
<td>9.6 Kbps</td>
</tr>
<tr>
<td></td>
<td>240 Kbps</td>
<td>240 Kbps</td>
</tr>
<tr>
<td></td>
<td>384 Kbps</td>
<td>384 Kbps</td>
</tr>
<tr>
<td>Typical data rate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS-95</td>
<td>FL</td>
<td>DO Revision 0</td>
</tr>
<tr>
<td>CDMA2000 1x</td>
<td>9 Kbps</td>
<td>400 to 700 Kbps</td>
</tr>
<tr>
<td>Kbps</td>
<td>60 to 100 Kbps</td>
<td>6 Kbps</td>
</tr>
<tr>
<td></td>
<td>40 Kbps</td>
<td>20 to 40 Kbps</td>
</tr>
<tr>
<td></td>
<td>250 to 300 Kbps</td>
<td>90 Kbps</td>
</tr>
<tr>
<td>Latency</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FL</td>
<td>DO Revision 0</td>
</tr>
<tr>
<td>IS-95</td>
<td>150 ms+</td>
<td>150 ms+</td>
</tr>
<tr>
<td>CDMA2000 1x</td>
<td>150 ms+</td>
<td>100 ms+</td>
</tr>
<tr>
<td>Latency</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>150 ms+</td>
<td>100 ms+</td>
</tr>
</tbody>
</table>

Note: GPRS = general packet radio services.
The relevant features of FBWA (IEEE 802.16-2004 [2]) were presented in Chapter 4. The IEEE 802.16-2004 standard was built from the ground up to support broadband data connectivity for the fixed environment. This standard was primarily developed to solve broadband backhaul connectivity issues as well as to provide quickly deployable hot spot coverage and to accommodate unserved areas in a cost-effective and logistics-friendly manner, but it did not support any mobility requirements. In December 2002, a working group was formed under the premise of IEEE 802.16e [1] to include mobility to complement the offerings of the IEEE 802.16a system below 6 GHz of spectrum. The final version of IEEE 802.16e was ratified and published in December 2005. Since the IEEE 802.16 family of standards deals only with the PHY and MAC layers and does not provide the end-to-end system specifications and device interoperability requirements, the WiMAX Forum was formed to bridge this gap. WiMAX Forum was formed to establish interoperability requirements and to promote industry-wide collaboration to reduce the cost of IEEE 802.16e-compliant devices [1] and to allow quick deployment of services. It is envisioned that WiMAX in the WMAN context would play a role similar to that of Wi-Fi in WLANs.

### Table 5.2
Long-Term Evolution of 3G Systems (Broadband Data Capabilities with Low Latency and High Spectral Efficiency)

<table>
<thead>
<tr>
<th></th>
<th>CDMA2000 Evolution</th>
<th>WCDMA Evolution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DO Revision A</td>
<td>DO Revision B</td>
</tr>
<tr>
<td><strong>Peak data rate</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FL</td>
<td>3.1 Mbps</td>
<td>9.3 Mbps (3x)</td>
</tr>
<tr>
<td>RL</td>
<td>1.8 Mbps</td>
<td>5.4 Mbps (3x)</td>
</tr>
<tr>
<td><strong>Typical data rate</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FL</td>
<td>500 to 900 Kbps</td>
<td>1.5-2.7 Mbps (3x)</td>
</tr>
<tr>
<td>RL</td>
<td>600 Kbps</td>
<td>1.8 Mbps (3x)</td>
</tr>
<tr>
<td><strong>Latency</strong></td>
<td>30 ms+</td>
<td>30 ms+</td>
</tr>
</tbody>
</table>

*Note: HSUPA = high-speed uplink packet access.*

#### 5.2 IEEE 802.16e Standard

The relevant features of FBWA (IEEE 802.16-2004 [2]) were presented in Chapter 4. The IEEE 802.16-2004 standard was built from the ground up to support broadband data connectivity for the fixed environment. This standard was primarily developed to solve broadband backhaul connectivity issues as well as to provide quickly deployable hot spot coverage and to accommodate unserved areas in a cost-effective and logistics-friendly manner, but it did not support any mobility requirements. In December 2002, a working group was formed under the premise of IEEE 802.16e [1] to include mobility to complement the offerings of the IEEE 802.16a system below 6 GHz of spectrum. The final version of IEEE 802.16e was ratified and published in December 2005. Since the IEEE 802.16 family of standards deals only with the PHY and MAC layers and does not provide the end-to-end system specifications and device interoperability requirements, the WiMAX Forum was formed to bridge this gap. WiMAX Forum was formed to establish interoperability requirements and to promote industry-wide collaboration to reduce the cost of IEEE 802.16e-compliant devices [1] and to allow quick deployment of services. It is envisioned that WiMAX in the WMAN context would play a role similar to that of Wi-Fi in WLANs.
5.3 IEEE 802.16e Enhancements for Mobility

The IEEE 802.16e air interface is spruced up to support dynamic radio channels to counter fast-varying channels in mobile environment. Several amendments to PHY and MAC layers have been incorporated to support roaming, handoff, swift power control, and flexibility to adapt to the dynamic mobile environments. The standard is designed to accommodate either TDD or FDD deployments, allowing for both full- and half-duplex terminals in the FDD case.

To accommodate unpredictable channel conditions as well as the variations in the spectrum availability across various geographical regions, it uses SOFDMA. SOFDMA is a variant of OFDMA that allows for a variable number of subcarriers, based on the available bandwidth, without affecting the subcarrier spacing and other values that affect the higher-layer processing. This allows for flexibility in resource allocations, basing them on the channel condition and spectrum availability for an individual user in a particular geographic location. In addition, several other enhancements such as support for MIMO, AASs, DFS, AMC, HARQ, and fast channel feedback [channel quality indication channel (CQICH)] as well as enhanced security features have been added for reliable and robust user experience.

To enhance the spectral efficiency of the air interface, higher-order modulation schemes (such as 64QAM) have been provisioned for both DL and UL. In addition to convolutional coding, turbo coding with a variable code rate and repetition and support for LDPC coding have been added as well. Various diversity techniques such as space-time coding have been included to improve NLOS performance and to extend the range and the throughput in fringe areas of coverage.

SOFDMA allows a wide range of flexibility in addressing the need for wide variation in spectrum allocation and user/operator preferences. The scalability is inherently supported by adjusting the FFT bin size while fixing the subcarrier frequency spacing. Since the subcarrier bandwidth and symbol duration is fixed, the impact to the upper layers is minimized to a great extent.

The SOFDMA modulation scheme makes IEEE 802.16e [1] systems backward incompatible to the FBWA IEEE 802.16-2004 specification, which is of little concern because it would require multimode user
equipment for roaming between fixed and mobile BWA systems based on the IEEE 802.16 family of standards.

Table 5.3 depicts the scalability parameters for the SOFDMA modulation scheme employed by the IEEE 802.16e standard [1], and Table 5.4 depicts supported DL and UL modulation and coding schemes for various profiles based on the IEEE 802.16e [1] standard.

IEEE 802.e profiles allow for numerous combinations of modulation and coding schemes to provide higher granularity of data rate to end users and service providers, as shown in Tables 5.5 and 5.6 for the 5- and 10-MHz bandwidths. The parameters depicted in the tables are for a frame duration of 5 ms, which contains 48 OFDM symbols, of which 44 are for data and the rest for pilot and guard band usage.

