This is to certify that the
dissertation entitled

SPACE-TIME CODING AND ITS APPLICATIONS IN EFFICIENT AND JAMMING-RESISTANT WIRELESS COMMUNICATIONS

presented by

Leonard E. Lightfoot

has been accepted towards fulfillment
of the requirements for the

Ph.D. degree in Electrical Engineering

Tongtong Li

Major Professor's Signature

4/21/2010

Date

SPACE-TIME CODING AND ITS APPLICATIONS IN EFFICIENT AND JAMMING-RESISTANT WIRELESS COMMUNICATIONS

By

Leonard E. Lightfoot

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Electrical Engineering

2010

ABSTRACT

SPACE-TIME CODING AND ITS APPLICATIONS IN EFFICIENT AND JAMMING-RESISTANT WIRELESS COMMUNICATIONS

By

Leonard E. Lightfoot

Along with the wide spread of various wireless devices, especially with the advent of user configurable intelligent devices, such as cognitive radios, the security threats of malicious jamming, detection, and interception is no longer limited to military communications. With the majority of today's transactions and communications relying heavily on wireless networks, security has become the key enabler for present and future high speed wireless networks. Patching or add-on security maybe effective in short term, but is far from adequate for addressing the needs on wireless security and can greatly complicate the communication systems. In this dissertation, we focus on the fundamental study of developing a spectrally efficient and secure wireless system by exploiting multiple diversity techniques.

First, we propose a more efficient space-time coding scheme based on the Alamouti scheme. Through bit-level inspection, our investigation reveals that the Alamouti scheme is a low efficient code and there is an opportunity for spectral efficiency enhancement. Unlike most of the existing methods which are designed to maximize the diversity or rate for space-time block codes, the proposed spectrally efficient Alamouti scheme aims to improve the code efficiency of the Alamouti codes, while achieving excellent transmit diversity and retaining the decoding simplicity. The code efficiency of the proposed scheme is enhanced by transmitting more information bits than redundancy bits per Alamouti block. Although the main focus of the proposed scheme is to improve the code efficiency for two transmit antennas, the same ideas

can be extended in a straightforward way to the Alamouti codes with more than two transmit antennas.

Second, we propose an innovative spectrally efficient, jamming-resistant wireless scheme by exploiting the joint space-time and frequency diversity. Recently, the collision-free frequency hopping (CFFH) system, which is based on the orthogonal frequency division multiple access (OFDMA) framework and the secure subcarrier assignment scheme, was proposed as a spectrally efficient anti-jamming system. In this research, we investigate the security features of the CFFH system and propose to enhance the inherent security of CFFH through joint space-time and frequency diversity. More specifically, (i) we analyze the limitations of the CFFH system and propose a new subcarrier assignment scheme based on secure permutation. The new algorithm is designed to ensure that malicious users cannot predict or repeat the hopping pattern of the authorized users and hence cannot launch follower jamming attacks; (ii) We improve the performance of the CFFH system under random jamming, by enhancing the system diversity through space-time coding, and introduce the space-time coded collision-free frequency hopping (STC-CFFH) system. The proposed STC-CFFH is found to be particularly powerful in eliminating both channel interference and hostile jamming interference. Our analysis indicates that the proposed scheme is both highly efficient and very robust under various jamming scenarios.

Third, we investigate the use of quasi-orthogonal space-time block codes (QO-STBCs) to mitigate jamming noise. The combination of constellation rotation QO-STBC and OFDM can exploit multipath diversity resulting in excellent performance under frequency-selective fading. Moreover, such systems must be robust against jamming interference, especially partial-band noise jamming. Hence, proper analytical tools are needed to assess the performance of QO-STBC-OFDM in the presence of jamming. In this research, (i) we derive analytical expressions for the exact pairwise error probability (PEP) of the QO-STBC-OFDM system using the moment generating function (MGF); (ii) We calculate the exact PEP under various situations, and derive the closed-form expressions and union bound for the bit error probability (BEP). Our simulation results show that the union bound is tight.

Dedicated to my family

ACKNOWLEDGMENTS

I would like to take this opportunity to express my gratitude to my advisor, Dr. Tongtong Li, for her continuous support, guidance and encouragement throughout the years. Even before she was my official advisor, she believed in me. Whenever I hit a road block with research, she gently but firmly pushed me. For these reasons and many more, I thank you, Dr. Li!!!

I want to also thank Dr. Percy Pierre, Dr. Subir Biswas and Dr. Jonathan Hall for serving on my PhD committee. I am deeply indebted to them for their guidance and support. Dr. Jian Ren , thank you for the technical advice on network security. Dr. Barbara O'Kelly, thank you for your valuable advice and for making my transition to graduate school a smooth one. Dr. Uche Wejinya, thank you for being a great mentor and friend.

To all my friends of the Sloan-Rigas program, and the NSBE organization, I thank you for making my life at Michigan State University an enjoyable experience. I would also like to thank all my friends around the country, Jamin, DeAndre, Chris, Dominic, Michelle, Kenny, and Ashley for all the fun times and encouraging conversations. I would like to send a special thank you to my lab mates Lei Zhang, Xiaochen Tang and Dr. Huahui Wang for our valuable discussions on research.

I would like to thank my parents, my brother, my sisters, my nephew, my nieces and my extended family for their love and constant support. Finally, I would like to send a very special thank you to my wife, Tinesha, for her unconditional love, patience and continuous support throughout the PhD process. Tinesha, you are my inspiration and I will forever be grateful to have you in my life. Love You!!!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

"Images in this dissertation are presented in color"

CHAPTER 1

Introduction

1.1 Growth of Wireless Communication Networks

Wireless communication is one of the most active areas in research today. While it has been a topic of study since the 1960s, the past few decades has seen a surge of research activities in the area. This is due to the fact that wireless technology offers organizations and users many benefits such as portability, flexibility, increased productivity and lower installation cost. Today, the wireless technology covers a broad range of services such as voice, video, and data services. As a result, there has been an explosive increase in demand for tetherless connectivity, which is driven by the cellar telephony and wireless data applications. In 2011, it is projected that the worldwide cellular telephony subscriber base will be 4.3 billion, roughly 62% of the projected world population [1–3]. Furthermore, the Internet is also growing tremendously, with 1.1 billion worldwide users as of March 2007 [4]. Based on the current growth trends, it is projected that global revenues from mobile data-centric applications will exceed $166 billion by 2010, in comparision to global revenues of $100 billion in 2005 [5].

The growth and technological advancements of wireless communication applications has accelerated the demand for increased data rates, wider coverage, improved link reliability and security of the wireless network. However, fulfilling these demands are challenging because the radio spectrum is limited and the wireless infrastructure has an inherent security problem. Moreover, the wireless channel is time varying due to the small-scale effect of multipath fading, as well as larger-scale effects such as path loss via distance attenuation and shadowing by obstacles. Lastly, unlike the wired counterpart where each transmitter-receiver pair is free from outside interfer-

ence, wireless users communicate over the air and there is unpredictable interference. The lack of protective physical boundary increases the potential of adversary interception and eavesdropping. Any adversary with the appropriate radio frequency (RF) equipment within the radio range can intercept the transmitted information. As highlighted, wireless networks are inherently unreliable and vulnerable to serious security threats.

1.2 Vulnerabilities and Security Threats of Wireless Networks

Along with the wide spread of various wireless devices, especially with the advent of user configurable intelligent devices, such as cognitive radios, the security threats of malicious jamming, detection, and interception are no longer limited to military communications. With today's business and social cultures relying heavily on wireless technologies to execute all day-to-day transactions and communications, security has become the key enabler for present and future high speed wireless networks.

