6-17-2013 12:00 AM

Secure OFDM System Design for Wireless Communications

Hao Li
The University of Western Ontario

Supervisor
Xianbin Wang
The University of Western Ontario

Graduate Program in Electrical and Computer Engineering
A thesis submitted in partial fulfillment of the requirements for the degree in Doctor of Philosophy

Secure OFDM System Design for Wireless Communications

(Thesis format: Monograph)

by

Hao Li

Graduate Program in Engineering Science

A thesis submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy

School of Graduate and Postdoctoral Studies
The University of Western Ontario
London, Ontario, Canada

Abstract

Wireless communications is widely employed in modern society and plays an increasingly important role in people's daily life. The broadcast nature of radio propagation, however, causes wireless communications particularly vulnerable to malicious attacks, and leads to critical challenges in securing the wireless transmission. Motivated by the insufficiency of traditional approaches to secure wireless communications, physical layer security that is emerging as a complement to the traditional upper-layer security mechanisms is investigated in this dissertation. Five novel techniques toward the physical layer security of wireless communications are proposed. The first two techniques focus on the security risk assessment in wireless networks to enable a situation-awareness based transmission protection. The third and fourth techniques utilize wireless medium characteristics to enhance the built-in security of wireless communication systems, so as to prevent passive eavesdropping. The last technique provides an embedded confidential signaling link for secure transmitter-receiver interaction in OFDM systems.

In order to effectively and efficiently defend against malicious attacks in a wireless network, the transmission nodes need to understand the communication risk in the operating environment. A security level awareness scheme is proposed in this dissertation, where the number of active users in a multipath fading environment is estimated. A time domain pilot correlation (TDPC) algorithm for detecting OFDM signals with frequency domain inserted pilots is proposed to recognize the presence of active users, based on the cyclic correlation between the complex conjugate multiplication of received signal segments and a local time domain pilot reference. Taking

advantage of a typical device fingerprint—I/Q imbalance, the number of active users is estimated through counting all the identified distinct transmitter I/Q imbalances.

With regard to enhancing the built-in security of wireless communication systems against passive eavesdropping, two novel anti-eavesdropping OFDM systems are proposed by exploiting the reciprocal, location-dependent and time-varying nature of wireless channels. Based on the instantaneous channel state information (CSI) between the transmitter and legitimate receiver, dynamic coordinate interleaving and subcarrier interleaving are employed in the two proposed secure OFDM systems, respectively. In the coordinate interleaving scheme, a transmitter performs coordinate interleaving at partial subcarriers of each OFDM signal, where the symbol coordinate of an OFDM subcarrier is interleaved in an opportunistic manner depending on the associated subcarrier channel gain or phase. The subcarrier interleaving strategy is realized by interleaving subcarriers of each OFDM signal according to the sorted order of their sub-channel gains. Since wireless channels associated with each pair of users at separate locations exhibit independent multipath fading, the frequently renewed security design can only be shared between legitimate users based on channel reciprocity. Consequently, eavesdropping is prevented due to mismatched information recovery at the eavesdropper.

In the final part of the dissertation, the proposed anti-eavesdropping OFDM systems are upgraded by enabling an efficient and confidential side information transmission mechanism between the legitimate users, without interrupting the data transmission and requiring additional time and frequency resources. In the design, the cyclic prefix of an OFDM signal is replaced by a specially tailored orthogonal sequence. The side information is conveyed by the confidential orthogonal sequence that maintains the same time and frequency characteristics as the data-carrying OFDM symbol.

Key words: Wireless communications, physical layer security, OFDM, security level awareness, eavesdropping prevention, embedded confidential signaling.

To my parents

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisor, Dr. Xianbin Wang, for his encouragement, guidance and support from the initial to the final stages during the study of my degree. It is a fruitful and enjoyable experience to learn from him.

My sincere thanks go to the members of my dissertation committee, Dr. Jean-Yves Chouinard, Dr. Evgueni Bordatchev, Dr. Quazi Mehbubar Rahman, and Dr. Jagath Samarabandu for taking the time out of their busy schedules to read my dissertation and provide me with their constructive comments and valuable suggestions.

I owe many thanks to the faculty, staff and students I met at The University of Western Ontario, who have helped me directly or indirectly in completing my studies and have made my study period a rewarding experience. I express heartfelt regards to all the members in our group, particularly Dr. Yulong Zou and Dr. Weikun Hou, who supported me in all respects during the completion of my research projects. I am also grateful to all my friends who care for me as brothers and sisters and have given me beneficial suggestions and ceaseless encouragement.

Last but not the least, I would like to thank my parents, my brother and sister-in-law, and the rest of my family for their love and support throughout this degree and my life. There are no words sufficient to represent my full gratitude to them.

Contents

List of Tables

List of Figures

List of Appendices

List of Abbreviations

3GPP	3rd Generation Partnership Project
ACK	Acknowledgement
AP	Access Point
ADC	Analog-to-Digital Converter
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
CDF	Cumulative Distribution Function
CLT	Central Limit Theorem
CP	Cyclic Prefix
CSI	Channel State Information
DSSS	Direct-Sequence Spread-Spectrum
DVB-H	Digital Video Broadcasting-Handheld
DVB-T	Digital Video Broadcasting-Terrestrial
DVB-T2	Digital Video Broadcasting-Second Generation Terrestrial
FAP	False Alarm Probability
FFT	Fast Fourier Transform
FHSS	Frequency-Hopping Spread-Spectrum
FO	Frequency Offset
IC	Integrated Circuit
ICI	Inter-Carrier Interference
IDFT	Inverse Discrete Fourier Transform
IEEE	Institute of Electrical and Electronics Engineers
IFFT	Inverse Fast Fourier Transform
IP	Internet Protocol
ISI	Intersymbol Interference
LO	Local Oscillator
LPF	Low-Pass Filter
LS	Least-Square
LTE	Long-Term Evolution
MAC	Media Access Control
Mbps	Megabits Per Second
MDP	Miss Detection Probability
MIMO	Multiple-Input Multiple-Output

OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
PAPR	Peak-to-Average Power Ratio
PCP	Precoded Cyclic Prefix
PDF	Probability Density Function
PDP	Power Delay Profile
RF	Radio Frequency
RF-DNA	Radio Frequency Distinct Native Attribute
RMS	Root-Mean-Square
RSS	Received Signal Strength
SER	Symbol Error Rate
SNR	Signal-to-Noise Ratio
TDD	Time-Division Duplexing
TDPC	Time Domain Pilot Correlation
TO	Timing Offset
UHF	Ultra-High Frequency
VHF	Very-High Frequency
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Networks
i.i.d.	independent and identically distributed

Chapter 1

Introduction

1.1 Research Motivation

Wireless communications, which removes the constraint of cable connections for information exchange, is becoming ubiquitous nowadays. Over the last few decades, wireless technologies have been widely employed in military, civilian and commercial services. However, due to the inherent broadcast nature of radio signal propagation, wireless communications is vulnerable to masses of malicious attacks, including eavesdropping, jamming, spoofing and so on [1]. Hence, securing wireless communication systems has become a critical issue along with the proliferation of wireless applications [1].

Traditionally, security strategies for wired communication systems, such as authentication and encryption at the link and upper layers, are extended to the wireless counterparts. However, the traditional approaches are not sufficient for securing wireless communications, due to the lack of a robust physical-layer protection [2]. As wired communication systems rely on a wire-based physical connection, adversaries inserting into the original link can be easily detected and illegal access to the network can be prevented. A secure physical layer is inherently provided by the channel access mechanism of wired communication systems, so that no special physical-layer protec-

tion is addressed in the traditional security strategies. Conversely, the physical layer of wireless communications is the most vulnerable and easy to compromise part of the system due to the unconstrained propagation of the electromagnetic wave. A secure physical layer would thus be a determinant in protecting the wireless transmission. Recently, physical layer security has emerged as an effective and valuable paradigm to improve the security of wireless communications, as a complement to the traditional security techniques.

Inherent physical-layer properties of wireless communications can be exploited to enhance the transmission security, including the situation- and user-dependent randomness from the wireless medium [2] and the unique radio frequency distinct native attribute (RF-DNA) of wireless devices [3]. These physical-layer properties can be employed for the transmission confidentiality enhancement, the user authentication, as well as the intrusion and spoofing detection in wireless networks. Several physical layer security schemes have been reported in the literature [4–12]. With a comprehensive study of the existing physical layer security techniques, we can find that the present schemes usually require significant modifications to off-the-shelf systems and have high computational complexity. Intelligent, effective, simple and efficient physical-layer approaches for securing wireless communication systems have yet to be investigated.

Orthogonal frequency-division multiplexing (OFDM) has been widely employed in modern high-speed wireless communication networks, such as Long-Term Evolution (LTE), Institute of Electrical and Electronics Engineers (IEEE) 802.11 and IEEE 802.16, because of its spectrum efficiency and robustness to multipath distortion. However, the conventional OFDM signal is vulnerable to malicious eavesdropping and intervention, due to its distinct time and frequency characteristics [13]. The traditional security strategies at upper layers of the protocol stack cannot completely address the security threats in wireless OFDM systems of a physical layer transparent to adversaries. It is therefore of great importance to enhance the security of OFDM at the physical layer.

1.1.1 Security Risk Assessment in Wireless Networks

In order to provide confidential, authenticated, integral and reliable communication between legitimate users, a wireless communication system needs to take some proper actions to defend against the malicious attacks. One fact to be addressed is that the transmission risk of an operating environment is time-varying due to variations of the channel conditions, the surrounding devices as well as the roles played by coexistent users [14]. As a result, the security scheme and implementation need to be evaluated regularly and updated corresponding to the security risk changes in the communication environment. Otherwise, insufficient defending would fail to protect the transmission security, and over-performed countermeasures would reduce the efficiency of the system since any security solution is resource-consuming.

In order to effectively and efficiently defend against malicious attacks in a wireless network, a wireless device should assess the security risk in the operating environment in the first place. Intuitively, a wireless device could identify all malicious attacks and then take corresponding actions to combat the identified attacks, which, however, is not enough since the detection of the types of attacks cannot indicate the severity of the security threat. Furthermore, the detection of all malicious attacks is unrealistic in the practical implementation. First of all, there are a mass of potential attacks and each typical security attack may have numerous derived varieties [14]. Hence, it is difficult for legitimate users to identify all malicious attacks in the detection phase. Second, the attack detection process is time- and power-consuming. Large numbers of tests have to be carried out in order to cover adequate potential attacks. Putting aside the latency caused by the attack detection phase to the data transmission, the detection results may be out-of-date, and legitimate users may suffer power-crisis. In addition, some attacks are hard to be identified in time, such as eavesdropping, spoofing, and attacks from adversaries with anti-reconnaissance capabilities. Therefore, security risk assessment in wireless networks cannot rely on the attack detection strategy.

To that end, security risk assessment schemes for wireless communications, which can effectively and efficiently evaluate the transmission risk in an operating environment, need to be investigated. In principle, any node in a network, even a present legitimate user, may intentionally or unintentionally perform hostile attacks such as eavesdropping and jamming, and becomes a potential threat [15]. It is near impossible to prevent some amount of data loss or disclosure from devices that can physically access the network [16]. The communication risk arises along with the increase of coexistent users. Hence, the number of active users in a network can generally indicate the security level of a wireless environment, and be used to guide developing the defending strategies. Compared with the risk assessment scheme that attempts to detect all potential attacks, the estimation of the number of active users is much simpler and easier to be implemented. Although the number of active users in a network cannot identify the attacks, it would imply the possible existence of attackers and the defending intensity needed in the operating environment.

Considering that device identities at upper layers of the protocol stack such as media access control (MAC) and Internet protocol (IP) addresses can be duplicated with little effort, mature estimation schemes for the number of active uses, which exploit the device-specific physical-layer characteristics of wireless devices, would be preferred. Moreover, in order to further improve the overall efficiency of a wireless communication system, we would like to avoid unnecessary estimation operation for the number of active users. A triggering mechanism can thus be employed, where the estimation procedure would only be performed after the confirmation of the existence of active users.

1.1.2 Eavesdropping-Resilient OFDM Systems

With the security risk assessment in a wireless communication environment, appropriate defending strategies can be designed and implemented. Malicious attacks in wireless communications can be classified into two categories: passive and ac-

tive [17]. Legitimate terminals can often perceive active attacks based on the sense of transmission anomalies, and then carry out corresponding protective measures. In contrast, even with specific detection procedures, passive attacks are hard to be detected since they usually do not leave any evidence about their illegal behaviors and crimes. Private information can be intercepted by adversaries without the awareness of the communicating pair. Accompanied with the fact that information collected by passive attacks is usually used to further the damage of other forms of attacks by adversaries, the threat of passive attacks is fatal. Therefore, wireless communication systems should strengthen their built-in security against passive attacks. Eavesdropping is a most common form of the passive attacks. This dissertation will concentrate on the eavesdropping relevant issues for simplicity.

The physical layer is responsible for the physical connection between end stations. It is the foundation of the information transmission. The security of wireless communications is thus conditioned on a secure physical layer. Unfortunately, the physical layer is the most vulnerable part of wireless communication systems since it does not depend on any human-made logical organization, but rather obeys uncontrollable laws of electromagnetic wave propagation [12]. As a result, the physical-layer built-in security of wireless communication systems against passive attacks must be enhanced. Considering the general acceptance of OFDM technology in modern wireless networks as well as the security weaknesses of OFDM systems, the built-in security enhancement at the physical layer of wireless OFDM systems needs to be addressed.

The physical-layer built-in information confidentiality can be realized by disrupting the information recovery in eavesdropping. Technically, plentiful randomness can be introduced into the signal structure in the legitimate communication, leading to dynamic signal structure that can only be recognized by legitimate users. In wireless communications, legitimate parties can harvest continual influx of randomness from the time-varying wireless channels. This user- and location-dependent randomness can be exploited for the communication security design. Because of channel reciprocity, the transmitter and receiver would experience and observe an identical

wireless channel. Consequently, the channel based randomness can be shared between the two ends of the channel. In contrast, wireless channels associated with different endpoints at separate locations generally exhibit uncorrelated propagation characteristics. It is thus impossible for an eavesdropper at a third location to track the randomness involved in the legitimate transmission and perform correct information recovery. As a result, the physical-layer built-in security of wireless communications against eavesdropping can be achieved. With regard to a specific design, its effectiveness and efficiency can be improved by consulting the security risk assessment result.

1.1.3 Secure OFDM Systems with Embedded Confidential Signaling Link

Secure communication systems should not only defend against malicious attacks but also maintain reliable legitimate transmission. Under some hostile channel conditions, transmitter-receiver interaction for certain security design relevant parameters may be needed in secure wireless communication systems, in order to guarantee the reliability of legitimate transmission while not degrading the transmission security. One example is the channel-based secure access where channel reciprocity is exploited by legitimate users to share the security design. Typically, the end stations of a wireless link can only have noisy observations of the channel due to the existence of noise and interference at the two ends. Hence, the channel estimates at the communicating pair are just correlated though the channel is inherently reciprocal. Under the situation of strong noise and interference, the transmission of certain security design relevant parameters between legitimate terminals may be required, so as to mitigate the impairment from imperfect reciprocity of the channel estimates and improve the reliability of legitimate transmission.

Generally, the security design relevant parameters do not have much content, but may be renewed frequently along with the update of the design. The transmitter-

receiver interaction should thus be always available. Moreover, the side information interaction with lower priority cannot interrupt or interfere the original data transmission, but should provide a reliable and confidential information exchange. In addition, such interaction should not ask for additional time and spectrum resources that are typically unavailable to the transmission of side information.

A candidate solution to solve the aforementioned problems is to transmit data and security design relevant parameters concurrently, through a confidential signaling link embedded into the secure communication system. As an advance of the secure OFDM systems with physical-layer built-in security enhancement, embedded confidential signaling strategies are worthy of research efforts. OFDM with precoded cyclic prefix (PCP-OFDM), which was originally proposed for the adaptive transmission in cognitive radio [18], can be extended and specially tailored for the transmission of security design relevant side information between legitimate users.

1.2 Dissertation Contributions

The main contributions of this dissertation are summarized as follows.

- In order to respond appropriately to malicious attacks in a wireless network, a security level awareness scheme for effectively and efficiently evaluating the security risk in wireless communication environments is proposed. Instead of attempting to detect all potential attacks, the proposed scheme simply estimates the number of active users in a transmission environment after recognizing their existence. Robust active user detection is achieved by a proposed time domain pilot correlation algorithm and its affiliated interference mitigation techniques. The number of active users is evaluated by a novel estimation method that exploits a typical device RF-DNA—I/Q imbalance.

- Two novel anti-eavesdropping OFDM systems are proposed by taking advantage of the channel reciprocity and the uncorrelation feature exhibited among

spatially separate wireless channels in rich multipath environments. Based on the instantaneous channel state information (CSI) between the transmitter and legitimate receiver, dynamic coordinate interleaving and subcarrier interleaving are employed in the two proposed secure OFDM systems, respectively. The "coordinate interleaving" strategy is carried out by interleaving the symbol coordinates at partial subcarriers of each OFDM signal, where subcarriers that perform coordinate interleaving are determined by the subcarrier channel gains or phases. The "subcarrier interleaving" scheme is realized by selectively interleaving subcarriers of each OFDM signal according to the sorted order of the subcarrier channel gains. In addition, techniques to mitigate the impairment from imperfect channel reciprocity are also investigated.

- This dissertation extends the previous study on PCP-OFDM in [18], and provides an embedded confidential signaling link for the transmitter-receiver interaction in secure OFDM systems. Specially tailored PCP sequences that have the same time and frequency characteristics as the data-carrying OFDM symbols are used to reliably and confidentially transmit the security design relevant system parameters between legitimate terminals.

1.3 Dissertation Organization

The following details the organization of remaining chapters of this dissertation.

It would be beneficial to first provide fundamentals related to the wireless communication security, including the typical malicious attacks, general security objectives and countermeasures, as well as principles of the security design. All of these are explained in Chapter 2. The security vulnerabilities of OFDM physical layer are also addressed in this chapter, after a review of the general aspects of OFDM technology.

Security risk awareness for wireless communications is investigated in Chapter 3 and Chapter 4. The proposed security level awareness scheme consists of two

procedures: 1) recognizing the existence of active users; 2) estimating the number of active users in the operating environment. Chapter 3 focuses on the proposed time-domain pilot correlation based user detection algorithm, followed by the number of active users estimation technique using transmitter I/Q imbalance in Chapter 4.

Following the discussions on the proposed security risk awareness techniques, this dissertation moves on to the proposed novel anti-eavesdropping OFDM systems. Chapter 5 provides insight into the proposed anti-eavesdropping OFDM system through CSI-based coordinate interleaving. In Chapter 6, the eavesdropping-resilient OFDM system using dynamic subcarrier interleaving is analyzed.

In addressing the issue of imperfect channel reciprocity, an embedded confidential signaling scheme is proposed and investigated in Chapter 7. It enables a reliable and confidential transmission of security design relevant system parameters between legitimate users, and thus upgrades the proposed anti-eavesdropping OFDM systems.

Finally, in Chapter 8, conclusions are drawn from the studies and future research directions are pointed out.

Chapter 2

Security Issues in Wireless Communications

This chapter summaries security risks and threats in wireless communication systems, accompanied with an insight survey of existing solutions to these security issues. OFDM technology, which has been adopted in lots of modern wireless communication networks, is also reviewed in this chapter. In addition, the security vulnerabilities of OFDM due to its distinct physical-layer time and frequency characteristics are addressed.

2.1 Risks and Threats in Wireless Communications

Wireless communications is ubiquitous nowadays and continues to flourish worldwide further. Various wireless communication systems, such as WiFi, WiMax and LTE, have widely permeated people's daily life from home to public venues. The main reason behind its proliferation is plentiful advantages offered by the wireless technology, such as the freedom of mobility, flexible options of connectivity, and low cost of network configuration. However, compared with the traditional wired com-

munications, much more security vulnerabilities are induced by the wireless transmission mechanism. First and foremost, the wireless medium is inherently an open-air medium. Adversaries can easily access a wireless network as long as they are within its coverage range, due to the broadcast nature of radio propagation. Furthermore, most wireless communication systems are highly standardized. Apart from security weaknesses in the communication standards, the standardization increases security risks of wireless transmission. Some system parameters, such as the composition of data packets and the protocol of network configuration, are public and available to adversaries. The information of such parameters would lower the technical difficulties in malicious attacking. In addition, the mobility and portability of wireless devices further facilitate adversaries to attack wireless communications.

Wireless communications is subject to a number of security risks and threats. Generally, malicious attacks in wireless communication networks can be classified into two categories: passive and active [17]. Passive attacks intercept legitimate message from wireless channels without interfering with the operation of legal networks. Conversely, active attacks attempt to disrupt the normal network operation instead of intercepting the legitimate traffic. The most common forms of passive and active attacks in wireless communications are listed as follows:

- *Eavesdropping*: Eavesdropping is the act that an attacker, named eavesdropper, passively listens to a network and intercepts the ongoing traffic [2]. Due to the openness of wireless medium, an eavesdropper is possible to access the data stream as long as it lies in the coverage of the transmitter. In the case that communication protocols are known by the eavesdropper, it can simply follow those protocols like normal participants and then intercept the sensitive and private information.

- *Traffic Analysis*: Traffic analysis is the process of intercepting and examining the collected data streams in order to deduce information from patterns of communication. Similar to eavesdropping, traffic analysis is also based on what the

attacker hears in the network. However, this sort of attack does not have to demodulate and understand the actual data in transmission [19]. It is often used to determine the locations, identities and behavior patterns of the communicating parties. Adversaries can then use the collected information from traffic analysis to support other forms of attacks [2].

- *Jamming*: Jamming occurs when intentional or unintentional interferences flood a communication link [20]. A hostile jammer can broadcast interference signals over a broad spectral band to degrade the channel condition and disrupt the legal information transmission. In the situation that the attacker has infinite power supply, it can even exhaust the resource for legitimate users and then destroy the legal communication.

- *Spoofing*: In spoofing, an attacker pretends to be an authorized client, device or user to gain access to a network protected by some forms of authentication mechanisms, so as to seize the system resource and intercept the confidential information [1]. Moreover, an attacker can also impersonate a network resource by positioning itself between the client and intended resource. When a victim initiates a connection, the attacker can intercept the connection, and then complete the connection to the intended resource. As a result, all communication between the client and intended resource is controlled by the adversary [1].

- *Injection and Data Modification*: Injection happens when an attacker adds commands and data to the existing connection to hijack the ongoing communication, or maliciously send commands and data to manipulate the available resource [2]. Moreover, adversaries can flood the network access point with connection messages, thereby tricking the network access point into exceeding a maximum limit and then denying authorized user access to the network [20]. Data modification refers to an attack in which an aggressor adds, deletes or even changes the network communication contents [2].

Table 2.1: Classification of security attacks in wireless networks

Security Attacks	
Passive Attacks	Active Attacks
Eavesdropping Traffic Analysis	Jamming Spoofing Injection and Data Modification

The classification of these security attacks is shown in Table 2.1. Under active attacks, communication anomalies can normally provide demonstrable evidence of malicious attacks, so that legitimate terminals can easily detect the attackers and then launch corresponding defending operations. In contrast, passive attacks without leaving much evidence about their illegal behaviors are difficult to be detected. Sensitive and private information may be intercepted by adversaries without the awareness of the communicating pair. The threats from eavesdropping and traffic analysis would be inherent risks in wireless networks that cannot be avoided [1]. Please note that malicious attacks typically do not stand alone. Adversaries usually coordinate several attacks to further the damage, where passive attacks such as eavesdropping and traffic analysis are essentially used to gather information for other forms of attacks. Therefore, as the foundation of malicious attacking and with the counter-detection feature, passive attacks can cause fatal damage to a wireless communication system.

It is also noteworthy that the risks and threats in wireless communications are time- and location-varying, due to the variations of channel conditions, surrounding devices as well as roles played by coexistent users.

2.2 Solutions to Secure Wireless Communications

Securing communication systems has been a problem of interest since the time of conception of network based communications [17]. The concept of secure communication is linked to two main desired objectives: effective defending against malicious attacks and reliable transmission between legitimate users. The first objective indi-

cates that a communication system should protect the **confidentiality**, **authenticity**, **integrity**, and **availability** of data transmission, by defending against various attacks [14, 21], where

- **Confidentiality** denotes the property that the transmitted information is prevented from unauthorized individuals, entities or processes;
- **Authenticity** is to provide the assurance of the identities of communicating nodes, which ensures that a received message comes from a desired transmitter and vice versa;
- **Integrity** indicates the capability to protect transmitted messages from being modified and destroyed by adversaries during the propagation;
- **Availability** means that a communication system is able to provide services whenever it is demanded by a legitimate entity.

With regard to the second objective, a message for an intended receiver should be reliably received by that user. In other words, the demodulation error rate at the legitimate receiver needs to satisfy an acceptable requirement.

In addition, since the risks and threats in wireless networks are time- and location-varying, the solutions to secure wireless communication systems need to be evaluated and updated regularly. In order to effectively and efficiently defend against the malicious attacks, a wireless device should intelligently perform proper security schemes corresponding to the real-time communication risk in an operating environment.

2.2.1 Traditional Security Approaches and Limitations

Traditional strategies to secure wireless communications mainly rely on a layered protocol architecture, by exploiting authentication and encryption at the link and upper layers.

The layered protocol architecture that dominates modern data communications is illustrated in Fig. 2.1. The physical layer is responsible for the establishment

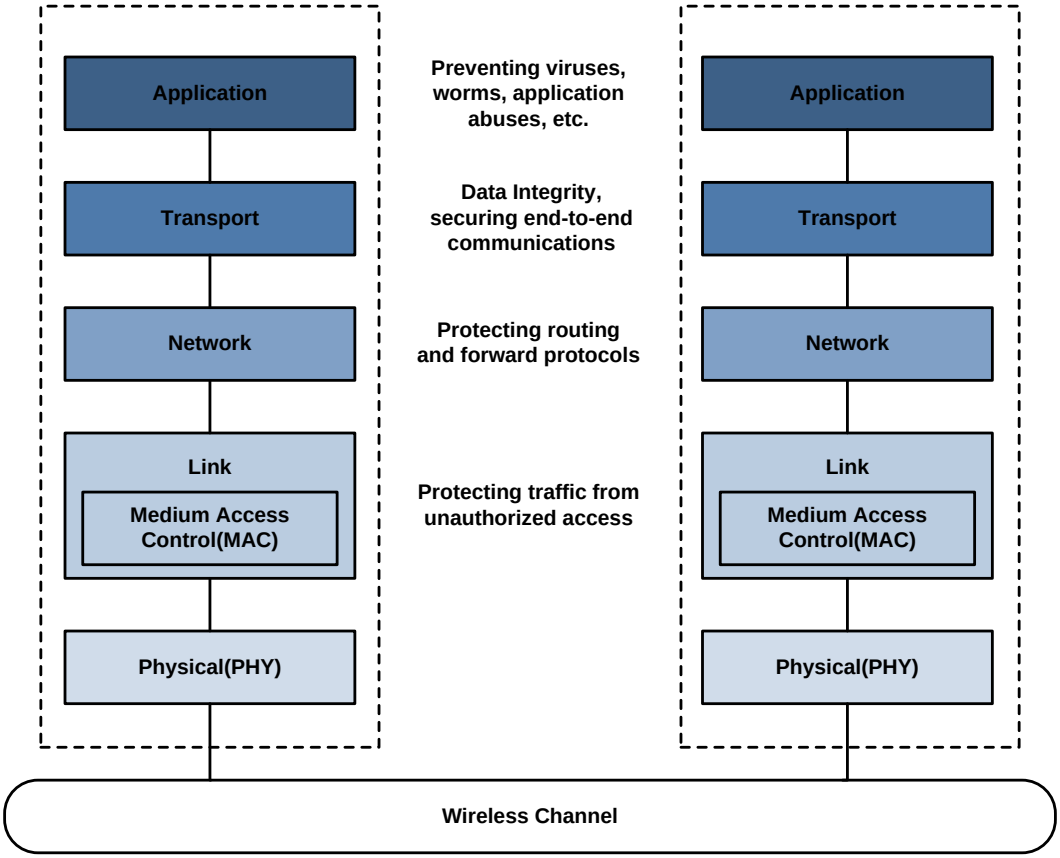


Figure 2.1: Layered protocol architecture in communication systems.

and termination of a connection to the communication medium. It is intended for defining the relationship between a device and the transmission medium. The link layer transfers data between two directly connected stations, and detects and possibly corrects errors that may occur at the physical layer. The network layer determines the route that a packet would need to take from the source to the destination. In addition, the transport layer provides transparent transfer of data between end users, and the application layer acts as a user interface in the network [22]. Traditionally, every layer in the protocol stack is secured with a certain algorithm, except the physical layer.

2.2.1.1 Traditional Authentication and its Limitations

Authentication, a process that a station recognizes the identity of its communication partner, is typically performed at the link layer, network layer, transport layer

and application layer. Link-layer authentication is executed by checking the MAC addresses of stations that attempt to be connected. Unfortunately, this authentication strategy is vulnerable since that the MAC address of a device is changeable. Adversaries can spoof a legitimate user by duplicating its MAC address, and then get the access to the network. Network-layer authentication relies on the IP addresses to identify nodes in a network, but it becomes vulnerable under route spoofing. An attacker can pick up any IP address desired. The transport layer utilizes the message authentication code to provide integrity and authenticity assurances of the data transmission. However, the message authentication code may be disclosed and duplicated as well. At the application layer, user authentication mechanisms like the login and password based authentication are employed, which are restricted by the safety of the password-like information. In addition to the user authentication mechanisms, the application layer can also make use of secure facilities available from the lower layers, such as checking the incoming and outgoing data and requiring the use of strong authentication. In this case, the application layer would inherit all the weaknesses belonging to lower layers of the protocol stack.

2.2.1.2 Traditional Encryption and its Limitations

Encryption, which is often carried out at all the upper four layers, is controlled by a private key either shared between legitimate users or only available to the intended receiver. In this approach, the transmitted data is encrypted using an encryption key (a shared private key in the symmetric-key scheme or a public key in the asymmetric-key scheme), and can only be decrypted by a terminal with a corresponding private decryption key. Adversaries without such private decryption key cannot read the encrypted message. The vulnerabilities of the traditional encryption are obvious, particularly in its key distribution and protection. In the symmetric-key scheme, since each possible communicating pair must agree on a secret key before the communication, the private key may be disclosed during the interaction between the

communication parties, even during their initial key exchange. In the asymmetric-key scheme, adversaries can exploit the public key to either conduct active attacks like injection or pretend to be the legitimate transmitter and then wangle the private decryption key. Furthermore, certain participants in a network may not have satisfactory security strength. They are easy to be defeated. As a result, the safety of the private key cannot be ensured. In addition, adversaries with tremendous power, memory and computational capability can attempt to crack the private key from the received signals, especially when the key has been used for a long time.

2.2.1.3 Other Weaknesses of Traditional Security Approaches

Traditional security strategies, such as the traditional authentication and encryption, merely rely on the inherent computational complexity to protect the transmitted information. They are more and more vulnerable with the significant evolution of hardware manufacturing technologies and the development of efficient software algorithms. Wireless devices nowadays are much more powerful and possess improved computational capability. Equipped with these devices, adversaries have high possibilities to crack the traditional authentication and encryption, let alone the inherent weaknesses of these security strategies.

In addition to the insufficiency of traditional security approaches in securing wireless communications, it has been demonstrated that the upper layer security schemes have low efficiency [23]. All the layers in the protocol stack are secured independently under the assumption that the traffic from the lower or upper layers is well behaved. Without a systematic view, individual security processes developed for different protocol layers may provide redundant security services, and hence consume more resource than necessary. Also, the layered security schemes are time-consuming since the operation of a certain layer has to wait for the process at lower or upper layers. They would induce excessive communication latency. Meanwhile, the layered security schemes are power inefficient due to the overhead produced by the authenti-

cation and encryption at each layer. It is noteworthy that most of the wireless mobile devices are battery-powered so that they are power-limited.

Furthermore, from a business point of view, the main universally available wireless systems such as the cellular system do not want to handle a complex security mechanism like traditional security approaches, because they are intended for mass use. Implementation of the layer-by-layer measures would make these systems very expensive and non-profitable to the service providers [12].

In summary, traditional security approaches have some inherent weaknesses that make them vulnerable to adversaries. Meanwhile, the effectiveness of these schemes, which depends on the computational complexities introduced into malicious attacks, is not guaranteed in the event of hardware manufacture and software algorithm breakthroughs. It becomes easier for adversaries to break these schemes as attack devices become more powerful and less costly and attack algorithms become more efficient. Moreover, such layered security schemes often lead to system capacity degradation, excessive communication latency and high power consumption [24].

2.2.2 Physical Layer Security

In wireless communications, the effectiveness and efficiency of traditional upper-layer security approaches are restricted by their weaknesses. Reviewing the information flow through the layered protocol stack, we can see that all upper layers depend upon the physical layer to deliver the data. The physical layer is the entry point of malicious attacks. A secure physical layer would therefore be a determinant in protecting the information transmission. Unfortunately, the physical layer of wireless communication systems is vulnerable due to the open-air nature of wireless medium. Hence, physical-layer security enhancement is critical in securing wireless communications.

In recent years, physical layer security, which improves communication security at the physical layer, has emerged as an efficient and valuable paradigm to complement

traditional wireless security techniques [13]. The innovative concept behind wireless physical layer security is to exploit the continual randomness from the wireless medium and the device-dependent RF attributes of wireless devices to secure wireless communications. As the new paradigm is independent of the traditional security techniques, it can be integrated with the upper-layer security solutions to enhance the total strength of security in wireless communications.

2.2.2.1 Wireless Channel based Physical Layer Security

Wireless channel based physical layer security takes advantage of the continual randomness inherent in wireless channels to improve the system security. Fundamental properties of wireless channels, including the reciprocity, spatial and temporal variations, are exploited in the security designs.

In wireless communications, the propagation through a radio link can be characterized by three categories of losses: multipath, shadowing, and distance loss [25]. Multipath refers to the many different propagation paths between the transmitter and receiver, where each path is characterized by its own phase, delay, and attenuation. It results into channel variations over distances in the order of a wavelength. Shadowing refers to local variations in the received signal strength caused by structures, hills, canyons, vehicles, and so on. Distance loss refers to the phenomenon that the received signal power decreases as the distance between the transmitter and receiver increases. Taking all of these factors together, the impulse response of a wireless channel can be mathematically modeled by [25]

$$h(t,\tau) = \sum_{i=0}^{L-1} \alpha_i(t) e^{\theta_i(t)} \delta(t-\tau_i), \tag{2.1}$$

where L denotes the number of channel paths, and the ith path has amplitude $\alpha_i(t)$, phase $\theta_i(t)$, and propagation delay τ_i at time t.

With plenty of theoretical analysis and experimental verification, it is widely rec-

ognized that wireless channels have the following properties:

- **Reciprocity**: A channel behaves in an identical manner irrespective of in which direction it is observed, so that the two ends of a communication link should ideally observe the same channel impulse response.

- **Spatial decorrelation**: Channel responses decorrelate rapidly in space, particularly in a rich multipath environment. Generally, a third party who lies more than half a wavelength away from a pair of communicating nodes experiences a fading channel uncorrelated to that between the communicating terminals [26].

- **Time variation**: Wireless channels are time-varying. The channel fading is random over time due to the multipath propagation.

The above properties, which do not exist for wired or optical channels, have been proved to be true in most terrestrial wireless communication systems [10].

The fading and noise inherently present over wireless channels, accompanied with the reciprocity, spatial and temporal variation properties of multipath channels can be exploited to enhance wireless communication security at the physical layer, including data protection, user authentication, secret key generation and so on.

2.2.2.2 RF-DNA based Physical Layer Security

RF-DNA based physical layer security relies on the device-dependent hardware imperfections that are caused by the manufacturing variability. The term RF-DNA is used to indicate the unique physical attributes of a wireless device induced by embedded processors and other analog circuits, in a manner analogous to biometric human fingerprint. Hardware imperfections, such as I/Q imbalance, frequency and magnitude errors, cannot be avoided in the manufacture. Even in the integrated circuit (IC) fabrication processes that are necessarily precise, structural variations are still introduced in the final device structure on a very small scale [3]. Meanwhile, hardware impairments are generally accepted in practical implementations as long as

process-induced variations are within acceptable tolerances. Therefore, no two devices can be exactly the same in practice. It has been validated that even wireless devices are fabricated using the same manufacturing and packaging processes, individual device exhibits unique RF characteristics that are significant enough for distinguishing one from another [27, 28].

RF-DNA based physical layer security can defend against malicious attacks such as spoofing and injection at the device level. The device-specific RF-DNAs that can be exploited to protect wireless communications include I/Q imbalance, transient phase, frequency error, phase error, and magnitude error [28].

2.2.2.3 State of the Art in Physical Layer Security

Extensive research efforts have been dedicated to physical layer security from both academia and industry. In the last decade, there has been considerable progress in this realm. Various methods have been proposed to take advantage of the randomness of wireless channels and RF-DNAs of wireless devices to enhance the security of wireless communications at the physical layer.

Theoretical Secrecy Capacity from Wireless Channels Information theoretic security examines the fundamental ability of the physical layer to secure communications [11]. Historically, the notion of information theoretic security was first introduced into communication systems by Shannon in [29], and then extended by Wyner's work in [30]. The so-called secrecy capacity was defined as the maximum rate achievable between the legitimate transmitter-receiver pair while being able to keep the message secret from unintended receivers. It was proved that confidential communication is possible if the desired receiver enjoys better channel conditions than the eavesdropper under the Gaussian wiretap channel model [31]. More recently, the secrecy capacity over fading channels was investigated [32–34]. It was shown that in the presence of multipath fading, information theoretic security is achievable even when the eavesdropper has a higher average signal-to-noise ratio (SNR) than the legitimate

receiver [32]. In addition, space-time diversity in wireless communication systems using multiple antennas was also exploited to enhance the information security and information-hiding capabilities [35].

Channel-based Data Protection The reciprocity and spatial decorrelation of wireless channels have been exploited to protect the confidentiality of data transmission at the physical layer. A key distribution method using the theory of reciprocity for antennas and electromagnetic propagation was proposed in [36]. A crosslayer secure coding scheme based on the statistical knowledge of wireless channels was presented in [37]. In addition, resource allocation [38, 39], transmit beamforming [40], artificial noise [41] and cooperation transmission [42] have been investigated to maximize the secrecy capacity, so as to realize the transmission confidentiality.

Channel-based Authentication Channel-based authentication algorithms can be generally divided into two categories: CSI and received signal strength (RSS) assisted authentication. Physical layer authentication algorithms that exploited the spatial variability of wireless channels were investigated [43, 44]. RSS, which is determined by the transmit power and CSI, is also used for authentication at the physical layer of wireless communication systems. Both RSS similarity and temporal RSS variation have been utilized to authenticate wireless users [45].

Channel-based Secret Key Generation The randomness inherent in wireless channels can benefit the secret key generation. [46] introduced a level crossing algorithm for key generation in fading wireless channels. A joint source-channel approach that combined existing source and channel models for key agreement over wireless fading channels was developed in [47]. Moreover, key extraction methods based on both the entire CSI and single channel parameter such as RSS were compared in [48].

RF-DNA based Device Identification and Authentication RF-DNA is generally employed for the device identification and authentication. A RF fingerprinting

technique that exploited the transient amplitude and phase responses was introduced to identify wireless devices in [49]. In [50], the authors used the frequency difference and phase shift difference between the ideal signal and the one transmitted to prevent spoofing, through a proposed nonparametric Bayesian method. Moreover, more than one device-specific features are combined to improve the reliability of the RF fingerprinting for wireless devices in [51]. Physical layer authentication based on the RF-DNAs of integrated circuits was investigated and validated in [3, 52].

2.3 OFDM and its Security Vulnerabilities

OFDM has been widely adopted in modern high-speed wireless communication networks such as LTE, IEEE 802.11 and IEEE 802.16, mainly due to its high spectral efficiency and robustness against multipath fading. Unfortunately, the distinct time and frequency characteristics of OFDM signals make OFDM communication systems extremely susceptible to malicious attacks from the adversaries.

2.3.1 Basic Concept of OFDM

OFDM was first introduced by S. Weinstein and P. Ebert in 1971 [53]. Compared with high data rate single-carrier communication systems, OFDM splits the serial data stream in parallel and divides the entire channel into many narrowband flat fading subchannels that are orthogonal to each other. These parallel data streams are modulated to transmit simultaneously over the orthogonal subcarriers/subchannels with a one-to-one correspondence and summed up to generate an OFDM symbol. A time domain OFDM symbol with N subcarriers can be given by

$$x(t) = \sum_{k=0}^{N-1} X(k) e^{j2\pi f_k t}, \quad 0 \leq t \leq T, \tag{2.2}$$

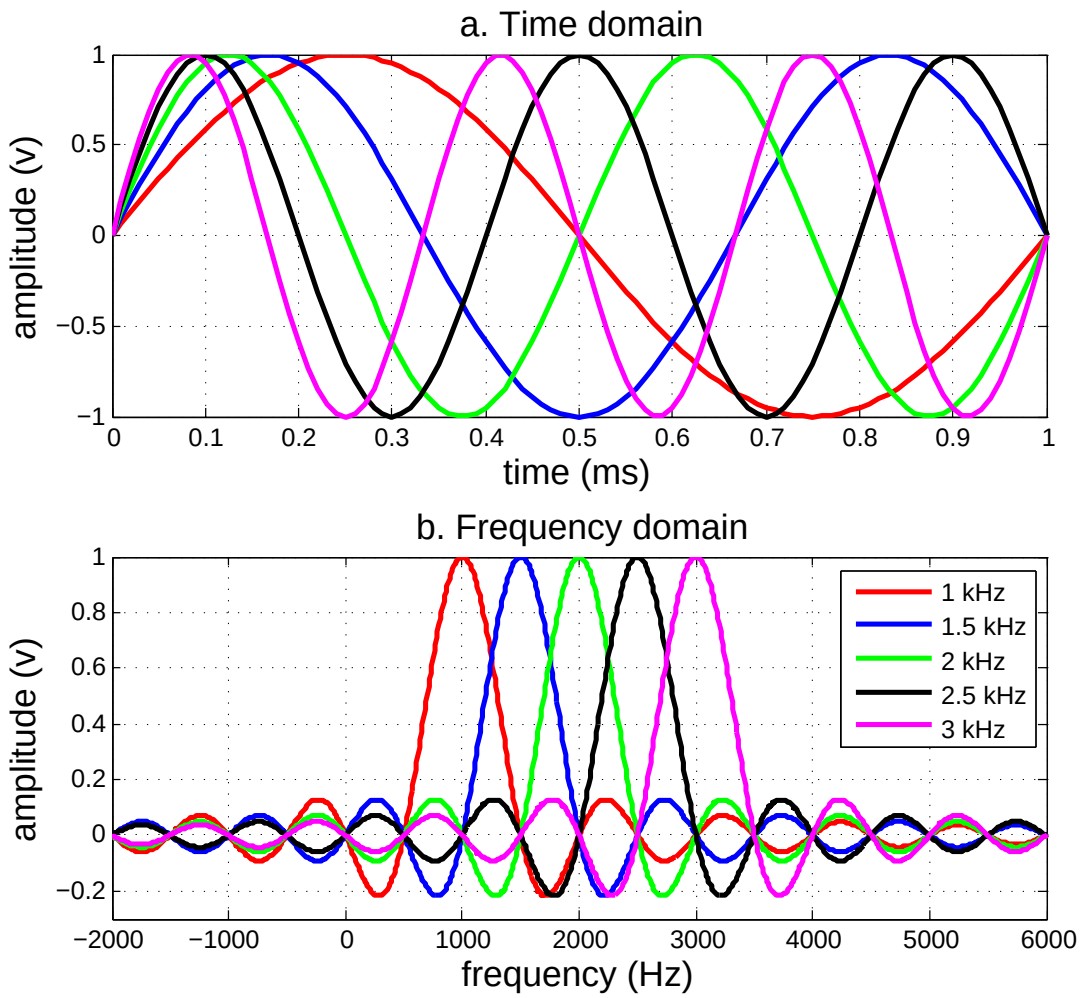


Figure 2.2: Illustration of an OFDM symbol with 5 subcarriers.

where $X(k)$ is the data stream transmitted on the kth subcarrier, and T is the symbol duration of one OFDM symbol. $f_k = k\Delta f$ is the frequency of the kth subcarrier, where Δf is the subcarrier spacing and $T\Delta f = 1$. Assuming that the time domain OFDM symbol $x(t)$ is sampled at an interval of $T_s = \frac{T}{N}$, the corresponding samples of $x(t)$ can be expressed as

$$x(n) = \sum_{k=0}^{N-1} X(k) e^{j2\pi f_k \frac{nT}{N}}, \quad n = 0, 1, \cdots, N-1. \tag{2.3}$$

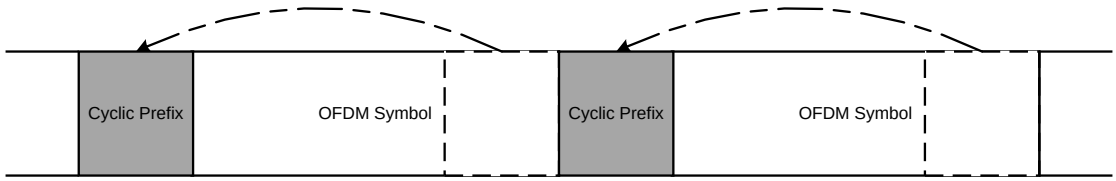


Figure 2.3: The structure of OFDM signal with cyclic prefix.

Substituting $f_k = \frac{k}{T}$ into (2.3), the above equation can be rewritten as

$$\begin{aligned} x(n) &= \sum_{k=0}^{N-1} X(k) e^{j2\pi \frac{k}{T} \frac{nT}{N}} \\ &= \sum_{k=0}^{N-1} X(k) e^{j2\pi \frac{kn}{N}}, \quad n = 0, 1, \cdots, N-1. \end{aligned} \tag{2.4}$$

Clearly, equation (2.4) is exactly the expression of inverse discrete Fourier transform (IDFT) of $X(k)$, which indicates that OFDM modulation process can be effectively implemented by using IDFT. In order to reduce the computational burden and provide a more efficient OFDM system, inverse fast Fourier transform (IFFT) can be employed instead of the IDFT. Figure 2.2 provides an illustration of an OFDM symbol with 5 subcarriers, where Fig. 2.2(a) represents the construction of the time domain OFDM symbol and Fig. 2.2(b) depicts how the OFDM symbol looks like in the frequency domain.

To deal with the time dispersion of wireless channels, a cyclic extension of the OFDM symbol is generally employed in OFDM systems, named cyclic prefix (CP). The basic idea of CP is to repeat the end part of the time domain OFDM symbol in the beginning to create a guard period between adjacent OFDM symbols. The cyclicly extended OFDM symbol is illustrated in Fig. 2.3. As long as the duration of CP is longer than the maximum excess delay of the wireless channel, the intersymbol interference (ISI) corrupted part of an OFDM signal stays within the guard period, and can be removed later at the receiver. Therefore, the impact of multipath distortion on the orthogonality among subcarriers of an OFDM signal can be removed.

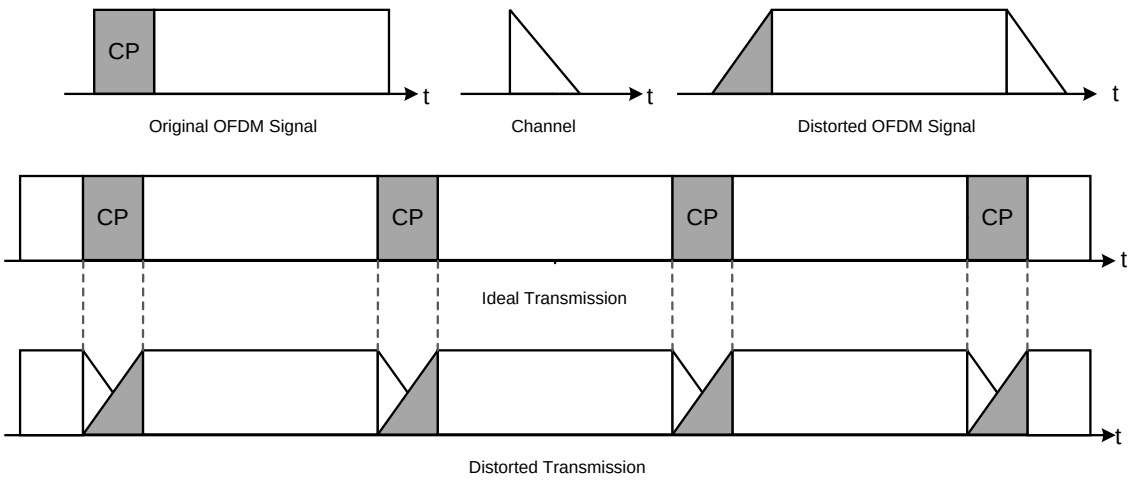


Figure 2.4: ISI elimination in OFDM using cyclic prefix.

Figure 2.4 demonstrates the principle of ISI elimination in OFDM using CP.

2.3.2 Applications of OFDM Technology

As an exciting technology for the modern wireless communications, OFDM has been employed by various existing and evolving standards. A brief introduction of some existing applications of OFDM is provided, including LTE, IEEE 802.11, IEEE 802.16 and Digital Video Broadcasting-Terrestrial (DVB-T).

LTE Long-Term Evolution is a standard for cellular services with high-speed data transmission [54]. Started in 2008, the 3rd Generation Partnership Project (3GPP) standard LTE provides an uplink speed of up to 50 megabits per second (Mbps) and a downlink speed of up to 100 Mbps. OFDM is the modulation scheme for the downlink of LTE, while its downlink multiplexing is accomplished via orthogonal frequency-division multiple access (OFDMA). The basic subcarrier spacing of an OFDM signal in LTE is 15 kHz, with a reduced subcarrier spacing of 7.5 kHz available for some special scenarios.