Due to the lack of harmonized frequency allocation for this new service, IEEE 802.16 has created many system profiles covering wide frequency bands, channel bandwidths, and duplexing schemes to allow for wider deployment and to support economy of scale. The initial profile based on the 3.5-GHz spectrum was created to accommodate the wide availability of this frequency band across the globe. Additionally, to provide fixed services in the license-exempt band, a 5.8-GHz spectrum profile was created as well to fill the demand for low-cost broadband services. To support the demand for mobile services in the MMDS band in the

<table>
<thead>
<tr>
<th>System Parameters</th>
<th>Numerology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel bandwidth (MHz)</td>
<td>1.25 5 10 20</td>
</tr>
<tr>
<td>Sampling frequency (MHz)</td>
<td>1.4 5.6 11.2 22.4</td>
</tr>
<tr>
<td>FFT size (NFFT)</td>
<td>128 512 1,024 2,048</td>
</tr>
<tr>
<td>Number of subchannels</td>
<td>2 8 16 32</td>
</tr>
<tr>
<td>Subcarrier frequency spacing</td>
<td>10.94 kHz</td>
</tr>
<tr>
<td>Useful symbol time (Tb = 1/f)</td>
<td>91.4 μs</td>
</tr>
<tr>
<td>Guard time (Tg = Tb/8)</td>
<td>11.4 μs</td>
</tr>
<tr>
<td>OFDMA symbol duration (Ts = Tb + Tg)</td>
<td>102.9 μs</td>
</tr>
<tr>
<td>Number of OFDMA symbols (5 ms)</td>
<td>48</td>
</tr>
</tbody>
</table>

Source: [3].
United States and Korea, it has also created two additional profiles in 2.5- and 2.3-GHz bands, respectively. Table 5.7 provides the details of the new profiles, which accommodate the MMDS bands in the United States and South Korea.

It is expected that the early version of the deployment would incorporate only minimal feature sets (such as best effort high-speed web access services in the beginning and enhanced real-time and guaranteed QoS capabilities to follow later) to get in the market, with new capabilities to be added as the services and offerings become popular and demand for them grows.

<table>
<thead>
<tr>
<th>Modulation</th>
<th>Downlink</th>
<th>Uplink</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>QPSK, 16QAM, 64QAM</td>
<td>QPSK, 16QAM, 64QAM</td>
</tr>
<tr>
<td>Code rate</td>
<td>Convolution code 1/2, 2/3, 3/4, 5/6</td>
<td>1/2, 2/3, 5/6</td>
</tr>
<tr>
<td></td>
<td>Turbo code 1/2, 2/3, 3/4, 5/6</td>
<td>1/2, 2/3, 5/6</td>
</tr>
<tr>
<td>Repetition</td>
<td>×2, ×4, ×6</td>
<td>×2, ×4, ×6</td>
</tr>
</tbody>
</table>

Table 5.5
System Parameters with Partially Used Subchannelization (PUSC) Subchannel

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Downlink 5 MHz</th>
<th>Downlink 10 MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>System bandwidth</td>
<td>5 MHz</td>
<td>10 MHz</td>
</tr>
<tr>
<td>FFT size</td>
<td>512</td>
<td>1,024</td>
</tr>
<tr>
<td>Null subcarriers</td>
<td>92</td>
<td>104</td>
</tr>
<tr>
<td>Pilot subcarriers</td>
<td>60</td>
<td>136</td>
</tr>
<tr>
<td>Data subcarriers</td>
<td>360</td>
<td>272</td>
</tr>
<tr>
<td>Subchannels</td>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td>Symbol period $T_s$</td>
<td>102.9 $\mu$s</td>
<td></td>
</tr>
<tr>
<td>Frame duration</td>
<td>5 ms</td>
<td></td>
</tr>
<tr>
<td>OFDM symbols/frame</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td>Data OFDM symbols</td>
<td>44</td>
<td></td>
</tr>
</tbody>
</table>
5.4 IEEE 802.16e MAC Enhancements

The original IEEE 802.16 MAC was built from the ground up to support broadband data services based on the time-tested data over cable service interface specification (DOCSIS) specifications. From the onset it was
designed to accommodate a variety of PHY specifications to address the needs of bursty data traffic, low-latency VoIP, and streaming video content. The MAC was primarily developed for PMP communication in a wireless environment. The support for higher-layer protocols such as ATM, Ethernet, or IP was built in, as was the provisioning to accommodate not yet developed future protocols. The MAC is designed for a truly broadband physical layer while delivering ATM-compatible QoS, UGS, rtPS, nrtPS, and best effort. These were discussed in Chapter 4.

The flexibility of the frame structure allows for dynamic adaptation of UL and DL burst profiles to match channel condition. This allows for slot-to-slot resource allocation variation to accommodate specific throughput requirements based on the channel condition being experienced by an individual user. Since the resource allocations to targeted users are conveyed in the MAP messages at the beginning of each frame, the scheduler can effectively change the resource allocation on a frame-by-frame basis to adapt to the dynamic nature of the traffic.

The MAC PDUs are designed to add efficiency and agility to support low-latency and bursty traffic throughput demand. To enable this, MAC allows for a variable-length PDU, including the concatenation of multiple MAC PDUs to reduce the PHY layer overhead. It also allows for the concatenation of multiple SDUs of the same service flow into a single MAC PDU to reduce MAC header overhead. Large SDUs are fragmented to achieve the prescribed level of QoS (especially latency requirements). The PHS is implemented to minimize overhead due to redundant SDU headers, which increases the throughput efficiency.

To reduce the delay and acknowledgment overhead in resource allocation, the 802.16 MAC allows for a self-adjusting bandwidth request/grant scheme. This scheme allows users to request bandwidth depending upon the QoS and traffic parameters of their services. Users can be accessed individually or in groups, and they are allowed to steal resources already allocated or to piggyback on the next request if additional resources are required. In comparison, a majority of contemporary wireless systems employ either collision avoidance or a generalized slotted aloha access scheme with a backoff mechanism for media access, which does not perform well in a relatively loaded cell.
5.5 IEEE 802.16e MAC

This section describes the MAC enhancements to the mobile version of 802.16 [1].

5.5.1 PMP

The IEEE 802.16e MAC [1] is a PMP connection-oriented protocol to support varying degrees of service flow and associated QoS in the context of a transport connection. Every transport connection associates with a service flow, which is used for service negotiation after registration and during the life of the connection. The service flow defines the QoS parameters for the PDUs that are exchanged on the connection. The MAC utilizes the service flow to manage QoS and bandwidth requirements of the UL and DL channels. Transport connection management functions (such as flow establishment, maintenance, and termination) are managed through the use of static and dynamic configurations of service flow connections.

The 48-bit universal MAC address, as defined in IEEE 802-2001, uniquely defines the air interface identity of a particular SS. It is used during the initial ranging and authentication processes to establish the appropriate connections for an SS. Each connection is identified by a 16-bit CID. At initialization, three management connection messages are set up between the BS and the SS to perform three uniquely different types of services. The basic management message is used to exchange short, time-urgent MAC management messages. Conversely, the primary management message is utilized to exchange longer, more delay-tolerant MAC management messages. On top, the secondary management message is intended for delay-tolerant, standards-based [dynamic host configuration protocol (DHCP), trivial file transfer protocol (TFTP), simple network management protocol (SNMP), and so forth] messages. Messages carried on the secondary management connection may be packed and/or fragmented and are required only for a managed SS.
5.5.2 MAC PDU Formats

The 802.16-2004 MAC PDU formats are equally applicable to IEEE 802.16e, except for a few exceptions. Only exceptions are discussed in this section.

5.5.2.1 MAC Header Formats

There is one defined generic MAC header for the DL MAC header, which begins each MAC PDU containing either MAC management messages or CS data. There are two MAC headers defined for UL MAC header formats. The first format has each MAC PDU containing either MAC management messages or CS data (Figure 5.2) and the second (Figure 5.3) is without any payload. For the latter format (usually for signaling), the MAC header is not followed by any MAC PDU payload and CRC.

The details of these header formats can be obtained from [1] (see Figure 5.4). The signaling frame header type I carries the bandwidth request, UL transport power, CINR, CQICH request, PHY header, UL sleep control, and sequence number (SN) reports.

The signaling frame header type II carries feedback information for MIMO control.

