September 2013

Physical-Layer Security Enhancement in Wireless Communication Systems

Hao Li
The University of Western Ontario

Supervisor
Dr. Xianbin Wang
The University of Western Ontario

PHYSICAL-LAYER SECURITY ENHANCEMENT IN WIRELESS COMMUNICATION SYSTEMS

(Thesis format: Monograph)

by

Hao Li

Graduate Program in Engineering Science Electrical and Computer Engineering

A thesis submitted in partial fulfillment
of the requirements for the degree of
Masters of Engineer Science

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

Abstract

Without any doubt, wireless infrastructures and services have fundamental impacts on every aspect of our lives. Despite of their popularities, wireless communications are vulnerable to various attacks due to the open nature of radio propagation. In fact, communication security in wireless networks is becoming more critical than ever. As a solution, conventional cryptographic techniques are deployed on upper layers of network protocols. Along with direct attacks from lower layer, wireless security challenges come with the rapid evolution of sophisticated decipher techniques. Conventional security mechanisms are not necessarily effective against potential attacks from the open wireless environment anymore. As an alternative, physical-layer(PHY) security, utilizing unique features from lower layer, becomes a new research focus for many wireless communication systems.

In this thesis, three mechanisms for PHY security enhancement are investigated. Beginning with a discussion on the security vulnerability in highly standardized infrastructures, the thesis proposed a time domain scrambling scheme of orthogonal frequency division multiplexing (OFDM) system to improve the PHY security. The method relies on secretly scrambling each OFDM symbol in time domain, resulting in constellation transformation in frequency domain, to hide transmission features. As a complement to existing secrecy capacity maximization based optimal cooperative jamming systems, a security strategy based on the compromised secrecy region (CSR) minimization in cooperative jamming is then proposed when instantaneous channel state information(CSI) is not available. The optimal parameters of the jammer are derived to minimize the CSR which exhibits high secrecy outage probability. At last, security enhancement of OFDM system in cooperative networks is also investigated. The function selection strategies of cooperative nodes are studied. Our approach is capable of enhancing the security of broadband communications by selecting the proper function of each cooperative node. Numerical results demonstrate the feasibility of three proposed physical layer security mechanisms by examining the communication reliability, achievable CSR and secrecy capacity respectively.

Keywords: physical layer security, OFDM, time domain scrambling,secrecy region, cooperative network

"A man can be destroyed but not defeated."

— Ernest Hemingway

Acknowledgments

I have taken efforts in pursuing for my master degree in the University of Western Ontario. However, it would not have been possible without the kind support and selfless help from many people. I would like to extend my sincere thanks to all of them.

I am highly indebted to my supervisor, Dr. Xianbin Wang, for his guidance and constant supervision as well as providing necessary and helpful information during the my study. Without help from Dr. Wang, this thesis could never be completed. His spirit of earnest and preciseness towards research inspire me all the time. I would like to express my gratitude to Dr. Wang for the fruitful and enjoyable experience learning from him.

Sincere thanks to Dr. R.K. Rao, Dr. Serguei L. Primak and Dr. Wenxing Zhou for sparing their precious time reading my thesis and serving as my examination committee.

I am also grateful to my colleague, Dr. Weikun Hou, for his countless and selfless help since the very first day I arrived at Western. From the very beginning flashing point of a research idea to the final paper submission at the last minute, with guidance from him, I always feel confident to overcome every difficulty in my research. Here, I would like to express my earnest thankfulness to Dr. Hou for all the help he has provided in the past two years.

I would like to thank my colleague, Dr. Hao Li, my so called "big brother", for all the tips about studying and living he provides. Also, deep thanks to all other colleagues, Dr. Ahmed Refaey, Dr. Yulong Zou, Jiazi Liu, Xin Gao, Peng Hao, Yitong Chen, Kai Liu, Yu He and Fuad Shamieh. It's of a great pleasure to work with them.

I would like to thank every staff in the university for their service. I would like to extend my thanks to all friends I have met in Canada for helping me when I was in trouble and bearing with me when I made mistakes.

Last but most importantly, I owe infinite gratitudes to my dearest parents who are thousands of miles away in my home country. For all these years, I could have achieved nothing without world's strongest support to me from them. Sorry for not being able to spend time with them in the past two years. I deeply appreciate their understanding and support.

Contents

Abstract ii

Acknowledgments iv

List of Figures vii

List of Abbreviations ix

1 Introduction 1
- 1 Motivations . . . 3
- 2 Research Objectives . . . 4
- 3 Contributions . . . 6
- 4 Thesis Outlines . . . 6

2 Background 8
- 1 Wireless Network Security . . . 8
  - 1.1 Security Attacks in Wireless Networks . . . 9
  - 1.2 Wireless Network Security Properties . . . 10
  - 1.3 Security Mechanisms . . . 11
    - 1.3.1 Cryptography in wireless networks . . . 11
    - 1.3.2 PHY Security Mechanisms in Wireless Networks . . . 16
  - 1.4 Brief Summary of the Section . . . 20
- 2 Orthogonal Frequency Division Multiplexing (OFDM) System . . . 20
  - 2.1 System Structure of OFDM . . . 22
  - 2.2 Mathematical Description of OFDM Infrastructure . . . 24
  - 2.3 Multi-path Effects and Cyclic Prefix . . . 25
    - 2.3.1 Multipath Effects . . . 25
    - 2.3.2 Cyclic Prefix . . . 28
  - 2.4 OFDM Interleaving . . . 31
    - 2.4.1 Frequency Domain Interleaving . . . 31
    - 2.4.2 Time-domain Interleaving . . . 32
    - 2.4.3 Bit-Interleaved OFDM . . . 32
    - 2.4.4 Symbol-interleaved OFDM . . . 33
  - 2.5 Brief Summary of the Section . . . 33
- 3 Cooperative Jamming . . . 34

3.1 Secrecy Capacity . . . 34
3.2 Cooperative Jamming System . . . 37
3.3 Brief Summary of the Section . . . 38
4 Chapter Summary . . . 39

3 Secure Transmission in OFDM System by Using Time Domain Scrambling 40
1 Introduction . . . 40
2 Conventional OFDM System . . . 42
3 Security Enhanced Time Domain Scrambling OFDM System . . . 43
3.1 System Description . . . 43
3.2 Constellation Transformation . . . 45
4 Secrecy Capacity . . . 51
5 Time Synchronization . . . 54
5.1 Time Offset Analysis . . . 54
5.2 Time Offset Compensation . . . 56
5.3 Application Example . . . 57
6 Simulations . . . 57
7 Chapter Summary . . . 64

4 Security Enhancement in Cooperative Jamming Using Compromised Secrecy Region Minimization 65
1 Introduction . . . 65
2 System Setup and Secrecy Region Derivation . . . 66
2.1 System Model . . . 67
2.2 Secrecy Capacity, Outage Probability and Secrecy Region . . . 67
3 Compromised Secrecy Region Minimization . . . 71
3.1 Outage Probability Approximation . . . 72
3.2 Compromised Secrecy Region Minimization Algorithm . . . 73
4 Simulations . . . 75
5 Chapter Summary . . . 81

5 Function Selection Strategy of Cooperative Node for Security Enhancement 82
1 Introduction . . . 82
2 System Formulation . . . 84
3 Function Selection Strategies of $R|J$ Node for Security Enhancement . . . 88
3.1 Mutual Exclusive $R|J$ Node Selection . . . 88
3.2 Coexistent $R|J$ Node Selection . . . 90
4 Simulations . . . 92
5 Chapter Summary . . . 96

6 Conclusions 97

Bibliography 99

Curriculum Vitae 104

List of Figures

2.1 A depiction of public (asymmetric) key encryption cryptography. 12
2.2 Description of private-key cryptography. 15
2.3 AES encryption of 10 rounds of processing for 128-bit key generation. 16
2.4 Spectrum efficiency comparison between frequency division multiplexing (FDM) and orthogonal frequency division multiplexing (OFDM). 21
2.5 System diagram of OFDM transmitter. 23
2.6 System diagram of OFDM receiver. 24
2.7 Waveforms of OFDM sub-carriers in time domain. 26
2.8 An example of single sub-carrier in frequency domain. 26
2.9 An example of orthogonal sub-carriers in frequency domain. 27
2.10 Illustration of multi-path effect. (a) Delays of signal caused by multi-path in time domain. (b) Frequency selective fading caused by multi-path effect. 29
2.11 Inter-Symbol Interference in OFDM system caused by multi-path effect of wireless channel. 30
2.12 Cyclic prefix (CP) insertion principle. 31
2.13 Communication system infrastructure with the existence of a wiretap channel. . 34
2.14 An illustration of cooperative jamming system structure. 37

3.1 Conventional OFDM system diagram. 42
3.2 Security enhancement based on time domain scrambling in OFDM systems. . . 44
3.3 Block diagram of the time domain scrambling security-enhanced OFDM 44
3.4 An illustration of the permutation function R. 46
3.5 Generation of constellation pattern by means of constellation transformation with mode A and phase Θ. 49
3.6 Scrambled constellation patterns of a BPSK modulation in time domain scrambling OFDM system. 52
3.7 BPSK constellations of legitimate and illegitimate receiver over AWGN channel under SNR=4,8,12 dB(From left to right). 58
3.8 BER performance of the proposed time domain scrambling security-enhanced OFDM system over AWGN channel. 60
3.9 BER performance of BPSK and QPSK modulations for the proposed time domain scrambling security-enhanced OFDM system over Rayleigh channel. . . . 61
3.10 Simulation results for time domain synchronization. 62
3.11 Simulation results for time domain synchronization (Continued). 63

4.1 System diagram of cooperative jamming with one jammer. 67

4.2 Demonstration of the secrecy region map. The simulation model is constructed under $c = 1$, $\alpha = 4$, $R = 0$ and $d_{tj} = d_{tr} = 75m$. 69
4.3 Example of the restricted boundary in the secrecy region map with a numerical overflow problem. The simulation parameters used are based on $c = 1$, $\alpha = 4$, $R = 0$ and $d_{tj} = d_{tr} = 1km$. 74
4.4 Golden section search algorithm 76
4.5 Area of CSR versus distance ratio ρ with different included angles θ. The power ratio $\rho = 1$. 77
4.6 Illustration of the relationship between area of CSR A_c versus distance ratio ρ and included angles θ. The power ratio $\rho = 1$. 78
4.7 Area of CSR A_c versus the distance ratio ρ with different power ratios μ. The included angle $\theta = 1\pi$. 79
4.8 Area of CSR A_c versus the power ratio μ with different distance ratio ρ. The included angle $\Theta = 1\pi$. 80

5.1 The scenario for the proposed secure OFDM transmission scheme with the assistance of multiple $R|J$ nodes. 84
5.2 Best secrecy achieved by different number of (0,1/2,1) $R|J$ nodes. 93
5.3 Comparison of the best secrecy capacity achieved by different selection strategy with two $R|J$ nodes. 94
5.4 Comparison of the best secrecy capacity achieved by different selection strategy with five $R|J$ nodes. 95

List of Abbreviations

ACDM	Algebraic Channel Decomposition
ADSL	Asymmetric Digital Subscriber Line
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CP	Cyclic Prefix
CSI	Channel State Information
CSR	Compromised Secrecy Region
DAB	Digital Audio Broadcasting
DES	Data Encryption Standard
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
DVB	Digital Video Broadcasting
ECB	Electronic Code Book
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
GI	Guard Interval
GPS	Global Positioning System
ICI	Inter-Carrier Interference
IFFT	Inverse Fast Fourier Transform
LTE	Long Term Evolution
MAC	Media Access Control
OFB	Output Feedback
OFDM	Orthogonal Frequency Division Multiplexing
PAPR	Peak to Average Ratio
PDA	Personal Digital Assistant
PHY	Physical Layer
PSK	Phase Shift Keying
QAM	Quadrature Amplitude Modulation
VDSL	Very High Bit Rate Digital Subscriber Line
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

Chapter 1

Introduction

Since the very first day Guglielmo Marconi[1] succeeded in long distance radio transmission across the Atlantic Ocean in 1901, the constant and rapid evolution of wireless communications has shown its invaluable potential. From early day's radio and telegraph to today's long-term evolution (LTE) standard of mobile communications, each milestone of the evolution witnesses the significant moment of human beings' social development. The benefits of wireless communications are everywhere. A reconnaissance update by a scout through telegraph may affect the outcome of a battle; a remote access to medical records by medical personnel at site of accident could save a life; a timely phone call to a stock exchange may bring forth a millionaire. As one of the most influential technology evolutions in history, wireless communication is also becoming as an important component of our daily lives nowadays as they are increasingly deployed in numerous applications. Countless applications, such as cellular telephones, personal digital assistants (PDAs), global positioning system (GPS), wireless keyboard, headsets, headphones and so on, have been deployed, all thanks to the development of wireless communications technologies. From social activities to the basic house-hold need, wireless communications, without any doubt, offer us a more convenient and innovative way of life style than ever before.

However, as the incredible popularity makes it become the observed of all observers, many new challenges to wireless communications have emerged. Due to the broadcast nature of radio signal propagation, growing concerns have been raised for the inherent security vulnerability in wireless networks. Anyone within the network coverage of an open, unencrypted wire-

less network is capable of passively eavesdropping the content of the transmission. Moreover, malicious attackers can also launch aggressive attacks to disrupt or manipulate the legitimate transmissions. Specifically speaking, wireless communication is vulnerable to several kinds of threats such as identity theft, network injection, eavesdropping and jamming. The malfunction of any wireless communication system caused by those security challenges may lead to disasters because of the important role it plays in our daily lives. Therefore, it is extremely important to protect the wireless transmissions from any undesired damages.

Unfortunately, provisioning of wireless security is more challenging than that in wire-line networks. The closed transmission environment of wire-line networks provides a relatively easier way for security provisioning. Nevertheless, because of the open nature of wireless mediums, ensuring wireless security is never easy due to the dynamically varying transmission environments. Fortunately, for years, researchers have developed various methods to secure the wireless transmissions. Most commonly implemented methods rely on cryptographic technologies on upper layers[2]. Existing security mechanisms, such as wired equivalent privacy (WEP) and WiFi protected access (WPA)[3], are mainly based on medium access control (MAC)-layer security. The fundamental principles of these schemes are using symmetric or asymmetric cryptographic techniques to encrypt signals. However, the security level of such mechanisms depends on the complexity of the secret key used for encryption. With rapidly increasing computational capability of computers following Moore's law[4], cracking methods are becoming much more sophisticated and innovative. Different security risks associated with the current MAC layer security schemes occur everyday. For example, WEP has become a notoriously weak security standard as the password it uses can simply be cracked in a few minutes with a basic laptop computer and widely available software tools. To improve the security, the length and complexity of the secret key needs to be increased such as WPA2 with a 256-bit key compared with 64 bits used in WEP. The problem is that the longer the key is, the more complicated and less efficient the system will be. The trade-off among security, cost and efficiency is by no means an easy problem to solve so far.

As an alternative, physical layer (PHY) security mechanism inspired by Wyner's wire-tap channel theory[5] has been explored recently. It relies on enhancing the secrecy capacity, which is the capacity difference between main channel and wiretap channel[6], to secure the wireless

transmission. Instead of using digital secret keys, it utilizes various non-replicable features of channel conditions and attributes of signals for security enhancement. Those physical features are used and optimized to increase the capacity of legitimate transmission channels and decrease the capacity of illegitimate transmission channels. The security can be guaranteed when maximized secrecy capacity, enlightened by Shannon's perfect secrecy theorem[7], is achieved. Regarding its advantages, PHY security mechanism does not require complicated encryption in the meantime physical features exploited are also difficult to counterfeit during transmission. In addition, a fascinating point of the PHY security mechanism is its diversity. According to the property of physical features and variety of system structures, unique and specialized security scheme can be implemented specifically to each system. The diversity and unpredictability of PHY approaches compensate the shortcomings brought by the highly standardized cipher based encryption on upper layer. Therefore, the PHY security mechanism flourishes in many wireless communication systems for its simplicity, variety and flexibility.

1 Motivations

In this section, motivations of this thesis are presented considering PHY security challenges in two practical wireless communication systems: orthogonal frequency division multiplexing (OFDM) system and cooperative network.

OFDM has been considered as a fundamental transmission technique for broadband communication systems. Its advantages, such as high efficiency of spectrum usage by allowing subcarrier overlaps, elimination of inter-symbol interference (ISI) and low sensitivity to time synchronization errors, make this technology attractive for broadband wireless communications. As a promising system, OFDM has been employed in various wireless standards like digital audio broadcasting(DAB), digital vdieo networks(DVB), wireless local area networks(WLAN) and wireless metropolitan area networks(WMAN). Nevertheless, standardized system features like cyclic prefix (CP), preambles and distinct spectrum characteristics may also reveal transmission details to potential eavesdroppers and attackers. The vulnerability of standardized system leaves a back door for the undesired who are familiar with OFDM system to sneak in. Therefore, in order to solve such problems, the distinct features in OFDM signals

need to be canceled. The first part of this thesis is focused on the PHY security mechanisms to block these back doors and enhance the security of OFDM system.

In addition, as an effective system for PHY security enhancement, cooperative jamming is widely implemented recently by utilizing channel spatial diversity and network cooperation [8]. The principle of cooperative jamming system is straight forward. During the source transmitting signal to the destination, a cooperative node simultaneously sends out a jamming signal to interfere eavesdropper. In doing so, the transmission security can be improved by increasing the secrecy capacity. For this reason, the conventional objective for cooperative jamming optimization aims at maximizing the system secrecy capacity. However, due to the random distribution of the eavesdropper and eavesdropper's intention not to be discovered by the legitimate transmission system, it is sometimes impractical to obtain the instantaneous channel information from illegitimate channel when the system parameters need to be optimized. Motivated by this, the second part of the thesis considers an alternative methodology of cooperative jamming optimization to deal with practical difficulty during system optimization.

As two popular wireless communication systems, cooperative networks and OFDM system have been converged in recent studies. High efficiency of spectrum usage offered by OFDM signal and reliable transmission rates provided by cooperative network make this combination a win-win situation for system performance. However, due to the wide-band spectrum that OFDM signals occupy and wide-range distributions of cooperative relay nodes, security threats also become much more complicated. Malicious attackers have more chances to break into the communication through any unsecured subcarrier channel or cooperative node. It is of a great need to investigate the security mechanism against potential security risks towards this combination. Motivated by this challenge, the last part of this thesis emphasizes on security strategies for the cooperative OFDM system to enhance its security level at physical layer.

2 Research Objectives

Due to the security vulnerability of wireless communications on PHY, the main research objectives in this thesis are to develop PHY security enhancement mechanisms specifically in the OFDM system and cooperative networks.

Our objective for the OFDM system is to develop a security mechanism to change and cancel the spectral characteristics of OFDM signals and increase the difficulties of signal interception on eavesdropper side. The first consideration is to alternate the highly standardized system feature. Since OFDM signals are transmitted over a large number of subcarriers, the simplest way is to secure the transmitted information by scrambling or interleaving these OFDM symbols. Existing mechanisms in literatures [9] interleave the data in frequency domain. The challenge is that the spectral characteristic of the OFDM signals is not necessarily changed. Malicious attackers still can intercept the transmission by analyzing the OFDM spectral feature and apply corresponding demodulation and decoding techniques. Other works [10] [11] apply phase shift and noise insertion to signal's constellation. Although this could be an effective method of alternating the feature of OFDM signals in frequency domain, the increased complexity for interception is still relatively low as eavesdropper may decode the phase shifted signal in a reverse order. In order to overcome these problems, our scheme should change not only the phase angle but also the amplitude of signal constellation.

In addition, for cooperative jamming system, our goal is to provide a statistical criterion in evaluating the system's security when short-term channel information is difficult to obtain. Despite that numerous works[12][13][14] have been dedicated in cooperative jamming optimization based on the principle of secrecy capacity maximization, most of them assume a pre-known instantaneous channel state information (CSI) of illegitimate channel. However, in reality, this is never an easy job. The difficulty in gaining short-term CSI of illegitimate channel leads to the problem of calculating channel capacity. Inspired by the work of [15] which utilized the statistical CSI to characterize the secrecy region in a small scale jamming system, we propose a criterion which is targeted to become a supplement of secrecy capacity maximization. It also has to be relatively generic solution to different cooperative system models.

Last but not least, we also aim at enhancing the security of OFDM system in cooperative networks by using best relay-jammer nodes selection strategies. Although some works [16][17] have investigated the security enhancement in cooperative networks, most of them only considered flat fading channel models. In reality, scenarios such as wide-band and frequency selective fading are much more complicated. Hence, we are focusing on analyzing

the system's security in situation of multi-subcarriers of OFDM signal and providing effective cooperative nodes selection strategies to maximize the system's security level.

3 Contributions

The main contributions of this thesis are summarized as follows:

- A time domain scrambling OFDM system to enhance the PHY security is proposed in Chapter 3. With the scrambled time domain OFDM signal, both frequency and time domain features of transmitted signal are covered. The inherent effect of the time domain scrambling OFDM signal is studied by analyzing the constellation transformation effect of the proposed scrambling OFDM system. The analytical and numerical results show the proposed scheme not only changes the phase angle but also changes the amplitudes of the signal's constellation.

- A security enhancement scheme in cooperative jamming system by using compromised secrecy region minimization is proposed in Chapter 4. With the minimized secrecy region statistically calculated from secrecy outage probability, the proposed scheme can evaluate and optimize the system without the necessity of knowing the exact position of eavesdropper. The outage probability approximation is implemented to solve the practical boundary problem in large scale system model. A searching algorithm is also performed to determine the minimum area value of the compromised secrecy region.

- Function selection strategy of cooperative node to enhance PHY security of OFDM system is proposed in Chapter 5. With proper selection of cooperative nodes' function, security of OFDM system in cooperative networks is maximized. Two selection strategies of different types of cooperative nodes, mutual exclusive and coexistent nodes, are analyzed and compared considering the security improvement.

4 Thesis Outlines

The rest of this thesis is organized as follows:

Chapter 2 describes the overall background information related to and used in the following chapters of the thesis. In the first section, literature survey and brief introduction to the wireless security have been presented. The second section introduces the basic knowledge of OFDM system including the structure of OFDM transceivers, mathematical descriptions and existing works on OFDM interleaving techniques. The final section of this chapter contains the introduction to the cooperative jamming system and the definition of secrecy capacity as well.

In Chapter 3, a time domain scrambling OFDM system is discussed in details. The comparison between conventional OFDM system and the proposed scheme is investigated. The analysis on the proposed scheme is studied including the constellation transformation effect, secrecy capacity increment and time synchronization problems. The simulation results supporting the proposed scheme are also provided.

In Chapter 4, a PHY security enhancement using compromised secrecy region minimization in cooperative jamming system is presented. The derivation of the secrecy region using secrecy outage probability is studied at first. Also, practical solution to boundary problem in drawing the secrecy map is introduced. A searching algorithm is implemented to find out the minimum of compromised secrecy region as well. The simulation results demonstrate the feasibility of evaluating the system's security by finding out the minimized compromised secrecy region.

In Chapter 5, function selection strategy of cooperative node to enhance security of OFDM system is proposed. The system formulation of OFDM system in cooperative network with several hybrid jammer and relay nodes is discussed. Two selection strategies to maximize the secrecy capacity of the system are provided. Numerical results to compare different strategies under various conditions are also given out.

Finally, Chapter 6 concludes all the key information appeared in previous chapters. In addition, some potential improvements of current works and future works to be finished are discussed as well.

Chapter 2

Background

In this chapter, technical background information related to this thesis is provided. In the first section, a literature survey of current wireless network security issues is conducted. Various wireless security risks and existing security provisioning mechanisms are reviewed. In the second section, the principle of orthogonal frequency division multiplexing (OFDM) system is introduced. In the third section, the mechanism of the cooperative jamming system is presented including the theorem of secrecy capacity.

1 Wireless Network Security

Due to the broad deployment of various wireless applications, wireless networks are becoming more and more important not only in military but also in civil applications. Military organizations highly rely on wireless communications such as exchanging information for various military operations. Meanwhile, ordinary people count on wireless infrastructures for many different things in daily life from reading news to credit card transactions. The widespread use of wireless network therefore requires information security and stability during the transmission. However, because of the broadcast nature of wireless transmission in the open air, it is, at least theoretically, accessible for all communication devices within the communication range to intercept and obtain any wireless transmission signals in the wireless medium. Therefore, the potential vulnerability of wireless networks may result in different kinds of attacks which can do harm to the legitimate transmission.

1.1 Security Attacks in Wireless Networks

Most wireless security attacks can be classified into passive attacks and active attacks. Passive attacks , which can be described as silently stealing transmitted information from wireless media, do not interrupt legitimate transmission. On the other side, active attacks, which use more aggressive intrusion techniques, often break or damage the legitimate transmissions.

Passive Attacks

- Monitor & Eavesdropping: The most common attack in wireless networks is monitoring and eavesdropping. The malicious attacker can intercept and recover the communication contents by passively listening to the communication.

- Traffic Analysis: Although the transmission can be encrypted to prevent from being decoded, the attacker can still determine the locations and identities of the communicating parties by analyzing the communication patterns[18].

- Camouflage Adversaries: Attackers hide as one of the dummy nodes in the network to trick the legitimate transmission partners to believe that it legitimately belongs to them. By doing this, the hidden node can behave as a part of normal system and intercept the transmission contents[19].

Active Attacks

- Denial of Service (DoS) Attack: The malicious attackers may launch attacks to exhaust the resources available to the legitimate transmissions[20]. As a result, no service will be available to the normal transmission. Jamming is one of the most widely used approaches to launch DoS attack. The wireless frequency spectrum is occupied by the jamming signals which makes the attacked communicating system has no spectrum resources to transmit their original contents.

- Routing Attacks: Routing attacks are generally launched at the network layer. By using routing attacks, a malicious node can prevent itself as one of legitimate relay node in the system[2]. However, the malicious node does not faithfully forward every detail of

the information that one legitimate rely node is supposed to do. It drops some part of the crucial information, manipulate some non-existing content and pass it on to the next node which in many cases will cause the entire system out of order or being deceived.

- Node Malfunction Attacks: Malicious attackers may launch attempts to capture one of the system's node to reveal the information included in it such as the cryptographic keys and transmission protocols[19]. In addition, attackers can utilize this kidnapped node to transmitted fake and inaccurate data which can damage the whole network.

1.2 Wireless Network Security Properties

As many wireless security attacks introduced above, a safe wireless network requires the following properties to mitigate any malicious incoming attacks.

- Integrity: Integrity stands for that the data from the source node should arrive at the destination node without being tampered[6]. A reliable wireless transmission requires the integrity of the received data even when a malicious node has a chance to hack and alter the original transmitted message.

- Availability: The transmission should be absolutely operational under any circumstance when the legitimate communication partner is working. The system is supposed to mitigate any malicious attacks while the legitimate transmission is happening.

- Confidentiality: While guaranteeing the authorized operations to work properly, the system also should protect the data privacy from being accessed to unauthorized users.

- Authentication: To guarantee the confidentiality, authentication is required to make sure potential attempts to the communications are all made by legitimate users. It is also used to justify the identity of the existing partner[21].

- Access Control: A communication system should have the ability to manage and control the devices that have the access to the legitimate transmission process[21][22]. It requires each potential access to be authenticated before it actually enters the communication

links. However, due to the broadcast nature of the wireless network, access control is one of the most difficult task for a wireless communication system.

1.3 Security Mechanisms

In oder to counter various security threats and meet with the security requirements for wireless networks, many security mechanisms are also developed. These mechanisms can be classified into two categories: mechanisms based on cryptography on upper layer and mechanisms based on perfect secrecy theory on lower layer. In this section, several existing security mechanisms are introduced and discussed.

1.3.1 Cryptography in wireless networks

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity and data origin authentication. Cryptography can also be defined as the conversion of data into a chaos code that can be deciphered and sent across a public or private network. Cryptography is divided into two categories. The first one is public-key cryptography. Asymmetric cryptography algorithms use different keys for encryption and decryption. Each node in the network has a pair of keys, the private key and public key. The other one is symmetric-key cryptography. In a symmetric-key algorithm, both parties of communication system use the same key for encryption and decryption.

Public-key Cryptography: As shown in Figure 2.1, public-key encryption encrypts a message with recipient's public key. The message cannot be deciphered by anyone else that has no corresponding private key. The way that can decipher the encrypted message is to posses the private key paired with the public key. This is used in an attempt to ensure confidentiality [23]. The cryptography can be used as digital signatures in which a message is signed with the sender's private key and can be verified by anyone who has access to the sender's public key. It is believed that the code size,data size, processing time, and power consumption make it undesirable for public key algorithm techniques. Public key algorithms such as RSA (*Ron Rivest*, *Adi Shamir* and *Leonard Adleman*) [24] are computationally intensive and usually execute thousands or even millions of multiplication instructions to perform a single-security operation.

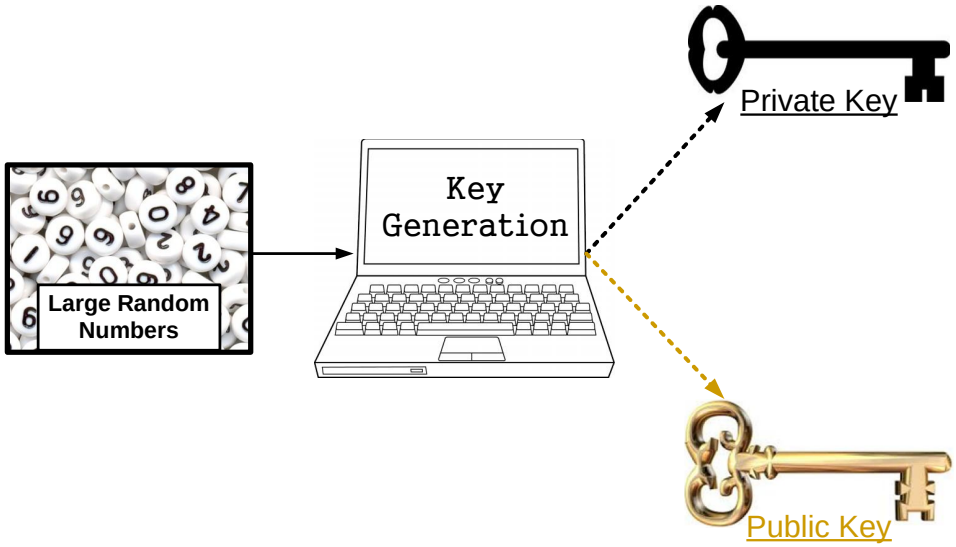


Figure 2.1: A depiction of public (asymmetric) key encryption cryptography.