IEEE 802.11 IEEE 802.11, with a marketing name of WiFi, is a set of popular standards for the broadband wireless local area network (WLAN). OFDM technology is employed in the IEEE 802.11 family such as 802.11a, 802.11g and 802.11n [55, 56]. IEEE 802.11a is an amendment to the original IEEE 802.11 standard, which uses a 52-subcarrier OFDM with a throughput of up to 54 Mbps in the 5 GHz band. Later, the system is extended to the 2.4 GHz band by the amendment IEEE 802.11g. In 2009, IEEE 802.11n was released, which can increase the network throughput to 600 Mbps by supporting multiple-input multiple-output and frame aggregation [56].

IEEE 802.16 IEEE 802.16, under a marketing name of WiMAX, is another series of wireless broadband standards developed for the global deployment of broadband wireless metropolitan area networks (WMAN) [57]. IEEE 802.16 specifies the air interface of fixed broadband wireless access systems that support multimedia services during the spectrum band from 10 to 60 GHz. License-exempt frequencies below 11 GHz are also considered in IEEE 802.16, where improved PHY and MAC mechanisms such as dynamic frequency selection are introduced [57]. OFDM technology is introduced into IEEE 802.16 to improve the overall system performance, including WMAN-OFDM and WMAN-OFDMA.

DVB-T Digital Video Broadcasting-Terrestrial is the DVB European-based consortium standard for the broadcast transmission of digital terrestrial television in very-high frequency (VHF) and ultra-high frequency (UHF). DVB-T makes efficient utilization of spectrum and can transmit Internet pages, compressed digital audio and video data, and so on. To address the transmission of information with high data rate, OFDM technology is adopted in DVB-T standard [58]. As one popular digital TV broadcast standard, DVB-T has been further developed into new standards, such as Digital Video Broadcasting-Second Generation Terrestrial (DVB-T2) [59] and Digital Video Broadcasting-Handheld (DVB-H) [60].

2.3.3 Security Vulnerabilities in OFDM

Due to the distinct time and frequency characteristics, the physical layer of OFDM systems is transparent to adversaries. Transmission parameters in an OFDM system, such as the symbol duration, CP length, sampling frequency and number of subcarriers, can be blindly estimated by any user within the listening range of the transmitter. Consequently, malicious attacks to OFDM systems can be launched by adversaries without any prior information.

Blind estimation techniques for OFDM system parameters have been extensively investigated. A blind OFDM receiver that exploited both time- and frequency-domain correlations of the received signal was designed in [61]. In [62], OFDM symbol duration was estimated using a cyclic correlation of the received signals, and the CP length was derived by performing a correlation test for the redundancy induced by the cyclic extension. For the sampling frequency used in an OFDM system, it can be estimated through a cyclic spectrum analysis method, as reported in [63]. Meanwhile, the number of subcarriers of an OFDM signal can be figured out through a Gaussianity test [62]. In case that not all subcarriers of an OFDM signal are employed for the transmission, active subcarriers can also be identified by analyzing the subcarrier power level at the output of fast Fourier transform (FFT) [64]. Moreover, based on the second-order cyclostationarity of OFDM signals, the parameter estimation for OFDM signals impaired by a time-dispersive channel was studied in [65]. Similarly, a blind OFDM signal recognition algorithm, which could achieve a reasonably good performance at low SNRs for various channel conditions, was also proposed [66].

To sum up, adversaries can locally derive all necessary physical-layer parameters of an OFDM system without any prior information, which makes OFDM fragile to both passive and active attacks from the adversaries. Transmission-level techniques for enhancing the built-in security of OFDM signals have yet to be investigated.

2.4 Summary

Wireless communications is susceptible to malicious attacks due to the open-air nature of wireless medium. Traditional security approaches that exploit authentication and encryption at the link and upper layers of the protocol stack cannot completely handle the security issues in modern wireless communication systems, because of their inherent weaknesses. Thus, physical layer security, which exploits the physical-layer features such as the continual randomness from wireless medium and the RF-DNAs of wireless devices to defend against malicious attacks, has emerged as an effective and valuable paradigm to complement the traditional wireless security techniques. In a study related to modern wireless communications, OFDM, which has been widely employed in modern wireless networks due to its high spectral efficiency and robustness against multipath fading, needs to be addressed. Unfortunately, OFDM is vulnerable to malicious attacks due to its distinct time and frequency characteristics at the physical layer. Therefore, it would be appropriate to consider OFDM in the investigation of physical layer security due to its wide popularity and inherent security vulnerabilities. In addition, it is noteworthy that solutions to secure wireless communications need to be updated regularly based on the situation awareness, since risks and threats in wireless networks are time- and location-varying.

Chapter 3

Active User Recognition through Low Complexity Time Domain OFDM Signal Detection

Effective and efficient security solutions can be performed by wireless communication systems based on the security risk assessment of the operating environment. As any user in a wireless network could be a potential security threat, the number of active users can be employed to indicate the security level of a wireless environment. In this chapter, a robust and simple OFDM signal detection algorithm is developed to recognize the presence of active users. The solution to estimate the number of active users will be provided later in Chapter 4.

The existence of active users can be recognized by verifying the presence of signals they radiated. In light of the widespread deployment of OFDM in wireless communications, a time domain pilot correlation (TDPC) algorithm to detect OFDM signals with frequency domain inserted pilots is proposed in this chapter. The proposed method is based on cyclic correlation between the complex conjugate multiplication of adjacent received signal segments and a local time domain pilot reference derived from the inserted pilots. The maximum correlation magnitude is compared with a

properly selected threshold to determine the existence of active users. Interference mitigation techniques, including periodic signal segmentation and complex conjugate multiplication based phase rotation locking, are developed in the algorithm to improve the detection reliability. It has been validated by simulation results that the TDPC algorithm can achieve reliable detection of OFDM signals even at low SNRs and is robust to both timing and frequency offsets.

3.1 Introduction

Effective and efficient security provisioning can be achieved in wireless communications relying on the risk awareness of the wireless environment. Since any user in a network, even a present legitimate user, can be a potential threat to the security of wireless transmissions [15], a communication system can determine the communication risk from the number of active users in an operating environment, and then launch appropriate defending strategies. In order to avoid unnecessary estimation process for the number of active users and improve the system efficiency, the presence of active users needs to be first confirmed. Generally, the existence of active users can be recognized through the detection of signals they radiated. As OFDM is one of the most widely-used technologies in modern wireless communication systems, reliable and efficient signal detection techniques for OFDM signals are worthy of research efforts.

Several technical challenges need to be addressed in the detection of OFDM signals in wireless networks. First, reliable signal detection should be accomplished within limited time duration, where the processing time is typically proportional to the complexity of a detection algorithm. Due to the mobility and flexibility of wireless communications, the operating environment is time-varying, leading to temporal validity of the detection results. Second, the SNR of signals received at the detection node may be very low since signals of active users may be severely attenuated by fading and shadowing. The low SNR condition normally results into an incorrect

detection decision. In addition, timing and frequency synchronization is unavailable at detection devices, particularly when the received signal strength is low. Since the existence of signals to be detected is unknown, it is impossible to perform timing and frequency offset estimation before the signal detection process. This challenge becomes more pronounced in detecting OFDM signals that are extremely sensitive to synchronization errors.

The detection of OFDM signals has received substantial attention from both academia and industry, particularly in the realm of spectrum sensing for cognitive radio communications. Detection techniques for OFDM can be generally classified into two categories: blind methods and feature based methods [67]. Energy detection is a typical blind method which makes a decision by estimating the energy of the received signals [68]. Non-blind methods rely on certain special features of OFDM signals that are usually introduced by the cyclic prefix and in-band pilots. The insertion of CP introduces cyclostationarity into OFDM signals, which can be employed to detect the presence of OFDM signals [69–72]. However, the performance of these CP-based signal detection methods highly depend on the length of CP. When the duration of CP is short, a long detection time is required to achieve satisfactory detection confidence. In-band pilot based frequency domain detection algorithms for OFDM signals were proposed in [73–76], but their implementations are limited by the computational complexity of FFT operation in the detection process though they usually have high detection reliability. Recently, a time domain symbol autocorrelation method for pilot inserted OFDM signals was reported [77]. Unfortunately, it failed to exploit the pilot patterns to differentiate different communication systems.

In this chapter, a time domain pilot correlation (TDPC) algorithm for detecting OFDM signals with frequency domain inserted pilots is developed. To be specific, the complex conjugate multiplication (CCM) of adjacent received signal segments is cyclicly correlated with a local time domain reference derived from the inserted pilots. The existence of active users is determined by comparing the maximum correlation magnitude with a properly selected threshold. In the proposed algorithm, timing

offset (TO) in the received signals is approximately compensated by the cyclic correlation due to the periodicity of the OFDM pilot sequence in the time domain. The impact of noise on the detection reliability is mitigated by a time domain segment averaging following the complex conjugate multiplication enabled phase rotation locking. The detection robustness to frequency offset (FO) is improved by only taking into consideration the magnitude of the correlation function, because frequency offset just leads to a phase rotation of the time domain OFDM signals. It is also noteworthy that this pilot based detection scheme can achieve a user identification purpose, since different OFDM systems often have different pilot patterns.

The organization of this chapter is as follows. The system model considered in this chapter is introduced in Section 3.2. The proposed TDPC detection algorithm and affiliated interference mitigation techniques are presented in Section 3.3. The simulation results are provided to validate the analysis and evaluate the performance of the proposed technique in Section 3.4. At last, this chapter is summarized in Section 3.5.

3.2 System Model

In this study, an OFDM based wireless network is considered, where OFDM signals would be present if any active user exists. The same as most of the OFDM based wireless communication systems, pilots are inserted into OFDM signals for channel estimation and synchronization [78], and are considered as public information in the network. In order to simplify the analysis, it is assumed that the same pilots are inserted at fixed subcarriers of each OFDM signal in the frequency domain. In addition, a slow time-varying Rayleigh fading channel is considered in the model, in which the channel impulse response is invariant over at least two adjacent OFDM signals.

With the insertion of the in-band pilots, N subcarriers of each OFDM signal can be divided into two sets: pilot subcarriers $P(k)$ and data subcarriers $D(k)$. The time

domain OFDM symbol after N-point IFFT can therefore be expressed as

$$x(n) = p(n) + d(n), \tag{3.1}$$

where

$$p(n) = \frac{1}{\sqrt{N}} \sum_{k \in \mathcal{P}} P(k) W_N^{kn}, \tag{3.2}$$

$$d(n) = \frac{1}{\sqrt{N}} \sum_{k \in \mathcal{D}} D(k) W_N^{kn}, \tag{3.3}$$

and

$$W_N = \exp(j2\pi/N). \tag{3.4}$$

$\mathcal{P}$ denotes the set of pilot subcarriers, while $\mathcal{D}$ denotes the set of data subcarriers. Before the signals are sent out by the transmitter, a cyclic prefix is inserted at the beginning of each OFDM symbol to deal with the delay spread of wireless channels [79]. Suppose the length of the CP is N_{CP}, which is longer than the channel delay spread, the total symbol duration of each transmitted OFDM signal becomes $N_s = N + N_{CP}$. It can be concluded from (3.1), a time domain OFDM signal can be taken as a summation of two components: time domain data-carrying sequence and time domain pilot sequence.

Propagated through a wireless channel with a length of L, the OFDM signal received at the detection device, including the impact of timing and frequency offsets between the transmitter and detection device[1], can be written as

$$\begin{aligned} r(n) &= W_N^{(n-\tau_0)\varepsilon} \sum_{l=0}^{L-1} h(l) x(n - \tau_0 - l) + w(n) \qquad (3.5) \\ &= W_N^{(n-\tau_0)\varepsilon} \sum_{l=0}^{L-1} h(l) p(n - \tau_0 - l) + W_N^{(n-\tau_0)\varepsilon} \sum_{l=0}^{L-1} h(l) d(n - \tau_0 - l) + w(n), \\ &\qquad\qquad n = 0, 1, \cdots, N_s - 1, \end{aligned}$$

[1]Please refer to Appendix A for a brief introduction of the timing and frequency offsets in OFDM.

where τ_0 represents the timing offset in terms of the sampling interval, ε is the frequency offset normalized by the subcarrier spacing, $h(l)$ denotes the complex fading gain of the lth path of the multipath channel, and $w(n)$ denotes the additive white Gaussian noise (AWGN) with a mean of 0 and a variance of σ_w^2.

In OFDM, the data subcarriers $D(k), k \in \mathcal{D}$ can generally be modeled as independent random variables. When the size of $\mathcal{D}$ is large, the time domain data sequence $d(n)$ can be considered as a zero-mean Gaussian distributed variable with a variance of σ_d^2, by invoking the central limit theorem (CLT). Under the assumption that $\sum_{l=0}^{L-1} |h(l)|^2 = 1$, the received data-carrying signal also follows a zero-mean Gaussian distribution with variance σ_d^2. As the pilots and transmitted data are independent of each other, the time domain data-carrying signal can then be treated as Gaussian noise to the time domain pilot sequence. Therefore, the received signal $r(n)$ can be rewritten as

$$r(n) = W_N^{(n-\tau_0)\varepsilon} \sum_{l=0}^{L-1} h(l)p(n-\tau_0-l) + \hat{w}(n), \tag{3.6}$$

where $\hat{w}(n)$ denotes a combined noise consisting of the data-carrying sequence and AWGN. Since $W_N^{(n-\tau_0)\varepsilon} \sum_{l=0}^{L-1} h(l)d(n-\tau_0-l)$ and $w(n)$ are independent of each other, $\hat{w}(n)$ follows a zero-mean Gaussian distribution with a variance of $\sigma_d^2+\sigma_w^2$. Obviously, the time domain pilot sequence provides a distinctive pattern for the detection of OFDM signals with frequency domain inserted pilots.

Without loss of generality, there are two hypotheses for the OFDM signal detection in the time domain:

$$\begin{aligned} \mathcal{H}_0 \quad &: \quad r(n) = w(n), \quad k = 0, 1, \cdots, N_s - 1; \\ \mathcal{H}_1 \quad &: \quad r(n) = W_N^{(n-\tau_0)\varepsilon} \sum_{l=0}^{L-1} h(l)p(n-\tau_0-l) + \hat{w}(n), \quad k = 0, 1, \cdots, N_s - 1. \end{aligned} \tag{3.7}$$

Here, hypothesis $\mathcal{H}_0$ means the absence of active users while $\mathcal{H}_1$ denotes the presence of active users.

3.3 Proposed TDPC Detection Algorithm

3.3.1 Interference Mitigation Techniques

Under the hypothesis that active users are present, the SNR of OFDM signals received at the detection device may be very low, due to the severe signal attenuation caused by fading and shadowing. Meanwhile, since the existence of active users is unknown prior to the detection process, timing and frequency synchronization cannot be achieved before the detection operation. Therefore, special interference mitigation techniques are developed to improve the detection reliability of the proposed TDPC algorithm.

One important fact is that all transmitted OFDM signals have an identical time domain pilot sequence with a period of N_s. As a result, even with an unknown timing offset, segmentation with a period of N_s would still provide a complete time domain pilot sequence in each signal segment but in a circularly rotated order. Cyclic correlation can thus be adopted to combat against the unknown timing offset. Time domain averaging can be employed to mitigate the interference from the data-carrying sequence and AWGN. However, it is noteworthy that frequency offset would cause a time domain phase rotation of the OFDM signals, so that direct time domain segment averaging may eliminate the pilot component when segments have inverse phases, and then degrade the detection performance. Considering that the phase rotation between each two adjacent OFDM segments is a constant, complex conjugate multiplication between every two adjacent received signal segments can be performed before the average operation to mitigate the effect of frequency offset.

The block diagram of the proposed TDPC detection algorithm is presented in Fig. 3.1. The first step of this algorithm is to segment the received signals with an equal length of N_s. When OFDM signals present, any two adjacent segments m and $m+1$

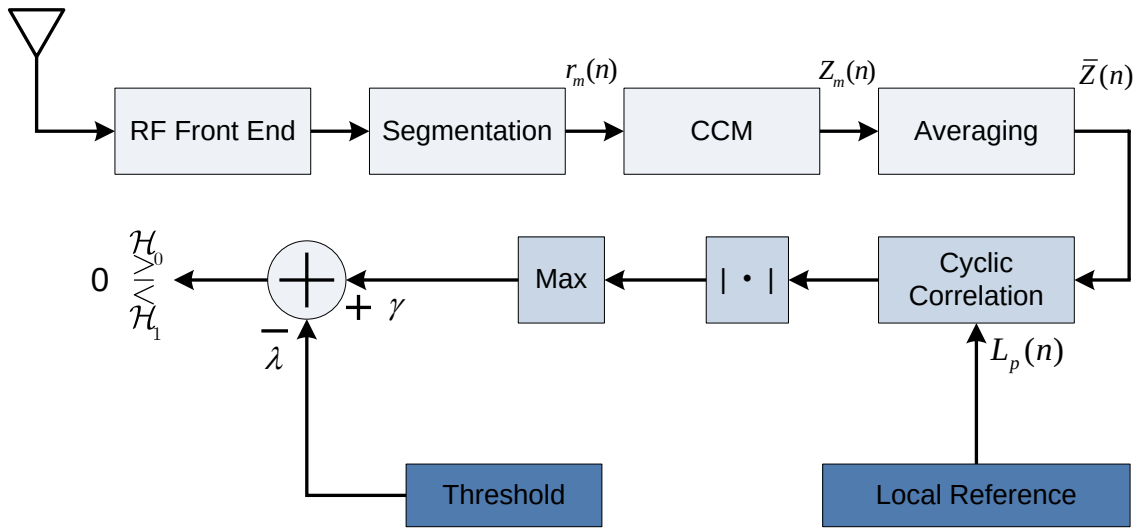


Figure 3.1: Block diagram of the proposed TDPC detection algorithm.

can be expressed as

$$r_m(n) = W_N^{(n+(m-1)N_s-\tau_0)\varepsilon} \sum_{l=0}^{L-1} h(l)p(n-\tau_0-l) + \hat{w}_m(n), \quad n = 0, 1, \cdots, N_s - 1, \tag{3.8}$$

and

$$r_{m+1}(n) = W_N^{(n+mN_s-\tau_0)\varepsilon} \sum_{l=0}^{L-1} h(l)p(n-\tau_0-l) + \hat{w}_{m+1}(n), \quad n = 0, 1, \cdots, N_s - 1. \tag{3.9}$$

Comparing $r_m(n)$ and $r_{m+1}(n)$, we can find that the phase rotation between two neighboring segments, which is induced by the frequency offset, is a constant $W_N^{N_s\varepsilon}$. Complex conjugate multiplication between two adjacent signal segments is thus em-

ployed in this algorithm to mitigate the damage of frequency offset, that is

$$\begin{aligned} Z_m(n) &= r_m^*(n) \times r_{m+1}(n) \\ &= W_N^{N_s\varepsilon} \left| \sum_{l=0}^{L-1} h(l)p(n-\tau_0-l) \right|^2 \\ &\quad + \hat{w}_{m+1}(n) W_N^{-(n+(m-1)N_s-\tau_0)\varepsilon} \left[\sum_{l=0}^{L-1} h(l)p(n-\tau_0-l) \right]^* \\ &\quad + \hat{w}_m^*(n) W_N^{(n+mN_s-\tau_0)\varepsilon} \left[\sum_{l=0}^{L-1} h(l)p(n-\tau_0-l) \right] \\ &\quad + \hat{w}_m^*(n)\hat{w}_{m+1}(n) \ . \end{aligned} \tag{3.10}$$

It can be found from (3.10) that the variances of the second and third terms of $Z_m(n)$ are proportional to the noise power $\sigma_d^2 + \sigma_w^2$, while the fourth term has a variance proportional to $(\sigma_d^2 + \sigma_w^2)^2$. As a result, when the SNR is very low, the variances of the second and third terms are relatively very small compared to that of the fourth term while they all have a mean of 0. It is thus reasonable to ignore the second and third terms. $Z_m(n)$ can then be approximated as

$$\begin{aligned} Z_m(n) &\approx W_N^{N_s\varepsilon} \left| \sum_{l=0}^{L-1} h(l)p(n-\tau_0-l) \right|^2 + \hat{w}_m^*(n)\hat{w}_{m+1}(n) \\ &= W_N^{N_s\varepsilon} \left| \sum_{l=0}^{L-1} h(l)p(n-\tau_0-l) \right|^2 + w'_m(n). \end{aligned} \tag{3.11}$$

Further expansion of (3.11) gives us

$$\begin{aligned} Z_m(n) &= W_N^{N_s\varepsilon} \sum_{l=0}^{L-1} |h(l)|^2 \, |p(n-\tau_0-l)|^2 \\ &\quad + W_N^{N_s\varepsilon} \sum_{l_1=0}^{L-1} \sum_{l_2=0, l_2\neq l_1}^{L-1} h(l_1)h^*(l_2)p(n-\tau_0-l_1)p^*(n-\tau_0-l_2) \\ &\quad + w'_m(n). \end{aligned} \tag{3.12}$$

Under the assumption of Rayleigh fading channel, $h(l)$ for $l = 0, 1, \cdots, L-1$ can be modelled as L independent and identically distributed (i.i.d.) complex Gaussian variables with zero-mean and variance σ_h^2. Therefore, $|h(l)|^2$ follows an exponential distribution with a parameter $1/\sigma_h^2$. In the second term of (3.12), $h(l_1)$ and $h^*(l_2)$ are two independent zero-mean complex Gaussian variables, while $W_N^{N_s\varepsilon}$, $p(n-\tau_0-l_1)$ and $p^*(n-\tau_0-l_2)$ can all be taken as constants for a specific communicating pair. Consequently, the second term of (3.12) would have a mean of 0. The averaging of $Z_m(n)$ over G pairs of successive OFDM segments can then be obtained as

$$\begin{aligned}
\bar{Z}(n) &= \frac{1}{G}\sum_{m=0}^{G-1} Z_{2m}(n) \\
&\approx \sigma_h^2 W_N^{N_s\varepsilon} \sum_{l=0}^{L-1} |p(n-\tau_0-l)|^2 + \bar{w}'_m(n) \\
&= \sigma_h^2 W_N^{N_s\varepsilon} \Lambda(n-\tau_0) + \bar{w}'_m(n),
\end{aligned} \tag{3.13}$$

where

$$\Lambda(n-\tau_0) = \sum_{l=0}^{L-1} |p(n-\tau_0-l)|^2 . \tag{3.14}$$

Note that the total number of segments employed in this calculation is $M = 2G$. It can be seen from (3.13) that the distortions from the multipath channel, data-carrying sequence and AWGN can be mitigated through the average operation. The reliability of signal detection can then be enhanced, particularly in low SNR environments.

3.3.2 Proposed Detection Metric

In the proposed OFDM signal detection algorithm, a local time domain pilot reference $L_p(n)$ is generated from the frequency domain inserted pilots that are public information in the network. Under a multipath channel with a length of L, the local

reference $L_p(n)$ can be derived as

$$L_p(n) = \Lambda(n) = \sum_{l=0}^{L-1} |p(n-l)|^2, \quad n = 0, 1, \cdots, N_s - 1. \tag{3.15}$$

In practice, any arbitrary point may be used as the initial sample time instance at the detection device, so that timing offset usually occurs. Considering that timing offset just cyclicly rotates the averaged CCM result $\bar{Z}(n)$ which includes a complete time domain pilot sequence when OFDM signals present, it can be compensated by cyclicly correlating $\bar{Z}(n)$ with the local reference $L_p(n)$. The cyclic correlation between $\bar{Z}(n)$ and $L_p(n)$, denoted by $T(\nu)$, can be calculated as

$$\begin{aligned} T(\nu) &= \frac{1}{N_s} \sum_{n=0}^{N_s-1} L_p(n) \bar{Z}\left(\mathrm{mod}\left\{\frac{n+\nu}{N_s}\right\}\right), \\ &\qquad \nu = 0, 1, \cdots, N_s - 1, \end{aligned} \tag{3.16}$$

where $\mathrm{mod}\{\cdot\}$ denotes the modulo operation. Under hypothesis $\mathcal{H}_1$, $T(\nu)$ can be rewritten as

$$\begin{aligned} T(\nu) &= \frac{\sigma_h^2}{N_s} \sum_{n=0}^{N_s-1} L_p(n) \Lambda\left(\mathrm{mod}\left\{\frac{n-\tau_0+\nu}{N_s}\right\}\right) W_N^{N_s\varepsilon} \\ &\quad + \frac{1}{N_s} \sum_{n=0}^{N_s-1} L_p(n) \bar{w}'_m\left(\mathrm{mod}\left\{\frac{n+\nu}{N_s}\right\}\right), \\ &\qquad \nu = 0, 1, \cdots, N_s - 1. \end{aligned} \tag{3.17}$$

Theoretically, when $\nu = \tau_0$, a correlation peak should be observed, that is

$$T(\tau_0) = \frac{\sigma_h^2}{N_s} \sum_{n=0}^{N_s-1} [\Lambda(n)]^2 W_N^{N_s\varepsilon} + \frac{1}{N_s} \sum_{n=0}^{N_s-1} \Lambda(n) \bar{w}'_m(n+\tau_0). \tag{3.18}$$

Since frequency offset would distort the correlation result by introducing a phase rotation $W_N^{N_s\varepsilon}$, the magnitude of $T(\nu)$ is calculated in this algorithm to further miti-

gate the effect of FO. As a result, when $\nu = \tau_0$, we can have

$$|T(\tau_0)| = \sqrt{\left\{\frac{\sigma_h^2}{N_s}\sum_{n=0}^{N_s-1}[\Lambda(n)]^2\right\}^2 + V}, \tag{3.19}$$

where V denotes the combining noise as

$$\begin{aligned} V &= \frac{\sigma_h^2}{N_s^2}\sum_{n_1=0}^{N_s-1}[\Lambda(n_1)]^2 W_N^{N_s\varepsilon}\sum_{n_2=0}^{N_s-1}\Lambda(n_2)\bar{w}_m'^*(n_2+\tau_0) \\ &+\frac{\sigma_h^2}{N_s^2}\sum_{n_1=0}^{N_s-1}[\Lambda(n_1)]^2 W_N^{-N_s\varepsilon}\sum_{n_2=0}^{N_s-1}\Lambda(n_2)\bar{w}_m'(n_2+\tau_0) \\ &+\frac{1}{N_s^2}\sum_{n_1=0}^{N_s-1}\Lambda(n_1)\bar{w}_m'^*(n_1+\tau_0)\sum_{n_2=0}^{N_s-1}\Lambda(n_2)\bar{w}_m'(n_2+\tau_0). \end{aligned} \tag{3.20}$$

As shown in (3.19), the phase rotation $W_N^{N_s\varepsilon}$ now only acts on the noise term V. Based on the previous average operation, the power of the noise $\bar{w}_m'(n)$ is significantly reduced. Consequently, the effect of the combining noise V on the magnitude of the correlation $T(\tau_0)$ is limited. A significant correlation peak should still be observed from $|T(\nu)|$ when $\nu = \tau_0$ under hypothesis $\mathcal{H}_1$. Therefore, the impact of frequency offset on the OFDM signal detection can be remarkably mitigated. The detection metric γ can then be obtained as

$$\gamma = \max\{|T(\nu)|\}. \tag{3.21}$$

On the other hand, under hypothesis $\mathcal{H}_0$, no OFDM signal is present. The received signal segments m and $m+1$ will be

$$r_m'(n) = w_m(n), \quad n = 0, 1, \cdots, N_s - 1, \tag{3.22}$$

$$r_{m+1}'(n) = w_{m+1}(n), \quad n = 0, 1, \cdots, N_s - 1. \tag{3.23}$$

After the complex conjugate multiplication, the averaged multiplication result over

G pairs of successive signal segments can be given by

$$\bar{Z}'(n) = \frac{1}{G}\sum_{m=0}^{G-1} w_{2m}^{*}(n) w_{2m+1}(n). \tag{3.24}$$

Following the cyclic correlation between $\bar{Z}'(n)$ and the local reference $L_p(n)$, the magnitude of the correlation, $|T'(\nu')|$, can be mathematically written as

$$\begin{aligned} |T'(\nu')| &= \left| \frac{1}{N_s} \sum_{n=0}^{N_s-1} L_p(n) \bar{Z}' \left(\mathrm{mod} \left\{ \frac{n+\nu'}{N_s} \right\} \right) \right|, \\ & \qquad \nu' = 0, 1, \cdots, N_s - 1. \end{aligned} \tag{3.25}$$

Then, the detection metric when active users are absent can be formulated as

$$\gamma' = \max \{ |T'(\nu')| \}, \tag{3.26}$$

where $\nu' = \tau'$ gives the maximum correlation magnitude.

Comparing γ with γ', we can find that when active users are present, the local reference is correlated with correlative OFDM signals, a correlation peak can thus be observed after the cyclic correlation. In contrast, when active users are absent, the local reference is just correlated with independent noise, the correlation would always be low. The proposed detection metric γ can therefore be used to identify the existence of active users in the OFDM network.

3.3.3 Detection Threshold Selection

The presence of OFDM signals is determined by comparing the detection metric γ against a properly selected threshold λ. If $\gamma > \lambda$, active users are deemed to be present. Otherwise, the detected spectrum channel is considered as vacant. Without loss of generality, the detection threshold in the proposed algorithm is selected with respect to a requirement of the false alarm probability (FAP) P_{fa}, i.e. the probability

that a false decision is made when active users are absent.

For the segment complex conjugate multiplication result $\bar{Z}'(n)$ in (3.24), since $w^*_{2m}(n)$ and $w_{2m+1}(n)$ are independent and identically distributed random variables, $\bar{Z}'(n)$ can be approximated as a Gaussian variable with a mean of 0 and a variance of $\frac{1}{G}\sigma_w^4$ according to the central limit theorem. Due to the property of Gaussian distribution, $T'(\tau')$ in (3.25) is also Gaussian distributed with a mean of 0 and a variance of $\frac{\sum_{n=0}^{N_s-1} L_p^2(n)}{GN_s^2}\sigma_w^4$. As the magnitude of a complex Gaussian variable follows a Rayleigh distribution, it can be asserted

$$|T'(\tau')| \sim Rayleigh\left(\sqrt{\frac{\sum_{n=0}^{N_s-1} L_p^2(n)}{2GN_s^2}}\sigma_w^2\right). \tag{3.27}$$

Then the false alarm probability P_{fa} with respect to γ' can be represented as

$$\begin{aligned} P_{fa} &= Prob(\gamma' > \lambda) \\ &= 1 - F_{ray}\left(\lambda; \sqrt{\frac{\sum_{n=0}^{N_s-1} L_p^2(n)}{2GN_s^2}}\sigma_w^2\right)^{N_s}, \end{aligned} \tag{3.28}$$

where $F_{ray}(x;\sigma)$ denotes the cumulative distribution function (CDF) of Rayleigh distribution,

$$F_{ray}(x;\sigma) = \int_{-\infty}^{x} \frac{u}{\sigma^2} \exp\left(\frac{-u^2}{2\sigma^2}\right) du. \tag{3.29}$$

Given a required false alarm probability P_{fa}, the threshold λ can then be selected as

$$\lambda = raylinv\left((1-P_{fa})^{1/N_s}, \sqrt{\frac{\sum_{n=0}^{N_s-1} L_p^2(n)}{2GN_s^2}}\sigma_w^2\right), \tag{3.30}$$

where $raylinv(y,\sigma)$ is the inverse of the Rayleigh cumulative distribution function.

3.4 Simulation Results

Simulations are carried out to evaluate the performance of the proposed OFDM signal detection algorithm using time domain pilot correlation. The robustness of the proposed TDPC detection algorithm to low SNR, timing offset and frequency offset are estimated. An OFDM system with 256 subcarriers is employed in the simulations. Without further specification, 16 pilots are inserted into each OFDM signal in the frequency domain; the false alarm probability requirement in the threshold selection is set to 0.1; frequency offset is assumed to be 0.1 and timing offset is randomly generated by MATLAB. Sixty received signal segments are averaged to mitigate the interference and noise in the detection operation. In addition, a Rayleigh fading channel with a length of 12 is taken into account in the simulations.

Figure 3.2 evaluates the miss detection probability (MDP) P_{md} (the probability of making an incorrect decision when active users are present) of the proposed TDPC algorithm under different false alarm probability requirements when different numbers of signal segments are averaged. As shown in the figure, a miss detection probability less than 0.001 can always be achieved when SNR is larger than -1 dB in this simulated channel condition. Additionally, with a looser false alarm probability requirement, a better detection performance, in terms of miss detection probability, can be observed. In the meantime, when more segments are averaged in the detection process, the interference and noise can be further mitigated, which leads to an enhanced detection reliability. In order to limit the time cost in the detection process when a large amount of segments need to be averaged in the low SNR environment, a buffer can be utilized to store the previous complex conjugate multiplication result $\bar{Z}_{t-1}(n)$. The averaging process can be reformulated as

$$\bar{Z}_t(n) = \frac{G-1}{G}\bar{Z}_{t-1}(n) + \frac{1}{G}Z_m(n). \tag{3.31}$$

As a result, once a new multiplication result is obtained, the averaging operation can

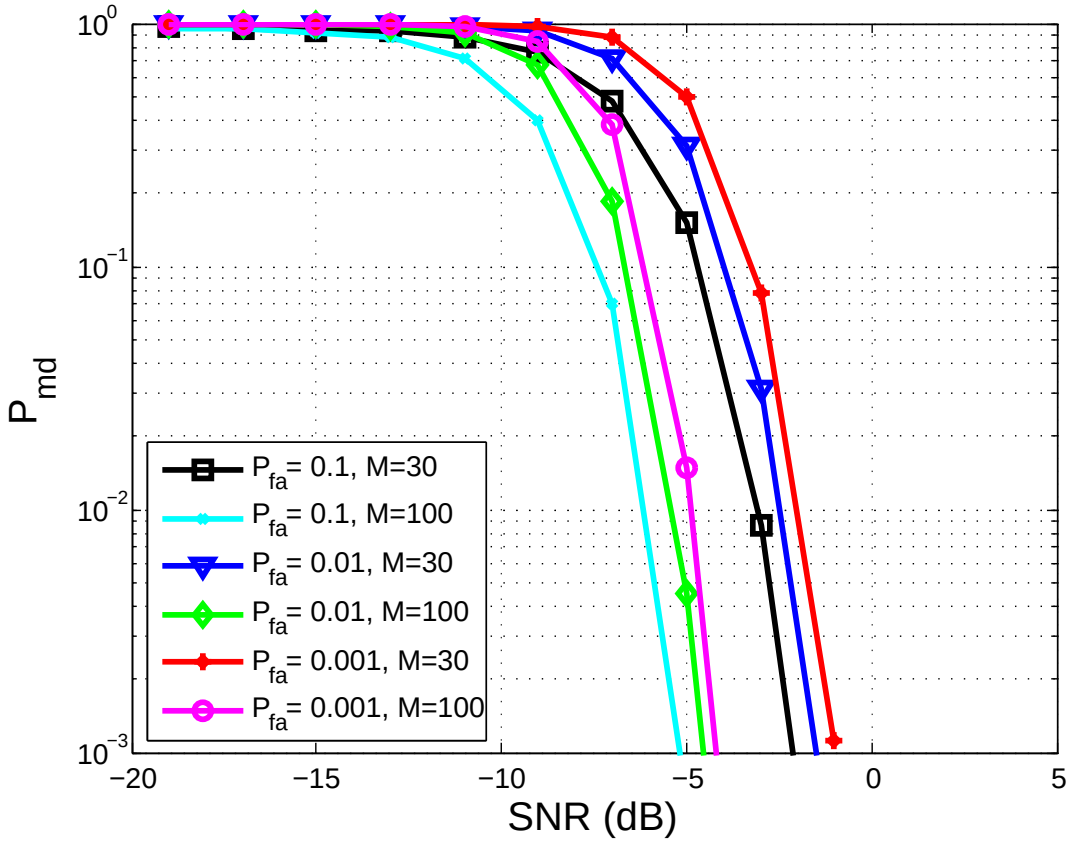


Figure 3.2: Probability of miss detection under different P_{fa} requirements when different numbers of signal segments are averaged. FO = 0.1 and TO is randomly generated.

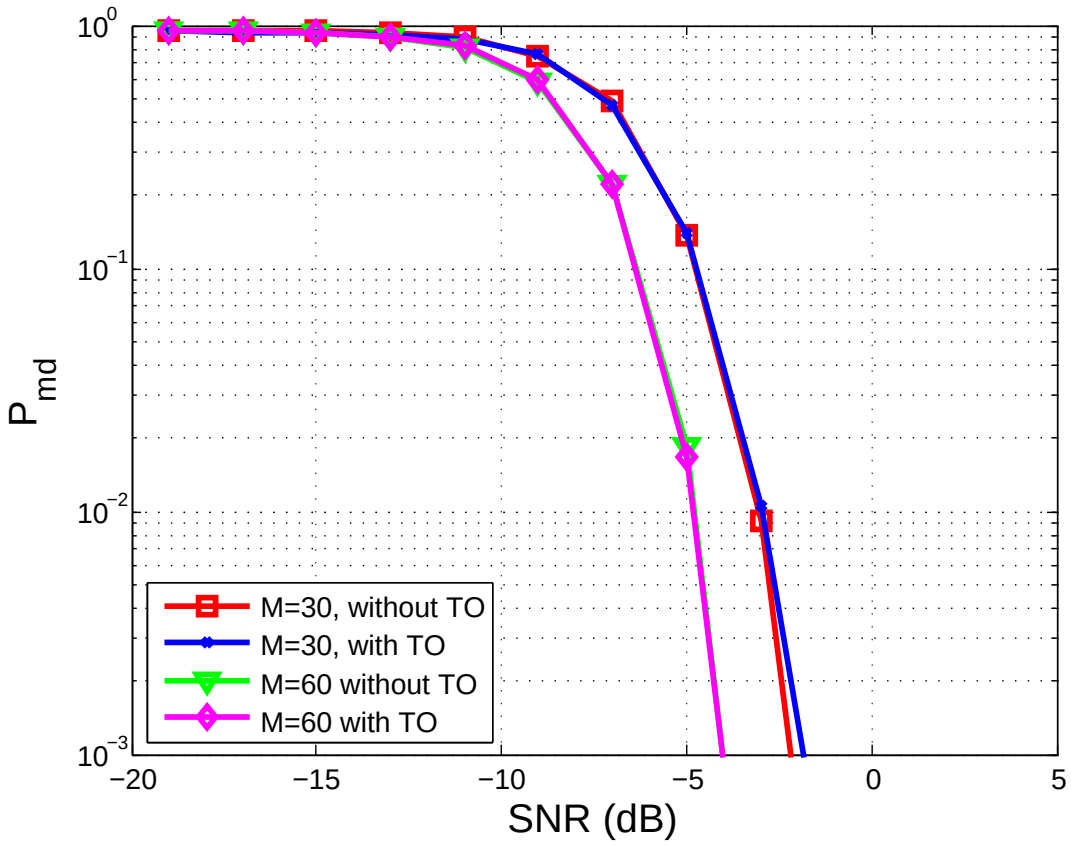


Figure 3.3: Robustness of the proposed TDPC algorithm to timing offset when $P_{fa} = 0.1$ and FO $= 0.1$.

be executed and a timely detection decision can be made by the proposed TDPC algorithm.

The robustness of the proposed detection algorithm to timing and frequency offsets is simulated and presented in Fig. 3.3 and Fig. 3.4, respectively. In Fig. 3.3, we evaluate the P_{md} of the detection algorithm with and without random timing offset between the transmitter and detection device when different numbers of received segments are averaged. It can be concluded from the simulation results that the detection performance only experiences little degradation when there is random timing offset, especially when more segments are averaged in the detection process to further mitigate the effect of the interference and noise. In the study of the robustness to frequency offset, carrier frequency offsets between the transmitted and received sig-

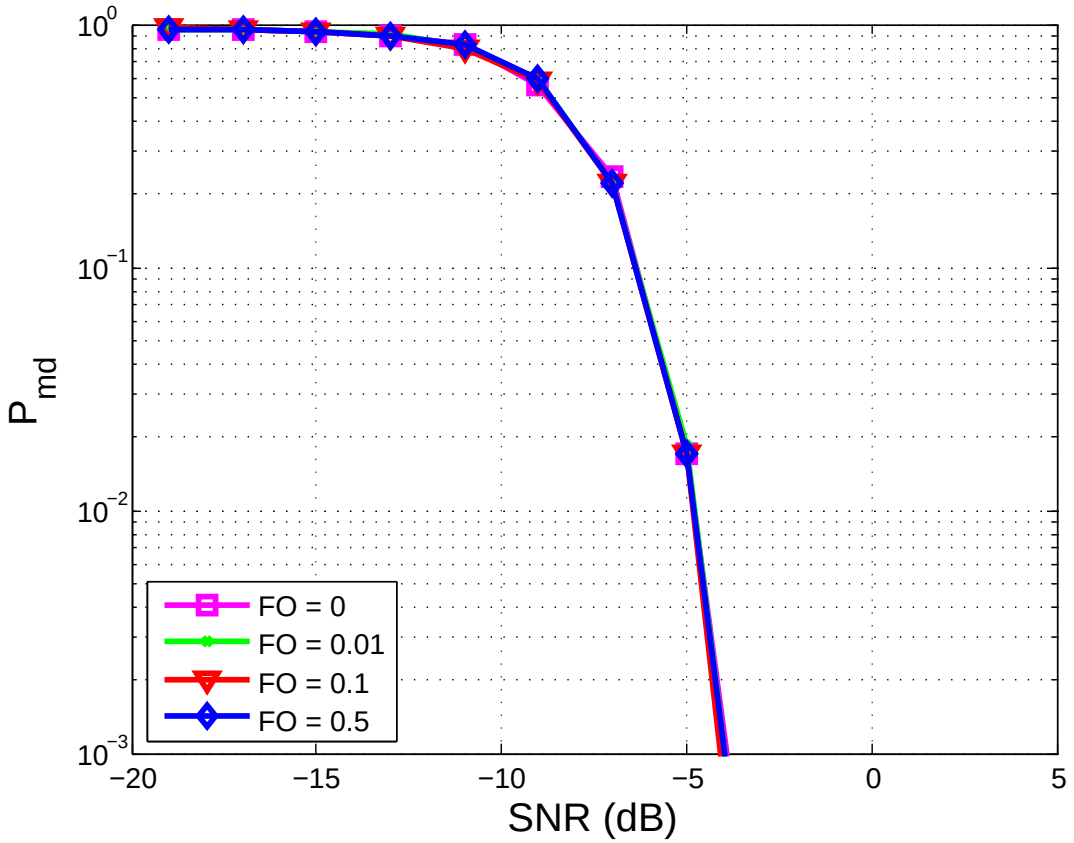


Figure 3.4: Robustness of the proposed TDPC algorithm to frequency offset when $P_{fa} = 0.1$ and TO is randomly generated.

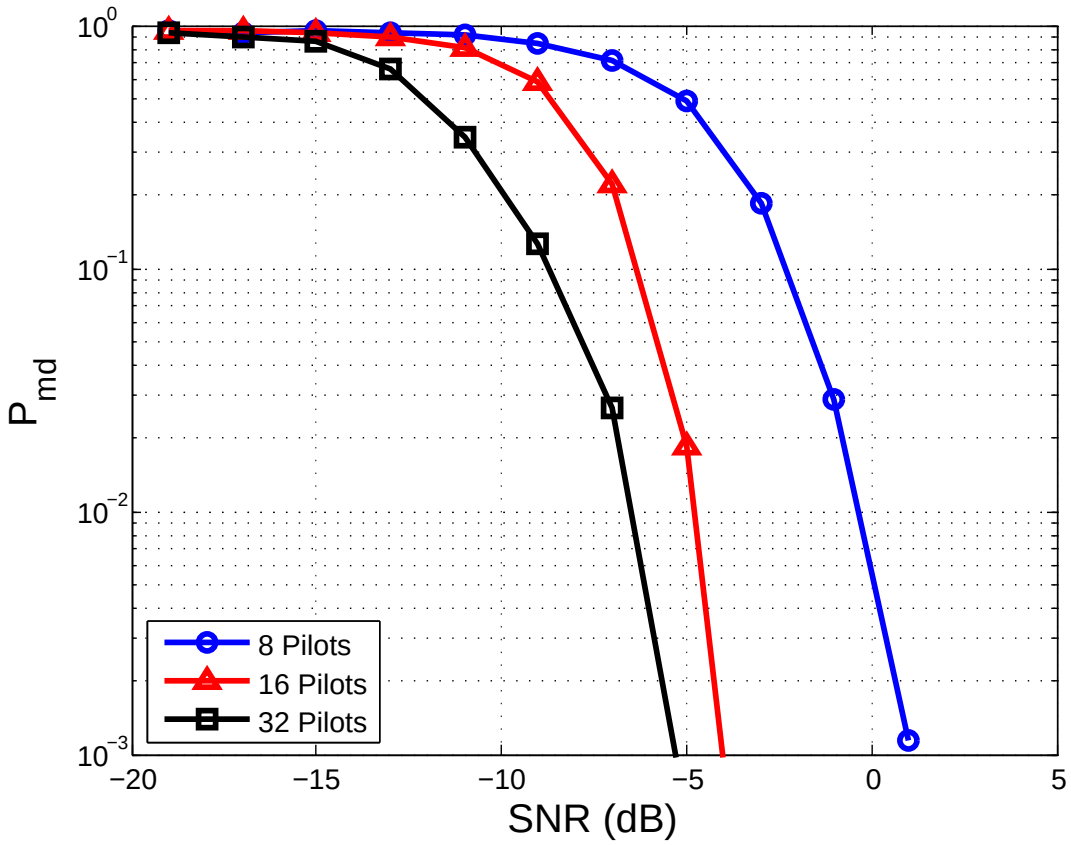


Figure 3.5: Effect of the number of pilots in each OFDM signal on the detection performance. $P_{fa} = 0.1$, FO $= 0.1$, and TO is randomly generated.

nals are set to 0, 0.01, 0.1 and 0.5, respectively, in the simulation. Undistinguishable detection performance in terms of miss detection probability is observed in Fig. 3.4. Therefore, the proposed OFDM signal detection algorithm is robust to both timing and frequency offsets.

The effect of the number of pilot subcarriers in an OFDM signal is also studied in the simulation. While the number of total subcarriers in each OFDM signal is fixed at 256, the number of pilots changes among 8, 16 and 32. It can be observed from Fig. 3.5 that a larger number of pilots in the OFDM signals would result into a better detection performance. This is easy to be explained by (3.5). When more subcarriers are used to transmit the pilots, a stronger time domain pilot pattern is included in each received OFDM signal, leading to a lower miss detection probability.

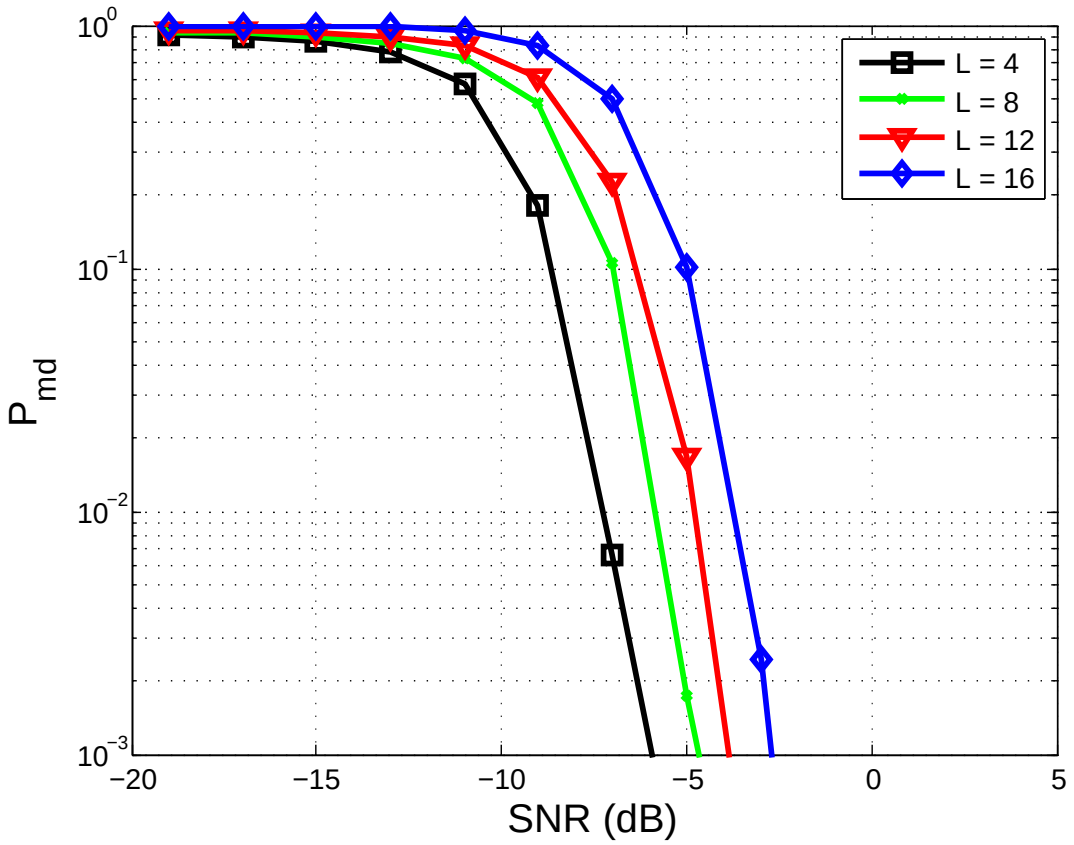


Figure 3.6: Performance of the proposed TDPC algorithm in multipath channels with different delay spreads. $P_{fa} = 0.1$, FO $= 0.1$, and TO is randomly generated.

The performance of the proposed TDPC algorithm in Rayleigh fading channels with different delay spreads is provided in Fig. 3.6. In the simulation, the lengths of the Rayleigh channels are set to 4, 8, 12, and 16, respectively. Frequency offset with a value of 0.1 and random timing offset are added. As shown in the figure, our proposed TDPC algorithm can have higher detection reliability in the Rayleigh fading channel with a shorter delay spread.