![Figure 5.2](image-url)  
*Figure 5.2* Generic frame header. *(From: [1]. © 2006 IEEE. Reprinted with permission.)*
**MAC Header and Special Subheaders**

Six types of subheaders [1] (i.e., extended subheader field, mesh, fragmentation, fast-feedback allocation, and grant management, in order of precedence) are allowed in a MAC PDU with a generic MAC header. If both the fragmentation subheader and the grant management subheader are indicated, the grant management subheader comes first. If the mesh subheader is indicated, it precedes all other subheaders except for the...
extended subheader. In the DL, the fast-feedback allocation subheader always appears as the last per-PDU subheader. The extended subheader field (ESF) bit in the generic MAC header indicates that the extended subheader is present. Using this field, a number of additional subheaders can be used within a PDU. The extended subheader always appears immediately after the generic MAC header and before all other subheaders. All extended subheaders are not encrypted.

**MAC Management Messages**

A predefined set of MAC management messages [1] is carried in the payload of the MAC PDU. All MAC management messages begin with a management message type field and may have additional fields. MAC management messages on the basic, broadcast, and initial ranging connections are neither fragmented nor packed. MAC management messages on the primary management connection may be packed and/or fragmented. MAC management messages on the broadcast connection may be fragmented. For the OFDMA PHY layers, management messages carried on the initial ranging, broadcast, basic, and primary management connections have CRC usage enabled (as shown in Figure 5.5).

**Ranging**  This feature is used to periodically check network round-trip delay and request power and/or DL burst profile settings for the SS/CPE. It is also used between the base transceiver station (BTS) and the SS to maintain RF communications link quality.

**QoS**  Enabling broadband applications, such as VoIP, data, and video, to run simultaneously over the RF link is one of the most compelling features of the QoS designed into WiMAX. This standard specifies multiple service flows and supports VLANs, in addition to several other QoS traits.

**DFS**  DFS is mandatory for operation of license-exempt WiMAX equipment. This feature allows for the assessment of frequency band availability before beginning operations and consequently assists in avoiding the usage of a frequency being used by another end user or service provider.

**Security**  This feature allows for secure operation and traffic flow over the WiMAX network. There are several encryption algorithms designed into
the standard (such as DES, 3DES, AES, and RC4) to accommodate wide varieties of application and service needs.

**AASs** This technique improves the connection and response between the SS and BSs, allowing for better link performance, signal stability, and overall network performance. These “smart” antennas shape the coverage area by beam forming and manage interference, which allows for maximum coverage and throughput between the BS and a particular subscriber or group of subscribers. Suppression of cochannel interference from other locations is another feature of smart antennas. These enhancements are made possible by the increase in processing power provided by the latest digital signal processors (DSPs), application-specific integrated
circuits (ASICs), field programmable gate arrays (FPGAs), and network processors being used in today’s equipment. Intel and TeleCIS have both partnered with ArrayComm on the development of smart antenna technology for BSs for mobile WiMAX.

Although MIMO is often lumped together with smart antenna technology, MIMO requires the placement of multiple radios and multiple antennas at both (transmit and receive) ends.

**Subchannelization** Using subchannelization within WiMAX provides better signal gain and performance on both the UL and DL signals. It allows an SS to concentrate its transmit power on a subset (subchannel) of the total OFDM subcarriers, resulting in coverage and capacity enhancements. Multiple SSs can be scheduled to transmit simultaneously on different subchannels. As mentioned previously, subchannelization is an optional feature within OFDM-256 that is generating much interest from service providers.

Without the use of subchannelization, the UL range is limited and tends to be asymmetrical, restricting the overall performance of the subscriber’s CPE. By providing lower power requirements with the use of subchannelization on UL and DL interfaces, this feature also reduces the cost of CPE systems.

### 5.5.3 Data Delivery Services for Mobile Networks

Data delivery service is associated with a certain predefined set of QoS-related service flow parameters. Data delivery service does not include assignment of specific values to the parameters.

#### 5.5.3.1 Types of Data Delivery Services

The type of data delivery service identifies a specific set of QoS parameters (see Table 5.8).

**UGS**

This type of service is to support real-time applications generating fixed-rate data. This data can be provided as either fixed- or variable-length PDUs.
Real-Time Variable Rate (RT-VR) Service

This service is to support real-time data applications with variable bit rates which require guaranteed data rate and delay.

NRT-VR Service

This QoS profile supports applications that require a guaranteed data rate but are insensitive to delays. It is desirable in certain cases to limit the data rate of these services to some maximum rate.

BE Service

This service is for applications with no rate or delay requirements.

ERT-VR Service

This service is to support real-time applications with variable data rates that require guaranteed data and delay, for example, VoIP with silence suppression.

5.5.4 Sleep-Mode Support for Mobile Stations

Sleep mode is a state in which a mobile station (MS) conducts prenegotiated periods of powerdown to conserve the battery, thus tearing down connection to the serving BS. These periods are characterized by
the unavailability of the MS, as observed from the serving BS, to DL or UL traffic. Sleep mode is intended to enhance the battery life of the MS and allow for efficient usage of resources of the serving BS. Implementation of sleep mode is optional for the MS and mandatory for the BS.

For each involved MS, the BS keeps one or several contexts, each one related to a certain power saving class. A power saving class is a group of connections that have common demand properties. For example, all BE and NRT-VR connections may be marked as belonging to a single class, while two UGS connections may belong to two different classes, if they have different intervals between consequent allocations. A power saving class may be repeatedly activated and deactivated. Activation of a certain power saving class means starting a sleep/listening windows sequence associated with this class. There are three types of power saving classes, which differ by their parameter sets, procedures of activation/deactivation, and policies of MS availability for data transmission.

A power saving class of type I is recommended for BE and NRT-VR types of connections. A power saving class of type II is recommended for UGS and RT-VR types of connections. A power saving class of type III is recommended for multicast connections as well as for management operations, for example, periodic ranging, DSx operations, and so forth. Power saving classes of this type are defined and activated by MOB_SLP-REQ/MOB_SLP-RSP or bandwidth request and UL sleep control header/DL sleep control extended subheader transaction.

Unavailability interval is a time interval that does not overlap with any listening window of any active power saving class. Availability interval is a time interval that does not overlap with any unavailability interval. During an unavailability interval, the BS does not transmit to the MS, so the MS may power down one or more physical operation components or perform other activities that do not require communication with the BS, such as scanning or associating with neighboring BSs. If there is a connection at the MS that is not associated with any active power saving class, the MS is considered available on a permanent basis. During an availability interval, the MS is expected to receive all DL transmissions just as in the normal state of operations (no sleep). In addition, the MS examines the DL channel descriptor (DCD) and UL channel descriptor (UCD) change counts and the frame number of the DL-MAP PHY
synchronization field to ensure synchronization with the BS. Upon detecting a changed DCD and/or UCD count in the DL-MAP, unless using the broadcast control pointer IE for tracking and updating DCD and/or UCD changes, the MS continues reception until receiving the corresponding updated message.

Figure 5.6 is an example of the behavior of an MS with two power saving classes: Class A contains several connections of BE and NRT-VR type, and class B contains a single connection of UGS type. Then, for class A the BS allocates a sequence of listening window of constant size and doubling sleep window. For class B the BS allocates a sequence of listening window of constant size and sleep window of constant size. The MS is considered unavailable (and may power down) within windows of unavailability, which are intersections of sleep windows of classes A and B.

5.5.5 MAC Layer Handover Procedures

An MS capable of performing handover (HO) undergoes predefined procedures. The HO process is used in a number of situations, such as the following:

**Figure 5.6** Example of sleep-mode operations with two power saving classes.
- When the MS moves and (due to signal fading, interference levels, or the like) needs to change the BS to which it is connected in order to provide a higher signal quality;
- When the MS can be serviced with higher QoS at another BS.