- RSA: The longest and most popularly used public-key cryptosystem is RSA [25]. Let the n-bit integer $N = pq$ be the product of two large primes of the same size. Generally speaking, N is set to have 1000 bits and p and q each is set to have around 500 bits. Let e and d be two integers that $ed \equiv 1(mod\ \varphi(N))$, where $\varphi(N) = (p-1)(q-1) = N + 1 - (p+q)$ is the Euler's totient function [26] of N. Integer N is the RSA modulus. Integer e is the encryption exponent. Integer d is the decryption exponent. Integers N and e are used to generate public key and made publicly known. The integer d is used as the private key which is only known to the destination who is supposed to receive the encrypted messages. Although with high security, also due to high complexity of public-key encryption, RSA is generally implemented to encrypt a short but crucially important or to encrypt a randomly chosen key which can be used in a corresponding private-key encryption scheme. The encryption process to send a message M is described as: the sender computes the cipher-text C, the least positive residue of M^e modulo N.

To decrypt C, the receiver computes the least positive residue of C^d modulo N. Using Euler's theorem from elementary number theory, one can easily show that $C^d \equiv M^{ed} \equiv M(modN)$.However, anyone who is able to factor $N = pq$ can break RSA at once by finding an inverse of e modulo $(p-1)(q-1)$. Boneh and Venkastesan [27] also suggest a way to break RSA by inverting the RSA function $M \rightarrow M^e$ modulo N. So RSA scheme could be suffered from various attacks such as factorization attack, side-channel attacks and several algorithmic attacks.

- Merkle-Hellman Knapsack Cryptosystem: The Knaspack problem can be described as follows: Given an n-turple v_i of positive integers and an integer V, find an n-bit integer $N = (\epsilon_{n-1}\epsilon_{n-2}...\epsilon_0)_2, \epsilon_i \in [0,1]$, such that $\sum_{i=0}^{n-1} \epsilon_i v_i = V$, if N exists [28]. The process of constructing a Merkle-Hellman Knapsack Cryptosystem to transmit $n-bit$ message M can be described as: Each user choses a superincreasing $n-turple\ v_0..., v_{n-1}$, an integer m which is greater than $\sum_{i=0}^{n-1} v_i$, and an integer a prime to m, $0 < a < m$. This is done by random process. The user computes $b = a^{-1} modm$, and also computes the $n-turple w_i$ defined by $w_i = av_i\ mod\ m$. The user protects $v_i, m, aandb$ as secret information and publishes the $n-turple$ of w_i as the enciphering key $K_E = w_0....w_{n-1}$. The deciphering key thereby is $K_D = (b, m)$. The sender can compute $C = f(M) = \sum_{i=0}^{n-1} \epsilon_i w_i$, and transmit it. In order to decipher the encrypted message, the receiver has to find the least positive residue V of bC modulo m. Since $bC = \sum \epsilon_i b w_i$,it follows that $V = \sum \epsilon_i v_i$. It is easy to find the unique solution $(\epsilon_{n-1}.....\epsilon_0) = M$ of the superincreasing knaspack problem. Although many believe that Merkle-Hellman Knapsack Cryptosystem should be secure, Shamir [29], in 1982, found an algorithm to solve this type of knaspack problem that is polynomial in n and proved that the cryptosystem is insecure.

- Elliptic Curve Cryptosystem: Assume an elliptic curve E over F is an equation:

$$y^2 = x^3 + ax + b, \tag{2.1}$$

where F is a field of characteristic not equal to 2 or 3; $a, b \in F$ and $4a^3 + 27b^2 \neq 0$. If K is a field containing F, then the set of K-points of E, denoted E(K), consists of all solutions

$(x, y) \in K \times K$ of Equation 2.1 together with a special point ∞ called the point at infinity [30]. The encryption process can be described as: assume that E is an elliptic curve over F and P is a publicly known point on the curve. The sender secretly chooses a random integer k_A and computes the point $k_A P$, which she sends to the receiver. Similarly, the receiver secretly chooses a random k_B, computes $k_B P$ and sends it to the sender. The common key is thereby $Q = k_A k_B P$. The sender computes Q by multiplying the point she received from the receiver by its secret k_A; The receiver computes Q by multiplying the point it received from the sender by his secret k_B. The eavesdropper which wants to eavesdrop the communication has to determine Q [31].

Private-key Cryptography: Private-key cryptography, also known as symmetric-key cryptography, utilizes same or similar key both in encryption and decryption process, as shown in Figure 2.2. The communication parties have to share and maintain the secret keys before the communication links are established. For this reason, the decryption can be simple and straight by using the reversed process in encryption. The symmetric cryptography can provide a guarantee on the decryption efficiency and system's security as long as the key is not cracked. In other words, secret key plays an important role in symmetric cryptography. As a result, the distribution of the initial private key is crucially important. The key has to be safely and secretly sent to receivers and senders while attackers should be kept away from any information about it.

- Data Encryption Standard (DES): DES is a block cipher that inputs a plain-text string and outputs a cipher-text string of the same length. The block size of DES is 64 bits and the key size is also 64 bits. The effective DES key size is 56 bits and there are 8 bits used for error detection[32]. There are mainly four modes of DES: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) mode and Output Feedback (OFB) mode. The major differences among these models are error propagation and size of cipher blocks and streams. However, 56-bit key length has been considered weak because of the advanced computational capability of modern computers. For the reason that DES uses the symmetric key algorithm, with enough powerful hardware, the brute force attack can be utilized to crack DES keys. The maximum number of attack attempts

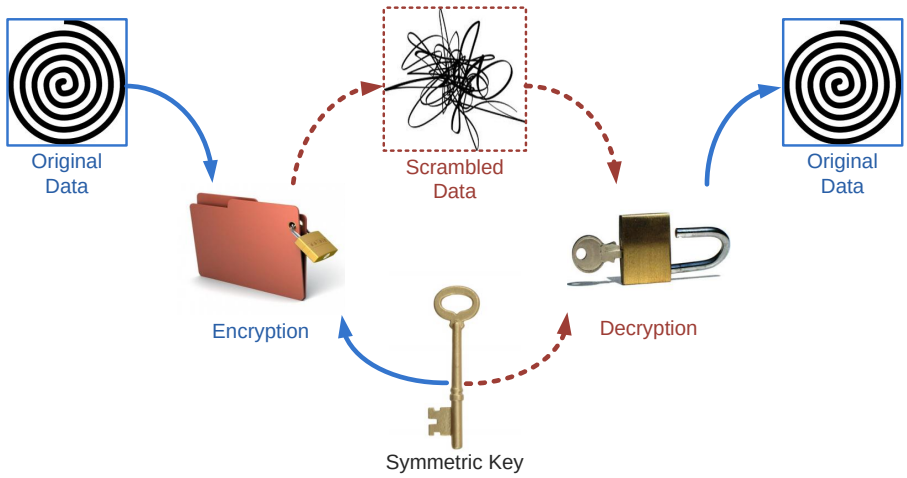


Figure 2.2: Private key cryptography, also known as symmetric key cryptography, utilizes same or similar key both in encryption and decryption.

is only $2^{56} \approx 7.2 \times 10^{16}$[33].

- Advanced Encryption Standard(AES): Replacing DES, Advanced Encryption Standard (AES) was proposed by US government in Federal Information Processing Standard (FIPS)[34] in 1997. AES is a symmetric block cipher with a block size of 128 bits. The length of secret key can be 128 bits, 192 bits or 256 bits which are called AES-128, AES-192, AES-256 correspondingly. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. As an example in Figure 2.3 which indicates a 128-bit key AES, each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption. AES also has the notion of a Word. A word consists of four bytes, that is 32-bits. Each round of processing works on the input state array and produces an output state array as well. Unlike DES, the decryption algorithm differs from the encryption algorithm. Although the same steps are used in encryption and decryption, the order in which the steps are carried out is different. Brute force

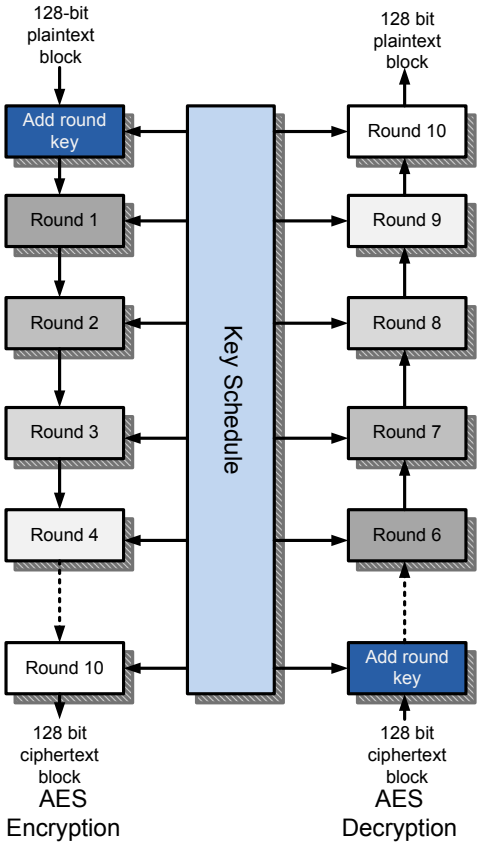


Figure 2.3: A work flow of AES encryption of 10 rounds of processing for 128-bit generation.

attack on AES-128 is not likely to be practical for now. The crack of AES-128 requires $2^{128} \approx 3.4 \times 10^{34}$ times of computations which is far more complicated than cracking a DES key.

1.3.2 PHY Security Mechanisms in Wireless Networks

While the common and conventional encryption techniques are used in the upper layers, PHY security mechanisms utilize the unique characteristics of transmission on PHY. Most physical features, such as the channel state information, power allocation and signal attributes, are difficult to be modified and duplicated. Therefore, more and more research interests have been put on designing various kinds of mechanisms using these physical features to enhance the wireless communication security[6].

Security Mechanisms Using Channel Characteristics: As wireless channel is the fundamental but important element in wireless communications, it conveys information and signals among different communication partners. The ubiquitous wireless channel therefore provides various features during the transmission. Based on exploitation of the channel characteristics, security mechanisms against attacks have been developed using the features such as radio frequency, channel pre-coding and transmission coefficients.

- Radio Fingerprinting: Radio fingerprinting is a process that identifies a transmitter by the unique "fingerprint" that characterizes its signal transmission. It is commonly used by cellular operators to prevent cloning of cell phone. The mechanism can be described as follows: each transmitter has unique rise time signature when manufactured. Once the rise time signature is captured and assigned, a different transmitter using different signatures is easily detected. O. Ureten and N. Serinken [35] proposed the radio fingerprinting system consisting of multiple sensor systems that capture radio features form each received signal. The intrusion detection component analyses the captured radio features. A dynamic fingerprint for each legitimate source identifier is generated according to these features. The evolution of each fingerprinting is monitored by the system. Once the fingerprinting behaves beyond expectation, an intrusion alert is issued. This mechanism help to discriminate intruders from legitimate communication entities.

- Channel Response Based Methods: Chris Sperandio and Paul Flikkema [36] proposed an Algebraic channel decomposition multiplexing (ACDM) precoding scheme in which the transmitted code vectors are generated. This describes the channel response between the transmitter and the intended receiver. In this scheme, even assume that the intruders may have the perfect knowledge of the transmission code vectors or their own channel responses, the variation of channel response from time to time also sets the obstacle for the intruder to decode. In addition a PHY authentication using CIR is proposed in [37]. The variation between two consecutive CIRs of each pair of transmitter and receiver is monitored. The noise-mitigation pattern of the channel response is used as a decision criterion. The anomalous behavior of an undesired transmitter can be detected using a channel-based hypothesis testing method if the pattern fails to follow the routine. The

authentication based on the inherent property of CIR is capable of differentiating the identity of the sender.

Coding Techniques Combining with Physical Features: The purpose of combing coding techniques with physical features is to mitigate effects of jamming and eavesdropping during the transmission. By combining physical features of the signals, the PHY coding techniques can enhance the effectiveness of conventional cryptography method on upper-layer. Error correction coding and spread spectrum coding take advantages of the unique features on PHY to help building the safe transmission.

- Error Correction Coding: Due to the linear response of conventional cryptography method, if there exists a single error in received encrypted message, a potential large number of errors will inevitably appear in the decrypted message. In order to solve the problem, D. Abbasi-Moghadam, V. T. Vakili and A. Falahati [38] proposed a method to combine turbo coding[39] and advanced encryption standard (AES). In their method, a secured communication session is set up by using the encrypted turbo codes. The pseudo random number generation algorithm[40] is implemented to select N bits from M turbo encoded bits. Based on the actual requirement of the redundant bits to secure the information, the method is capable of making a flexible choice of the number of bits according to the channel. This method also has the advantages of higher-speed encryption and decryption with higher security, smaller encoder and decoder size.

- Spread Spectrum Coding: Spread spectrum[41], a signaling technique, is an effective solution to enhance PHY security. In spread spectrum, a signal is spread by a pseudo-noise sequence over a wide frequency band much wider than the original signals' frequency range according to a certain coding algorithm. The transmitted signal is spread over broadband spectrum using direct sequence spread spectrum (DSSS). Frequency-hopping spread spectrum (FHSS) continuously alternates the carrier's central frequency for several times within each bit duration. The size of keys differentiates the spread spectrum from conventional cryptographies. Conventional cryptography utilizes a large size of the secret key to guarantee a high computational complexity of brutal force attack to the key

while spread spectrum only requires a limited key size according to the range of carrier frequencies and number of different sequences.

Security Improvements Using Power Allocations: Allocation of transmitted power is also one of the most important features on PHY. In some cases, owing to different allocated power, it is capable to identify the communication partner as legitimate or illegitimate. In other occasions, high secrecy can also be achieved by manipulating the power allocation of the transmitted signal. The common schemes in power approaches on PHY include directional antennas and injection of artificial noise.

- Directional Antennas: Directional transmission is capable of improving spatial reuse and enhancing communication coverage for the reciprocity of beamwidth to peak gain. G. Noubir [42] compared directional antennas with omni-directional antennas under various jamming conditions. The results show that the transmitted data can not be normally and correctly received by the receiver within the coverage range if omni-directional antenna is used. Meanwhile the node can still receive signal if a directional antenna is in use. The comparison shows that the use of directional antennas can improve wireless network capacity and avoid jamming attempts under some conditions.

- Artificial Noise Injection: The perfect secrecy[5][7], which means the wiretap channel capacity is lower than legitimate channel capacity, can be achieved by properly injecting artificial noise. S. Goel and R. Negi[43] suggested that adding artificial noise can be used to achieve such perfect secrecy. In their method , artificial noise is generated by multiple antennas or the coordination of helping nodes. Artificial noise is utilized to decrease the receptivity of legitimate receiver, but has only a small influence or none influence on legitimate receiver. The benefit of artificial noise injection is that even if the eavesdropper occupies a better channel condition than legitimate channel, by adding artificial noise into the transmission, it is still possible to guarantee an acceptable secrecy for a secured transmission.

1.4 Brief Summary of the Section

As of great importance, security issues in wireless communications receive lots of attentions. Due to the vulnerability of wireless transmission to various attacks in open air, security mechanisms are needed to meet with the requirements of a secure transmission. In achieving this goal, many wireless security approaches, both on upper layer and lower layer, are designed to counter these threats and secure the wireless communications.

2 Orthogonal Frequency Division Multiplexing (OFDM) System

First proposed by Robert W. Chang [44] in 1966, orthogonal frequency division multiplexing (OFDM) is a method of transmitting digital data using multiple orthogonal sub-carrier frequencies. It shares the spectrum with several users by using these orthogonal sub-carriers during the transmission. The main concept in OFDM is the orthogonality of the sub-carrier which makes it different from frequency division multiplexing (FDM). In FDM, carriers are placed without overlapping and do not have relationship with each other. However, in OFDM, those sub-carriers overlap one by one orthogonally. The orthogonality allows simultaneous transmission of a large number of sub-carriers in a tight frequency spectrum without interference from each other. The advantage of doing this is that frequency spectrum is compressed. In other words, the bandwidth is saved with overlapped carriers as shown in Figure 2.4.

Nowadays, as a promising technology, OFDM has been widely used in various areas. In cable and wireless communications, OFDM are applied in applications such as asymmetric digital subscribe line (ADSL), very high bit rate digital subscribe line (VDSL), digital video broadcasting (DVB) series (including DVB-T, DVB-H and DVB-T2), digital audio broadcasting (DAB) series (including DAB and DAB+) and etc. The popularity of OFDM shows its advantages on several aspects. The primary advantage of OFDM over single sub-carrier scheme is that it has the ability to fight against severe channel conditions such as interferences and frequency selective fading due to multi-path effect. In addition, for the reason that each sub-carrier of OFDM is narrow-band compared with the bandwidth used for transmission, the frequency

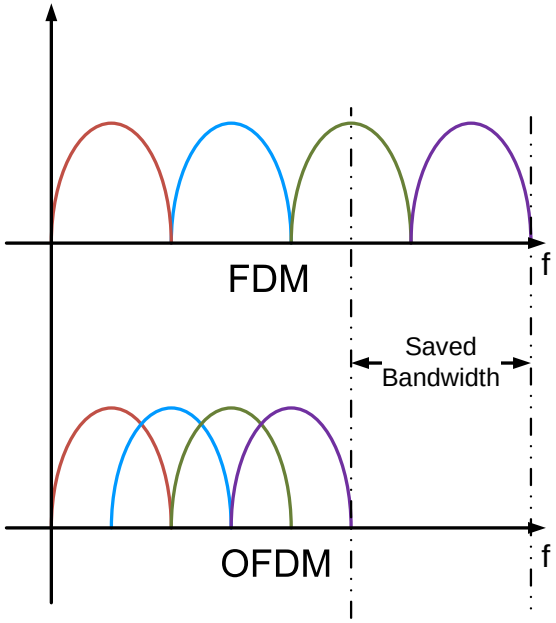


Figure 2.4: Spectrum efficiency comparison between frequency division multiplexing (FDM) and orthogonal frequency division multiplexing (OFDM).

equalization is simplified as those sub-carriers can be regarded as flat fading. Also, it is possible and affordable to use guard interval to eliminate inter-symbol-interference (ISI) because of the slow symbol rate. In summary, the main advantages of OFDM are listed as below:

- High spectral efficiency compared to single carrier modulation schemes.
- Easy adaptation to various channel conditions without the necessity of complex time-domain equalization.
- Robustness against intersymbol interference (ISI) and fading effects in multipath propagation.
- Efficient implementation using fast Fourier transform(FFT).
- Low sensitive to time synchronization errors.

2.1 System Structure of OFDM

In this section, the basic system model of OFDM system including transmitter and receiver is introduced.

OFDM Transmitter

The basic system model of OFDM transmitter is shown in Figure 2.5. The function of transmitter can be described as follows:

- The incoming serial data with high rate is first converted into parallel sequence with low data rate. The number of paralleled sequence depends on the number of sub-carriers required by transmission.

- Each paralleled sequence is modulated independently using modulation schemes such as quadrature amplitude modulation (QAM) or phase shift keying (PSK) (including BPSK, QPSK and etc.).

- All paralleled sequence are considered as one inverse fast Fourier transformation (IFFT) block so that IFFT process can modulate these signals onto N orthogonal sub-carriers. The IFFT process generates a set of complex time-domain signals. In addition, according to requirement of frequency equalization, several pilot sequence can also be added as paralleled sequence before IFFT process.

- Cyclic prefix (CP) is added before both real and imaginary part of complex time domain signal sequence to prevent multi-path effect. The length of cyclic prefix depends on the estimated delay of multipath channel condition.

- Both real and imaginary component with CP insertion are modulated on to carrier frequency f_c using two orthogonal waves correspondingly. The summation of two modulated signal generates the OFDM signal which can be sent to receiver at last.

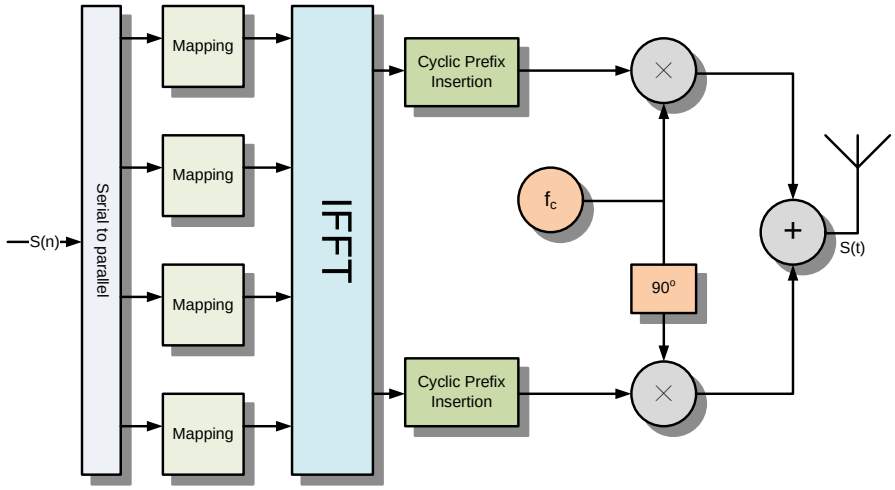


Figure 2.5: System diagram of OFDM transmitter.

OFDM Receiver

OFDM receiver mainly performs a reverse process of the transmitter. The system model of OFDM receiver is shown in Figure 2.6. The function of receiver can also be described as follows:

- The received OFDM signal is first downshifted in frequency domain by corresponding carrier frequency f_c into two orthogonal baseband signals which respectively stand for real and imaginary component of the complex time-domain signal.
- A cyclic prefix removal process is utilized to eliminate the redundancy which may be distorted by multi-path channel.
- A fast Fourier transform process is used to demodulate signal from each sub-carrier frequency. The demodulated signal, regarded as frequency-domain signal, is equalized by frequency equalization block to eliminate the channel impact.
- The frequency domain signal is de-mapped using corresponding constellation mapping scheme which is used at transmitter.

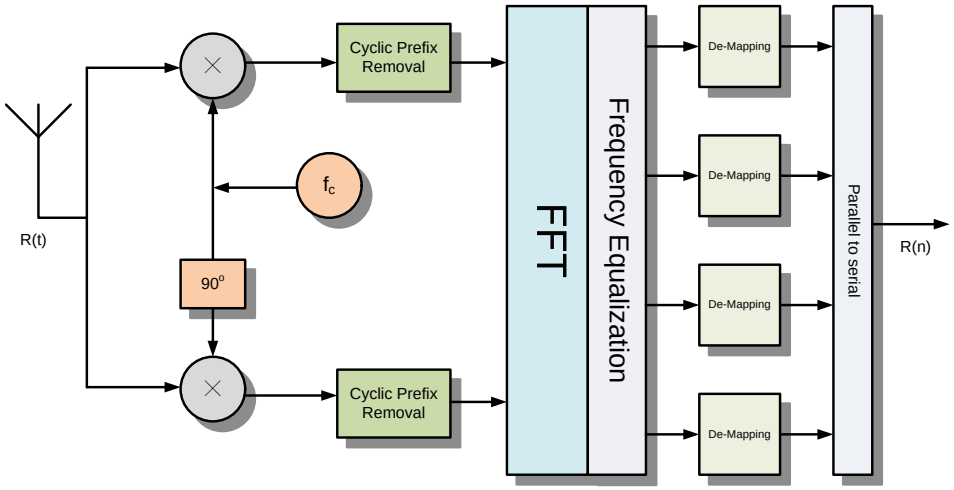


Figure 2.6: System diagram of OFDM receiver.

- After paralleled signal passing through parallel-to-serial converter, the binary data stream is finally recovered.

2.2 Mathematical Description of OFDM Infrastructure

As shown in Figure 2.7, the time domain waveform of an OFDM signal is the summation of all orthogonal sub-carriers' waveforms. Given that N sub-carriers are required during the transmission, the time domain OFDM signal is expressed as:

$$S(t) = \sum_{k=o}^{N-1} D_k e^{j2\pi kt/T}, (0 \leq t < T), \tag{2.2}$$

where D_k is the set of data symbol, N is the number of sub-carriers and T is the OFDM symbol duration time. Equation. 2.2 stands for the process that the data symbol is modulated onto N sub-carriers by inverse Fourier transformation.

In order to avoid interference caused by multi-path fading channels, a guard interval of length T_g is inserted prior to the OFDM block. Within this period of interval time duration, the

signal

$$S_g(t) = S(t), (T - T_g \leq t < T), \tag{2.3}$$

is copied and moved to this interval as a cyclic prefix. Therefore, the OFDM signal along with cyclic prefix thus can be described as:

$$S(t) = \sum_{k=o}^{N-1} D_k e^{j2\pi kt/T}, (-T_g \leq t < T). \tag{2.4}$$

As shown in Figure 2.8 and Figure 2.9, the sub-carriers also have the orthogonality which can be expressed as:

$$\begin{aligned} &\frac{1}{T}\int_0^T (e^{j2\pi k_1 t/T})^* (e^{j2\pi k_2 t/T}) dt \\ =&\frac{1}{T}\int_0^T (e^{j2\pi (k_2-k_1) t/T}) dt \\ =&\delta_{k_1 k_2}, \end{aligned} \tag{2.5}$$

where $(.)*$ denotes the complex conjugate operation and δ stands for Kronecker delta:

$$\delta_{k_1 k_2} = \begin{cases} 0, \ if \ k_1 \neq k_2 \\ 1, \ if \ k_1 = k_2 \end{cases} \tag{2.6}$$

2.3 Multi-path Effects and Cyclic Prefix

2.3.1 Multipath Effects

In real wireless transmission, the condition of communication media is complicated. One of the most common situations is that the original signal may have multiple paths to the destination node. This phenomenon is called as "Muti-path Effect" of communication channel. Because of the objects, such as mountains, tall buildings, walls and vehicles, signals are reflected and deviated from the straight propagation path. Hence, same signal may arrive at the destination at different time due to the longer deviated paths that the signal travels on. The summation of the tardy copies of the signal may results in the distortion of the signal.

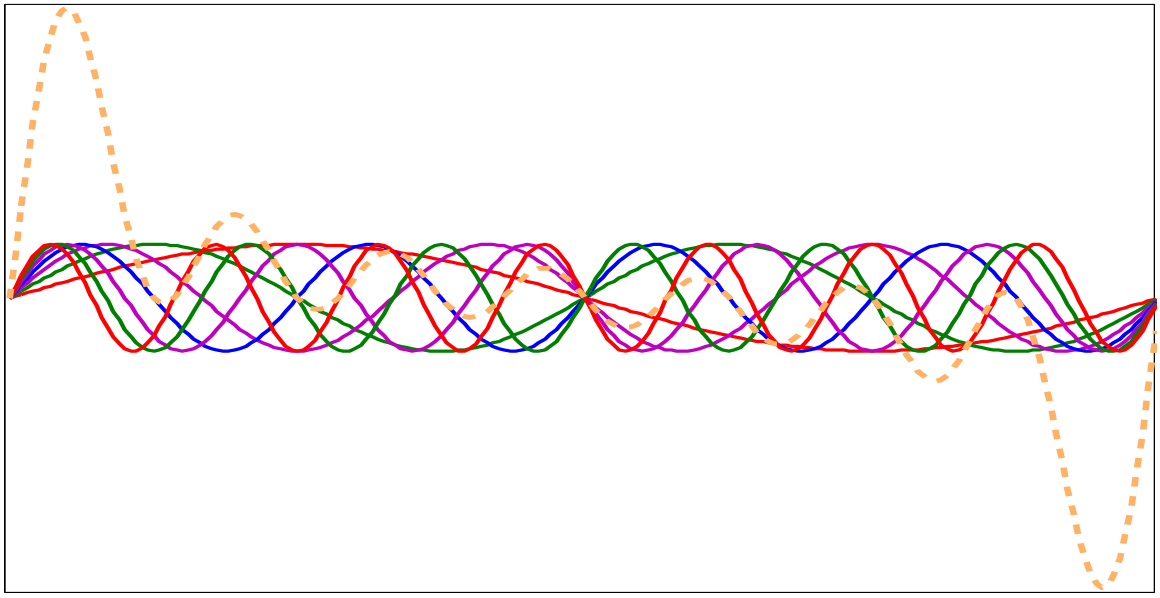


Figure 2.7: Waveforms of OFDM sub-carriers in time domain.

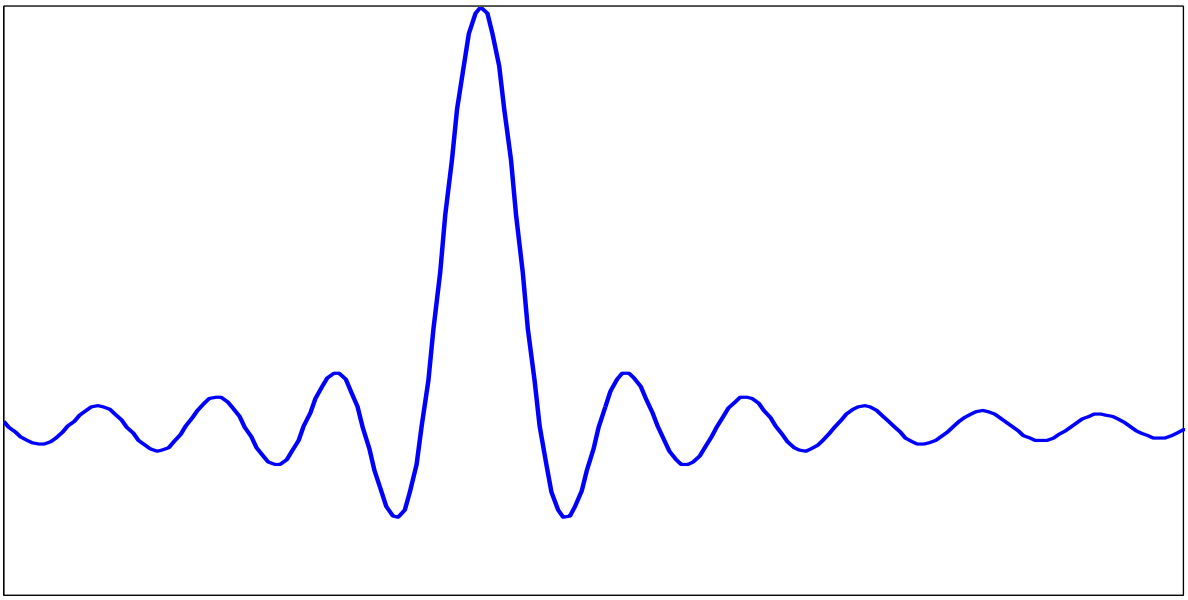


Figure 2.8: An example of single sub-carrier in frequency domain.