3.5 Summary

In order to enable a robust and simple active user detection in wireless networks, a time domain pilot correlation algorithm for detecting OFDM signals with frequency

domain inserted pilots is proposed in this chapter. The time domain cyclic correlation between the complex conjugate multiplication of adjacent received signal segments and a local pilot-based reference is utilized to detect the presence of OFDM signals. The noise effect on the detection reliability is mitigated by a time domain signal segment average following the phase rotation locking processing. The robustness of the proposed detection algorithm to timing offset is improved by the time domain OFDM symbol length based segmentation and the cyclic correlation. The robustness to frequency offset is enhanced by the segment complex conjugate multiplication and the use of the correlation magnitude. Simulation results show that the performance of the proposed detection technique is satisfactory in hostile multipath channel conditions with the presence of both timing and frequency offsets.

Chapter 4

Exploiting Transmitter I/Q Imbalance for Estimating the Number of Active Users

After recognizing the existence of active users in a wireless environment, we would like to estimate the total number of those active users for further security risk analysis. The number of active users in a network is crucial for understanding the security level of wireless operating environments. Since any node in a network could perform malicious attacks and be a potential threat, the transmission risk arises with the increase of active users. This chapter proposes a novel estimation technique for the number of active users by exploiting a typical device RF-DNA—I/Q imbalance, which has been identified as a device-specific hardware impairment and can be utilized to distinguish different wireless devices. In the proposed approach, I/Q imbalance of a transmitter is first estimated from its transmitting signals. The estimate is then compared with the observed I/Q imbalances of previously identified users through a hypothesis testing, where the Euclidean distances between the new estimate and previous observations are adopted as the test metric. If all the Euclidean distances are larger than a properly selected threshold, a new active user is claimed. Finally,

the number of active users is determined by counting all the distinct I/Q imbalances. Simulation results are provided to validate the proposed estimation scheme.

4.1 Introduction

Due to the inherent broadcast nature of radio propagation, wireless communications is vulnerable to a variety of malicious attacks. In principle, any node in a network, even a present legitimate user, may perform hostile attacks such as eavesdropping and jamming. It is almost impossible to prevent data loss or disclosure from one device that can physically access the network [16]. The communication security risk arises along with the increase of coexistent users. Hence, the number of active users in a network can generally indicate the security level of an operating environment, and be used to guide the developing of defending strategies [15]. Ideally, the association mechanism of communication protocols would provide the information of active users. However, the number of clients associated to an access point (AP) is usually not the same as the number of active users in a wireless network. Spoofing attacks can be launched with little effort in wireless communications. Meanwhile, some adversaries may not need to associate with or even strive to hide themselves from APs. Thus, sophisticated strategies to estimate the number of active users need to be developed.

Various techniques for estimating the number of active users have emerged in the last decade. Most of the existing work exploited the statistics of packet retransmissions to estimate the number of active users, which arises from the fact that the network throughput is sensitive to the number of stations competing for channel access [80]. An extended Kalman filter approach, coupled with a change detection mechanism to capture variations in the number of competing terminals in a network, was investigated in [81]. Vercauteren *et al.* proposed two Bayesian estimators, in which the number of competing terminals was modeled as a Markov chain with unknown transition matrix [82]. However, although the aforementioned solutions do

not rely on association mechanisms of network protocols, they are still highly related to certain protocol specifications such as the contention window size. In addition to the packet retransmission statistics, station location information was also adopted to determine the number of active users [83]. Nevertheless, such a scheme only works in a static network, and its performance exceedingly depends on the relative positions among active terminals and the locating precision.

Recently, RF-DNAs of wireless devices have drawn much attention from both academia and industry due to their potential security applications. Hardware impairments, such as I/Q imbalance, frequency and magnitude errors, are acceptable as long as process-caused variations are within a tolerated range. It has been verified that even devices are fabricated using the same manufacturing and packaging processes, the impairments induced by the analog circuits cannot be identical and are normally significant enough for distinguishing one device from all others [3, 27, 52]. In the literature, device RF-DNAs were mainly employed for user identification and authentication using experimental methodologies [27, 52]. In [50], Nguyen *et al.* mentioned that device RF-DNAs could be used to determine the number of attackers in a network. However, they did not pay enough attention on such application. Systematic analysis and design of estimating the number of active users based on device RF-DNAs still remain open.

To that end, this chapter investigates a device RF-DNA based estimation scheme for the number of active users, by exploiting the I/Q imbalance that is recognized as a typical feature of device-specific front-end imperfection. Specifically, I/Q imbalance of a transmitter is first estimated from its transmitting signals. A mathematical model of the I/Q imbalance observation at a receiver, biased by estimation errors, is derived. Then, a hypothesis testing is adopted to determine whether the estimate belongs to any of previously identified users, by comparing the Euclidean distance between the new estimate and previous I/Q imbalance estimate of each identified user with a properly selected threshold. A different-device decision is made when the distance is larger than the threshold, and a new active user is claimed if all the

comparisons give a different-device decision. At the end, the number of active users is obtained by counting all the findings. The proposed scheme is independent of the network protocol and the transmission standard, and it can be easily extended to other device RF-DNAs.

The reminder of this chapter is organized as follows. Section 4.2 introduces the system model and transmitter I/Q imbalance. The proposed estimation algorithm for the number of active users is described in Section 4.3, followed by simulation results in Section 4.4. Finally, conclusions are drawn in Section 4.5.

4.2 System Model and Preliminaries

4.2.1 System Model

In this chapter, a wireless network that consists of multiple active stations is considered. Each terminal in the network is surrounded by several wireless devices which can all be regarded as potential security threats in principle. In order to evaluate the security level of the operating environment and then perform effective defending strategies, a station that is going to transmit data would like to estimate the number of active users in the network.

The wireless network is assumed to be operated in a time-division duplexing (TDD) scheme, where all the stations alternately transmit their signals. This assumption corresponds to numerous practical wireless communication systems, such as WiFi and WiMax. Moreover, it is assumed that the network is in a workable status. Signals transmitted by any node in the network are physically available to all the other terminals.

4.2.2 I/Q Imbalance Induced by the Transmitter

I/Q imbalance characterizes both the amplitude mismatch and phase mismatch between the in-phase (I) and quadrature (Q) branches of a signal constellation, as

illustrated in Fig. 4.1. Generally, I/Q imbalance is caused by two parts of an imperfect radio frequency (RF) front-end circuit in a wideband system: imperfect local oscillator (LO) and imperfect low-pass filter (LPF). Imperfect LO induces frequency-independent amplitude and phase mismatches, while mismatches caused by the imperfection of LPF are frequency-dependent. Since the I/Q imbalance induced by imperfect LO is typically more significant than that caused by LPF imperfection in RF circuits [84], this study only targets on the LO-induced I/Q imbalance. The I/Q imbalance is thus modeled as frequency-independent and constant over the signal bandwidth.

Letting $x(t) = x_I(t) + jx_Q(t)$ represent the baseband signal at a transmitter, the corresponding RF signal $s(t)$, which is distorted by the I/Q imbalance induced by hardware imperfections of the transmitter RF circuit, can be modeled as

$$s(t) = x_I(t)\cos(2\pi f_c t) - (1+\varepsilon)\, x_Q(t)\sin(2\pi f_c t + \phi)\,, \tag{4.1}$$

where f_c denotes the carrier frequency, ε and ϕ indicate the amplitude imbalance and phase orthogonality mismatch between the I and Q branches, respectively. With a perfect receiver that does not induce any I/Q imbalance, the down-converted signal after the LPF at the receiver can be written as

$$y_I(t) = \frac{1}{2}\left[x_I(t) - (1+\varepsilon)\, x_Q(t)\sin(\phi)\right] \otimes h(t) + w'_I(t), \tag{4.2}$$

and

$$y_Q(t) = \frac{1}{2}\left[(1+\varepsilon)\, x_Q(t)\cos(\phi)\right] \otimes h(t) + w'_Q(t), \tag{4.3}$$

where $y_I(t)$ and $y_Q(t)$ represent the in-phase and quadrature components of the received signal, respectively. $\otimes$ indicates the convolution operation. $h(t)$ is the time domain baseband equivalent channel impulse response with a length of L. Under the assumption of a slow time-varying wireless channel, the channel impulse response is taken as invariant during each signal block. $w'(t) = w'_I(t) + jw'_Q(t)$ is the noise after

the translation from RF to baseband, which can be approximated as additive white Gaussian noise by ignoring the impact of LPF on its whiteness. Additionally, the signal $x(t)$, channel $h(t)$ and AWGN $w'(t)$ are considered as statistically independent. After the digital signal processing, the baseband received signal can finally be given by

$$\begin{aligned} y(t) &= 2\left[y_I(t) + jy_Q(t)\right] \\ &= \left[x_I(t) + j\left(1+\varepsilon\right)e^{j\phi}x_Q(t)\right] \otimes h(t) + w(t) \\ &= \left[\mu x(t) + (1-\mu)x^*(t)\right] \otimes h(t) + w(t), \end{aligned} \tag{4.4}$$

where μ is a defined I/Q imbalance parameter that characterizes both the amplitude mismatch ε and phase mismatch ϕ. Mathematically, μ can be described as

$$\mu = \frac{[1 + (1+\varepsilon)e^{j\phi}]}{2}. \tag{4.5}$$

$w(t)$ denotes the AWGN acting on the baseband received signal $y(t)$, which follows a complex Gaussian distribution with zero mean and variance of σ^2, i.e. $w(t) \sim CN(0, \sigma^2)$.

4.3 Proposed Estimation Technique for the Number of Active Users

4.3.1 Estimation of the Transmitter I/Q Imbalance

The goal of the proposed technique is to utilize estimates of transmitter I/Q imbalances to differentiate different transmitters and then determine the number of active users in a network. Hence, I do not focus on the development of I/Q imbalance estimation techniques. Various I/Q imbalance estimation algorithms have been reported in the past decade [84–87]. In this chapter, a training signal based

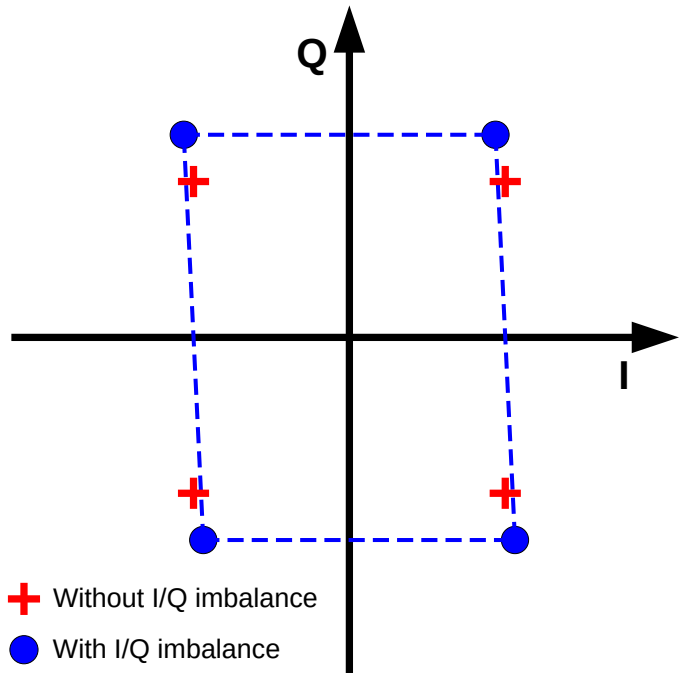


Figure 4.1: Illustration of signal constellation distorted by I/Q imbalance.

estimation scheme is taken as an example to extract the transmitter I/Q imbalance. Since we are merely interested in how many different I/Q imbalances exist but not the actual values of their amplitude and phase mismatches, only the I/Q imbalance parameter μ that is highly competent for the differentiation purpose is estimated.

Training signals, which are usually public information in wireless communication systems for channel estimation and signal synchronization purposes, can be exploited to estimate the transmitter I/Q imbalance. Under the assumption of perfect synchronization, the I/Q imbalance parameter μ can be extracted from the correlation between the received and the conjugate of transmitted training signals at baseband. Given a sampled training signal $x(n)$, $n = 0, 1, \cdots, N-1$, the correlation between

$x^*(n)$ and the kth received training signal $y_k(n)$ can be expressed as

$$\begin{aligned}
\Gamma_k &= \frac{1}{N}\sum_{n=0}^{N-1}\left[y_k(n)x^*(n)\right] \\
&= \mu_k \underbrace{\frac{1}{N}\sum_{n=0}^{N-1}\left\{\left[h_k(n)\otimes x(n)\right]x^*(n)\right\}}_{c_k} \\
&\quad +(1-\mu_k)\underbrace{\frac{1}{N}\sum_{n=0}^{N-1}\left\{\left[h_k(n)\otimes x^*(n)\right]x^*(n)\right\}}_{\gamma_k} \\
&\quad +\frac{1}{N}\sum_{n=0}^{N-1}\left[w_k(n)x^*(n)\right], \qquad (4.6)
\end{aligned}$$

where the subscript k indicates variables associated with the kth received training signal. With perfect channel estimation for $h_k(n)$, the receiver can easily calculate c_k and γ_k. As a result, the estimate of the transmitter I/Q imbalance parameter, $\hat{\mu}_k$, can be obtained as

$$\begin{aligned}
\hat{\mu}_k &= \frac{\Gamma_k-\gamma_k}{c_k-\gamma_k} \\
&= \mu_k + \frac{1}{(c_k-\gamma_k)\,N}\sum_{n=0}^{N-1}\left[w_k(n)x^*(n)\right] \\
&= \mu_k + \Delta_{\mu_k}, \qquad (4.7)
\end{aligned}$$

where Δ_{μ_k} is the estimation error of μ_k, which can be modeled as a zero-mean complex Gaussian variable as

$$\Delta_{\mu_k} \sim CN\left(0, \sigma^2_{\mu_k} = \frac{\bar{E}_x\sigma_k^2}{N\left|c_k-\gamma_k\right|^2}\right), \qquad (4.8)$$

in which $\bar{E}_x$ denotes the power of the training signal, i.e. $\bar{E}_x = \frac{1}{N}\sum_{n=0}^{N-1}|x(n)|^2$. It can be concluded from (4.8) that the estimation error Δ_{μ_k} is independent of the true

value of the I/Q imbalance parameter μ_k.

4.3.2 Differentiation of Different Transmitters based on Observed I/Q Imbalances

In order to determine the number of active users in a network, the estimation node has to differentiate different transmitters by judging whether any two I/Q imbalance estimates are from an identical device or not. Given two I/Q imbalance observations $\hat{\mu}_l = \mu_l + \Delta_{\mu_l}$ and $\hat{\mu}_k = \mu_k + \Delta_{\mu_k}$, the differentiating procedure can be modeled as a binary hypothesis testing as

$$\begin{cases} \mathcal{H}_0: & \mu_l = \mu_k \\ \mathcal{H}_1: & \mu_l \neq \mu_k \end{cases}. \tag{4.9}$$

Δ_{μ_l} and Δ_{μ_k} are estimation errors of μ_l and μ_k, respectively, which are independent zero-mean Gaussian variables referring to (4.8). In the proposed differentiation algorithm, the Euclidean distance between vectors $\hat{\mu}_l$ and $\hat{\mu}_k$ is defined as the test metric, that is

$$\Lambda(l,k) = \left|\hat{\mu}_l - \hat{\mu}_k\right|, \tag{4.10}$$

where $|\cdot|$ denotes the norm operation. Compared with a properly selected decision threshold T, if $\Lambda(l,k)$ is larger than T, it is claimed that these two observations are from different transmitters; otherwise, $\hat{\mu}_l$ and $\hat{\mu}_k$ are taken as two I/Q imbalance estimates of an identical transmitter, which are deviated by distortions from the noise and multipath channel.

The same as a common binary detection problem, two types of errors may occur during the testing: false alarm and miss detection. Under hypothesis $\mathcal{H}_0$, the test statistic $\Lambda(l,k)$ can be rewritten as

$$\Lambda(l,k)\big|\mathcal{H}_0 = \left|\Delta_{\mu_l} - \Delta_{\mu_k}\right|. \tag{4.11}$$

The term $\Delta_{\mu_l} - \Delta_{\mu_k}$ is zero-mean complex Gaussian distributed with a variance of

$\sigma^2_{\mu_l} + \sigma^2_{\mu_k}$. As a result, $\Lambda(l,k)|\mathcal{H}_0$ follows a Rayleigh distribution with parameter $\delta = \sqrt{\frac{\sigma^2_{\mu_l}+\sigma^2_{\mu_k}}{2}}$. The false alarm probability, P_{fa}, can therefore be derived as

$$\begin{aligned} P_{fa} &= P\Big\{\Lambda(l,k) > T\Big|\mathcal{H}_0\Big\} \\ &= P\Big\{\ |\Delta_{\mu_l} - \Delta_{\mu_k}| > T\Big\} \\ &= e^{\frac{-T^2}{\sigma^2_{\mu_l}+\sigma^2_{\mu_k}}}. \end{aligned} \tag{4.12}$$

Similarly, under hypothesis $\mathcal{H}_1$, the test statistic turns to be

$$\Lambda(l,k)\big|\mathcal{H}_1 = \big|\mu_l - \mu_k + \Delta_{\mu_l} - \Delta_{\mu_k}\big|, \tag{4.13}$$

where the term $\mu_l - \mu_k + \Delta_{\mu_l} - \Delta_{\mu_k}$ follows a complex Gaussian distribution with mean $\mu_l - \mu_k$ and variance $\sigma^2_{\mu_l} + \sigma^2_{\mu_k}$. Hence, $\Lambda(l,k)|\mathcal{H}_1$ follows a Rice distribution as

$$\Lambda(l,k)|\mathcal{H}_1 \sim \text{Rice}\left(\big|\mu_l - \mu_k\big|, \sqrt{\frac{\sigma^2_{\mu_l} + \sigma^2_{\mu_k}}{2}}\right). \tag{4.14}$$

Consequently, the miss detection probability, P_{md}, can be calculated as

$$\begin{aligned} P_{md} &= P\Big\{\Lambda(l,k) \le T\Big|\mathcal{H}_1\Big\} \\ &= P\Big\{\big|\mu_l - \mu_k + \Delta_{\mu_l} - \Delta_{\mu_k}\big| \le T\Big\} \\ &= 1 - Q_1\left(\frac{|\mu_l - \mu_k|}{\sqrt{\frac{\sigma^2_{\mu_l}+\sigma^2_{\mu_k}}{2}}}, \frac{T}{\sqrt{\frac{\sigma^2_{\mu_l}+\sigma^2_{\mu_k}}{2}}}\right), \end{aligned} \tag{4.15}$$

where $Q_1(\cdot,\cdot)$ is the first-order Marcum Q-function,

$$Q_1(a,b) = \int_b^\infty x e^{-\frac{x^2+a^2}{2}} \sum_{i=0}^{\infty} \frac{(ax/2)^{2i}}{i!\Gamma(i+1)} dx. \tag{4.16}$$

As shown in (4.12) and (4.15), FAP is just a function of estimation errors, and is

independent of the true value of the I/Q imbalance; in contrast, MDP is a function of the I/Q imbalance distance $|\mu_l - \mu_k|$. In practical implementation, an estimation node has no prior information about I/Q imbalances of the transmitters, so that the theoretical MDP cannot be obtained in the differentiating procedure. Therefore, the decision threshold T in the binary hypothesis test should be chosen based on a given requirement of FAP. Mathematically, a suitable decision threshold can be selected as

$$\begin{aligned} T &= \sqrt{-\ln\Big(P_{fa}\Big)\Big(\sigma_{\mu_l}^2 + \sigma_{\mu_k}^2\Big)} \\ &= \sqrt{-\ln\Big(P_{fa}\Big)\Big(\frac{\bar{E}_x\sigma_l^2}{N|c_l-\gamma_l|^2} + \frac{\bar{E}_x\sigma_k^2}{N|c_k-\gamma_k|^2}\Big)}. \end{aligned} \tag{4.17}$$

Please note that a new I/Q imbalance observation needs to be compared with I/Q imbalance estimates of all the identified active users. The discovery of a new station is claimed if and only if all the testings give a different-device decision.

4.3.3 Estimation of the Number of Active Users

Exploiting the proposed transmitter differentiation algorithm, different terminals can be identified based on their distinct I/Q imbalances. Thereafter, the number of active users in the network is determined by counting all the findings.

During an observation time window, the estimation node can obtain multiple transmitter I/Q imbalance estimates from the received training signals. Let $\boldsymbol{\Xi}$ denote the set of all the I/Q imbalance observations, and $\boldsymbol{\Omega}$ indicate the set of I/Q imbalance estimates belonging to the identified active users. The procedure for determining the number of active users can be summarized as follows:

1. Estimate $\Xi(1)$ and put it into $\boldsymbol{\Omega}$ as the I/Q imbalance estimate of the first identified active user, and then make a new estimate $\Xi(m), m = 2$;

2. Choose a suitable decision threshold $T(m)$ for the identification of $\Xi(m), m \geq 2$, according to the used training signal and corresponding channel condition;

3. Compare the Euclidean distances between $\Xi(m)$ and all the elements in the set $\mathbf{\Omega}$. If all the distances are larger than the selected threshold $T(m)$, put $\Xi(m)$ into set $\mathbf{\Omega}$;

4. If the time window does not expire, make a new estimate $\Xi(m), m = m+1$ and then go to Step 2; otherwise, go to Step 5;

5. Count the number of elements in the set $\mathbf{\Omega}$.

4.4 Simulation Results

Matlab simulations are carried out to validate the proposed estimation technique for the number of active users. An OFDM signal with 64 subcarriers and 4-QAM symbol modulation is adopted as the training signal in the simulations. The sampling frequency is set to 20 MHz. Without further specification, a Rayleigh fading channel with an exponential power delay profile (PDP) of a root-mean-square (RMS) delay of 50 ns is considered, which leads to a 12-tap time-domain channel impulse response. As a result, the cyclic prefix length of the OFDM signal, which is 16 in the simulations, is larger than the delay induced by the multipath channel. In addition, perfect channel estimation and synchronization are assumed to be achieved in the simulations.

4.4.1 FAP and MDP of the I/Q Imbalance based Transmitter Differentiation

Figures 4.2 and 4.3 present the simulated false alarm and miss detection probabilities of the proposed transmitter differentiation algorithm in differentiating two I/Q imbalance estimates, respectively. A transmitter with I/Q imbalance $\varepsilon = 0.25$ and $\phi = 5°$ is employed in the simulation for FAP. The decision threshold is selected based on a FAP requirement varying from 0.1 to 0.001. It can be found from Fig. 4.2 that the simulated FAPs are very close to their theoretical values in the considered

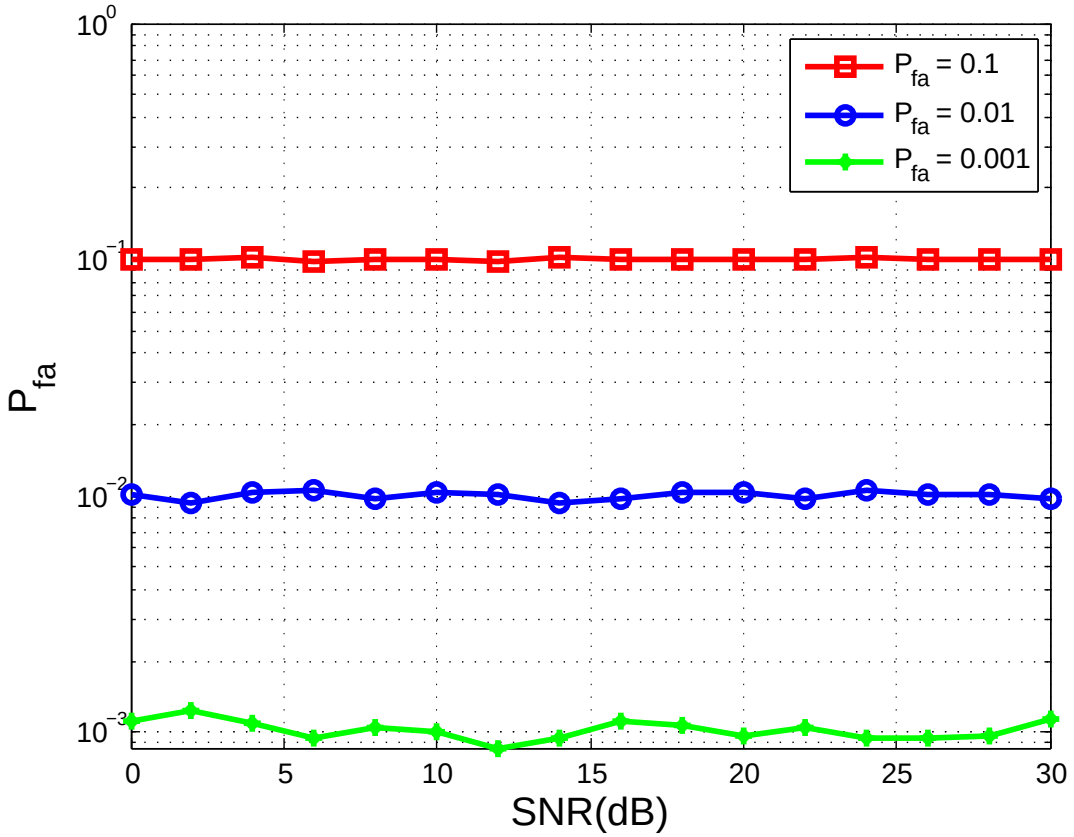


Figure 4.2: FAP in differentiating two I/Q imbalance estimates of an identical transmitter with I/Q imbalance $\varepsilon = 0.25$ and $\phi = 5°$.

Rayleigh fading channel during a signal-to-noise ratio range from 0 dB to 30 dB.

In the simulation for MDP, the two I/Q imbalance estimates are observed from two distinct transmitters. One transmitter has I/Q imbalance $\varepsilon = 0.25$ and $\phi = 5°$, the other suffers I/Q imbalance $\varepsilon = 0.05$ and $\phi = 15°$. The FAPs used in selecting the decision threshold are 0.1, 0.01 and 0.001, respectively. As shown in Fig. 4.3, when SNR is around 20 dB, MDPs in differentiating the two transmitters can be as low as 0.01. Moreover, a lower MDP can be observed under the same SNR condition when a larger FAP is acceptable in the differentiating process. It is noteworthy that the MDP also depends on the difference between I/Q imbalances of different transmitters, as addressed in the theoretical analysis in (4.15). A larger I/Q imbalance distance would reduce the probability of miss detection in the transmitter differentiation.

4.4.2 Accuracy of the Estimation for the Number of Active Users

In the evaluation of the proposed estimation algorithm for the number of active users, six transmitters are assumed to be present in the network. The amplitude and phase mismatches between I and Q branches of their signal constellations, i.e. (ε, ϕ), are $(-0.3, -15°), (-0.3, 15°), (-0.1, -5°), (0.1, 5°), (0.3, 15°), (0.3, -15°)$, respectively. Two estimates are obtained for each transmitter in the observation time window. Furthermore, a Rayleigh fading channel with an exponential PDP of 100 ns RMS delay, which would cause inter-symbol interference to the training signals, is also considered. Taking the event that the estimated number of active users is not equal to six as an estimation error in the simulation, error probabilities of the proposed estimation algorithm under different channel conditions are evaluated, as shown in Fig. 4.4. Acceptable performance can be observed from the simulation results. In addition, the estimation accuracy degrades when inter-symbol interference is caused by the multipath channel.

In order to study the statistics of estimation errors, the frequency of occurrence

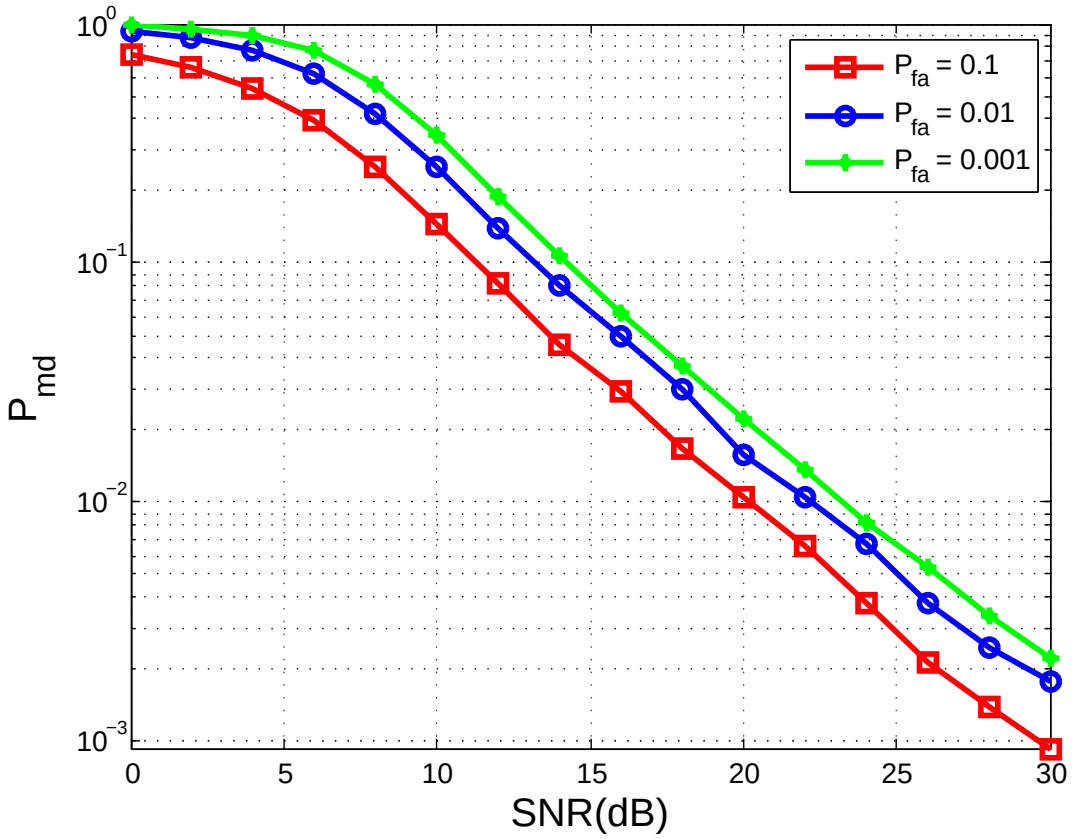


Figure 4.3: MDP in differentiating two I/Q imbalance estimates of distinct transmitters. One transmitter has I/Q imbalance $\varepsilon = 0.25$ and $\phi = 5°$, the other has $\varepsilon = 0.05$ and $\phi = 15°$.

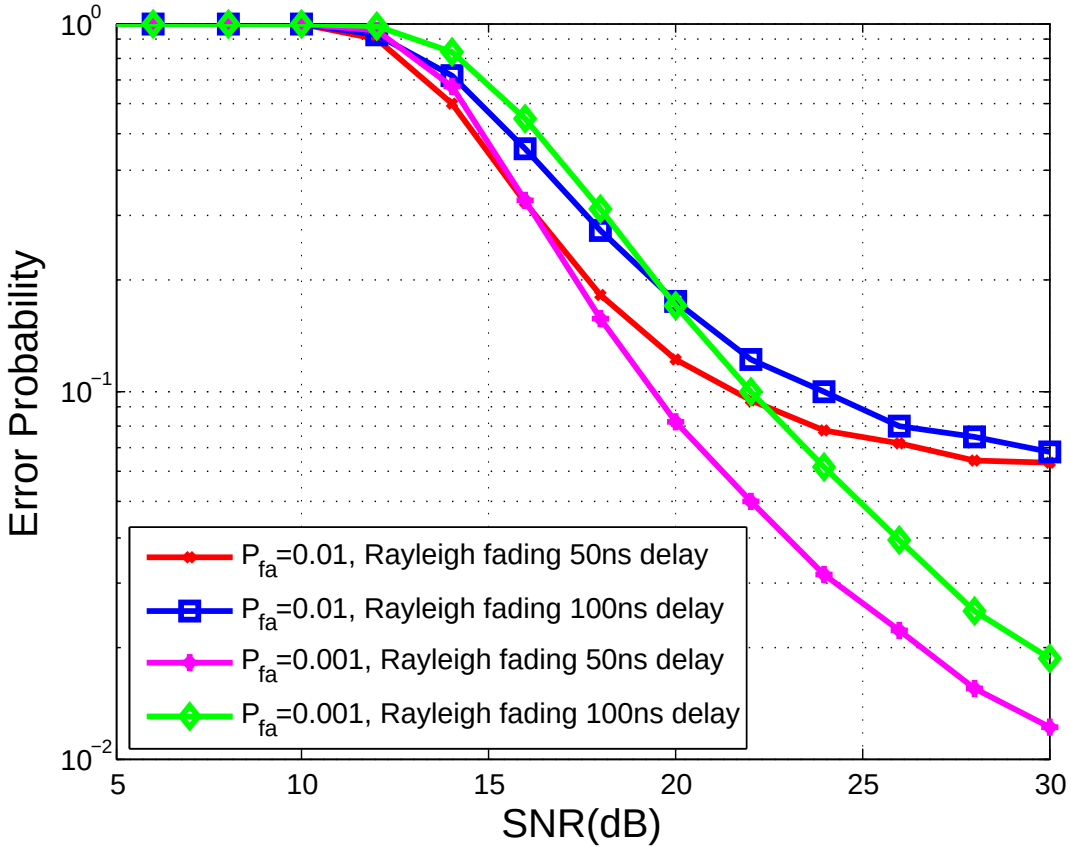


Figure 4.4: Error probability in estimating the number of active users when there are six transmitters in the network. Their I/Q imbalances are $(-0.3, -15°)$, $(-0.3, 15°)$, $(-0.1, -5°)$, $(0.1, 5°)$, $(0.3, 15°)$ and $(0.3, -15°)$, respectively.

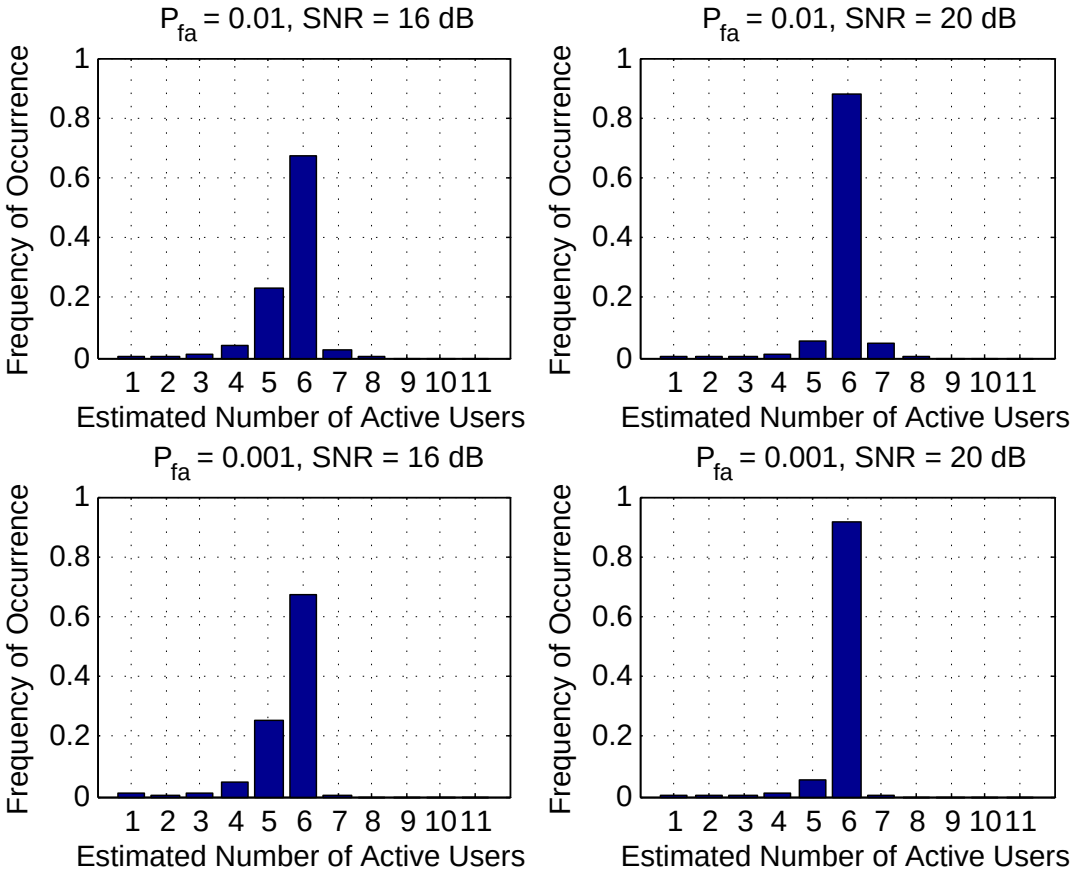


Figure 4.5: Statistical analysis for the estimation results when six active transmitters exist in the network.

for all the estimated numbers of active users is analyzed. Figure 4.5 demonstrates the frequency of occurrence when SNR = 16 dB and SNR = 20 dB in the Rayleigh fading channel of 50 ns RMS delay. In most of incorrect estimations, the estimated number of active users is just one away from the true value, caused by either false alarm or miss detection. Generally, this small deviation will not significantly affect perceiving the security level of the operating environment.

4.5 Summary

In this chapter, a novel device RF-DNA based estimation technique for the number of active users in a wireless network is proposed. As a typical device RF-DNA that

has device-specific nature, transmitter I/Q imbalance is exploited in the design. I/Q imbalance of a transmitter is first estimated from its transmitting signals, and then compared with the I/Q imbalance estimate of each previously identified active user through a hypothesis testing, where the Euclidean distance between the new and previous estimates is adopted as the test metric. If the distance is larger than a selected threshold, the two estimates are considered to be from different wireless devices. A new active user is claimed if and only if all the comparisons give a different-device decision. At the end of an estimation time window, the number of active users is obtained by counting all the identified transmitters. Simulation results have been provided to validate the proposed estimation technique.

Chapter 5

Anti-Eavesdropping OFDM System with CSI-based Coordinate Interleaving

In light of the security weaknesses of OFDM technology and its general acceptance in modern wireless communications, the security of OFDM communication systems needs to enhanced. This dissertation concentrates on the built-in security enhancement of wireless OFDM systems against eavesdropping. Two novel physical-layer eavesdropping prevention strategies for OFDM are proposed. This chapter provides insight into the proposed dynamic coordinate interleaving method, which can be employed in most existing wireless OFDM systems. For situations that the modulated data symbols transmitted at OFDM subcarriers are not in a complex-number structure, another dynamic subcarrier interleaving technique is investigated and presented in Chapter 6.

A novel anti-eavesdropping OFDM system through dynamic subcarrier coordinate interleaving is proposed in this chapter, by exploiting the reciprocal, location-dependent and time-varying nature of wireless channels. In the proposed OFDM system, the transmitter performs coordinate interleaving at partial OFDM subcarri-

ers, where the symbol coordinate of an OFDM subcarrier is interleaved in an opportunistic manner depending on the instantaneous channel state information between the transmitter and intended receiver. More specifically, a subcarrier symbol associated with a CSI (i.e., channel gain or phase) larger than a predefined threshold is coordinate interleaved. Since wireless channels associated with each pair of users at separate locations exhibit independent multipath fading, the frequently updated coordinate interleaving pattern can only be shared between legitimate users based on channel reciprocity. Consequently, eavesdropping is prevented due to mismatched de-interleaving at the eavesdropper. Two coordinate interleaving schemes are investigated by employing the subcarrier channel gain and phase in determining the interleaving pattern, respectively. In order to simultaneously evaluate the eavesdropping resilience and transmission reliability of anti-eavesdropping communication systems, a novel evaluation criterion, named probability of confidential transmission, is also proposed. Theoretical analysis and simulation results are provided to validate the effectiveness of the proposed anti-eavesdropping OFDM system. As confirmed by simulation results, the proposed system significantly outperforms the conventional OFDM system in terms of the probability of confidential transmission.

5.1 Introduction

Securing wireless communications is a critical challenge due to the inherent broadcast nature of radio signal propagation. Adversaries can possibly intercept legitimate transmissions as long as they lie within the radio transmission coverage. Traditional communication securing mechanisms largely rely on cryptographic techniques at upper layers of the protocol stacks, where the security is generally guaranteed by using either pre-distributed or public cryptography keys between communication nodes [88]. However, with limited randomness and potential secrecy leakage in such highly standardized practices, key distribution and protection face severe threats of being cracked. In recent years, physical layer security, exploiting the continual influx

of the situation- and user-dependent randomness from wireless multipath channels, is emerging as an effective means to complement conventional wireless security techniques [13]. The new physical layer security paradigms benefit from fundamental properties of wireless channels, such as reciprocity, as well as temporal and spatial variations.

5.1.1 State of the Art in Eavesdropping Prevention

Eavesdropping, particularly passive eavesdropping, is one of the primary security problems in a wireless network. A passive eavesdropper can overhear wireless signals and infer the transmitted information without being detected by legitimate users. Several studies for preventing eavesdropping at the physical layer in wireless communications have been developed. Information theoretic aspects of secrecy [89, 90], which originated from Shannon's notion of perfect secrecy [29], demonstrated that as long as the eavesdropper's channel is worse than the legitimate receiver's channel, perfect secrecy can be achieved without any cryptographic key.

Differing from the theoretical security techniques, several practical approaches dealing with eavesdropping have also been investigated:

- *Transmitter beamforming and friendly jamming.* Transmitter beamforming was proposed to facilitate the transmission confidentiality in [40], where the maximum secrecy sum rate was achieved when eavesdropper's channel state information was known. Artificial noise [41] was generated using multiple antennas or cooperative nodes, and was injected into the null-subspace of the intended receiver's channel to prevent eavesdropping.

- *Network cooperation.* The authors of [91] proposed an anti-eavesdropping space-time network coding scheme to prevent eavesdropping under the collaboration of the user nodes in a cluster. Similarly, relay technique was utilized to defend against eavesdroppers in [92, 93] at the cost of collaborative nodes.

- *Coded transmission.* Security can also be enhanced through spread-spectrum techniques at the physical layer such as direct-sequence spread-spectrum (DSSS) and frequency-hopping spread-spectrum (FHSS) [94], in which a signal is typically spread over a frequency band with frequency bandwidth much wider than that of the original information. In [95], messages were transmitted over punctured bits to hide data from eavesdroppers by using low-density parity-check codes.

- *Resource allocation.* Power and subcarrier allocation techniques have also been introduced to improve the security against eavesdropping [96, 97]. The optimal resource allocation was studied with respect to instantaneous channel conditions under a total transmit power constraint and security constraints.

It can be concluded that the aforementioned security approaches require additional resource, significant changes of the network protocol and device hardware, or high computational complexity. Effective practical alternatives with minimum additional resource requirement, modification to off-the-shelf systems and operational complexity have yet to be investigated.

5.1.2 Physical Layer Security of OFDM Systems

OFDM has been widely adopted in many high-speed wireless communication networks, such as Long-Term Evolution Advanced, IEEE 802.16 and IEEE 802.11, mainly because of its high spectral efficiency and robustness against multipath fading. Unfortunately, the distinct physical-layer time and frequency characteristics of conventional OFDM signals can be exploited for interception purposes by adversaries, resulting in the OFDM system being vulnerable to eavesdropping attacks. Thus, it is of practical interest to investigate the physical layer security in OFDM due to its wide popularity and its inherent security weaknesses.

Extensive research efforts have been devoted to improve the physical layer security of OFDM systems against eavesdropping. Waveform feature suppression strategies,

including frequency hopping [98], cyclic prefix and pilot tone elimination [99], as well as CP size variation and random signal insertion [100], have been employed to enhance OFDM security. Besides significant modifications to off-the-shelf systems, these approaches have a critical requirement that the feature suppression processing needs to be kept unknown to adversaries. It cannot be easily fulfilled in practical implementations. Encryption methods have also been investigated to prevent OFDM signals from eavesdropping [101, 102]. Nevertheless, aside from their computational complexity induced by the involved encryption key generation, key distribution and management in these techniques face severe threats of being cracked.

Recently, the randomness of wireless channels was exploited to strengthen the security of OFDM transmission as well. The physical layer security of OFDM systems over wireless channels was investigated from an information-theoretic perspective in [13]. A secure OFDM system was investigated by degrading the eavesdropper's channel condition, where distributed transmitters independently send out pre-equalized OFDM signals [103]. In addition, an optimal power allocation scheme under power and security constraints for the wire-tap OFDM system was presented in [104]. However, these security techniques require the knowledge of the eavesdropping channel, which is conditioned on a successful detection of eavesdroppers. Therefore, it is expected to develop simple proactive eavesdropping prevention for OFDM at the physical layer, without the requirements of eavesdropping channel information, significant modifications to off-the-shelf systems as well as additional resource.

5.1.3 Contributions of the Proposed Secure OFDM System

The concept of coordinate interleaving was originally introduced into communication systems to improve the reliability of modulated signals in fading channels by increasing the modulation diversity [105, 106]. It was later extended to space-time code designs for multiple-input multiple-output (MIMO) wireless transmission [107, 108]. In [109, 110], coordinate interleaving method was utilized to improve the error rate

performance in cooperative relay networks. Furthermore, it has been verified that the peak-to-average power ratio (PAPR) of OFDM signals could be reduced with a properly designed coordinate interleaving [111]. However, none of these works take into account the security issues.

In this chapter, a simple and effective anti-eavesdropping OFDM system is proposed by exploiting coordinate interleaving at partial subcarriers of each OFDM signal. Subcarriers that perform coordinate interleaving are chosen according to the real-time channel state information between the transmitter and intended receiver. Both subcarrier channel gain and phase are investigated for determining whether a subcarrier is to be interleaved, leading to two different coordinate interleaving schemes. More specifically, the transmitter interleaves the real and imaginary components of a subcarrier symbol when its associated channel gain (or channel phase) is larger than a predefined threshold. Based on channel reciprocity, the legitimate receiver can locally deduce subcarriers that undergo coordinate interleaving without any additional signaling. In contrast, due to the independence of spatially separate wireless channels in a rich multipath environment, the subcarrier coordinate interleaving pattern is unavailable to eavesdroppers at a third location. Consequently, de-interleaving at eavesdroppers is disrupted and eavesdropping is then prevented. In order to simultaneously evaluate the eavesdropping resilience and transmission reliability of anti-eavesdropping communication systems, a novel performance evaluation criterion, named probability of confidential transmission, is also proposed in this study. Compared to existing security approaches, the proposed anti-eavesdropping OFDM system does not require eavesdropping channel information or additional information exchange, only needs minor modifications to off-the-shelf systems, and has low computational complexity.

Organization The reminder of this chapter is organized as follows. Section 5.2 introduces the system model and preliminaries. The proposed OFDM security technique exploiting the channel gain based coordinate interleaving is analyzed in Section 5.3, followed by the channel phase based coordinate interleaving scheme in Section

5.4. System optimization with a trade-off between eavesdropping resilience and transmission reliability, as well as the proposed performance evaluation criterion for anti-eavesdropping systems, is discussed in Section 5.5. Simulation results are provided in Section 5.6, and conclusions are finally drawn in Section 5.7.

Notations Boldface letter $\mathbf{A}$ identifies a random variable vector $\mathbf{A}$ and $A(k)$ denotes its kth element. $[\cdot]^T$ indicates the complex nonconjugate transposition. Bold upper case letter with superscript N represents an $N \times N$ matrix. Complex Gaussian random variable X with mean m and variance σ^2, and with independent and identically distributed real and imaginary components, is denoted as $X \sim CN\left(m, \sigma^2\right)$.

5.2 System Model and Preliminaries

5.2.1 System Model

In this study, an OFDM wireless network that consists of three nodes is considered, where a transmitter communicates with a legitimate receiver in the presence of a passive eavesdropper, as shown in Fig. 5.1. The forward and reverse channels between legitimate users are assumed to occupy the same frequency band and remain constant over several time slots. Hence, the transmitter and legitimate receiver would experience and observe an identical common channel (channel between the transmitter and the legitimate receiver), based on the reciprocity property of wireless channels.

Generally, a third party that is more than half a wavelength away from the intended receiver experiences a fading process independent of that between legitimate terminals [26]. For instance, at 2.4 GHz, two receivers that are roughly separated by 6.25 *cm* would suffer independent channel impairments. In most practical scenarios, the eavesdropper is spatially separated from the legitimate users with a much farther distance, in order to avoid being detected. As a result, the common channel and eavesdropping channel (channel between the transmitter and the eavesdropper) are

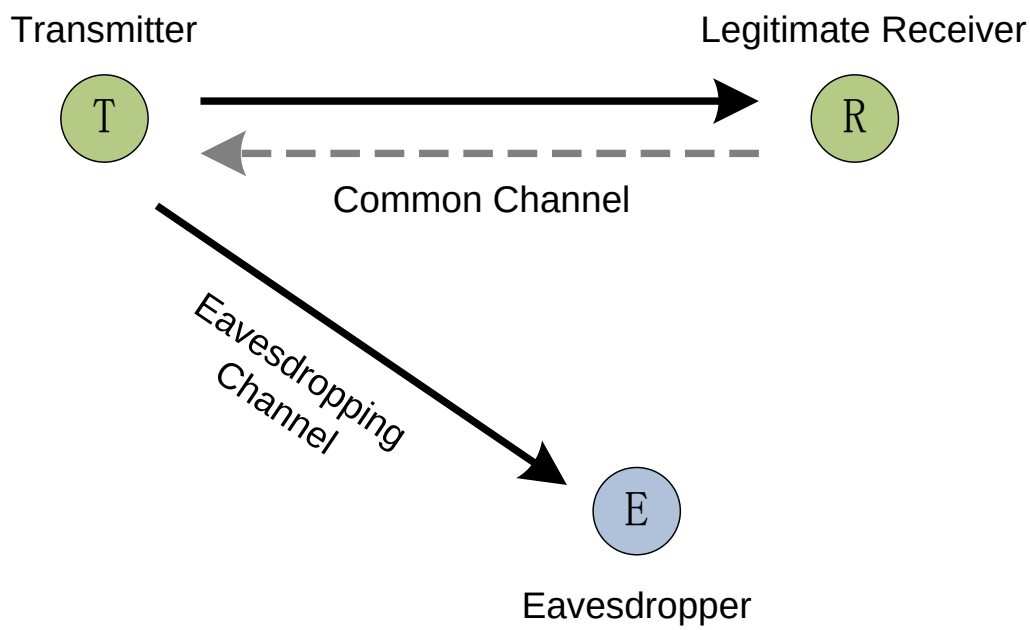


Figure 5.1: Wireless communications in the presence of a passive eavesdropper.

modelled as independent of each other in the analysis.