A BS broadcasts information about the network topology using the MOB_NBR-ADV message. The message provides channel information for neighboring BSs that is normally provided by each BS’s own DCD/UCD message transmissions. A BS may obtain that information over the backbone network. Availability of this information facilitates MS synchronization with a neighboring BS without the need to monitor transmission from the neighboring BS for DCD/UCD broadcasts. A BS may allocate time intervals to an MS so that it may seek and monitor the suitability of neighbor BSs as targets for HO. The time during which the MS scans for an available BS is referred to as a scanning interval.

5.5.5.1 Association Procedure

Association is an optional initial ranging procedure that occurs during an scanning interval with respect to one of the neighboring BSs. The function of association is to enable the MS to acquire and obtain ranging parameters and service availability information in order to select a proper HO target and/or to expedite a potential future HO to a target BS. Obtained ranging parameters of an associated BS may be further used for setting initial ranging values in future ranging events during actual HO. There are three levels of association, as described below:

Association Level 0: Scan/Association Without Coordination

When this association level is chosen by the network, the serving BS and the MS negotiate about the association duration and intervals. The serving BS allocates periodic intervals during which the MS may range neighboring BSs; however, the target BS has no knowledge of the MS and provides only contention-based ranging allocations. An MS chooses randomly a ranging code from the initial ranging domain of the target
BS and transmits it in the contention-based ranging interval of the target BS.

**Association Level 1: Association with Coordination**

When this association level is chosen, the serving BS provides association parameters to the MS and coordinates association between the MS and neighboring BSs.

**Association Level 2: Network-Assisted Association Reporting**

The MS may request to perform association with network-assisted association reporting by sending the MOB_SCN-REQ message to the serving BS. This message will include a list of neighboring BSs with which the MS wishes to perform association. The serving BS may also request this type of association unilaterally by sending the MOB_SCN-RSP message. The serving BS coordinates the association procedure with the requested neighboring BSs.

Upon completion of an MS’s successful initial ranging of a BS, if the RNG-RSP message contains a service level prediction parameter set to 2, the MS may mark the BS as associated in its MS local association table of identities, recording elements of the RNG-RSP to the MS local association table and setting an appropriate aging timer. The association state in the MS local association table is aged-out after ASC-AGING-TIMER times out and the association entry is removed.

**5.5.5.2 HO Process**

The HO process in which an MS migrates from the air interface provided by one BS to the air interface provided by another consists of the following stages:

- **Cell reselection.** Cell reselection refers to the process of an MS scanning and/or associating with one or more BSs in order to determine their suitability, along with other performance considerations, as an HO target.

- **HO decision and initiation.** An HO begins with a decision for an MS to hand over from a serving BS to a target BS. The decision originates at either the MS or the serving BS.
• **Synchronization to target BS DL.** The MS synchronizes to DL transmissions of the target BS and obtains DL and UL transmission parameters.

• **Ranging.** The MS and target BS conduct initial ranging or HO ranging. If the MS RNG-REQ includes the serving BS identity (BSID), the target BS makes a request to the serving BS for information on the MS over the backbone network, and the serving BS responds. Regardless of whether it has received MS information from the serving BS, the target BS requests MS information from the backbone network. A network reentry proceeds but is shortened by the target BS due to MS information already having been obtained from the serving BS over the backbone network. Depending on the amount of information obtained, the target BS decides to skip one or several network entry steps.

• **Termination of MS context.** This is the final step in the HO process. Termination of the MS context is defined as serving the BS with termination of context of all connections belonging to the MS and the context associated with them.

• **HO cancellation.** An MS may cancel HO at any time prior to expiration of the Resource_Retain_Time interval after transmission of the MOB_HO-IND message.

Figure 5.7 depicts the HO process and its similarity to the initial network entry process.

### 5.5.6 Security Sublayer

The security sublayer provides subscribers with privacy, authentication, or confidentiality across the broadband wireless network. It does this by applying cryptographic transforms to MAC protocol data units (MPDUs) carried across connections between the MS and the BS. In addition, the security sublayer provides operators with strong protection from theft of service, altering, and spoofing of packet. The BS protects against unauthorized access to these data transport services by security enforcement of the associated service flows across the network. The
security sublayer employs an authenticated client/server key management protocol in which the BS, the server, controls distribution of keying material to a client MS. Additionally, the basic security mechanisms are

Figure 5.7 HO and initial network entry.
strengthened by adding digital certificate–based SS device authentication to the key management protocol. Figure 5.8 shows the security sublayer.

5.5.6.1 PKM Protocol
The PKM protocol allows for both mutual authentication and unilateral authentication. IEEE 802.16e supports two PKM protocols:

- PKM version 1 (PKMv1);
- PKM version 2 (PKMv2).

PKMv2 has more enhanced features, such as new key hierarchy, AES-CMAC, AES key wraps, and multicast and broadcast services (MBSs). The PKMv1 protocol is similar to that of a fixed wireless access system as described in Chapter 4; hence, PKMv2 is discussed in this chapter.

Figure 5.8 Security sublayer.
PKMv2

**TEK Exchange Overview for PMP Topology**

If the SS and BS decide “no authorization” as their authorization policy, the SS and BS perform neither the SA-TEK handshake nor the key request/key reply handshake. Upon achieving authorization, an SS starts a separate TEK state machine for each of the SAIDs identified in the authorization reply or PKMv2 SA-TEK-RSP message, if data traffic encryption is provisioned for one or more service flows. Each TEK state machine operating within the SS is responsible for managing the keying material associated with its respective SAID. TEK state machines periodically send key request messages to the BS, requesting a refresh of keying materials for their respective SAIDs. The BS responds to a key request with a key reply message containing the BS’s active keying material for a specific SAID.

**Key Derivation**

The PKMv2 hierarchy defines what keys are present in the system and how the keys are generated. Since there are two authentication schemes, one based on RSA and one based on EAP, there are two primary sources of keying material. The keys used to protect management message integrity and to transport the traffic encryption keys are derived from source key material generated by the authentication and authorization processes. The RSA-based authorization process yields the pre–primary AK (pre-PAK), and the EAP-based authentication process yields the MSK, the shared master key that is derived by the two sides in the course of executing the EAP inner method. Keys used to protect multicast and broadcast service traffic are derived from the multicast and broadcast service AK (MBSAK). These keys form the roots of the key hierarchy.

**Associations**

Keying material is held within associations. There are three types of association: The SA maintains keying material for unicast connections, the group security associations (GSAs) hold keying material used to secure multicast groups, and the multicast and broadcast services group security associations (MBSGSA) hold keying material for MBS services. If the SS
and BS decide “no authorization” as their authorization policies, they do not have any security association.

**Security Context**

The security context is a set of parameters linked to a key in each hierarchy that defines the scope while the key usage is considered to be secure. Examples of these parameters are key lifetime and counters ensuring that the same encryption will not be used more than once. When the context of the key expires, a new key is obtained to continue working.

**Preauthentication**

In anticipation of an HO, an MS may seek to use preauthentication to facilitate an accelerated reentry at a particular target BS. Preauthentication results in establishment of an AK (with a unique AK name) in the MS and target BS.

### 5.6 Physical Layer Description

The mobile WiMAX air interface has adopted OFDMA for improved multipath performance in NLOS environments. SOFDMA [4] is introduced in the IEEE 802.16e Amendment to support scalable channel bandwidths from 1.25 to 20 MHz.

The basics of OFDM are dealt with in detail in Chapter 2. IEEE 802.16-2004 is the basis on which its mobile version was developed as IEEE 802.16e. The four physical modes, including OFDMA, supported by FBWA are described in detail in Chapter 4. An introduction to OFDMA is provided here [5–7], and further enhancements are discussed. OFDMA gives mobile WiMAX the capability to meet the stringent requirements necessary for delivering broadband services in a challenging mobile environment. OFDMA provides multiplexing operation of data streams from multiple users onto the DL subchannels and UL multiple access by means of UL subchannels. Figure 5.9 shows the OFDMA subcarrier structure.