Incorporating security into the wireless infrastructure has its challenges. First, the underlying wireless medium is broadcast by nature and more vulnerable to security attacks due to the lack of physical boundary. Second, the wireless channel is inherently unreliable, time varying and hard to predict. Lastly, the physical layer of the wireless network model is generally not equipped with built-in security. In the following subsections, we discuss two major security threats in wireless networks, eavesdropping and malicious jamming.

1.2.1 Eavesdropping

Eavesdropping consists of an adversary capturing transmitted information from the airlink. Eavesdropping is considered an easy attack because the wireless channel is broadcast by nature. Furthermore, radio signals are not directional, therefore, anyone with the proper radio receiver can capture the transmitted information.

The lack of built-in security at the physical layer simplifies the adversaries' job of discovering the transmitted message even if the message in encrypted. An accurately received encrypted message means that the only barrier between the adversary and the original message is the need for correct decryption. Due to the weakness of some existing encryption algorithms, it is not too difficult for an adversary to decode the original message. For example, several research groups [6–8] found the 40-bit/128-bit wired equivalent privacy (WEP) [9] thoroughly flawed because of the relatively weak encryption algorithm it uses.

1.2.2 Malicious Jamming

In wireless networks, one of the most commonly used techniques for limiting the effectiveness of an opponent's communication is referred to as jamming. Generally, intentional jamming, also known as malicious jamming, intends to disable the legitimate transmission by saturating the receiver with noise or false information through deliberate radiation of radio signals, and thus significantly decreasing the signal-to-interference-plus-noise ratio (SINR). In other words, malicious jamming can be viewed as a denial of service (DoS) attack.

Conventionally, jamming signals are classified into four types: (i) Tone-jamming [10–12], where the jamming power is concentrated around carrier frequencies; (ii) Partial-time jamming [13–15], where the jamming occurs at certain time periods during the signal transmission. Partial-time jamming can be considered as a two-state Markov process. When the jammer is in state 0, it is off; when the jammer is in state 1, the jammer emits the interfering signal. State 1 occurs with probability of ρ, for which the variance of jamming signals is $\frac{N_J}{\rho}$, where N_J is the power spectral density of the jamming signal. State 0 occurs with probability of $(1-\rho)$, for which the variance of jamming signals is 0. (iii) Full-band jamming [16,17], where the power of the jammer is uniformly distributed over the bandwidth; (iv) Partial-band jamming [18–20], where the jamming power is characterized by the additive Gaussian noise interference power $\frac{N_J}{\rho}$ over a fraction ρ of the total bandwidth and negligible

interference over the remaining fraction $(1-\rho)$ of the band.

With the increased use and dependence of wireless communications in today's society, malicious jamming attacks are no longer only a concern for military applications. In order for wireless networks to become a reliable information exchange platform, security must be strengthened.

1.3 Existing Spread-Spectrum Techniques

1.3.1 Spread-Spectrum Systems

The physical layer of the open system interconnection (OSI) model is not equipped with built-in security and suffers from adversary attacks such as eavesdropping and malicious jamming. A response to the eavesdropping and jamming threats was the implementation of the spread-spectrum technology. Spread-spectrum systems encompass modulation techniques in which the signal of interest is spread to occupy a much larger transmission bandwidth. Spread-spectrum techniques were originally developed for miliary applications, but have gained interest in commercial applications due to the promise of greater tolerance to interference. The advantages of spread-spectrum techniques are [21, 22]:

- Force adversary to monitor an expanded frequency band.
- Resistance to unintended or malicious jamming.
- Provides location privacy.
- Low probability of detection or interception.
- Increased tolerance to multipath.
- Sharing of a single channel among multiple users.

Two basic multiple access spread-spectrum techniques used in broadband cellular networks and wireless local area network (WLAN) communications are *direct-sequence*

code division multiple access (DS-CDMA) and *frequency hopping* (FH). DS-CDMA technique may be regarded as a special case of FH, thus we focus our attention on FH systems.

1.3.2 The Frequency Hopping Technique and Its Limitations

In traditional FH systems, the transmitter hops in a pseudo-random manner among available frequencies according to a pre-specified algorithm, the receiver then operates in strict synchronization with the transmitter and remains tuned to the same center frequency. The pseudo-random hopping of frequencies during radio transmission minimizes the possibility of hostile jamming and unauthorized interception.

For FH systems, the inherent security relies on the difficulty to follow the desired user's transmission frequency without the knowledge of the hopping pattern. Although frequency hopping is designed to minimize the probability of the unauthorized interception of telecommunications, the conventional FH scheme has two major limitations: (i) Strong requirement on frequency acquisition, and (ii) low spectral efficiency over large bandwidth. Typically, FH systems require large bandwidth, which is proportional to the product of the hopping rate and the total number of all the available channels. In conventional frequency hopping multiple access (FHMA), each user hops independently based on its own pseudo-random number (PN) sequence, and a collision occurs whenever there are two users over the same frequency band. Mainly limited by the collision effect, the spectral efficiency of the conventional FH system is very low. In the literature, considerable efforts have been devoted to increasing the spectral efficiency of FH systems by applying high-dimensional modulation schemes [23–29]. However, existing work is far from adequate to address the ever-increasing demand on inherently secure high data rate wireless communication, thus new techniques that are more efficient and reliable have to be developed.

1.4 Proposed Research Directions

This dissertation is focused on the fundamental study of developing spectrally efficient and inherently secure wireless interface by introducing antenna diversity, and integrating advanced signal processing techniques and cryptographic techniques into the physical layer transceiver design. More specifically, the proposed research directions are briefly summarized in the following subsections.

1.4.1 Spectrally Efficient Space-Time Coding

The integration of the Internet and multimedia applications in the next generation of wireless communications has increased the demand for wide-band high data rate services. Due to the limited radio spectrum, the high data rates can only be achieved by more efficient signaling techniques. Research in information theory has shown that large gains in capacity of wireless channels are feasible in multiple-input multiple-output (MIMO) systems [30–32]. The MIMO system consists of multiple antennas at both ends of the communication link and increases the channel capacity linearly as the number of transmit and receive antennas grows simultaneously. An effective and practical way to approaching the capacity of MIMO wireless channels is to employ space-time coding. Space-time codes can achieve rich transmit diversity and power gain over spatially uncoded systems without sacrificing the bandwidth. There are various approaches in coding structures, including *space-time block codes* and *space-time trellis codes*. Due to the decoding simplicity of space-time block codes, it is preferred over space-time trellis codes. The Alamouti space-time block code is the only full-rate full diversity complex orthogonal code, but the code efficiency can be further improved.

In this dissertation, we aim to: (i) Investigate the efficiency of the Alamouti scheme from a bit-level perspective by introducing the concepts of *Alamouti patterns* and *irregular partitioning*; (ii) Improve the spectrally efficiency of the Alamouti scheme. More specifically, we enhance the code efficiency of the Alamouti code by increasing the number of information bits transmitted in each Alamouti block.