5.2.2 Multipath Channels in OFDM System

Assume that OFDM signals with N subcarriers are transmitted by the transmitter. At the legitimate receiver, the frequency domain received signals after removing the cyclic prefix, $\mathbf{R} = [R(0), R(1), \cdots, R(N-1)]^T$, can be written as

$$\mathbf{R} = \text{diag}\{\mathbf{H}\}^N \mathbf{S} + \mathbf{W}, \tag{5.1}$$

where $\text{diag}\{\mathbf{H}\}^N$, which is an $N \times N$ diagonal matrix with all its main diagonal entries $\mathbf{H} = [H(0), H(1), \cdots, H(N-1)]^T$, identifies the complex frequency domain channel responses of the common channel; $N \times 1$ vector $\mathbf{S}$ denotes the modulated symbols transmitted by the N subcarriers, which are mapped into a two-dimensional constellation; and vector $\mathbf{W}$ of size $N \times 1$ indicates the white Gaussian noise following the distribution $CN(0, \sigma_w^2)$. For the frequency domain channel vector $\mathbf{H}$, it is characterized

by the associated time domain channel coefficients $\mathbf{h} = [h(0), h(1), \cdots, h(L-1)]^T$ as

$$\mathbf{H} = \mathbf{F}^N \mathbf{h}, \tag{5.2}$$

where $\mathbf{F}^N$ is the N-point FFT matrix with its (n,k)th entry $(exp\{-j2\pi nk/N\}/\sqrt{N})$. Under the assumption of a Rayleigh fading channel, $\mathbf{h}$ can be modelled as L independent and identically distributed zero-mean complex Gaussian random variables, so that $\mathbf{H}$ is also complex Gaussian distributed due to central limit theorem. Throughout this chapter, $\{H(0), H(1), \cdots, H(N-1)\}$ are approximated as i.i.d. random variables following the distribution $CN(0, \sigma_H^2)$.

The same modelling and approximation can be applied to the analysis of the eavesdropping channel $\mathbf{H_E}$. Similarly, $\{H_E(0), H_E(1), \cdots, H_E(N-1)\}$ are modelled as i.i.d. complex Gaussian variables following the distribution $CN(0, \sigma_{H_E}^2)$ in the discussion.

5.2.3 Channel Estimates in the Network

Estimation errors generally occur at the channel estimators, due to the presence of noise, interference and hardware limitations in wireless communication systems. As a result, only a noisy channel estimate can be obtained by all the nodes in the network. The observations of the common channel at the transmitter and legitimate receiver, $\hat{\mathbf{H}}_\mathbf{T}$ and $\hat{\mathbf{H}}_\mathbf{R}$, respectively, can be given by

$$\hat{\mathbf{H}}_{\mathbf{T/R}} = \mathbf{H} + \Delta\mathbf{H}_{\mathbf{T/R}}, \tag{5.3}$$

where subscripts T and R indicate vectors associated with the transmitter and legitimate receiver, respectively. $\Delta\mathbf{H}_{\mathbf{T/R}}$ of size $N \times 1$ is the estimation error of the common channel $\mathbf{H}$ at the transmitter/legitimate receiver, which can be modelled as a zero-mean complex Gaussian variable vector with all its elements being independently distributed. With a further assumption that estimation errors at all subcarriers of an

OFDM signal are identically distributed, $\Delta H_T(k)$ and $\Delta H_R(k)$ can be modelled as

$$\Delta H_T(k) \sim CN(0, \sigma_T^2), \quad k = 0, 1, \cdots, N-1, \tag{5.4}$$

and

$$\Delta H_R(k) \sim CN(0, \sigma_R^2), \quad k = 0, 1, \cdots, N-1, \tag{5.5}$$

respectively. Please note that the noise, interference as well as hardware limitations at the transmitter are usually independent of that at the legitimate receiver, even when they follow the same statistical distributions at the two ends. The estimation errors $\Delta\mathbf{H_T}$ and $\Delta\mathbf{H_R}$ would thus be independent of each other as well.

Similarly, the noisy estimate of the eavesdropper's CSI can be written as

$$\hat{\mathbf{H}}_\mathbf{E} = \mathbf{H_E} + \Delta\mathbf{H_E}, \tag{5.6}$$

where $\hat{\mathbf{H}}_\mathbf{E}$ is the estimate of the eavesdropping channel $\mathbf{H_E}$ with estimation error $\Delta\mathbf{H_E}$. $\Delta H_E(k)$ for $k = 0, 1, \cdots, N-1$ can also be modeled as i.i.d. zero-mean complex Gaussian variables with variance σ_E^2. It is noteworthy that $\mathbf{H_E}$ is independent of $\mathbf{H}$, and $\Delta\mathbf{H_E}$ is independent of both $\Delta\mathbf{H_T}$ and $\Delta\mathbf{H_R}$. Therefore, $\hat{\mathbf{H}}_\mathbf{E}$ should be independent of both $\hat{\mathbf{H}}_\mathbf{T}$ and $\hat{\mathbf{H}}_\mathbf{R}$.

5.3 Proposed Secure OFDM System Using Channel Gain based Coordinate Interleaving

In the proposed anti-eavesdropping OFDM system, the real and imaginary components of modulated symbols at partial OFDM subcarriers are interleaved in an opportunistic manner. Subcarriers of each OFDM signal that perform coordinate interleaving are dynamically determined by the CSI of the common channel. Two coordinate interleaving schemes are investigated, which exploit the subcarrier channel

gain and phase in determining the coordinate interleaving pattern, respectively. The channel gain based scheme is introduced in this section, and the channel phase based scheme is discussed later in Section 5.4.

In order to provide a deep insight into the gain and phase of the noisy channel estimates, we rewrite the observed channel frequency responses in a geometrical form. Referring to (5.3), the noisy channel observations at the transmitter and legitimate receiver can be geometrically expressed as

$$\left|\hat{H}_{T/R}\left(k\right)\right|e^{j\hat{\theta}_{T/R}(k)} = \left|H\left(k\right)\right|e^{j\theta(k)} + \left|\Delta H_{T/R}\left(k\right)\right|e^{j\Delta\theta_{T/R}(k)}, \quad k = 0, 1, \cdots, N-1, \tag{5.7}$$

where $|\cdot|$ indicates the norm operation, $\hat{\theta}_{T/R}(k)$ denotes the estimated channel phase at the kth subcarrier of the common channel while $\theta(k)$ is its exact value, and $\Delta\theta_{T/R}(k)$ represents the phase of the estimation error $\Delta H_{T/R}\left(k\right)$. Similarly, the estimate of the eavesdropping channel can be rewritten in a geometrical form as

$$\left|\hat{H}_{E}\left(k\right)\right|e^{j\hat{\theta}_{E}(k)} = \left|H_{E}\left(k\right)\right|e^{j\theta(k)} + \left|\Delta H_{E}\left(k\right)\right|e^{j\Delta\theta_{E}(k)}, \quad k = 0, 1, \cdots, N-1, \tag{5.8}$$

where $\hat{\theta}_E(k)$, $\theta(k)$ and $\Delta\theta_E(k)$ denote the phases of the estimated channel response $\hat{H}_E\left(k\right)$, the eavesdropper channel $H_E\left(k\right)$, and the estimation error $\Delta H_E\left(k\right)$, respectively.

Please note that in the proposed anti-eavesdropping OFDM system, we may not need to involve all N subcarriers of each OFDM signal in the opportunistic coordinate interleaving. Instead, a subcarrier set $\mathcal{M}$, with M out of the N subcarriers, can be utilized in the security design, where $M \leq N$.

5.3.1 Subcarrier Channel Gain based Coordinate Interleaving

In the security scheme using channel gain based coordinate interleaving, the instantaneous channel gain of each subcarrier belonging to the set $\mathcal{M}$ in an OFDM signal is compared with a properly selected threshold. If the channel gain of a subcarrier is larger than the threshold, the transmitter performs coordinate interleaving at that subcarrier; otherwise, the modulated symbol at that subcarrier is transmitted in the original format.

The subcarrier channel gain obtained at the transmitter, which is employed to initiate the coordinate interleaving pattern, can be given by

$$\lambda_T(k) = \left|\hat{H}_T(k)\right|^2, \quad k = 0, 1, \cdots, N-1. \tag{5.9}$$

Since $\hat{H}_T(k)$ follows a complex Gaussian distribution $CN\left(0, \sigma^2_{\hat{H}_T}\right)$, where $\sigma^2_{\hat{H}_T} = \sigma^2_H + \sigma^2_T$, the channel gain $\lambda_T(k)$ is exponentially distributed with a probability density function (PDF) $f_T(\lambda_T(k)) = \frac{1}{\sigma^2_{\hat{H}_T}} e^{-\lambda_T(k)/\sigma^2_{\hat{H}_T}}$ and a CDF $F_T(\lambda_T(k)) = 1 - e^{-\lambda_T(k)/\sigma^2_{\hat{H}_T}}$. Given a predefined threshold Λ_T, the pattern of the channel gain based coordinated interleaving at the kth subcarrier can be expressed as

$$\begin{cases} \lambda_T(k) > \Lambda_T, & \text{interleaving} \\ \lambda_T(k) \leq \Lambda_T, & \text{un-interleaving} \end{cases}, \quad k \in \mathcal{M}. \tag{5.10}$$

The threshold Λ_T needs to be selected to maximize the difficulty of eavesdropping. In our case, an equal probability of both decisions in (5.10) would achieve this purpose, that is

$$P(\lambda_T(k) > \Lambda_T) = P(\lambda_T(k) \leq \Lambda_T) = \frac{1}{2}. \tag{5.11}$$

Since $\lambda_T(k)$ follows an exponential distribution with parameter $1/\sigma^2_{\hat{H}_T}$, the threshold

Λ_T can be chosen as

$$\Lambda_T = -\sigma^2_{\hat{H}_T} \ln \frac{1}{2}. \tag{5.12}$$

5.3.2 Performance of Eavesdropping Prevention

No information about the coordinate interleaving pattern will be sent out by the transmitter of the proposed anti-eavesdropping OFDM system. Any node in the network that wants to de-interleave and demodulate the transmitted data has to locally derive the coordinate interleaving pattern of each OFDM signal.

Since the eavesdropping channel $\mathbf{H_E}$ and common channel $\mathbf{H}$, as well as the channel estimates $\hat{\mathbf{H}}_\mathbf{E}$ and $\hat{\mathbf{H}}_\mathbf{T}$, are statistically independent, the channel gains $\lambda_\mathbf{E}$ and $\lambda_\mathbf{T}$ should be independent of each other. Consequently, the eavesdropper has no more information than a random guess about whether the symbol at any OFDM subcarrier in the set $\mathcal{M}$ is coordinate interleaved. Due to the independence between $\lambda_\mathbf{E}$ and $\lambda_\mathbf{T}$, the derivation of the interleaving pattern from $\lambda_\mathbf{E}$ can also be taken as a random guess. With an equal probability of interleaving and un-interleaving at an OFDM subcarrier in $\mathcal{M}$, the probability that the eavesdropper makes a correct guess of the coordinate interleaving pattern at one subcarrier would be

$$p_E(k) = \frac{1}{2}, \quad k \in \mathcal{M}. \tag{5.13}$$

Under the assumption that M subcarriers are involved in the opportunistic coordinate interleaving for the security purpose, the probability that the eavesdropper makes an incorrect decision for the interleaving pattern of an OFDM signal, P_E, can be given by

$$P_E = 1 - \frac{1}{2^M}. \tag{5.14}$$

Let P_S denote the symbol error rate (SER) of the conventional OFDM system using a certain modulation scheme in a Rayleigh fading channel. The SER of eavesdropping under the same channel condition when legitimate users adopt the proposed

channel gain based coordinate interleaving, $P_{S,E}$, can be calculated as

$$P_{S,E} = 1 - (1 - P_E)(1 - P_S). \tag{5.15}$$

5.3.3 Performance of Legitimate Transmission

In the proposed anti-eavesdropping OFDM system, the legitimate receiver locally derives the coordinate interleaving pattern from its own estimate of the common channel, and then performs de-interleaving and data demodulation. Ideally, the transmitter and intended receiver could have the same channel observations due to channel reciprocity. The opportunistic coordinate interleaving would thus not degrade the reliability of legitimate transmission. In practice, the legitimate node pair can only have two noisy estimates of the common channel due to their independent estimation errors. Hence, the performance of legitimate transmission with noisy channel estimates needs to be evaluated.

Referring to the analysis in Section 5.2, the noisy channel estimate of the common channel at the legitimate receiver follows a complex Gaussian distribution $CN\left(0, \sigma^2_{\hat{H}_R}\right)$, where $\sigma^2_{\hat{H}_R} = \sigma^2_H + \sigma^2_R$. Therefore, the channel gain $\lambda_R(k) = \left|\hat{H}_R(k)\right|^2$ is exponentially distributed with parameter $1/\sigma^2_{\hat{H}_R}$. In order to derive the interleaving pattern initiated at the transmitter, the receiver compares its observed subcarrier channel gains with a threshold Λ_R. Similar to the analysis in (5.12), we can obtain the threshold used at the intended receiver, Λ_R, as

$$\Lambda_R = -\sigma^2_{\hat{H}_R} \ln \frac{1}{2}. \tag{5.16}$$

The reliability of legitimate transmission is degraded when the transmitter and legitimate receiver generate mismatched coordinate interleaving patterns. The probability of disagreement between the transmitter and legitimate receiver on whether

one subcarrier in the set $\mathcal{M}$ is interleaved, $p_L(k)$, can be calculated as

$$\begin{aligned} p_L(k) &= P(\lambda_R(k) > \Lambda_R | \lambda_T(k) \leq \Lambda_T) + P(\lambda_R(k) \leq \Lambda_R | \lambda_T(k) > \Lambda_T) \\ &= \frac{1}{2} P(\lambda_R(k) > \Lambda_R, \lambda_T(k) \leq \Lambda_T) + \frac{1}{2} P(\lambda_R(k) \leq \Lambda_R, \lambda_T(k) > \Lambda_T). \end{aligned} \tag{5.17}$$

Challenges here are to derive $P(\lambda_R(k) > \Lambda_R, \lambda_T(k) \leq \Lambda_T)$ and $P(\lambda_R(k) \leq \Lambda_R, \lambda_T(k) > \Lambda_T)$. Considering that $\hat{H}_T(k)$ and $\hat{H}_R(k)$ are two Gaussian variables conditioned on the common channel $H(k)$, we can take $\hat{H}_R(k)$ as a noisy version of $\hat{H}_T(k)$, that is

$$\hat{H}_R(k) = \hat{H}_T(k) + \Delta H_{TR}(k), \quad k = 0, 1, \cdots, N-1, \tag{5.18}$$

where

$$\Delta H_{TR}(k) = \Delta H_R(k) - \Delta H_T(k) \tag{5.19}$$

identifies the composed channel estimation error of the transmitter/receiver and receiver/transmitter transmission link. It follows a zero-mean complex Gaussian distribution with a variance of $\sigma_{TR}^2 = \sigma_T^2 + \sigma_R^2$. Consequently, $\hat{H}_R(k)$ can be approximated as a complex Gaussian random variable with a mean of $\hat{H}_T(k)$ and a variance of σ_{TR}^2. The channel gain $\lambda_R(k)$ is thus noncentral Chi-square distributed with 2 degree of freedom, with a PDF

$$f_R(\lambda_R(k)) = \frac{1}{\sigma_{TR}^2} e^{-(\lambda_T(k)+\lambda_R(k))/\sigma_{TR}^2} I_0\left(\frac{\sqrt{\lambda_R(k)\lambda_T(k)}}{2\sigma_{TR}^2}\right), \tag{5.20}$$

and a CDF

$$F_R(\lambda_R(k)) = 1 - Q_1\left(\frac{\sqrt{2\lambda_T(k)}}{\sigma_{TR}}, \frac{\sqrt{2\lambda_R(k)}}{\sigma_{TR}}\right), \tag{5.21}$$

where $I_A(x)$ represents the Bessel function of Ath order as

$$I_A(x) = \sum_{k=0}^{\infty} \frac{(x/2)^{A+2k}}{k!\Gamma(A+k+1)}, \tag{5.22}$$

and $Q_c(a,b)$ denotes the Marcum Q-function, that is

$$Q_c(a,b) = \int_b^{\infty} x \left(\frac{x}{a}\right)^{c-1} e^{-\frac{x^2+a^2}{2}} I_{c-1}(ax)\, dx. \tag{5.23}$$

The disagreement probability $p_L(k)$ for the kth subcarrier can then be derived as

$$\begin{aligned} p_L(k) &= \frac{1}{2}\int_{-\infty}^{\Lambda_T} f_T(\lambda_T(k)) \left\{ \int_{\Lambda_R}^{+\infty} f_R(\lambda_R(k))\, d\lambda_R(k) \right\} d\lambda_T(k) \\ &\quad + \frac{1}{2}\int_{\Lambda_T}^{+\infty} f_T(\lambda_T(k)) \left\{ \int_{-\infty}^{\Lambda_R} f_R(\lambda_R(k))\, d\lambda_R(k) \right\} d\lambda_T(k) \\ &= \frac{1}{2}\int_{-\infty}^{\Lambda_T} f_T(\lambda_T(k)) \left[1 - F_R(\Lambda_R)\right] d\lambda_T(k) \\ &\quad + \frac{1}{2}\int_{\Lambda_T}^{+\infty} f_T(\lambda_T(k))\, F_R(\Lambda_R)\, d\lambda_T(k). \end{aligned} \tag{5.24}$$

Unfortunately, the integral of the Marcum Q-function in (5.24) cannot be worked out, and thus $p_L(k)$ cannot be evaluated in a closed form. However, it can be concluded from (5.24) that $p_L(k)$ would be a variable independent of the subcarrier index k after the definite integral, since the boundaries of the integral interval are uncorrelated to k. Therefore, the index k can be removed from $p_L(k)$. In this study, numerical results will be provided to evaluate this disagreement probability p_L.

When M subcarriers are involved in the channel gain based coordinate interleaving which are independent of one another, the interleaving pattern mismatch probability for an OFDM signal at the legitimate receiver, P_L, would be

$$P_L = 1 - (1 - p_L)^M. \tag{5.25}$$

Then, we can have the SER of legitimate transmission in the proposed anti-eavesdropping OFDM system using channel gain based coordinate interleaving, that is

$$P_{S,L} = 1 - (1 - P_L)(1 - P_S). \tag{5.26}$$

5.4 Proposed Secure OFDM System Using Channel Phase based Coordinate Interleaving

Channel phase is another typical CSI parameter in wireless communications. OFDM eavesdropping prevention technique that exploits channel phase based coordinate interleaving is investigated in this section.

5.4.1 Subcarrier Channel Phase based Coordinate Interleaving

In the channel phase based security scheme, the transmitter compares the instantaneous channel phases of OFDM subcarriers involved in the security design with a properly selected threshold to determine whether the real and imaginary parts of the symbols at those subcarriers are interleaved. As the noisy channel estimate $\hat{\mathbf{H}}_{\mathbf{T}}$ follows a zero-mean complex Gaussian distribution $CN\left(0, \sigma^2_{\hat{H}_T}\right)$, the estimated phases of the N subcarriers in an OFDM signal, $\left\{\hat{\theta}_T(0), \hat{\theta}_T(1), \cdots, \hat{\theta}_T(N-1)\right\}$, are i.i.d. variables uniformly distributed over $[0, 2\pi)$. Similar to the subcarrier channel gain based scheme, the pattern of the channel phase based coordinate interleaving at the kth subcarrier can be mathematically expressed as

$$\begin{cases} \hat{\theta}_T(k) > \Lambda'_T, & \text{interleaving} \\ \hat{\theta}_T(k) \leq \Lambda'_T, & \text{un-interleaving} \end{cases}, \quad k \in \mathcal{M}, \tag{5.27}$$

where Λ'_T denotes the threshold used by the transmitter in the channel phase based scheme. In order to maximize the difficulty of eavesdropping, an OFDM subcarrier in the set $\mathcal{M}$ should have equal probability of being and not being coordinate interleaved. Considering that $\hat{\theta}_T(k)$ follows a uniform distribution over $[0, 2\pi)$, the threshold Λ'_T can be selected as

$$\Lambda'_T = \pi. \tag{5.28}$$

5.4.2 Performance of Eavesdropping Prevention

As addressed previously, the eavesdropper at a third location experiences a multipath channel independent of the common channel. The subcarrier channel phase estimate at the eavesdropper $\hat{\theta}_{\mathbf{E}}$ is uncorrelated to that observed at the transmitter, i.e. $\hat{\theta}_{\mathbf{T}}$. Hence, the eavesdropper can only make a random guess of the coordinate interleaving pattern initiated by the transmitter. Again, as a binary hypothesis problem where both possible outcomes have the same occurrence probability, the probability that the eavesdropper makes a correct decision of whether the modulated symbol at a subcarrier is coordinate interleaved would be

$$p'_E(k) = \frac{1}{2}, \quad k \in \mathcal{M}. \tag{5.29}$$

In the situation that M subcarriers are included in the opportunistic coordinate interleaving for the security enhancement, the probability that the eavesdropper obtains a mismatched interleaving pattern for an OFDM signal can be calculated as

$$P'_E = 1 - \frac{1}{2^M}. \tag{5.30}$$

Consequently, the SER of eavesdropping in the subcarrier channel phase based subcarrier coordinate interleaving scheme, $P'_{S,E}$, can be given by

$$P'_{S,E} = 1 - \left(1 - P'_E\right)\left(1 - P_S\right). \tag{5.31}$$

5.4.3 Performance of Legitimate Transmission

Since the observation of the common channel at the legitimate receiver, i.e. $\hat{\mathbf{H}}_{\mathbf{R}}$, follows a zero-mean complex Gaussian distribution $CN\big(0, \sigma^2_{\hat{H}_R}\big)$, the corresponding subcarrier channel phases $\big\{\hat{\theta}_R(0), \hat{\theta}_R(1), \cdots, \hat{\theta}_R(N-1)\big\}$ are also i.i.d. variables uniformly distributed over $[0, 2\pi)$. Therefore, the threshold used to derive the channel phase based coordinate interleaving pattern at the legitimate receiver, Λ'_R, should

also be π, i.e. $\Lambda'_R = \pi$. The probability of disagreement between the two nodes of the common channel on whether the kth subcarrier is coordinate interleaved in the channel phase based scheme, $p'_L(k)$, can then be calculated as

$$\begin{aligned} p'_L(k) &= P\left(\hat{\theta}_R(k) > \Lambda'_R | \hat{\theta}_T(k) \leq \Lambda'_T\right) + P\left(\hat{\theta}_R(k) \leq \Lambda'_R | \hat{\theta}_T(k) > \Lambda'_T\right) \\ &= \frac{1}{2} P\left(\hat{\theta}_R(k) > \pi, \hat{\theta}_T(k) \leq \pi\right) + \frac{1}{2} P\left(\hat{\theta}_R(k) \leq \pi, \hat{\theta}_T(k) > \pi\right). \end{aligned} \quad (5.32)$$

The subcarrier channel phase estimates at the transmitter and legitimate receiver, i.e. $\hat{\theta}_{\mathbf{T}}$ and $\hat{\theta}_{\mathbf{R}}$, respectively, are conditioned on the exact phase of the common channel θ. As a result, we can treat $\hat{\theta}_R(k)$ as a noisy version of $\hat{\theta}_T(k)$ for all N subcarriers of an OFDM signal. Mathematically, it can be expressed as

$$\hat{\theta}_R(k) = \hat{\theta}_T(k) + \Delta\theta(k), \quad k = 0, 1, \cdots, N-1, \quad (5.33)$$

where $\Delta\theta(k)$ is the phase estimation error between the estimates $\hat{\theta}_R(k)$ and $\hat{\theta}_T(k)$. As illustrated in Fig. 5.2, $\Delta\theta(k)$ can be derived from the noisy channel estimate as

$$\Delta\theta(k) = \tan^{-1}\left\{\frac{\left|\Delta H_{TR}(k)\right| \sin\left[\Delta\theta_{TR}(k) - \hat{\theta}_T(k)\right]}{\left|\hat{H}_T(k)\right| + \left|\Delta H_{TR}(k)\right| \cos\left[\Delta\theta_{TR}(k) - \hat{\theta}_T(k)\right]}\right\}. \quad (5.34)$$

For the trigonometric function $\tan x$, it can be approximated to x when x is small. Therefore, during a high SNR range that typically leads to a small estimation error, $\Delta\theta(k)$ can be approximated as

$$\Delta\theta(k) \approx \frac{\left|\Delta H_{TR}(k)\right| \sin\left[\Delta\theta_{TR}(k) - \hat{\theta}_T(k)\right]}{\left|\hat{H}_T(k)\right|}. \quad (5.35)$$

Referring to the statistics study in [112], the numerator of (5.35) follows a zero-mean Gaussian distribution with variance $\sigma^2_{TR}/2$. Meanwhile, the denominator $\left|\hat{H}_T(k)\right|$ is a Rayleigh distributed variable with a parameter $\sqrt{\sigma^2_{\hat{H}_T}/2}$. Based on the results

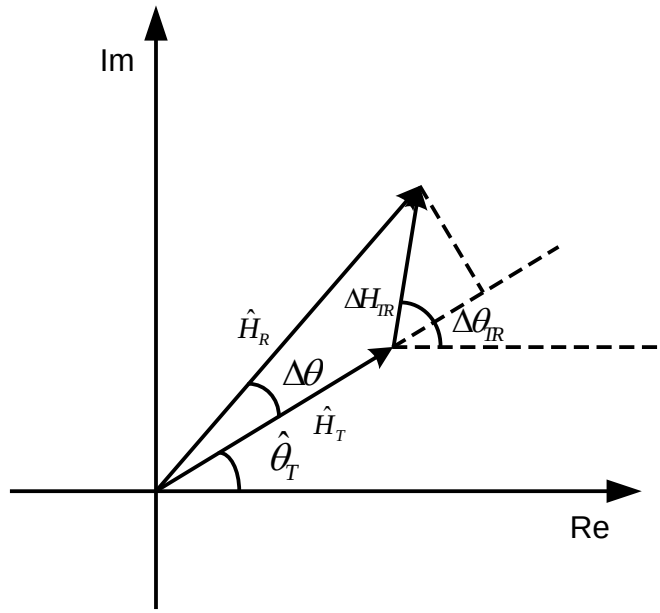


Figure 5.2: Derivation of the phase estimation error from the noisy channel estimates.

in [113] for the probability distribution of the ratio between a zero-mean Gaussian variable and a Rayleigh variable, the PDF and CDF of $\Delta\theta(k)$, i.e. $f_\theta\left(\Delta\theta(k)\right)$ and $F_\theta\left(\Delta\theta(k)\right)$, respectively, can be derived as

$$f_\theta\left(\Delta\theta(k)\right) = \frac{\sigma_{TR}^2 \sigma_{\hat{H}_T}}{2\left(\sigma_{\hat{H}_T}^2 \Delta\theta(k)^2 + \sigma_{TR}^2\right)^{3/2}} \tag{5.36}$$

and

$$F_\theta\left(\Delta\theta(k)\right) = \frac{1}{2} + \frac{\sigma_{\hat{H}_T} \Delta\theta(k)}{2\sqrt{\sigma_{\hat{H}_T}^2 \Delta\theta(k)^2 + \sigma_{TR}^2}}. \tag{5.37}$$

The probability of disagreement between the transmitter and legitimate receiver on whether the kth subcarrier is coordinate interleaved in the channel phase based

security scheme, $p'_L(k)$, can then be calculated as

$$
\begin{aligned}
p'_L(k) &= P(\hat{\theta}_R(k) > \Lambda'_R | \hat{\theta}_T(k) \leq \Lambda'_T) + P(\hat{\theta}'_R(k) \leq \Lambda'_R | \hat{\theta}_T(k) > \Lambda'_T) \\
&= \frac{1}{2}\int_0^{\pi}\left[\int_{\pi-\hat{\theta}_T(k)}^{2\pi-\hat{\theta}_T(k)} f_\theta(\Delta\theta(k))\, d\Delta\theta(k)\right]\frac{1}{2\pi}d\hat{\theta}_T(k) \\
&\quad + \frac{1}{2}\int_{\pi}^{2\pi}\left[\int_{-\hat{\theta}_T(k)}^{\pi-\hat{\theta}_T(k)} f_\theta(\Delta\theta(k))\, d\Delta\theta(k)\right]\frac{1}{2\pi}d\hat{\theta}_T(k) \\
&= \frac{1}{2}\int_0^{\pi}\left\{\frac{\sigma_{\hat{H}_T}\left[2\pi-\hat{\theta}_T(k)\right]}{2\sqrt{\sigma^2_{\hat{H}_T}\left[2\pi-\hat{\theta}_T(k)\right]^2+\sigma^2_{TR}}} - \frac{\sigma_{\hat{H}_T}\left[\pi-\hat{\theta}_T(k)\right]}{2\sqrt{\sigma^2_{\hat{H}_T}\left[\pi-\hat{\theta}_T(k)\right]^2+\sigma^2_{TR}}}\right\}\frac{1}{2\pi}d\hat{\theta}_T(k) \\
&\quad + \frac{1}{2}\int_{\pi}^{2\pi}\left\{\frac{\sigma_{\hat{H}_T}\left[\pi-\hat{\theta}_T(k)\right]}{2\sqrt{\sigma^2_{\hat{H}_T}\left[\pi-\hat{\theta}_T(k)\right]^2+\sigma^2_{TR}}} + \frac{\sigma_{\hat{H}_T}\hat{\theta}_T(k)}{2\sqrt{\sigma^2_{\hat{H}_T}\left[\hat{\theta}_T(k)\right]^2+\sigma^2_{TR}}}\right\}\frac{1}{2\pi}d\hat{\theta}_T(k).
\end{aligned}
\tag{5.38}
$$

Let $t = \pi - \hat{\theta}_T(k)$, $t' = 2\pi - \hat{\theta}_T(k)$, and $t'' = \hat{\theta}_T(k)$, we can rewrite (5.38) as

$$
\begin{aligned}
p'_L(k) &= \frac{1}{4\pi}\int_{\pi}^{2\pi}\frac{\sigma_{\hat{H}_T}t'}{2\sqrt{\sigma^2_{\hat{H}_T}t'^2+\sigma^2_{TR}}}dt' - \frac{1}{4\pi}\int_0^{\pi}\frac{\sigma_{\hat{H}_T}t}{2\sqrt{\sigma^2_{\hat{H}_T}t^2+\sigma^2_{TR}}}dt \\
&\quad + \frac{1}{4\pi}\int_{-\pi}^{0}\frac{\sigma_{\hat{H}_T}t}{2\sqrt{\sigma^2_{\hat{H}_T}t^2+\sigma^2_{TR}}}dt + \frac{1}{4\pi}\int_{\pi}^{2\pi}\frac{\sigma_{\hat{H}_T}t''}{2\sqrt{\sigma^2_{\hat{H}_T}t''^2+\sigma^2_{TR}}}dt'' \\
&= \frac{1}{2\pi}\frac{\sqrt{\sigma^2_{\hat{H}_T}4\pi^2+\sigma^2_{TR}} - \sqrt{\sigma^2_{\hat{H}_T}\pi^2+\sigma^2_{TR}}}{2\sigma_{\hat{H}_T}} \\
&\quad + \frac{1}{4\pi}\left(\frac{\sigma_{TR} - \sqrt{\sigma^2_{\hat{H}_T}\pi^2+\sigma^2_{TR}}}{2\sigma_{\hat{H}_T}} - \frac{\sqrt{\sigma^2_{\hat{H}_T}\pi^2+\sigma^2_{TR}} - \sigma_{TR}}{2\sigma_{\hat{H}_T}}\right) \\
&= \frac{\sqrt{\sigma^2_{\hat{H}_T}4\pi^2+\sigma^2_{TR}} - \sqrt{\sigma^2_{\hat{H}_T}\pi^2+\sigma^2_{TR}}}{4\pi\sigma_{\hat{H}_T}} + \frac{\sigma_{TR} - \sqrt{\sigma^2_{\hat{H}_T}\pi^2+\sigma^2_{TR}}}{4\pi\sigma_{\hat{H}_T}} \\
&= \frac{\sqrt{\sigma^2_{\hat{H}_T}4\pi^2+\sigma^2_{TR}} + \sigma_{TR} - 2\sqrt{\sigma^2_{\hat{H}_T}\pi^2+\sigma^2_{TR}}}{4\pi\sigma_{\hat{H}_T}}.
\end{aligned}
\tag{5.39}
$$

In the case that M subcarriers are involved in the channel phase based subcarrier coordinate interleaving, the interleaving pattern mismatch probability between the transmitter and legitimate receiver for an OFDM signal can be given by

$$P'_L = 1 - (1 - p'_L)^M . \tag{5.40}$$

Similarly, we can have the SER of the legitimate transmission in the proposed anti-eavesdropping OFDM system using channel phased based coordinate interleaving as

$$P'_{S,L} = 1 - (1 - P'_L)(1 - P_S) . \tag{5.41}$$

5.5 System Optimization with the Trade-off between Eavesdropping Resilience and Transmission Reliability

One superior anti-eavesdropping communication system should effectively prevent eavesdropping and concurrently maintain reliable legitimate transmission. As the eavesdropping prevention operation may degrade the legitimate transmission, a trade-off between the resilience against eavesdropping and the reliability of legitimate transmission needs to be realized. It can be concluded from the performance analysis of the proposed anti-eavesdropping system, including both channel gain and channel phase based schemes, the resilience of the proposed system against eavesdropping is decided by the number of subcarriers involved in the opportunistic coordinate interleaving in each OFDM signal. Meanwhile, the reliability of legitimate transmission depends on estimation errors in the channel estimates, as well as the number of subcarriers involved in the security design. Therefore, the proposed anti-eavesdropping OFDM system can be optimized by choosing a proper size of subcarrier set involved in the security design, and mitigating channel estimation errors to a tolerable level.

5.5.1 Proposed Evaluation Criterion for Anti-Eavesdropping Communication Systems

An anti-eavesdropping communication system should effectively defend against eavesdropping attacks and also minimize the impairment from the performed security processing to the legitimate transmission. Therefore, the evaluation of an anti-eavesdropping communication system must take into account its performances of eavesdropping prevention and legitimate transmission simultaneously. Unfortunately, no evaluation criterion can be found in the literature for assessing anti-eavesdropping communication systems in such a proper way.

To that end, a novel evaluation criterion for anti-eavesdropping communication systems, named probability of confidential transmission, is proposed in this study. It is defined as the probability that the transmitted data is correctly received by the legitimate receiver but not intercepted by the eavesdropper. Mathematically, we can express the probability of confidential transmission as

$$\Pi = P\big(E_{L,C}, E_{E,D}\big), \tag{5.42}$$

where $E_{L,C}$ denotes the event that the transmitted data is correctly received by the legitimate receiver, and $E_{E,D}$ indicates the event that eavesdropping is successfully prevented by the anti-eavesdropping communication system.

In the proposed anti-eavesdropping OFDM system, the performances of legitimate transmission and eavesdropping prevention are associated with two independent wireless channels. The two events $E_{L,C}$ and $E_{E,D}$ can be modelled as two independent variables. Consequently, the probability of confidential transmission in the channel gain based subcarrier coordinate interleaving scheme can be calculated as

$$\begin{aligned} \Pi_g &= P\big(E_{L,C}\big)P\big(E_{E,D}\big) \\ &= \big(1 - P_{S,L}\big)P_{S,E}, \end{aligned} \tag{5.43}$$

and the probability of confidential transmission in the channel phase based security scheme can be given by

$$\Pi_p = \left(1 - P'_{S,L}\right) P'_{S,E}. \tag{5.44}$$

5.5.2 Selection of the Size of Subcarrier Set Involved in the Opportunistic Coordinate Interleaving

It has been proved in (5.14) and (5.30) that the probability an eavesdropper making an incorrect guess of the interleaving pattern in an OFDM signal, for both the channel gain and phase based schemes, equals to $(1-1/2^M)$. This probability reflects the resilience of the system against eavesdropping, and can be used to guide the selection of number of subcarriers involved in the opportunistic coordinate interleaving in each OFDM signal. Given a requirement of such probability Ξ, the size of the subcarrier set, M, can be decided as

$$M = \left\lceil \log_2 \left(\frac{1}{1-\Xi} \right) \right\rceil, \tag{5.45}$$

where $\lceil \cdot \rceil$ denotes the ceiling function. It can be found from (5.45) that a strong eavesdropping prevention capability can be achieved by just involving a few subcarriers of each OFDM signal in the security design. For instance, when $M = 10$, P_E and P'_E have already been larger than 0.999, which would lead to a SER that almost equals to 100% at the eavesdropper.

From the perspective of legitimate transmission, the interleaving pattern mismatch probability at the intended receiver reduces along with the decrease of M, as demonstrated in (5.25) and (5.40). Consequently, we need to keep M as low as possible in order to maintain a reliable legitimate transmission. As an anti-eavesdropping communication system, it first needs to guarantee an acceptable resilience against eavesdropping, and then endeavors to enhance the reliability of legitimate transmission. Thus, the number of subcarriers involved in the opportunistic coordinate interleaving

of the proposed anti-eavesdropping OFDM system can be decided by (5.45), based on minimum requirements of P_E and P'_E.

5.5.3 Channel Estimation Error Mitigation Technique

In addition to restricting the number of subcarriers involved in the opportunistic coordinate interleaving in each OFDM signal, the reliability of legitimate transmission can be further improved through mitigating the channel estimation errors. Considering that errors in the channel estimates are i.i.d. zero-mean Gaussian variables, one candidate solution is to average multiple channel estimates that have an identical true value. In a slow time-varying wireless channel, the channel impulse response can be invariant over several signal periods. For instance, in the IEEE 802.11g system, the channel coherence time is approximately 53 ms according to the typical pedestrian walking speed 1 m/s, while the period of an OFDM signal is 4 us. As a result, the channel fading can ideally be considered as invariant over more than 10000 successive OFDM signals. The averaging based channel estimation error mitigation technique is thus exercisable in practice. Assuming that Ω estimates are averaged to provide a more accurate channel estimate, the variance of the estimation error after the averaging processing can be reduced by $1/\Omega$.

5.6 Simulation Results

Simulations are carried out following the specifications of IEEE 802.11g standard. Each OFDM signal is generated through a 64-point IFFT, and has a cyclic prefix of length 16. 4-QAM is adopted as the modulation scheme for all subcarriers. Unless stated otherwise, the transmitted OFDM signals are propagated through a Rayleigh fading channel with exponential power delay profile of 50 ns RMS delay. Moreover, training symbols with unit energy at each subcarrier are transmitted and exploited for the channel estimation, while least-square (LS) channel estimation technique is

adopted at all nodes in the network. In order to achieve a fair comparison, the statistical models of the common channel and eavesdropping channel, as well as the noise power levels at all nodes, are set to be the same. In addition, perfect synchronization is assumed to be achieved at both the legitimate receiver and the eavesdropper.

The probability of confidential transmission in the conventional OFDM system is provided as a benchmark reference in the simulations. Since the conventional OFDM system has a physical layer that is transparent to eavesdroppers, its eavesdropping prevention performance can be characterized by the SER under the eavesdropping channel. As a result, the probability of confidential transmission in the conventional OFDM system, Π_c, can be given by

$$\Pi_c = (1 - P_S)\, P_S. \tag{5.46}$$

5.6.1 Performance of the Channel Gain based Security Scheme

5.6.1.1 Interleaving Pattern Mismatch Probabilities in the Channel Gain based Scheme

First of all, the interleaving pattern mismatch probability between the transmitter and eavesdropper is evaluated, where the transmitter derives the coordinate interleaving pattern from the channel gain of the common channel and the eavesdropper estimates the interleaving pattern from the channel gain of the eavesdropping channel. Simulation results are presented in Fig. 5.3. In the left subfigure, we change the number of subcarriers involved in the opportunistic coordinate interleaving in each OFDM signal, but fix the amount of channel estimates averaged for the estimation error mitigation to 30. The mismatch probability P_E decreases when the size of the subcarrier set reduces. However, the variation is ignorable and the mismatch probability is always close to 100%. In the right subfigure, we fix the number of subcarriers involved in the coordinate interleaving to 32 and study the impact of the number of averaged channel estimates on P_E. Since the interleaving pattern mismatch be-

tween the transmitter and eavesdropper is dominated by the independence between the common channel and eavesdropping channel, the estimation errors almost have no impact on P_E that is always close to 100% in the simulations.

The mismatch probability between the coordinate interleaving pattern at the transmitter and that at the legitimate receiver is simulated and plotted in Fig. 5.4. As shown in the figure, when the number of averaged channel estimates is fixed to 30, the mismatch probability P_L significantly reduces with the decrease of the number of subcarriers involved in the opportunistic coordinate interleaving. Moreover, when more channel estimates are averaged to mitigate the estimation errors, the transmitter and legitimate receiver are more likely to derive an identical coordinate interleaving pattern.

5.6.1.2 Probability of Confidential Transmission in the Channel Gain based Scheme

The performance of the proposed channel gain based anti-eavesdropping OFDM system, in terms of the probability of confidential transmission Π_g, is depicted in Fig. 5.5. As a benchmark reference, the probability of confidential transmission of the conventional OFDM system is also provided in the evaluation. In the simulation, we set $\Omega = 30$ and vary the size of the subcarrier set from 16 to 64. Compared with the conventional OFDM, the proposed anti-eavesdropping OFDM system has a little worse performance in the low SNR range when the resilience against eavesdropping and the reliability of legitimate transmission are simultaneously evaluated. The reason for this phenomenon is that the legitimate transmission in the proposed system is not so reliable as that in the conventional OFDM system during the low SNR range, caused by the interleaving pattern mismatch between the transmitter and legitimate receiver. However, when the SNR is larger than 15 dB, which is the typical SNR condition in wireless communications, the proposed system has a probability of confidential transmission much higher than that of the conventional OFDM system.

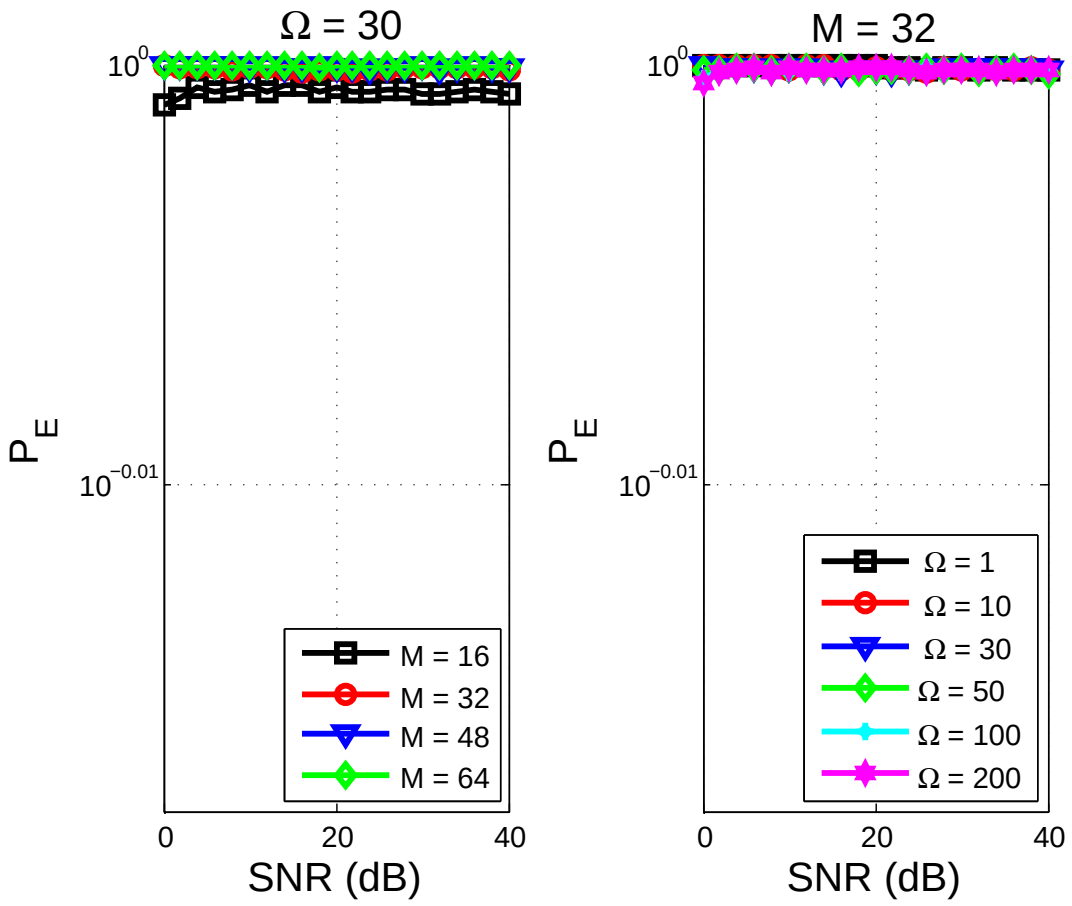


Figure 5.3: Interleaving pattern mismatch probability at the eavesdropper in the channel gain based scheme.

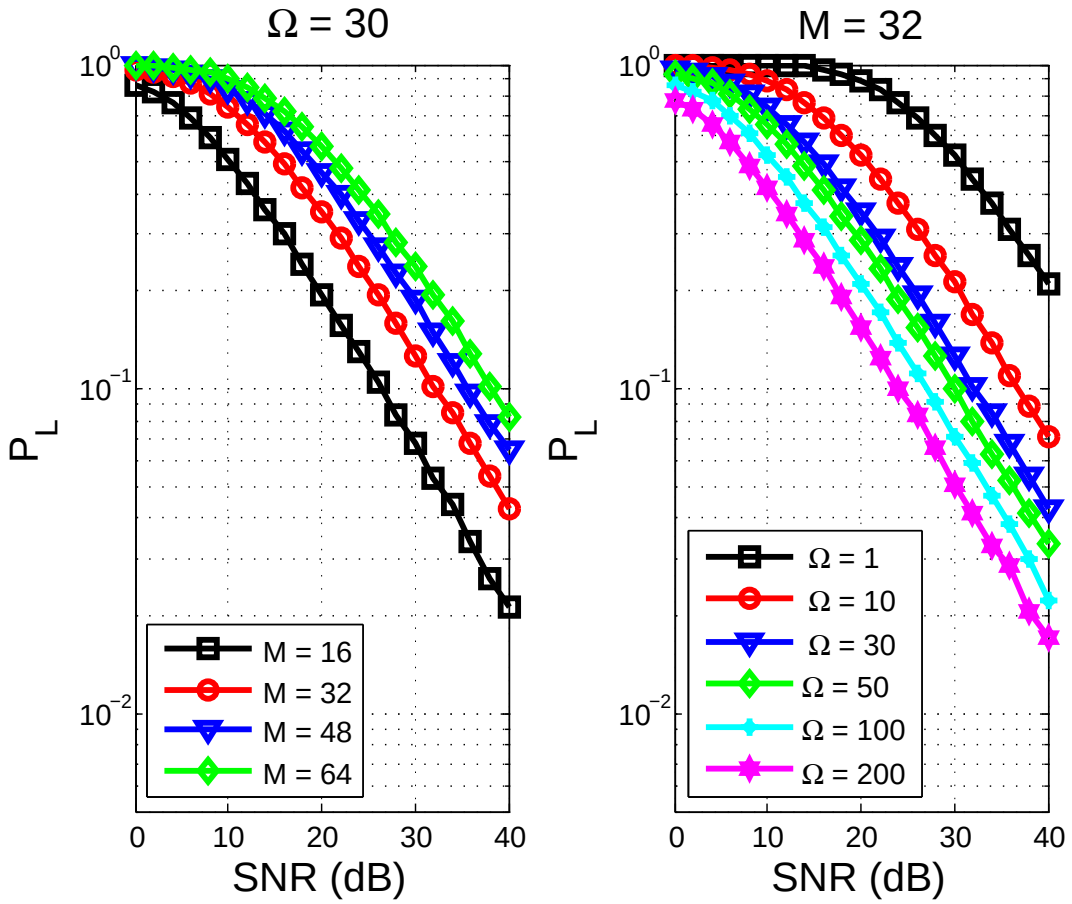


Figure 5.4: Interleaving pattern mismatch probability at the legitimate receiver in the channel gain based scheme.