Three types of subcarrier constitute the OFDMA symbol structure:

- Data subcarriers for data transmission;
- Pilot subcarriers for estimation and synchronization purposes;
- Null subcarriers for no transmission, used for guard bands and dc carriers.

Data and pilot carriers are active subcarriers and are grouped into subsets of subcarriers called *subchannels*. Subchannelization is supported in the DL as well as in the UL [4]. Forty-eight data tones (subcarriers), which is equal to one slot duration, is the minimum frequency-time resource allocation unit of subchannelization.

There are two types of subcarrier permutations for subchannelization:

- *Diversity*. Here the subcarriers are drawn pseudo-randomly to form a subchannel. It provides frequency diversity and intercell interference averaging. Diversity permutation performs well in mobile applications.
- *Contiguous*. A block of contiguous subcarriers are grouped together to from a subchannel. Contiguous subcarrier permutations are well suited for fixed, portable, and low-mobility environments.

The option of these two subcarriers permutations enables the system designers to trade off mobility for throughput.

IEEE 802.16e supports multiple PHY modes [8]:

![Figure 5.9 OFDMA subcarrier structure.](image-url)
• Single carrier;
• OFDM 256 FFT;
• OFDM 2,048 FFT;
• SOFDMA 1,024 FFT;
• SOFDMA 512 FFT;
• SOFDMA 128 FFT.

The key difference between the fixed and mobile versions of the IEEE 802.16 standard is an efficient SOFDMA modulation scheme. This difference breaks the compatibility of the mobile 802.16 to the original 802.16-2004 that set the basis for the development of its mobile version. A wide range of bandwidth is supported by SOFDMA, which provides flexibility to address the need for various spectrum allocation and usage model requirements. The FFT size can be adjusted based on the channel and bandwidth; thus, scalability is supported by adjusting the FFT size while the subcarrier frequency spacing remains fixed at 10.94 kHz. Table 5.3 lists the parameters of SOFDMA. SOFDMA can assign a subset of subcarriers to individual users. By using different subcarriers, multiple users can connect at the same time on the same frequency without interference. The number of subcarriers can be adjusted dynamically for different conditions. The Korean version of WiMAX, WiBro, is basically a subset of SOFDMA at 1,024 FFT.

### 5.6.1 TDD Frame Structure

The 802.16e PHY [4] supports TDD and full- and half-duplex FDD operation, but TDD is the preferred duplexing mode, and the initial release of Mobile WiMAX certification profiles will include only TDD. The later releases may consider FDD. To counter interference issues, TDD does require system-wide synchronization. TDD is the preferred duplexing mode for the following reasons:

• TDD ensures channel reciprocity for better support of link adaptation, MIMO, and other closed-loop advanced antenna technologies.
- TDD enables adjustment of the DL/UL ratio to efficiently support asymmetric DL/UL traffic.

- TDD requires only a single channel for both the DL and the UL, providing greater flexibility for adaptation to varied global spectrum allocations.

- Transceiver designs for TDD implementations are less complex and are therefore less expensive.

The OFDM frame structure for a TDD implementation is shown in Figure 5.10. Each frame is divided into DL and UL subframes separated by TTGs and RTGs to prevent collision of DL and UL transmissions. The control information used in the frame are as follows:

![WiMAX OFDMA frame structure](image-url)

**Figure 5.10** WiMAX OFDMA frame structure.
• **Preamble.** The preamble is used for synchronization and it is the first OFDM symbol of the frame.

• **FCH.** The preamble is followed by the FCH, which provides the frame configuration information such as the MAP message length and coding scheme and usable subchannels.

• **DL-MAP and UL-MAP.** Subchannel allocation and other control information for the DL and UL subframes are provided by the DL-MAP and UL-MAP.

• **UL ranging.** The UL ranging subchannel is allocated for the MS to perform closed-loop time, frequency, and power adjustment as well as bandwidth requests.

• **UL CQICH.** The UL CQICH is allocated for the MS to feed back channel-state information.

• **UL ACK.** The UL ACK is allocated for the MS to feed back DL HARQ acknowledge.

### 5.7 Conclusions

IEEE 802.16e is an enhancement and revision of IEEE 802.16-2004 that promises to make mobile wireless Internet access prevalent. The security issues that presented a threat to the FBWA have been resolved in its mobile version.

### References


About the Authors

Uma Shanker Jha is the director of product management for the CDMA technologies division of Qualcomm Inc., and in this capacity he manages next generation products and develops the business strategies and manages the technical road map for these products. Prior to this, he was the chief mobility architect and technical fellow at Boeing and chief technology officer at Airify Corporation. He has had numerous other leading management/technical leadership positions at Morphics, Philips, Rockwell, General Dynamics, and Northrop.

Dr. Jha received a B.S.E.E. from BIT Sindri, India, an M.S.E.E. from California State University at Fullerton, an engineer degree (equivalent to a Ph.D. without a thesis) from the University of Southern California, Los Angeles, and a Ph.D. from Aalborg University, Denmark. He has 12 issued/filed patents and has published more than 20 papers in refereed journals and conference proceedings.

Dr. Jha is a senior member of the IEEE and is a recognized authority in the wireless communication field. He serves on many organizing and technical program committees of IEEE and industry-sponsored conferences and symposia. He is a highly sought-after panelist, keynote speaker, and lecturer on a wide variety of wireless communication topics around the world. Very recently he organized the Ninth Wireless
Personal Multimedia Communication (WPMC) Symposium in San Diego, California, and was the general chair of WPMC 2006.

**Ramjee Prasad** received a B.Sc. (Eng.) from the Bihar Institute of Technology, Sindri, India, and an M.Sc. (Eng.) and a Ph.D. from Birla Institute of Technology (BIT), Ranchi, India, in 1968, 1970, and 1979, respectively. He joined BIT as a senior research fellow in 1970 and became an associate professor in 1980. While he was with BIT, Professor Prasad supervised a number of research projects in the area of microwave and plasma engineering. From 1983 to 1988, he was with the University of Dar es Salaam (UDSM), Tanzania, where he became a professor of telecommunications in the Department of Electrical Engineering in 1986. At UDSM, he was responsible for the collaborative project on satellite communications for rural zones with Eindhoven University of Technology, the Netherlands. From February 1988 through May 1999, Professor Prasad was with the Telecommunications and Traffic Control Systems Group at Delft University of Technology (DUT), where he was actively involved in the area of wireless personal and multimedia communications (WPMC). He was the founding head and program director of the Center for Wireless and Personal Communications at the International Research Center for Telecommunications—Transmission and Radar. Since June 1999, Professor Prasad has been with Aalborg University, where he is the director of the Centre for TeleInFrastruktur and is also the chair of the wireless information and multimedia communications section. He was involved in the European ACTS project FRAMES (Future Radio Wideband Multiple Access Systems) as a DUT project leader. He is a project leader of several international, industrially funded projects. He is the project coordinator of the European sixth framework integrated project titled “My Personal Adaptive Global NET Beyond (MAGNET Beyond).” He has published more than 500 technical papers, contributed to several books, and has authored, coauthored, and edited 19 books: *CDMA for Wireless Personal Communications, Universal Wireless Personal Communications, Wideband CDMA for Third Generation Mobile Communications, OFDM for Wireless Multimedia Communications, Third Generation Mobile Communication Systems, WCDMA: Towards IP Mobility and Mobile Internet, Towards a Global 3G System: Advanced Mobile Communications in Europe (Volumes 1 and 2), IP/ATM*

Professor Prasad has served as a member of the advisory and program committees of several IEEE international conferences. He has also presented keynote speeches, and delivered papers and tutorials on WPMC at various universities, technical institutions, and IEEE conferences. He was also a member of the European cooperation in the scientific and technical research (COST-231) project dealing with the evolution of land mobile radio (including personal) communications as an expert for the Netherlands, and he was a member of the COST-259 project. He was the founder and chairman of the IEEE Vehicular Technology/Communications Society Joint Chapter, Benelux Section, and is now the honorary chairman. In addition, Professor Prasad is the founder and chairman of the IEEE Symposium on Communications and Vehicular Technology (SCVT) in the Benelux, and he was the symposium chairman of SCVT'93.