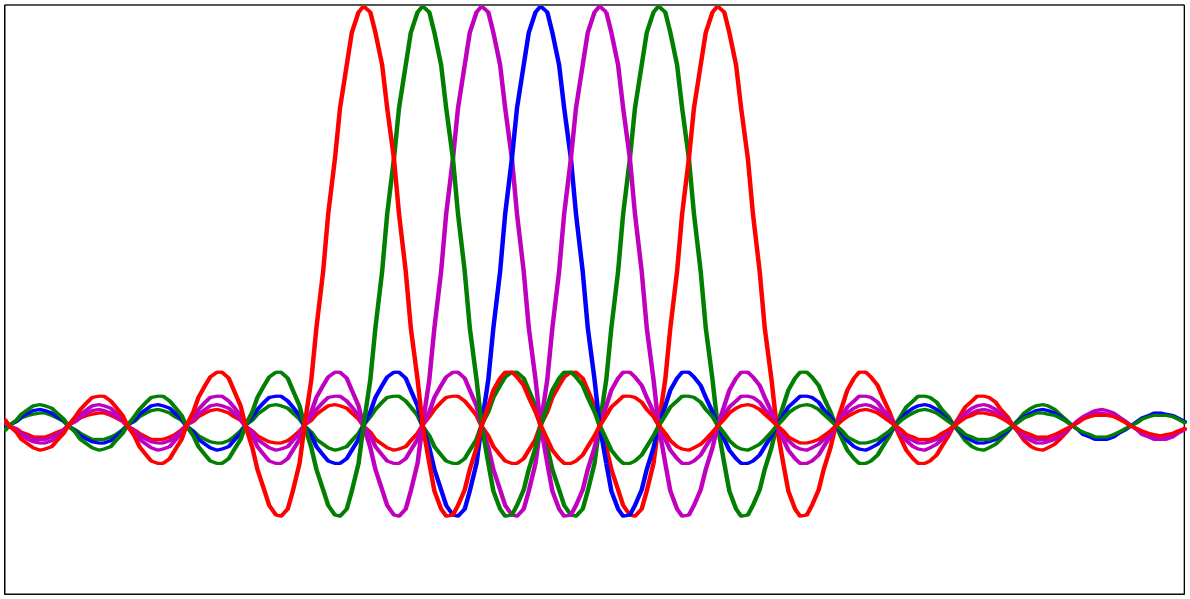


Figure 2.9: An example of orthogonal sub-carriers in frequency domain.

Suppose a single pulse signal $\delta(t)$ is transmitted in a channel with infinite bandwidth:

$$s(t) = \delta(t). \tag{2.7}$$

If there is no multi-path in the channel, the received signal is:

$$r_{singlepath}(t) = h(t) = \rho e^{j\theta}\delta(t), \tag{2.8}$$

where $\rho e^{j\theta}$ is the complex amplitude of the received pulse caused by the channel. The spectra of the received signal $R_{singlepath}(t)$ therefore can be obtained by a Fourier transform:

$$\begin{aligned} R_{singlepath}(f) &= \mathscr{F}(r_{singlepath}(t)) \\ &= \int_{-\inf}^{+\inf} r_{singlepath}(t)e^{-j*2\pi ft}dt \\ &= \int_{-\inf}^{+\inf} \rho e^{j\theta}\delta(t)e^{-j*2\pi ft}dt \\ &= \rho e^{j\theta} \end{aligned}. \tag{2.9}$$

The equation above is constant versus frequency f. It means that the channel impulse

response in frequency domain remains flat and the signal is not distorted.

If multi-path exists in the channel as shown in Figure 2.10(a), the received signal is :

$$r_{multipath}(t) = h(t) = \sum_{N=0}^{N-1} \rho_N e^{j\theta_N} \delta(t - T_N), \tag{2.10}$$

where N represents the number of arrived signal copies from different paths; $\rho_N e^{j\theta_N}$ stands for the complex amplitude of Nth arrived signal; T_n is the delay time of Nth signal compared to the first arrived main signal. The corresponding frequency response similarly can be obtained:

$$\begin{aligned} R_{multipath}(f) &= \mathscr{F}(r_{multipath}(t)) \\ &= \int_{-\infty}^{+\inf} r_{multipath}(t) e^{-j*2\pi ft} dt \\ &= \int_{-\inf}^{+\inf} \left[\sum_{N=0}^{N-1} \rho_N e^{j\theta_N} \delta(t - T_N) \right] e^{-j*2\pi ft} dt \\ &= \sum_{N=0}^{N-1} \rho_N e^{j\theta_N} e^{-j*2\pi f T_N} \end{aligned} \tag{2.11}$$

From equation above, it can be observed that for different frequency, the magnitude of channel response in frequency domain may vary which is depicted in Figure 2.10(b).

2.3.2 Cyclic Prefix

In digital system, the delay of signal leads to inter-symbol interference (ISI). During OFDM transmission, due to the delayed arrival of previous symbol, the subsequent symbol is likely to be overlapped. It happens under the condition that transmission interval between two adjacent symbols is less than the delay time of multi-path channel. As shown in Figure 2.11, if

$$t_i < t_d, \tag{2.12}$$

where $t_i = t_3 - t_2$ is the transmission time interval between two continuous symbols; $t_d = t1 - t_0$ is the maximum time delay caused by multi-path channel, the subsequent symbol will be overlapped between t_3 and t_4. Once overlapped, the following symbol will be superimposed and distorted which will bring difficulties in decoding and may result in a high error rates.

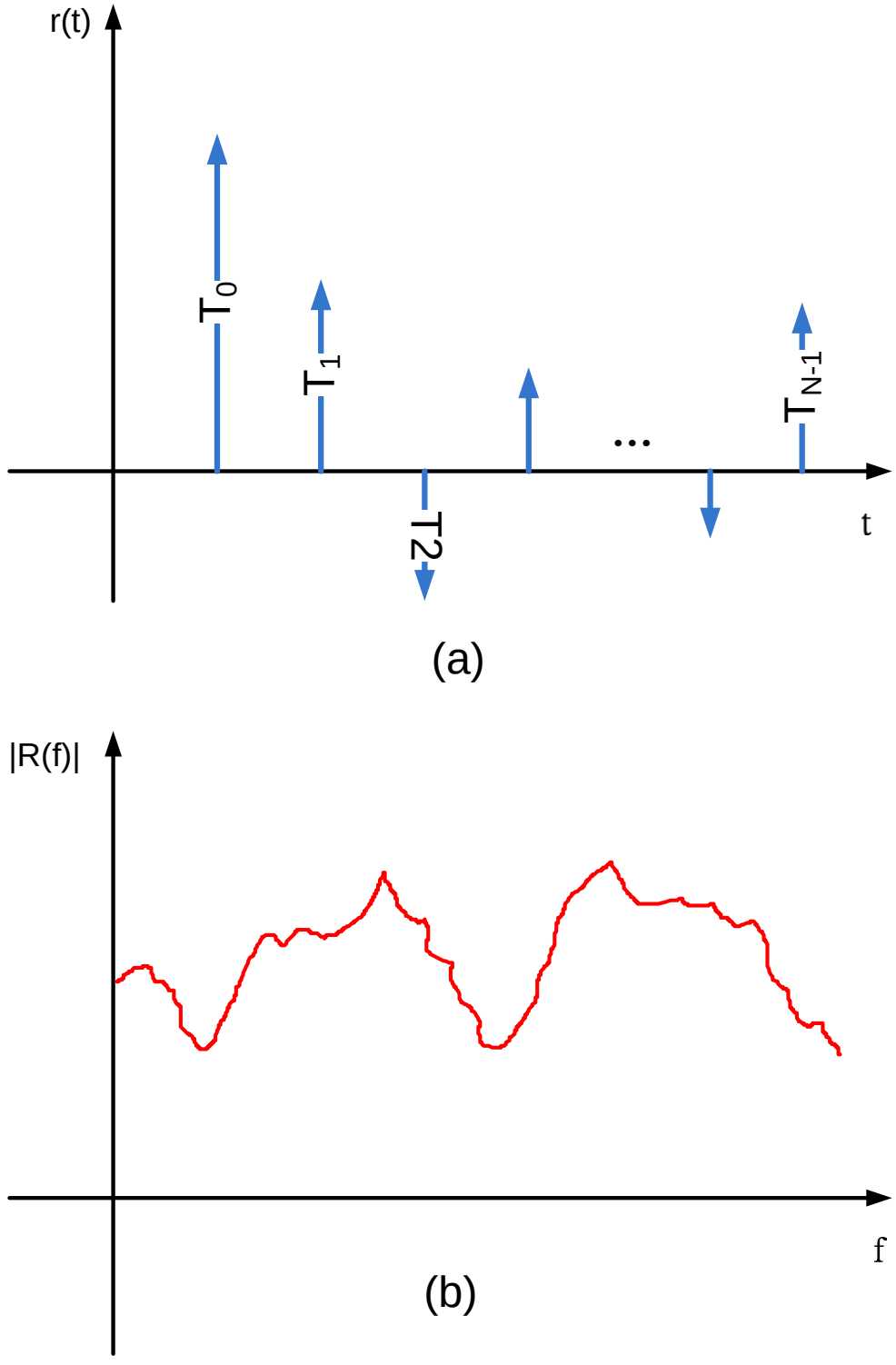


Figure 2.10: Illustration of multi-path effect. (a) Delays of signal caused by multi-path in time domain. (b) Frequency selective fading caused by multi-path effect.

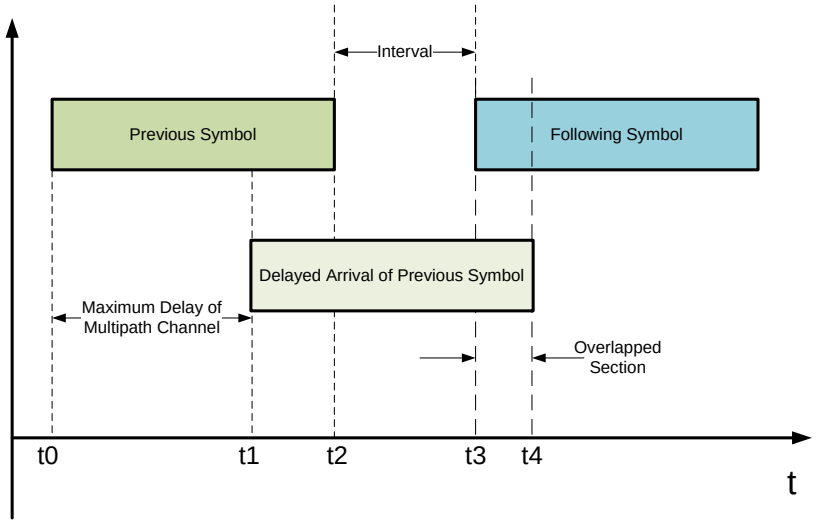


Figure 2.11: Depiction of Inter-Symbol Interference in OFDM system caused by multi-path effect of wireless channel. If transmission interval between two adjacent symbols is less than the maximum delay time of multi-path channel, the following symbol is overlapped by the late arrival of previous symbol.

In order to solve the problem, the time interval t_i, which performs as a guard interval (GI), should be more than t_d. If blank space is long enough between two consecutive symbols, the interference problem will be eliminated. However, it is not practical to insert blank signal in between two consecutive OFDM symbols. In reality, the hardware is always producing signals continuously. It is less efficient and hard to implement the function of periodically stopping the machine to produce a short blank interval.

Instead of reserving blank time interval in between two consecutive symbols, a more practical and efficient method is to extend the symbol into the empty time slot. The rear part of each OFDM symbol is copied and moved to the begin of itself. Such method is called cyclic prefix (CP) insertion. The length of the part that is copied is longer or equal to the time duration of the maximum time delay of the multi-path effect. This makes each symbol longer than one cycle. Once the replenishment is done, the OFDM system may keep sending out the symbols incessantly. Consequently, as shown in Figure 2.12, only the CP part of the following symbol is overlapped by the previous symbol. As long as a corresponding process at receiver can discard this period of signal when decoding, the property of the rest part of the symbol remains

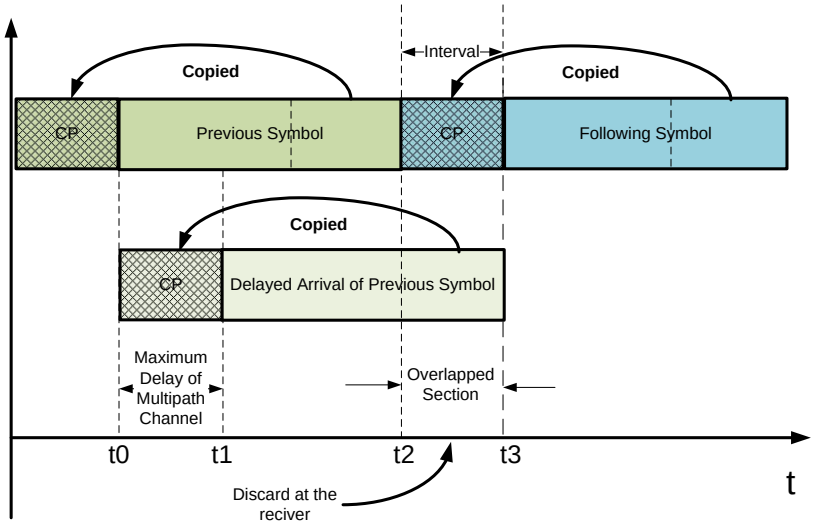


Figure 2.12: Depiction of cyclic prefix (CP) insertion. The rear part of each OFDM symbol is copied and moved to the begin of itself to extend the signal filling the time interval between two consecutive symbols.

unchanged.

2.4 OFDM Interleaving

The reasons for interleaving OFDM signal is to attempt to uniformly distribute the errors caused by channel distortion. By doing this, the error correction decoder may correctly decode all the bits errors even if a high concentration of burst errors happens. Two ways of interleaving are generally implemented, namely frequency interleaving and time interleaving. On one hand, the resistance to fading in frequency-selective channel is increased by frequency interleaving. On another hand, time interleaving offers benefit in slowly fading channel.

2.4.1 Frequency Domain Interleaving

The frequency domain interleaving happens before inverse fast Fourier transformation (IFFT). Because of the frequency selective fading of typical radio channels, the OFDM subcarriers generally have different amplitudes. Deep fades in the frequency spectrum may cause groups of

subcarriers to be less reliable than others, thereby causing bit errors to occur in bursts rather than being randomly scattered. Most forward error correction codes are not designed to deal with error bursts. Therefore, the original idea of frequency domain interleaving is to reduce this effect. At the transmitter, the coded bits are permuted in a certain way, which makes sure that adjacent bits or symbols are separated by several bits or symbols after interleaving. At the receiver, the reverse permutation is performed before decoding.

2.4.2 Time-domain Interleaving

Although the frequency domain interleaving is the most common way for OFDM interleaving technique, a more interesting way is to interleave the OFDM symbols in time domain. Haifeng Wang and Jorma Lilleberg proposed an OFDM transceiver with time domain scrambling in [45]. The conventional OFDM symbols after IFFT operation are scrambled in time domain prior to the transmission to cancel inter-cell interference. In addtion, Guido Stolfi and Luiz A. Baccla proposed a transform-based time interleaving algorithm in which binary information is spread over several consecutive symbols that can be further scrambled in the frequency domain [46]. Conventional time domain symbol interleaving is replaced by an inverse Fourier transform performed on subsets of the digital data input. In this way, the individual carrier of and OFDM symbol is no longer modulated by discrete-amplitude QAM or PSK symbols, but rather by a non quantized complex signal whose distribution is nearly Gaussian. Once symbols are permutated in time domain, time and spectral performance is greatly changed. This phenomenon gives the possibility to secure the transmission. Without a correct re-permutation, the received signal will be chaos both in time domain and frequency domain.

2.4.3 Bit-Interleaved OFDM

Bit-interleaved OFDM interleaves input bits before mapping. Defeng Huang proposed a bit-Interleaved Time-Frequency coded modulation OFDM system (BITFCM) in [47]. This scheme exploited both the time varying and frequency-varying nature of the channels resulting in high diversity order. Using BITFCM scheme, a reduced-complexity maximum-likelihood decoding approach was proposed to achieve good performance with low complexity for low minimum normalized Doppler frequency shift. For high maximum normalized Doppler fre-

quency shift condition, the inter-carrier interference (ICI) can be large, and an error floor will be induced. To solve this problem, two ICI- mitigation schemes are also proposed by taking advantage of the second-order channel statistics and the complete channel information. Although bit-interleaved OFDM can be regarded as an interleaving technique for OFDM, it actually relates more to upper layer signal processing procedure.

2.4.4 Symbol-interleaved OFDM

Another technique of frequency domain interleaving is symbol-interleaved OFDM. This method is to permutate symbols after mapping in transmitter. One unique chaos based scrambling of OFDM constellation symbols for securing system on PHY is proposed by Muhammad Asif Khan [9] . This scrambling algorithm acts as random interleaver. It has good random properties and it is also memory efficient because it can also be completely specified by a logistic map. The scrambling is reversible. It uses 1-D chaotic map to generate the scrambling matrix. The initial condition of 1-D chaotic logistic map serves as key to generate scrambler. The results show that all data are recovered with zero error. The proposed scrambling method is extremely sensitive to initial conditions. Hence, with different initial conditions, it is unable to recover the data correctly.

2.5 Brief Summary of the Section

As a popular wireless communication system, OFDM system is widely implemented in various applications because of several advantages. In this section, the system structure of OFDM transmitter and receiver are introduced. The mathematical expression for the system infrastructure is also presented. To overcome the distortion and interference caused by multipath channel, cyclic prefix is utilized and its principle is explained in details. At last, existing works on OFDM interleaving techniques are surveyed as well.

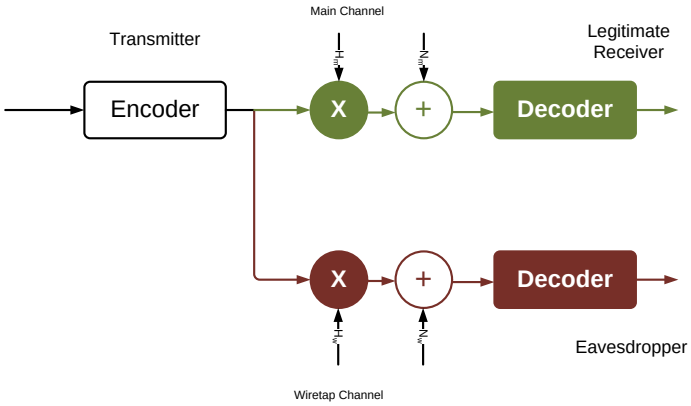


Figure 2.13: Communication system infrastructure with the existence of a wiretap channel.

3 Cooperative Jamming

In most cases of wireless communications, interference and noise are always considered as undesired factors. Interference management and avoidance are also key process to establish an acceptable system performance in a multi-user system[48][49]. Generally speaking, during a wireless transmission, the common way to enhance the system's performance is to limit all kinds of interference. However, when it comes to secure transmission, interference and noise can also be exploited as a useful tool to enhance the system security. By exploring the benefits of interference and noise, researchers have recently developed new cooperative jamming strategies in cooperative system. The idea in essence is to put the eavesdropper in a situation that can only receive less information than the desired receiver. In this section, we will briefly introduce the notion of secrecy capacity and the basic mechanism of cooperative jamming system.

3.1 Secrecy Capacity

The very first theory about the wiretap channel was proposed by Wyner in [5].

As depicted in Figure.2.13, the wire-tapper has access to information that passes through

both the main channel and the wiretap channel. Consider a message block w^k is encoded into the codeword x^n to be transmitted into the fading channel and the output in the main channel will therefore be:

$$y_M(i) = h_M(i)x(i) + n_M(i), \tag{2.13}$$

where $h_M(i)$ is the time varying complex fading coefficient which is also channel state information(CSI) and $n_M(i)$ denotes the zero-mean circularly symmetric complex Gaussian noise.

The eavesdropper (wire-tapper) is capable of eavesdropping the signal sent by the transmitter. The signal received by the eavesdropper is:

$$y_W(i) = h_W(i)x(i) + n_W(i). \tag{2.14}$$

The channel is power limited in the sense that

$$\frac{1}{n}\sum_{i=1}^{n} E[|X(i)|^2] < P, \tag{2.15}$$

where P is the average transmit signal power. In addition, the power of noise in both main and wire-tap channel is N_M and N_W.

Thus, the instantaneous SNR at desired receiver is :

$$\gamma_M(i) = \frac{P|h_M(i)|^2}{N_M} = \frac{P|h_M|^2}{N_M} = \gamma_M, \tag{2.16}$$

where the channel fading is quasi-static fading that $h_M(i) = h_M$. The average SNR therefore is:

$$\overline{\gamma}_M(i) = \frac{PE[|h_M(i)|^2]}{N_M} = \frac{Pe[|h_M|^2]}{N_M} = \overline{\gamma}_M. \tag{2.17}$$

Similarly, the instantaneous SNR at eavesdropper is given by:

$$\gamma_W(i) = \frac{P|h_W(i)|^2}{N_W} = \frac{P|h_W|^2}{N_W} = \gamma_W, \tag{2.18}$$

and the average SNR is:

$$\overline{\gamma}_W(i) = \frac{PE[|h_W(i)|^2]}{N_W} = \frac{PE[|h_W|^2]}{N_W} = \overline{\gamma}_W. \tag{2.19}$$

Shannon-Hartley theorem [7] defines that the capacity of a channel that the maximum of information can be transmitted is related to the bandwidth and signal to noise ratio:

$$C = B\log_2(1 + \frac{S}{N}). \tag{2.20}$$

Thus, the capacity of the main channel is:

$$C_M = \frac{1}{2}\log_2(1 + \gamma_M). \tag{2.21}$$

Likewise, the capacity of the eavesdropper's channel is:

$$C_W = \frac{1}{2}\log_2(1 + \gamma_W). \tag{2.22}$$

By far the channel capacity of either main channel and eavesdropper channel has been explored.

The secrecy channel is characterized as the capacity difference between the legitimate channel and eavesdropper's channel. The notion can be explained in a way that if the maximum of information transmitted in legitimate channel is higher than the maximum of information transmitted in the wire-tap channel, the eavesdropper can never receive enough information to break through the legitimate transmission. This is also called as "Perfect Secrecy". Therefore, the mathematic expression of secrecy capacity is :

$$C_s = C_M - C_W. \tag{2.23}$$

Note that if $\gamma_M > \gamma_W$ which means legitimate receiver can receive more information, the transmission is secured. Otherwise, if $\gamma_M < \gamma_W$, the transmission is unsecured and C_s will become negative. The unsecured situation has no secrecy capacity therefore C_s under such

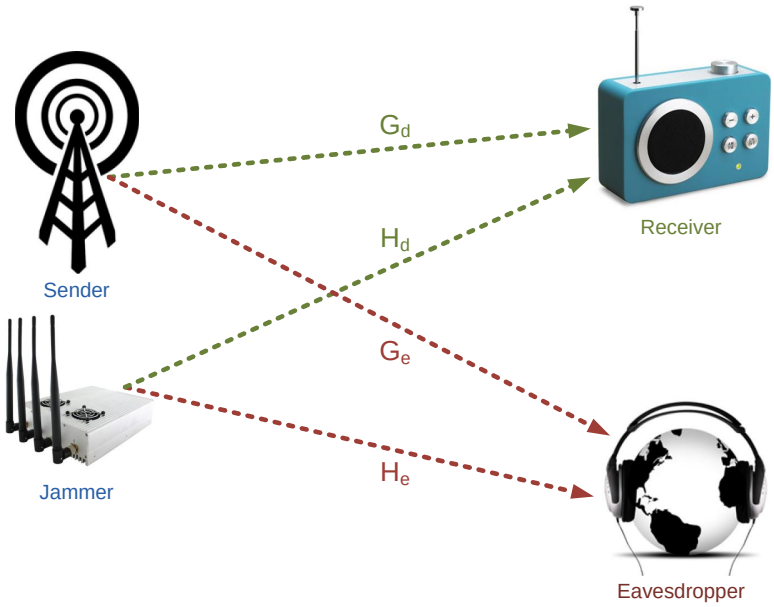


Figure 2.14: An illustration of cooperative jamming system structure.

condition is defined as zero:

$$C_s = \begin{cases} \frac{1}{2}\log_2(1+\gamma_M) - \frac{1}{2}\log_2(1+\gamma_W), & \gamma_M > \gamma_W \\ 0, & \gamma_M < \gamma_W \end{cases}. \tag{2.24}$$

3.2 Cooperative Jamming System

Cooperative jamming is an approach that has been recently proposed for improving PHY based security for wireless networks in the presence of an eavesdropper. While the source transmits its message to the destination, a relay node transmits a jamming signal to create interference to the eavesdropper. The purpose of doing this is to increase the difference of channel capacity between legitimate channel and illegitimate channel so as to maximize the secrecy capacity of the system.

A simple example can demonstrate the mechanism of how cooperative jamming system works. The general system model of a cooperative jamming system is shown in Figure.2.14

The signal received at the destination D as y_d and the at the eavesdropper E as y_e:

$$\begin{aligned} y_d &= \sqrt{P_s} g_d X_s + \sqrt{P_j} h_d x + n_d \\ y_e &= \sqrt{P_s} g_e X_s + \sqrt{P_j} h_e x + n_e, \end{aligned} \tag{2.25}$$

where g_d and g_e are channels from source to destination and eavesdropper; h_d and h_e are channels from jammer to destination and eavesdropper; X_s is the source signal; x is the emitting interfering signal sent by the jammer. Both X_s and x are unit power. $\sqrt{P_s}$ and $\sqrt{P_j}$ are allocated power of transmitter and jammer. According to the conception of secrecy capacity, which is:

$$C_s = Max(C_d - C_e, 0). \tag{2.26}$$

The channel capacity of main channel and wiretap channel thus can be expressed as:

$$\begin{aligned} C_d &= \frac{1}{2} log_2(1 + \frac{P_s |g_d|^2}{P_j |h_d|^2 + \sigma_d^2}), \\ C_e &= \frac{1}{2} log_2(1 + \frac{P_s |g_e|^2}{P_j |h_e|^2 + \sigma_e^2}). \end{aligned} \tag{2.27}$$

Notice that different from the general form of channel capacity as discussed in previous section, the channel capacity of both main and wiretap channel depend on three factors: power of transmission in transmitter and jammer, CSI of legitimate channel and wiretap channel and noise.

By applying different power allocation schemes or beam-forming technologies, C_d and C_e are controllable which means by using cooperative jamming system, it is possible to maximize the secrecy rate at destination or minimize it at eavesdropper to guarantee the security of the entire system.

3.3 Brief Summary of the Section

Opposite to traditional concept of interference and noise, cooperative jamming system takes advantages of them to achieve the best secrecy during the cooperative transmission. In this section, the principle and mathematical definition of secrecy capacity are explained. Designed

to achieve the most secrecy capacity, the cooperative jamming system is also introduced.

4 Chapter Summary

In this chapter, the background information to be used in this thesis is introduced.

In the first section, literature survey on current wireless network security issue is conducted. Issues, such as the categories of security attacks in wireless networks, the requirements for wireless network security as well as current mechanisms against those attacks, are detailedly provided.

In the second section, the fundamental principle of orthogonal frequency division multiplexing (OFDM) is also introduced in this chapter. The system structure of an OFDM system is discussed and the mathematical expression is also presented. The merits of OFDM system against multipath effect are explored including the definition of multipath effect and the usage of cyclic prefix. Also some currently used interleaving techniques in OFDM system are introduced as well.

In the third section, the concept of cooperative jamming system to enhance the system security is discussed. The definition of secrecy capacity to achieve perfect secrecy of the system is derived. Followed that, the general system structure of a cooperative jamming system is also introduced.

Chapter 3

Secure Transmission in OFDM System by Using Time Domain Scrambling

1 Introduction

Due to the rapid growth of wireless applications, security in wireless transmissions has been raised as a critical issue. Currently, most security mechanisms are applied to upper layers of the protocol stack such as security algorithms Wired Equivalent Privacy (WEP) and WEP2. However, due to the highly standardized wireless communications protocol, security and confidentiality on physical layer becomes vulnerable to eavesdropping and malicious attacks in many circumstances. Specifically, signal transmission in a wireless channel on physical layer becomes transparent to eavesdroppers within the coverage who know the transmission parameter and protocols between the communication parties. As a result, malicious attacks could be easily launched by capturing and recovering the intercepted data. Therefore, PHY security has become a challenging problem in wireless communications [2].

Among various wireless communication systems, orthogonal frequency division multiplexing (OFDM) is one of the most popular and standardized models due to its high efficiency of spectrum usage and robustness to inter-symbol interference (ISI). Nevertheless, unique features in standardized OFDM systems such as cyclic prefix (CP), in-band pilots and distinct spectrum characteristic, on the other hand, may also divulge transmission details. These properties could be exploited by eavesdroppers to easily capture, synchronize and recover the transmitted data

on PHY.

Consequently, the security on PHY becomes an emergent requirement for wireless communication systems. For OFDM systems, there are some research efforts made in this area [50] [51]. A chaos based frequency domain bit-interleaving method for OFDM systems was proposed in [9]. The fundamental idea is focused on a random interleaver which is used to scramble data in the frequency domain. The benefit of this method is its simplicity of the system because the scrambling process is achieved in the frequency domain and the remaining parts of the OFDM system will be kept unaltered. However, the problem is also obvious since it still maintains the characteristics of OFDM transmissions in frequency domain. Any eavesdropper can detect and recognize the OFDM signal and apply corresponding decoding techniques such as blind parameter estimation. Constellation rotation and noise insertion approaches to enhance the security of the OFDM system were proposed in [10] and [11]. These approaches rotate the constellation diagram in the frequency domain and change some features of OFDM transmission as well. However, the constellation alternation only modifies the phase angle, where the signals are still vulnerable to being cryptanalyzed.

In this chapter, a security enhancement for the OFDM system by using time domain scrambling is proposed. Sample sequence in each OFDM symbol is scrambled in the time domain to cancel transmission characteristics. The system not only changes phase angles but also amplitudes in the constellation diagram over each subcarrier. Depending on frequency of changing permutation order during the entire transmission, this approach may provide varying constellation patterns from time to time. Moreover, due to the pseudo random combination of random data and permutation order, it can also generate a variety of constellation patterns to increase interception complexity at illegitimate receivers without dramatic performance degradation.

The rest of this chapter is organized as follows: In section 2, the conventional OFDM system and its potential security problem are reviewed. Section 3 gives out the proposed system including system descriptions and related theoretical analysis. In section 4, the secrecy capacity used as the metric of secrecy is presented. Section 5 shows related simulation results. Finally, it comes to the conclusions in section 6.

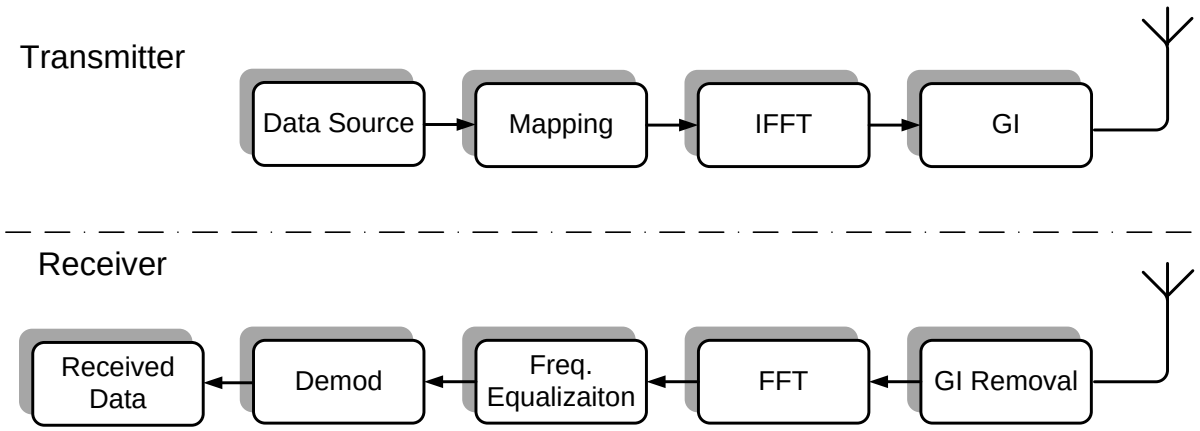


Figure 3.1: Conventional OFDM system diagram.