1.4.2 Secure Space-Time Coded Collision-Free Frequency Hopping System

Originally developed for military communications, frequency hopping (FH) was designed to prevent hostile jamming, interception and detection [33]. However, the conventional FH scheme has two major limitations: (i) Strong requirement on frequency acquisition, and (ii) low spectral efficiency over large bandwidth. In an effort to provide anti-jamming communications in OFDMA systems, the combination of the FH technique and the OFDMA scheme, called FH-OFDMA, has been proposed [34, 35]. However, as the system is based on the conventional FH techniques, the spectral efficiency is seriously limited by the collision effect. Along with the ever increasing demand on inherently secure high data-rate wireless communications, new techniques that are more efficient and reliable have to be developed.

Recently, the collision-free frequency hopping (CFFH) system, which is based on the orthogonal frequency division multiple access (OFDMA) framework and the secure subcarrier assignment scheme was proposed as a spectrally efficient anti-jamming system. In this dissertation, we investigate the security features of the CFFH system, and propose to enhance the inherent security of CFFH through joint space-time and frequency diversity.

First, we analyze the security limitations of the previously proposed subcarrier assignment and propose a new subcarrier assignment scheme based on secure permutation. The new algorithm is designed to ensure that: (i) Each user hops to a new set of subcarriers in a pseudo-random manner at the beginning of each hopping period; (ii) Different users always transmit on non-overlapping sets of subcarriers; (iii) Malicious users cannot predict or repeat the hopping pattern of the authorized users, and hence cannot launch follower jamming attacks. Moreover, using the fast Fourier transform (FFT) based OFDMA framework, CFFH has the same high spectral efficiency as that of OFDM, and at the same time can relax the complex frequency synchronization problem suffered by conventional FH systems.

Second, we observe that although CFFH is very robust under partial-band jam-

ming, where the jamming interference spans over a fraction of the total bandwidth, it is still sensitive to random jamming. In this dissertation, we propose to overcome this drawback through space-time coding and introduce the space-time coded collision-free frequency hopping (STC-CFFH) system. The proposed STC-CFFH is found to be particularly powerful in eliminating both channel interference and hostile jamming interference. Our analysis indicates that the proposed scheme is both highly efficient and very robust under various jamming environments.

1.4.3 Jamming Mitigation Using Quasi-Orthogonal Space-Time Block Codes

Full-rate orthogonal space-time block codes with complex elements in its transmission matrix only exist for two transmit antennas. In an effort to provide full-rate transmission for space-time block codes with more than two transmit antennas, quasi-orthogonal space-time block codes (QO-STBCs) were proposed. With the quasi-orthogonal structure, the orthogonality of the code is relaxed to provide a higher symbol transmission rate. Furthermore, by introducing signal constellation rotation into the QO-STBC design, we can improve the bit error rate performance.

The combination of QO-STBCs with orthogonal frequency division multiplexing (QO-STBC-OFDM) can exploit multipath diversity and achieve spectrally efficient communications. However, future wireless communication systems must be robust against both unintentional and intentional interference. As a result, there is a need for proper analytical tools to assess the performance of QO-STBC-OFDM in the presence of partial-band noise jamming. First, we derive analytical expressions for the exact pairwise error probability (PEP) of the QO-STBC-OFDM system in the presence of partial-band noise jamming using the moment generating function (MGF). Second, we calculate the PEP under various situations, and derive the closed-form expressions and union bound for the bit error probability (BEP). Our numerical analysis and simulation results show that the union bound is tight.

1.5 Overview of the Dissertation

In the dissertation, we aim to address the following specific problems:

- How to improve the code efficiency of the conventional Alamouti scheme, while achieving high transmit diversity and retaining the decoding simplicity?
- How to enhance the spectral efficiency of the conventional frequency hopping systems, while maintaining the anti-jamming security feature?
- How to analytically assess the performance of multiple input, multiple output systems in the presence of partial-band noise jamming?

The dissertation is structured as follows.

Chapter II provides an overview of space-time codes. First, the encoding and decoding algorithms, and the performance of the classic Alamouti scheme with two transmit antennas is reviewed. Second, the generalized space-time block codes for systems with more than two transmit antennas is discussed. The generalized space-time block codes includes real and complex signal constellation designs. Finally, we review the code structure and performance of quasi-orthogonal space-time block codes with four transmit antennas.

Chapter III presents a spectrally efficient Alamouti scheme for high data rate communications over multiple-antenna channels. Unlike most of the existing methods which are designed to achieve full-rate and/or full-diversity, the proposed scheme aims at increasing the spectral efficiency. The proposed scheme increases the code efficiency of the traditional Alamouti scheme by increasing the number of information bits transmitted in each Alamouti block. Furthermore, the proposed scheme achieves high transmit diversity and retains the decoding simplicity of the maximum likelihood decoder. Finally, simulation examples are provided to demonstrate the effectiveness of the proposed scheme.

Chapter IV exploits an encryption based protection mechanism to strengthen the efficiency and anti-jamming features of the dynamic spectrum access control.

First, we develop a collision-free frequency hopping (CFFH) system based on the orthogonal frequency division multiplexing (OFDM) framework. Second, we investigate the limitations in the subcarrier assignment algorithm and propose a new subcarrier assignment algorithm based on the secure permutation scheme. The new secure subcarrier assignment algorithm is designed to ensure that: (i) Each user hops to a new set of subcarriers in a pseudo-random manner at the beginning of each hopping period; (ii) Different users always transmit on non-overlapping sets of subcarriers, such that malicious users cannot predict or repeat the hopping pattern of the authorized users, and hence cannot launch follower jamming attacks. Third, we enhance the anti-jamming property of the CFFH system by incorporating space-time coding (STC). The enhanced system is referred to as STC-CFFH. Our analysis indicates that STC-CFFH is particularly powerful in eliminating channel distortion and hostile jamming interference, including both random jamming and follower jamming attacks. Simulation examples are provided to illustrate the performance of the proposed schemes.

Chapter V investigates the use of quasi-orthogonal space-time block codes (QO-STBCs) to mitigate jamming noise. Unlike orthogonal space-time block codes, QO-STBCs are capable of providing full diversity and full-rate transmission for codes designed for more than two transmit antennas. With QO-STBCs, the orthogonality of the code is relaxed and by introducing signal constellation rotation into the QO-STBC design, we can improve the bit error rate performance. First, we derive analytical expressions for the exact pairwise error probability (PEP) of the QO-STBC orthogonal frequency division multiplexing (QO-STBC-OFDM) system using the moment generating function (MGF). Second, we calculate the exact PEP, and derive the closed-form expressions and union bound for the bit error probability (BEP). Finally, simulations are performed and compared with the theoretical results.

Chapter VI summarizes the contributions of the dissertation. By using space-time coding, we are able to exploit space diversity in conjunction with time and frequency diversity, resulting in efficient and jamming-resistant wireless communications for OFDM systems. For future research, we consider secure communications and dynamic resource allocation for cognitive radio networks.

CHAPTER 2

An Overview of Space-Time Coding

In this chapter, we provide an overview of space-time codes. We first review the encoding and decoding algorithms, and the performance of the Alamouti scheme with two transmit antennas. Second, we discuss generalized space-time block codes for systems with more than two transmit antennas. The generalized space-time block codes includes real and complex signal constellation designs. Finally, we review the code structure and performance of quasi-orthogonal space-time block codes with four transmit antennas.