In addition, Professor Prasad is the coordinating editor and editor-in-chief of the Springer International Journal on Wireless Personal Communications and editorial board member of other international journals. He was the technical program chairman of the PIMRC'94 International Symposium held in The Hague, the Netherlands, September 19–23, 1994, and also of the Third Communication Theory Mini-Conference in Conjunction with GLOBECOM'94, held in San Francisco, California, November 27–30, 1994. He was the conference chairman of the fiftieth IEEE Vehicular Technology Conference and the steering committee chairman of the Second International Symposium for WPMC, both held in Amsterdam, the Netherlands, September 19–23, 1999. He was the
general chairman of WPMC’01, which was held in Aalborg, Denmark, September 9–12, 2001, and of the first International Wireless Summit (IWS 2005) also held in Aalborg, Denmark, September 17–22, 2005.

Professor Prasad was also the founding chairman of the European Center of Excellence in Telecommunications, known as HERMES, and now is the honorary chairman. He is a fellow of IEE, a fellow of IETE, a senior member of IEEE, a member of The Netherlands Electronics and Radio Society (NERG), and a member of IDA (Engineering Society in Denmark).

Professor Prasad is advisor to several multinational companies. He has received several international awards, the latest being the Telenor Nordic 2005 Research Prize.
Index

2.4-GHz ISM, 94
3G cellular systems evolution, 159
3rd Generation Partnership Project (3GPP), 104
3.5-GHz band, 93
5-GHz UNII bands, 93
Access terminals (ATs), 103
Adaptive antenna systems (AASs), 90, 171
Adaptive modulation and coding (AMC) schemes, 158
Advanced Encryption Standard (AES), 133
Application-specific integrated circuits (ASICs), 171–72
Asymmetric digital subscriber loop (ADSL), 153
ATM CS, 118
Automatic repeat request (ARQ), 102
MAC, 123
TDM and, 102
Bit error rate (BER), 42
Bluetooth
concept, 5
defined, 5
frequency-hopping TDD, 6
system characteristics, 6

Broadband
defined, 3
on demand, 113
gap, 111
underserved, 113
wireless landscape, 96–97
worldwide market growth, 114
Broadband Radio Access Network (BRAN), 13
Broadband wireless access (BWA), 85–104
air interface, 100–101
basics, 87–96
considerations, 88–93
deployment considerations, 103
frequency band allocation, 93–94
global deployment, 99–103
interoperability, 99–103
issues, 104
optimized solutions, 85–86
PHY layer, 100–101
PMP applications, 117
proprietary, 92
QoS, 102–3
requirements, xi
spectrum under consideration, 92
survivability, 96
Broadband wireless access (continued)

- technology, 87, 88
- worldwide deployment, 91

Broadcast channel (BCCH), 73

Burst allocation, DL, 139

Capacity, OFDMA, 80–81

Carrier frequency offset, 40–43

Carrier-to-interference-and-noise ratio (CINR), 143, 146

CBC message authentication code (CBC-MAC), 133

CDMA
  - direct sequence, 67
  - frequency-hopping, 67
  - high processing gain and, 100
  - multicarrier, 67

CDMA2000, 22, 97–99

Cell redirection, 177

Cellular backhaul, 113

Channel coding, 71
  - encoding, 152–53
  - FEC, 148
  - interleaving, 148
  - randomization, 148, 152–53
  - steps, 147

Channel quality indication channel (CQICH), 162

Channel quality measurements
  - WirelessMAN-OFDM PHY, 150
  - WirelessMAN-SCa PHY, 146
  - WirelessMAN-SC PHY, 143

Channels
  - coherence bandwidth, 49
  - Rayleigh fading, 48
  - response function envelope, 48

Coding technique, 64

Control mechanism, 149–50
  - band requesting, 149–50
  - power control, 150
  - ranging, 149
  - synchronization, 149

- See also WirelessMAN-OFDM PHY

Counter mode encryption (CTR), 133

Cryptographic methods, 133–35

data encryption, 133

HMAC digest, 134–35

PDU payload format, 133–34

TEK encryption, 134

- See also Security sublayer

Data delivery services, 172–73
  - BE, 173
  - defined, 172
  - ERT-VR, 173
  - NRT-VR, 173
  - RT-VR, 173
  - UGS, 172

- See also MAC (IEEE 802.16e)

Data Encryption Standard (DES), 131

Data Over Cable Service Interface Specification (DOCSIS), 154, 165

Delay spread
  - frequency domain interpretation, 53
  - time domain interpretation, 52

Demand-assigned multiple access (DAMA), 135

Digital divide, 19, 111

Digital signal processors (DSPs), 171

Digital subscriber line (DSL), 14
  - market, 111
  - operators, 111
  - technologies, 113

Digital-to-analog (D/A) converter, 50

Direct sequence spread spectrum (DSSS), 11

Discrete Fourier transform (DFT), 29

DL channel descriptor (DCD), 174

DL media access profile (DL-MAP), 125

DL PHY, 137–41
  - burst allocation, 139
  - FDD subframe structure, 138
  - modulation, 140–41
  - physical medium dependent sublayer, 139–40
  - TDD subframe structure, 138
  - transmission convergence sublayer, 139

- See also WirelessMAN-SC PHY

Doppler shifts, 40–41, 47

Dynamic channel allocation (DCA), 77–80
Index

algorithm, 79–80
frame layout, 79
simple, 80
Dynamic frequency selection (DFS), 100, 170
Dynamic host configuration protocol (DHCP), 167
Encoding, 153