2 Conventional OFDM System

The research on conventional OFDM system can be traced back around half-century ago [52]. The principle of OFDM systems, as shown in Figure 3.1, is to modulate data sequences onto a series of orthogonal subcarriers by applying the N-point Inverse Fast Transformation (IFFT) to each OFDM block $b(n)$ in order to obtain the time domain symbol $s(m)$:

$$s(m) = \text{IFFT}\left[b(n)\right] = \sum_{i=0}^{N-1} b(i)e^{j2\pi im/N}. \tag{3.1}$$

After passing through the channel and removing the guard interval (GI), the received signal $y(m)$ is converted to the frequency domain. The corresponding FFT of $y(m)$ is $Y(n)$:

$$Y(n) = \text{FFT}\left[y(m)\right] = \sum_{i=0}^{N-1} y_i(i)e^{-j2\pi in/N}. \tag{3.2}$$

Then the following demodulation is used to make decisions on each subcarrier in the frequency domain and recover the original transmitted binary data. Although in conventional OFDM systems, scrambling and interleaving techniques are generally used for peak-to-average power ratio (PAPR) reduction [53] [54] [55] [45], they may hide transmission features in the process.

In previous work, secured OFDM systems by using scrambling or interleaving techniques

have been studied but major emphasis is laid on the frequency domain. Although the system complexity is acceptable, the feature of constellation of scrambled signals remains unchanged as before. It is still possible for eavesdroppers to analyze intercepted signal on the frequency spectrum and crack the system on PHY. The system security is at risk due to this potential vulnerability. Therefore, a security enhanced OFDM scheme by using time domain scrambling techniques is proposed in this chapter to fill the gap.

3 Security Enhanced Time Domain Scrambling OFDM System

In this section, the system description of the proposed security enhanced time domain scrambling OFDM system is provided. The corresponding analysis on constellation transformation effect from the time domain scrambling is analyzed as well.

3.1 System Description

The assumptions are:

1. Illegitimate receiver knows all standardized transmission parameters between legitimate users

2. Secret keys to permutation order are pre-shared by legitimate users but not by illegitimate user.

The proposed time domain scrambling scheme rearranges the sample sequence in one symbol as shown in Figure 3.2. Once scrambled in the time domain in a coded way, the transmitted signal will be greatly changed and varied on the frequency spectrum which no longer exhibits like an OFDM signal. The original data can only be obtained by the legitimate receiver who knows the time domain permutation order. Meanwhile, the illegitimate receiver who is ignorant of the permutation can merely convert the time domain sequence of the intercepted signal into the frequency domain. Consequently, the data received and processed by the illegitimate receiver will not be the same as the original one.

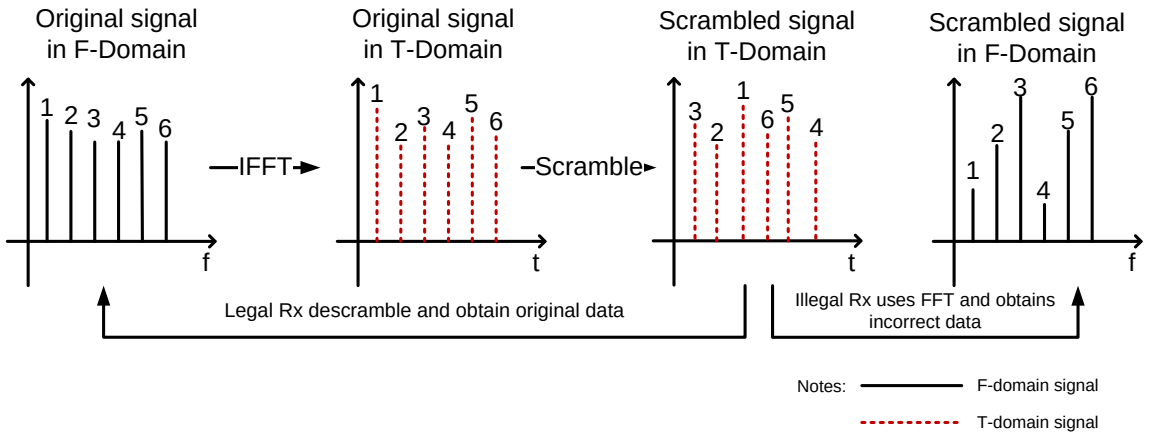


Figure 3.2: Security enhancement based on time domain scrambling in OFDM systems.

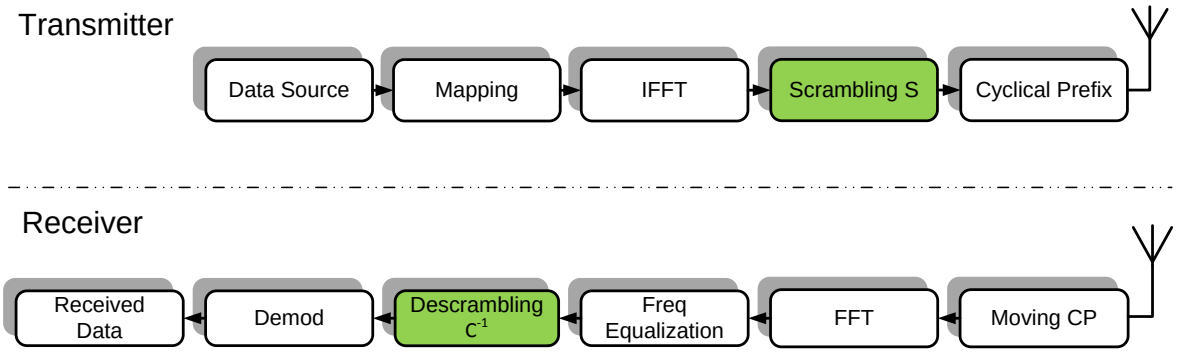


Figure 3.3: Block diagram of the time domain scrambling security-enhanced OFDM .

The system diagram of proposed scheme is shown in Figure 3.3. Similar to the conventional OFDM system, the bit stream is firstly mapped into symbols according to a specific modulation scheme such as BPSK, QPSK, QAM and etc. Complex symbols are modulated onto N-subcarriers by using N-Point IFFT block to form an OFDM symbol. In the proposed system, one scrambling block S is used after IFFT block to rearrange the time domain sequence. Correspondingly, in the receiver, one de-scrambling block C^{-1} is required to turn the sequence back to its original order.

A brief introduction to the signal flow in the system is presented here and detailed explanations will be provided in the next subsection. According to the description above, the

transmitted signal **x** can be written as:

$$\mathbf{x} = \mathbf{b}\mathbf{F}^{-1}\mathbf{S}_R\mathbf{G}, \tag{3.3}$$

where **b** is the data sequence; $\mathbf{S}_R$ is the time domain scrambling matrix; $\mathbf{F}^{-1}$ is the IFFT matrix; **G** is the CP insertion matrix. Respectively, the received signal **y** at the receiver is:

$$\begin{aligned} \mathbf{y} =& \mathbf{b}\mathbf{F}^{-1}\mathbf{S}_R\mathbf{G}\mathbf{H}_t\mathbf{T} + \mathbf{w} \\ =& \mathbf{b}\mathbf{F}^{-1}\mathbf{S}_R\mathbf{F}\mathbf{H}_f\mathbf{F}^{-1} + \mathbf{w}, \end{aligned} \tag{3.4}$$

where **F** is the FFT matrix; **w** is the additive white gaussian noise vector; $\mathbf{H}_t$ is the CIR matrix in the time domain; $\mathbf{H}_f$ is a diagonal CIR matrix in the frequency domain; **T** is the truncation matrix used to remove CP. Thus **GhT** is a circular square matrix which equals to $\mathbf{F}\mathbf{H}_f\mathbf{F}^{-1}$. Finally, the recovery procedure could be described as:

$$\mathbf{b}_r = \mathbf{y}\mathbf{F}\mathbf{H}_f^{-1}\mathbf{C}^{-1}, \tag{3.5}$$

where $\mathbf{H}_f^{-1}$ and $\mathbf{C}^{-1}$ are respectively the inverse diagonal CIR matrix and the inverse constellation rotation matrix.

3.2 Constellation Transformation

The impact of the time domain scrambling is the constellation transformation effect which is used to cover the transmission features of the OFDM system. Suppose one mapped block **b** can be written as $\mathbf{b} = [b_0\ b_2\ b_3\ ...\ b_{N-1}]$, where N elements are complex number in the frequency domain.

By using N-Point IFFT transformation process, the time domain OFDM symbol can be represented as:

$$\mathbf{b}_t = \mathbf{b}\mathbf{F}^{-1}, \tag{3.6}$$

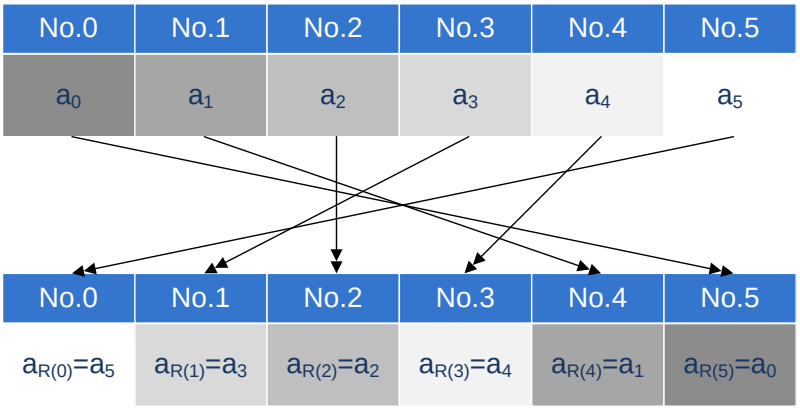


Figure 3.4: An illustration of the permutation function R.

where $\mathbf{F}^{-1}$ is:

$$\mathbf{F}^{-1} = \frac{1}{N}\begin{pmatrix} W_N^{-0\cdot 0} & W_N^{-0\cdot 1} & W_N^{-0\cdot 2} & \dots & W_N^{-0\cdot(N-1)} \\ W_N^{-1\cdot 0} & \dots & \dots & \dots & W_N^{-1\cdot(N-1)} \\ W_N^{-1\cdot 0} & \dots & \dots & \dots & W_N^{-2\cdot(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ W_N^{-(N-1)\cdot 0} & W_N^{-(N-1)\cdot 1} & W_N^{-(N-1)\cdot 2} & \dots & W_N^{-(N-1)\cdot(N-1)} \end{pmatrix}, \tag{3.7}$$

where

$$W_N^{-n\cdot k} = e^{2\pi j\cdot\frac{n\cdot k}{N}}.$$

The time domain scrambling matrix is an $N \times N$ Permutation Matrix. The permutation function R of N elements denotes permutation mapping:

$$R :< 0, 1, 2, ...N-1 > \rightarrow < 0, 1, 2, ...N-1 > . \tag{3.8}$$

$R(n)$ represents that sample in the nth position of scrambled sequence is occupied by sample in the $R(n)^{th}$ element of original sequence.

For example, as illustrated in Figure 3.4, if original sequence is $[a_0, a_1, a_2, a_3, a_4, a_5]$ and scrambled sequence is $[a_5, a_3, a_2, a_4, a_1, a_0]$, then:

$$R(0) = 5, R(1) = 3, R(2) = 2, R(3) = 4, R(4) = 1, R(5) = 0.$$

Thus, the scrambling matrix can be written as:

$$\mathbf{S}_R = \left(\mathbf{e}_{R(0)} \quad \mathbf{e}_{R(1)} \quad \mathbf{e}_{R(2)} \ldots \quad \mathbf{e}_{R(N-1)}\right), \tag{3.9}$$

where $\mathbf{e}_{R(n)}$ denotes a column vector with N elements in which there are 1 in the $R(n)^{th}$ position and 0s in any other positions.

For instance: In above example the scrambling matrix is supposed to be:

$$\mathbf{S}_R = \left(\mathbf{e}_{R(0)} \quad \mathbf{e}_{R(1)} \quad \mathbf{e}_{R(2)} \quad \mathbf{e}_{R(3)} \quad \mathbf{e}_{R(4)} \quad \mathbf{e}_{R(5)}\right) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{3.10}$$

The permutation function R is corresponding to a certain codeword to generate different permutation orders.

By using $\mathbf{S}_R$ matrix, scrambled time domain sequence $\mathbf{B}_{ts}$ can be obtained:

$$\begin{aligned} \mathbf{b}_{ts} &= \mathbf{b}_t \mathbf{S}_R \\ &= \mathbf{b}\mathbf{F}^{-1}\mathbf{S}_R \end{aligned} \tag{3.11}$$

In order to examine the frequency domain performance of scrambled time domain symbols, $\mathbf{b}_{ts}$ is required to be converted back into the frequency domain again by using an FFT matrix $\mathbf{F}$. Hence,

$$\begin{aligned} \mathbf{b}_{tsf} &= \mathbf{b}_{ts}\mathbf{F} = \mathbf{b}_t \mathbf{S}_R \mathbf{F} \\ &= \mathbf{b}\mathbf{F}^{-1}\mathbf{S}_R\mathbf{F} \end{aligned} \tag{3.12}$$

represents the time domain scrambled symbol in the frequency domain.

The equation above points out that the transformation matrix is only relative to $\mathbf{F}^{-1}$ $\mathbf{S}_R$ $\mathbf{F}$.

Define constellation rotation matrix (CRM) $\mathbf{C}$ as

$$\mathbf{C} = \mathbf{F}^{-1}\mathbf{S}_R\mathbf{F}. \tag{3.13}$$

$R(n)$ is used to represent the algebra calculation of $\mathbf{C}$.

$$\mathbf{C} = \frac{1}{N}\begin{pmatrix} \sum_{n=0}^{n=N-1} W_N^{-0\cdot R(n)+n\cdot 0} & \sum_{n=0}^{n=N-1} W_N^{-0\cdot R(n)+n\cdot 1} & \cdots & \sum_{n=0}^{n=N-1} W_N^{-0\cdot R(n)+n\cdot (N-1)} \\ \sum_{n=0}^{n=N-1} W_N^{-1\cdot R(n)+n\cdot 0} & \sum_{n=0}^{n=N-1} W_N^{-1\cdot R(n)+n\cdot 1} & \cdots & \sum_{n=0}^{n=N-1} W_N^{-1\cdot R(n)+n\cdot (N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{n=0}^{n=N-1} W_N^{-(N-1)\cdot R(n)+n\cdot 0} & \sum_{n=0}^{n=N-1} W_N^{-(N-1)\cdot R(n)+n\cdot 1} & \cdots & \sum_{n=0}^{n=N-1} W_N^{-(N-1)\cdot R(n)+n\cdot (N-1)} \end{pmatrix}. \tag{3.14}$$

Let

$$u_m(K) = \frac{1}{N}\cdot \sum_{n=0}^{n=N-1} W_N^{-K\cdot R(n)+n\cdot m}. \tag{3.15}$$

The matrix $\mathbf{C}$ in the above equation can be simplified as

$$\mathbf{C} = \begin{pmatrix} u_0(0) & u_1(0) & u_2(0) & \cdots & u_{N-1}(0) \\ u_0(1) & u_1(1) & u_2(1) & \cdots & u_{N-1}(1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ u_0(N-1) & u_1(N-1) & u_2(N-1) & \cdots & u_{N-1}(N-1) \end{pmatrix}. \tag{3.16}$$

The scrambled symbol in the frequency domain can be represented by using the simplified CRM $\mathbf{C}$:

$$\begin{aligned} \mathbf{b}_{tsf} &= \mathbf{b}\mathbf{C} \\ &= [b_0^S\ b_1^S\ b_2^S\ \ldots\ b_{N-1}^S], \end{aligned} \tag{3.17}$$

where

$$b_m^S = \sum_{K=0}^{K=N-1} b(K)u_m(K). \tag{3.18}$$

Therefore, the descrambling matrix $\mathbf{C}^{-1}$ is the inverse matrix of the CRM $\mathbf{C}$, which is:

$$\mathbf{C}^{-1} = \frac{\mathbf{C}^*}{|\mathbf{C}|}, \tag{3.19}$$

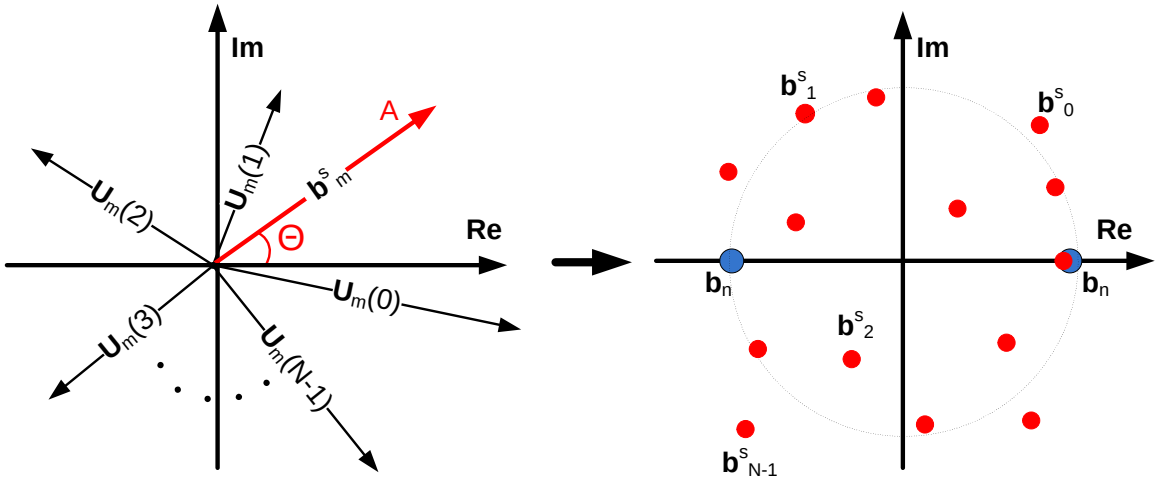


Figure 3.5: Generation of constellation pattern by means of constellation transformation with mode A and phase Θ.

where, $\mathbf{C}^*$ is the adjugate matrix of $\mathbf{C}$ and $|\mathbf{C}|$ is the determinant.

In addition, as column vector $\mathbf{u}_m$ is a group of complex number, the multiplication of $\mathbf{b}$ and $\mathbf{u}_m$ can be regarded as a constellation transformation of the original signal $\mathbf{b}$ by a mode A and phase Θ as shown in Figure 3.5.

Moreover, the vector $\mathbf{u}_m$ is not only a constellation transformation factor but also an orthogonal basis function. Consider $u_{m1}(K)$ and $u^*_{m2}(K)$

$$\begin{aligned} u_{m1}(K) &= \frac{1}{N} \cdot \sum_{n=0}^{n=N-1} W_N^{-K \cdot R(n)+n \cdot m1} \\ &= \frac{1}{N}[W_N^{-K \cdot R(0)+0 \cdot m1} + W_N^{-K \cdot R(1)+1 \cdot m1} \ldots + W_N^{-K \cdot R(N-1)+(N-1) \cdot m1}] \end{aligned} \tag{3.20}$$

$$\begin{aligned} u^*_{m2}(K) &= \frac{1}{N} \cdot \sum_{n=0}^{n=N-1} W_N^{K \cdot R(n)-n \cdot m2} \\ &= \frac{1}{N}[W_N^{K \cdot R(0)-0 \cdot m2} + W_N^{K \cdot R(1)-1 \cdot m2} \ldots + W_N^{K \cdot R(N-1)-(N-1) \cdot m2}] \end{aligned} \tag{3.21}$$

The multiplication of $u_{m1}(K)$ and $u^*_{m2}(K)$ can be obtained:

$$\begin{aligned} u_{m1}(K) * u^*_{m2}(K) = &\frac{1}{N^2}[W_N^{-K(R(0)-R(0))+0m1-0m2} + W_N^{-K(R(0)-R(1))+0m1-1m2} ... + W_N^{-K(R(0)-R(N-1))+0m1-(N-1)m2} \\ &+W_N^{-K(R(1)-R(0))+1m1-0m2} + W_N^{-K(R(1)-R(1))+1m1-1m2} ... + W_N^{-K(R(1)-R(N-1))+1m1-(N-1)m2} \\ &\vdots \\ &\vdots \\ &+W_N^{-K(R(N-1)-R(0))+(N-1)m1-0m2} + W_N^{-K(R(N-1)-R(1))+(N-1)m1-1m2} ... + W_N^{-K\cdot 0+(N-1)(m1-m2)}] \end{aligned} \tag{3.22}$$

Notice that, for $W_N^{KC} = e^{-2\pi j \cdot \frac{K \cdot C}{N}}$, if constant integer $C \neq 0$, then

$$\sum_{K=0}^{K=N-1} W_N^{KC} = 0.$$

if $C = 0$, then

$$\sum_{K=0}^{K=N-1} W_N^{KC} = N$$

Also notice that, as mentioned in Equation 3.8 about the permutation function,

$$R(a) \neq R(b), \ if \ a \neq b$$

According to these prerequisites, it is possible to obtain and simplify the summation of the multiplication of $u_{m1}(K)$ *and* $u^*_{m2}(K)$:

$$\begin{aligned} \sum_{K=0}^{K=N-1} u_{m1}(K) * u^*_{m2}(K) = &\frac{1}{N^2}[N * W_N^{0(m1-m2)} + 0 ... + 0 \\ &+0 + N * W_N^{1(m1-m2)} ... + 0 \\ &\vdots \\ &\vdots \\ &+0 + 0 ... + N * W_N^{(N-1)(m1-m2)}] \\ = &\frac{1}{N} \sum_{n=0}^{N-1} W_N^{n\cdot(m1-m2)} \end{aligned} \tag{3.23}$$

Therefore, it is approved that the auto-correlation of u_m meets the requirement of an orthogonal basis function:

$$\sum_{K=0}^{K=N-1} u_{m1}(K) * u_{m2}^{*}(K) = \begin{cases} 1, & m1 = m2 \\ 0, & m1 \neq m2 \end{cases}. \tag{3.24}$$

The derivation by far reveals that the time domain scrambled signal can be regarded as a projection of original signal onto a new coordinate. The new coordinate depends on permutation function R. With R changing, different constellation patterns yield as shown in Figure 3.6. (a) denotes the original constellation while (b), (c)and (d) denote the scrambled constellation patterns of a BPSK modulation scheme in OFDM system.

If permutation is only a sequential shift of the sequence, it creates a constellation rotation pattern in phase as shown in (a) and (b). Otherwise, a random-like constellation pattern yields as shown in (c) which changes both amplitude A and phase Θ. As long as legitimate users changes function R from time to time, the system will create varying patterns and it will become difficult for eavesdropper to follow and discover which kind of modulation scheme is actually used during current transmission.

4 Secrecy Capacity

In order to measure the security capability of the proposed system, the secrecy capacity of OFDM system is investigated in this section. The secrecy capacity stands for limits on the amount of information that can be reliably communicated in a way that an illegitimate receiver cannot decode the information [56] [57]. According to [58], it is defined as:

$$\begin{aligned} C_s &= C_l - C_i \\ &= \log(1 + \frac{P}{N_l}) - \log(1 + \frac{P}{N_i}), \end{aligned} \tag{3.25}$$

where C_l is the channel capacity of the legitimate receiver and C_i indicates the channel capacity of the illegitimate receiver. Here P denotes the signal power. N_l and N_i denote the noise powers for the legitimate and the illegitimate receiver correspondingly.

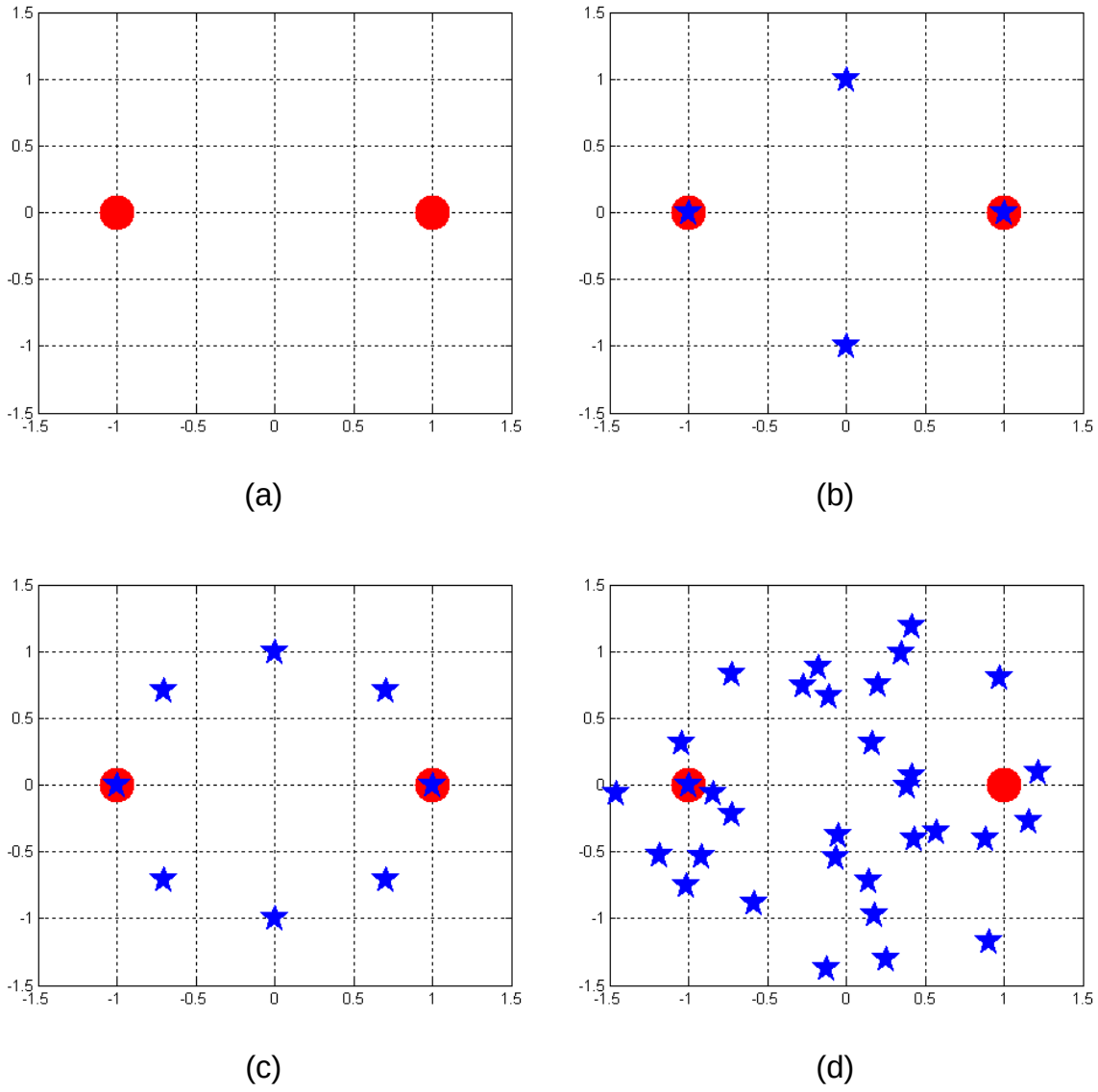


Figure 3.6: Scrambled constellation patterns of a BPSK modulation in time domain scrambling OFDM system.

In an OFDM system, as the transmitted signal is modulated onto several subcarriers, the signal on each subcarrier occupies an independent channel. Therefore the secrecy capacity of an OFDM system is a summation of secrecy capacity of every subcarrier channel. For our proposed system, the secrecy capacity is given out:

$$\begin{aligned} C_s &= \sum_{n=1}^{N} C_{s_n} \\ &= \sum_{n=1}^{N} \left(\log(1 + \frac{P_n}{N_{ln}}) - \log(1 + \frac{P_n}{N_{in}}) \right). \end{aligned} \tag{3.26}$$

where N is the total number of sub-carriers and n is the subcarrier index; $\frac{P_n}{N_{in}}$ and $\frac{P_n}{N_{ln}}$ are signal to noise ratio on each subcarrier which are determined by the deviation of received symbol from sent ones. Denote transmitted symbols as b_s and received symbols at the illegitimate receiver as b_r.

Since each subcarrier is narrow band compared with the bandwidth used for transmission, we consider each subcarrier channel as flat fading channel. Taking *nth* subcarrier into consideration, we may express the received signal b_{rn} at illegitimate receiver:

$$b_{rn} = \sqrt{P_{sn}} h_n c_n b_{sn} + n_{en}, \tag{3.27}$$

where P_{sn} is the transmitted power and and n_{en} is the noise over *nth* subcarrier; $c_n = \frac{\sum_{i=0}^{i=N-1} b_{si} u_n(i)}{b_{sn}}$ stands for the complex constellation transformation factor that caused by time domain scrambling. Equivalently,

$$\begin{aligned} \hat{b}_{rn} =& c_n b_{sn} + \frac{n_{en}}{\sqrt{P_{sn}} h_n} \\ =& b_{sn} + c_n b_{sn} - b_{sn} + \frac{n_{en}}{\sqrt{P_{sn}} h_n} \\ =& b_{sn} + \left[\sum_{i=0}^{i=N-1} b_{si} u_n(i) - b_{sn} \right] + \frac{n_{en}}{\sqrt{P_{sn}} h_n} \\ =& b_{sn} + \hat{n}_{en}, \end{aligned} \tag{3.28}$$

where $\hat{n}_{en} = \left[\sum_{i=0}^{i=N-1} b_{si} u_n(i) - b_{sn} \right] + \frac{n_{en}}{\sqrt{P_{sn}} h_n}$. As can be observed, the equivalent noise $\hat{n}_{en}$ includes two components: inter-carrier interference (ICI) from other subcarriers and additive noise from channel. In another point of view, the time domain scrambling process also e-

quivalently increase the noise power if correct descrambling process is not implemented. The averaged noise power N_{in} is hence regarded as the summation of squares of deviations between received signals and sent signals:

$$N_{in} = \frac{1}{K}\sum_{k=1}^{K} E\left[|\hat{b}_{rn_k} - b_{sn_k}|^2\right], \tag{3.29}$$

where K is the total number of symbols transmitted on each subcarrier. The definition of N_{ln} is similar to N_{in}. Signal power P_n over *nth* subcarrier equals to:

$$P_n = \frac{1}{K}\sum_{k=1}^{K} E\left[|b_{sn_k}|^2\right]. \tag{3.30}$$

Due to the randomness of the constellation transformation introduced by the scrambling process, symbols at the illegitimate receiver deviate from the original constellation points. If C_s is positive, it indicates the system is able to transmit signals to the desired receiver and avoid being cracked by eavesdroppers. If C_s is negative, illegitimate receivers will have a better command of the received signal than the legitimate receiver which means the system is insecure. Thus, the higher C_s is, the more secure the system will be.