2.1 Introduction

Over the past few decades, the demand for cellular and wireless local area networks has grown exponentially. Wireless multimedia services such as video conferencing, mobile computing and high-speed Internet access requires an increase in information throughput that is orders of magnitude below the current achievable data rates. Furthermore, the stringent limitations imposed on the available radio spectrum constraints the evolution of high data rate systems. The only way to meet increasing demand of capacity in wireless networks is to design efficient signaling techniques. A technological technique that has shown large gains in capacity is a system with multiple antennas at the transmitter and receiver. A system with multiple transmit and receive antennas is called a multiple-input multiple-output (MIMO) system. Advances in turbo coding [36], low density parity check codes [37,38], and the compu-

tational power of today's integrated circuits, enables the feasibility of implementing MIMO systems and the associated signal processing algorithms.

Space-time coding is a signal technique design aimed at approaching the information theoretic capacity limit of MIMO systems. Similar to ordinary channel codes, space-time codes employs redundancy to protect against channel fading, noise and interference. The transmitted signals of space-time codes are jointly correlated in space and time domains. Space-time codes are classified into two types: *space-time block codes* and *space-time trellis codes.* Space-time trellis codes [39, 40] designed for 2-4 transmit antennas, performs exceptionally well in slow fading environments (indoor data transmissions). However, the decoding of space-time trellis codes requires a multidimensional version of the Viterbi algorithm [41], which involves non-linear processing. Accordingly, for a fixed number of transmit antennas, the decoding complexity of space-time trellis codes increases exponentially with the transmission rate. On the other hand, space-time block codes resolves the decoding complexity problem of space-time trellis codes, but does not perform as well. Despite, the performance penalty, space-time block codes are preferred because of its decoding simplicity and satisfactory performance capability.

Space-time block codes was pioneered by Siavash Alamouti. In 1998, Alamouti developed a full transmit diversity scheme for two transmit antennas. The full diversity scheme is known as the Alamouti code [42], which utilizes a simple maximum likelihood algorithm to decode the desired signal. Alamouti's work motivated Vahid Tarok *et al.* [30, 43–48] to generalize space-time block codes to accommodate the use of more than two transmit antennas. The generalized space-time block codes includes real and complex signal constellation designs, and also takes advantage of the simple maximum likelihood decoding algorithm. However, generalize space-time blocks for more than two antennas do not provide full-rate transmission.

In an effort to provide full-rate transmission for space-time block codes with more than two transmit antennas, quasi-orthogonal space-time block codes (QO-STBCs) [49, 50], were proposed. With the quasi-orthogonal structure, the orthogonality of the code is relaxed to provide a higher symbol transmission.

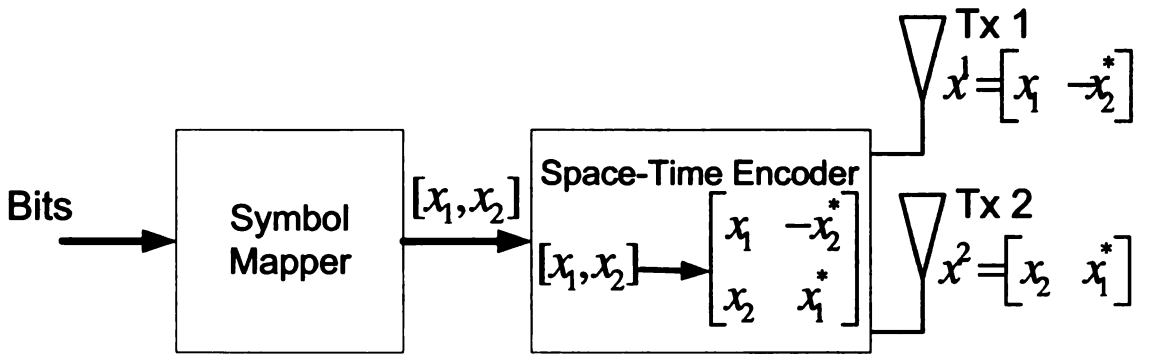

Figure 2.1. Transmitter for the Alamouti Scheme

The rest of the chapter is organized as follows: In Section 2.2, we introduce the encoding and decoding schemes, and the performance of the Alamouti code. In Section 2.3, we review generalized space-time block codes for systems with more than two antennas. In Section 2.4, we discuss quasi-orthogonal space-time block codes.

2.2 Alamouti Space-Time Coding

The Alamouti code is the first and only full-rate, full transmit diversity space-time block code. The key features of the Alamouti code is that it achieves satisfactory performance and only requires the linear processing of the maximum likelihood decoding algorithm. In this section, we discuss the encoding, decoding and performance of the Alamouti code.

2.2.1 Alamouti Encoding

The Alamouti code considers a system with two transmit antennas. In Figure 2.1, a block diagram of the Alamouti space-time encoder is depicted with two transmit antennas. Initially, a block of information bits are transformed into a stream of baseband constellation complex symbols through a mapper. Then, the space-time encoder takes two complex symbols x_1 and x_2 in each encoding operation and maps

them to a transmission code matrix given by

$$\mathbf{X} = \begin{bmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{bmatrix}, \tag{2.1}$$

where * is the complex conjugate operator. At the first transmission period t, symbols x_1 and x_2 are transmitted from the first and second transmit antennas, respectively. During the second transmission period $t+T$, symbols $-x_2^*$ and x_1^* are transmitted from the first and second transmit antennas, respectively, where T is the symbol period.

From the transmission code matrix, it is clear that the Alamouti encoding is done in both space and time domains. In fact, the Alamouti code is orthogonal. Let us define the transmit sequence from antenna one and two by $\mathbf{x}^1 = [x_1, -x_2^*]$ and $\mathbf{x}^2 = [x_2, x_1^*]$, respectively. The Alamouti code is othogorthonal since the inner product of transmit sequences $\mathbf{x}^1$ and $\mathbf{x}^2$ is zero.

2.2.2 Alamouti Decoding

The Alamouti code considers a system with one receive antenna. The receiver design of the Alamouti scheme is depicted in Figure 2.2. The fading channel coefficients from the first and second transmit antennas to the receive antenna at time t are denoted by $h_1(t)$ and $h_2(t)$, respectively. Assuming that the fading channel coefficients are constant across two consecutive symbol transmission periods (quasi-static), the fading coefficients can be expressed as

$$h_1(t) = h_1(t+T) = h_1 = |h_1|e^{j\theta 1}, \tag{2.2}$$

$$h_2(t) = h_2(t+T) = h_2 = |h_2|e^{j\theta 2}, \tag{2.3}$$

where $|h_i|$ and θ_i, $i = 1, 2$, are the amplitude gain and phase shift for the path from transmit antenna i to the receive antenna.

At the receiver, the received signals over two consecutive symbol periods are de-