FBWA, xiii, 107–55
  addressable markets, 113
  advantages, 112
  applications, 113–17
  deployment issues, 153–54
  driving factors, 110–17
  infrastructures, 112
  introduction, 107–10
  MAC, 117–35
  market segments, 112–13
  needs, 110–12
  PHY layer, 135–53
  request mechanisms, 124
Federated PNs, 9, 10
Field programmable gate arrays (FPGAs), 172
Fixed broadband wireless access (FBWA).
  See FBWA
Forward error correction (FEC) codes, 64
  channel coding, 148
  selectable types, 140
Frequency band allocation, 93–94
  2.4-GHz ISM, 94
  3.5-GHz, 93
  5-GHz UNII, 93
  MMDS, 94
  WRC, 93–94
Frequency division duplexing (FDD), 19, 125
  bandwidth allocation, 136
  DL subframe structure, 138
  WirelessMAN-SC PHY, 136–37
Frequency-hopping
  OFDMA, 66–67
  pattern, 76–77
  random operation, 76–77
  spread spectrum (FHSS), 11
Frequency offset, 38–43
  carrier, 40–43
  ICI due to, 43
  initial, synchronization, 74
  sampling clock mismatch, 38–40
  between transmitter/receiver, 54
Golay complementary sequences, 64
Group security associations (GSAs), 181
Guard period (GP), 53
  CP in, 58
  symbol extension with, 54
Handover (HO), 175–78
  association procedure, 176–77
  cancellation, 178
  cell redirection, 177
  decision and initiation, 177
  illustrated, 179
  procedures, 175–78
  process, 177–78
  ranging, 178
  stages, 177–78
  See also MAC (IEEE 802.16e)
Hashed message authentication code (HMAC), 128–29
  digest calculation, 134–35
  sequence number, 135
Header formats (MAC), 168–72
  generic, 168
  management messages, 170–72
  subheaders, 169–70
High Performance LAN (HIPERLAN), 13
Hybrid automatic repeat request (HARQ), 99
ICI, 54–59
  eliminate, 57
  loss due to frequency offset, 43
  mitigation of, 57–59
  multipath effect on, 55
  performance degradation due to, 56–57
IEEE 802
  defined, 85
  family, 86
IEEE 802.11 standards, 11–12
IEEE 802.16e standard, 108, 161
IEEE 802.16e standard (continued)
MAC, 167–82
MAC enhancements, 165–66
mobility enhancements, 162–65
systems, 157
See also MBWA
IEEE 802.16 standards, xii, xiii, 17–18, 115
elements, 89
NLOS wireless point-to-multipoint
connections, 116
protocol layering, 109
ratification, 89
salient features, 91
versions, 90
Working Group, 108
IEEE Standards Association (IEEE-SA), 88
Infrastructure
FBWA, 112
wireless networks, 16
Initial acquisition channel (IACH), 73
Integrated Services Digital Network
(ISDN), 88
Integrity check value (ICV), 133
Interference cancellation (IC), 101
Interleaving, 148
International Telecommunication Union
(ITU), 88
Internet Engineering Task Force (IETF), 9
Inverse fast Fourier transform (IFFT), 33
ISI
issues, 50–59
mitigation, 53–54
performance degradation due to, 52–53
Local multipoint distribution system
(LMDS), 99
Low-density parity check codes (LDPC), 101
Low-noise amplifier (LNA), 59
MAC (FBWA), 117–35
ARQ mechanism, 123
authorization, 128
bandwidth allocation, 124
connection identifiers (CIDs), 110
CPS, 119–30
management messages, 120
network entry, 129–30
object model, 127
optimization, 117
PHY layer, 182–86
PHY support, 124–25
for point-to-multipoint (PMP)
aplications, 117
polling, 124
QoS, 125–29
ranging/negotiation of SS capabilities, 129
request mechanisms, 124
scheduling services, 123
security sublayer, 130–35
service class, 127–28
service data units (SDUs), 110
service flow creation, 128
service flow identifiers (SFIDs), 110
service flow management, 128–29
service flows, 125–27
service-specific CS, 118
MAC (IEEE 802.16e), 167–82
data delivery services, 172–73
efficiencies, 165–66
handover procedures, 175–78
header formats, 168–72
MAC PDU formats, 168–72
PMP, 167
security sublayer, 178–82
self-adjusting bandwidth, 166
sleep-mode support, 173–75
MAC PDUs
concatenation, 121
construction and transmission, 121–22
conventions, 121
CRC calculation, 121–22
encryption, 122
formats, 119
fragmentation, 121
IEEE 802.16e formats, 168–72
packing, 121
padding, 122
payload format, 133–34
secure encapsulation, 130
variable-length, 166

MBWA, xiii, 14, 157–86
  introduction, 157–60
  requirements/specifications, 157
See also IEEE 802.16e
Mobile ad hoc networks (MANETs), 9
Mobile broadband wireless access.
  See MBWA
Mobile WiMAX, 95
Modified Bessel function, 49
Modulation
  DL, 140–41
  initial timing, 73–74
  OFDMA, 71–73
Multicast and broadcast services group
  security associations (MBSGSA), 181
Multichannel multipoint distribution
  service (MMDS), 92
  bands, 164, 165
  deployment, 92
Multimedia Mobile Access
  Communication (MMAC), 13
Multipath
  defined, 47
  delay spread, 49
  effect on ICI, 55
  intensity profile, 49
  issues, 46–49
  propagation as Gaussian scatterers, 47
My Personal Adaptive Global Net
  (MAGNET), 7
Nyquist criterion, 52
OFDM
  carrier phase noise, 46
  concept, 30–33
  demodulator, 36
  FFT, 19
  frequency offset, 38–43
  impairment issues, 38
  ISI issues, 50–59
  model, 33–36
  modulator, 35
  multipath issues, 46–49
  PAPR, 59–65
  principle, 30
receiver block diagram, 34
receivers, 31, 40
spectral efficiency, 30
subcarrier spectra, 32
systems/issues, 29–81
time-frequency interpretation, 36–65
timing offset, 43–46
transmitter block diagram, 34
waveform, 101
in WLAN standards, 11
OFDMA, 19, 65–81
  advantages, 68–69
  burst and synchronization requirements, 76
capacity, 80–81
channel coding, 71
dynamic channel allocation, 77–80
frame (TDMA) structure, 70
frequency description, 151–52
frequency-hopping, 66–67
frequency structure, 71, 72
initial frequency offset synchronization, 74
initial modulation timing synchronization, 73–74
modulation, 71–73
power control, 75–76
random frequency-hopping operation, 76–77
ranging, 151–52
scalable (SOFDMA), 90, 160, 162–63
simple dynamic channel allocation, 80
subcarrier structure, 183
synchronization accuracy, 74–75
system description, 67–81
system parameters, 68
time and frequency synchronization, 73
time-frequency grid, 66, 69
OFDM signals, 32
  frequency spectrum, 63
  windowing of, 62
OFDM symbol
  with cyclic extension, 57
description, 146–47
  envelope, 63
extension with guard period, 54
OFDM symbol (continued)
  increases, 40
  index, 39
  mapping, 71
  spectra, 33
  time structure, 147
On-demand connectivity, 114
Orthogonal frequency division multiple-access. See OFDMA
Orthogonal frequency division multiplexing. See OFDM
Orthogonality loss
  due to frequency offset, 43
  due to sampling offset, 41
  due to timing offset, 44–46
Packet CS, 118
PAPR, 59–65
  coding technique, 64–65
  mitigation, 60–65
  peak cancellation technique, 62–64
  signal distortion technique, 61–62
Peak cancellation technique, 62–64
  defined, 62
  illustrated, 64
  See also PAPR
Peak windowing, 61–62
Personal area networks (PANs), 4–6
  defined, 4
  network concept, 6
  See also Wireless PANs
Phase noise, carrier, 46
PHY layer (FBWA), 135–53
  MAC support, 124–25
  mode support, 135
  WirelessMAN-OFDMA PHY, 150–53
  WirelessMAN-OFDM PHY, 146–50
  WirelessMAN-SCa PHY, 143–46
  WirelessMAN-SC PHY, 135–43
  See also FBWA
PHY layer (IEEE 802.16e), 182–86
  multiple mode support, 183–84
  subcarriers, 182–83
  subchannelization, 183
  TDD frame structure, 184–86
Physical medium dependence (PMD)
  DL, 139–40
  UL, 142–43
PKMv2, 180, 181–82
  associations, 181–82
  features, 181
  key derivation, 181
  preauthentication, 182
  security context, 182
  TEK exchange, 181
  See also Privacy and key management (PKM) protocol
PNs
  communicating clusters, 7
  conceptual illustration, 8
  federated, 9, 10
  realization, 9
Point-to-multipoint (PMP)
  BWA, 117
  IEEE 802.16e MAC, 167
Polling, 124
Power amplifier (PA), 59
Power control, 75–76
  closed-loop, 75
  open-loop, 75
  operation in mobile station, 77
  WirelessMAN-OFDM PHY, 150
Power delay profile, 49
Preview, this book, 23–25
Privacy and key management (PKM) protocol, 130, 131–32, 180–82
  security associations, 131
  security capabilities selection, 132
  SS authorization/authorization key exchange, 131–32
  TEK exchange, 132
  See also PKMv2
Public-key encryption algorithm (PkcS1), 131
Quality of service (QoS), 2
  BWA, 102–3
  MAC, 125–29
  MAC management messages, 170
  ParamSet, 126
Random access channel (RACH), 74
Randomization, 148, 152–53
Range
- network types, 4–10
  - transmitted power, 4–15
Rayleigh distribution, 48
Rayleigh fading channel, 48
Receive signal strength indicator (RSSI), 143, 146
Residential broadband, 113
Rician density function, 48
SA identifiers (SAIDs), 131
Sampling clock
  - analog-to-digital (A/D), 38
    - mismatch, 38–40
Sampling offset, loss of orthogonality, 41
Satellites, 14–15
Scalable OFDMA (SOFDMA), 90, 160
  - backward compatibility, 162
    - defined, 162
  - scalability parameters, 163
Scatternets, 6
Scheduling services, MAC, 123
Security sublayer (FBWA), 130–35
  - architecture, 130
    - cryptographic methods, 133–35
    - key management protocol, 131–32
    - secure encapsulation, 130
See also MAC (FBWA)
Security sublayer (IEEE 802.16e), 178–82
  - illustrated, 180
    - PKM protocol, 180–82
See also MAC (IEEE 802.16e)
Service flows, 125–27
  - creation, 128
    - management, 128–29
Signal clipping, 61
Signal distortion technique, 61–62
  - peak cancellation, 62–64
  - peak windowing, 61–62
  - signal clipping, 61
Signaling, wireless networks, 15–16
Signal-to-noise ratio (SNR), 38, 40
Simple network management protocol (SNMP), 167
Sleep-mode support, mobile stations, 173–75
SOHO wireless, 114
Space-time coding (STC), 100
Subchannelization
  - subcarrier permutations, 183
    - within WiMAX, 172
Symbol-scrambling technique, 64–65
Synchronization
  - accuracy, 74–75
  - initial frequency offset, 74
  - initial modulation timing, 73–74
    - requirements, 76
    - time and frequency, 73
WirelessMAN-OFDM PHY, 149–50
TEK
  - encryption of, 134
    - management, 134
    - state machine, 132
Time division duplexing (TDD), 19
  - DL subframe structure, 138
    - frame duration, 125
IEEE 802.16e PHY, 184–86
  - mode, 77, 78
WirelessMAN-SC PHY, 136–37
Time division multiplexing (TDM), 102
Timing jitter, 44
Timing offset, 43–46
  - effect, 43
    - loss of orthogonality due to, 44–46
    - phase shift representation, 43–44
Transmission convergence sublayer, DL, 139
Trivial file transfer protocol (TFTP), 167
UL channel descriptor (UCD), 174–75
UL media access profile (UL-MAP), 125
UL PHY, 141–43
  - conceptual block diagram, 142
    - PMD sublayer, 142–43
    - subframe, 141–42
See also WirelessMAN-SC PHY
Ultra-wideband (UWB), 7
Underserved areas, 113
Universal Mobile Telecommunications Services (UMTS), 22–23
Unlicensed National Information Infrastructure (UNII) bands, 93
WiBro, 19–22
    architecture, 22
    architecture components, 21
    characteristics, 20
    defined, 19–20
    download rate, 20
    services, 21