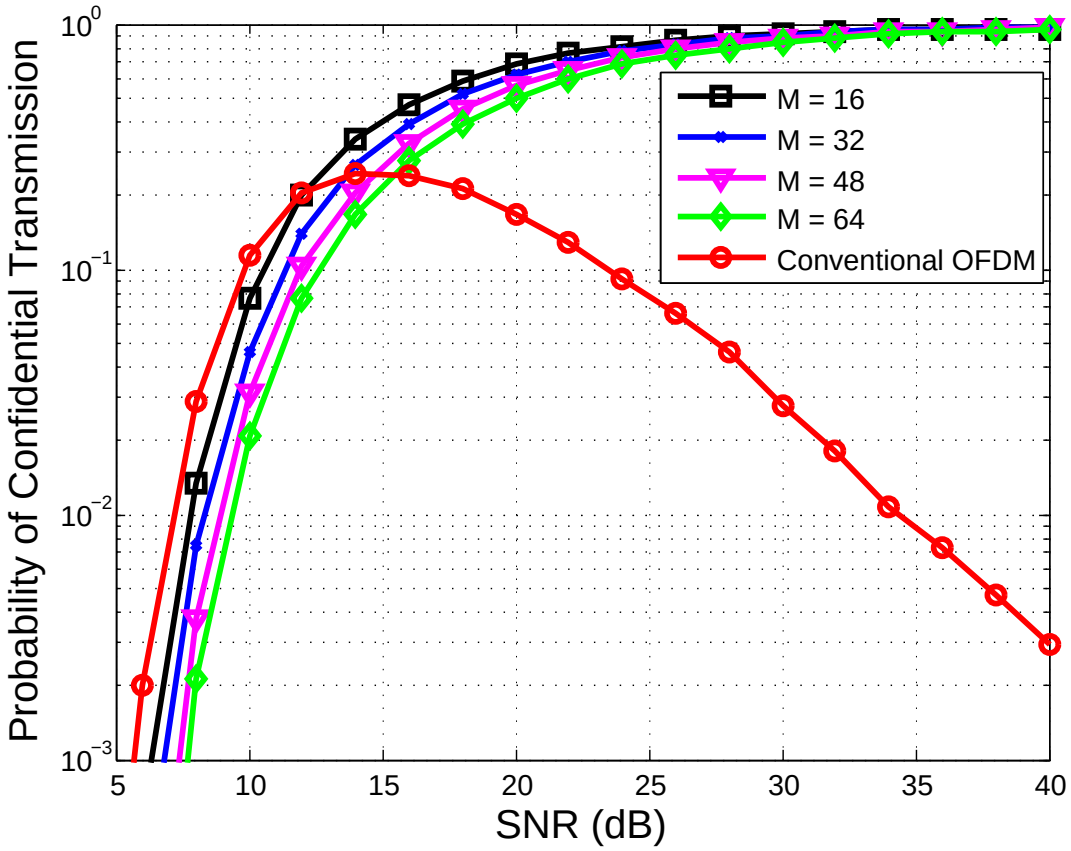


Figure 5.5: Comparison of confidential transmission probabilities between the channel gain based anti-eavesdropping system and the conventional OFDM when $\Omega = 30$.

Moreover, during the low SNR range, a smaller number of subcarriers involved in the security design would lead to a better performance of the proposed anti-eavesdropping system. Nevertheless, the impact of M on Π_g turns to be indistinct during the high SNR range. In addition, there is an interesting finding that the conventional OFDM system reaches a peak performance when SNR is around 14 dB. After that, its probability of confidential transmission decreases with the increase of SNR since the conventional OFDM system is easier to be intercepted in a better channel condition.

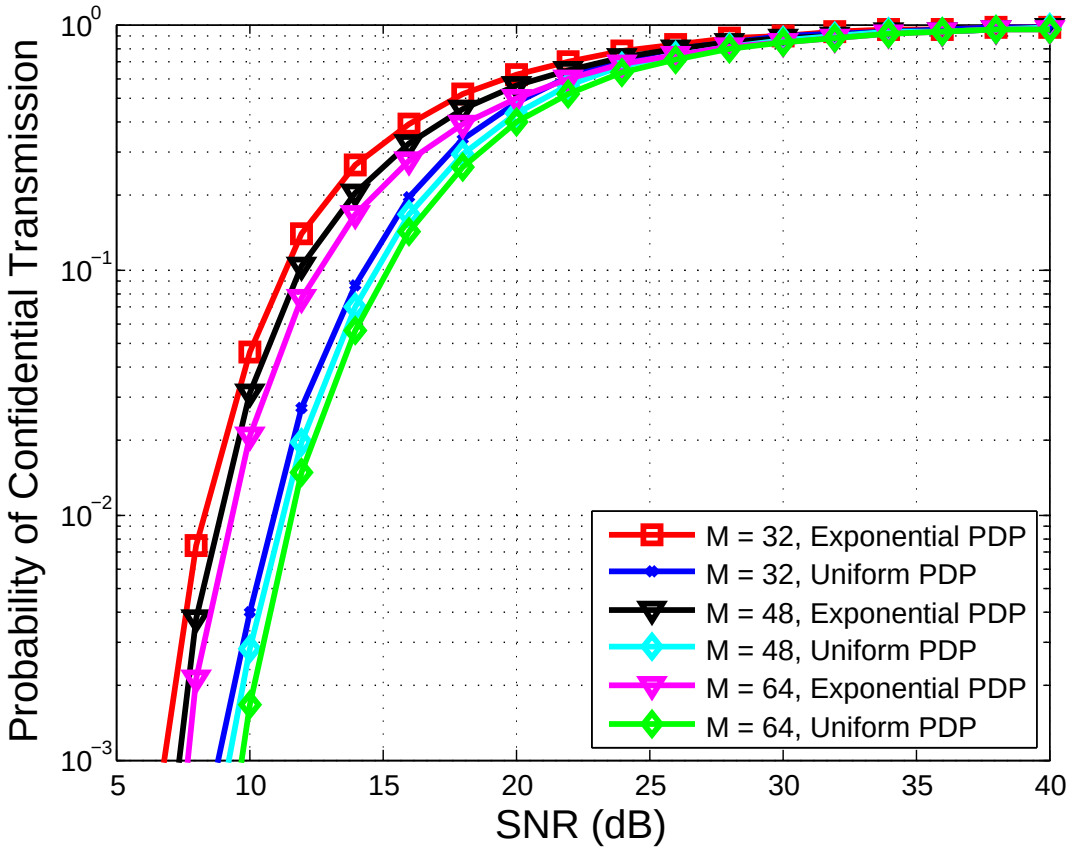


Figure 5.6: Probability of confidential transmission in the channel gain based scheme under different channel models when $\Omega = 30$.

5.6.1.3 Probability of Confidential Transmission in the Channel Gain based Scheme under Different Channel Models

The probability of confidential transmission in the channel gain based security scheme under different wireless channel models is also evaluated in the study. Another Rayleigh fading channel with an uniform PDP of 800 ns delay spread, which introduces a more hostile multipath environment, is considered in the simulation. As presented in Fig. 5.6, a more hostile multipath environment would degrade the confidential transmission probability of the proposed anti-eavesdropping OFDM system, where the performance loss mainly comes from the degradation of the legitimate transmission.

5.6.2 Performance of the Channel Phase based Security Scheme

5.6.2.1 Interleaving Pattern Mismatch Probabilities in the Channel Phase based Scheme

The eavesdropper's interleaving pattern mismatch probability in the channel phase based security scheme is provided in Fig. 5.7, where the transmitter and eavesdropper derive the coordinate interleaving patterns from subcarrier channel phases of the common channel and eavesdropping channel, respectively. It can be found that the mismatch probability P'_E is always close to 100%, no matter how many subcarriers are involved in the opportunistic coordinate interleaving and how many channel estimates are averaged to mitigate the estimation errors.

Figure 5.8 plots the interleaving pattern mismatch probability at the legitimate receiver in the channel phase based security scheme, denoted by P'_L. Similar to the mismatch probability P_L in the channel gain based scheme, P'_L can be reduced by involving less subcarriers in the opportunistic coordinate interleaving and averaging more channel estimates to mitigate the channel estimation errors.

5.6.2.2 Probability of Confidential Transmission in the Channel Phase based Scheme

The probability of confidential transmission in the proposed channel phase based anti-eavesdropping OFDM system, Π_p, is evaluated in Fig. 5.9. The channel phase based scheme has a confidential transmission probability similar to that of the conventional OFDM when the SNR is lower than 12 dB. With the increase of SNR, the proposed system can achieve an obviously higher probability of confidential transmission. In addition, no significant impact of M on the probability of confidential transmission can be found in the proposed channel phase based scheme.

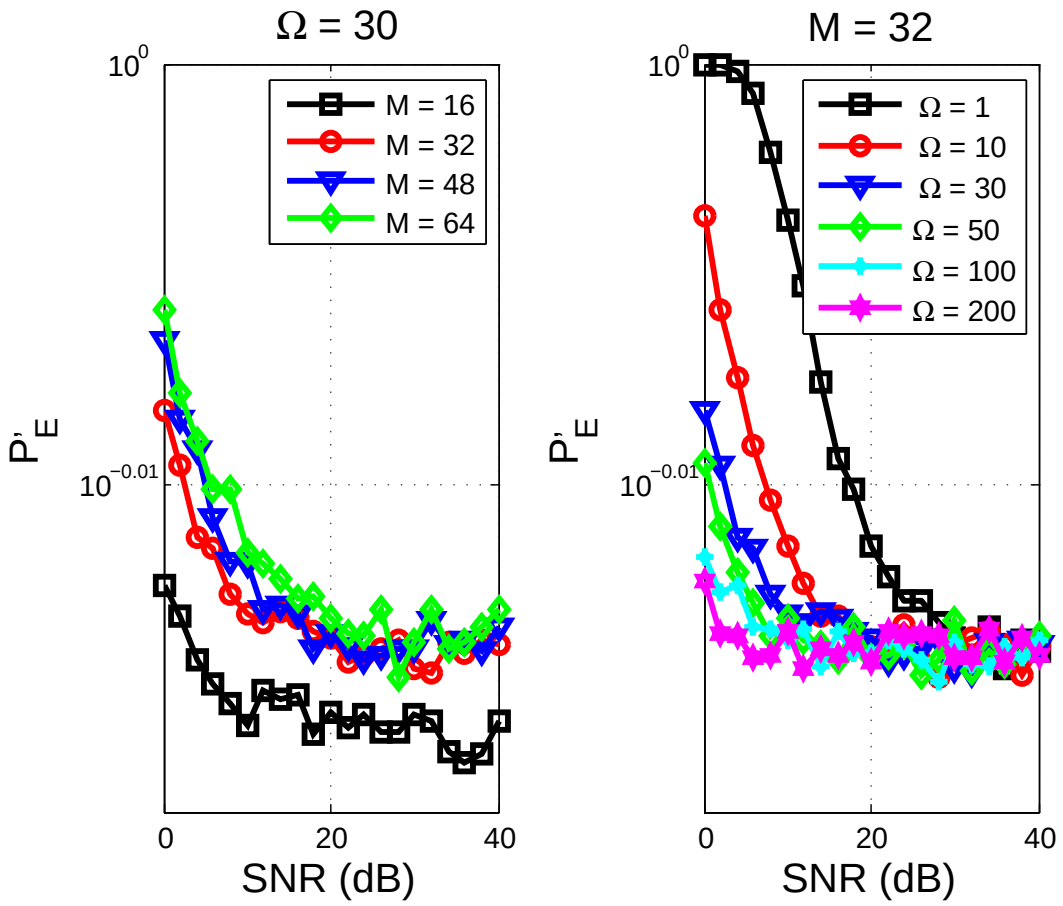


Figure 5.7: Interleaving pattern mismatch probability at the eavesdropper in the channel phase based scheme.

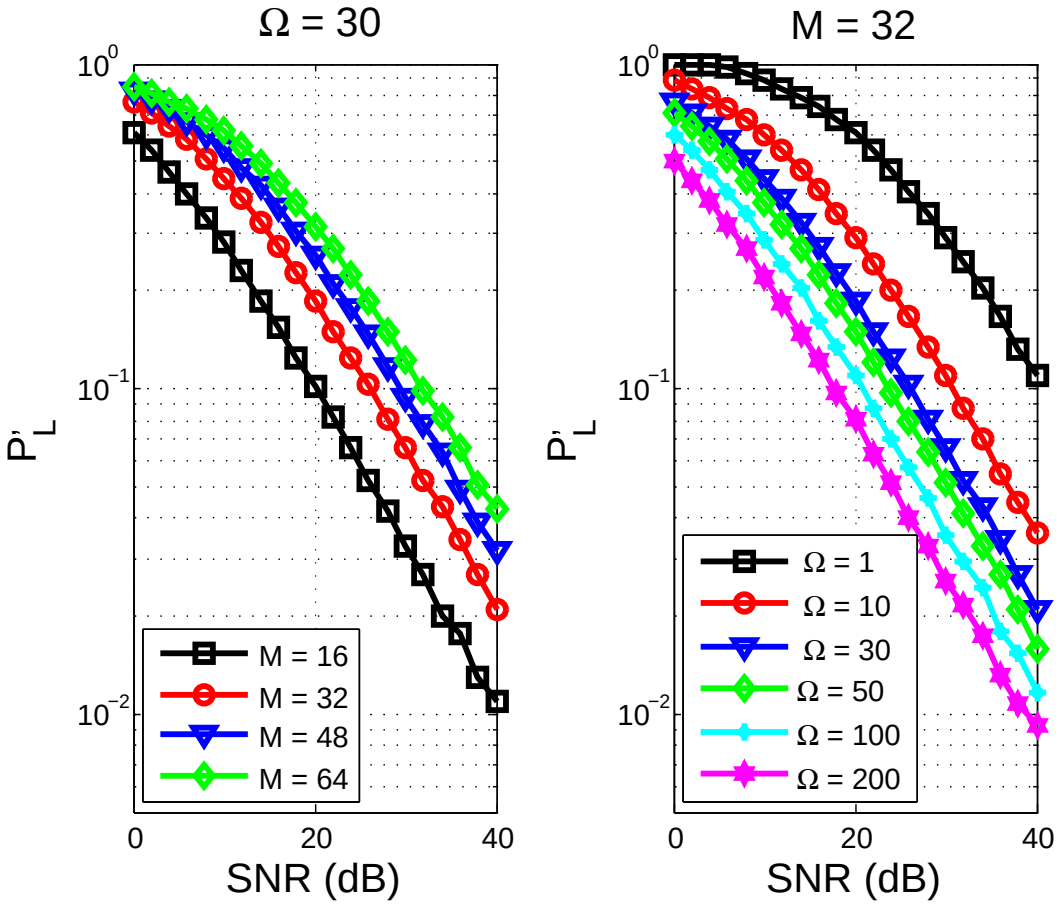


Figure 5.8: Interleaving pattern mismatch probability at the legitimate receiver in the channel phase based scheme.

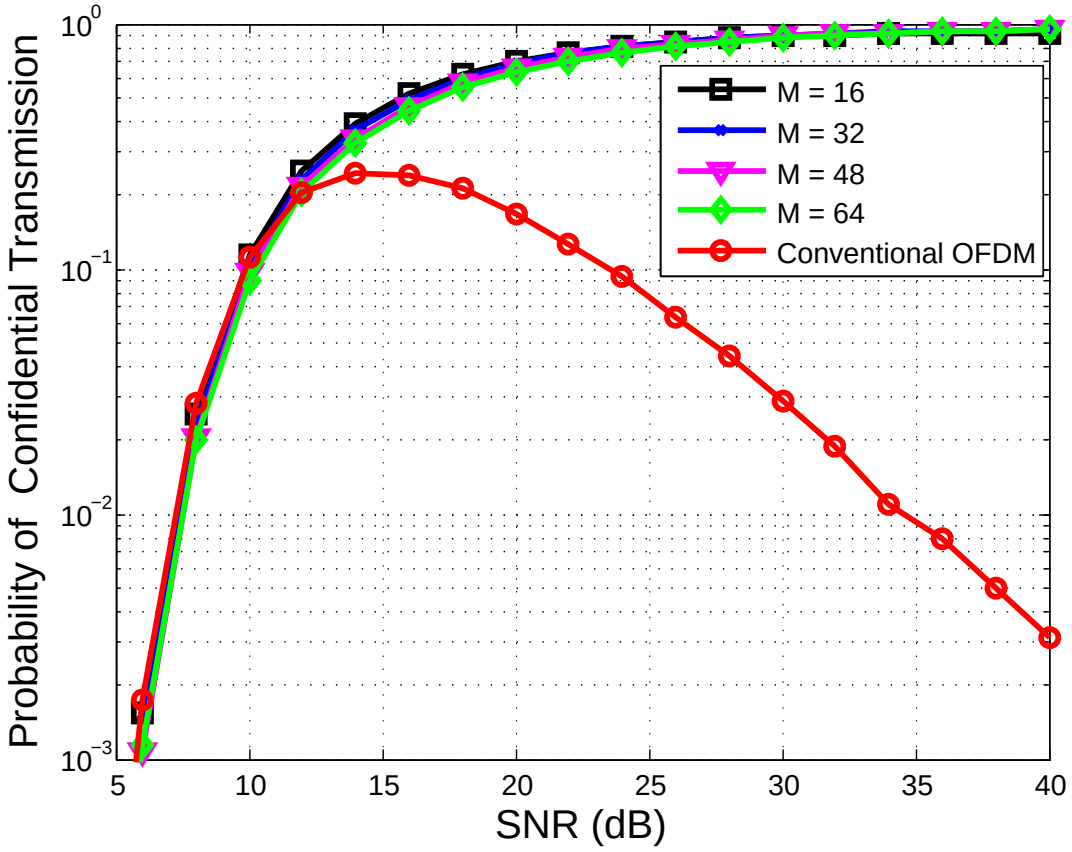


Figure 5.9: Comparison of confidential transmission probabilities between the channel phase based anti-eavesdropping system and the conventional OFDM when $\Omega = 30$.

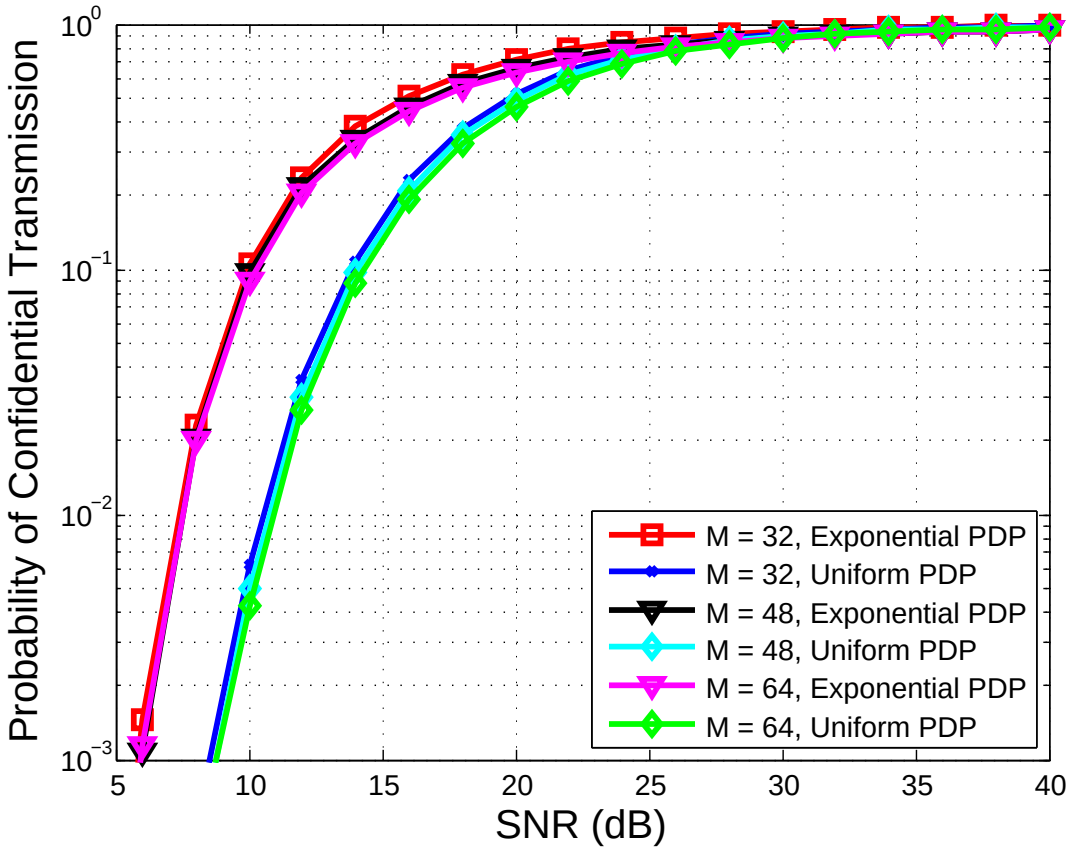


Figure 5.10: Probability of confidential transmission in the channel phase based scheme under different channel models when $\Omega = 30$.

5.6.2.3 Probability of Confidential Transmission in the Channel Phase based Scheme under Different Channel Models

The Rayleigh fading channel with an uniform PDP of 800 ns delay spread is also considered for evaluating the probability of confidential transmission in the channel phase based security scheme. Similar to the results in the channel gain based coordinate interleaving, the channel phase based anti-eavesdropping system has a worse performance in the more hostile Rayleigh fading channel, as shown in Fig. 5.10.

5.6.3 Performance Comparison between the Channel Gain and Channel Phase based Schemes

A comprehensive comparison between the proposed channel gain and channel phase based coordinate interleaving schemes is conducted in this subsection, using the previously presented simulation results. From the perspective of the interleaving pattern mismatch probability, the channel gain and channel phase based schemes can both achieve quite high mismatch probabilities between the transmitter and eavesdropper. However, regarding to the interleaving pattern mismatch probability between the transmitter and legitimate receiver, the channel phase based scheme has a lower mismatch probability under the same channel condition. The main reason for this phenomenon is that channel gains are more sensitive to the noise and interference, compared to channel phases [88]. When we simultaneously evaluate their eavesdropping resilience and transmission reliability, as shown in Figs. 5.5, 5.6, 5.9 and 5.10, the channel phase based scheme performs slightly better than the channel gain based scheme, particularly in a low SNR range.

Merely considering the probability of confidential transmission, the proposed channel phase based scheme would be slightly better than the channel gain based security design. However, when more factors, such as the computational complexity and hardware limitations in the implementation, are taken into account, the channel gain based scheme may be preferred since it is easier to perform and can also effectively defend against eavesdropping. Overall, both the channel gain and channel phase based dynamic coordinate interleaving can effectively prevent eavesdropping and, at the same time, provide a reliable legitimate transmission. The selection between the proposed channel gain and channel phase based security schemes would depend on the operating environment, the available power and hardware, as well as the acceptable computational complexity.

5.7 Summary

In this chapter, an eavesdropping prevention strategy in OFDM systems through dynamic subcarrier coordinate interleaving is proposed, by taking advantage of the reciprocal, location-dependent and time-varying nature of wireless channels. Symbol coordinates of the subcarriers in each OFDM signal are interleaved in an opportunistic manner depending on the reciprocal channel state information between the transmitter and legitimate receiver. Two coordinate interleaving schemes are investigated, which employ the subcarrier channel gain and phase in determining the interleaving pattern, respectively. More specifically, the transmitter performs coordinate interleaving at subcarriers with channel gains (or channel phases) larger than a predefined threshold. Since wireless channels associated with each pair of users at separate locations exhibit independent propagation characteristics, the frequently updated selection of subcarriers undergoing coordinate interleaving is only shared between legitimate users based on channel reciprocity. Without a matched subcarrier coordinate de-interleaving pattern, erroneous information recovery is carried out at the eavesdropper so that eavesdropping is prevented. In order to simultaneously evaluate the eavesdropping resilience and transmission reliability of anti-eavesdropping communication systems, a novel evaluation criterion, named probability of confidential transmission, is also proposed in this study. Theoretical analysis and simulation results are provided to validate the proposed anti-eavesdropping OFDM system.

Chapter 6

Eavesdropping-Resilient OFDM Using Dynamic Subcarrier Interleaving

The built-in security of wireless OFDM communication systems against eavesdropping can be remarkably improved through the proposed dynamic coordinate interleaving strategy in Chapter 5. One noteworthy prerequisite of that strategy is that data symbols transmitted at OFDM subcarriers must be in a complex-number structure. It is true that most modulation schemes adopted in modern wireless OFDM networks produce complex data symbols, such as QPSK and QAM. However, we cannot neglect the possible utilization of modulation schemes that modulate data bits into a real-number structure, like BPSK. Eavesdropping prevention techniques without the restriction of symbol modulation schemes utilized in OFDM systems thus need to be investigated.

This chapter proposes a novel and effective eavesdropping-resilient OFDM system through dynamic subcarrier interleaving, without any restriction of the adopted symbol modulation scheme. The built-in security of the proposed secure OFDM system is enhanced by exploiting the channel reciprocity and uncorrelation feature exhibited

among spatially separate wireless channels in rich multipath environments. The transmitter employs its dynamic and reciprocal channel state information to the intended receiver in designing the subcarrier interleaving pattern. More specifically, subcarriers are interleaved according to the sorted order of their channel gains. In order to mitigate the impairment of imperfect channel reciprocity, only partial subcarriers of each OFDM symbol are included in the interleaving. A subcarrier selection algorithm is also investigated to realize a trade-off between the eavesdropping resilience and legitimate transmission reliability. Because of channel reciprocity, identical CSI information is shared between legitimate parties, so that the subcarrier interleaving scheme initiated by the transmitter can be figured out at the legitimate receiver locally without any feedback from the transmitter. In contrast, due to the fact that spatially separate wireless channels are independent of each other, an eavesdropper at a third location cannot derive the identical subcarrier interleaving pattern used at the transmitter. Consequently, mismatched information recovery occurs at the eavesdropper, thus preventing malicious eavesdropping. The proposed secure OFDM system is validated through both theoretical analysis and simulations. From simulation results, eavesdropping on the proposed system suffers a SER close to 100% while the legitimation transmission has a SER matching to that of conventional OFDM systems.

6.1 Introduction

OFDM has been widely employed in modern high-speed wireless communication networks. Unfortunately, the conventional OFDM signal is vulnerable to malicious eavesdropping and intervention, due to its distinct time and frequency characteristics [13]. Traditional upper-layer security mechanisms cannot completely address the security threats in wireless OFDM systems, because of the transparence of their physical layer transmission parameters, It is therefore of significant importance to enhance the security of OFDM systems at the physical layer.

Physical layer security, which targets the communication security at the physical layer, is emerging as an effective complement to the traditional security strategies in securing wireless transmissions [13]. Extensive research efforts have been devoted to improve the physical layer security of OFDM systems against eavesdropping recently [13, 98–104]. Generally, the existing security enhancement techniques for wireless OFDM systems are conditioned on the knowledge of eavesdropping channel, additional resource, significant modifications to off-the-shelf systems, or high operational complexity. Simple but effective security approaches for OFDM at the physical layer have yet to be investigated. Chapter 5 of this dissertation proposes a simple and effective anti-eavesdropping OFDM system based on dynamic coordinate interleaving, which can prevent eavesdropping and concurrently maintain a reliable legitimate transmission. However, such anti-eavesdropping OFDM system would ask for a symbol modulation scheme that modulates data bits into a complex-number structure. In light of the possible employment of modulation schemes generating real data symbols in OFDM systems, eavesdropping prevention techniques without any restriction of symbol modulation schemes also need to be investigated for wireless OFDM communication networks.

An effective and simple eavesdropping-resilient OFDM system is proposed in this chapter by exploiting the dynamic subcarrier interleaving, inspired by the channel reciprocity between legitimate user terminals and the uncorrelated behavior of spatially separate wireless channels in rich multipath environments. Although subcarrier interleaving has been introduced into OFDM systems to improve the transmission reliability [114–118], the transmission security in OFDM systems has been largely ignored. In this contribution, the CSI between the transmitter and legitimate receiver are utilized to defend against eavesdropping. To be specific, partial subcarriers of each OFDM signal are selected and then interleaved according to the sorted order of their channel gains. A subcarrier selection algorithm is investigated to combat the imperfect channel reciprocity between legitimate users, so as to realize a trade-off between the eavesdropping resilience and legitimate transmission reliability. Based on channel

reciprocity, the frequently renewed subcarrier selection and interleaving scheme can be shared between legitimate terminals without involving the exchange of secret information. Due to the channel spatial decorrelation, the subcarrier interleaving pattern is not available to eavesdroppers that experience independent channels, so that the information recovery for eavesdropping is interrupted. The proposed system is validated through analytical and simulation results. Compared to conventional OFDM systems, our approach is much more resilient to eavesdropping. Differing from prior works, the proposed scheme can avoid additional resource consumption, has limited computational complexity, only needs minor modifications of existing systems, and is free from the restriction of modulation schemes adopted in the OFDM systems.

The reminder of this chapter is organized as follows. Section 6.2 introduces the system model and relevant background about the multipath channel in OFDM systems. The proposed eavesdropping-resilient OFDM system is described in Section 6.3, followed by a performance evaluation in Section 6.4. The interleaved subcarrier selection algorithm is investigated in Section 6.5. Simulation results are provided in Section 6.6. Finally, the conclusions are drawn in Section 6.7.

Notations Throughout the chapter, bold letters are used to identify a vector, i.e. $\mathbf{X} = \{X(1), X(2), \cdots, X(N-1)\}$. Complex Gaussian random variable X with mean m, variance σ^2, and with independent and identically distributed real and imaginary components is denoted as $X \sim CN(m, \sigma^2)$.

6.2 Problem Formulation and Preliminaries

6.2.1 System Model

The wireless communication system model considered in this chapter is presented in Fig. 6.1. A source node communicates with a legitimate receiver using OFDM, in the presence of a passive and silent eavesdropper in a richly scattered radio environment. The eavesdropper can overhear all the communications between the legitimate

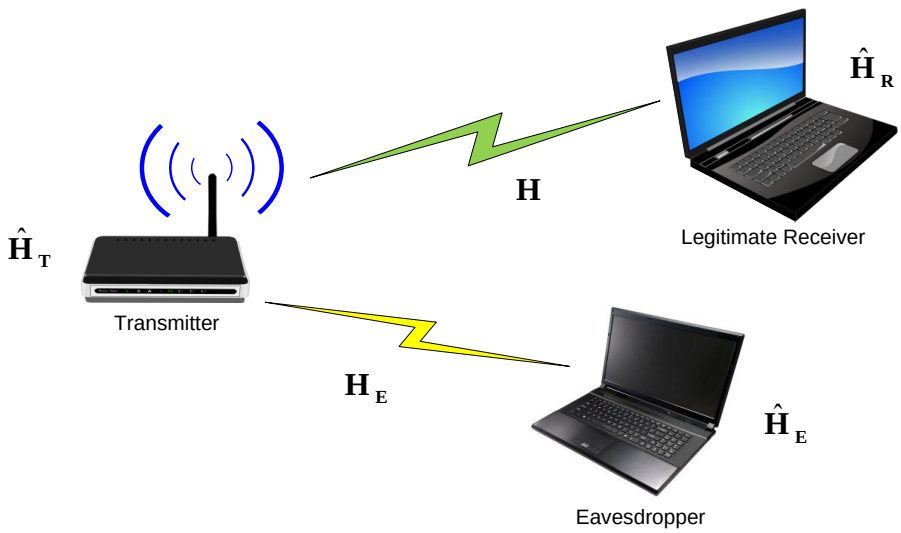


Figure 6.1: Wireless communication scenario consisting of two legitimate terminals and an eavesdropper.

users but it is not interested in disrupting the legitimate transmission. The forward and reverse channels between legitimate users occupy the same frequency band and remain constant over several time slots. In addition, the underlying noise and interference in both the common channel and the eavesdropping channel can be modeled as additive white Gaussian noise.

Generally, a third party who is at a distance larger than half a wavelength from the intended receiver, experiences fading conditions that are uncorrelated to those between the original legitimate communicating terminals [26]. In most practical scenarios, the eavesdropper has to be sufficiently separated from the legitimate terminals to avoid being detected, that is, with a distance more than half a wavelength. Therefore, the common channel and the eavesdropping channel are modeled as independent of each other throughout this chapter.

6.2.2 Multipath Channel in OFDM Systems

Considering an OFDM system with N subcarriers, the received signal at the output of fast Fourier transform can be described as

$$R(k) = H(k)\,S(k) + W(k)\,, \quad k = 0, 1, \cdots, N-1, \tag{6.1}$$

where $S(k)$ and $R(k)$ represent the data transmitted and received at the kth subcarrier, respectively, $W(k)$ indicates a complex AWGN with variance of σ_k^2, and $H(k)$ is the frequency domain channel response at the kth subcarrier, which can be represented as

$$H(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{L-1} h(n)\, e^{-j2\pi \frac{kn}{N}}, \tag{6.2}$$

where $h(n)$ denotes the time domain channel response associated with the nth channel tap. In Rayleigh fading, $\{h(0), h(1), \cdots, h(L-1)\}$ can be considered as independent and identically distributed zero-mean complex Gaussian random variables. Therefore, $H(k)$, which is characterized by the L time domain channel taps, can be modeled as $CN(0, \sigma_H^2)$ due to central limit theorem. Assuming that the subcarrier interval is larger than the coherence bandwidth of the wireless channel, all the subcarriers, i.e. $H(k), k = 0, 1, \cdots, N-1$, experience independent and identically distributed fading. Since OFDM subcarriers, as well as the channel responses acting on the subcarriers, are independent of each other, all subcarriers of an OFDM signal can be treated independently.

6.2.3 Principle Behind the Proposed Design

The randomness of wireless multipath channels is exploited to enhance the transmission security at the physical layer in the design. A dynamic subcarrier interleaving scheme is proposed for securing OFDM systems against eavesdropping, by taking advantage of the reciprocity, spatial decorrelation and time variation of wireless channels.

Channel reciprocity indicates that the wireless channel behaves in an identical manner irrespective of in which direction it is observed. Therefore, both the transmitter and the legitimate receiver would theoretically have an identical estimate of the common channel $H(k)$ and then derive the same CSI-based interleaving pattern. In practice, all nodes in a network can only obtain a noisy version of the channels due to estimation errors at channel estimators, induced by interference, noise, as well as hardware limitations [119]. Thus, the frequency domain channel responses observed at the legitimate nodes during a channel coherence time take the form as

$$\hat{H}_T(k) = H(k) + \Delta H_T(k), \quad k = 0, 1, \cdots, N-1, \tag{6.3}$$

and

$$\hat{H}_R(k) = H(k) + \Delta H_R(k), \quad k = 0, 1, \cdots, N-1, \tag{6.4}$$

where $\hat{H}_T(k)$ and $\hat{H}_R(k)$ denote the estimates of the common channel $H(k)$ at the transmitter and the legitimate receiver, respectively. $\Delta H_T(k)$ and $\Delta H_R(k)$ are the corresponding estimation errors, which can be modeled as zero-mean Gaussian random variables. Following the assumption that $H(k), k = 0, 1, \cdots, N-1$ are i.i.d., $\Delta H_{T/R}(k)$ for $k = 0, 1, \cdots, N-1$ should also be statistically independent but may not be identically distributed. In order to facilitate the analysis, $\Delta H_{T/R}(k), k = 0, 1, \cdots, N-1$ are assumed to be i.i.d. in the following discussion, so that

$$\Delta H_{T/R}(k) \sim CN\left(0, \sigma^2_{T/R}\right), \tag{6.5}$$

where $\sigma^2_{T/R}$ is the variance of the estimation errors. Since $H(k)$ and $\Delta H_{T/R}(k)$ are independent, $\hat{H}_{T/R}(k)$ also follows a complex Gaussian distribution with zero mean and variance of $\sigma^2_{\hat{H}_{T/R}} = \sigma^2_H + \sigma^2_{T/R}$. Therefore, the estimates of the common channel at the transmitter and intended receiver may not be perfectly reciprocal in practice, but they are correlated at least.

Channel spatial decorrelation denotes the fact that wireless channels associated

with different endpoints at separate locations typically exhibit uncorrelated propagation characteristics [10]. As a result, for an eavesdropper at a third location, the eavesdropping channel $H_E(k)$ would be uncorrelated to the common channel $H(k)$. It is thus hard for the eavesdropper to track the subcarrier interleaving scheme involved in the legitimate transmission and to recover the information in transmission. Eavesdropping can then be prevented. Considering that estimation errors exist in the channel estimate, the noisy channel observations at the eavesdropper, $\hat{H}_E(k)$, can be expressed as

$$\hat{H}_E(k) = H_E(k) + \Delta H_E(k), \quad k = 0, 1, \cdots, N-1. \tag{6.6}$$

Similarly, the channel estimation error $\Delta H_E(k)$ follows a complex Gaussian distribution $CN\left(0, \sigma_E^2\right)$ and $\hat{H}_E(k), k = 0, 1, \cdots, N-1$ can be modeled as i.i.d. complex Gaussian variables. Since $\Delta H_E(k)$ is independent of $\Delta H_T(k)$ and $\Delta H_R(k)$, the channel estimate at the eavesdropper, $\hat{H}_E(k)$, should also be independent of the estimates $\hat{H}_T(k)$ and $\hat{H}_R(k)$ obtained at legitimate terminals.

In addition, wireless channels are time-varying and thus introduce continual influx of randomness. Consequently, the CSI-based subcarrier interleaving scheme would be renewed frequently, which further strengthens the security.

6.3 Proposed Secure OFDM System with Dynamic Subcarrier Interleaving

The proposed eavesdropping-resilient OFDM system with dynamic subcarrier interleaving is illustrated in Fig. 6.2. At the transmitter, M out of the N subcarriers of an OFDM signal are selected and interleaved after the symbol modulation. Accordingly, subcarrier deinterleaving is carried out at the receiver between equalization and the symbol demodulation processes. The selection of M subcarriers and the interleaving permutation are determined by the real-time CSI between the transmitter and the legitimate receiver. The other processing steps of the proposed system are

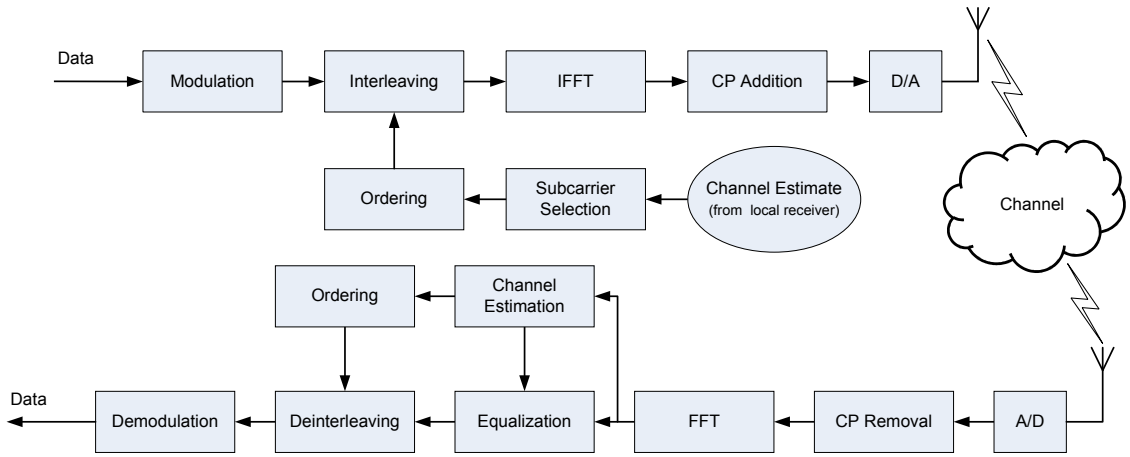


Figure 6.2: Block diagram of the proposed eavesdropping-resilient OFDM system using dynamic subcarrier interleaving.

identical to those of a conventional OFDM system.

6.3.1 Interleaved Subcarrier Selection

In practical systems, the transmitter can estimate the CSI of the common channel via handshaking signals or feedback such as acknowledgement (ACK) packet from the intended receiver, while the receiver can obtain the temporal channel estimation from training signals or inserted pilots. Their observations are ideally identical but only correlated in practice, because of the asymmetric observations caused by the noise, interference and hardware limitations, as shown in (6.3) and (6.4). Although the radio channel is reciprocal, estimates of the radio channel are not perfectly reciprocal [120].

In order to mitigate the impairment of imperfect channel reciprocity between legitimate users, a combination of M subcarriers that can provide an interleaving pattern robust to estimation deviations under the current channel condition is selected for the interleaving at the transmitter, where $M \leq N$. A trade-off between the resilience to eavesdropping and the reliability of legitimate transmission is realized in the proposed subcarrier selection algorithm. A detailed discussion of the subcarrier selection algorithm will be presented in Section 6.5, after analyzing how the proposed interleaving scheme acts on the performances of eavesdropping prevention and legitimate

transmission in Section 6.4. A side information indicator $\mathbf{I}$ is adopted to indicate the M selected subcarriers as follows

$$I(k) = \begin{cases} 1, & selected \\ 0, & otherwise \end{cases}, \quad k = 0, 1, \cdots, N-1. \tag{6.7}$$

If the transmitter claims that the kth subcarrier is included in the interleaving, we have $I(k) = 1$; otherwise, $I(k) = 0$.

6.3.2 Subcarrier Interleaving

Following the subcarrier selection, the M collected subcarriers are interleaved according to the descending order of their channel gains observed at the transmitter. The order of the M subcarriers can be expressed as

$$\left|\hat{H}_T(0)_k\right|^2 \geq \cdots \geq \left|\hat{H}_T(\iota)_k\right|^2 \geq \cdots \geq \left|\hat{H}_T(M-1)_k\right|^2. \tag{6.8}$$

Without further indication, indices k and ι will be included in the subcarrier specification, where k denotes the exact position of the subcarrier among the N subcarriers and ι represents the descending order of the subcarrier sorted according to the channel gains of the M selected subcarriers.

6.3.3 Sharing of the Side Information I

Essentially, no signalling for the subcarrier selection indicator $\mathbf{I}$ and the subcarrier interleaving permutation between the legitimate parties is expected in the proposed system. Owing to channel reciprocity, the legitimate receiver should be able to figure out the interleaving permutation as well as the indicator $\mathbf{I}$ based on its own channel estimate $\hat{\mathbf{H}}_{\mathbf{R}}$, and then de-interleave the M interleaved subcarriers accordingly. Alternatively, the side information indicator $\mathbf{I}$ can also be sent out along with the data by the transmitter. The "$\mathbf{I}$ hiding" scheme can avoid a leak of any side information

to eavesdroppers but may reduce the reliability of the legitimate transmission since a mismatched **I** derivation may occur due to the asymmetric CSI observations. In contrast, the "**I** sharing" scheme can improve the transmission reliability between legitimate participants, but faces a potential threat that an eavesdropper may intercept **I** that is transmitted in radio channels.

It will be proved in Section 6.4 that the subcarrier interleaving permutation dominates the eavesdropping prevention capability, rather than the side information **I**. Even if an eavesdropper has by "chance" intercepted the subcarrier selection indicator, eavesdropping is still difficult due to the rapid spatial decorrelation and temporal variation of radio channels. Therefore, in the proposed secure OFDM system, the transmitter is allowed to send the subcarrier selection indicator **I** to the intended receiver to improve the legitimate transmission reliability.

6.4 Performance Evaluation

In this section, the performance of eavesdropping prevention achieved by the CSI-based dynamic subcarrier interleaving, as well as the reliability of legitimate transmission under noisy channel observations, is investigated. The probabilities of deriving an identical interleaving permutation and demodulated symbol error rates at both the eavesdropper and legitimate receiver are evaluated in the performance analysis.

6.4.1 Performance of Eavesdropping Prevention

In the proposed OFDM system, M out of the N subcarriers of each OFDM signal are selected and interleaved. Two scenarios have to be taken into consideration in the evaluation: eavesdroppers with, and without, the side information **I**.

6.4.1.1 Probability of Identical Interleaving Permutation at the Eavesdropper's End

The radio channels decorrelate rapidly in space, particularly in typical wireless scenarios with rich scattering conditions. Under the assumption that the common channel $\mathbf{H}$ and the eavesdropping channel $\mathbf{H_E}$ are independent, the estimated frequency domain channel responses at the transmitter and the eavesdropper, $\hat{\mathbf{H}}_\mathbf{T}$ and $\hat{\mathbf{H}}_\mathbf{E}$ respectively, as well as their channel gains $\left|\hat{\mathbf{H}}_\mathbf{T}\right|^2$ and $\left|\hat{\mathbf{H}}_\mathbf{E}\right|^2$, should be statistically independent. Furthermore, the orders of the channel gains among the total N subcarriers or any subset of the N subcarriers are also statistically independent. Consequently, an eavesdropper has no more information than a random guess about the interleaving scheme. Throughout this chapter, it is assumed that the eavesdropper attempts to derive the subcarrier interleaving scheme based on its own channel state estimate of the eavesdropping channel. Note that the interleaving pattern developed from the channel gain order of an uncorrelated channel can also be taken as a random guess of the interleaving scheme employed at the transmitter.

Under the scenario that the subcarrier selection indicator $\mathbf{I}$ is available to the eavesdropper, the eavesdropper only needs to guess the subcarrier interleaving permutation. For the M selected subcarriers, there are in total $M!$ potential permutations. Therefore, the probability that an eavesdropper derives an interleaving pattern identical to that developed by the transmitter, P_{E_M}, is

$$P_{E_M} = \frac{1}{M!}. \tag{6.9}$$

In the situation where the eavesdropper has no information about $\mathbf{I}$, in addition to determining the interleaving permutation, the eavesdropper has also to guess which M out of the N subcarriers are interleaved for each OFDM signal with a success probability $1/\binom{N}{M}$. In this case, the probability to derive the interleaving pattern

utilized by the transmitter, $P_{E_{NM}}$, is

$$\begin{aligned} P_{E_{NM}} &= \frac{1}{\binom{N}{M}} \frac{1}{M!} \\ &= \frac{(N-M)!}{N!}. \end{aligned} \tag{6.10}$$

Although $P_{E_{NM}}$ is smaller than P_{E_M} when $M \neq N$, it can be observed that P_{E_M} can already reach a negligible value even though M is small. For instance, when $M = 8$, P_{E_M} can be as low as 2.5×10^{-5}. As a result, an interception of the subcarrier selection indicator $\mathbf{I}$ at the eavesdropper will not menace the eavesdropping prevention capability of the proposed system, owing to the security achievement obtained from the interleaving permutation. Therefore, the indicator $\mathbf{I}$ can be sent out by the transmitter to improve the reliability of legitimate transmissions in the proposed OFDM system, as introduced in Section 6.3.

6.4.1.2 Symbol Error Rate at the Eavesdropper

Let P_S denote the SER of the conventional OFDM system using a certain modulation scheme in a Rayleigh fading channel. The SER of eavesdropping under the same channel condition when legitimate users adopt the proposed eavesdropping-resilient OFDM system, $P_{S,E}$, can be evaluated as

$$P_{S,E} = 1 - P_{E_{M/NM}} \left(1 - P_S\right). \tag{6.11}$$

6.4.2 Performance of Legitimate Transmission

6.4.2.1 Probability of Identical Interleaving Permutation at the Legitimate Receiver

Ideally, the legitimate receiver could derive the same subcarrier selection indicator $\mathbf{I}$ and interleaving permutation as that used at the transmitter due to channel reciprocity. As a result, the performance of legitimate transmission should be identical

to that of the conventional OFDM system. In practice, however, channel reciprocity is susceptible to the noise, interference and hardware limitations, which would lead to an estimation deviation at the channel estimator. The performance of legitimate transmission thus needs to be evaluated under a more practical assumption: imperfect channel reciprocity. Since the instantaneous subcarrier selection indicator $\mathbf{I}$ is sent to the intended receiver by the transmitter, instead of being purely developed by the receiver in the proposed system, we suppose that no errors are made about $\mathbf{I}$ at the legitimate receiver in the following analysis. In other words, it is assumed that the imperfect channel reciprocity can only cause a misunderstanding of the interleaving permutation at the legitimate receiver.