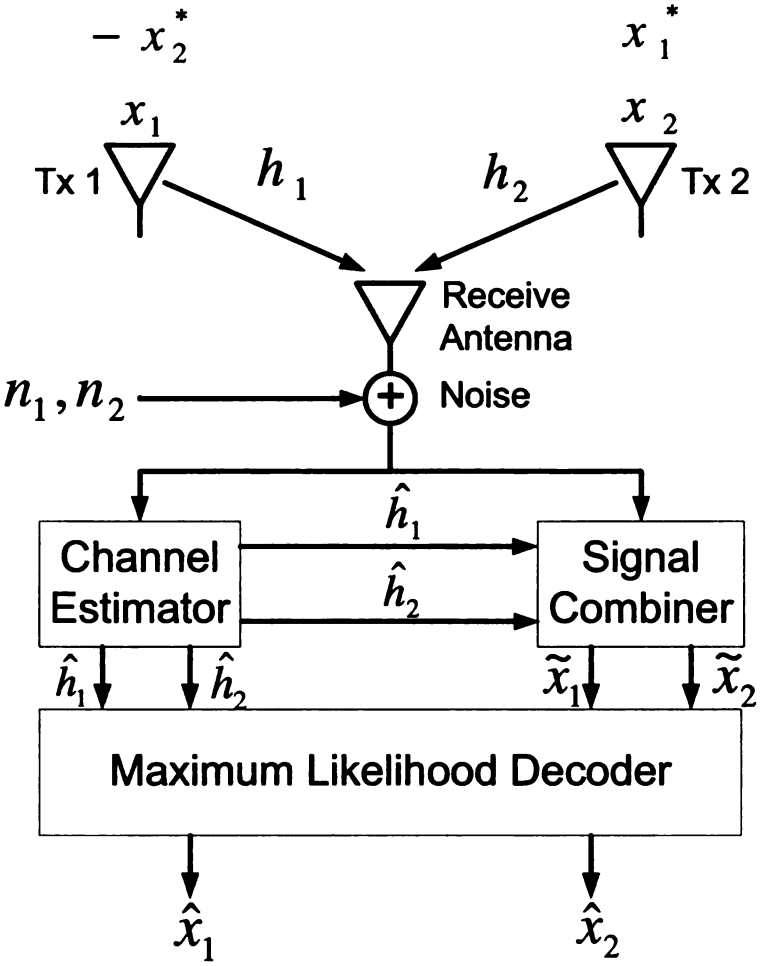

Figure 2.2. Receiver for the Alamouti Scheme

noted as r_1 and r_2 for the first and second transmission periods, respectively. The received signals are expressed as

$$r_1 = h_1 x_1 + h_2 x_2 + n_1, \tag{2.4}$$

$$r_2 = -h_1 x_2^* + h_2 x_1^* + n_2, \tag{2.5}$$

where n_1 and n_2 are independent additive white Gaussian noise with zero mean and variance σ_N^2.

Assuming ideal channel state information (CSI), and perfect synchronization between the transmitter and receiver, the desired signals can be recovered by the use of

a signal combiner and a maximum likelihood decoder. The signal combiner generates two decision statistics $\tilde{x}_1$ and $\tilde{x}_2$, by combining the received signals with the fading channel coefficients. The decision statistics can be expressed as

$$\begin{aligned} \tilde{x}_1 &= h_1^* r_1 + h_2 r_2^*, \\ \tilde{x}_2 &= h_2^* r_1 - h_1 r_2^*. \end{aligned} \tag{2.6}$$

The decision statistics can be rewritten by substituting r_1 and r_2 from (2.5) into (2.6), and expressed as

$$\begin{aligned} \tilde{x}_1 &= (|h_1|^2 + |h_2|^2)x_1 + h_1^* n_1 + h_2 n_2^*, \\ \tilde{x}_2 &= (|h_1|^2 + |h_2|^2)x_2 - h_1 n_2^* + h_2^* n_1. \end{aligned} \tag{2.7}$$

Note that the decision statistics $\tilde{x}_i$ is only a function of symbols x_i, $i = 1, 2$, thus the maximum likelihood decoding rule can be evaluated as two independent decoding rules. If we use the notation $d^2(x, y) = (x - y)(x^* - y^*) = |x - y|^2$ as the squared Euclidean distance between signals x and y, the independent decoding rules for x_1 and x_2 are expressed as,

$$\hat{x}_1 = \arg \min_{\hat{x}_1 \in S} (|h_1|^2 + |h_2|^2 + 1)|\hat{x}_1|^2 + d^2(\tilde{x}_1, \hat{x}_1), \tag{2.8}$$

$$\hat{x}_2 = \arg \min_{\hat{x}_2 \in S} (|h_1|^2 + |h_2|^2 + 1)|\hat{x}_2|^2 + d^2(\tilde{x}_2, \hat{x}_2). \tag{2.9}$$

For phase-shift keying (PSK) signal constellations, the term $(|h_1|^2 + |h_2|^2 + 1)$ is constant for each estimated symbol, therefore the decsion rule in (2.8) and (2.9) can be simplified to

$$\hat{x}_1 = \arg \min_{\hat{x}_1 \in S} d^2(\tilde{x}_1, \hat{x}_1), \tag{2.10}$$

$$\hat{x}_2 = \arg \min_{\hat{x}_2 \in S} d^2(\tilde{x}_2, \hat{x}_2). \tag{2.11}$$

2.2.3 Performance of the Alamouti Scheme

In this subsection, the bit error rate (BER) performance of the Alamouti scheme on slow Rayleigh fading channels is evaluated by simulation. For comparison, the BER performance of the maximal ratio combining (MRC) scheme is also simulated over slow Rayleigh fading channels. Each system transmits binary phase shift keying (BPSK) symbols. In Figure 2.3, we consider a system with one transmit and one receive antenna (no diversity), and a MRC system with one transmit antenna and two receive antennas, and Alamouti system with two transmit antennas and one receive antenna. From the Figure 2.3, it can be seen that the Alamouti code suffers a 3dB performance penalty. This is due to the fact that the power from each transmit antenna in the Alamouti code is half of the power from the transmit antenna in the MRC scheme. If the transmit antennas in the Alamouti code transmit the same power as the MRC scheme, then the Alamouti code would be equivalent to the MRC scheme. Also, in Figure 2.3, the Alamouti scheme and the MRC scheme have the same slope, which indicate that the Alamouti scheme has the same diversity order as the MRC scheme.

In Figure 2.4, the Alamouti scheme with one and two receive antennas are simulated over slow Rayleigh fading channels with BPSK modulation. From the figure we see that increasing the number of receive antenna improves the BER performance significantly.

2.3 Orthogonal Space-Time Block Codes

The satisfactory performance and decoding simplicity of the Alamouti scheme generated interest in multi-antenna systems with more than two transmit antennas. The simple maximum likelihood decoder provides full diversity gain at the receiver. Hence, a system with two transmit antennas and n_R receive antennas guarantees an overall diversity gain of $2n_R$, without CSI at the transmitter. The full diversity gain is achieved by the orthogonality between the sequences generated by the two transmit antennas. As a result, the Alamouti scheme was generalized to an arbitrary number

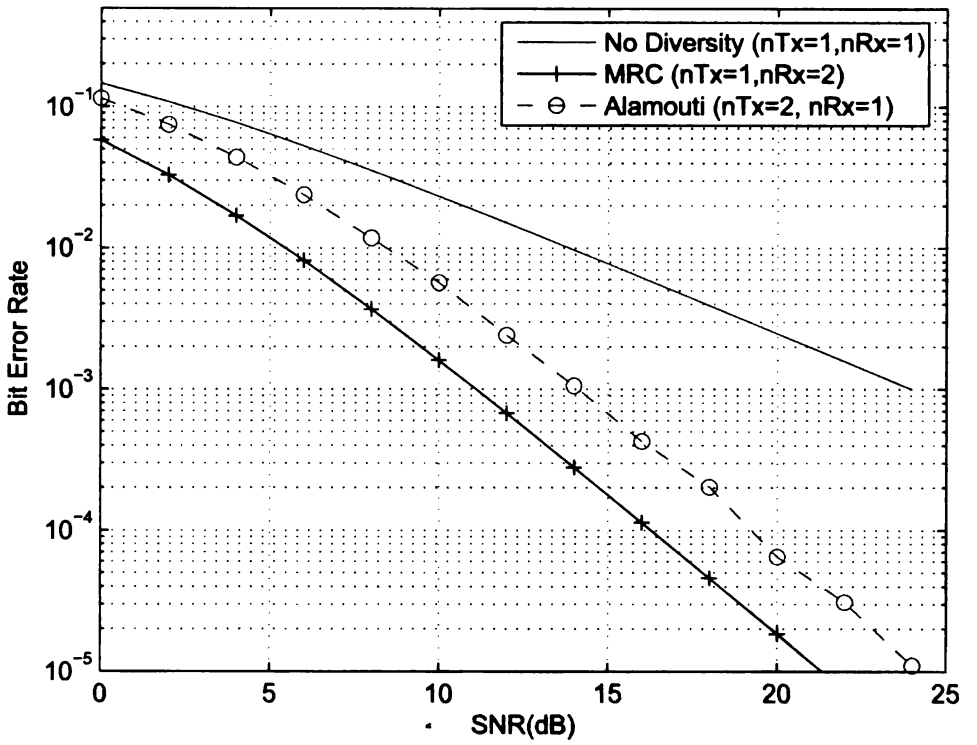

Figure 2.3. BER performance of Alamouti and MRC schemes.