In the proposed system, once the constellation diagram is transformed, the received signal at the illegitimate receiver side becomes random-noise-like signal. From the perspective of the illegitimate receiver, SNR will become constantly low.

5 Time Synchronization

As the scrambling scheme is operated in time domain, the inevitable time varying impairments caused by any possible synchronization error between transmitter and receiver raise our interests to investigate its impacts on our proposed scheme.

5.1 Time Offset Analysis

According to Equation (3.18), the scrambled symbol b_m^S in frequency domain is considered as a projection from the original symbol $b(K)$ with a series of constellation transformation

factors $u_m(K)$. At the receiver, if a time offset $\triangle t$ is introduced, the actual time domain signal $S(n + \triangle t)$ equals to:

$$\begin{aligned} S(n + \triangle t) &= I\widetilde{FFT}(\sum b(K)u_m(K)) \\ &= I\widetilde{FFT}(b_m^S) \\ &= \frac{1}{N}\sum_{m=0}^{m=N-1} b_m^S W_N^{-m(n+\Delta t)} \end{aligned} \tag{3.31}$$

The equivalent frequency domain signal $\bar{\bar{S}}$, which is converted from $S(n + \triangle t)$, can be described as:

$$\begin{aligned} \bar{\bar{S}}(L) =& FFT(S(n + \triangle t)) \\ =& \sum_{n=0}^{N-1}(\frac{1}{N}\sum_{m=0}^{m=N-1} b_m^S W_N^{-m(n+\Delta t)})W_N^{Ln} \\ =& \frac{1}{N} * [(b_0^S W_N^{-0(0+\Delta t)} + b_1^S W_N^{-1(0+\Delta t)} ... + b_L^S W_N^{-(L)(0+\Delta t)} ... + b_{N-1}^S W_N^{-(N-1)(0+\Delta t)}) * W_N^{L0} \\ &+ (b_0^S W_N^{-0(1+\Delta t)} + b_1^S W_N^{-1(1+\Delta t)} ... + b_L^S W_N^{-(L)(1+\Delta t)} ... + b_{N-1}^S W_N^{-(N-1)(1+\Delta t)}) * W_N^{L1} \\ &\vdots \\ &\vdots \\ &+ (b_0^S W_N^{-0(N-1+\Delta t)} + b_1^S W_N^{-1(N-1+\Delta t)} ... + b_L^S W_N^{-(L)(N-1+\Delta t)} ... + b_{N-1}^S W_N^{-(N-1)(N-1+\Delta t)}) * W_N^{L(N-1)}] \end{aligned} \tag{3.32}$$

If $L - m \neq 0$, then

$$\sum_{n=0}^{n=N-1} W_N^{(L-m)*n} = 0.$$

If $L - m = 0$, then

$$\sum_{n=0}^{n=N-1} W_N^{0*n} = \sum_{n=0}^{n=N-1} 1 = N.$$

Therefore, Equation 3.32 can be simplified into:

$$\begin{aligned}\bar{\dot{S}}(L) =& FFT(S(n+\triangle t)) \\ =& \frac{1}{N} * b_L^S W_N^{-L\Delta t} * \sum_{n=0}^{n=N-1} W_N^{0*n} \\ =& \frac{1}{N} * b_L^S W_N^{-L\Delta t} * N \\ =& \bar{S}(L) W_N^{-L\Delta t},\end{aligned} \tag{3.33}$$

where $\bar{S}$ is the frequency domain signal without time shift and $\bar{\dot{S}}$ is the frequency domain signal introduced with time shift. Apparently according to the Equation (3.32), a time offset to the scrambled system only equals to a phase shift on the frequency domain. The constellation of frequency domain signal with time shift is similar to the conventional OFDM. Each *Lth* subcarrier is phase-rotated by $2\pi L\Delta t$.

5.2 Time Offset Compensation

However, according to Equation (3.31) and (3.32) above we notice that the scrambling process is not affected by the generation of this shift. The only variation $W_N^{-L\Delta t}$ in the equation is caused by the time shift Δt. This suggests that the time shift cancellation process to the time offset also will not be correlated to scrambling process.

The cancellation process for our proposed system thereby is similar to the conventional cancellation procedure in traditional OFDM system. As long as each sample is adjusted by multiplying a de-variation factor $W_N^{L\Delta t}$ before the de-scrambling process:

$$\bar{S}(L) = \bar{\dot{S}}(L) W_N^{L\Delta t}, \tag{3.34}$$

The time offset will be compensated accordingly and the time synchronization problem will be simply solved.

Although the proposed scrambling system manipulates OFDM symbol on the time domain, the inherent characteristic of this system is only a projection of constellation diagram. Therefore, scrambling process will not cause new synchronization problems to the system. The

traditional way of compensation for time-offset also works perfectly on our proposed system.

5.3 Application Example

In this section, we present an example of our proposed time domain scrambling OFDM system in Wi-fi transmission protocol for the real world application.

802.11a allows transmission and reception of data at 1.5 to 54 $Mbit/s$. It uses the same data link layer protocol and frame format as the original standard but an OFDM based air interface.

We consider the proposed scheme to be utilized in 802.11a protocol. The frame format of the proposed system with 64 sub-carrier OFDM in 802.11a is described as follows:

- Sequence control field: use a two-byte section used for identifying message order as well as eliminating duplicate frames.
- Quality of Service control field: add two-byte section to verify the quality of service.
- Frame body: Contains 1024 bytes of the data sequence. The first 8 bytes are used for channel estimation to generate the scrambling order. The rest 1016 bytes are used for the data from higher layer but scrambled according to specific scrambling order.
- Frame Check Sequence: last 4 bytes used in standard 802.11 frame to check the integrity of retrieved frames. When station receives a frame it can calculate this sequence and compare it to the one received. If match, it is assumed that the frame was not distorted.

6 Simulations

As discussed above, the constellation of the time domain scrambled signal can be regarded as a projection of the original signal. The system performance is not affected by using the time domain scrambling method. Simulations are provided to justify the feasibility and performance of the system.

Figure 3.7 visually illustrates constellations between legitimate and illegitimate receivers of the simulated system over AWGN channel under different signal to noise ratio. Top figures represent constellation diagrams received and processed by the legitimate receiver which

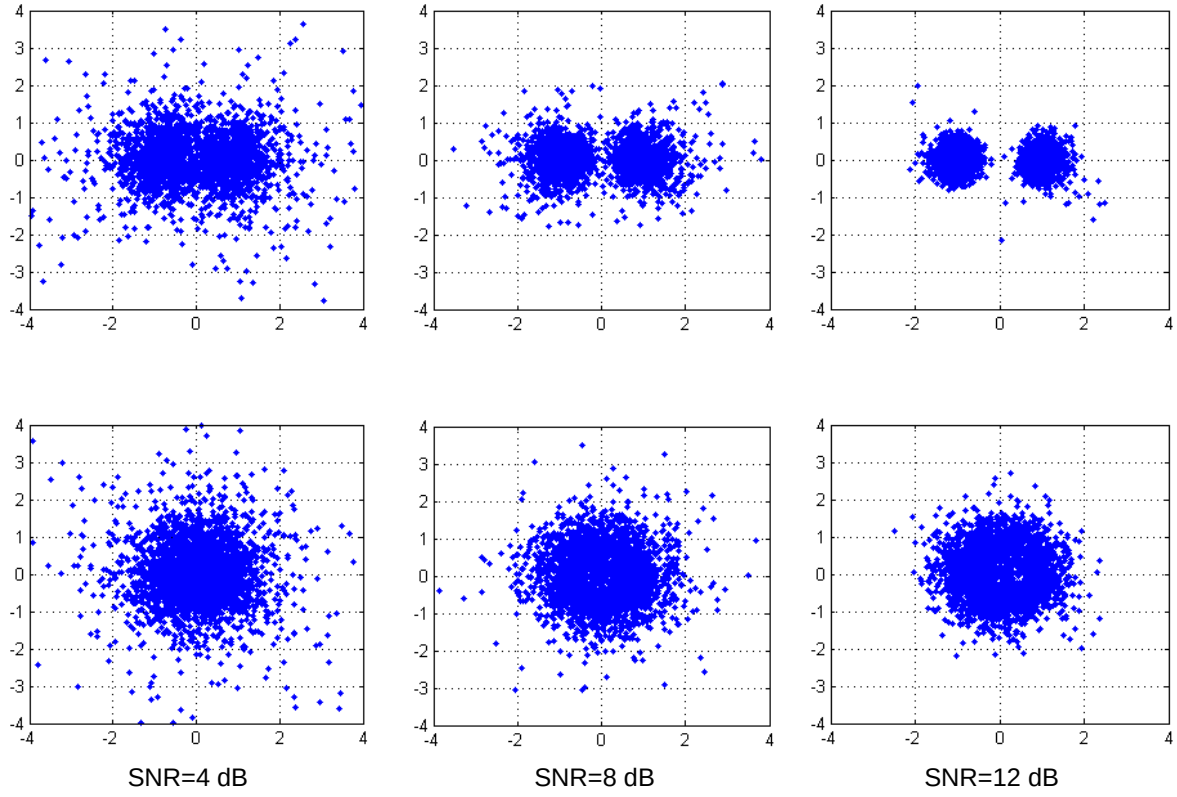


Figure 3.7: BPSK constellations of legitimate and illegitimate receiver over AWGN channel under SNR=4,8,12 dB(From left to right).

knows the permutation and bottom figures are constellations received by the illegitimate receiver. With SNR increasing from 4 to 12 dB, characteristics of the binary phase shift keying (BPSK) modulation scheme become more and more crystal clear for the legitimate constellation. However, constellations received by the illegitimate receiver maintain chaos-like all the time.

Figure 3.8 and Figure 3.9 respectively show the BER performance of proposed the time domain scrambling OFDM system. In order to demonstrate the security enhancement of the proposed system, bit error rate (BER) performances in illegitimate receivers are also included in both figures. In Figure 3.8, when the time domain scrambling is applied, bit error rate in illegitimate user keeps -6.0 dB which is high and almost constant with signal to noise ration (SNR) value rising. It shows that the illegitimate receiver suffers from incredibly higher BER than the legitimate receiver especially in a good transmission environment (high SNR). It also implies that the illegitimate user can hardly detect signal during the entire transmission process.

In Figure 3.9, BER performances using BPSK and quadrapole phase shift keying (QPSK) modulation schemes in Rayleigh channel are shown. The BER curves of the legitimate receiver obey the theoretical values. In comparison, the BER performances of illegitimate receiver over the Rayleigh channel, similar to Figure 3.8, maintain constantly high (approximately around -6.0 dB) if the time domain scrambling is applied. In addition, the secrecy capacity of the system is also shown in the figure. The secrecy capacity is constantly a positive value. It also synchronously rises with SNR from 1 $bits/s$ to 316 $bits/s$. In other words, the equivalent noise containing ICI caused by the scrambling process still has critical impacts on the eavesdropper at high SNR. This means the wiretap channel becomes a worse version of the main channel even if the actual channel condition becomes better.

Figure. 3.10 and Figure. 3.11 demonstrate simulation results for the time synchronization with 1/32, 1/16, 1/8 and 1/4 sampling-interval time offset respectively. As can be observed from Figure. 3.10(a) and 3.10(b), when time offsets are relatively small (1/32 and 1/16 sampling intervals correspondingly), BER curves of legitimate receiver with scrambling are roughly same as those without scrambling. When time offsets become large, e.g. 1/8 and 1/4 sampling intervals in Figure. 3.11(a) and 3.11(b), BER curves of scrambled signal are worse than those with none-scrambled signal. The worst case happens at high SNR. For example, in

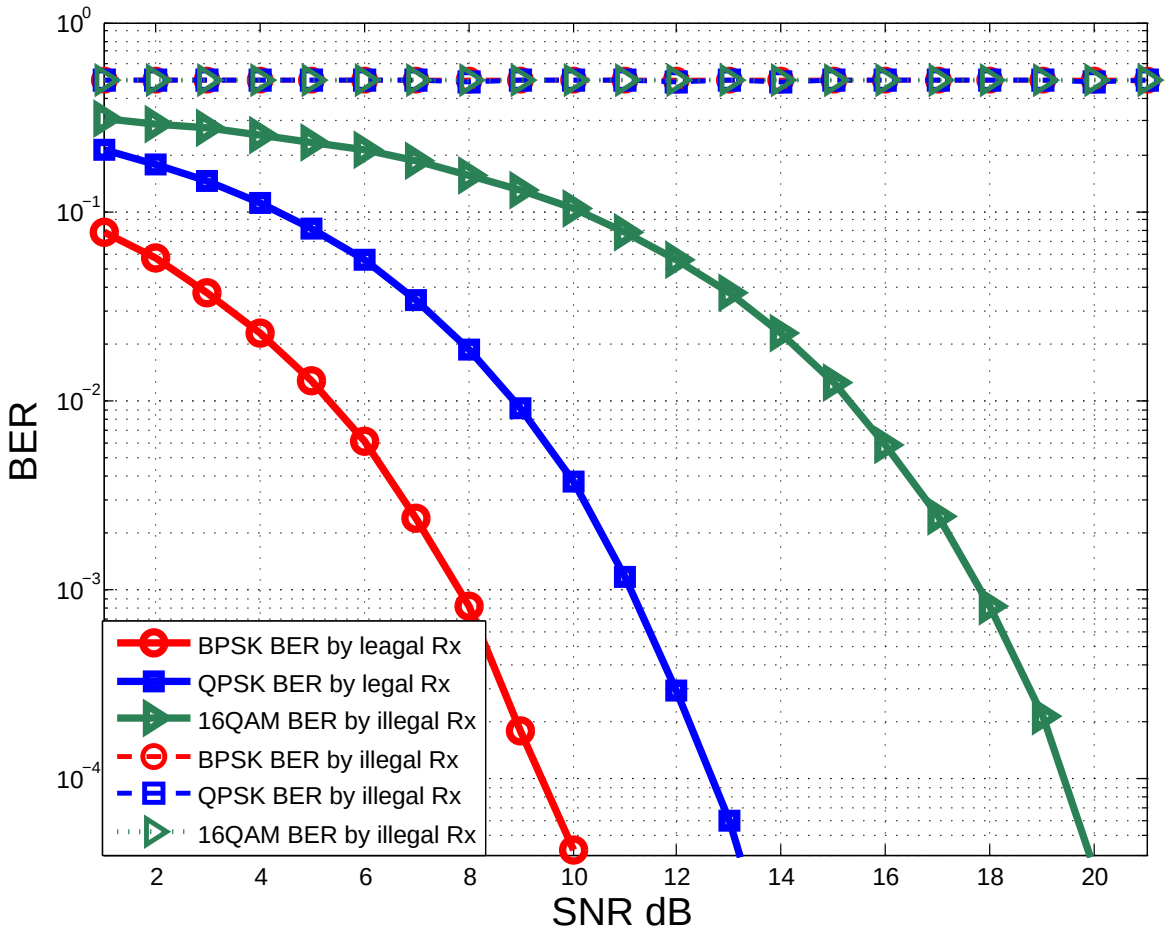
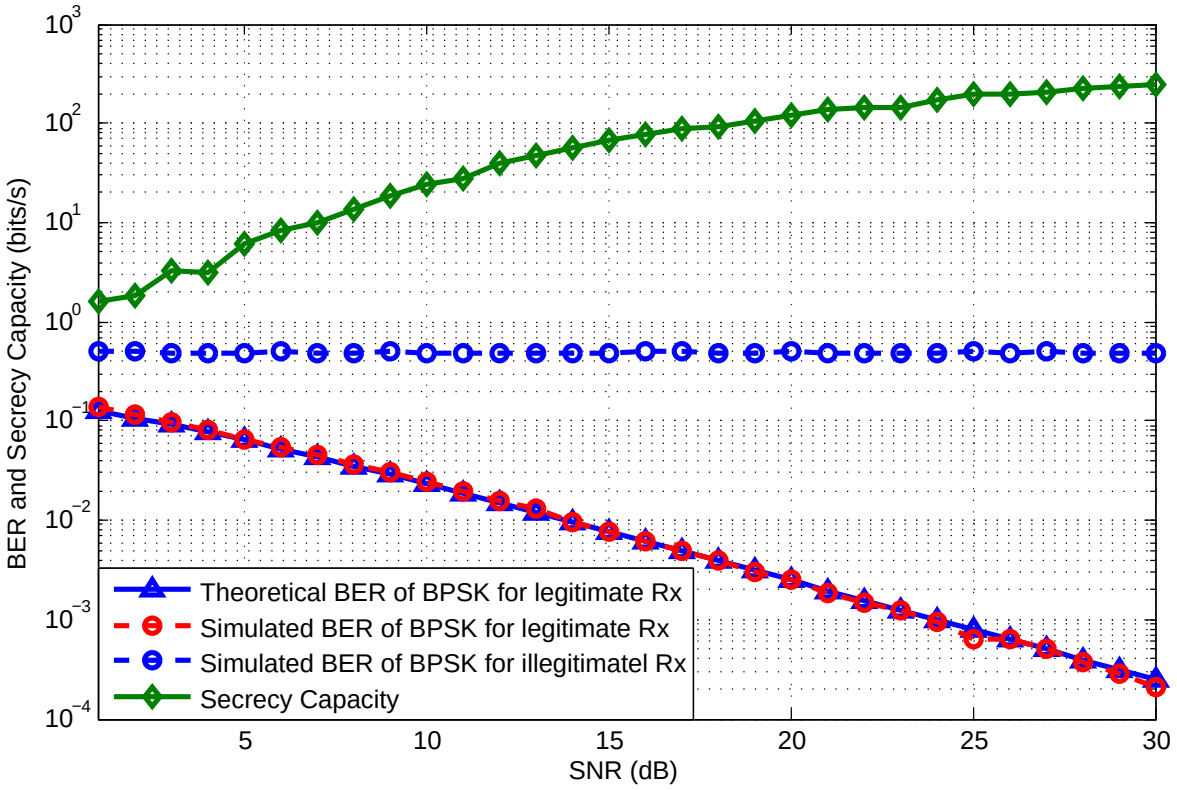
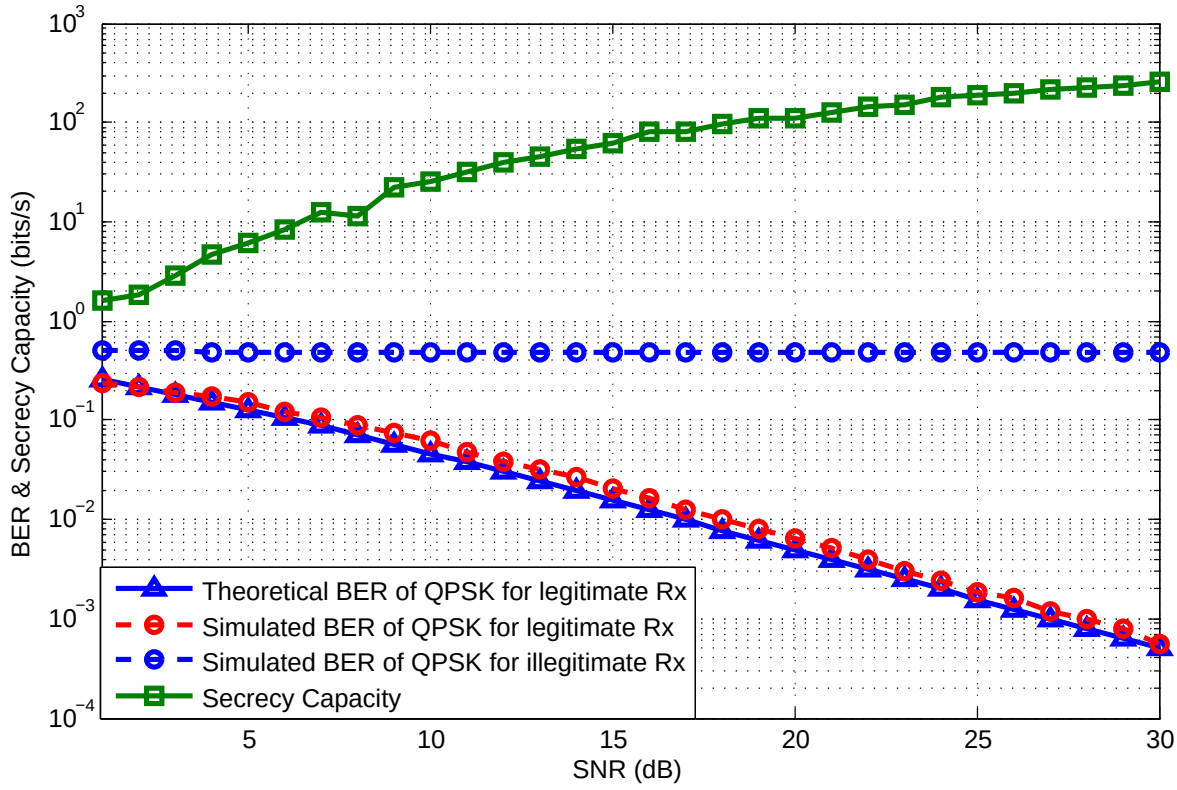


Figure 3.8: BER performance of the proposed time domain scrambling security-enhanced OFDM system over AWGN channel.

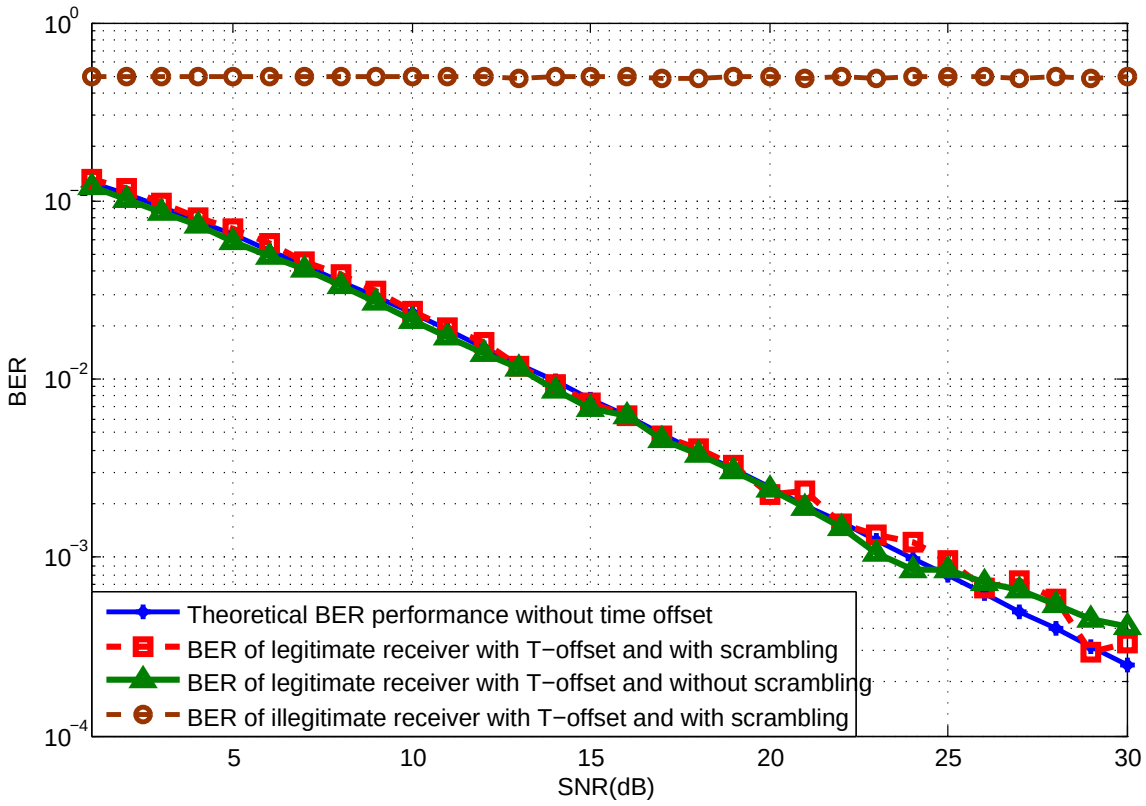


(a) BPSK modulation.

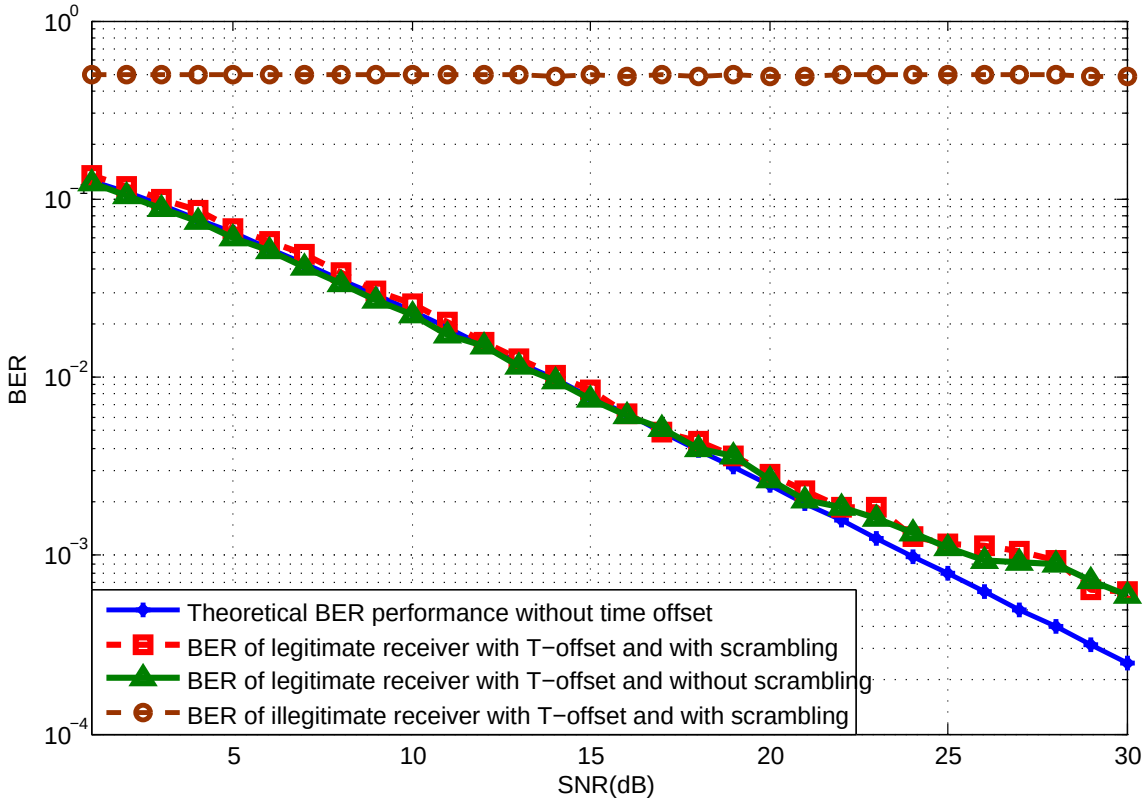


(b) QPSK modulation.

Figure 3.9: BER performance of BPSK and QPSK modulations for the proposed time domain scrambling security-enhanced OFDM system over Rayleigh channel.

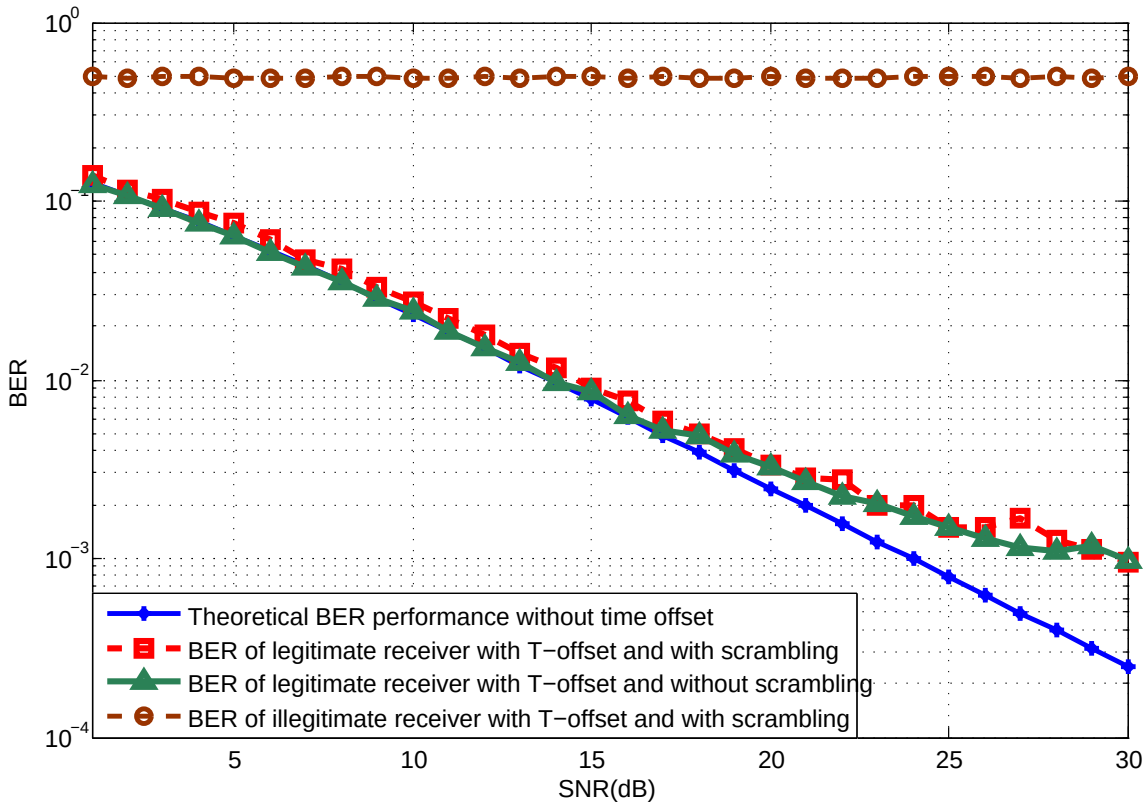


(a) Comparision of scrambled and none-scrambled signals with 1/32 sampling-interval time offset.