In order to study the probability that the transmitter and the legitimate receiver derive an identical interleaving permutation based on their CSI observations of the common channel, we first investigate the correlation between their observed frequency domain channel responses. Substituting (6.3) into (6.4), the channel estimate at the legitimate receiver can be rewritten as

$$\begin{aligned} \hat{H}_R(k) &= \hat{H}_T(k) - \Delta H_T(k) + \Delta H_R(k) \\ &= \hat{H}_T(k) + \Delta H_{TR}(k), \quad k = 0, 1, \cdots, N-1, \end{aligned} \tag{6.12}$$

where $\Delta H_{TR}(k) = -\Delta H_T(k) + \Delta H_R(k)$ is the composed channel estimation error of the transmitter/receiver and receiver/transmitter transmission links. Since the two terminals of a communication link generally experience independent interference and noise, the estimation errors at the transmitter and the receiver, i.e. $\Delta H_T(k)$ and $\Delta H_R(k)$ respectively, can be taken as independent. Consequently, the composed channel estimation error $\Delta H_{TR}(k)$ can be modeled as a zero mean complex Gaussian variable as

$$\Delta H_{TR}(k) \sim CN\left(0, \sigma_T^2 + \sigma_R^2\right). \tag{6.13}$$

In the proposed eavesdropping-resilient OFDM system, the legitimate receiver

seeks to derive the interleaving pattern that is dynamically designed based on the estimate $\hat{\mathbf{H}}_{\mathbf{T}}$ at the transmitter. As shown in (6.12), the observation $\hat{\mathbf{H}}_{\mathbf{R}}$ at the legitimate receiver can be considered as a noisy version of $\hat{\mathbf{H}}_{\mathbf{T}}$. Therefore, $\hat{\mathbf{H}}_{\mathbf{R}}$ can be modeled as a complex Gaussian random variable with the mean of $\hat{\mathbf{H}}_{\mathbf{T}}$ and a variance equal to $\sigma_{TR}^2 = \sigma_T^2 + \sigma_R^2$. The channel gain $\hat{\lambda}_{Rk} = \left|\hat{H}_R(k)\right|^2$ is then noncentral Chi-square distributed with 2 degree of freedom, with a probability density function

$$f_{Rk}\left(\hat{\lambda}_{Rk}\right) = \frac{1}{\sigma_{TR}^2} e^{-\left(\frac{\left|\hat{H}_T(k)\right|^2 + \hat{\lambda}_{Rk}}{\sigma_{TR}^2}\right)} I_0\left(\frac{\sqrt{\hat{\lambda}_{Rk}\left|\hat{H}_T(k)\right|^2}}{2\sigma_{TR}^2}\right), \tag{6.14}$$

and a cumulative distribution function

$$F_{Rk}\left(\hat{\lambda}_{Rk}\right) = 1 - Q_1\left(\frac{\sqrt{2}\left|\hat{H}_T(k)\right|}{\sigma_{TR}}, \frac{\sqrt{2\hat{\lambda}_{Rk}}}{\sigma_{TR}}\right), \tag{6.15}$$

where $I_\theta(x)$ represents the θth order Bessel function as

$$I_\theta(x) = \sum_{k=0}^{\infty} \frac{(x/2)^{\theta+2k}}{k!\Gamma(\theta+k+1)}, \tag{6.16}$$

and $Q_\theta(a,b)$ denotes the Marcum Q-function, that is

$$Q_\theta(a,b) = \int_b^\infty x\left(\frac{x}{a}\right)^{\theta-1} e^{-\frac{x^2+a^2}{2}} I_{\theta-1}(ax)\,dx. \tag{6.17}$$

Let Φ_T denote the event that $\left|\hat{H}_T(0)_k\right|^2 \geq \cdots \geq \left|\hat{H}_T(\iota)_k\right|^2 \geq \cdots \geq \left|\hat{H}_T(M-1)_k\right|^2$ and Φ_R denote the event that $\left|\hat{H}_R(0)_k\right|^2 \geq \cdots \geq \left|\hat{H}_R(\iota)_k\right|^2 \geq \cdots \geq \left|\hat{H}_R(M-1)_k\right|^2$. The probability that the legitimate receiver derives the same interleaving permutation based on the channel estimate $\hat{\mathbf{H}}_{\mathbf{R}}$, P_L, can be described as

$$P_L = P(\Phi_R|\Phi_T) = \frac{P(\Phi_R \cap \Phi_T)}{P(\Phi_T)}. \tag{6.18}$$

The M subcarrier channel gains of the common channel observed at the transmitter, $\hat{\lambda}_{Tk}$ for $k = 0, 1, \cdots, M-1$, are independent and identically distributed exponential random variables with parameter $\sigma^2_{\hat{H}_T}$. Referring to the order statistics theory [121], $P(\Phi_T)$ can be calculated as

$$\begin{aligned} P(\Phi_T) &= \int_{-\infty}^{+\infty} \int_{\hat{\lambda}_{T0}}^{+\infty} \int_{\hat{\lambda}_{T1}}^{+\infty} \cdots \int_{\hat{\lambda}_{T(M-2)}}^{+\infty} \\ &\quad f\left(\hat{\lambda}_{T0}, \cdots, \hat{\lambda}_{T(M-1)}\right) d\hat{\lambda}_{T0} d\hat{\lambda}_{T1} \cdots d\hat{\lambda}_{T(M-1)}, \end{aligned} \tag{6.19}$$

where $f\left(\hat{\lambda}_{T0}, \cdots, \hat{\lambda}_{T(M-1)}\right)$ is the joint PDF of the M subcarrier channel gains observed at the transmitter. Since $\hat{H}_T(k)$ follows a complex Gaussian distribution $CN\left(0, \sigma^2_{\hat{H}_T}\right)$, the channel gain of an estimated subcarrier channel, $\hat{\lambda}_{Tk} = \left|\hat{H}_T(k)\right|^2$, is exponentially distributed, with a PDF $f\left(\hat{\lambda}_{Tk}\right) = \frac{1}{\sigma^2_{\hat{H}_T}} e^{-\hat{\lambda}_{Tk}/\sigma^2_{\hat{H}_T}}$ and a CDF $F\left(\hat{\lambda}_{Tk}\right) = 1 - e^{-\hat{\lambda}_{Tk}/\sigma^2_{\hat{H}_T}}$. Meanwhile, considering that all the subcarriers are independently distributed, we have

$$\begin{aligned} f\left(\hat{\lambda}_{T0}, \cdots, \hat{\lambda}_{T(M-1)}\right) &= \prod_{\iota=0}^{M-1} f\left(\hat{\lambda}_{T\iota}\right) \\ &= \left(\frac{1}{\sigma^2_{\hat{H}_T}}\right)^M e^{-\sum_{\iota=0}^{M-1} \hat{\lambda}_{T\iota}/\sigma^2_{\hat{H}_T}}. \end{aligned} \tag{6.20}$$

Then, $P(\Phi_T)$ in (6.19) can be integrated as follows:

$$\begin{aligned} P(\Phi_T) &= \int_{-\infty}^{+\infty} \int_{\hat{\lambda}_{T0}}^{+\infty} \int_{\hat{\lambda}_{T1}}^{+\infty} \cdots \int_{\hat{\lambda}_{T(M-2)}}^{+\infty} \\ &\quad f\left(\hat{\lambda}_{T0}, \cdots, \hat{\lambda}_{T(M-1)}\right) d\hat{\lambda}_{T0} d\hat{\lambda}_{T1} \cdots d\hat{\lambda}_{T(M-1)} \\ &= \int_{-\infty}^{+\infty} f(\hat{\lambda}_{T0}) d\hat{\lambda}_{T0} \int_{\hat{\lambda}_{T0}}^{+\infty} f(\hat{\lambda}_{T1}) d\hat{\lambda}_{T1} \cdots \\ &\quad \cdots \int_{\hat{\lambda}_{T(M-2)}}^{+\infty} f(\hat{\lambda}_{T(M-1)}) d\hat{\lambda}_{T(M-1)} \end{aligned}$$

$$
\begin{aligned}
&= \int_{-\infty}^{+\infty} f(\hat{\lambda}_{T(M-1)}) d\hat{\lambda}_{T(M-1)} \int_{-\infty}^{\hat{\lambda}_{T(M-1)}} f(\hat{\lambda}_{T(M-2)}) d\hat{\lambda}_{T(M-2)} \cdots \\
&\quad \cdots \int_{-\infty}^{\hat{\lambda}_{T2}} f(\hat{\lambda}_{T1}) d\hat{\lambda}_{T1} \int_{-\infty}^{\hat{\lambda}_{T1}} f(\hat{\lambda}_{T0}) d\hat{\lambda}_{T0} \\
&= \int_{-\infty}^{+\infty} f(\hat{\lambda}_{T(M-1)}) d\hat{\lambda}_{T(M-1)} \int_{-\infty}^{\hat{\lambda}_{T(M-1)}} f(\hat{\lambda}_{T(M-2)}) d\hat{\lambda}_{T(M-2)} \cdots \\
&\quad \cdots \int_{-\infty}^{\hat{\lambda}_{T3}} f(\hat{\lambda}_{T2}) d\hat{\lambda}_{T2} \int_{-\infty}^{\hat{\lambda}_{T2}} f(\hat{\lambda}_{T1}) F(\hat{\lambda}_{T1}) d\hat{\lambda}_{T1} \\
&= \int_{-\infty}^{+\infty} f(\hat{\lambda}_{T(M-1)}) d\hat{\lambda}_{T(M-1)} \int_{-\infty}^{\hat{\lambda}_{T(M-1)}} f(\hat{\lambda}_{T(M-2)}) d\hat{\lambda}_{T(M-2)} \cdots \\
&\quad \cdots \int_{-\infty}^{\hat{\lambda}_{T4}} f(\hat{\lambda}_{T3}) d\hat{\lambda}_{T3} \int_{-\infty}^{\hat{\lambda}_{T3}} f(\hat{\lambda}_{T2}) \frac{1}{2} F^2(\hat{\lambda}_{T2}) d\hat{\lambda}_{T2} \\
&= \int_{-\infty}^{+\infty} f(\hat{\lambda}_{T(M-1)}) d\hat{\lambda}_{T(M-1)} \int_{-\infty}^{\hat{\lambda}_{T(M-1)}} f(\hat{\lambda}_{T(M-2)}) d\hat{\lambda}_{T(M-2)} \cdots \\
&\quad \cdots \int_{-\infty}^{\hat{\lambda}_{T5}} f(\hat{\lambda}_{T4}) d\hat{\lambda}_{T4} \int_{-\infty}^{\hat{\lambda}_{T4}} f(\hat{\lambda}_{T3}) \frac{1}{3 \times 2} F^3(\hat{\lambda}_{T3}) d\hat{\lambda}_{T3}. \qquad (6.21)
\end{aligned}
$$

Following the pattern of this integral, we can finally obtain

$$
\begin{aligned}
P(\Phi_T) &= \int_{-\infty}^{+\infty} f(\hat{\lambda}_{T(M-1)}) \frac{1}{(M-1)!} F^{M-1}(\hat{\lambda}_{T(M-1)}) d\hat{\lambda}_{T(M-1)} \\
&= \int_{-\infty}^{+\infty} \frac{1}{(M-1)!} F^{M-1}(\hat{\lambda}_{T(M-1)}) dF(\hat{\lambda}_{T(M-1)}) \\
&= \frac{1}{M!} F^M(\hat{\lambda}_{T(M-1)}) \Big|_{-\infty}^{+\infty} = \frac{1}{M!}. \qquad (6.22)
\end{aligned}
$$

Similarly, the probability $P(\Phi_R \cap \Phi_T)$ can also be derived based on the order statistics theory result as

$$
\begin{aligned}
P(\Phi_R \cap \Phi_T) &= \int_{-\infty}^{+\infty} \int_{\hat{\lambda}_{T0}}^{+\infty} \cdots \int_{\hat{\lambda}_{T(M-2)}}^{+\infty} f\left(\hat{\lambda}_{T0}, \cdots, \hat{\lambda}_{T(M-1)}\right) \\
&\quad \left\{ \int_{-\infty}^{+\infty} \int_{\hat{\lambda}_{R0}}^{+\infty} \cdots \int_{\hat{\lambda}_{R(M-2)}}^{+\infty} f\left(\hat{\lambda}_{R0}, \cdots, \hat{\lambda}_{R(M-1)}\right) \right. \\
&\quad \left. d\hat{\lambda}_{R0} d\hat{\lambda}_{R1} \cdots d\hat{\lambda}_{R(M-1)} \right\} d\hat{\lambda}_{T0} d\hat{\lambda}_{T1} \cdots d\hat{\lambda}_{T(M-1)}, \qquad (6.23)
\end{aligned}
$$

where $f\left(\hat{\lambda}_{R0},\cdots,\hat{\lambda}_{R(M-1)}\right)$ denotes the joint PDF for the M subcarrier channel gains observed at the legitimate receiver. Because the channel gains of the subcarriers are independent, this joint PDF can be expressed as

$$f\left(\hat{\lambda}_{R0},\cdots,\hat{\lambda}_{R(M-1)}\right)=\prod_{\iota=0}^{M-1}f_{R\iota}\left(\hat{\lambda}_{R\iota}\right). \tag{6.24}$$

Therefore, (6.23) can be rewritten as

$$\begin{aligned}P(\Phi_R\cap\Phi_T) &= \int_{-\infty}^{+\infty}\int_{\hat{\lambda}_{T0}}^{+\infty}\cdots\int_{\hat{\lambda}_{T(M-2)}}^{+\infty}f\left(\hat{\lambda}_{T0}\right)\cdots f\left(\hat{\lambda}_{T(M-1)}\right)\\ &\quad\left\{\int_{-\infty}^{+\infty}f_{R0}(\hat{\lambda}_{R0})d\hat{\lambda}_{R0}\int_{\hat{\lambda}_{R0}}^{+\infty}f_{R1}(\hat{\lambda}_{R1})d\hat{\lambda}_{R1}\cdots\right.\\ &\quad\left.\cdots\int_{\hat{\lambda}_{R(M-2)}}^{+\infty}f_{R(M-1)}(\hat{\lambda}_{R(M-1)})d\hat{\lambda}_{R(M-1)}\right\}\\ &\quad d\hat{\lambda}_{T0}d\hat{\lambda}_{T1}\cdots d\hat{\lambda}_{T(M-1)}.\end{aligned} \tag{6.25}$$

Unfortunately, the integration of (6.25) cannot be worked out analytically, and thus the probability of deriving an identical interleaving permutation at the legitimate user, P_L, cannot be expressed in a closed form. Therefore, in this study, the probability P_L will be evaluated and compared with P_{E_M} and $P_{E_{NM}}$ through computer simulations.

6.4.2.2 Symbol Error Rate at the Legitimate Receiver

Similar to the SER analysis for the eavesdropper, the SER at the legitimate receiver of the proposed OFDM system can be described as

$$P_{S,L}=1-P_L\left(1-P_S\right). \tag{6.26}$$

6.5 Interleaved Subcarrier Selection Algorithm

It can be concluded from the performance evaluation that the selection of interleaved subcarriers impacts both eavesdropping prevention and legitimate transmission in the presence of imperfect channel reciprocity. A combination of M subcarriers, which can make the interleaving pattern unrecognizable to eavesdroppers while being robust to the deviation of channel estimations between the legitimate participants, needs to be collected. In the selection of the M interleaved subcarriers, a trade-off between the eavesdropping resilience and the legitimate transmission reliability can be realized by answering two questions: 1) How many subcarriers have to be interleaved? 2) Which M out of the N subcarriers should be selected?

6.5.1 Size M of the Set of Interleaved Subcarriers

Referring to the analysis in Section 6.4, the probability that an eavesdropper successfully derives the actual interleaving permutation used by the transmitter is uniquely determined by the size, M, of the set of selected and interleaved subcarriers, as shown in (6.9) and (6.10). A system which can successfully defend against eavesdropping when the side information $\mathbf{I}$ has been intercepted by eavesdroppers, should also work well when $\mathbf{I}$ is not available to eavesdroppers. Therefore, the minimum requirement of M, M_{min}, can be determined from P_{E_M}. Given the constraint of P_{E_M} in preventing eavesdropping, Ω, M_{min} can be decided by conducting the inverse factorial of $1/\Omega$. Mathematically, the derivation of M_{min} can be represented as

$$M_{min} = \left\lceil F_{IF}\left(\frac{1}{\Omega}\right)\right\rceil, \tag{6.27}$$

where $F_{IF}(\cdot)$ denotes the inverse factorial function and $\lceil\cdot\rceil$ is the ceiling function. As a result, we have $(1/M_{min}!) \leq \Omega$. For instance, for Ω constraints $[0.0001, 0.001, 0.01]$, M_{min} would be $[8, 7, 5]$, respectively.

6.5.2 Location of the M Subcarriers

The minimum amount of interleaved subcarriers is determined according to a given requirement of eavesdropping prevention. Meanwhile, the location of the M subcarriers needs to be selected to mitigate the impairment of imperfect channel reciprocity on the derivation of the subcarrier interleaving permutation at the intended receiver. In the proposed subcarrier interleaving scheme, the selected subcarriers are interleaved according to the sorted order of their channel gains. Subcarriers having large channel gain intervals between them can thus provide an interleaving permutation insensitive to distortions caused by interference, noise, etc.

Assume that subcarrier i and subcarrier j observed at the transmitter have channel gains $\left|\hat{H}_T(i)\right|^2$ and $\left|\hat{H}_T(j)\right|^2$, respectively, where $\left|\hat{H}_T(i)\right|^2 \geq \left|\hat{H}_T(j)\right|^2$. The order mismatch probability of these two subcarriers at the legitimate receiver, using the noisy channel estimates, can be expressed as

$$\begin{aligned} P_e &= P\left\{\left|\hat{H}_R(i)\right|^2 < \left|\hat{H}_R(j)\right|^2\right\} \\ &= P\left\{\left|\hat{H}_R(i)\right|^2 - \left|\hat{H}_R(j)\right|^2 < 0\right\}. \end{aligned} \tag{6.28}$$

Based on the statistic theory result about the difference of two independent noncentral Chi-Square random variables with 2 degree of freedom [122], the order mismatch probability P_e can be calculated as

$$\begin{aligned} P_e &= Q_1\left(\frac{\sqrt{2}\left|\hat{H}_T(j)\right|}{\sigma_{TR}}, \frac{\sqrt{2}\left|\hat{H}_T(i)\right|}{\sigma_{TR}}\right) \\ &\quad -\frac{1}{2}e^{\left[-\frac{|\hat{H}_T(i)|^2+|\hat{H}_T(j)|^2}{\sigma_{TR}^2}\right]} I_0\left(\frac{2\left|\hat{H}_T(i)\right|\left|\hat{H}_T(j)\right|}{\sigma_{TR}^2}\right), \end{aligned} \tag{6.29}$$

where $Q_1(\cdot,\cdot)$ is the first-order Marcum Q-function, $I_0(\cdot)$ represents the 0th-order Bessel function. Let D denote the observed channel gain interval between subcarriers

i and j at the transmitter, i.e. $\left|\hat{H}_T(i)\right|^2 = \left|\hat{H}_T(j)\right|^2 + D$, equation (6.29) can be rewritten as

$$\begin{aligned} P_e &= Q_1\left(\frac{\sqrt{2}\sqrt{\left|\hat{H}_T(i)\right|^2 - D}}{\sigma_{TR}}, \frac{\sqrt{2}\left|\hat{H}_T(i)\right|}{\sigma_{TR}}\right) \\ &\quad -\frac{1}{2}e^{\left[-\frac{2|\hat{H}_T(i)|^2 - D}{\sigma_{TR}^2}\right]} I_0\left(\frac{2\left|\hat{H}_T(i)\right|\sqrt{\left|\hat{H}_T(i)\right|^2 - D}}{\sigma_{TR}^2}\right). \end{aligned} \tag{6.30}$$

Obviously, the order mismatch probability P_e is determined by the channel gain $\left|\hat{H}_T(i)\right|^2$, the channel gain difference D, as well as the noise power σ_{TR}^2.

Given a limitation for the order mismatch probability of two adjacent interleaved subcarriers, denoted by Λ , the required channel gain interval between two adjacent interleaved subcarriers under a certain channel condition can be determined from the inversion of (6.30), which can then be utilized as a criterion to choose the interleaved subcarriers. Unfortunately, D cannot be evaluated in a closed form from (6.30), and thus numerical techniques, or an approximation, has to be used. In this study, a look-up table for D under different channel conditions with various order mismatch probabilities P_e, is generated by simulations. Part of the look-up table for $P_e = 0.01$ is shown in Table 6.1.

6.5.3 Summary of the Interleaved Subcarrier Selection Algorithm

In the proposed eavesdropping-resilient OFDM system, interleaved subcarriers are selected based on the constraints of P_{E_M} and P_e, i.e. Ω and Λ, respectively. Ω determines the minimum number of interleaved subcarriers, while Λ determines which subcarriers can be interleaved. It is noteworthy that when we select the location of the interleaved subcarriers using Λ, the size of the set of qualified subcarriers, M,

Table 6.1: Look-up table for interleaved subcarrier selection

$\left\lvert \hat{H}_T(j) \right\rvert^2$	$10\log_{10}\left(1/\sigma_{TR}^2\right)$ dB															
	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37
0.02	0.040	0.030	0.025	0.020	0.015	0.010	0.010	0.010	0.005	0.005	0.005	0.005	0.005	0.005	0.005	0.005
0.04	0.080	0.060	0.045	0.035	0.030	0.020	0.020	0.015	0.010	0.010	0.010	0.005	0.005	0.005	0.005	0.005
0.06	0.120	0.090	0.070	0.055	0.040	0.030	0.025	0.020	0.015	0.015	0.010	0.010	0.010	0.005	0.005	0.005
0.08	0.160	0.120	0.090	0.070	0.055	0.040	0.035	0.025	0.020	0.015	0.015	0.010	0.010	0.010	0.005	0.005
0.10	0.200	0.150	0.115	0.085	0.065	0.050	0.040	0.030	0.025	0.020	0.015	0.015	0.010	0.010	0.010	0.005
0.12	0.240	0.180	0.135	0.105	0.080	0.060	0.050	0.040	0.030	0.025	0.020	0.015	0.015	0.010	0.010	0.010
0.14	0.280	0.210	0.155	0.120	0.090	0.070	0.055	0.045	0.035	0.030	0.025	0.020	0.015	0.010	0.010	0.010
0.16	0.320	0.235	0.180	0.135	0.105	0.080	0.065	0.050	0.040	0.030	0.025	0.020	0.015	0.015	0.010	0.010
0.18	0.355	0.265	0.200	0.155	0.115	0.090	0.070	0.055	0.045	0.035	0.030	0.025	0.020	0.015	0.010	0.010
0.20	0.395	0.280	0.225	0.170	0.130	0.100	0.080	0.060	0.050	0.040	0.030	0.025	0.020	0.015	0.015	0.010
0.40	-	-	0.445	0.335	0.260	0.200	0.155	0.120	0.095	0.075	0.060	0.050	0.040	0.030	0.025	0.020
0.60	-	-	-	-	0.385	0.300	0.230	0.180	0.140	0.110	0.090	0.070	0.055	0.045	0.035	0.030
0.80	-	-	-	-	-	0.395	0.305	0.240	0.190	0.150	0.115	0.095	0.075	0.060	0.045	0.040
1.00		-	-	-	-	0.495	0.385	0.300	0.235	0.185	0.145	0.115	0.090	0.075	0.060	0.045
1.20	-	-	-	-	-	-	0.460	0.360	0.280	0.220	0.175	0.140	0.110	0.085	0.070	0.055
1.40	-	-	-	-	-	-	-	0.420	0.325	0.255	0.205	0.160	0.125	0.100	0.080	0.065
1.60	-	-	-	-	-	-	-	0.475	0.375	0.295	0.230	0.185	0.145	0.115	0.090	0.075
1.80	-	-	-	-	-	-	-	-	0.420	0.330	0.260	0.205	0.160	0.130	0.100	0.080
2.00	-	-	-	-	-	-	-	-	0.465	0.365	0.290	0.230	0.180	0.145	0.115	0.090

may be either larger or smaller than M_{min}, depending on the channel conditions. As an eavesdropping-resilient system, it should ensure the capability to defend against eavesdropping first, and then endeavour to mitigate the side-effect on the legitimate transmission. Therefore, the subcarrier selection should give top priority to the M_{min} requirement. In the situation where $M < M_{min}$, the requirement of P_e can be relaxed to include more subcarriers in the interleaving. When $M > M_{min}$, all the M subcarriers can be selected and interleaved to further improve the eavesdropping prevention capability.

The proposed subcarrier selection algorithm can be summarized as follows:

1. The minimum number of subcarriers that need to be interleaved is decided by Ω;

2. All the N subcarriers of an OFDM signal are descendingly ordered according to their channel gains observed at the transmitter;

3. The subcarrier having the largest channel gain is selected first;

4. With the channel gain of the previously selected subcarrier, the estimated noise power and the $P_e \leq \Lambda$ requirement, the channel gain distance between the previously selected subcarrier and the next subcarrier, D, can be updated by referring to the look-up table such as Table 6.1;

5. The subcarrier, which has a channel gain at least D smaller than that of the previously selected subcarrier and at the same time is closest to the previously selected subcarrier among all the qualified subcarriers, is selected;

6. Steps 4 and 5 are repeated until reaching the end of the order for the N subcarriers. Then M out of the N subcarriers have been selected out;

7. If $M \geq M_{min}$, the subcarrier selection is completed; otherwise, one has to relax the requirement of P_e, and then repeat steps 4 and 5 until $M \geq M_{min}$ can be achieved.

6.6 Simulation Results

Simulations are carried out to validate the proposed eavesdropping-resilient OFDM system following the specifications of the IEEE 802.11g system. The OFDM signal is generated using 64-point IFFT with a cyclic prefix of length 16. The modulation scheme 4-QAM is adopted for all the subcarriers and the sampling frequency is 20 MHz. For the interleaved subcarrier selection, parameter Ω is set to 0.01, leading to $M_{min} = 5$. Meanwhile, parameter Λ is set to 0.01 and 0.001, respectively. Unless stated otherwise, the subcarrier selection indicator $\mathbf{I}$ is assumed to be known by the legitimate receiver as well as by the eavesdropper. In addition, a Rayleigh fading channel is considered in the simulations. Training symbols with unit energy at each subcarrier are sent out and exploited for the channel estimation, while least-square channel estimation technique is employed at all the nodes in the network. Consequently, the channel estimates can be expressed as

$$\begin{aligned} \hat{H}(k) &= \frac{Y(k)}{X(k)} = H(k) + \frac{W(k)}{X(k)} \\ &= H(k) + W'(k), \quad k = 0, 1, \cdots, N-1, \end{aligned} \tag{6.31}$$

where $W'(k)$ and $W(k)$ have the same statistical properties.

In order to make a fair comparison, it is assumed that the common channel and the eavesdropping channel follow an identical statistical model, and the noise level at all the nodes is the same as well. Perfect synchronization is also assumed at both the legitimate receiver and eavesdropper's end.

6.6.1 Security and Reliability of the CSI-based Subcarrier Interleaving Scheme

As the interleaving permutation mismatch probabilities at both the legitimate receiver and the eavesdropper, directly determine the security against eavesdropping and the reliability of legitimate transmission in the proposed system, they are evalu-

ated in this subsection. A Rayleigh fading channel with uniform power delay profile, with a delay spread as long as the CP length, i.e. 800 ns, for the 802.11g system, is used in the simulations. As shown in Fig. 6.3, the interleaving permutation mismatch probabilities at the eavesdropper are always close to 100% in the simulated channel conditions, whether $P_e = 0.01$ or $P_e = 0.001$. Accordingly, the information recovery by eavesdropping is severely disrupted, which makes the transmitted data unrecognizable to eavesdroppers. In contrast, the interleaving permutation mismatch probabilities at the legitimate user is negligible when the SNR is larger than 24 dB. In other words, the legitimate transmission of the proposed system would be as good as the conventional OFDM system in a high SNR range. Please note that the interleaving permutation mismatch between legitimate users is mainly caused by the channel estimation errors. Thus, a channel estimation technique inducing smaller estimation errors can further improve the reliability of the legitimate transmission.

6.6.2 Performance of the Proposed Secure OFDM System

In this subsection, SERs at the legitimate receiver and the eavesdropper are compared under different channel environments to validate the security of the proposed OFDM system against eavesdropping. Meanwhile, the SER of the conventional OFDM system is also provided as a bench-mark reference to evaluate the reliability of legitimate transmissions in the proposed system.

Figure 6.4 presents the SERs of the proposed and the conventional OFDM systems under a Rayleigh fading channel with uniform PDP of 800 ns delay spread. It can be observed from this figure that the eavesdropper always has a SER close to 100% when it strives to intercept signals transmitted from the proposed eavesdropping-resilient OFDM system. In contrast, the performance of the legitimate transmission can be as good as that of the conventional OFDM system in that simulated rich multipath environment.

A simultaneous evaluation of the eavesdropping resilience and transmission relia-

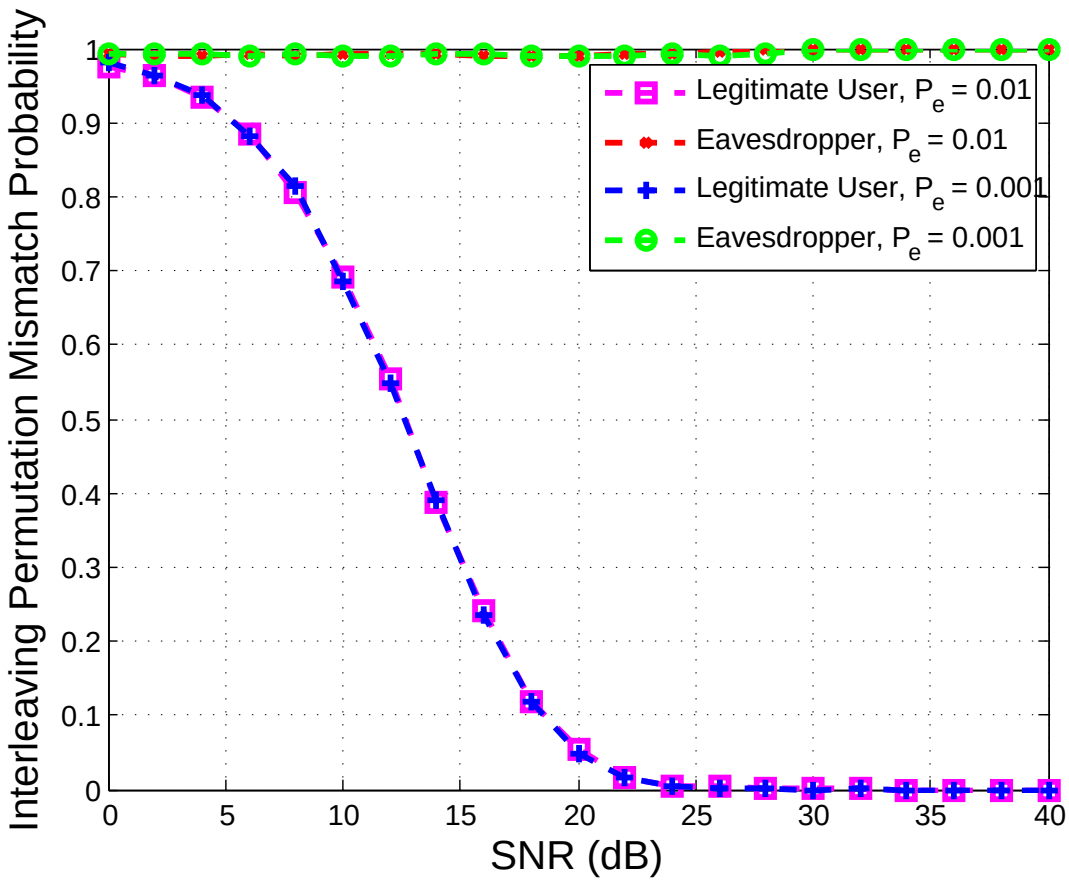


Figure 6.3: Interleaving permutation mismatch probabilities at the legitimate receiver and eavesdropper under a Rayleigh fading channel with uniform PDP of 800 ns delay.

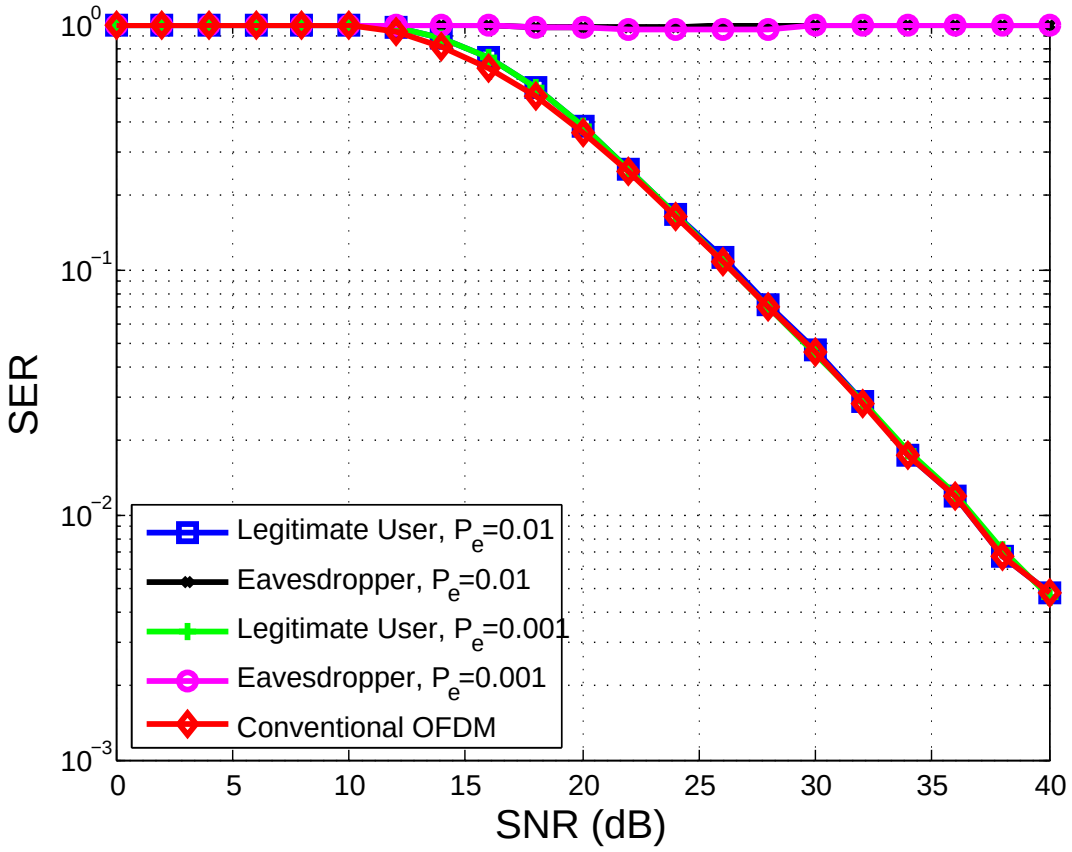


Figure 6.4: SERs at the legitimate receiver and eavesdropper under a Rayleigh fading channel with uniform PDP of 800 ns delay.

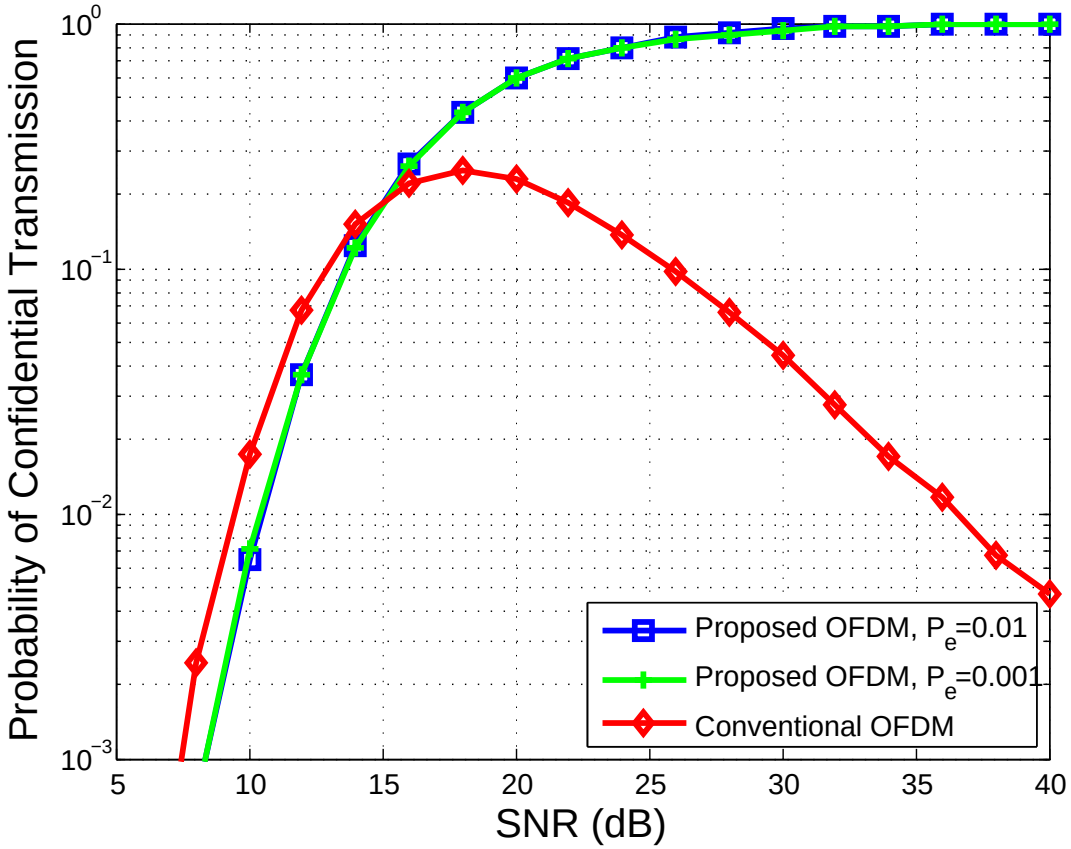


Figure 6.5: Comparison of confidential transmission probabilities between the proposed and conventional OFDM systems under a Rayleigh fading channel with uniform PDP of 800 ns delay.

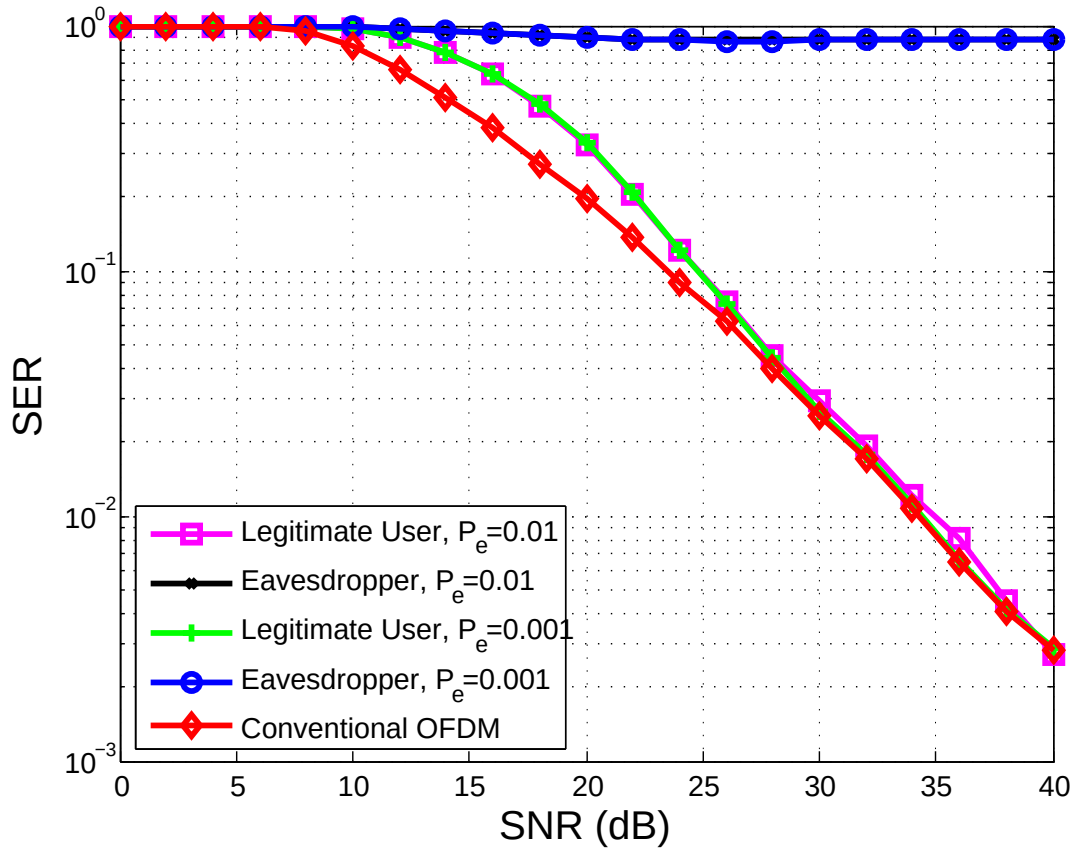


Figure 6.6: SERs at the legitimate receiver and eavesdropper under a Rayleigh fading channel with exponential PDP of 50 ns RMS delay.

bility of this eavesdropping-resilient OFDM system, in terms of our proposed evaluation criterion for anti-eavesdropping communication systems in Chapter 5, i.e. the probability of confidential transmission, is also performed. The novel evaluation criterion is defined as the probability that the transmitted data is correctly received by the legitimate receiver but not intercepted by the eavesdropper. In the proposed eavesdropping-resilient OFDM system, the probability of confidential transmission can be calculated as

$$\Pi = \left(1 - P_{S,L}\right) P_{S,E}. \tag{6.32}$$

As depicted in Fig. 6.5, the proposed OFDM system outperforms the conventional OFDM system, particularly in the high SNR range.

The SER vs. SNR performance of the proposed secure OFDM system under a different channel condition is depicted in Fig. 6.6, where a Rayleigh fading channel with exponential PDP of 50 ns RMS delay spread is considered. This represents a multipath channel with much less scattering in comparison with the one used before. As illustrated in this figure, the eavesdropper still suffers from a very high SER though the SER is a bit less than that observed in Fig. 6.4. Comparing the performance of the legitimate transmission with that of the conventional OFDM under the same channel condition, legitimate users of the proposed OFDM system would now experience a performance loss. However, the performance degradation becomes less significant when the SER is less than 0.1. In addition, by using a smaller value of P_e in the selection of the interleaved subcarriers, the legitimate receiver can obtain a lower SER, such that the SER gap between the proposed system and the conventional OFDM system can be reduced.

Comparing the performance results in Fig. 6.4 and Fig. 6.6, which are under different Rayleigh fading conditions, the performance degradation of the proposed eavesdropping-resilient OFDM system can be explained as follows: the reciprocity and spatial variation properties of time-varying wireless channels, which are exploited as the principle behind the proposed system, are more effective and reliable in rich multipath environments. Therefore, a rich scattering multipath environment is highly favorable to the proposed secure OFDM system.

6.6.3 Impact of the Side Information I on Eavesdropping Prevention

As discussed in Section 6.3, the subcarrier selection indicator **I** may, or may not, be available to the eavesdropper, depending on whether it is sent out by the transmitter. The impact of the side information **I** on the eavesdropping prevention is also studied in the simulations. SERs of eavesdroppers with and without the side information **I** are compared in Fig. 6.7 and Fig. 6.8 for Rayleigh fading channels with uniform PDP

of 800 ns delay spread and exponential PDP of 50 ns RMS delay spread, respectively. In the simulations, the eavesdropper estimates the subcarrier selection based on its own channel observations and the information of Ω and Λ, when the side information $\mathbf{I}$ is not available. It is noteworthy that this operation can be taken as a random guess of the indicator $\mathbf{I}$ since the common channel and the eavesdropping channel are uncorrelated.

In both simulated communication environments, the eavesdropper experiences a higher SER when the subcarrier selection indicator $\mathbf{I}$ is not available, compared to the case where $\mathbf{I}$ has been intercepted. However, as shown in the figures, the SERs of eavesdropping are all considerably high, even when eavesdroppers can intercept, by chance, the indicator $\mathbf{I}$. This is because the eavesdropping prevention capability is dominated by the interleaving permutation but not the side information $\mathbf{I}$ as such. The eavesdropper at a separate location observes an uncorrelated channel such that it is hard for the eavesdropper to derive an identical interleaving permutation, even though it knows exactly which subcarriers have been interleaved. As a result, information recovery for eavesdropping is severely affected, thus leading to high SERs. In addition, it can be observed from both Fig. 6.7 and Fig. 6.8 that there is a fluctuation in the eavesdropper's SNR values over the whole SNR range. The reason for this phenomenon is that the amount of interleaved subcarriers, M, varies in the subcarrier selection according to the channel conditions, and this parameter would directly affect the SER of eavesdropping as shown in (6.11). Moreover, the fluctuations of SERs are minor, particularly when the subcarrier selection indicator $\mathbf{I}$ has not been intercepted by the eavesdropper.

6.7 Summary

In this chapter, an eavesdropping-resilient OFDM system without any restriction of the utilized symbol modulation scheme is achieved through dynamic subcarrier interleaving. Exploiting the CSI between the transmitter and legitimate receiver,

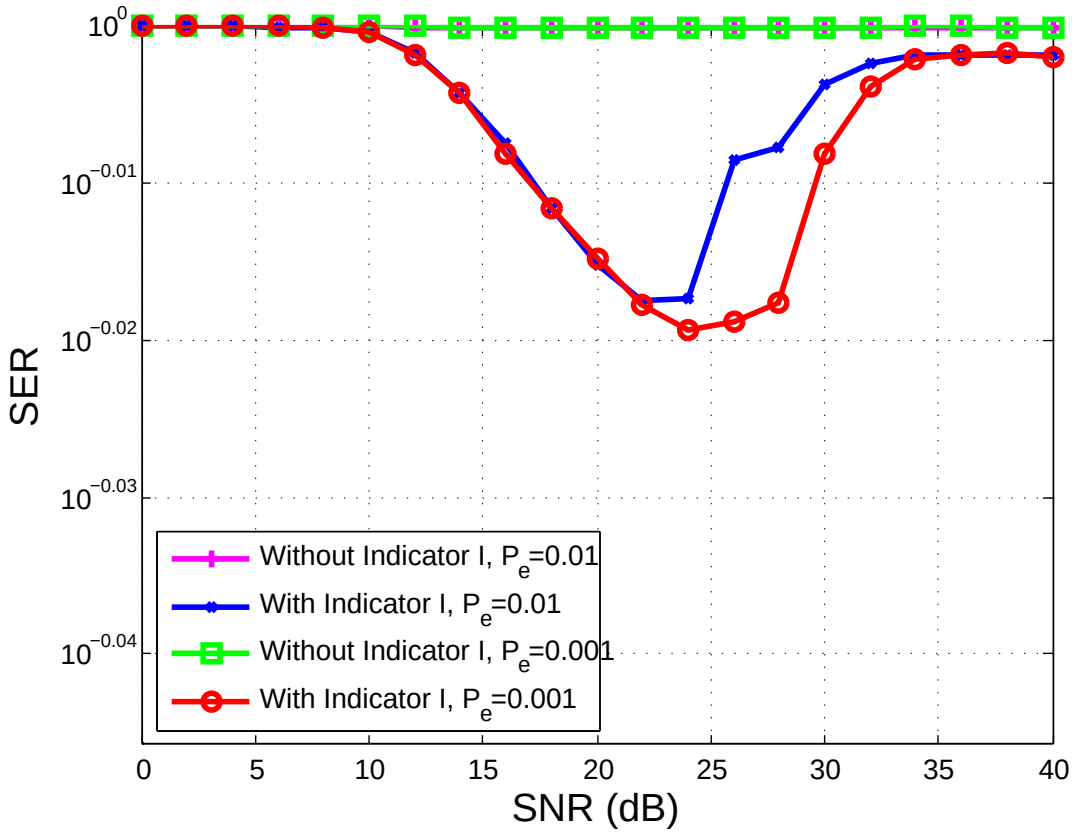


Figure 6.7: SER comparison for eavesdroppers with and without the subcarrier selection indicator under a Rayleigh fading channel with uniform PDP of 800 ns delay.

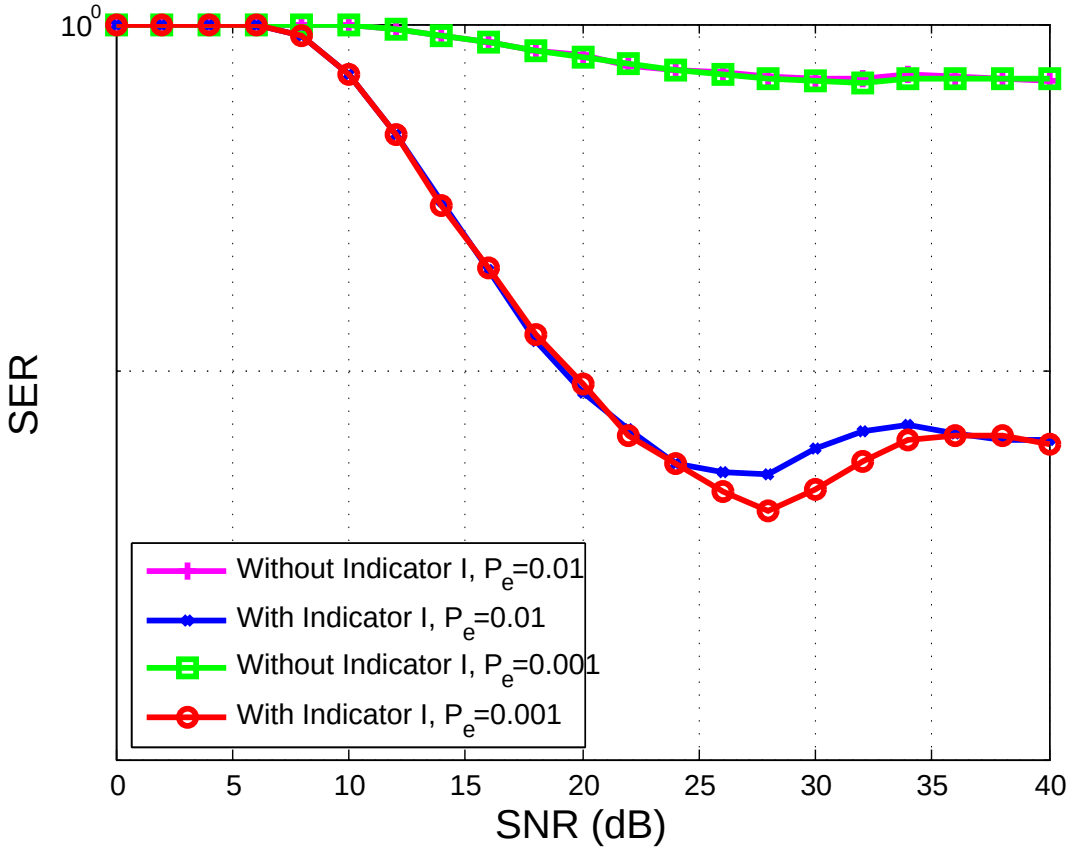


Figure 6.8: SER comparison for eavesdroppers with and without the subcarrier selection indicator under a Rayleigh fading channel with exponential PDP of 50 ns RMS delay.

partial subcarriers of each OFDM signal are selected and then interleaved according to the sorted order of their channel gains. Since wireless channels associated with each pair of users at separate locations exhibit independent fading processes, the frequently renewed subcarrier interleaving scheme can only be shared between legitimate nodes based on channel reciprocity. As a result, mismatched information recovery is carried out at the eavesdropper without an identical subcarrier interleaving pattern, so that eavesdropping is prevented. In order to mitigate the impairment from imperfect channel reciprocity between legitimate parties, the interleaved subcarriers are selected to achieve a trade-off between the eavesdropping resilience and legitimate transmission reliability. Theoretical analysis and computer simulation results have been provided to validate the proposed eavesdropping-resilient OFDM system. It is observed from the simulation results that eavesdropping on the proposed system suffers from SER values close to 100% while the legitimation transmission has a SER performance similar to that of conventional OFDM systems.

Chapter 7

Secure OFDM Systems with Embedded Confidential Signaling

Two nodes of a communication link would theoretically experience and observe the same channel fading due to channel reciprocity. Security design based on the randomness of the common channel can therefore be shared between legitimate terminals. In practical implementations, as channel estimates are generally distorted by noise, interference and hardware limitations, estimates at the two nodes of a wireless channel are not perfectly reciprocal though the channel is reciprocal inherently. The reliability of legitimate transmission will thus be impaired once misunderstanding of the channel based security design occurs at the legitimate receiver. Hence, solutions to mitigate the impact of imperfect channel reciprocity on the channel based security strategies need to be investigated, such as the inherent robustness improvement of the security algorithm and the transmission of insensitive side information relevant to the security design.