of transmit antennas by applying the theory of orthogonal designs. The generalized schemes are referred to as orthogonal space-time block codes. The key features of orthogonal space-time codes is its capability of achieving full transmit diversity, while allowing a very simple maximum likelihood decoding algorithm.

Let n_T represent the number of transmit antennas and p represent the number of time periods for the transmission of one block of coded symbols. In general, a space-time block code is defined by an $n_T \times p$ transmission matrix, and k is the number of symbols the encoder takes as input for each encoding operation. In other words, during each encoding operation, k symbols are encoded into a $n_T \times p$ transmission matrix, which is transmitted in p time periods. The rate of the space-time block code is defined as the ratio between the number of symbols the encoder takes as its input and the number of space-time coded symbols transmitted from each antenna. The

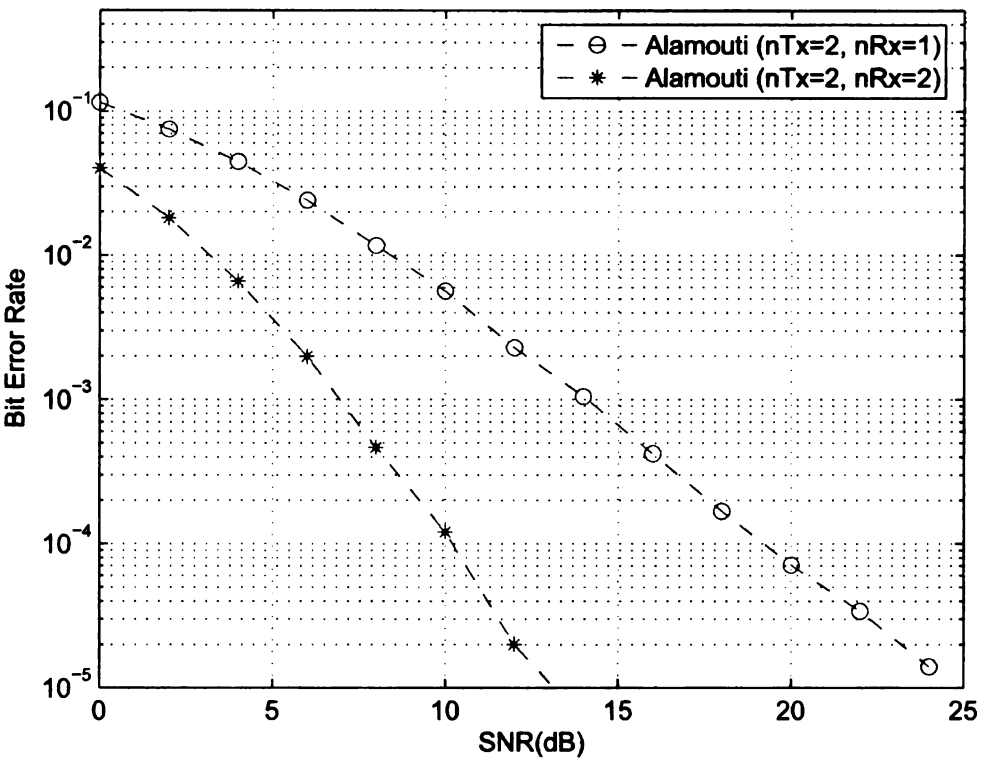

Figure 2.4. BER performance of Alamouti scheme with one receive antenna and two receive antennas.

rate is represented as

$$R = \frac{k}{p}. \tag{2.12}$$

The orthogonal space-time transmission matrix is constructed such that the rows and columns of each matrix are orthogonal to each other. In other words, the dot product of each row with another row is zero. The orthogonality of the transmission matrix yields full transmit diversity of n_T. In addition, orthogonality of the transmission matrix allows the receiver to decouple the signals transmitted from different antennas with the simple maximum likelihood decoding algorithm, which is based only on linear processing of the received signals. However, the orthogonality of the transmission matrix does not translate to full rate ($R = 1$) of the transmission matrix. In fact, the rate of the code matrix depends on how the code is constructed. In the following subsections, we show that it is relatively easy to construct full rate codes with real signal constellations, whereas the choice of full rate code matrices of complex signal constellations are more restricted.

2.3.1 Orthogonal Space-Time Block Codes for Real Signal Constellations

Orthogonal space-time block code designs are based on two types of signal constellations: *real* and *complex*. In this subsection, we discuss the construction of orthogonal space-time block codes for real signal constellations. We first introduce orthogonal space-time block codes with a square transmission matrix, then present orthogonal space-time block codes with non-square transmission matrix.

Let us denote orthogonal space-time block codes as $\mathbf{X}_{n_T}$. Note that, orthogonal space-time block codes with square transmission matrix have size $n_T \times n_T$. For any arbitrary real signal constellation, a square transmission matrix $\mathbf{X}_{n_T}$ exist only if the number of transmit antennas $n_T = 2, 4$, or 8 [43]. The transmission matrix for

$n_T = 2$ is given by

$$\mathbf{X}_2 = \begin{bmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{bmatrix}. \tag{2.13}$$

The transmission matrix for $n_T = 4$ is given by

$$\mathbf{X}_4 = \begin{bmatrix} x_1 & -x_2 & -x_3 & -x_4 \\ x_2 & x_1 & x_4 & -x_3 \\ x_3 & -x_4 & x_1 & x_2 \\ x_4 & x_3 & -x_2 & x_1 \end{bmatrix}. \tag{2.14}$$

The transmission matrix for $n_T = 8$ is given by

$$\mathbf{X}_8 = \begin{bmatrix} x_1 & -x_2 & -x_3 & -x_4 & -x_5 & -x_6 & -x_7 & -x_8 \\ x_2 & x_1 & -x_4 & x_3 & -x_6 & x_5 & x_8 & -x_7 \\ x_3 & x_4 & x_1 & -x_2 & -x_7 & -x_8 & x_5 & x_6 \\ x_4 & -x_3 & x_2 & x_1 & -x_8 & x_7 & -x_6 & x_5 \\ x_5 & x_6 & x_7 & x_8 & x_1 & -x_2 & -x_3 & -x4 \\ x_6 & -x_5 & x_8 & -x_7 & x_2 & x_1 & x_4 & -x_3 \\ x_7 & -x_8 & -x_5 & x_6 & x_3 & -x_4 & x_1 & x_2 \\ x_8 & x_7 & -x_6 & -x_5 & x_4 & x_3 & -x_2 & x_1 \end{bmatrix}. \tag{2.15}$$