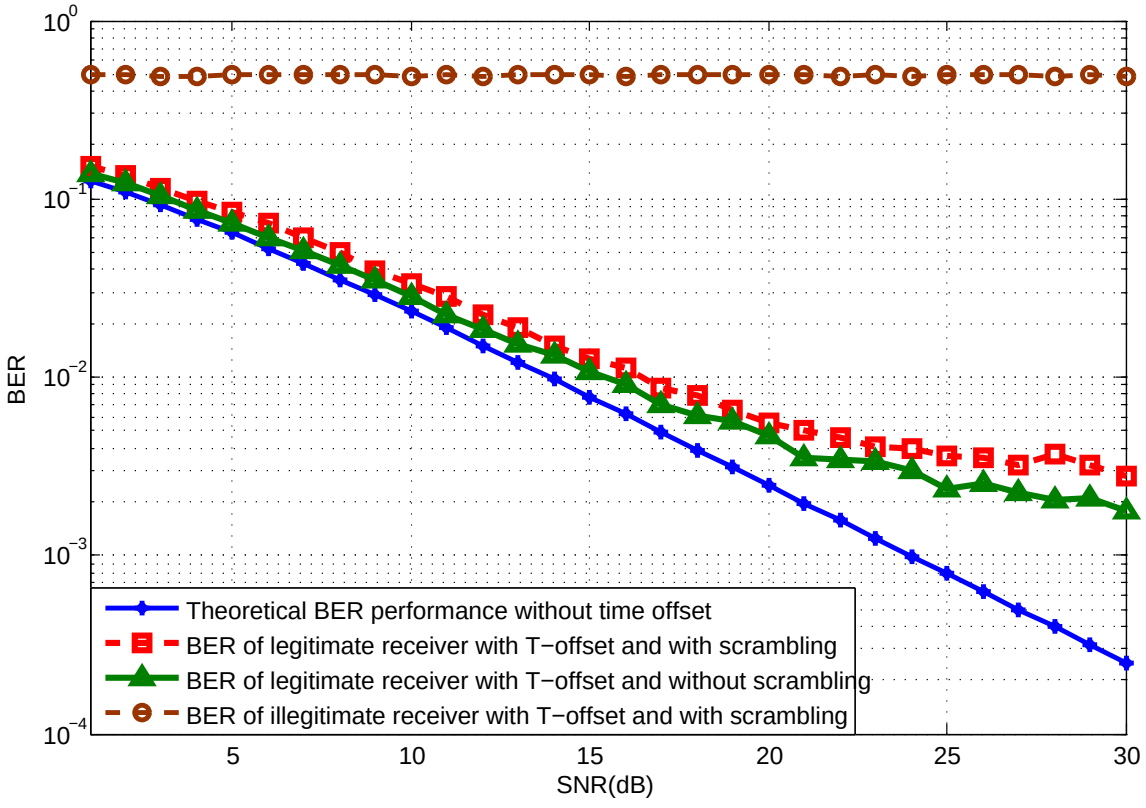


(b) Comparision of scrambled and none-scrambled signals with 1/16 sampling-interval time offset.

Figure 3.10: Simulation results for time domain synchronization.



(a) Comparision of scrambled and none-scrambled signals with 1/8 sampling-interval time offset.



(b) Comparision of scrambled and none-scrambled signals with 1/4 sampling-interval time offset.

Figure 3.11: Simulation results for time domain synchronization (Continued).

between $SNR = 25dB$ and $SNR = 30dB$ of Figure. 3.11(b), scrambled signals have 1 to 2 dB disadvantages in around -25dB BER (roughly 4% to 8% degradations) over none-scrambled signals. This indicates that the scrambling process may result in some degradations when fractional sampling-interval time offsets occur but compared with the overall BER performance, the degradations are inconspicuous and negligible.

From simulation results, we can conclude that the time domain scrambling OFDM scheme is able to enhance the transmission security between transmitters and receivers by transforming the constellation diagrams of signals. On another hand, the proposed system only introduces negligible negative performance on the system compared to the conventional OFDM system.

7 Chapter Summary

In this chapter, a scheme to enhance PHY security for OFDM systems is proposed based on the time domain scrambling technique. According to the scheme, samples in each OFDM symbol are scrambled in the time domain before transmission in order to eliminate the inherent signal statistics features. The resultant signal at the receiver is de-scrambled for subsequent recovery. The proposed scheme significantly increases time complexity for cracking, thereby reducing the possibilities for illegal interception. Our secrecy capacity analysis demonstrates that security capability of the proposed scheme is promising. In addition, our analysis on the proposed time domain scrambling technique shows that the system performance will be retained because the time domain scrambling is equivalent to the constellation transformation.

Chapter 4

Security Enhancement in Cooperative Jamming Using Compromised Secrecy Region Minimization

1 Introduction

Among the existing PHY security mechanisms, cooperative jamming is a promising option for security enhancement by utilizing channel spatial diversity and network cooperation [8]. During the source transmitting stage to the destination, a cooperative node simultaneously sends out a jamming signal to interfere eavesdropper. In doing so, the transmission security can be improved by increasing the secrecy capacity, which represents the capacity difference between the legitimate channel and the eavesdropping channel. The traditional objective for cooperative jamming optimization therefore aims at maximizing the system secrecy capacity.

Several existing works on cooperative jamming optimization strategies can be found in the literature. In [12], a beam-forming technique is applied to jamming signal design subject to transmitting power constraints in a multi-antenna relay model. In [14], generation of jamming signal is studied to reduce the illegitimate channel capacity. The work of [13] considers different power allocation schemes to maximize the secrecy capacity subject to power constraint of each cooperative jammer and relay. Most aforementioned schemes follow the principle of

secrecy capacity maximization. In addition, the majority of these schemes assume pre-known instantaneous channel state information (CSI) of the illegitimate channel for system secrecy optimization. However, in reality, due to the uncertainty and random distribution of eavesdroppers, it is impractical to obtain the short-term CSI of illegitimate nodes. The work of [15] therefore utilized the statistical CSI including path-loss and fading effects of the illegitimate channel to characterize the secrecy region in a small scale jamming system. Compared with [12, 14, 13], the scheme in [15] provides a more practical way to statistically assess the system security risk.

As an extension of [15], we propose a compromised secrecy region (CSR) minimization scheme based on cooperative jamming to enhance communication security. By using path-loss and fading effects of the wireless channel, secrecy region characterized by a specific outage probability is obtained. Unlike conventional secrecy capacity maximization approaches, our proposed method minimize the area of CSR that presents high outage probability by utilizing the traverse algorithm to search the jammer's optimal location and allocated power. In addition, to solve the overflow problem in determining the secrecy region, the associated outage probability is approximated based on an asymptotic expansion for numerical computer simulations. As a result, the limitation in calculating the secrecy region is eliminated. By considering the randomly-distributed eavesdropper in a statistical manner, the proposed scheme can enhance the system security through minimizing unsecured area without the necessity to know the exact eavesdropper's location.

The rest of the chapter is organized as follows. In Section 2, the system model with cooperative jammer is presented. The secrecy region and CSR are then derived and analyzed. Secrecy outage probability approximation along with CSR minimization are described in Section 3. Simulation results on the relationship between CSR and jammer's location and allocated power are provided in Section 4. Finally, it comes to the conclusions in Section 5.

2 System Setup and Secrecy Region Derivation

In this section, we first present the system model for cooperative jamming with one jammer. After briefly introducing the secrecy capacity and associated outage probability, we discuss the

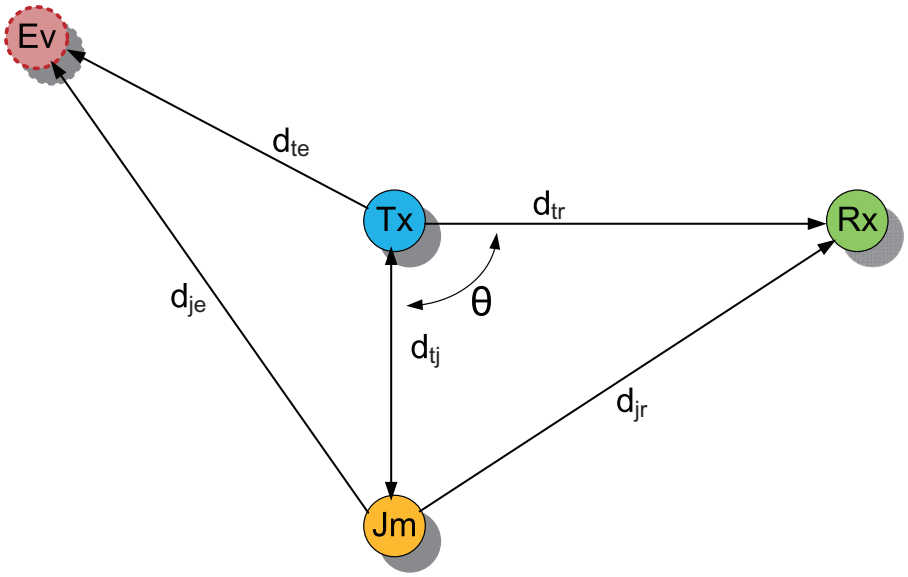


Figure 4.1: System diagram of cooperative jamming with one jammer.

secrecy region and CSR of the considered system.

2.1 System Model

As shown in Figure 4.1, the cooperative jamming system is designed to include one transmitter (Tx), one cooperative jammer (Jm), one legitimate receiver (Rx) and one illegitimate receiver (Ev). Positions of Tx, Jm and Rx are settled in the considered system while the position of Ev is undetermined and may come within the area around Tx.

All the channels are modeled as the Rayleigh fading channel. Jm sends out white Gaussian noise as jamming signals to both Rx and Ev with power P_j, meanwhile Tx broadcasts the useful information signal with power P_t. For simplicity, channel noise N_0 is considered as white Gaussian noise and same to all nodes. The distances between Tx, Jm, Rx and Ev are denoted as d_{tj}, d_{tr}, d_{te}, d_{jr} and d_{je} respectively. The included angle in between d_{tj} and d_{tr} is θ.

2.2 Secrecy Capacity, Outage Probability and Secrecy Region

The secrecy capacity of a wire-tap channel accounts for the difference of channel capacities associated with the legitimate user and the eavesdropper [5]. It indicates the imbalanced

receptiveness of useful information between Rx and Ev in the communication system. Hence the secrecy capacity is defined as [59]:

$$\begin{aligned} C_s &= C_r - C_e \\ &= \frac{1}{2}\ln(1 + SINR_r) - \frac{1}{2}\ln(1 + SINR_e). \end{aligned}$$

where $SINR_r$ and $SINR_e$ are the signal-to-interference-and-noise ratio (SINR) of the corresponding channels. Secure communication is guaranteed when $C_s > 0$. Otherwise, when $C_s < 0$, the system becomes insecure because Ev experiences better channel conditions with higher channel capacity than Rx. Due to the randomness of Rayleigh fading channels, given the secrecy capacity R, the secrecy outage probability can be defined as [60]:

$$P_{out}(R) = P[C_s < R], \tag{4.1}$$

which indicates the occurrence probability of secrecy outage that the secrecy rate C_s is lower than R. In such conditions, the security of the system is compromised.

For both legitimate and illegitimate users, SINR are decided by path-loss and fading effects [15]. The path-loss coefficients are modeled as:

$$L = \frac{c}{d^{\alpha}} \tag{4.2}$$

where c, α and d are the path-loss constant, path-loss exponent and the distance between the two communicating nodes. In Rayleigh fading, the channel power coefficient G follows the exponential distribution:

$$f(G) = \lambda e^{-\lambda G}. \tag{4.3}$$

Without loss of generality, channel power G is modeled as a random variable with unit mean $E(G) = \frac{1}{\lambda} = 1$, hence $\lambda = 1$.

Based on (4.2) and (4.3), the $SINR_r$ of Rx can be expressed by:

$$SINR_r = \frac{P_t L_{tr} G_{tr}}{N_0 + P_j L_{jr} G_{jr}}, \tag{4.4}$$

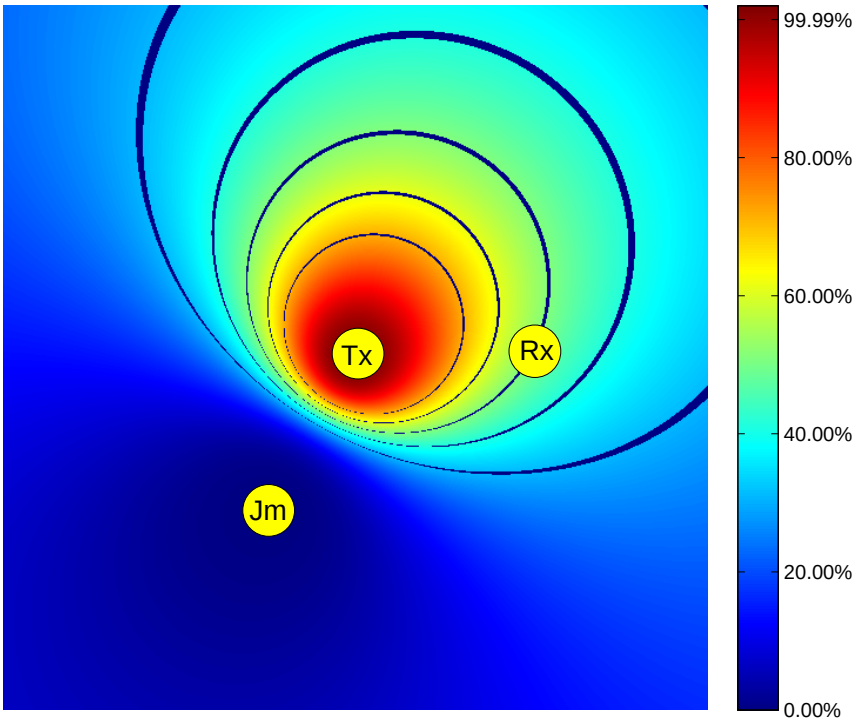


Figure 4.2: Demonstration of the secrecy region map. The simulation model is constructed under $c = 1$, $\alpha = 4$, $R = 0$ and $d_{tj} = d_{tr} = 75m$.

Similarly, the $SINR_e$ of Ev can be obtained by

$$SINR_e = \frac{P_t L_{te} G_{te}}{N_0 + P_j L_{je} G_{je}}, \tag{4.5}$$

where L_{ab} and G_{ab} are the corresponding path-loss coefficient and fading coefficient between node A and node B, respectively.

For now, the secrecy outage probability of the system can be described by distance d and the exponential random variable G as:

$$\begin{aligned} P_{out}(R) = P\Big[&\frac{1}{2}\ln\left(1 + \frac{P_t L_{tr} G_{tr}}{N_0 + P_j L_{jr} G_{jr}}\right) \\ &- \frac{1}{2}\ln\left(1 + \frac{P_t L_{te} G_{te}}{N_0 + P_j L_{je} G_{je}}\right) < R\Big] \\ = P\Big[&G_{tr} < (e^{2R} - 1)\frac{N_0 + P_j L_{jr} G_{jr}}{P_t L_{tr}} \\ &+ e^{2R}\frac{P_t L_{te} G_{te}}{P_t L_{tr}}\frac{N_0 + P_j L_{jr} G_{jr}}{N_0 + P_j L_{je} G_{je}}\Big] \end{aligned} \tag{4.6}$$

As random variables $G_{tr}, G_{jr}, G_{te}, G_{je}$ follow exponential distribution with unit mean and are independent from each other, their joint power density function (pdf) is:

$$\begin{aligned} f(G_{tr}, G_{jr}, G_{te}, G_{je}) =& f(G_{tr}) f(G_{jr}) f(G_{te}) f(G_{je}) \\ =& e^{-G_{tr} - G_{jr} - G_{te} - G_{je}} \end{aligned} \tag{4.7}$$

Then the outage probability can be obtained with a quadruple integral over varialbes $G_{tr}, G_{jr}, G_{te}, G_{je}$:

$$P_{out}[R] = \int_0^{\infty}\!\!\int\!\!\int\!\!\int \left(\int_0^{M} e^{-G_{tr} - G_{jr} - G_{te} - G_{je}} dG_{tr}\right) dG_{jr} dG_{te} G_{je} \tag{4.8}$$

where

$$M = \frac{e^{2R} L_{te} G_{te} (N_0 + P_j L_{jr} G_{jr})}{L_{tr}(N_0 + P_j L_{je} G_{je})} + \frac{N_0 + P_j L_{jr} G_{jr}}{P_t L_{tr}}(e^{2R} - 1)$$

is the upper limit of the integral for G_{tr}.

The result of equation (4.8) can be achieved by calculus [15]:

$$
\begin{aligned}
P_{out}[R] = e^{-\frac{N_0 e^{2R}-1}{P_j L_{je}}} P_j^{-2} L_{je}^{-1} L_{jr}^{-1} (\frac{e^{2R}-1}{P_t L_{tr}} - \frac{1}{P_j L_{jr}} \\
- e^{2R} \frac{L_{te}}{P_j L_{tr} L_{je}})^{-2} \Big[e^{2R} \frac{L_{te}}{L_{tr}} (\frac{N_0(e^{2R}-1)}{P_t L_{tr}} + \frac{N_0 L_{jr}}{P_j} \\
- e^{2R} \frac{N_0 L_{te}}{P_j L_{je} L_{tr}} + 1) \times e^{\upsilon_1} E_1(\upsilon_1) + (\frac{N_0(e^{2R}-1)}{P_t L_{tr}} \\
+ \frac{N_0 L_{jr}}{P_j} - e^{2R} \frac{N_0 L_{te}}{P_j L_{je} L_{tr}} - e^{2R} \frac{L_{te}}{L_{tr}}) \times e^{\upsilon_2} E_1(\upsilon_2) \Big] \\
- N_0 e^{-\frac{N_0(e^{2R}-1)}{P_t L_{tr}}} \Big[P_t P_j L_{tr} L_{jr} (\frac{e^{2R}-1}{P_t L_{tr}} - \frac{1}{P_j L_{jr}} \\
- e^{2R} \frac{L_{te}}{P_j L_{tr} L_{je}}) \Big]^{-1} + 1
\end{aligned}
\tag{4.9}
$$

where $\upsilon_1 = \frac{L_{tr}+e^{2R}L_{te}}{P_j L_{je} L_{tr}}$, $\upsilon_2 = \frac{e^{2R}L_{te}+L_{tr}}{e^{2R}L_{te}}(\frac{N_0(e^{2R}-1)}{P_t L_{tr}} + \frac{N_0}{P_j L_{jr}})$ and $E_1(u) = \int_u^\infty \frac{e^{-x}}{x} dx$ stands for the exponential integral.

According to Equation (4.9), the outage probability is an explicit function of L_{te} and L_{je} that are determined by d_{te} and d_{je} respectively. Once the positions of Tx,Rx and Jm are given, system secrecy regions with different secrecy outage probabilities can be determined according to (4.9). As shown in Figure 4.2, each location on the map experiences a particular outage probability that the system secrecy capacity C_s is less than the secrecy rate R if the Ev is placed at that location. By setting a target value γ_{min} for the secrecy probability $P_{out}(R)$, a geographic map with the area that $P_{out}(R)$ being lower than a target possibility γ_{min} can be drawn accordingly. It is thus called a safe region A_s related to γ_{min}. Conversely, the area with $P_{out}(R) > \gamma_{min}$ is called the compromised secrecy region (CSR) A_c. In light of the above discussion, a cooperative jamming system to enhance the security based on the principle of the CSR minimization will be discussed in the following.

3 Compromised Secrecy Region Minimization

In this section, to solve the potential numerical problem in calculating (4.9), an approximation for secrecy outage probability is provided. And the algorithm for the CSR minimization is described afterwards.

3.1 Outage Probability Approximation

Although the secrecy outage probability is provided in Equation (4.9), it is difficult to formulate the safe and compromised region in the cooperative jamming system. As an alternative, the area of the CSR can be calculated numerically by computer simulations. However, due to the finite word-length and computational capability of the computer, the numerical calculation of (4.9) may confront an overflow problem when running the computer simulation. In particular, the two components $e^{\upsilon_1}E_1(\upsilon_1)$ and $e^{\upsilon_2}E_1(\upsilon_2)$ in Equation (4.9), containing the multiplications of the exponential term e^x and exponential integral $E_1(x)$, may cause the data overflow as d_{te} and d_{je} increases in simulation.

The impact of the overflow problem to computer simulation is shown in Figure 4.3. It is observed that for the plotting outside the white boundary in the figure, secrecy outage probability $P_{out}(R)$ equals to zero and no longer changes, which cannot accurately reflect the geographical characteristics of the secrecy region in this area. This is due to the finite word-length phenomenon caused by the exponential increasing term e^x and rapidly decreasing exponential integral $E_1(x)$ in numerical calculation, thereby limiting the range of valid value x in computer simulation.

Given an overflow threshold η in the simulation, the valid regions based on Equation (4.9) are subject to the conditions that:

$$\begin{cases} \upsilon_1 < \eta \\ \upsilon_2 < \eta \end{cases} \Rightarrow \begin{cases} d_{je} < [\frac{c\eta P_j}{N_0} - e^{2R} d_{tr}^{\alpha} \varsigma]^{\frac{1}{\alpha}} \\ d_{te} < [(\eta \frac{P_j c}{N_0 d_{jr}^{\alpha}} - 1)^{\frac{1}{\alpha}} d_{tr}] \end{cases} \tag{4.10}$$

where $\varsigma = (\frac{d_{je}}{d_{te}})^{\alpha} \approx 1$ when $d_{je} \gg d_{tr}$. The secrecy region that can be numerically calculated is limited to the limited boundaries determined by the two distances d_{je} and d_{te}. $P_{out}(R)$ cannot be determined outside the intersected area when d_{tj} is too large. In summary, the overflow problem will result in the inaccurate calculation of CSR as the considered secrecy region increases to a certain scale.

Consequently, an approximation of the exponential term and exponential integral is necessary to eliminate this overflow problem.

We use the asymptotic expansion approximation of exponential integral developed in the

literature [61] for numerical calculation when the variable is large:

$$\begin{aligned}\int_u^\infty \frac{e^{-x}}{x}dx = u^{-1}e^{-u} - u^{-2}e^{-u} + 2!u^{-3}e^{-u} - 3!u^{-4}e^{-u} \\ ...(-1)^n n!u^{-(n+1)}e^{-u} - (-1)^n n\int_u^\infty \frac{e^{-x}}{x^{-(n+1)}}dx\end{aligned}. \tag{4.11}$$

For $e^u(-1)^n n\int_u^\infty \frac{e^{-x}}{x^{-(n+1)}}dx \to 0$ when $u \geq n > 1$,

$$e^u E_1(u) = e^u \int_u^\infty \frac{e^{-x}}{x}dx = \sum_{i=0}^{n}(-1)^i i!u^{-(i+1)}, \tag{4.12}$$

where n is the number of terms used in approximation. Generally, when $u > 50$, the approximation with $n < 50$ is used to substitute the original equation to expand the boundary.

3.2 Compromised Secrecy Region Minimization Algorithm

Without loss of generality, the power P_j of Jm and the distance d_{tj} between Tx and Jm are set to be: $P_j = \mu P_t,\ d_{tj} = \rho d_{tr}$, where μ and ρ are power ratio and distance ratio respectively.

As shown in Figure 4.2, the CSR with the highest outage probability is closely surrounding Tx. In practical situation, Ev may want to avoid staying too close to Tx to reduce the risk of being discovered. So the area with the highest secrecy outage probability indicating Ev close to Tx are not our interest. Therefore, a highest target probability γ_{max} is set and only the outage probability in a certain range is considered. Denoting A_c as the area corresponding to the outage probability in the range of $\gamma_{min} < P_{out}(R) < \gamma_{max}$, the CSR minimization can be formulated as:

$$\begin{aligned}&\min_{\gamma_{min}<P_{out}(R)<\gamma_{max}} \{A_c\}. \\ &s.t.\ \mu \in (0, +\infty)\ ,\ \rho \in (0, +\infty)\ \&\ \theta \in [0, 2\pi).\end{aligned} \tag{4.13}$$

The size of the CSR depends on the jamming power decided by μ and the location decided by ρ and θ of the jammer. By optimizing A_c under the condition of μ, ρ and θ, the smallest CSR and the best system secrecy can be achieved. However it is nontrivial to obtain an analytical solution for A_c due to the involved complexity of $P_{out}(R)$. Therefore, a golden section searching procedure is utilized to gradually approach the minimum value of the area A_c of the CSR. The

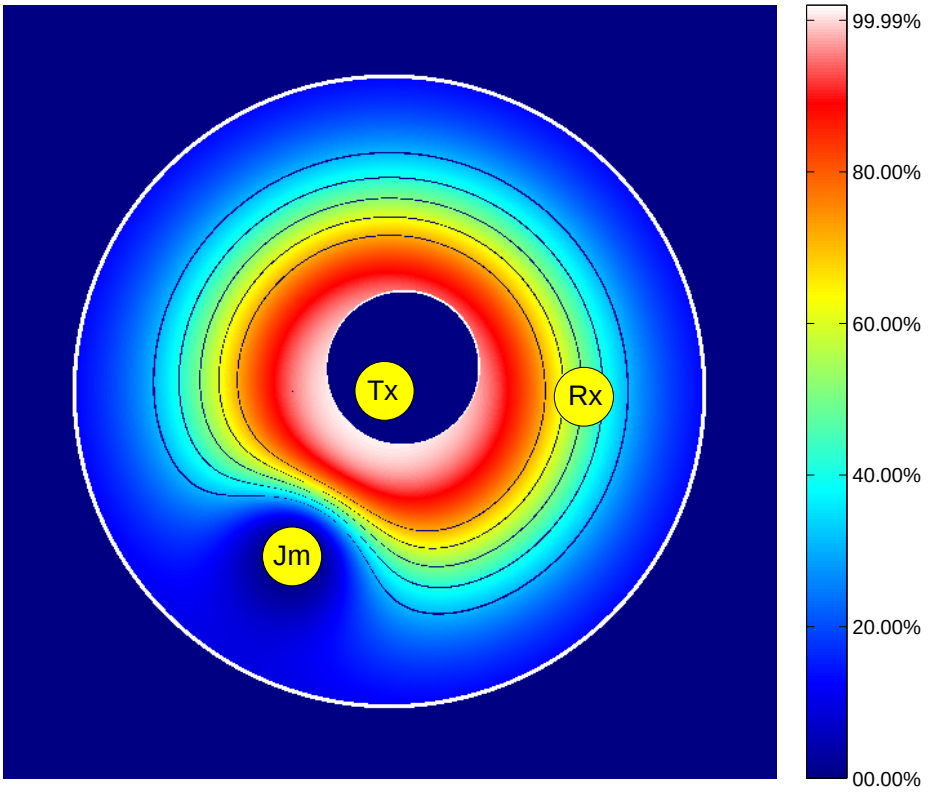


Figure 4.3: Example of the restricted boundary in the secrecy region map with a numerical overflow problem. The simulation parameters used are based on $c = 1$, $\alpha = 4$, $R = 0$ and $d_{tj} = d_{tr} = 1km$.

algorithm is summarized in details as follows:

S1 Perform the initial variable range estimation.

S2 Select initial variable values x_1, x_3, and $x_2 = \frac{x_3 + x_1\varphi}{1+\varphi}$, where φ is the constant Golden Section Ratio.

S3 If $|x_3 - x_1| < \varepsilon$, where ε is the preset accuracy bound, go to $S6$. Otherwise, if $A_c(x_2) < A_c(X_1)$ and $A_c(x_2) < A_c(X_3)$ go to $S4$.

S4 If $|x_2 - x_1| < |x_3 - x_2|$, choose x_4 when $\begin{cases} x_4 - x_2 = \varphi(x_2 - x_1) \\ x_3 - x_4 = x_2 - x_1 \end{cases}$; Otherwise, choose x_4 when $\begin{cases} x_2 - x_4 = \varphi(x_4 - x_1) \\ x_3 - x_2 = x_4 - x_1 \end{cases}$.

S5 If $A_c(x_4) > A_c(x_2)$, set $x_1 = x_1, x_3 = x_4, x_2 = x_2$; If $A_c(x_4) \leq A_c(x_2)$, set $x_1 = x_2, x_3 = x_3, x_2 = x_4$. Repeat $S3$.

S6 Terminate and return x_2 and $A_c(2)$.

Note that the termination condition ε can be adjusted according to different accuracy level of the system. It is also noteworthy that the minimum of A_c can be found under a proper initial range for parameter setting. This initial estimation range can be empirically obtained as the system parameters is practical only if d_{tj} and P_j have comparative magnitudes with d_{tr} and P_t respectively in reality.