Techniques to enhance the inherent robustness of security designs to imperfect channel reciprocity have been studied in Chapter 5 and Chapter 6. In this chapter, an efficient side information transmission mechanism between the transmitter and legitimate receiver is provided, in order to assist the security design understanding at

the intended receiver and then strengthen the reliability of legitimate transmission. OFDM with precoded cyclic prefix (PCP-OFDM), which was originally proposed for the adaptive transmission in cognitive radio, is extended and specifically tailored for the confidential transmission of side information between legitimate users. In this design, the side information relevant to the security design is conveyed by a specially tailored PCP, and concurrently transmitted with the data-carrying OFDM symbol. A set of orthogonal sequences, which is only known by legitimate users, is one-to-one mapped to all the potential side information. An orthogonal sequence is chosen in the transmission of each OFDM symbol corresponding to the present security design. The PCP symbol is then generated by passing the selected orthogonal sequence through an OFDM modulator, so as to maintain the same time and frequency characteristics as the data-carrying OFDM symbol. With the inherent orthogonality among all the candidate PCPs, the information conveyed by the PCP symbol can be reliably detected through cross correlations between the received PCP and elements in the local PCP library of the receiver. The local candidate PCP that leads to the maximum correlation peak will be taken as the PCP sent out by the transmitter, and then used to assist the understanding of the adopted security design. Theoretical analysis and simulation results are provided to validate the proposed design.

7.1 Introduction

In secure wireless OFDM systems where transmitted OFDM signals are constructed according to the real-time status of the common channel, no signaling between the transmitter and legitimate receiver is needed ideally due to channel reciprocity. Practically, all the nodes in a network can only observe a noisy version of their undergoing channels because of estimation errors caused by the noise, interference and hardware limitations. Although the radio channel is reciprocal, estimates of the radio channel are not perfectly reciprocal. As a result, the real-time security design initiated at the transmitter and that locally derived at the legitimate receiver,

which are based on their individual estimates of the common channel, may not be identical. Data demodulation error is then caused by the misunderstanding of the security design. Consequently, the reliability of legitimate transmission is degraded.

As a superior secure communication system, it should effectively defend against malicious attacks but also maintain reliable legitimate transmission. It has been demonstrated in Chapter 6, the sharing of certain insensitive side information relevant to the security design, such as the subcarrier selection indicator $\mathbf{I}$ in the proposed eavesdropping-resilient OFDM system using dynamic subcarrier interleaving, can significantly enhance the reliability of legitimate transmission. On the other hand, even this type of side information happens to be intercepted by the eavesdropper during the transmission, the damage to the system security is ignorable. Therefore, the transmission of such side information between the transmitter and legitimate receiver can be performed, particularly in a hostile communication environment.

There are several challenges in sharing the side information relevant to the channel based security design in a wireless OFDM system:

- The transmission needs to be always available. Since the secure OFDM system is designed according to the real-time wireless channel, the relevant side information would be updated frequently, even symbol by symbol.

- The sharing of the side information should not interrupt or interfere the data transmission. The data transmission in a secure OFDM system would have a higher priority than the sharing of side information. As a result, we cannot stop data transmission to send the side information. Also, the transmission of the side information should minimize or even avoid the interference to the data transmission.

- The transmission cannot occupy additional time and spectrum resources. The time and spectrum resources are limited for wireless communications. The sharing of side information needs to be completed within the time and spectrum

resources allocated for the original data transmission in the OFDM system. No additional resource is available and can be provided.

- The transmission should be reliable and confidential. The shared side information is used to mitigate the impairment from the imperfect reciprocity of channel estimates between the transmitter and legitimate receiver, and then improve the reliability of legitimate transmission. Therefore, the transmission of the side information itself should be reliable. Moreover, although the leakage of such side information would only cause minor damage to the security of the system, we still need to keep this transmitter-receiver interaction as confidential as possible.

Several simultaneous communication strategies have been reported in the literature. In [123, 124], the inphase and quadrature branches of the signal constellation are used to carry different data that need to be transmitted concurrently. By doing this, the throughput of each data stream reduces compared to the scenario that one data stream occupies both I and Q branches of the signal constellation. Another concurrent transmission strategy is to make the two data streams orthogonal to each other and then mix them physically [125, 126], conditioned on a perfect orthogonality. Moreover, Zhao *et al.* proposed to enable simultaneous communications by using the multiple-input and multiple-output technology, at the cost of additional antennas [127].

In [18], a novel OFDM system with a precoded cyclic prefix, named PCP-OFDM, was proposed for fast transmitter-receiver interaction in adaptive transmission. In the original PCP-OFDM, the traditional cyclic prefix is replaced by two precoded Kasami sequences that convey system parameters related to the current adaptation scheme. Since the cyclic prefix is typically included in OFDM signals as a guard interval to eliminate the inter-symbol interference, no additional time and spectrum resources are required by the PCP signaling link. Moreover, the PCP caused ISI and inter-carrier interference (ICI) to the data-carrying OFDM symbol in a multipath

channel can be removed through a proposed interference cancellation algorithm. As a result, a reliable data transmission comparable to the traditional OFDM system can be achieved by the PCP-OFDM system.

This chapter extends the previous study on the PCP-OFDM system, and provides an embedded confidential signaling link for the transmission of security design relevant side information in secure OFDM systems. Technically, the side information relevant to the security design is conveyed by a specially tailored PCP, and concurrently transmitted with the data-carrying OFDM symbols. A set of orthogonal sequences, which is only known by legitimate users, is one-to-one mapped to all the potential information to be transmitted. An orthogonal sequence is chosen in the transmission of each OFDM symbol corresponding to the present security design. The PCP symbol is then generated by passing the selected orthogonal sequence through an OFDM modulator, so as to maintain the same time and frequency characteristics as the data-carrying OFDM symbol. With the inherent orthogonality among all the candidate PCPs, the information transmitted through the PCP signaling link can be reliably identified by cross correlations between the received PCP and elements in the local PCP library at the receiver. The local candidate PCP that leads to the maximum correlation peak will be taken as the PCP sent out by the transmitter, and then used to assist the understanding of the adopted security design. It can be found that the PCP enabled side information transmission mechanism does not interrupt the data transmission and requires no additional time and frequency resources.

The rest of this chapter is organized as follows. Section 7.2 introduces the transmitter and receiver design in the PCP-OFDM system. The PCP generation and detection for the embedded confidential signaling are addressed in Section 7.3, followed by the performance analysis of the PCP detection and PCP-OFDM demodulation in Section 7.4. Simulation results are provided in Section 7.5. At last, the chapter is summarized in Section 7.6.

7.2 Transmitter and Receiver Design for PCP-OFDM System

The block diagram of the PCP-OFDM system is illustrated in Fig. 7.1. The transmitter in Fig. 7.1(a) is basically the same as that in a traditional OFDM system, except that the cyclic prefix is now replaced by a precoded sequence. More specifically, the PCPs are generated from orthogonal sequences modulated by an OFDM modulator, corresponding to the real-time security design. Generation and detection of such PCPs will be discussed in Section 7.3. The PCPs are considered as known in this section.

7.2.1 Transmitter Design for PCP-OFDM System

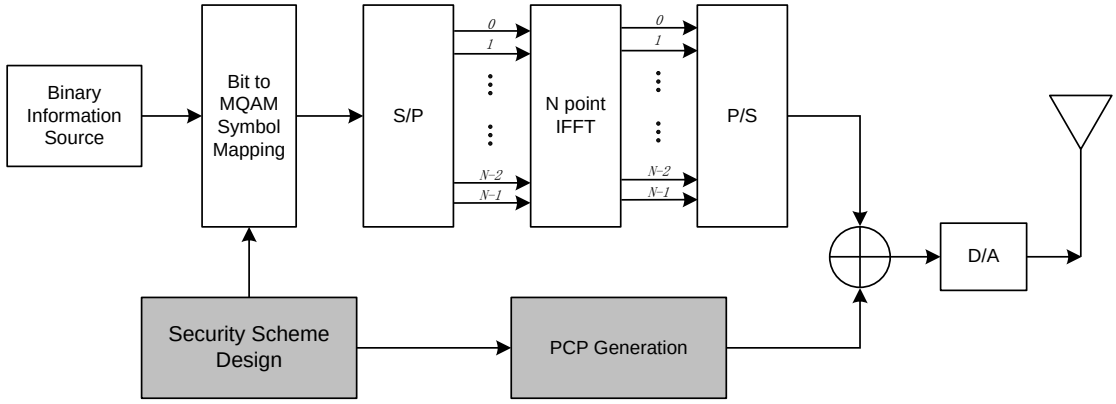
Each OFDM symbol in Fig. 7.1(a) is specified by an N-point time-domain vector $\mathbf{x}$ obtained via an inverse fast Fourier transform of the complex data vector $\mathbf{X}$ of size N. Without loss of generality, the data-carrying OFDM symbol in time domain can be expressed in vector form as

$$\mathbf{x} = \left(\mathbf{F}^N\right)^* \mathbf{X}, \tag{7.1}$$

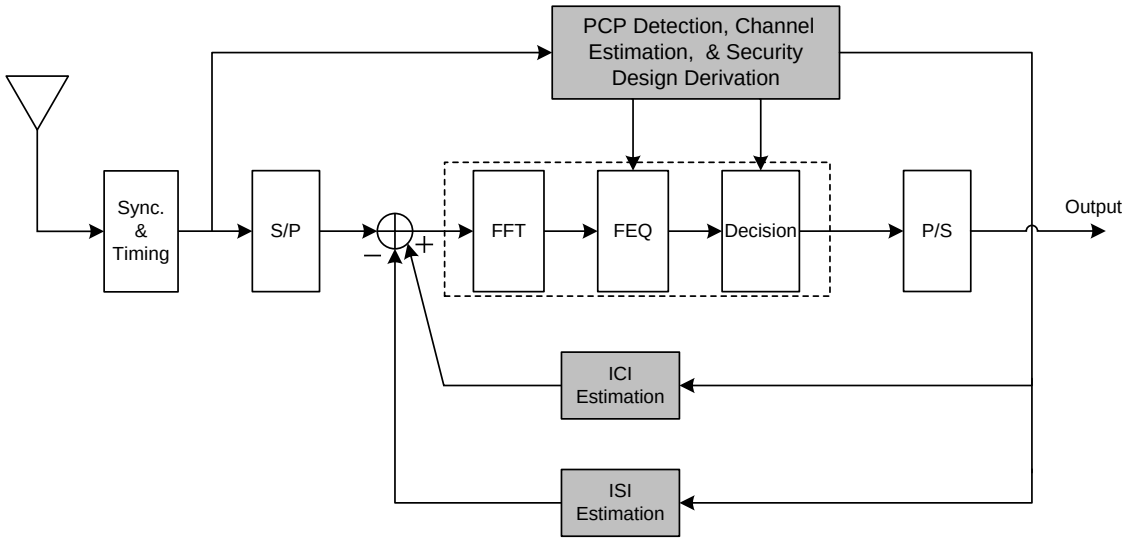
where $\mathbf{F}^N$ is the FFT transform matrix with its (n,k)th entry $(exp\{-j2\pi nk/N\}/\sqrt{N})$. Operator $(\cdot)^*$ denotes the conjugate transpose.

Before the transmission of the data-carrying OFDM symbol in (7.1), PCP sequence with length of N_{cp} is inserted as its prefix. Generation and demodulation of the PCP will be discussed in Section 7.3. Here we just need to take the PCP as a random sequence with the same time and frequency characteristics as the data-carrying OFDM symbol. With the purpose of a complete removal of ISI, the duration of PCP is set to be longer than or at least equal to the delay spread of the multipath channel. A generated PCP-OFDM signal after the PCP insertion can be written as

$$\mathbf{x_{pcp}} = \left[c_p\left(0\right),\ \cdots,\ c_p\left(N_{cp}-1\right),\ x\left(0\right),\ \cdots,\ x\left(N-1\right),\right], \tag{7.2}$$



a. Transmitter



b. Receiver

Figure 7.1: Block diagram of the PCP-OFDM system: (a) Transmitter, (b) Receiver.

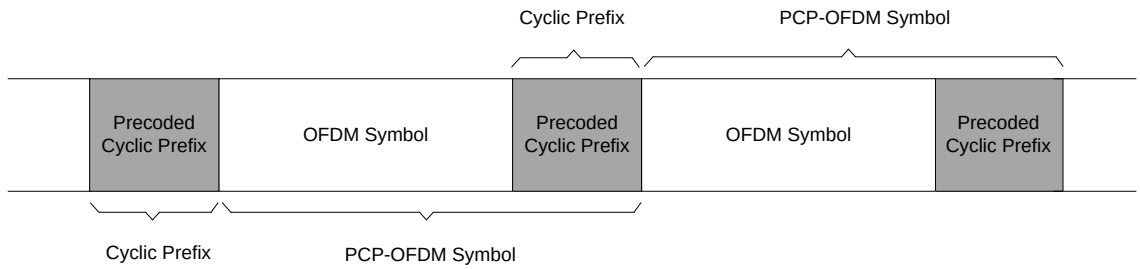


Figure 7.2: The structure of PCP-OFDM signals.

where $\mathbf{c}_p = [c_p(0), \cdots, c_p(N_{cp}-1)]$ denotes the generated PCP symbol.

When there is no change in the system security design, the information needs to be sent out through the PCP link is not renewed. Consequently, each data-carrying OFDM symbol is preceded and succeeded by the same PCP. This is equivalent of generating a new OFDM signal of $N + 2N_{cp}$ samples with one PCP sequence as its last N_{cp} samples and the other identical sequence as its cyclic prefix in the first N_{cp} samples, as illustrated in Fig. 7.2. Hence, it creates a series of new OFDM signals with cyclic structure similar to traditional OFDM signals protected by cyclic prefix.

In a more general scenario, the OFDM symbol is preceded and succeeded by two different PCPs, due to the variation of the wireless channel and corresponding security design. This also includes the scenario of zero vector as the second PCP, representing the end of the transmission. Therefore, the following signal vector $\mathbf{x}'$ can be used for the interference analysis and PCP-OFDM signal demodulation, that is

$$\begin{aligned}\mathbf{x}' &= [c_{p1}(0), \cdots, c_{p1}(N_{cp}-1), x(0), \cdots, x(N-1), \\ &\quad c_{p2}(0), \cdots, c_{p2}(N_{cp}-1)]^T, \end{aligned} \tag{7.3}$$

where $\mathbf{c}_{p1}$ and $\mathbf{c}_{p2}$ denote the PCP sequences with identical bandwidth for preceding and subsequent OFDM symbols, respectively. When there is no change in the information to be transmitted in the PCP signaling link, we have,

$$c_{p1}(n) = c_{p2}(n), \quad n = 0, 1, \cdots, N_{cp}-1. \tag{7.4}$$

Considering an L-tap static complex channel within one OFDM signal, $\mathbf{h} = [h_0, h_1, \cdots, h_{L-1}]^T$, for the signal propagation and interference analysis, including the worst case $L = N_{cp} + 1$, the received signal $\mathbf{r}$ corresponding to the transmitted signal vector $\mathbf{x}'$, with a size of $(N + 2N_{cp} + L - 1) \times 1$, can be expressed as

$$\mathbf{r} = \begin{bmatrix} h_0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ h_1 & h_0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ h_{L-1} & h_{L-2} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_{L-1} & \cdots & h_1 & h_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h_{L-1} & h_{L-2} & \cdots & h_0 \\ 0 & 0 & \cdots & 0 & h_{L-1} & \cdots & h_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & h_{L-1} \end{bmatrix} \mathbf{x}' + \mathbf{w}', \tag{7.5}$$

where the size of the channel matrix in (7.5) is $(N + 2N_{cp} + L - 1) \times (N + 2N_{cp})$, and $\mathbf{w}'$ is an AWGN vector with the same size as $\mathbf{r}$. The received signal over one OFDM symbol and two adjacent PCPs, $\mathbf{r}$, is depicted in Fig. 7.3. As highlighted by the shaded region in the figure, the transmitted signal appearing at the receiver is spread by the multipath channel, resulting into ISI and ICI. The ISI from the adjacent blocks and ICI within the current OFDM symbol have to be canceled for a successful demodulation of the data-carrying symbol.

7.2.2 Receiver Design for PCP-OFDM System

The receiver of the PCP-OFDM system, with a frequency domain equalization and time domain interference cancellation, is presented in Fig. 7.1(b). The transmitted PCP is first identified. After that, the data-carrying OFDM symbol is demodulated, following the ISI and ICI cancellation. The same as the observation period (OP)

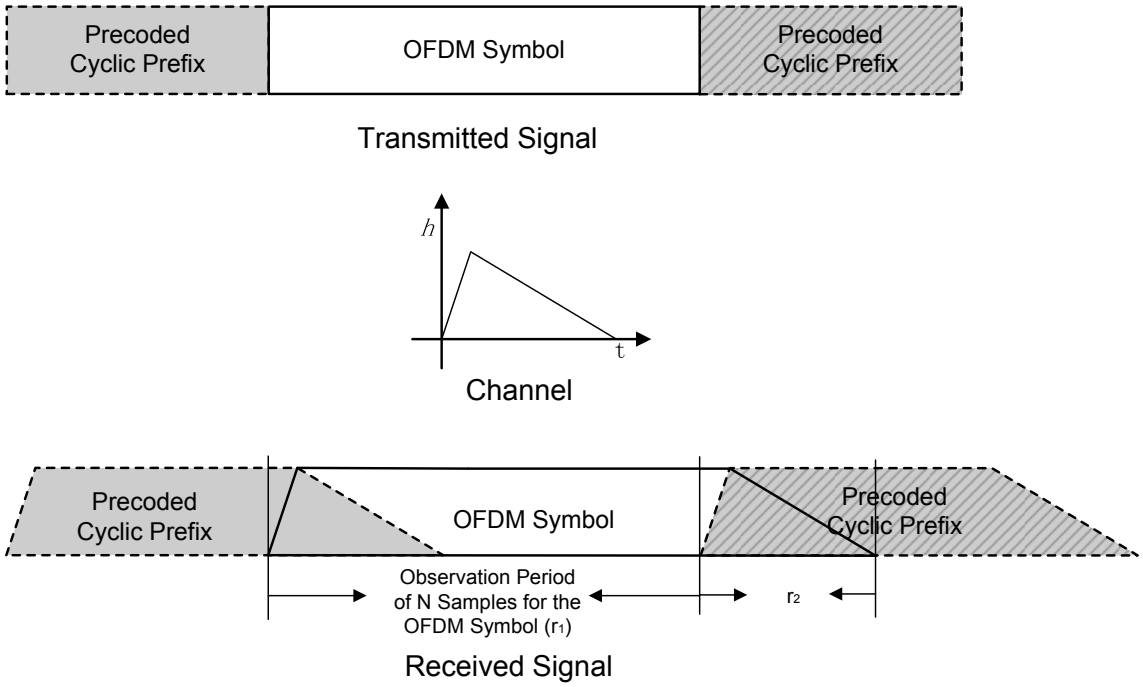


Figure 7.3: Signal propagation of one OFDM symbol and its neighboring PCPs.

normally used in a traditional OFDM receiver for the data demodulation, only N samples from the received signal are considered for demodulating the data-carrying OFDM symbol in the proposed receiver. The exact location of OP and the channel impulse response can be determined using the techniques in [128–130].

The PCP detection technique will be presented in Section 7.3. With the identified PCP sequences and estimated channel impulse response, ISI from the preceding PCP sequence due to the dispersive nature of multipath channel, can be computed and subtracted from the received signal. Meanwhile, ICI, which exists because of the lack of the cyclic structure in the PCP-OFDM signal when only N samples of the received signal are used for the demodulation process, needs to be eliminated by rebuilding the cyclic structure. To provide insights into the ISI and ICI within an PCP-OFDM signal in a multipath channel, two $N \times N$ matrices are constructed to describe the

impact from the channel. The first matrix

$$\mathbf{C} = \begin{bmatrix} h_0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ h_1 & h_0 & \cdots & 0 & 0 & \ddots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ h_{L-1} & h_{L-2} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_{L-1} & \cdots & h_1 & h_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h_{L-1} & h_{L-2} & \cdots & h_0 \end{bmatrix}, \tag{7.6}$$

represents the channel seen by the data-carrying OFDM symbol. The second matrix

$$\mathbf{C}_T = \begin{bmatrix} 0 & \cdots & 0 & h_{L-1} & h_{L-2} & \cdots & h_1 \\ 0 & \cdots & 0 & 0 & h_{L-1} & \cdots & h_2 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & h_{L-1} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}, \tag{7.7}$$

stands for the tail part of the channel impulse response that generates ISI in the succeeding symbol. These two matrices have an interesting property that

$$\mathbf{C} + \mathbf{C}_T = \mathbf{C}_{cycl}, \tag{7.8}$$

where $\mathbf{C}_{cycl}$ is the "ideal" channel matrix, i.e. the matrix that results in a cyclic convolution between the transmitted signal and the channel [130]. Based on (7.5), (7.6) and (7.7), we can express the received data-carrying OFDM symbol in the OP, i.e. $[r(N_{cp}),\ r(N_{cp}+1), \cdots, r(N_{cp}+N-1)]^T$, as

$$\mathbf{r}_1 = \mathbf{C}\mathbf{x} + \mathbf{C}_T\mathbf{R}_{c_{p1}} + \mathbf{w'}_N, \tag{7.9}$$

where $\mathbf{R}_{c_{p1}}$ is zero-padded signal vector of $\mathbf{c}_{p1}$, which can be expressed as

$$\mathbf{R}_{c_{p1}} = [\ \underbrace{0,\ \cdots,\ 0}_{(N-L+1)},\ \underbrace{c_{p1}(P-L+1),\ \cdots,\ c_{p1}(P-1)}_{(L-1)}\ ]^T. \tag{7.10}$$

$\mathbf{w'}_N$ is the noise acting on the samples during the OP, i.e. $\mathbf{w'}_N = [w'(N_{cp}),\ w'(N_{cp}+1), \cdots, w'(N_{cp}+N-1)]^T$.

In order to utilize a simple equalization and demodulation procedure like that in the traditional OFDM system, the following ideal received signal vector $\mathbf{r}_i$ has to be constructed

$$\mathbf{r}_i = \mathbf{r}_1 - \mathbf{C}_T\mathbf{R}_{c_{p1}} + \mathbf{C}_T\mathbf{x}. \tag{7.11}$$

The signal structure depicted in (7.11) suggests that the first step of the proposed hybrid domain receiver in demodulating $\mathbf{x}$ is to remove the ISI term by subtracting $\mathbf{C}_T\mathbf{R}_{c_{p1}}$ from the preceding PCP sequence. For any reasonable channel signal-to-noise ratio of interest, the error from the estimated channel is small enough and hence we will have reliable ISI cancellation.

After ISI removal, the next step is to remove the ICI term, or equivalently to perform cyclic reconstruction for the received data-carrying OFDM symbol. Here we employ an ICI cancellation approach in the time domain. Consider the propagation of signal vector $\mathbf{x}'$ in (7.3), as illustrated in Fig. 7.3. Let $\mathbf{r}_2$ of size N denote the received signal vector lying out of the OP but containing part of the data-carrying OFDM symbol due to the channel multipath distortion, that is

$$\mathbf{r}_2 = [\ \underbrace{r(N_{cp}+N),\ \cdots,\ r(N_{cp}+N+L-2)}_{(L-1)},\ \underbrace{0,\ \cdots,\ 0}_{(N-L+1)}\ ]^T. \tag{7.12}$$

$\mathbf{r}_2$ consists of signal components from both the data-carrying OFDM symbol and its following PCP. When $\mathbf{r}_1$ is used for the demodulation of the PCP-OFDM signal, we can find the remaining tail from the previous OFDM symbol in $\mathbf{r}_2$ is actually the signal needed to reconstruct the signal cyclic structure. By subtracting the signal component

of the second PCP from (7.12), the remaining tail from the previous data-carrying OFDM symbol, which is used to eliminate ICI, can be obtained using [131]

$$\mathbf{C}_T\mathbf{x} = \mathbf{r}_2 - \mathbf{C}_H\mathbf{R}_{c_{p2}}, \tag{7.13}$$

where the $N \times N$ matrix $\mathbf{C}_H$ is

$$\mathbf{C}_H = \begin{bmatrix} h_0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ h_1 & h_0 & \cdots & 0 & 0 & \ddots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ h_{L-2} & h_{L-3} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}, \tag{7.14}$$

and $\mathbf{R}_{c_{p2}}$ is the identified PCP following the data-carrying OFDM symbol, i.e

$$\mathbf{R}_{c_{p2}} = [\ \underbrace{c_{p2}(0),\ \cdots,\ c_{p2}(L-2)}_{(L-1)},\ \underbrace{0,\ \cdots,\ 0}_{(N-L+1)}\ ]^T. \tag{7.15}$$

Therefore, the ideal signal vector for the equalization and demodulation of the data-carrying OFDM symbol can be derived as

$$\mathbf{r}_i = \mathbf{r}_1 - \mathbf{C}_T\mathbf{R}_{c_{p1}} + \mathbf{r}_2 - \mathbf{C}_H\mathbf{R}_{c_{p2}}. \tag{7.16}$$

When the channel estimation is accurate, the ideal signal in the above equation turns to be

$$\mathbf{r}_i = \mathbf{C}_{cycl}\left\{\left(\mathbf{F}^N\right)^*\mathbf{X}\right\} + \mathbf{w}_N. \tag{7.17}$$

As for an OFDM system with cyclic prefix, the circulant matrix $\mathbf{C}_{cycl}$ can be diagonalized by $N \times N$ (I)FFT matrices [131]. For the equalization and demodulation

purposes, applying an FFT matrix to the above equation leads to

$$\mathbf{F}^N \mathbf{r}_i = \mathbf{F}^N \left\{ \mathbf{C}_{cycl} \left\{ \left(\mathbf{F}^N \right)^* \mathbf{X} \right\} + \mathbf{w}_N \right\} = \mathbf{D}_N(\tilde{\mathbf{H}}_N)\tilde{\mathbf{X}}, \tag{7.18}$$

where $\mathbf{D}_N(\tilde{\mathbf{H}}_N)$ is $N \times N$ diagonal matrix with the estimated frequency domain channel transfer function as its diagonal elements. As a result, the complete zero-forcing demodulation process is

$$\tilde{\mathbf{X}} = \mathbf{D}_N^{-1}(\tilde{\mathbf{H}}_N) \left\{ \mathbf{F}^N \mathbf{r}_i \right\}. \tag{7.19}$$

7.3 PCP Design for the Secure OFDM Systems

In the secure OFDM systems using channel based security techniques, the side information relevant to the security design can be shared between legitimate parties to mitigate the impairment from imperfect channel reciprocity and then improve the reliability of legitimate transmission. Usually, the side information does not contain much content. However, the transmission of such information needs to be reliable and confidential, without the requirement of additional time and spectrum resources and interruption to the data transmission. In the proposed strategy, the side information is conveyed by specially tailored PCPs, which are transmitted in a concurrent manner with the data-carrying OFDM symbols.

7.3.1 PCP Generation

In order to achieve a secure and reliable transmission through the PCP link, the side information to be transmitted is represented by a set of orthogonal sequences, where each orthogonal sequence uniquely indicates a potential value of the side information. Please note that the side information in a security design typically has limited content. The used orthogonal sequences are kept privately, and are only available to the legitimate users. In case the orthogonal sequences are cracked by adversaries,

they will be renewed immediately.

Let $\boldsymbol{\Upsilon}$ denotes the set of M_s orthogonal sequences indicating the potential information to be transmitted in the PCP, where each sequence has a length of N_{cp} according to the length of the PCP. We have

$$\boldsymbol{\Upsilon} = [\epsilon_0,\ \epsilon_1,\ \cdots,\ \epsilon_{M_s}], \tag{7.20}$$

where

$$\frac{1}{N_{cp}} \sum_{n=0}^{N_{cp}-1} \epsilon_i(n)\epsilon_v^*(n) = \begin{cases} 0, & i \neq v \\ 1, & i = v \end{cases}. \tag{7.21}$$

It is noteworthy that the size of M_s is decided by the selected orthogonal sequences and the sequence length N_{cp}. Since the design of orthogonal sequences is out of the scope of this study, this dissertation does not focus on this issue. The development of orthogonal sequences can be found in [132–134].

Generally, the orthogonal sequences are in a binary form, which would occupy infinite bandwidth and have time and frequency characteristics distinct from the data-carrying OFDM symbol. The time- and frequency-characteristic difference between PCPs and data-carrying symbol can facilitate eavesdropping and traffic analysis at adversaries, thus needs to be removed. For this reason, we would like to pass the orthogonal sequence through an OFDM modulator. For an orthogonal sequence with a length of N_{cp}, an OFDM modulator with N_{cp}-point IFFT is employed. Under the assumption that ϵ_i is selected to be transmitted according to the present side information, the output of the N_{cp}-point IFFT, which is used as the PCP symbol, can be expressed as

$$c_{p,i}(n) = \sqrt{\frac{1}{N_{cp}}} \sum_{k=0}^{N_{cp}-1} \epsilon_i(k) e^{j2\pi \frac{kn}{N_{cp}}}, \quad n = 0, 1, \cdots, N_{cp} - 1. \tag{7.22}$$

It is noteworthy that the same sampling frequency is adopted for both PCPs and data-carrying OFDM symbols to make they occupy the same bandwidth.

In the case that ϵ_i is orthogonal to ϵ_v, we can prove that $c_{p,i}(n)$ is also orthogonal to $c_{p,v}(n)$ as follows:

$$\begin{aligned}
\frac{1}{N_{cp}}\sum_{n=0}^{N_{cp}-1} c_{p,i}(n)c^*_{p,v}(n) &= \frac{1}{N_{cp}}\frac{1}{N_{cp}}\sum_{n=0}^{N_{cp}-1}\left\{\sum_{k_i=0}^{N_{cp}-1}\epsilon_i(k_i)e^{j2\pi\frac{k_i n}{N_{cp}}}\right. \\
&\quad \left.\sum_{k_v=0}^{N_{cp}-1}\epsilon^*_k(k_v)e^{-j2\pi\frac{k_v n}{N_{cp}}}\right\} \\
&= \frac{1}{N_{cp}^2}\sum_{k_i=0}^{N_{cp}-1}\sum_{k_v=0}^{N_{cp}-1}\epsilon_i(k_i)\epsilon^*_v(k_v)\sum_{n=0}^{N_{cp}-1}e^{j2\pi\frac{(k_i-k_v)n}{N_{cp}}}. \quad (7.23)
\end{aligned}$$

If $k_i \neq k_v$, we can always have

$$\sum_{n=0}^{N_{cp}-1} e^{j2\pi\frac{(k_i-k_v)n}{N_{cp}}} = 0. \quad (7.24)$$

If $k_i = k_v$, equation (7.23) can be rewritten as

$$\begin{aligned}
\frac{1}{N_{cp}}\sum_{n=0}^{N_{cp}-1} c_{p,i}(n)c^*_{p,v}(n) &= \frac{1}{N_{cp}}\sum_{k_i=0}^{N_{cp}-1}\epsilon_i(k_i)\epsilon^*_v(k_i) \\
&= 0. \quad (7.25)
\end{aligned}$$

Therefore, the Fourier transform would not change the orthogonality of the sequences. $c_{p,i}(n)$ is still orthogonal to $c_{p,v}(n)$.

Considering that both the real and imaginary parts of PCP symbols can convey information, the information of $2\log_2(M_s)$ bits can be transmitted by each generated PCP symbol with a length of N_{cp}.

7.3.2 PCP Detection

The legitimate receiver, which has the information of all the candidate orthogonal sequences, can locally generate all the possible PCP symbols that are orthogonal to each other. Depending on the orthogonality, the transmitted PCP can be detected

by correlating the received PCP with all the possible PCPs in the local library at the receiver. Under a multipath channel $\mathbf{h} = [h_0,\ h_1,\ \cdots,\ h_{L-1}]^T$, the correlation peak corresponding to the strongest path h_k will be used for the PCP detection.

Assuming that perfect synchronization is achieved through training signals or in-band pilot of the PCP-OFDM signal, the PCP detection process can be mathematically expressed as

$$C_m = \sum_{n=0}^{N_{cp}-1} r(n) c_{p,m}^*(n), \quad m = 0, 1, \cdots, M_s - 1, \tag{7.26}$$

where $c_{p,m}$ is the mth locally generated PCP symbol at the receiver. The candidate PCP $c_{p,m}$ that leads to the maximum output in (7.26) will be taken as the PCP signal sent out by the transmitter, and then used to assist the understanding of the current security design. The correlation peak corresponding to the strongest path h_k when $c_{p,m}$ is transmitted can be given by

$$C_{m,k} = h_k N_{cp} + w_c, \tag{7.27}$$

where w_c denotes the interference to the correlation result. Please note that signal components from other multipath taps would act as interference to the correlation peak, in addition to the AWGN. Consequently, the interference w_c can be approximated as a zero-mean Gaussian noise with a variance

$$\sigma_{w_c}^2 \approx N_{cp} \left(\sum_{l=0, l\neq k}^{L-1} |h_l|^2 \left[\sigma_P^2 + \frac{|l-k|}{N_{cp}} (\sigma_s^2 - \sigma_P^2) \right] + \sigma_w^2 \right), \tag{7.28}$$

where σ_P^2 denotes the variance of the shifted autocorrelation of PCP symbol $c_{p,m}$, σ_s^2 denotes the variance of correlation between the data-carrying OFDM symbol and PCP sequence $c_{p,m}$, and σ_w^2 is the variance of the AWGN.

7.4 Performance Analysis

7.4.1 Error Probability of PCP Detection

Under the assumption that $c_{p,m}$ is used for the current PCP-OFDM signal at the transmitter, the correlation result of a correct PCP detection can be written as (7.27). In contrast, when other local PCPs are correlated with the received PCP, we can obtain a result as $0 + w'_c$. If $h_k N_{cp} \leq w'_c - w_c$, an incorrect PCP detection occurs. Therefore, the error probability of each test in the PCP detection can be derived as

$$\begin{aligned} P_{e,m} &= P\Big\{h_k N_{cp} \leq w'_c - w_c\Big\} \\ &= Q\left(\frac{h_k N_{cp}}{\sqrt{\sigma^2_{w_c} + \sigma^2_{w'_c}}}\right), \end{aligned} \tag{7.29}$$

where

$$Q(a) = \int_a^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{y^2}{2}} dy. \tag{7.30}$$

The overall error probability after M_s cross correlations can then be calculated as

$$\begin{aligned} P_e &= 1 - (1 - P_{e,m})^{M_s - 1} \\ &= 1 - \left[1 - Q\left(\frac{h_k N_{cp}}{\sqrt{\sigma^2_{w_c} + \sigma^2_{w'_c}}}\right)\right]^{M_s - 1}. \end{aligned} \tag{7.31}$$

It can be found from (7.31) that the error probability of PCP detection is independent of the transmitted PCP symbols. In other words, all the potential PCPs that are orthogonal to each other would have the same detection error rate.

7.4.2 Error Probability of PCP-OFDM Demodulation

In this evaluation, we concentrate on the demodulation errors of the data-carrying OFDM symbol, caused by imperfect ISI and ICI cancellation with incorrect PCP

detection. The errors induced by the misunderstanding of the security processing, which primarily depend on the reliability of a specific security design, are not covered in the analysis.

With the overall PCP detection error rate derived in (7.31), the data demodulation performance of the PCP-OFDM system can be determined. Note that two PCPs need to be decided for demodulating a data-carrying OFDM symbol. The detection errors for $\mathbf{c}_{p1}$ and $\mathbf{c}_{p2}$ may result into different impacts on the data demodulation, as the impairments from $\mathbf{c}_{p1}$ and $\mathbf{c}_{p2}$ are different. Assume P_{e1} is the symbol error rate in demodulating the data-carrying OFDM symbol when the two PCP detections are correct, P_{e2} is the SER when the detection of $\mathbf{c}_{p1}$ is incorrect but the detection of $\mathbf{c}_{p2}$ is correct, P_{e3} is the SER under a correct $\mathbf{c}_{p1}$ detection but incorrect $\mathbf{c}_{p2}$ detection, and P_{e4} is the SER when both PCP detections are incorrect. The overall error rate for the PCP-OFDM data demodulation, under the assumption that each of the M_s orthogonal sequences has an equal probability to be transmitted, can be evaluated as

$$\begin{aligned}
P_{e,o} &= \frac{1}{M_s}\sum_{m=0}^{M_s-1}\Big[(1-P_e)^2\times P_{e1}+(1-P_e)\times P_e\times P_{e2} \\
&\quad +(1-P_e)\times P_e\times P_{e3}+P_e^2P_{e4}\Big] \\
&= \left[1-Q\left(\frac{h_kN_{cp}}{\sqrt{\sigma_{w_c}^2+\sigma_{w_c'}^2}}\right)\right]^{2(M_s-1)}\times P_{e1} \\
&\quad +\left\{\left[1-Q\left(\frac{h_kN_{cp}}{\sqrt{\sigma_{w_c}^2+\sigma_{w_c'}^2}}\right)\right]^{M_s-1}\right. \\
&\qquad \left.-\left[1-Q\left(\frac{h_kN_{cp}}{\sqrt{\sigma_{w_c}^2+\sigma_{w_c'}^2}}\right)\right]^{2(M_s-1)}\right\}\times\left(P_{e2}+P_{e3}\right) \\
&\quad +\left\{1-\left[1-Q\left(\frac{h_kN_{cp}}{\sqrt{\sigma_{w_c}^2+\sigma_{w_c'}^2}}\right)\right]^{M_s-1}\right\}^2\times P_{e4}.
\end{aligned} \tag{7.32}$$

When the PCP detection error rate is low, the data demodulation performance of the

PCP-OFDM system would be close to that of the traditional OFDM system.

7.5 Simulation Results

Computer simulations have been carried out to verify the proposed secure OFDM system with embedded confidential signaling. PCP-OFDM signals are generated as Fig. 7.1(a), where each data-carrying OFDM symbol has 64 subcarriers and the length of the PCP is 16. Walsh codes with a size of 16 are adopted as the orthogonal sequences to generate the PCP symbols. Sampling frequency for both the PCPs and data-carrying OFDM symbols is set to 20 MHz. Moreover, Rayleigh fading channels with exponential power delay profile of RMS delays 10 ns, 15 ns, 30 ns, 50 ns and 70 ns, are considered. Under the sampling frequency of 20 MHz, the lengths of the corresponding Rayleigh fading channels are 3, 5, 8, 12, 16, respectively. In addition, perfect synchronization and channel estimation are assumed in the simulations.

The error probabilities of the PCP detection under different Rayleigh fading channels are presented in Fig. 7.4. The error probability of PCP detection increases with the increase of the channel delay spread. Please note that no channel equalization is carried out for the PCP detection in the design, in order to reduce the operational complexity. As the PCP symbol does not have a cyclic structure, equalization of the PCP symbol has to seek help from the time domain iterative equalization techniques, which would result into a huge computation burden. Without the channel equalization, ISI from previous signals would disrupt the PCP detection. A longer delay spread would cause a stronger ISI, and then degrade the detection performance more severely. Fortunately, with the employment of orthogonal sequences, satisfactory PCP detection performance can still be obtained without the channel equalization. As shown in the figure, even when the delay spread is equal to the length of the PCP, the detection error rate has already reduced to 0.1 when SNR is 10 dB. In addition, it can be observed that the error probability curves turn to be flat during the high SNR range. This is because that the PCP detection is mainly distorted by the ISI

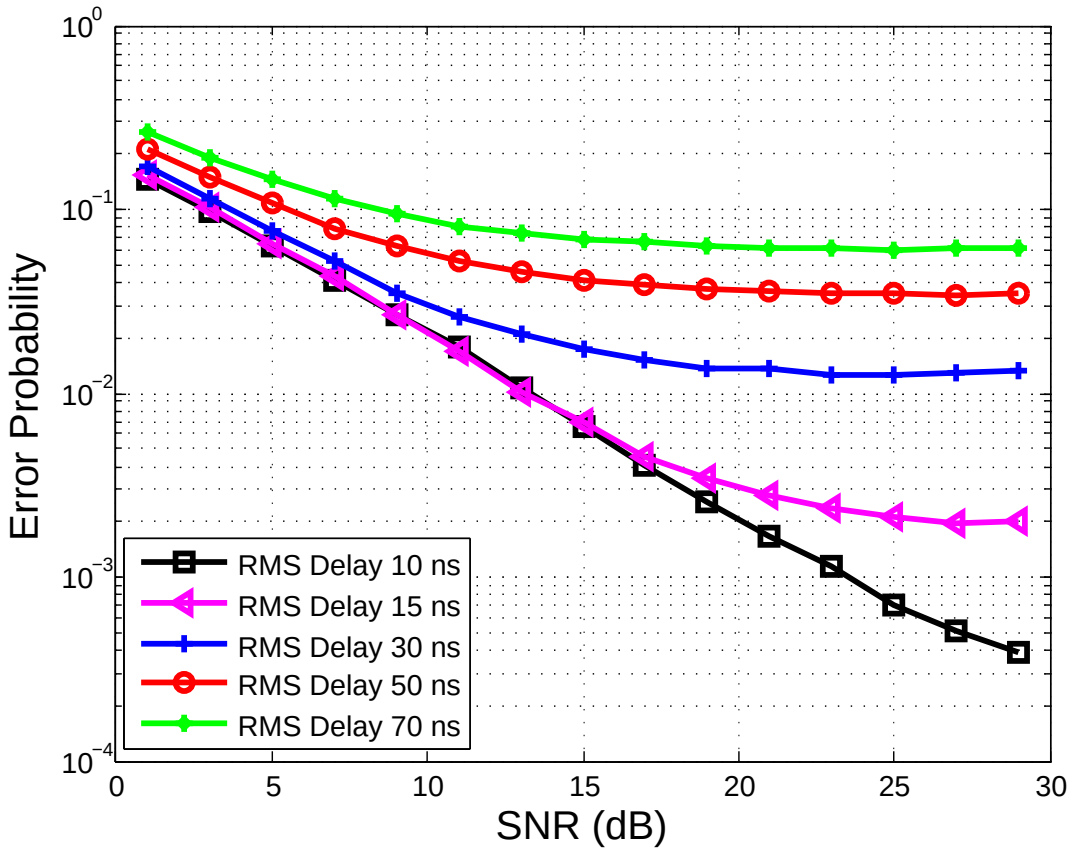


Figure 7.4: Error probability of the PCP enabled confidential signaling under different channel conditions.

from multipath spread but not the noise when the SNR is high.

Since the ISI from multipath delay spread dominates the PCP detection performance, particularly in the high SNR range, interference mitigate techniques can be executed to improve the PCP detection reliability. Consider the duration of a PCP-OFDM signal is usually much less than the channel coherence time. For example, in an IEEE 802.11 network, the duration of an OFDM symbol is 4 us while the channel coherence time is approximately 53 ms according to a pedestrian walking speed of 1 m/s. There is a big chance that a data-carrying OFDM symbol is accompanied by two identical PCPs, since the channel based security design is not renewed so frequently. As a result, the two PCPs can be averaged to mitigate the interference

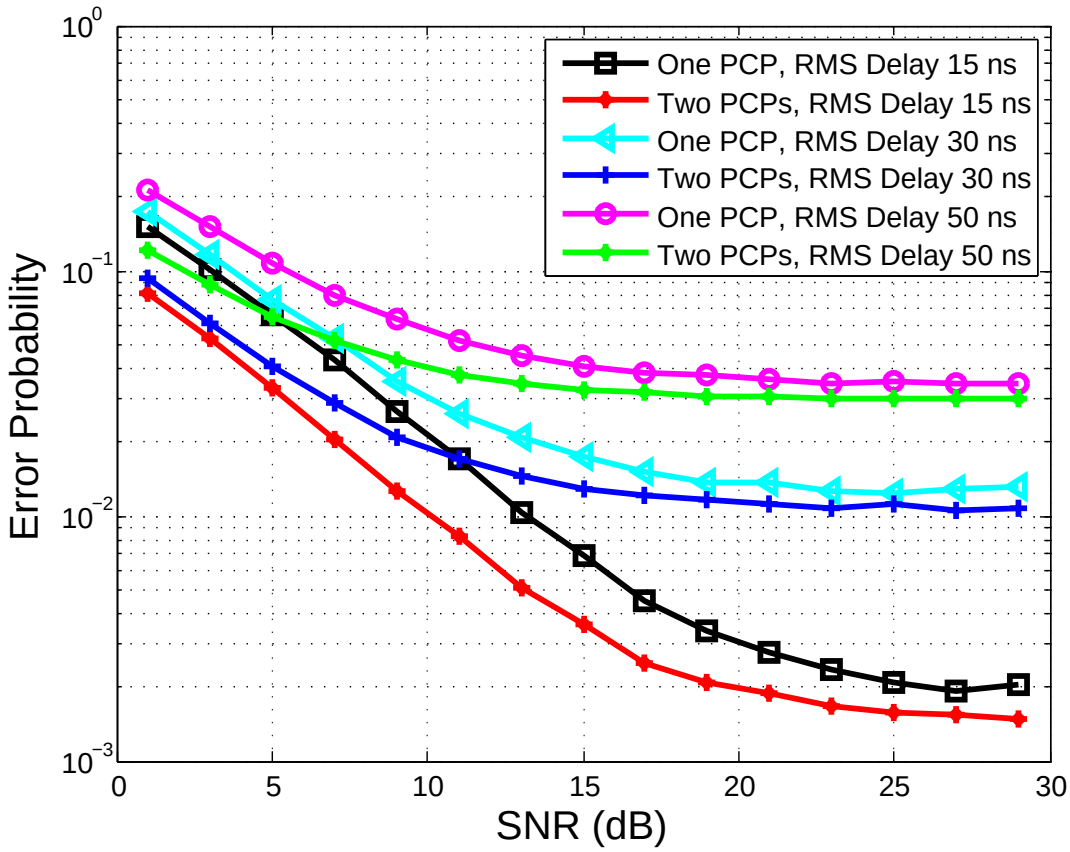


Figure 7.5: Error probability of the PCP enabled confidential signaling with interference mitigation process.

and AWGN. Simulation results when two successively received PCPs are averaged for the PCP detection are compared with the detection performance using only one PCP in Fig. 7.5. Significant performance improvement of the PCP detection can be observed when the interference mitigation process is operated.

The bit error rate (BER) and SER of data demodulation in the proposed secure OFDM system with embedded confidential signaling are depicted in Fig. 7.6 and Fig. 7.7, respectively. No interference mitigation process is carried out for the PCP detection in these simulations. The BER and SER of the traditional CP-OFDM system are provided as a benchmark in the study. As shown in the figures, the data demodulation performance of the PCP-OFDM system is comparable to that of the

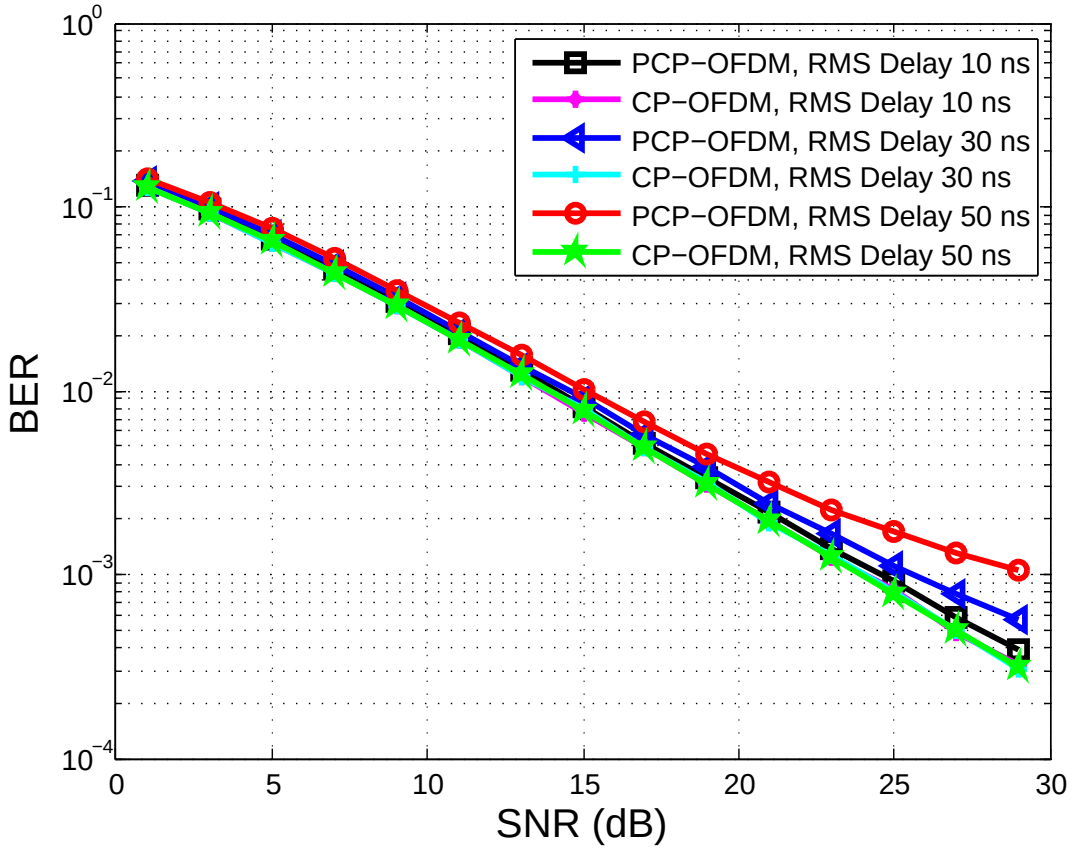


Figure 7.6: BER of the secure OFDM system with embedded confidential signaling under different channel conditions.