The following codes have full rate ($R = 1$) and offer full transmit diversity of n_T. For example, if we consider (2.14), we observe that there are four transmit antennas (corresponding to the number of rows), and there are four transmission periods (corresponding to the number of columns). Also, the transmission matrix contains four symbols (x_1, x_2, x_3, x_4). As a result, the rate of $\mathbf{X}_4$ is given by

$$R = \frac{k}{p} = \frac{4}{4} = 1. \tag{2.16}$$

Full rate non-square real constellation code matrices also exist. From [43], non-

square code matrices with $n_T = 3, 5, 6$, and 7 are constructed as follows

$$\mathbf{X}_3 = \begin{bmatrix} x_1 & -x_2 & -x_3 & -x_4 \\ x_2 & x_1 & x_4 & -x_3 \\ x_3 & -x_4 & x_1 & x_2 \end{bmatrix}, \tag{2.17}$$

$$\mathbf{X}_5 = \begin{bmatrix} x_1 & -x_2 & -x_3 & -x_4 & -x_5 & -x_6 & -x_7 & -x_8 \\ x_2 & x_1 & -x_4 & x_3 & -x_6 & x_5 & x_8 & -x_7 \\ x_3 & x_4 & x_1 & -x_2 & -x_7 & -x_8 & x_5 & x_6 \\ x_4 & -x_3 & x_2 & x_1 & -x_8 & x_7 & -x_6 & x_5 \\ x_5 & x_6 & x_7 & x_8 & x_1 & -x_2 & -x_3 & -x4 \end{bmatrix}, \tag{2.18}$$

$$\mathbf{X}_6 = \begin{bmatrix} x_1 & -x_2 & -x_3 & -x_4 & -x_5 & -x_6 & -x_7 & -x_8 \\ x_2 & x_1 & -x_4 & x_3 & -x_6 & x_5 & x_8 & -x_7 \\ x_3 & x_4 & x_1 & -x_2 & -x_7 & -x_8 & x_5 & x_6 \\ x_4 & -x_3 & x_2 & x_1 & -x_8 & x_7 & -x_6 & x_5 \\ x_5 & x_6 & x_7 & x_8 & x_1 & -x_2 & -x_3 & -x4 \\ x_6 & -x_5 & x_8 & -x_7 & x_2 & x_1 & x_4 & -x_3 \end{bmatrix}, \tag{2.19}$$

$$\mathbf{X}_7 = \begin{bmatrix} x_1 & -x_2 & -x_3 & -x_4 & -x_5 & -x_6 & -x_7 & -x_8 \\ x_2 & x_1 & -x_4 & x_3 & -x_6 & x_5 & x_8 & -x_7 \\ x_3 & x_4 & x_1 & -x_2 & -x_7 & -x_8 & x_5 & x_6 \\ x_4 & -x_3 & x_2 & x_1 & -x_8 & x_7 & -x_6 & x_5 \\ x_5 & x_6 & x_7 & x_8 & x_1 & -x_2 & -x_3 & -x4 \\ x_6 & -x_5 & x_8 & -x_7 & x_2 & x_1 & x_4 & -x_3 \\ x_7 & -x_8 & -x_5 & x_6 & x_3 & -x_4 & x_1 & x_2 \end{bmatrix}. \tag{2.20}$$

Similar to the square transmission code construction, the non-square code is full

rate. For example, if we consider transmission matrix $\mathbf{X}_6$, we observe a total of eight symbols ($k = 8$) and eight transmission periods ($p = 8$). As a result, transmission matrix $\mathbf{X}_6$ has a rate of

$$R = \frac{k}{p} = \frac{8}{8} = 1. \tag{2.21}$$

2.3.2 Orthogonal Space-Time Block Codes for Complex Signal Constellations

In the previous subsection, we observed that constructing full transmit diversity, full rate orthogonal space-time block codes for real signal constellations is relatively easy. However, symbol constellations used in wireless communication typically contains complex constellations. Complex orthogonal design matrices have size $n_T \times p$ with entries of $x_1, x_2, \cdots, x_p$ and their conjugates. Such matrices have full transmit diversity of n_T with code rate k/p.

The Alamouti code is a complex orthogonal design matrix for two transmit antennas and is expressed as

$$\mathbf{X}_2^c = \begin{bmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{bmatrix}. \tag{2.22}$$

The Alamouti code is the only full transmit diversity, full rate space-time block code with complex constellation [43]. Consequently, the design goal of complex orthogonal matrices for more than two transmit antennas is to provide full transmit diversity and minimize the value of p to minimize the decoding delay.

For an arbitrary complex signal constellation, there are orthogonal space-time block codes that can achieve code rates of 1/2 and 3/4. Complex transmission matrices $\mathbf{X}_3^c$ and $\mathbf{X}_4^c$ are orthogonal designs for space-time block codes with three and four transmit antennas, respectively. Matrices $\mathbf{X}_3^c$ and $\mathbf{X}_4^c$ have a code rate of 1/2

and are expressed as [43]

$$\mathbf{X}_3^c = \begin{bmatrix} x_1 & -x_2 & -x_3 & -x_4 & x_1^* & -x_2^* & -x_3^* & -x_4^* \\ x_2 & x_1 & x_4 & -x_3 & x_2^* & x_1^* & x_4^* & -x_3^* \\ x_3 & -x_4 & x_1 & x_2 & x_3^* & -x_4^* & x_1^* & x_2^* \end{bmatrix}, \tag{2.23}$$

$$\mathbf{X}_4^c = \begin{bmatrix} x_1 & -x_2 & -x_3 & -x_4 & x_1^* & -x_2^* & -x_3^* & -x_4^* \\ x_2 & x_1 & x_4 & -x_3 & x_2^* & x_1^* & x_4^* & -x_3^* \\ x_3 & -x_4 & x_1 & x_2 & x_3^* & -x_4^* & x_1^* & x_2^* \\ x_4 & x_3 & -x_2 & x_1 & x_4^* & x_3^* & -x_2^* & x_1^* \end{bmatrix}. \tag{2.24}$$

Transmission matrix $\mathbf{X}_3^c$ consist of four complex symbols, which are transmitted in eight time periods via three transmit antenna; hence the code rate is 1/2. Similarly, transmission matrix $\mathbf{X}_4^c$ has a code rate of 1/2.

Transmission matrices $\mathbf{X}_3^h$ and $\mathbf{X}_4^h$ are complex generalized orthogonal designs for space-time block codes with rate 3/4. These codes are expressed as [43]

$$\mathbf{X}_3^h = \begin{bmatrix} x_1 & -x_2^* & \frac{x_3^*}{\sqrt{2}} & \frac{x_3^*}{\sqrt{2}} \\ x_2 & x_1^* & \frac{x_3^*}{\sqrt{2}} & \frac{-x_3^*}{\sqrt{2}} \\ \frac{x_3}{\sqrt{2}} & \frac{x_3}{\sqrt{2}} & \frac{-x_1-x_1^*+x_2-x_2^*}{2} & \frac{x_2+x_2^*+x_1-x_1^*}{2} \end{bmatrix}, \tag{2.25}$$

$$\mathbf{X}_4^h = \begin{bmatrix} x_1 & -x_2^* & \frac{x_3^*}{\sqrt{2}} & \frac{x_3^*}{\sqrt{2}} \\ x_2 & x_1^* & \frac{x_3^*}{\sqrt{2}} & \frac{-x_3^*}{\sqrt{2}} \\ \frac{x_3}{\sqrt{2}} & \frac{x_3}{\sqrt{2}} & \frac{-x_1-x_1^*+x_2-x_2^*}{2} & \frac{x_2+x_2^*+x_1-x_1^*}{2} \\ \frac{x_3}{\sqrt{2}} & \frac{-x_3}{\sqrt{2}} & \frac{-x_2-x_2^*+x_1-x_1^*}{2} & \frac{-x_1-x_1^*-x_2+x_2^*}{2} \end{bmatrix}. \tag{2.26}$$

Transmission matrix $\mathbf{X}_3^h$ consist of three complex symbols, which are transmitted in eight four periods via three transmit antenna, hence the code rate is 3/4. Similarly, transmission matrix $\mathbf{X}_4^c$ has a code rate of 3/4.