4 Simulations

In this section, numerical results for CSR minimization are provided and several characteristics of the secrecy region will be discussed. The simulation model is constructed in the scenario that Tx, Rx, Jm as well as Ev are located in an area of $1km$ by $1km$ map size. The path-loss constant c is set to be 1 and the path-loss exponent α is assigned to be 4. The approximation terms $n = 6$. For simplicity, the target secrecy rate R is set to 0. Meanwhile, the

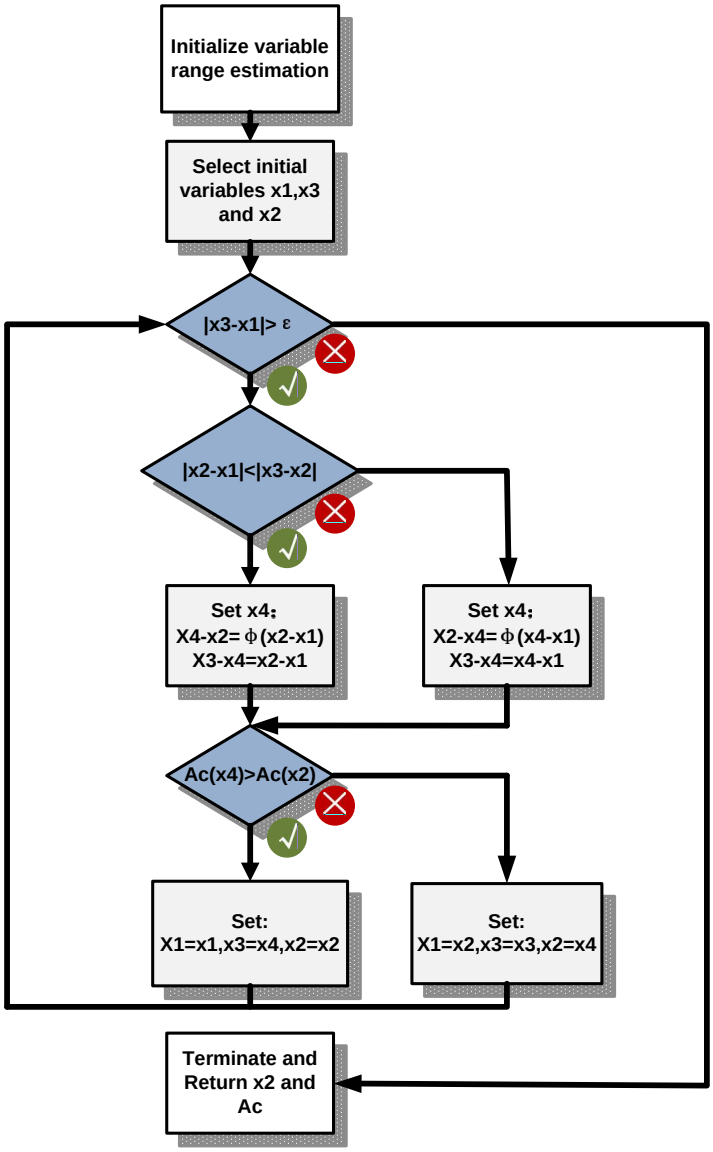


Figure 4.4: Golden section search algorithm

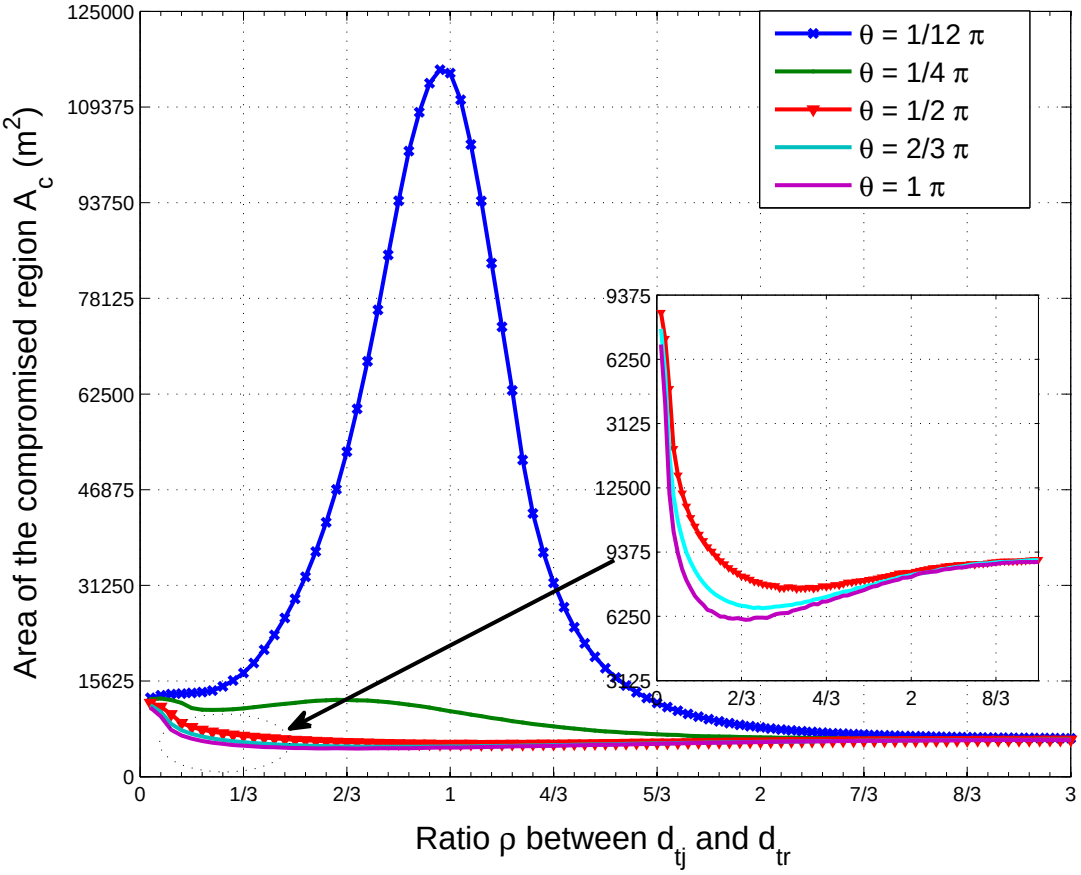


Figure 4.5: Area of CSR versus distance ratio ρ with different included angles θ. The power ratio $\rho = 1$.

highest target possibility γ_{max} is 0.8 and lowest target possibility γ_{min} is 0.5. With reference to Figure 4.1, Tx is located in the center of the map whose coordinator is considered as $(0, 0)$. Correspondingly, the location of Rx is (0, 62.5) which is 62.5 m east to Tx. The power of transmitter is 10 dB.

Figure 4.5 demonstrates the relationship between the distance d_{tj} and the area of CSR when $\rho = 1$. The area changes with the increment of the ratio ρ from 0 to 3. However, when the included angle between d_{tj} and d_{tr} is smaller than $\frac{1}{2}\pi$ such as $\theta = \frac{1}{12}\pi$ and $\theta = \frac{1}{4}\pi$, the curves of the area of CSR do not exhibit convexity. Moreover, when ρ ranges from $\frac{1}{3}$ to $\frac{3}{2}$ in which d_{tj} and d_{tr} have the comparative length, the CSR increases dramatically. This phenomenon indicates Jm can not be located in a circle sector of an included angle less than $\frac{1}{2}\pi$ between the ligature

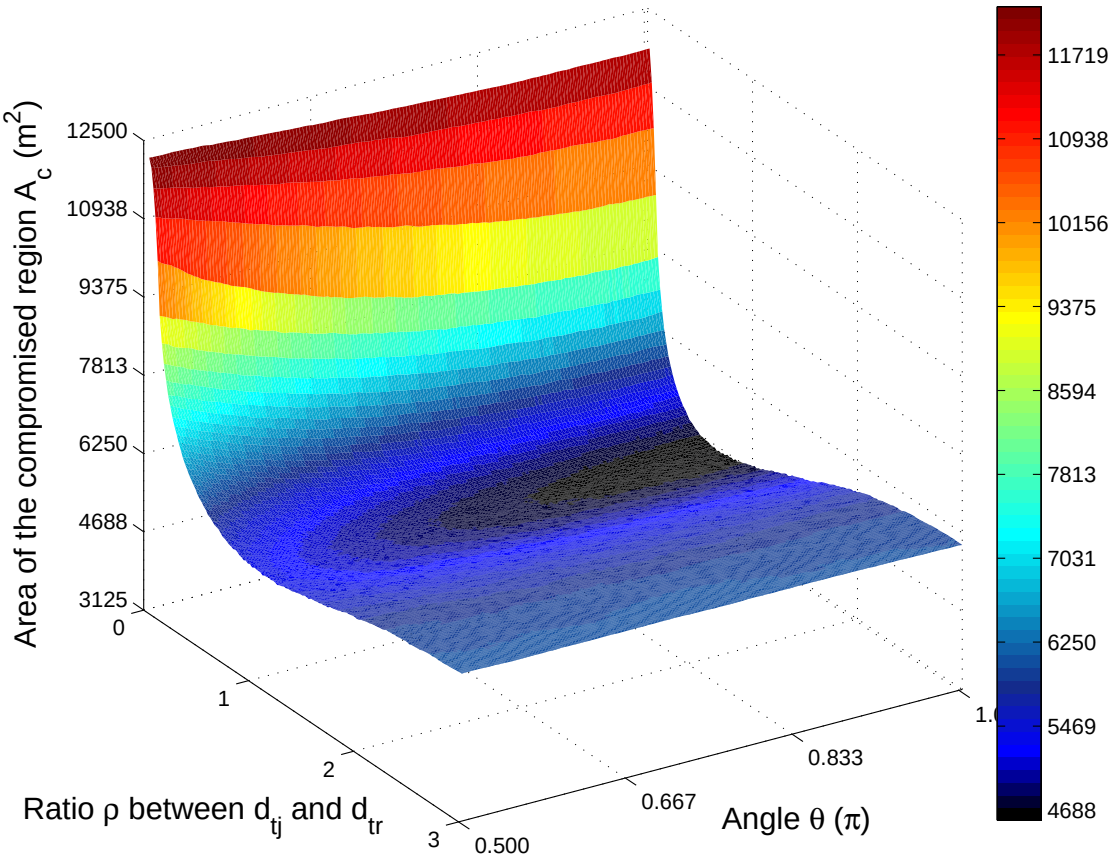


Figure 4.6: Illustration of the relationship between area of CSR A_c versus distance ratio ρ and included angles θ. The power ratio $\rho = 1$.

of $Tx \rightarrow Jm$ and the ligature of $Tx \rightarrow Rx$. The reason is that the jamming power will have a more strong negative impact on Rx when Jm is placed in the aforementioned area. On the other hand, as can be observed from the figure, when θ is larger than $\frac{1}{2}\pi$, the curve of the area displays the convexity and the minimum value of the area of CSR is obtainable. In addition, along with the increment of θ, the minimal point of each curve decreases. When $\theta = 1\pi$ which means Tx, Rx and Jm are aligned, the least minimal point can be achieved.

In order to address the problem more clearly, we plot the relationship between the area of CSR A_c versus distance ratio ρ and the included angle θ in a 3-D figure as illustrated in Figure 4.6. The value range of θ is restricted from $\frac{1}{2}\pi$ to 1π because valid range should be larger than

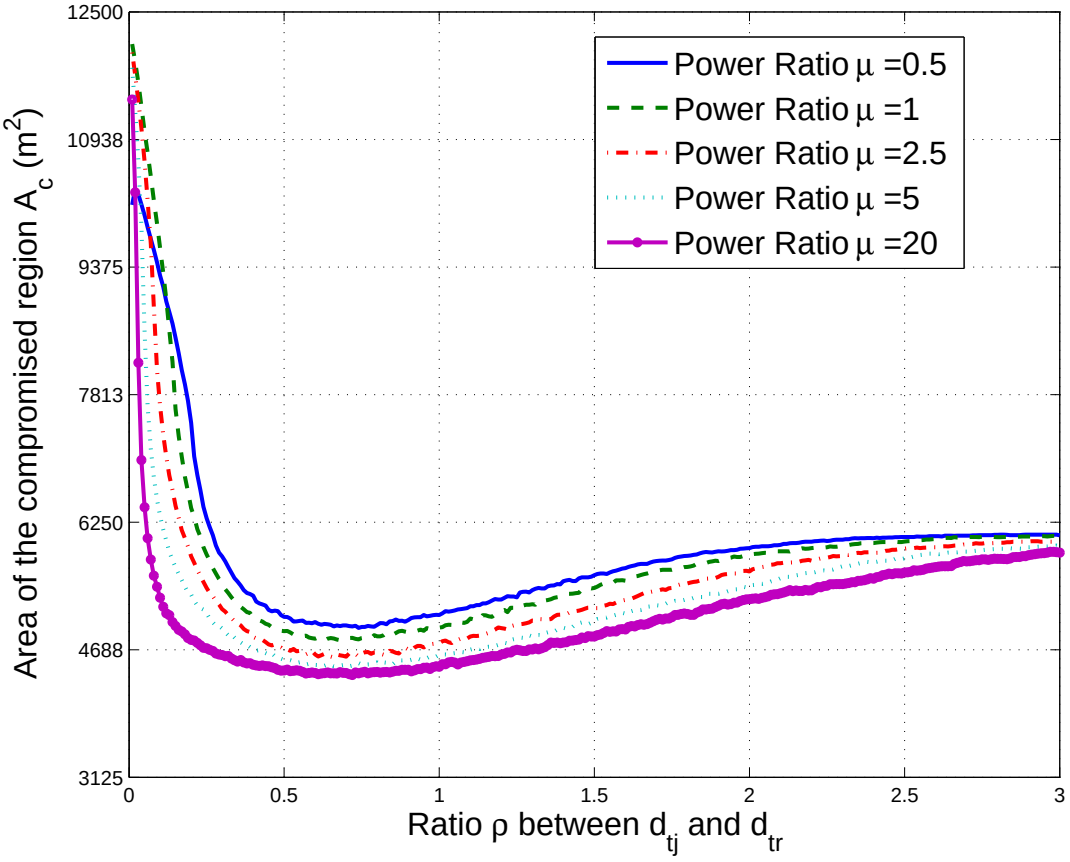


Figure 4.7: Area of CSR A_c versus the distance ratio ρ with different power ratios μ. The included angle $\theta = 1\pi$.

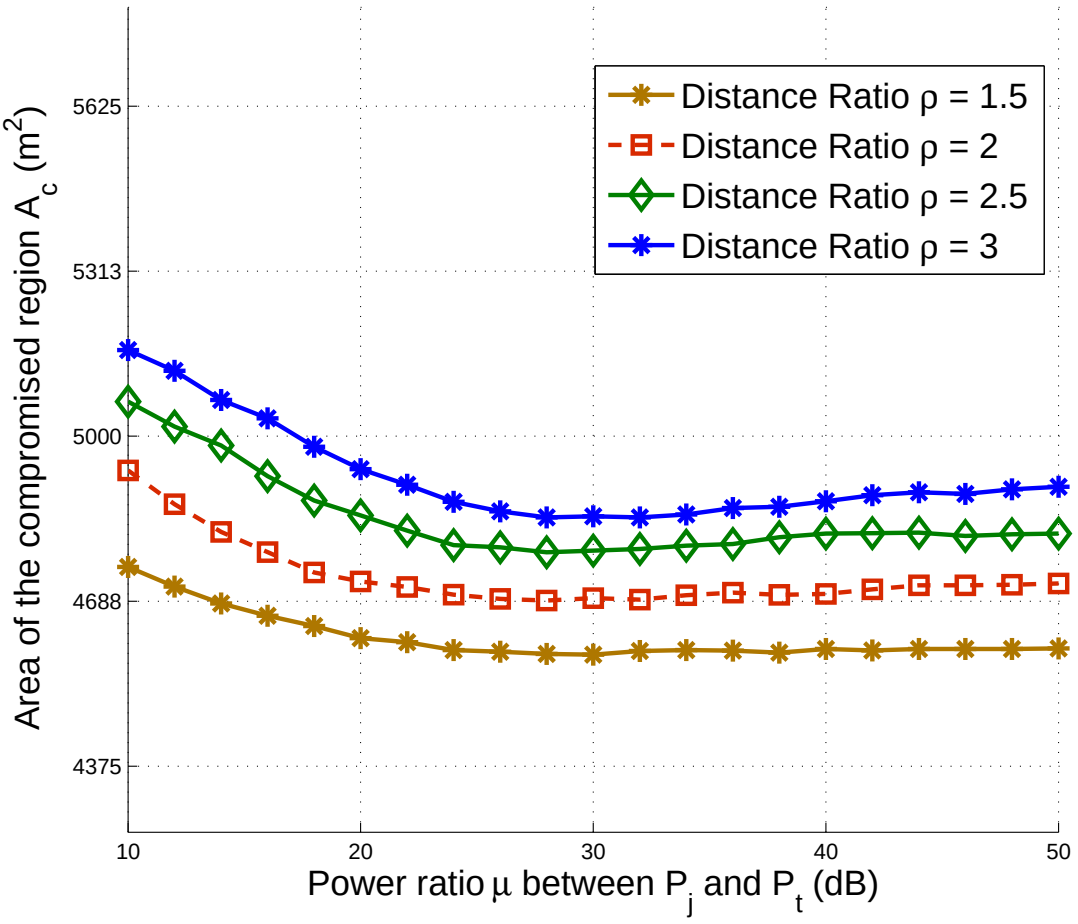


Figure 4.8: Area of CSR A_c versus the power ratio μ with different distance ratio ρ. The included angle $\Theta = 1\pi$.

$\frac{1}{2}\pi$ and the symmetry will duplicate the plot when $\theta = 1\pi$ to $\frac{3}{2}\pi$. From this figure, the dark area indicates the minimal points. It is also distinct to point out that when $\theta = 1\pi$, the minimum of the area of CSR will be obtained.

The relevance between CSR and jammer's allocated power is presented in Figure 4.7 and 4.8. Figure 4.7 illustrates the variation of the compromised area versus distance ratio ρ under different power ratio μ. By using the result from above-mentioned simulations, Jm is located to the place where $\theta = 1\pi$. Each curve of the compromised area exhibits the convexity and the minimum can be achieved by using the minimization searching algorithm. In Figure 4.8, we also reveal the relationship between P_j and A_c. When distance ratio ρ is low, the power of Jm will only have a limited impact on the area of CSR. Nonetheless, with d_{tj} increasing to $\rho = 3$, obvious convexity can be observed and the minimum of A_c is thus achievable.

5 Chapter Summary

In this chapter, we propose a compromised secrecy region (CSR) minimization strategy in cooperative jamming system to enhance security of wireless communications. Different from traditional optimization schemes, the proposed strategy is focused on evaluating the system security using the concept of secrecy region. Derived from the statistical CSI of wireless channels, the outage probability is exploited to determine the secrecy region of the system. Through a numerical approximation of the outage probability, the CSR is minimized by calculating the optimal location and allocated power of the cooperative jammer. The proposed scheme provides a new security optimization criterion dispensing with the knowledge of the location of random-distributed eavesdropper. Finally, the proposed CSR minimization strategy is validated by numerical results.

Chapter 5

Function Selection Strategy of Cooperative Node for Security Enhancement

1 Introduction

Cooperative relaying of information among wireless partners is a powerful technique in improving the reliability and coverage of wireless networks. As a popular and widely deployed system structure, communication security in cooperative relay networks is also an important issue. As the increased number of relay nodes which act as a sources or partial sources, the probability for any malicious attackers to break through the transmission also increases. As a result, information sent by the source node is inevitably leaked to the eavesdropper. For this reason, it is of great importance to establish a method to reduce or eliminate the information leakage to the eavesdropper while maintaining acceptable transmission rate to the intended receiver.

Some works have been dedicated to increase the performance such as transmission rate maximization between transmission parties [62][63]. However, the improvement is conducted without considering the existence of eavesdroppers. When taking security issue into consideration, these performance enhancements may be conflicted to the practical situation or have a

negative impact. If the eavesdropper exists, the reception of signal at the eavesdropper or any malicious attackers is improved at great probability as well when the relay nodes enhance the receptivity of legitimate receiver. Hence, the improvement of cooperative relay network needs to be considered in the presence of eavesdroppers.

As discussed in Chapter.4, cooperative jamming strategy is one of the promising options for enhancing the system security in cooperative networks. Most existing works have been made by maximizing the secrecy capacity of the system. Z. Ding [16] proposed a two-opportunistic secrecy communication scheme without knowing the eavesdropper's channel stat information. In [17], security enhancement schemes by combining relay selection and beam-forming were proposed. However, many existing schemes only considered flat fading channel models. In reality, more and more wide-band wireless communications system have been exploited such as orthogonal frequency division multiplexing (OFDM) as discussed in Chapter.3. The implementation of cooperative networks with multi-carrier system requires the consideration of channel capacities of different channels while the security enhancements are developed.

In this chapter, we propose a function selection strategy of cooperative jammer and relay to enhance security in OFDM system. The scheme considers the scenario that the OFDM systemis working in cooperative networks. Several hybrid cooperative nodes can perform as relay or jammer during the transmission. By properly selecting the function of any cooperative node, the scheme is aiming at maximizing the overall secrecy capacity over each sub-carrier channel. The proposed scheme combines the advantages of both cooperative jammer and cooperative relay networks. While increasing the transmission rate using cooperative relay nodes, it can also guarantee the network's security using cooperative jammer nodes.

The chapter is organized as follows: In section 2, the system of multi-hybrid relay and jammer nodes is formulated. In section 3, the function strategies of the hybrid nodes for security enhancement are discussed including the selection of mutual exclusive type of nodes and coexistent type of nodes. In section 4, simulation results show the performances of each kind of selection strategy and demonstrate the effectiveness of the proposed scheme. Finally, in section 5, it comes to the chapter summary.

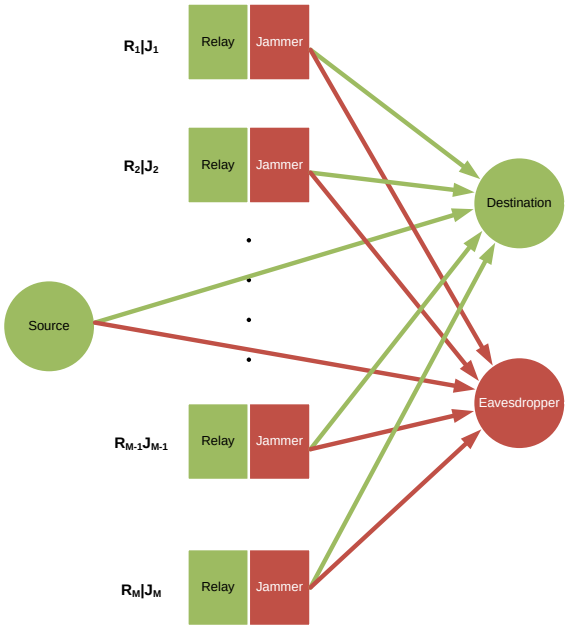


Figure 5.1: The scenario for the proposed secure OFDM transmission scheme with the assistance of multiple $R|J$ nodes.

2 System Formulation

In this section, we consider the system as shown in Figure. 5.1. The network is composed of one source node (S), one destination node (D), one eavesdropper (E) and M cooperative nodes ($R|J$). Notice that each cooperative node can either perform as a relay node (R) which relays the OFDM signal from the source node or as a jammer node (J) which emits noise to the channel to jam the eavesdropper. Assume that the source transmits the signal at power P_s and the summation of transmitting power of all $R|J$ nodes is P_{RJ}. Without losing generality, we also assume that channel condition is pre-known to source, cooperative nodes, eavesdropper and destination. According to the feature of OFDM signal, each subcarrier bandwidth is narrow enough to be considered as flat fading channel compared with the total transmitting bandwidth. If each OFDM symbol contains N subcarriers, the channel condition in the network can be depicted as:

$$\begin{aligned}\mathbf{H}_{S\to D} &= [h_1^0, h_2^0, h_3^0 ... h_N^0],\\ \mathbf{H}_{S\to E} &= [h_{e1}^0, h_{e2}^0, h_{e3}^0 ... h_{eN}^0],\\ \mathbf{H}_{R_m|J_m\to D} &= [h_1^m, h_2^m, h_3^m ... h_N^m],\\ \mathbf{H}_{R_m|J_m\to E} &= [h_{e1}^m, h_{e2}^m, h_{e3}^m ... h_{eN}^m],\end{aligned} \tag{5.1}$$

where $\mathbf{H}_{S\to D}$, $\mathbf{H}_{S\to E}$, $\mathbf{H}_{R_m|J_m\to D}$ and $\mathbf{H}_{R_m|J_m\to E}$ respectively stand for the channel state information (CSI) of source to destination, source to eavesdropper, the *mth* $R|J$ node to destination and eavesdropper; $h_n^m = |h_n^m|e^{j\theta_n^m}$ $h_{en}^m = |h_n^m|e^{j\theta_{en}^m}$stands for the complex channel response of nth subcarrier.

Taking each subcarrier into consideration, we may depict the channel response on *nth* subcarrier as a vector:

$$\begin{aligned}\mathbf{H}_n &= [h_n^0, h_n^1, h_n^2 ... h_n^M],\\ \mathbf{H}_{en} &= [h_{en}^0, h_{en}^1, h_{en}^2 ... h_{en}^M],\end{aligned} \tag{5.2}$$

where $\mathbf{H}_n$ and $\mathbf{H}_{en}$ depict the channel response vector of nth subcarrier from transmitters to destination and transmitters to eavesdropper respectively. Then the received signals of the *nth* subcarrier at destination and eavesdropper at time $i = 1, 2, 3...K$ are:

$$\begin{aligned}y_D = \quad & a_0 h_n^0 S_n(i) + a_1 h_n^1 S_n(i) + ...a_M h_n^M S(i)\\ & + b_0 h_n^0 X_n(i) + b_1 h_n^1 X_n(i) + ...b_M h_n^M X_n(i)\\ & + n_{nd}(i)\\ = \quad & \mathbf{A}\mathbf{H}_n^T S_n(i) + \mathbf{B}\mathbf{H}_n^T X_n(i) + n_{nd}(i)\end{aligned}, \tag{5.3}$$

$$\begin{aligned}y_E = \quad & a_0 h_{en}^0 S_n(i) + a_1 h_{en}^1 S_n(i) + ...a_M h_{en}^M S(i)\\ & + b_0 h_{en}^0 X_n(i) + b_1 h_{en}^1 X_n(i) + ...b_M h_{en}^M X_n(i)\\ & + n_{ne}(i)\\ = \quad & \mathbf{A}\mathbf{H}_{en}^T S_n(i) + \mathbf{B}\mathbf{H}_{en}^T X_n(i) + n_{ne}(i)\end{aligned}, \tag{5.4}$$

where $S_n(i)$ is the transmitted signal of subcarrier n at time i; $X_n(i)$ is the jamming signal which is independent and identically distributed (i.i.d.) Gaussian noise with zero mean and variance

δ_n^2 on subcarrier n; $\mathbf{n}_{nd}(i)$ and $\mathbf{n}_{nd}(i)$ are also i.i.d. Gaussian noise with zero mean and variance δ_{nd}^2 and δ_{ne}^2 correspondingly; $\mathbf{A} = [a_0, a_1...a_M]$ and $\mathbf{B} = [b_0, b_1...b_M]$ are used to depict whether a $R|J$ cooperative node is used as a relay or a jammer. For example, if $R_m|J_m$ is used as a relay, $a_m = 1$, $b_m = 0$ otherwise if it is a jammer, $a_m = 0$, $b_m = 1$.

For the reason that X_n is i.i.d. Gaussian noise, the equivalent noise received at both legitimate receiver and eavesdropper contains the noise from jammers and AWGN channel. Thus, Equation. 5.3 and 5.4 can be equivalently written as:

$$\widetilde{y}_D = S_n(i) + \widetilde{n}_d(i), \tag{5.5}$$

$$\widetilde{y}_E = S_n(i) + \widetilde{n}_e(i), \tag{5.6}$$

where

$$\widetilde{n}_{nd}(i) = \frac{\mathbf{B}\mathbf{H}_n^T X_n(i) + n_{nd}(i)}{\mathbf{A}\mathbf{H}_n^T}$$

and

$$\widetilde{n}_{ne}(i) = \frac{\mathbf{B}\mathbf{H}_{en}^T X_n(i) + n_{ne}(i)}{\mathbf{A}\mathbf{H}_{en}^T}.$$

$\widetilde{n}_{nd}(i)$ and $\widetilde{n}_{ne}(i)$ follow Gaussian distribution because X_n follows $N(0, \delta_x^2)$ and n_{nd} and n_{ne} follow $N(0, \delta_0^2)$. The variance of them can be obtained as follows:

$$var[\widetilde{n}_{nd}] = \frac{\mathbf{B}|\mathbf{H}_n^T|^2\delta_x^2 + \delta_0^2}{|\mathbf{A}\mathbf{H}_n^T|^2} \tag{5.7}$$

$$var[\widetilde{n}_{ne}] = \frac{\mathbf{B}|\mathbf{H}_{en}^T|^2\delta_x^2 + \delta_0^2}{|\mathbf{A}\mathbf{H}_{en}^T|^2} \tag{5.8}$$

The signal to noise ratio at legitimate receiver and eavesdropper thus can be depicted as:

$$\begin{aligned}\gamma_{nd} =& \frac{P_s/N}{var[\widetilde{n}_{nd}]} \\ =& \frac{P_s/N|\mathbf{A}\mathbf{H}_n^T|^2}{\mathbf{B}|\mathbf{H}_n^T|^2\delta_x^2 + \delta_0^2}\end{aligned} \tag{5.9}$$

$$\begin{aligned}\gamma_{ne} =& \frac{P_s/N}{var[\widetilde{n}_{ne}]} \\ =& \frac{P_s/N|\mathbf{A}\mathbf{H}_{en}^T|^2}{\mathbf{B}|\mathbf{H}_{en}^T|^2\delta_x^2 + \delta_0^2}\end{aligned} \tag{5.10}$$

By far, the channel capacity over the $n-th$ subcarrier can be written as:

$$C_{nd} = \frac{1}{2}\log_2(1+\gamma_{nd}), \tag{5.11}$$

$$C_{ne} = \frac{1}{2}\log_2(1+\gamma_{ne}), \tag{5.12}$$

In the above equation, $\frac{1}{2}$ indicates that for the two-slot orthogonal protocol, there is only one slot dedicated to the transmission from the relays to nodes D and E. Based on the above equations, the secrecy capacity of the system over the $n-th$ subcarrier can be obtained:

$$\begin{aligned}C_{ns} =& C_{nd} - C_{ne} \\ =& \frac{1}{2}\log_2(\frac{1+\gamma_{nd}}{1+\gamma_{ne}})\end{aligned} \tag{5.13}$$

Since the OFDM have N subcarriers, the over all secrecy capacity of the system is the summation of secrecy capacity C_{ns} over each subcarrier. Therefore, the system's secrecy capacity can be written as:

$$\begin{aligned}C_s =& \sum_{n=1}^{N} C_{ns} \\ =& \frac{1}{2}\log_2\left(\frac{\prod_{n=1}^{N}(1+\gamma_{nd})}{\prod_{n=1}^{N}(1+\gamma_{ne})}\right)\end{aligned} \tag{5.14}$$

As can be observed, the secrecy capacity of the entire system is related to the following factors: CSI of each subcarrier channel from transmitter and different $R|J$ nodes to both legitimate receiver and eavesdropper; Power allocation strategy of transmitter and $R|J$ nodes; Function selection of each $R|J$ node to perform as a jammer or relay. Here for simplicity, CSI of each path is regarded as constant during a specific time slot. Also, the power allocation strategy over each $R|J$ node and transmitter is fixed.Suppose all nodes transmit uniformly over each

subcarrier, the source and the $R|J$ nodes have the average power on the *nth* subcarrier:

$$\frac{1}{K}\sum_{0}^{K} E[|S(i)|^2] \leqq \frac{P_s}{N}$$

$$\frac{1}{K}\sum_{0}^{K} E[a_n|X(i)|^2 + b_n|S(i)|^2] \leqq \frac{P_{RJ}}{MN} = \delta_x^2.$$

3 Function Selection Strategies of $R|J$ Node for Security Enhancement

3.1 Mutual Exclusive $R|J$ Node Selection

From the Equation 5.14, if the proper relay and jammer are selected, the overall secrecy capacity can be positive which means the overall channel condition to the destination is better than that to the eavesdropper. However, if the inappropriate functions of $R|J$ nodes are selected, the secrecy capacity may become negative. The system is unsecured since the wire-tap channel has a higher capacity than the legitimate channel. In this condition, the secrecy capacity is considered as zero. The achievable system secrecy thus can be written as:

$$\begin{aligned} C_s &= \left[\sum_{n=1}^{N} C_{ns}\right]^+ \\ &= \begin{cases} \frac{1}{2}\log_2\left(\frac{\prod_{n=1}^{N}(1+\gamma_{nd})}{\prod_{n=1}^{N}(1+\gamma_{ne})}\right) & , \sum_{n=1}^{N} C_{ns} > 0 \\ 0 & , \sum_{n=1}^{N} C_{ns} < 0 \end{cases} \end{aligned} \tag{5.15}$$

We consider the selection strategy under the situation that the $R|J$ node can only perform as a jammer or a relay during a specific time duration. Although for a specific subcarrier of $R|J$ node, its $\mathbf{H}_n$ and $\mathbf{H}_{en}$ may be suitable for being used as a jammer or as a relay, our criterion on selecting the function of $R|J$ nodes is only related to the adaptability of this node over all subcarrier channels. In other words, when we choose a node to make it perform as a jammer or relay, we only concern if it is suitable for all subcarrier channels.