Wideband code division multiple access (WCDMA), 22

WiMAX, xii–xiii, 17–19
    advantages, 97
    backhaul connections, 97
    comparative analysis, 22–23
    coverage range, 97
    defined, 13, 17
    development, 17
    experimental, 91
    fixed, 94–96
    flavors, 18
    functions, 18–19
    IP connectivity, 97
    markets, 115
    mobile, 95
    OFDMA frame structure, 185
    usage models, 13–14
    user product equipment, commercial availability, 92

WiMAX-certified equipment, 107

WiMAX Forum, 86
    interoperability requirements, 161
    member countries, 87
    timeline for product certification, 91

Wireless broadband. See WiBro

Wireless Internet service provider (WISP), 95–96

Wireless LANs (WLANs), 10–13
    FHSS, 11
    links, 11
    OFDM, 11
    role, 10

Wireless local loop (WLL), 87

WirelessMAN-OFDMA PHY, 150–53
    channel coding, 152–53
    defined, 150–51
    ranging, 151–52

See also PHY layer

WirelessMAN-OFDM PHY, 146–50
    channel coding, 147–48
    channel quality measurements, 150
    control quality measurements, 150
    defined, 146
    OFDM symbol description, 146–47

See also PHY layer

Wireless MANs, 13–14

WirelessMAN-SCa PHY, 143–46
    burst, 144
    burst frame, 144
    burst set, 144
    channel quality measurements, 146
    defined, 143
    MAC frame, 144
    payload, 143
    transmit processing, 144–45

See also PHY layer

WirelessMAN-SC PHY, 135–43
    channel quality measurements, 143
    defined, 135
    DL PHY, 137–41
    FDD and TDD operation, 136–37
    operation, 136
    UL PHY, 141–43

See also PHY layer

Wireless networks
    classifications, 3–17
    infrastructure, 16
    range, 4–15
    signaling, 15–16
    WLAN, 10–13
    WMAN, 13–14
    WPAN, 4–10
    WWAN, 14–15

Wireless PANs (WPANs), 7

Wireless technologies
    comparison, 23
    progression, 3

Wireless WANs (WWANs), 14–15, 97–99
    mobile communications, 15
    satellites, 14–15

World Radio Conference (WRC), 91

ZigBee, 7, 93–94
The Artech House Universal Personal Communications Series
Ramjee Prasad, Series Editor

4G Roadmap and Emerging Communication Technologies, Young Kyun Kim and Ramjee Prasad

802.11 WLANs and IP Networking: Security, QoS, and Mobility, Anand R. Prasad and Neeli R. Prasad

CDMA for Wireless Personal Communications, Ramjee Prasad

From WPANs to Personal Networks: Technologies and Applications, Ramjee Prasad and Luc Deneire

IPIATM Mobile Satellite Networks, John Farserotu and Ramjee Prasad

Multicarrier Techniques for 4G Mobile Communications, Shinsuke Hara and Ramjee Prasad

OFDM Towards Broadband Wireless Access, Uma Shanker Jha and Ramjee Prasad

OFDM for Wireless Communications Systems, Ramjee Prasad

OFDM for Wireless Multimedia Communications, Richard van Nee and Ramjee Prasad


Radio over Fiber Technologies for Mobile Communications Networks, Hamed Al-Raweshidy and Shozo Komaki, editors

Simulation and Software Radio for Mobile Communications, Hiroshi Harada and Ramjee Prasad

Space-Time Codes and MIMO Systems, Mohinder Jankiraman

TDD-CDMA for Wireless Communications, Riaz Esmailzadeh and Masao Nakagawa

Technology Trends in Wireless Communications, Ramjee Prasad and Marina Ruggieri

Third Generation Mobile Communication Systems, Ramjee Prasad, Werner Mohr, and Walter Konhäuser, editors

Towards a Global 3G System: Advanced Mobile Communications in Europe, Volume 1, Ramjee Prasad, editor

Towards a Global 3G System: Advanced Mobile Communications in Europe, Volume 2, Ramjee Prasad, editor
Towards the Wireless Information Society: Heterogeneous Networks, Volume 2, Ramjee Prasad, editor
Towards the Wireless Information Society: Systems, Services, and Applications, Volume 1, Ramjee Prasad, editor
Universal Wireless Personal Communications, Ramjee Prasad
WCDMA: Towards IP Mobility and Mobile Internet, Tero Ojanperä and Ramjee Prasad, editors
Wideband CDMA for Third Generation Mobile Communications, Tero Ojanperä and Ramjee Prasad, editors
Wireless Communications Security, Hideki Imai, Mohammad Ghulam Rahman, and Kazukuni Kobara
Wireless IP and Building the Mobile Internet, Sudhir Dixit and Ramjee Prasad, editors
WLAN Systems and Wireless IP for Next Generation Communications, Neeli Prasad and Anand Prasad, editors
WLANs and WPANs towards 4G Wireless, Ramjee Prasad and Luis Muñoz

For further information on these and other Artech House titles, including previously considered out-of-print books now available through our In-Print-Forever® (IPF®) program, contact:

Artech House
685 Canton Street
Norwood, MA 02062
Phone: 781-769-9750
Fax: 781-769-6334
e-mail: artech@artechhouse.com

Artech House
46 Gillingham Street
London SW1V 1AH UK
Phone: +44 (0)20 7596-8750
Fax: +44 (0)20 7630-0166
e-mail: artech-uk@artechhouse.com

Find us on the World Wide Web at: www.artechhouse.com