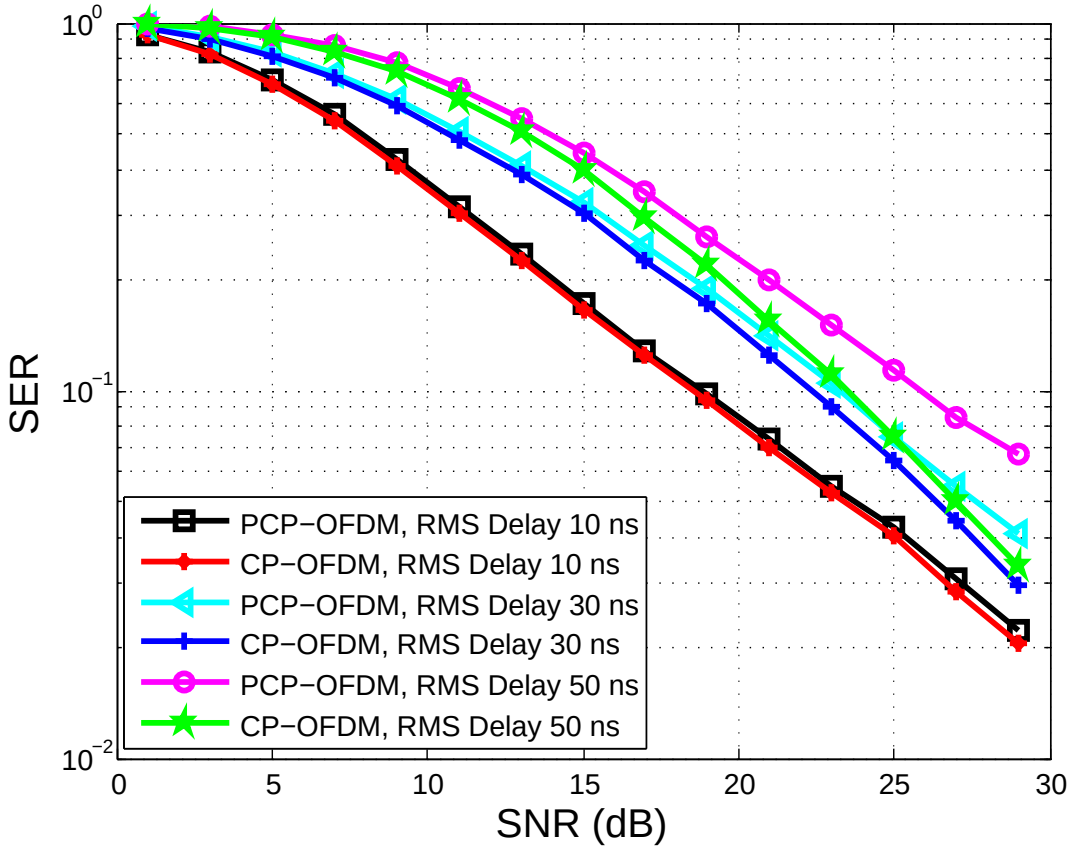


Figure 7.7: SER of the secure OFDM system with embedded confidential signaling under different channel conditions.

traditional CP-OFDM system, especially in a multipath channel with a short delay spread. When ISI on the PCP symbol is strong because of a long multipath channel, the performance of PCP-OFDM is worse than that of the CP-OFDM. The performance loss of data demodulation comes from the imperfect ISI and ICI cancellation for the data-carrying OFDM symbol, essentially due to the incorrect PCP detection.

7.6 Summary

An embedded confidential signaling strategy for secure OFDM systems is investigated in this chapter, in which the traditional cyclic prefix of an OFDM signal is replaced by a specially designed orthogonal sequence, named PCP. The security design relevant side information is conveyed by the PCP, and concurrently transmitted with the data-carrying OFDM symbol. Consequently, information sharing between the transmitter and legitimate receiver is enabled by the PCP signaling link without interrupting the data transmission and requiring additional time and spectrum resources. In order to achieve a secure and reliable transmission through the PCP link, a set of orthogonal sequences, which is only known by legitimate users, is one-to-one mapped to the potential information to be transmitted. An orthogonal sequence is chosen in the transmission of each OFDM symbol corresponding to the present security design. The PCP symbol is then generated by passing the selected orthogonal sequence through an OFDM modulator, so as to maintain the same time and frequency characteristics as the data-carrying OFDM symbol. With the inherent orthogonality among all the candidate PCPs, the transmitted side information can be reliably detected through cross correlations between the received PCP and elements in the local PCP library of the receiver. The local candidate PCP that leads to the maximum correlation peak will be taken as the PCP sent out by the transmitter, and then used to assist the derivation of the adopted security design. Theoretical analysis and simulation results have been provided to validate the proposed embedded confidential signaling link in secure OFDM systems.

Chapter 8

Conclusions & Future Work

8.1 Conclusions

Securing wireless communications is challenging due to the inherent broadcast nature of radio propagation. Traditional security mechanisms that do not address the security issues at the physical layer cannot completely protect wireless networks. To that end, physical layer security is emerging as a complement to traditional strategies for securing wireless communications. This dissertation has investigated physical layer security to: 1) evaluate the security level of wireless environments for developing adaptive security strategies, 2) enhance the built-in security of wireless OFDM communication systems against passive eavesdropping, and 3) provide an embedded signaling link for reliably and confidentially transmitting the data and security design relevant parameters simultaneously.

Chapter 2 provides fundamentals related to the wireless communication security, including risks and threats in wireless communication systems, general security objectives, and constraints of traditional upper-layer security approaches. The concept of physical layer security in wireless communications along with a literature survey of existing techniques is also presented. Furthermore, OFDM technology is reviewed. The security weaknesses of OFDM physical layer due to its distinct time and frequency

characteristics are addressed.

Chapter 3 investigates a time domain pilot correlation based detection technique for recognizing the existence of active users in a wireless network. The proposed technique is based on a cyclic correlation between the complex conjugate multiplication of adjacent received signal segments and a local reference derived from the in-band pilots. The noise effect on the detection reliability is mitigated by a time domain segment averaging following the phase rotation locking processing. The robustness of the proposed detection algorithm to timing offset is improved by the time domain OFDM symbol length based segmentation and the cyclic correlation. The robustness to frequency offset is enhanced by the complex conjugate multiplication and the use of the correlation magnitude. Simulation results show that the detection performance of the proposed technique is satisfactory under low SNR conditions, even though both timing and frequency offsets exist.

Chapter 4 proposes a novel device RF-DNA based estimation technique for the number of active users in a network. Since any node in a network may act as a malicious attacker and be a potential threat, the number of active users in a network is crucial for understanding the security level of the wireless operating environment. As a typical device RF-DNA that has device-specific nature, transmitter I/Q imbalance is explored in the design. I/Q imbalance of a transmitter is first estimated from its transmitting signals, and then compared with the I/Q imbalance estimate of each previously identified active user through a hypothesis testing, where the Euclidean distance between the new and previous estimates is adopted as the test metric. If all the distances are larger than a properly selected threshold, a new active user is claimed. Finally, the number of active users is obtained by counting all the distinct I/Q imbalances. Simulation results have been provided to validate the proposed estimation technique.

Chapter 5 proposes a novel and effective anti-eavesdropping OFDM system through dynamic coordinate interleaving, by exploiting the channel reciprocity and uncorrelation feature exhibited among spatially separate wireless channels. Two coordinate

interleaving based security schemes are investigated, which employ the subcarrier channel gain and phase in determining the interleaving pattern, respectively. Depending on the CSI associated with the transmitter and legitimate receiver, the symbol coordinate at a subcarrier with channel gain or channel phase larger than a predefined threshold is interleaved. Since wireless channels associated with each pair of users at separate locations exhibit independent propagation characteristics, the frequently renewed selection of subcarriers undergoing coordinate interleaving is only shared by legitimate users based on channel reciprocity. Without a matched subcarrier coordinate de-interleaving pattern, erroneous information recovery is performed at the eavesdropper so that eavesdropping is prevented. Theoretical analysis and simulation results have been provided to validate the effectiveness of the proposed secure OFDM system against eavesdropping.

In Chapter 6, another novel eavesdropping-resilient OFDM system through dynamic subcarrier interleaving is investigated as an alternative solution to prevent eavesdropping, by taking advantage of the reciprocal, location-dependent and time-varying nature of wireless channels. A transmitter employs its instantaneous CSI to an intended receiver in designing the subcarrier interleaving pattern, where partial subcarriers of each OFDM signal are selected and interleaved according to the sorted order of their channel gains. Since wireless channels associated with each pair of users at separate locations exhibit independent frequency selectivity, the frequently renewed subcarrier interleaving scheme is only shared between legitimate nodes based on channel reciprocity. As a result, mismatched information recovery is carried out at the eavesdropper without an identical subcarrier interleaving pattern, thus preventing malicious eavesdropping. In order to mitigate the impairment from imperfect channel reciprocity between legitimate parties, a subcarrier selection algorithm is also investigated to realize a trade-off between the eavesdropping resilience and legitimate transmission reliability. It is observed from simulation results that eavesdropping on the proposed system suffers a SER close to 100% while the legitimate transmission has a SER matching to that of conventional OFDM systems.

Chapter 7 provides an embedded confidential signaling link for the transmission of security design relevant side information in secure OFDM systems. Extending our previous study on PCP-OFDM, the sharing of the security design relevant side information between legitimate users is enabled by a specially tailored PCP sequence. To be specific, a set of orthogonal sequences, which is only known by legitimate users, is one-to-one mapped to the potential information to be transmitted. An orthogonal sequence is chosen in the transmission of each OFDM symbol corresponding to the present security design. The PCP sequence is then generated by passing the selected orthogonal sequence through an OFDM modulator, in order to maintain the same time and frequency characteristics as the concurrently transmitted data-carrying OFDM symbol. With the inherent orthogonality among all the candidate PCPs, the side information transmitted through the PCP signaling link can be reliably identified through cross correlations between the received PCP and elements in the local PCP library at the receiver, and then used to assist the derivation of the security design initiated by the transmitter. The validity of the PCP enabled signaling link has been demonstrated by theoretical analysis and simulation results.

8.2 Future Work

There are several topics related to the presented research worthwhile for further study. Some of them are listed as follows:

- On the topic of security level assessment in wireless networks, the presented scheme explores the number of active users as the evaluation metric. However, other network relevant parameters that can also indicate the security status in wireless environments can be exploited to increase the evaluation accuracy.

- In the proposed device RF-DNA based estimation technique for the number of active users in a network, only one typical hardware impairment in wireless devices—I/Q imbalance, is addressed. The proposed estimation technique can

be further extended to other device RF-DNAs as well, such as frequency and magnitude errors.

- Regarding the enhancement of the built-in security in wireless communication systems, this dissertation concentrates on the security against passive attacks, considering that passive attacks often cause fatal damage to a wireless communication system. It is thus necessary to extend the current work to a general scenario consisting of both passive and active attacks.

- In the wireless channel based physical layer security approaches, the randomness of the wireless channel between the transmitter and legitimate receiver is exploited for the security design. As a precondition, the identity of the legitimate receiver must be accurately verified. Therefore, reliable and efficient authentication techniques also need to be investigated.

Appendices

Appendix A

Timing and Frequency Offsets in OFDM

A.1 Timing Offset

Timing offset, which comes from the effect of sampling time error at the receiver side, is a serious problem in OFDM system. Since large timing offset can be easily corrected with OFDM frame synchronization, the timing offset addressed in the appendix is the residue error after the frame synchronization. Assume $X(k)$ is the frequency domain data to be transmitted using the OFDM system. After the processing of the OFDM transmitter introduced in Chapter 2, the corresponding time domain OFDM signal $x(t)$ is up-converted and transmitted over the wireless channel. At the receiver side, the received signal is sampled with the analog-to-digital converter (ADC) for demodulation and information recovery, where timing errors may exist and thus degrade the receiver performance. The OFDM process chain with timing offset is shown in Fig. A.1, where $y(n)$ denotes the received time domain signal and $Y(k)$ stands for the output of the FFT.

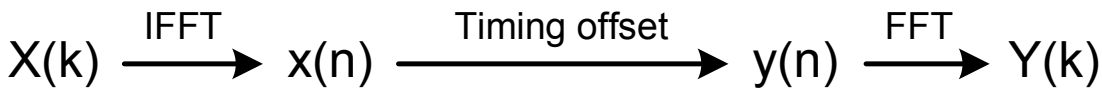


Figure A.1: OFDM process chain with timing offset.

With IFFT, the time domain transmitted OFDM signal from $X(k)$ is obtained as

$$x(n) = \sum_{k=0}^{N-1} X(k) e^{j2\pi \frac{kn}{N}}, \quad n = 0, 1, \cdots, N-1. \tag{A.1}$$

Let Δn denote the relative timing offset, which is the ratio of the timing offset to the sampling interval. If the received signal is sampled with the timing error Δn, $y(n)$ will be a time shifted version of $x(n)$. Mathematically,

$$\begin{aligned} y(n) &= x(n + \Delta n) \\ &= \sum_{k=0}^{N-1} X(k) e^{j2\pi \frac{k(n+\Delta n)}{N}}, \quad n = 0, 1, \cdots, N-1. \end{aligned} \tag{A.2}$$

Since large timing offset is easy to be compensated, usually only the residual error (fractional timing offset) exists in the following processing, and the orthogonality of the OFDM signal will normally not be destroyed by the timing offset. In this case, the recovered data after FFT at the receiver can be expressed as

$$\begin{aligned} Y(k) &= \frac{1}{N} \sum_{n=0}^{N-1} \left[\sum_{l=0}^{N-1} X(l) e^{j2\pi \frac{l(n+\Delta n)}{N}} \right] e^{-j2\pi \frac{kn}{N}} \\ &= \frac{1}{N} \sum_{l=0}^{N-1} X(l) e^{j2\pi \frac{l\Delta n}{N}} \left[\sum_{n=0}^{N-1} e^{j2\pi \frac{(l-k)n}{N}} \right] \\ &= X(k) e^{j2\pi \frac{k\Delta n}{N}}, \quad k = 0, 1, \cdots, N-1. \end{aligned} \tag{A.3}$$

Equation (A.3) shows that the fractional timing offset causes a phase rotation of the recovered signal, which is linearly proportional to the subcarrier index.

A.2 Frequency Offset

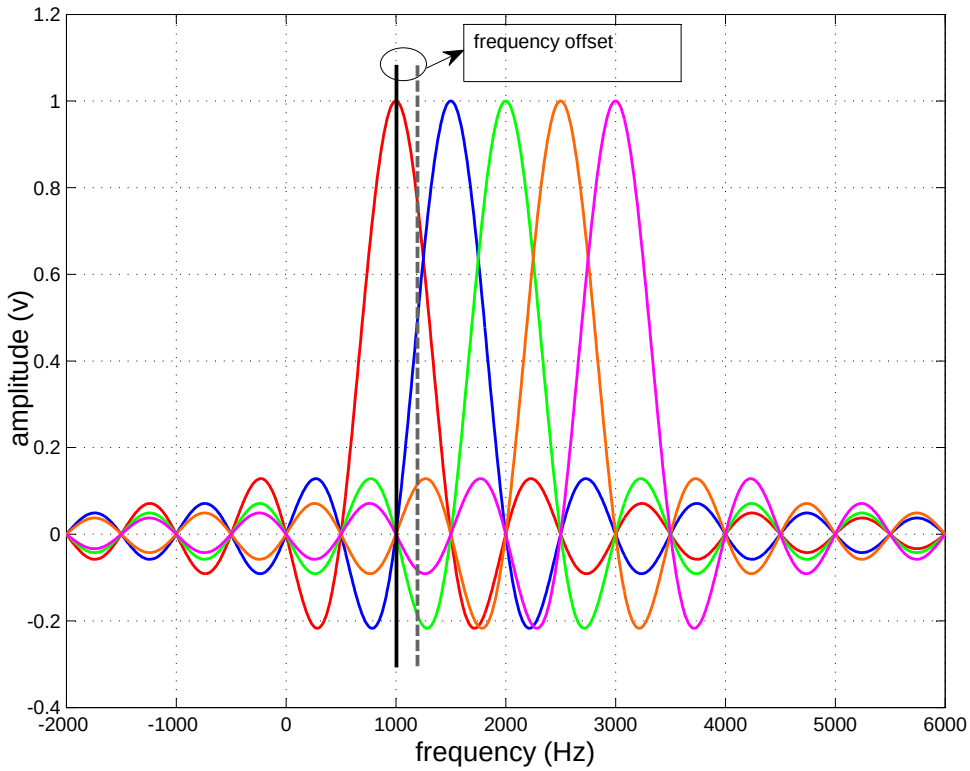


Figure A.2: Illustration of frequency offset in OFDM signals.

Since there are local oscillator errors and Doppler frequency shifts in wireless OFDM system, frequency offset always exists between the transmitter and receiver, as illustrated in Fig. A.2. Similar to the analysis of timing offset, the OFDM process chain with frequency offset is given as Fig. A.3.

$$X(k) \xrightarrow{\text{IFFT}} x(n) \xrightarrow{\text{Freuqency offset}} \tilde{y}(n) \xrightarrow{\text{FFT}} \tilde{Y}(k)$$

Figure A.3: OFDM process chain with frequency offset.

In order to avoid potential confusion, the received signal with frequency offset is represented by $\tilde{y}(n)$ and the corresponding recovered data is denoted by $\tilde{Y}(k)$. Let

Δk represent the relative frequency offset, which is defined as the ratio of the actual frequency offset to the subcarrier spacing. The received signal with frequency offset Δk can be written as

$$\begin{aligned}
\tilde{y}(n) &= \sum_{k=0}^{N-1} X(k) e^{j2\pi \frac{(k+\Delta k)n}{N}} \\
&= \sum_{k=0}^{N-1} X(k) e^{j2\pi \frac{kn}{N}} e^{j2\pi \frac{\Delta kn}{N}} \\
&= x(n) e^{j2\pi \frac{\Delta kn}{N}}, \quad n = 0, 1, \cdots, N-1. \qquad \text{(A.4)}
\end{aligned}$$

As shown in (A.4), the effect of frequency offset on each time domain OFDM sample $x(n)$ is a phase shift of $2\pi\Delta kn/N$. The data symbol after the FFT can thus be given by

$$\begin{aligned}
\tilde{Y}(k) &= \frac{1}{N} \sum_{n=0}^{N-1} \left[\sum_{l=0}^{N-1} X(l) e^{j2\pi \frac{(l+\Delta k)n}{N}} \right] e^{-j2\pi \frac{kn}{N}} \\
&= \frac{1}{N} \sum_{n=0}^{N-1} \left[\sum_{l=0}^{N-1} X(l) e^{j2\pi \frac{(l-k+\Delta k)n}{N}} \right] \\
&= \frac{1}{N} \sum_{l=0}^{N-1} X(l) \left[\sum_{n=0}^{N-1} e^{j2\pi \frac{(l-k+\Delta k)n}{N}} \right], \\
&\qquad k = 0, 1, \cdots, N-1. \qquad \text{(A.5)}
\end{aligned}$$

With the geometric series expansion, i.e. $\sum_{n=0}^{N-1} a^n = \frac{1-a^N}{1-a}$, equation (A.5) can be

rewritten as

$$\begin{aligned}
\tilde{Y}(k) &= \frac{1}{N}\sum_{l=0}^{N-1} X(l)\frac{1-e^{j2\pi(l-k+\Delta k)}}{1-e^{j2\pi\frac{l-k+\Delta k}{N}}} \\
&= \frac{1}{N}\sum_{l=0}^{N-1} X(l)\frac{e^{j\pi(l-k+\Delta k)}\left(e^{-j\pi(l-k+\Delta k)}-e^{j\pi(l-k+\Delta k)}\right)}{e^{j\pi\frac{l-k+\Delta k}{N}}\left(e^{-j\pi\frac{l-k+\Delta k}{N}}-e^{j\pi\frac{l-k+\Delta k}{N}}\right)} \\
&= \frac{1}{N}\sum_{l=0}^{N-1} X(l)\frac{e^{j\pi(l-k+\Delta k)}}{e^{j\pi\frac{l-k+\Delta k}{N}}}\frac{-2j\sin(\pi(l-k+\Delta k))}{-2j\sin(\pi\frac{l-k+\Delta k}{N})} \\
&= \frac{1}{N}\sum_{l=0}^{N-1} X(l)e^{j\pi(l-k+\Delta k)\frac{N-1}{N}}\frac{\sin(\pi(l-k+\Delta k))}{\sin(\pi\frac{l-k+\Delta k}{N})}, \\
&\qquad\qquad k=0,1,\cdots,N-1. \qquad \text{(A.6)}
\end{aligned}$$

For a small x, $\sin(x) \approx x$. It can be used to simplify the above equation, especially when N is very large. Thus,

$$\begin{aligned}
\tilde{Y}(k) &\approx \sum_{l=0}^{N-1} X(l)e^{j\pi(l-k+\Delta k)\frac{N-1}{N}}\frac{\sin(\pi(l-k+\Delta k))}{\pi(l-k+\Delta k)} \\
&= X(k)e^{j\pi(\Delta k)\frac{N-1}{N}}\frac{\sin(\pi\Delta k)}{\pi\Delta k} \\
&\quad + \sum_{l=0,l\neq k}^{N-1} X(l)e^{j\pi(l-k+\Delta k)\frac{N-1}{N}}\frac{\sin(\pi(l-k+\Delta k))}{\pi(l-k+\Delta k)}, \\
&\qquad\qquad k=0,1,\cdots,N-1, \qquad \text{(A.7)}
\end{aligned}$$

where $\sum_{l=0,l\neq k}^{N-1} X(l)e^{j\pi(l-k+\Delta k)\frac{N-1}{N}}\frac{\sin(\pi(l-k+\Delta k))}{\pi(l-k+\Delta k)}$ is referred to as inter-carrier interference caused by the sidelobes of other subcarriers due to frequency offset. It can be concluded from (A.7) that a phase shift and an amplitude attenuation are introduced by the frequency offset to the demodulated output. At the same time, the recovered data is interfered by the signals from other subcarriers of the same OFDM symbol due to the loss of the orthogonality.

Bibliography

[1] A. E. Earle, *Wireless Security Handbook*, Auerbach Publications, 2005.

[2] Y.-S. Shiu, *et al.*,"Physical Layer Security in Wireless Networks: A Tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66-74, Apr. 2011.

[3] W. E. Cobb, *et al.*, "Intrinsic Physical-Layer Authentication of Integrated Circuit," *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 1, pp. 14-24, Feb. 2012.

[4] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-Layer Authentication," *IEEE Trans. Inf. Forens. Security*, vol. 3, no. 1, pp. 38-51, Mar. 2008.

[5] A. A. Tomko, C. J. Rieser, and L. H. Buell, "Physical-Layer Intrusion Detection in Wireless Networks," in *Proc. IEEE Military Commun. Conf.*, 2006, pp. 1-7.

[6] J. H. Lee amd R. M. Buehrer, "Characterization and Detection of Location Spoofing Attacks," *IEEE J. Commun. Netw.*, vol. 14, no. 4, pp. 396-409, Aug. 2012.

[7] J. Huang and A. L. Swindlehurst, "Robust Secure Transmission in MISO Channels Based on Worst-Case Optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696-1707, Apr. 2012.

[8] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the Application of Cooperative Transmission to Secrecy Communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359-368, Feb. 2012.

[9] Y. S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical Layer Security in Wireless Networks: a Tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66-74, Apr. 2011.

[10] S. Mathur *et al.*, "Exploiting the Physical Layer for Enhanced Security," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 63-70, Oct. 2010.

[11] H. V. Poor, "Information and Inference in the Wireless Physical Layer," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 40-47, Feb. 2012.

[12] P. Stavroulakis and M. Stamp (Eds.), *Handbook of Information and Communication Security*, Springer, 2010.

[13] F. Renna, N. Laurenti, and H. V. Poor, "Physical-Layer Secrecy for OFDM Transmissions over Fading Channels," *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 4, pp. 1354-1367, Aug. 2012.

[14] H. Chaouchi and M. Laurent-Maknavicius, *Wireless and Mobile Network Security*, ISTE Ltd. and John Wiley & Sons, Inc., 2009.

[15] D. Dzung, *et al.*, "Security for Industrial Communication Systems," *Proc. IEEE*, vol. 93, no. 6, pp. 1152-1177, Jun. 2005.

[16] D. Reed, "Applying the OSI Seven Layer Network Model to Information Security," *SANS Institute*, 2004.

[17] W. Stallings, *Crytography and Network Security Principles and Practices*, Prentice Hall PTR, 2006.

[18] X. Wang, H. Li, and H. Lin, "A New Adaptive OFDM System with Precoded Cyclic Prefix for Dynamic Cognitive Radio Communications," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 431-442, Feb. 2011.

[19] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[20] D. Prabakar, M. Marikkannan, and S. Karthik, "Various Security Threats and Issues in Wireless Networks: A Survey," *Int. J. Adv. Research Comput. Eng. & Technol.*, vol. 1, no. 10, pp. 296-299, Dec. 2012.

[21] Y. Zhou, Y. Fang and Y. Zhang, "Securing Wireless Sensor Networks: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 10, no. 3, pp. 6 - 28, 2008.

[22] A. S. Tanenbaum, *Computer Networks*, Prentice Hall PTR, 2004.

[23] T. Kavitha and D. Sridharan, "Security Vulnerabilities in Wireless Sensor Networks: A Survey," *J. Inf. Assurance Security*, vol. 5, pp. 31-44, 2010.

[24] D. Ma and G. Tsudik, "Security and Privacy in Emerging Wireless Networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 12-21, Oct. 2010.

[25] D. Parsons, *The Mobile Radio Propagation Channel*, Wiley: New York, 1992.

[26] A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2005.

[27] W. E. Cobb, *et al.*, "Physical Layer Identification of Embedded Devices Using RF-DNA Fingerprinting," in *Proc. IEEE Military Commun. Conf.*, 2010, pp. 682-687.

[28] V. Brik, *et al.*, "Wireless Device Identification with Radiometric Signatures," in *Proc. ACM Int. Conf. Mobile Computing and Networking*, 2008, pp. 116-127.

[29] C. E. Shannon, "Commnuication Theory of Secrecy Systems," *Bell Syst. Tech. Journal*, vol. 28, pp. 656-715, 1949.

[30] A. D. Wyner, "The Wiretap Channel," *Bell System Technique Journal*, vol. 54, pp. 1355-1387, 1975.

[31] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451-456,Jul. 1978.

[32] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Information Theory*, 2006, pp. 356-360.

[33] M. Bloch, *et al.*, "Wireless Information-Theoretic Security," *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 25152534, Jun. 2008.

[34] Y. Liang, H. V. Poor, and S. Shamai, "Secure Communication Over Fading Channels," *IEEE Trans. Infom. Theory*, vol. 54, no. 6, pp. 2470-2492, Jun. 2008.

[35] III A. O. Hero, "Secure space-time communication," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3235-3249, Dec. 2003.

[36] R. Wilson, D. Tse, and R. A. Scholta, "Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels," *IEEE Trans. Inf. Forens. Security*, vol. 2, no. 3, pp. 364-375, Sept. 2007.

[37] O. O. Koyluoglu and H. E. Gamal, "Polar Coding for Secure Transmission and Key Agreement," *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 5, pp. 1472-1483, Oct. 2012.

[38] X. Wang, *et al.*, "Power and Subcarrier Allocation for Physical-Layer Security in OFDMA-Based Broadband Wireless Networks," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 3, pp. 693-702, Sept. 2011.

[39] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure Resource Allocation and Scheduling for OFDMA Decode-and-Forward Relay Networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528-3540, Oct. 2011.

[40] H. M. Wang, Q. Yin, and X. G. Xia, "Distributed Beamforming for Physical-Layer Security of Two-Way Relay Networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532-3545, Jul. 2012.

[41] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[42] Z. Ding, *et al.*, "On the Application of Cooperative Transmission to Secrecy Communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359-368, Feb. 2012.

[43] L. Xiao, *et al.*, "Using the Physical Layer for Wireless Authentication in Time-Variant Channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571-2579, Jul. 2008.

[44] P. Baracca, N. Laurenti, and S. Tomasin, "Physical Layer Authentication over MIMO Fading Wiretap Channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564-2573, Jul. 2012.

[45] K. Zhang, K. Govindan, and P. Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56-62, Oct. 2010.

[46] C. Ye, *et al.*, "Information-Theoretically Secret Key Generation for Fading Wireless Channels," *IEEE Trans. Inf. Forens. Security*, vol. 5, no. 2, pp. 240-254, Jun. 2010.

[47] L. Lai, Y. Liang, and H. V. Poor, "A Unified Framework for Key Agreement over Wireless Fading Channels," *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 2, pp. 480-490, Apr. 2012.

[48] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting Channel Diversity in Secret Key Generation From Multipath Fading Randomness," *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 5, pp. 1484-1497, Oct. 2012.

[49] W. C. Suski II, *et al.*, "Using Spectral Fingerprints to Improve Wireless Network Security," in *Proc. IEEE Global Commun. Conf.*, 2008, pp. 1-5.

[50] N. T. Nguyen, *et al.*, "Device Fingerprinting to Enhance Wireless Security Using Nonparametric Bayeian Method," in *Proc. IEEE Int. Conf. Comput. Commun.*, 2011, pp. 1404-1412.

[51] A. Candore, O. Kocabas, and F. Koushanfar, "Robust Stable Radiometric Fingerprinting for Wireless Devices," in *IEEE Int. Workshop Hardware-Oriented Security and Trust*, 2009, pp. 43-49.

[52] V. Lakafosis, "RF Fingerprinting Physical Objects for Anticounterfeiting Applications," *IEEE Trans. Microw. Theory Tech.*, vol. 59, no. 2, pp. 504-514, Feb. 2011.

[53] S. Weinstein and P. Ebert, "Data Transmission by Frequency-Division Multiplexing Using the Discrete Fourier Transform," *IEEE Trans. Commun. Technol.*, vol. 19, no. 5, pp. 628-634, Oct. 1971.

[54] 3GPP LTE Encyclopedia, "An Introduction to LTE," Dec. 2010.

[55] IEEE Standard, "IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Network-Specific Requirement - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," Jun. 2007.

[56] IEEE Standard, "IEEE Standard for Information technology - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput," Oct. 2009.

[57] IEEE Standard, "The Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems," Jun. 2004.

[58] ETSI, "Digital Video Broadcasting: Framing Structure, Channel Coding, and Modulation for Digital Terrestrial Television," European Telecommunication Standard EN300744, Aug. 1997.

[59] DVB, "A122: Framing structure, channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2)," DVB Document A122r1, Jan. 2008.

[60] ETSI, "Digital Vedio Broadcasting (DVB); Transmisssion System for Handheld Terminals (DVB-H)," European Telecommunication Standard EN302304, Nov. 2004.

[61] T. Cui and C. Tellambura, "Blind Receiver Design for OFDM Systems over Doubly Selective Channels," *IEEE Trans. Wireless Commun.*, vol. 55, no. 5, pp. 906-917, May 2007.

[62] H. Li, *et al.*, "OFDM modulation classification and parameters extraction," in *Proc. IEEE Int. Conf. Cognitive Radio Oriented Wireless Networks and Commun.*, 2006, pp. 1-6.

[63] M. Shi, Y. Bar-Ness, and W. Su, "Blind OFDM Systems Parameters Estimation for Software Defined Radio," in *Proc. IEEE Int. Symp. New Frontiers in Dynamic Spectrum Access Netw.*, 2007, pp. 119-122.

[64] Y. Kiong and M. Motani, "On implementation of link adaptation in OFDM wireless networks," in *Proc. IEEE Int. Conf. Commun.*, 2004, pp. 195-199.

[65] A. Punchihewa, V. K. Bhargava, and C. Despins, "Blind Estimation of OFDM Parameters in Cognitive Radio Networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 733-738, Mar. 2011.

[66] Q. Zhang, *et al.*, "Second-Order Cyclostationarity of BT-SCLD Signals: Theoretical Developments and Applications to Signal Classification and Blind Parameter Estimation," *IEEE Trans. Wireless Commun.*, accepted for publication.

[67] N. Kundargi and A. Tewfik, "Sequential Pilot Sensing of ATSC Signals in IEEE 802.22 Cognitive Radio Networks," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Process.*, 2008, pp. 2789-2792.

[68] J. E. Slat and H. H. Nquyen, "Performance Prediction for Energy Detection of Unknown Signals," *IEEE Trans. Veh. Technol.*, vol. 57, no. 6, pp. 3900-3904, Nov. 2008.

[69] N. Khambekar, L. Dong, and V. Chaudhary, "Utilizing OFDM Guard Interval for Spectrum Sensing," in *Proc. IEEE Wireless Commun. and Networking Conf.*, Mar. 2007, pp. 38-42.

[70] T. Yucek and H. Arslan, "OFDM Signal Identification and Transmission Parameter Estimation for Cognitive Radio Applications," in *Proc. IEEE Global Commun. Conf.*, Dec. 2007, pp. 4056-4060.

[71] N. Han, G. Zheng, S. H. Sohn, and J. M. Kim, "Cyclic autocorrelation based blind OFDM detection and identification for cognitive radio," in *Proc. IEEE Int. Conf. Wireless Commun., Networking and Mobile Computing*, Oct. 2008, pp. 1-5.

[72] S. Chaudhari, V. Koivunen and H. V. Poor, "Autocorrelation-Based Decentralized Sequential Detection of OFDM Signals in Cognitive Radios," *IEEE Trans. on Signal Process.*, vol. 57, no. 7, pp. 2690-2700, 2009.

[73] C. Cordeiro, M. Ghosh, Dave Cavalcanti and K. Challapali, "Spectrum Sensing for Dynamic Spectrum Access of TV Bands," in *Proc. IEEE Int. Conf. Cognitive Radio Oriented Wireless Networks and Communications*, 2007, pp. 225-233.

[74] N. Kundargi and A. Tewfik, "Sequential Pilot Sensing of ATSC Signals in IEEE 802.22 Cognitive Radio Networks," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Process.*, 2008, pp. 2789-2792.

[75] H. Li, X. Wang, C. Wang and J.-Y. Chouinard, "Robust Spectrum Sensing of OFDM Signal without Noise Variance Knowledge," in *Proc. IEEE Canadian Workshop Inform. Theory*, 2009, pp. 91-94.

[76] H.-W. Chen, X. Wang, C.-L. Wang and H. Lin, "Spectrum Sensing of Unsynchronized OFDM Signals for Cognitive Radio Communications," in *Proc. IEEE Veh. Technol. Conf.*, 2009, pp. 1-5.

[77] H.-S. Chen, W. Gao and D. G. Daut, "Spectrum Sesning for OFDM Systems Employing Pilot Tones," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5862-5870, Dec. 2009.

[78] Y. Li, "Pilot-Symbol-Aided Channel Estimation for OFDM in Wireless Systems," in *Proc. IEEE Veh. Technol. Conf.*, 1999, pp. 1131-1135.

[79] J. A. C. Bingham, "Multicarrier Modulation for Data Transmission," *IEEE Commun. Mag.*, vol. 28, no. 5, pp. 5-14, May 1990.

[80] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535-547, Mar. 2000.

[81] G. Bianchi and I. Tinnirello, "Kalman Filter Estimation of the Number of Competing Terminals in an IEEE 802.11 Network," in *Proc. IEEE Int. Conf. Comput. Commun.*, 2003, pp. 844-852.

[82] T. Vercauteren, A. L. Toledo, and X. Wang, "Batch and Sequential Bayesian Estimators of the Number of Active Terminals in an IEEE 802.11 Network," *IEEE Trans. Signal Process.*, vol. 55, no. 2, pp. 437-450, Feb. 2007.

[83] J. Yang, *et al.*, "Determining the Number of Attacks and Localizing Multiple Adversaries in Wireless Spoofing Attacks," in *Proc. IEEE Int. Conf. Comput. Commun.*, 2009, pp. 666-674.

[84] K.-Y. Sung and C.-C. Chao, "Estimation and Compensation of I/Q Imbalance in OFDM Direct-Conversion Receivers," *IEEE J. Sel. Topics Signal Process.*, vol. 3, no. 3, pp. 438-453, Jun. 2009.

[85] S. Traverso, *et al.*, "Decision-Directed Channel Estimation and High I/Q Imbalancxe Compensation in OFDM Receivers," *IEEE Trans. Commun.*, vol. 57, no. 5, pp. 1246-1249, May. 2009.

[86] Y. Tsai, C.-P. Yen, and X. Wang, "Blind Frequency-Dependent I/Q Imbalance Compensation for Direct-Conversion Receivers," *IEEE Trans. Wireless Commun.*, vol. 9, no. 6, pp. 1976-1986, Jun. 2010.

[87] Y.-C. Pan and S.-M. Phoong, "A Time-Domain Joint Estimation Algorithm for CFO and I/Q Imbalance in Wideband Direct-Conversion Receivers," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2353-2361, Jul. 2012.

[88] K. Ren, H. Su, and Q. Wang, "Secret Key Generation Exploiting Channel Characteristics in Wireless Communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6-12, Aug. 2011.

[89] P. Gopala, L. Lai, and H. E. Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-5698, Oct. 2008.

[90] Y. Liang, A. Somekh-Baruch, H. V. Poor, and S. Shamai, "Capacity of Cognitive Interference Channels With and Without Secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604-619, Feb. 2009.

[91] Z. Gao, Y. H. Yang, and K. J. R. Liu, "Anti-Eavesdropping Space-Time Network Coding for Cooperative Communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3898-3908, Nov. 2011.

[92] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[93] Y. Zou, X. Wang, and W. Shen, "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks," *IEEE J. Sel. Areas Commun.*, under 2nd round review.

[94] T. Li, J. Ren, Q. Ling, and A. Jain, "Physical Layer Built-in Security Analysis and Enhancement of CDMA SYstems," in *Proc. IEEE Military Commun. Conf.*, 2005, pp. 956-962.

[95] D. Klinc, *et al.*, "LDPC Codes for the Gaussian Wiretap Channel," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 3, pp. 532-540, Sept. 2011.

[96] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and Subcarrier Allocation for Physical-Layer Security in OFDMA-Based Broadband Wireless Networks," *IEEE Trans. Inf. Forens. Security*, vol 6, nop. 3, pp. 693-702, Sept. 2011.

[97] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-Efficient Resource Allocation for Secure OFDMA Systems," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2572-2585, Jul. 2012.

[98] R. Meyer and M. Newhouse, "OFDM Waveform Feature Suppression," in *Proc. IEEE Military Commun. Conf.*, 2002, pp. 582-586.

[99] X. Wang, P. Ho, and Y. Wu, "Robust Channel Estimates and ISI Cancellation for OFDM Systems with Suppressed Features," *IEEE J. Sel. Areas Commun.*, vol .23, no. 5, pp. 963-972, May 2005.

[100] T. Yucek and H. Arslan, "Feature Suppression for Physical-Layer Security in OFDM Systems," in *Proc. IEEE Military Commun. Conf.*, 2007, pp. 1-5.

[101] W.-J. Lin and J.-C. Yen, "An Integrating Channel Coding and Cryptography Design for OFDM based WALNs," in *Proc. IEEE Int. Symp. Consum. Electron.*, 2009, pp. 657-660.

[102] R. Ma, L. Dai, Z. Wang, and J. Wang, "Secure Communication in TDS-OFDM System Using Constellation Rotation and Noise Insertion," *IEEE Trans. Consum. Electron.*, vol. 56, no. 3, pp. 1328-1332, Aug. 2010.

[103] A. Chorti and H. V. Poor, "Faster than Nyquist Inference Assisted Secret Communication for OFDM Systems," in *Proc. IEEE Asilomar Conf. Signals, Systems and Comput.*, 2011, pp. 183-187.

[104] E. A. Jorswieck and A. Wolf, "Resource Allocation for the Wire-tap Multicarrier Broadcast Channel," in *Proc. IEEE Int. Conf. Telecommun.*, 2008, pp. 1-6.

[105] G. Caire, G. Taricco, and E. Biglieri, "Bit-Interleaved Coded Modulation," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 927-946, May 1998.

[106] J. Boutros and E. Viterbo, "Signal Space Diversity: A Power and Bandwidth-Efficient Diversity Technique for the Rayleigh Fading Channel," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1453-1467, 1998.

[107] K. V. Srinivas, *et al*, "Co-ordinate Interleaved Spatial Multiplexing with Channel State Information," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 2755-2762, Jun. 2009.

[108] C. Yoon, H. Lee, and J. Kang, "Performance Evaluation of Space-Time Block Codes from Coordinate Interleaved Orthogonal Designs in Shadowed Fading Channels," *IEEE Trans. Veh. Technol.*, vol. 60, no. 3, pp. 1289-1295, Mar. 2011.

[109] J. Harshan and B. S. Rajan, "Co-ordinate Interleaved Distributed Space-Time Coding for Two-Antenna-Relays Networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1783-1791, Apr. 2009

[110] O. Oruc and U. Aygolu, "Bandwodth-Efficient Code Design for Coordinate Interleaved Coded Cooperation," *IET Commun.*, vol. 3, no. 9, pp. 1509-1519, Sept. 2009.

[111] S.-K. Kim and H.-G. Ryu, "Co-ordinate Interleaving in the OFDM System and Performance Improvement in Fading Channel," in *Proc. IEEE Asia-Pacific Conf. Commun.*, 2008. pp. 1-5.

[112] Y. E. H. Shehadeh, O. Alfandi, and D. Hogrefe, "Towards Robust Key Extraction from Multipath Wireless Channels," *IEEE J. Commun. Netw.*, vol. 14, no. 4, pp. 385-394, Aug. 2012.

[113] M. K. Simon, *Probability Distributions Involving Gaussiam Random Variables*, Springer, 2006.

[114] W. Y. Zou and Y. Wu, "COFDM: An Overview," *IEEE Trans. Broadcast.*, vol. 41, no. 1, pp. 1-8, Mar. 1995.

[115] S.-W. Lei and V. K. N. Lau, "Performance Analysis of Adaptive Interleaving for OFDM Systems," *IEEE Trans. Vel. Technol.*, vol. 51, no. 3, pp. 435-444, May 2002.

[116] A. Filippi and E. Costa, "Low-Complexity Interleaved Subcarrier Allocation in Multicarrier Multiple-Access Systems," *IEEE Trans Commun.*, vol. 55, no. 1, pp. 35- 39, Jan. 2007.

[117] A. D. S. Jayalath and C. Tellambura, "The Use of Interleaving to Reduce the Peak-to-Average Power Ratio of and OFDM Signal," in *Proc. IEEE Global Commun. Conf.*,Dec. 2000, pp. 82-86.

[118] P. Mukunthan and P. Dananjayan, "PAPR Reduction by Modified PTS Combinaed with Interleaving Technique for OFDM System with QPSK Subcarriers," in *Proc. IEEE Int. Conf. Advances in Eng., Sci. and Manage.*, Mar. 2012, pp 410-415.

[119] M. K. Ozdemir and H. Arslan, "Channel Estimation for Wireless OFDM Systems,", *IEEE Commun. Surv. Tut.*, vol. 9, no. 2, pp. 18-48, 2007.

[120] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High Rate Uncorrelated Bit Extraction for Shared Secrect Key Generation from Channel Measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17-30, Jan. 2010.

[121] H. A. David, "Order Statistics," New York:Wiley, 1981.

[122] M. K. Simon and M.-S. Alouini, "On the Difference of Two Chi-Square Variates with Application to Outage Probability Computation," *IEEE Trans. Commun.*, vol. 49, no. 11, pp. 1946-1954, Nov. 2001.

[123] M.-S. Alouini, X. Tang, and A. J. Goldsmith, "An Adaptive Modulation Scheme for Simultaneous Voice and Data Transmission over Fading Channels," *IEEE J. Sel. Areas in Commun.*, vol. 17, no. 5, pp. 837-850, May 1999.

[124] Md. J. Hossain, *et al.*, "Adaptive Hierarchical Modulation for Simultaneous Voice and Multiclass Data Transmission over Fading Channels," *IEEE Trans. Vel. Technol.*, vol. 55, no. 4, pp. 1181-1194, Jul. 2006.

[125] S. Chen and H. Leung, "Concurrent Data Transmission Through Analog Speech Channel Using Data Hiding," *IEEE Signal Process. Lett.*, vol. 12, no. 8, pp. 581-584, Aug. 2005.

[126] J. Kim and D.-H. Cho, "Simulataneous Transmission of MAP IE and Data for Minimizing MAC Overhead in IEEE 802.16e OFDMA Systems," *IEEE Trans. Wireless Commun.*, vol. 8, no. 11, pp. 5431-5435, Nov. 2009.

[127] P. Zhao, *et al.*, "Performance of a Concurrent Link SDMA MAC under Practical PHY Operating Conditions," *IEEE Trans. Vel. Technol.*, vol. 60, no. 3, pp. 1301-1307, Mar. 2011.

[128] S. Ma, X. Pan, G. Yang, and T. Ng, "Blind symbol synchronization based on cyclic prefix for OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1746-1751, May 2009.

[129] A. Filippi and S. Serbetli, "OFDM symbol synchronizationn using frequency domain pilots in time domain," *IEEE Trans. Wir. Commun.*, vol. 8, no. 6, pp. 3240-3248, Jun. 2009.

[130] X. Wang, P. Ho, and Y. Wu, "Robust channel estimation and ISI cancellation for OFDM systems with suppressed features," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 5, pp. 963-972, May, 2005.

[131] B. Muquet, Z. Wang, G. B. Giannakis, M.D. Courville, and P. Duhamel, "Cyclic prefixing or zero padding for wireless multicarrier transmissions," *IEEE Trans. Commun.*, vol. 50, no. 12, pp. 2136-2148, Dec. 2002.

[132] P. Fan and M. Darnell, *Squence Design for Communications Applications*, John Wiley & Sons, 1996.

[133] D. Torrieri, *Principles of Spread-Spectrum Communication Systems*, Springer, 2006.

[134] K. Yang, Y.-K. Kim, and P. V. Kumar, "Quasi-Orthogonal Sequences for Code-Division Multiple-Access Systems," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 982-993, May 2000.

Curriculum Vitae

NAME:	Hao Li
POST-SECONDARY EDUCATION AND DEGREES:	The University of Western Ontario London, Ontario, Canada Jan. 2010 - date Ph.D. candidate
	The University of Western Ontario London, Ontario, Canada Sept. 2008 - Dec. 2009 M.E.Sc.
	University of Electronic Science and Technology of China Chengdu, Sichuan, P.R.China Sept. 2004 - Jul. 2008 B.E.Sc. (Hons)
RELATED WORK EXPERIENCE:	Teaching Assistant The University of Western Ontario Sept. 2008 - date
	Research Assistant The University of Western Ontario Sept. 2008 - date

Publications:

International Refereed Journals:

[1] H. Li, X. Wang, and Y. Zou, "Subcarrier Coordinate Interleaving for Eavesdropping Prevention in OFDM Systems," submitted to *IEEE Transactions on Wireless Communications*.

[2] H. Li, X. Wang, Y. Zou, and J.-Y. Chouinard, "Eavesdropping-Resilient OFDM System Using Dynamic Subcarrier Interleaving," submitted to *IEEE Transactions on Information Forensics and Security*.

[3] H. Li, X. Wang, and J. Nadeau, "Robust Spectrum Sensing for Orthogonal Frequency Division Multiplexing Signal without Synchronization and Prior Noise Knowledge," *Wireless Communications and Mobile Computing*, DOI: 10.1002/wcm.2221, Mar. 2012.

[4] X. Wang, H. Li, and H. Lin, "A New Adaptive OFDM System with Precoded Cyclic Prefix for Dynamic Cognitive Radio Communications," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 2, pp. 431-442, Feb. 2011.

[5] C. Wang, X. Wang, and H. Li, "Fundamental Limitations on Pilot-based Spectrum Sensing at Very Low SNR," *Wireless Personal Communications*, DOI: 10.1007/s11277-011-0362-z, 2011.

International Conferences:

[1] H. Li, X. Wang, and Y. Zou, "Exploiting Transmitter I/Q Imbalance for Estimating the Number of Active Users," accepted by *2013 IEEE Global Communications Conference*.

[2] H. Li, X. Wang, Y. Zou, and W. Hou, "Eavesdropping-Resilient OFDM System Using CSI-based Dynamic Subcarrier Allocation," accepted by *2013 IEEE Vehicular Technology Conference - Spring*.

[3] C. Wang, X. Wang, and H. Li, "Enhanced Two-step Spectrum Sensing Algorithm for OFDM Signal," in *Proc. IEEE Canadian Conference on Electrical and Computer Engineering*, May 2011.

[4] H. Li, X. Wang, and J.-Y. Chouinard, "Robust Spectrum Sensing and User Identification for PCP-OFDM Signal Using Noise Insensitive Threshold," in *Proc. IEEE Vehicular Technology Conference - Fall*, Sept. 2010.

[5] X. Wang, H. Li, S. Primak, and V.-H. Pham, "A Low Complexity Time Domain Spectrum Sensing Technique for OFDM (Invited Paper)," in *Proc. International Conference on Communications and Networking in China*, Aug. 2010.

[6] C. Wang, X. Wang, H. Li, and P. Ho, "Multi-window Spectrum Sensing of Unsynchronized OFDM Signal at Very Low SNR," in *Proc. IEEE Global Communications Conference*, Dec. 2009.

[7] H. Li, X. Wang, C. Wang, and J.-Y. Chouinard, "Robust Spectrum Sensing of OFDM Signal without Noise Variance Knowledge," in *Proc. IEEE Canadian Workshop on Information Theory*, May 2009.

Internal Technical Reports:

[1] X. Wang, H. Li, and J. Nadeau, "Situation Aware Rate Adaptation (SARA) Algorithm for IEEE 802.11 using both Long-Term and Short-Term Communication Performance and Environment Monitoring," project report prepared for TELOIP Inc., Aug. 2012.

[2] X. Wang, V.-H. Pham, H. Li, and J. Nadeau, "A Reactive Rate Adaptation Algorithm for 802.11 using both Long-Term and Short-Term Link Performance Indicators," project report prepared for TELOIP Inc., Sept. 2011.

[3] X. Wang, V.-H. Pham, J. Nadeau, H. Li, and T. Zhou, "An Effective Rate Adaptation Algorithm for 802.11 using both Long-Term and Short-Term Communication Performance and Environment Monitoring (II)," project report prepared for TELOIP Inc., May 2011.

[4] X. Wang, V.-H. Pham, J. Nadeau, H. Li, and T. Zhou, "An Effective Rate Adaptation Algorithm for 802.11 using both Long-Term and Short-Term Communication Performance and Environment Monitoring (I)," project report prepared for TELOIP Inc., Feb. 2011.

[5] X. Wang, H. Li, and G. Liu, "Multi-Stage Signal Detection and Identification in Watchdog Sensor Network," project report prepared for Defence Research and Development Canada (DRDC), Apr. 2011.

[6] X. Wang, G. Liu, H. Li, J. Nadeau, and W. Hou, "A Survey of Wireless Communication Standards and Signal Sensing / Identification Techniques," project report prepared for Defence Research and Development Canada (DRDC), Feb. 2011.