Recall the selection vector **A** and **B** in previous section:

$$\mathbf{A} = [a_0, a_1, ...a_M], \tag{5.16}$$

$$\mathbf{B} = [b_0, b_1, ...b_M], \tag{5.17}$$

The mutual exclusive function of the $m - th$ $R|J$ node is expressed as:

$$a_m \oplus b_m = 1,$$

where a_m and b_m are binary number. Here we assume no $R|J$ node is suspended which means each node has to work either as jammer or relay. For example, if there are 5 $R|J$ nodes in all and node 1,3,5 are chosen as relay $\mathbf{A} = [1, 1, 0, 1, 0, 1]$, then node 2,4 have to emit interference to both receiver and eavesdropper $\mathbf{B} = [0, 0, 1, 0, 1, 0]$. a_0 and b_0 stand for the transmitter. We consider the transmitter constant perform as a source, thus $a_0 = 1$ and $b_0 = 0$ under any circumstances.

The selection process examines all $R|J$ nodes at the same time with each possible choice. If there are M $R|J$ nodes exist, the number of examination is 2^M. For each possible combination, there is a secrecy capacity C_{sk}. Therefore the entire examination process generates a secrecy capacity vector which can be depicted as:

$$\mathbf{C}_s = [C_{s1}, C_{s2}..., C_{s2^M}] \tag{5.18}$$

In order to improve the system security, we have to select the proper functions of all $R|J$ nodes and try to maximize the overall secrecy capacity C_S which is:

$$\begin{aligned} &Max\ \{\mathbf{C}_s\} \\ &\quad subject\ to\ \mathbf{A}, \mathbf{B}. \end{aligned} \tag{5.19}$$

The mutual exclusive $R|J$ nodes selection is a simple strategy as each one of them only have 2 status $(a_m, b_m) = (1, 0)$ or $(0, 1)$. Because of the limited combination of all $R|J$ nodes, the time complexity of searching for the best combination is short. While implemented in real

scenario, this strategy can quickly response to the varying channel conditions.

3.2 Coexistent $R|J$ Node Selection

A more complex strategy compared with mutual exclusive one is the coexistent $R|J$ node selection strategy. If each $R|J$ node can perform as jammer and relay simultaneously, it can enhance the transmission rate between legitimate channel and decrease the receptiveness of eavesdropper in the same time.

For simplicity, we consider that each $R|J$ node can distribute half of its power to act as a jammer or as a relay. In this scenario, for $R_m|J_m$ node, three possibilities of the status exist which are:

$$(a_m, b_m) = [(1, 0), (\frac{1}{2}, \frac{1}{2}), (0, 1)] \tag{5.20}$$

As for each $R|J$ node, since there are three possible selection strategies, we call the node as $(0, 1/2, 1)$ $R|J$ node. The total number of combinations for all $R|J$ nodes is 3^M. The corresponding secrecy capacity vector can be generated as:

$$\mathbf{C}_s = [C_{s1}, C_{s2}..., C_{s3^M}] \tag{5.21}$$

In order to achieve best secrecy, the combination that generates the highest secrecy capacity for the network is chosen:

$$\begin{aligned} &Max\ \{\mathbf{C}_s\} \\ &\quad subject\ to\ \mathbf{A}, \mathbf{B}. \end{aligned} \tag{5.22}$$

Compared with mutual exclusive selection $O(2^n)$, the time complexity of coexistent selection while searching for the best combination is higher $O(3^n)$. When the number of $R|J$ nodes is limited, i.e. $M < 6$. The time complexity of coexistent selection is still acceptable. However, when the number is large, i.e. $M > 5$, each process of searching for the best combination requires more than 500 times comparison which may add huge load to the network.

Similarly, if the possible selections of the $R|J$ nodes increases to $(0, 1/4, 1/2, 3/4, 1)$ $R|J$ node, under the same condition, it will provide more accurate best secrecy than $(0, 1/2, 1)$ $R|J$ node and mutual exclusive node. However, the better performance is achieved at the cost of

even higher time complex which is $O(5^n)$.

The most general form of coexistent $R|J$ node selection is that each node can distribute arbitrary proportion of its power as a jammer or relay. Considering $R_m|J_m$ node without losing generality,:

$$(a_m, b_m) = (\sin^2\theta_m, \cos^2\theta_m), \tag{5.23}$$

and the selection vector $\mathbf{A}$ and $\mathbf{B}$ can be expressed as:

$$\mathbf{A} = [1, \sin^2\theta_1, ... \sin^2\theta_M] \tag{5.24}$$

$$\mathbf{B} = [0, \cos^2\theta_1, ... \cos^2\theta_M] \tag{5.25}$$

The ideal result of finding the best combination of all nodes thus can be expressed as:

$$\begin{aligned} &Max\ \{\mathbf{C}_s\} \\ &\quad subject\ to\ [\theta_1, \theta_2, ...\theta_M], \theta_m \in [0, \pi). \end{aligned} \tag{5.26}$$

Since variable vector θ has M dimensions, the optimal result is not easy to achieve. Hence, we consider a suboptimal solution to this problem. In such scenario, each $R|J$ node is separately examined. The selection vectors for $R_m|J_m$ node are A_m,B_m:

$$\mathbf{A} = [\frac{1}{M}, 0, ... \sin^2\theta_m ...0] \tag{5.27}$$

$$\mathbf{B} = [0, 0, ... \cos^2\theta_m ...0] \tag{5.28}$$

Thus we transform the problem into 1-dimension. The best secrecy C_{sm} for $m-th$ $R|J$ node thereby can be find by:

$$\begin{aligned} C_{sm} &= Max\ \{C_s\} \\ &\quad subject\ to\ \mathbf{A}_m, \mathbf{B}_m, \theta_m \in [0, \pi). \end{aligned} \tag{5.29}$$

Therefore,

$$\mathbf{C}_s = [C_{s1}, C_{s2} .... C_{sM}], \tag{5.30}$$

is the best secrecy capacity that can be achieved by each $R|J$ node separately.

4 Simulations

In this chapter, the simulation environment is constructed to test the different $R|J$ node selection strategies under various conditions. The environment is listed as follows: OFDM with 64 subcarriers is chosen as the transmitted signal; The channel is considered as Rayleigh fading channel with zero mean and unit variance; Maximum time delay is set to be $T = 8$ so as the cyclic prefix of OFDM $G = 8$; The allocated power of transmitter and all $R|J$ nodes are with unit value $P_s = 1$ and $P_{rj} = 1$.

In Figure. 5.2, the best secrecy capacity achieved by different number of $(0, 1/2, 1)$ nodes versus SNR is shown. In this scenario, we only considered the coexistent $(0, 1/2, 1)$ $R|J$ nodes strategy. With the increasing SNR, as can be observed, secrecy capacity also increases. The structure with $M = 4$ $R|J$ nodes has the best performance at all time meanwhile the structure with $M = 2$ has the worst. The curve of $M = 5$ has the second best performance. The simulation result shows that although the more nodes exist in the network the more combinations there will be, it is not guaranteed that more nodes can achieve the higher best-secrecy-capacity than the structure with fewer nodes.

Figure.5.3 and Figure.5.4, are comparisons of the best secrecy capacity achieved by different selection strategy in a network of $M = 2$ and $M = 5$ $R|J$ nodes respectively. In the structure of 2 nodes shown in Figure. 5.3, from $SNR = 0dB$ to $SNR = 9dB$, best secrecy can be achieved by $(0, 1/4, 1/2, 3/4, 1)$ nodes coexistent nodes structure. From 9 dB to 17 dB, the best secrecy is achieved by $(0, 1/2, 1)$ coexistent nodes structure. At the highest SNR from 17dB to 26dB, the selection of $(0, 1/4, 1/2, 3/4, 1)$ once again achieves the best secrecy. In the structure with 5 nodes shown in Figure.5.4, the selection of $(0, 1/4, 1/2, 3/4, 1)$ coexistent nodes constantly achieve the best secrecy while the suboptimal solution to the general form of coexistent nodes achieves the worst best-secrecy-capacity.

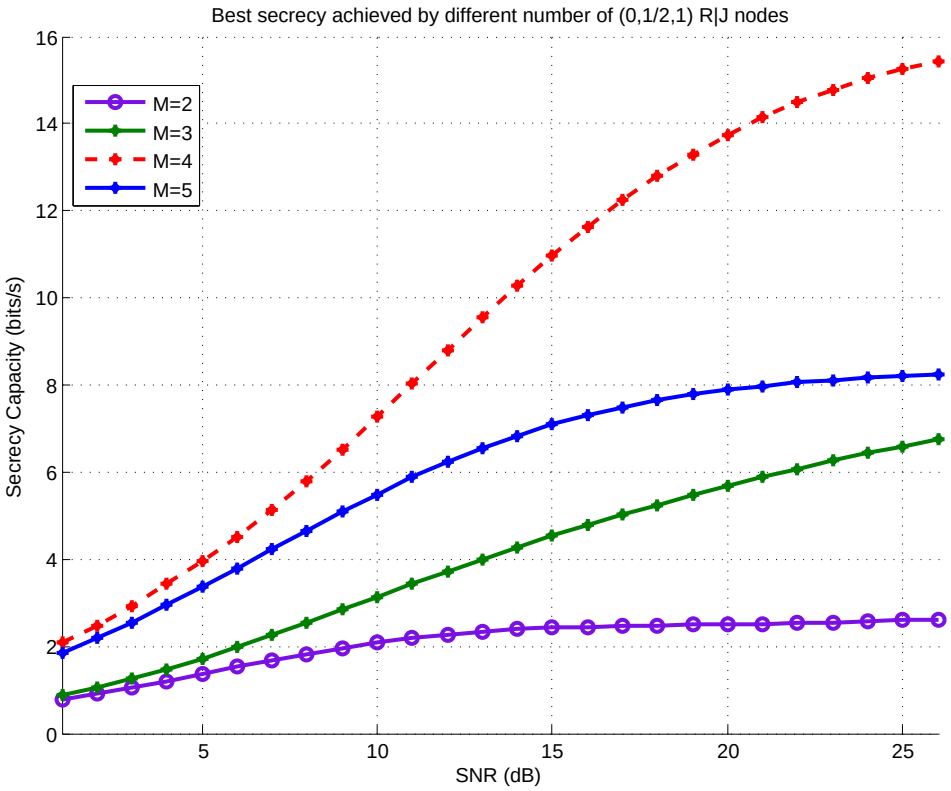


Figure 5.2: Best secrecy achieved by different number of (0,1/2,1) $R|J$ nodes.

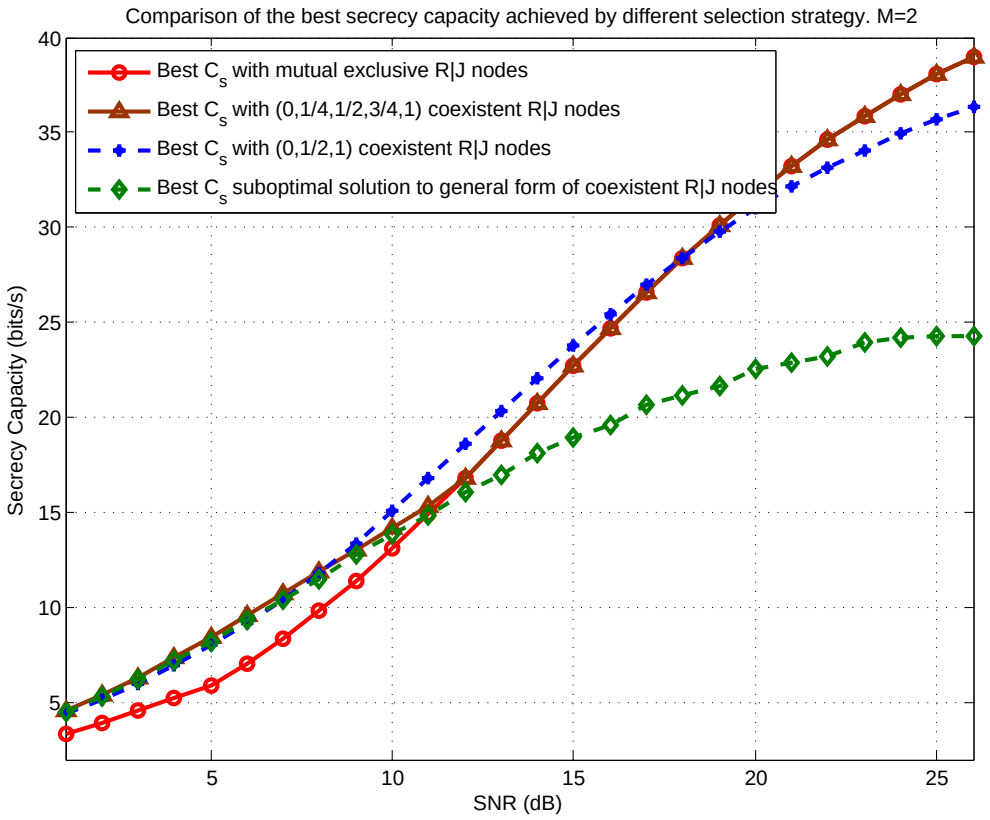


Figure 5.3: Comparison of the best secrecy capacity achieved by different selection strategy with two $R|J$ nodes.

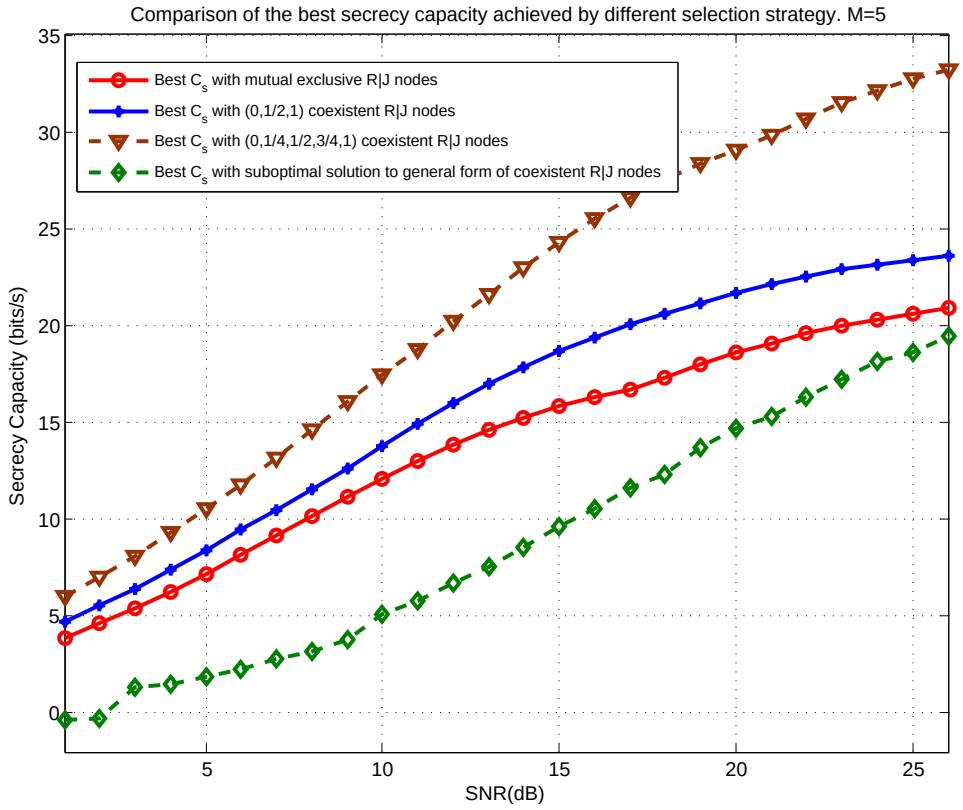


Figure 5.4: Comparison of the best secrecy capacity achieved by different selection strategy with five $R|J$ nodes.

5 Chapter Summary

A secure OFDM transmission scheme to enhance system security is proposed in this chapter by selecting the proper function of each relay and jammer node within the network. The cooperative OFDM network with several nodes of hybrid function which can act as jammer or relay is investigated. Two category selection strategies, mutual exclusive nodes selection and coexistent nodes selection, are studied receptively. With proper function selection strategy under different transmission environment, the best secrecy capacity can be achieved. The best achievable secrecy reduces the leaked information to the eavesdropper and therefore secure the transmission of OFDM system. Numerical results also demonstrate the effectiveness of proposed function selection strategies for enhancing the security of OFDM system in cooperative networks.

Chapter 6

Conclusions

In this thesis, security enhancements of wireless network are studied. The thesis starts with a comprehensive survey of background information regarding with current wireless network security issues and popular wireless systems such as orthogonal frequency division multiplexing (OFDM) and cooperative jamming system. Aiming at enhancing the wireless security and improving the insufficiencies of existing works, several security enhancement mechanisms of wireless communications on physical layer(PHY) are investigated to solve different problems.

In order to overcome potential security risks of OFDM system due to its distinct signal features, a time-domain scrambling OFDM to enhance PHY security is proposed in the first part of the thesis. The scrambling process conducted in time domain transforms the constellation diagram of the system. The thesis analyzes the effect of time domain scrambling process. The scheme increases the complexity of constellation of a conventional OFDM signal so that lower the probability of a malicious attack.

For the purpose of evaluating the security level and optimizing the system under the condition that instantaneous channel state information is not achievable, an optimization strategy using compromised secrecy region (CSR) minimization in cooperative jamming system is proposed. By statistically analyzing the secrecy region using secrecy outage probability, CSR minimization guarantees the system secrecy dispensing with the knowledge of instantaneous channel state information from illegitimate channel.

To direct at improving the secrecy of cooperative networks over frequency selective fading channel, selection strategies of cooperative node function are proposed in Chapter 5. The

system model of cooperative OFDM is formulated considering secrecy capacity over each subcarrier channel. Two function selection strategies are developed in order to maximize the system's overall secrecy capacity.

The main contributions of this thesis are summarized as follows:

- We propose a time domain scrambling OFDM system to enhance its PHY security. The inherent effect of the time domain scrambling OFDM signal is unveiled by analyzing the constellation transformation effect of the proposed scrambling OFDM system. The analysis and numerical results show the proposed scheme not only changes the phase angle but also changes the amplitudes of the signal's constellation which increase the difficulty of cracking the system.

- We improve the security in cooperative jamming system by using compromised secrecy region minimization without using instantaneous CSI from illegitimate channel. Solution to the boundary problem happening in large scale system is provided by using approximation to the secrecy outage probability. Searching algorithm to look for minimum CSR is also provided.

- We investigate selection strategies of cooperative node function to enhance the security level of OFDM system in cooperative networks. Secrecy capacity under multi-channel condition is considered and several selection strategies of different types of cooperative nodes ,including mutual exclusive nodes and coexistent nodes, are provided.

Future Works

There are several interesting areas which are worthwhile for future investigations:

- In the time-domain scrambling OFDM topic, we assume both legitimate transmitter and receiver have a pre-known secret key to the scrambling process. However, in reality, a secret key distribution is required before the communication links are established. Therefore, it is also important to develop a valid key distribution mechanism for legitimate transceivers.

- In the compromised secrecy region minimization topic, it is very useful to consider the cooperative jamming system with more than one jammer. As can be predicted, the more jammers the system has, the more accurate the compromised secrecy region will be. Although the conditions regarding with the derivation of secrecy map will increase with the increasing number of jammers, the multi-jammer scenario is a model closer to the reality application.

- In cooperative nodes function selection topic, we construct the system with cooperative nodes which have equally distributed transmitting power. A more practical situation in which $R|J$ nodes have different power weights is worthy of being investigated for future work. The proper power allocation scheme is capable of achieving a wider range of secrecy capacity in the same channel condition compared to equally distributed power scheme. It can be predicted that the dynamic change of the power weight for each node will make the system more adaptive to the rapid variation of channel conditions.

Bibliography

[1] B. Birch, *"Giants of Science - Guglielmo Marconi"*. Blackbirch Press, 1 edition, 2001.

[2] Y. 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 Communications*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[3] J. Choi, S. Y. Chang, and Y. C. H. D. Ko, "Secure mac-layer protocol for captive portals in wireless hotspots," *2011 IEEE International Conference on Communications (ICC)*, pp. 1–5, 5–9, Jun. 2011.

[4] R. Schaller, "Moore's law: past, present and future," *Spectrum, IEEE*, vol. 34, no. 6, pp. 52,59, 1997.

[5] A. Wyner, "The wiretap channel," *Bell Syst Tech*, vol. 54, pp. 1355–1387, Oct. 1975.

[6] S. Mathur, A. R. Reznik, and C. Ye, "Exploiting the physical layer for enhanced security," *IEEE Wireless Communications*, vol. 17, pp. 63–70, Oct. 2010.

[7] R. Hartley, "Transmission of information," *Bell System Technical Journal*.

[8] P. Liu, Z. Tao, Z. Lin, E. Erkip, and S. Panwar, "Cooperative wireless communications: a cross-layer approach," *IEEE Wireless Communications*, vol. 13, no. 4, pp. 84–92, Aug. 2006.

[9] M. A. Khan, V. J. M. Asim, and R. S. Manzoor, "Chaos based constellation scrambling in ofdm systems: Security & interleaving issues," *Information Technology*, vol. 4, pp. 1–7, Aug. 2008.

[10] M. Tahir, S. P. W. Jarot, and M. U. Siddiqi, "Wireless physical layer security using encryption and channel pre-compensation," *Computer Applications and Industrial Electronics (ICCAIE)*, pp. 304–309, Dec. 2010.

[11] R. Ma, L. Dai, Z. Wang, and J. Wang, "Secure communication in tds-ofdm system using constellation rotation and noise insertion," *IEEE Trans, Consumer Electronics*, vol. 56, no. 3, pp. 1328–1332, Aug. 2010.

[12] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[13] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani, "Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper," *011 IEEE International Conference on Communications (ICC)*, pp. 1–5,5–9, Jun. 2011.

[14] V. Aggarwal, L. Sankar, A. Calderbank, and H. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *2009 Information Theory and Applications Workshop*, pp. 295–300,8–13, Feb. 2009.

[15] J. Vilela, J. B. M. Bloch, and S. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 1.6, no. 2, pp. 256–266, Jun. 2011.

[16] Z. Ding, K. K. Leung, D. L. Goechel, and D. Towsley, "Opportunistic relaying for secrecy communications: cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, 2011.

[17] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *Journal of Commun and Networks*, vol. 14, no. 4, pp. 364–373, 2012.

[18] G. Danezis, "Introducing trafiňĄc analysis," *Digital Privacy: Theory, Technologies and Practices*, 2007.

[19] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *international journal of computer science and information security*, vol. 4, 2009.

[20] Wikipedia(https://en.wikipedia.org/wiki/Denial_of_service_attack), "Denial of service attack,"

[21] J. Volbrecht and R. Moskowitz, "Wireless lan access control and authentication," *a white paper from Interlink Networks Resource Library*, 2001.

[22] B. Q. Hai and Z. Ying, "Study on the access control model in information security," *Quad-regional Radio Science and Wireless Technology Conference*, pp. 830–834, 2011.

[23] Wikipedia(http://en.wikipedia.org/wiki/Public-key_cryptography), "Public-key cryptography,"

[24] J. Sen, "A survey on wireless sensor network security," *IEEE, Wireless Communications*, vol. 1, no. 2, Aug. 2009.

[25] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems.," *Communication of the ACM*, pp. 120–126, 1978.

[26] Wikipedia(https://en.wikipedia.org/wiki/Euler%27s_totient_function), "Euler's totient function,"

[27] D. Boneh and R. Venkastesan, "Breaking rsa may not be equivalent to factoring," *Advances in Cryptology-ASIACRYPT2001, Lecture Notes in Computer Science*, pp. 514–532, 2001.

[28] M. Babioff, N. Immorlica, D. Kempe, and R. Kleinberg, "A knapsck secretary problem with applications," *Proceedings of the 10th International Workshop on Approximation and the 11th International Workshop on Randomization, and Combinatorial Optimization.*, pp. 16–28, 2007.

[29] A. Shamir, "A polynomial time algorithm for breaking the basic merkele-hellman cryptosystem," *Proceedings of the 23rd Annual Symposium on Foundations of Computer Scinece*, pp. 145–152, 1982.

[30] Wikipedia(https://en.wikipedia.org/wiki/Elliptic_curve_cryptography), "Elliptic curve cryptography,"

[31] N. Koblitz and A. J. Menezes, "A survey of public-key cryptosystems," *SIAM Review*, vol. 46, no. 4, pp. 599–634, 2004.

[32] E. Conrad and S. Misenar, "Data encryption standard(des)," *CISSP Study Guide*, pp. 229–231, Sep., 2012.

[33] N. I. of Standards and Technology, "Data encryption standards (des)," *Processing standards publication*, 1999.

[34] N. I. of Standards and Technology(NIST), "Announcing the advanced encryption standard (aes)," *Federal Information Processing Standards Publication 197*, 2001.

[35] O. Ureten and N. Serinken, "Wireless security through rf fingerprinting," *Electrical and Computer Engineering, Canadian Journal of*, vol. 32, no. 1, pp. 27–33, 2007.

[36] C. Sperandio and P. Flikkema, "Wireless physical layer secuirty via transmit precoding over dispersive channels: optimum linear eavesdropping," *Proc. MILCOM*, pp. 1113–17, 2002.

[37] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent propoerties of channel impulse response," *In Proc. MILCOM 2011*, 2011.

[38] D. Abbasi-Moghadam, V. T. Vakili, and A. Falahati, "Combination of turbo coding and cryptography in non-geo satellite communication systems," *Int'l Symp. Telecommun*, pp. 27–28, 2008.

[39] Wikipedia(http://en.wikipedia.org/wiki/Turbo_code), "Turbo coding,"

[40] W. Janke, "Pseudo random numbers: Generation and quality checks," *Quantum Simulations of Complex Many-Body Systems: From Theory to Algorithms, Lecture Notes*, vol. 10, pp. 447–458, 2002.

[41] R. L. Pickholtz, D. L. Schilling, and L. Milstein, "Theory of spread spectrum communications- a tutorial," *IEEE Transactions on Communications*, vol. COM-30, no. 5, pp. 855–884, 1982.

[42] G. Noubir, "On connectivity in ad hoc network under jamming using directional antennas and mobility," *2nd Int'l Conference. Wired and Wireless Internet Commun.*, pp. 54–62, 2004.

[43] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," *Military Communications Conference*, vol. 3,17-20, pp. 1501,1506, 2005.

[44] R. W. Chang, "Synthesis of band-limited orthogonal signals for multichannel data transmission," *Bell Systems Tech. Jounal*, vol. 45, pp. 1775–1796, 1966.

[45] H. Wang and J. Lilleberg, "Conventional and scrambling ofdm system switch in multicell environments," *IEEE, Wireless Communications and Networking Conference*, vol. 1, no. 2, pp. 1–5, Apr. 2006.

[46] G. Stolfi and L. BaccalaÌĄ, "Fourier transform time interleaving in ofdm modulation," *Spread Spectrum Techniques and Applications, 2006 IEEE Ninth International Symposium on*, pp. 158,162,28–31, 2006.

[47] D. Huang, K. Letaief, and J. Lu, "Bit-interleaved time-frequency coded modulation for ofdm systems over time-varying channels," *Communications, IEEE Transactions on*, vol. 5, no. 7, pp. 1191,1199, 2005.

[48] C.Rose, S. Ulukus, and R. D. Yates, "Wireless systems and interference avoidance," *IEEE Transactions on Wireless Communications*, vol. 1, no. 3, pp. 415–428, 2002.

[49] R. D. Yates, "A framework for uplink power control in cellular radio systems," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 7, pp. 1341–1347, 1995.

[50] X. Wang, P. Ho, and Y. Wu, "Robust channel estimation and isi cancellation for ofdm systems with suppressed features," *IEEE Journal, Selected Areas in Communications*, vol. 23, no. 5, pp. 963–972, May 2005.

[51] X. Wang, F. J. Liu, D. Fan, H. Tang, and P. Mason, "Continuous physical layer authentication using a novel adaptive ofdm system," *IEEE ICC, 2011*, pp. 1–5, 5–9, Jun. 2005.

[52] S. Weinstein and P. Ebert, "Data transmission by frequency-division multiplexing using the discrete fourier transform," *IEEE Trans, Communication Technology*, vol. 19, no. 5, pp. 628–634, Oct. 1971.

[53] V. G. S. Prasad and K. V. S. Hari, "Interleaved orthogonal frequency division multiplexing system," *Acoustics, Speech, and Signal Processing (ICASSP)*, vol. 3, pp. III–2745–III–2748, May 2002.

[54] E. Alsusa and L. Yang, "A new papr reduction tecnique using time domain symbol scrambling for ofdm systems," *Acoustics, Speech, and Signal Processing (ICASSP)*, pp. 1–4, Feb. 2007.

[55] X. Wu, B. Zhou, J. Wang, and Z. Mao, "Low complexity time domain interleaved partitioning partial transmit sequence scheme for peak to averagepower ratio reduction of orthogonal frequency division multiplexing systems," *Springer Wireless Pers. Commun.*, vol. 60, no. 2, pp. 227–294, Mar. 2010.

[56] A. Wyner, "The wiretap channel," *Bell Syst Tech*, vol. 54, pp. 1355–1387, Oct. 1975.

[57] B. Dunn, "An introduction to secrecy capacity," *IPronounced CHEE-sar*, Dec. 2006.

[58] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," *Information Theory*, pp. 356–360, Jul. 2006.

[59] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," *2006 IEEE International Symposium on Information Theory*, pp. 356–360,9–14, Jul. 2006.

[60] S. Tomasin, M. Levorato, and M. Zorzi, "Analysis of outage probability for cooperative networks with harq," *IEEE International Symposium on 2007 Information Theory*, pp. 2716–2720, 24–29, Jun. 2007.

[61] P. H. Tseng and T. C. Lee, "Numberical evaluation of exponential integral: Theis well function approximation," *Journal of Hydrology*, vol. 205, ISS 1-2, pp. 38–51, Feb. 1998.

[62] A. Sendonaris and E. Erkip, "User cooperation diversity- part i: system description," *IEEE Trans. Commun*, vol. 8, no. 11, pp. 1927–1938, 2003.

[63] Y. Jing and H. Jakarhami, "Singel and mutiple relay selection schemes and their achievable diversity orders," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1414–1423, 2009.

Curriculum Vitae

Name:	Hao Li
Place of Birth	Zhengzhou, China
Year of Birth	1988
Post-Secondary Education and Degrees:	2007-2011 B.Eng Shanghai Jiaotong University, Shanghai, China Electrical and Electronic Engineering
Related Work Experience:	Teaching Assistant The University of Western Ontario 2011-2013

Publications:

1. H. Li, X. Wang and W. Hou, "Secure Transmission in OFDM Systems by Using Time Domain Scrambling", *IEEE VTC 2013 Spring*, 2013.

2. H. Li, X. Wang and W. Hou, "Security Enhancement in Cooperative Jamming Using Compromised Secrecy Region Minimization", *IEEE Canadian Workshop on Information Theory 2013 (CWIT 2013)*, PP.225-229, 2013