2.3.3 Decoding Orthogonal Space-Time Block Codes

Decoding orthogonal space-time block codes with more than two antennas is similar to decoding the Alamouti scheme. Assuming the channel coefficients $h_{j,i}(t)$ are constant over p symbol periods, such that

$$h_{j,i}(t) = h_{j,i}, \quad t = 1, 2, \cdots, p, \tag{2.27}$$

where i and j represent the transmit and receive antenna, respectively. The maximum likelihood decoding algorithm is used to construct the decision statistics for the transmitted signal x_i. As an example, we calculate the decision statistics for the space-time block code $\mathbf{X}_3^c$. The decision statistics for the other codes can be found in [43]. The decision statistics for $\mathbf{X}_3^c$ are

$$\tilde{x}_1 = \sum_{j=1}^{n_R} (r_1^j h_{j,1}^* + r_2^j h_{j,2}^* + r_3^j h_{j,3}^* + (r_5^j)^* h_{j,1} + (r_6^j)^* h_{j,2} + (r_7^j)^* h_{j,3}), \tag{2.28}$$

$$\tilde{x}_2 = \sum_{j=1}^{n_R} (r_1^j h_{j,2}^* - r_2^j h_{j,1}^* + r_4^j h_{j,3}^* + (r_5^j)^* h_{j,2} - (r_6^j)^* h_{j,1} + (r_8^j)^* h_{j,3}), \tag{2.29}$$

$$\tilde{x}_3 = \sum_{j=1}^{n_R} (r_1^j h_{j,3}^* - r_3^j h_{j,1}^* - r_4^j h_{j,2}^* + (r_5^j)^* h_{j,3} - (r_7^j)^* h_{j,1} - (r_8^j)^* h_{j,2}), \tag{2.30}$$

$$\tilde{x}_4 = \sum_{j=1}^{n_R} (-r_2^j h_{j,3}^* + r_3^j h_{j,2}^* - r_4^j h_{j,1}^* - (r_6^j)^* h_{j,3} + (r_7^j)^* h_{j,2} - (r_8^j)^* h_{j,1}). \tag{2.31}$$

2.4 Quasi-Orthogonal Space-Time Block Codes

Although, orthogonal space-time block codes are attractive for its full transmit diversity and linear maximum likelihood (ML) decoding properties, the full-rate orthogonal space-time block code for complex signal constellations only exist for two transmit antennas. In an effort to provide full-rate transmission for space-time block codes with more than two transmit antennas, quasi-orthogonal space-time codes (QO-STBCs) were proposed by three groups of researchers from three major telecommunication laboratories around the same time. Jafarkhani from the AT&T Laboratory named

his code QO-STBC [49], Tirkkonen, Boariu and Hottinen from Nokia Research named their code ABBA [50] for the code structure, and Papadias and Foschini from Lucent Technology Bell Laboratory did not name their code [51].

With the quasi-orthogonal structure, the orthogonality of the code is relaxed to provide a higher symbol transmission rate. Specifically, the data symbols in the QO-STBC are separable into groups after match filtering. The maximum likelihood (ML) decoding of QO-STBC is performed by jointly detecting symbols group by group, separately and in parallel. Whereas, in orthogonal STBCs, the decoding is performed by detecting single symbols. As a result, the decoding complexity of the QO-STBC is slightly higher than orthogonal STBC, but lower than a general non-orthogonal STBC.

2.4.1 Code Structure and Pairwise Decoding of Quasi-Orthogonal Space-Time Block Codes

Code Structure of Quasi-Orthogonal Space-Time Block Codes

The main advantages of codes from orthogonal designs are simple separate decoding and full diversity. However, orthogonal STBCs for more than two transmit antennas suffer from bandwidth inefficiency. In an effort to provide full diversity without the penalty in bandwidth efficiency, three independent research groups proposed QO-STBCs [49–51].

The first example of the QO-STBC is designed by Jafarkhani, which is denoted as **J4** and has the following code structure:

$$\mathbf{X_{J4}} = \begin{bmatrix} A & B \\ -\bar{B} & \bar{A} \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2^* & x_1^* & -x_4^* & x_3^* \\ -x_3^* & -x_4^* & x_1^* & x_2^* \\ x_4 & -x_3 & -x_2 & x_1 \end{bmatrix}, \tag{2.32}$$

where

$$A = \begin{bmatrix} x_1 & x_2 \\ -x_2^* & x_1^* \end{bmatrix} \text{ and } B = \begin{bmatrix} x_3 & x_4 \\ -x_4^* & x_3^* \end{bmatrix}, \tag{2.33}$$

and $\bar{A}$ and $\bar{B}$ are the complex conjugate of A and B, respectively.

A second example of the QO-STBC is known as the ABBA code and is proposed by Tirkkonen, Boariu, and Hottinen [50], which we denote as the **TBH** scheme. The **TBH** scheme has the following code structure

$$\mathbf{X_{TBH}} = \begin{bmatrix} A & B \\ B & A \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2^* & x_1^* & -x_4^* & x_3^* \\ x_3 & x_4 & x_1 & x_2 \\ -x_4^* & x_3^* & -x_2^* & x_1^* \end{bmatrix}, \tag{2.34}$$

where A, and B are the same as those in (2.33).

A third example of the QO-STBC code is proposed by Papadias and Foschini, and is denoted as **PF**. The code structure of the **PF** code is

$$\mathbf{X_{PF}} = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2^* & -x_1^* & x_4^* & -x_3^* \\ x_3 & -x_4 & -x_1 & x_2 \\ x_4^* & x_3^* & -x_2^* & -x_1^* \end{bmatrix}. \tag{2.35}$$

Pairwise Decoding of Quasi-Orthogonal Space-Time Block Codes

For each of the three QO-STBCs, the four transmitted data symbols contained in the codeword can be separated into two groups. As a result, the ML decoding can be performed by jointly detecting two complex symbols in each group separately. To illustrate the ML decoding of the QO-STBC, we consider the **J4** code in (2.32) as an example.

At the receiver, the maximum likelihood decision metric can be calculated as the

sum of two terms $f_{14}(x_1, x_4)+f_{23}(x_2, x_3)$, where $f_{14}(x_1, x_4)$ is independent of symbols x_2 and x_3, and $f_{23}(x_2, x_3)$ is independent of symbols x_1 and x_4. The minimization of the maximum likelihood decision metric is equivalent to the minimizing these two terms independently. After simple manipulation of the maximum likelihood decision metric, $f_{14}(x_1, x_4)$ and $f_{23}(x_2, x_3)$ can be express as

$$\begin{aligned} f_{14}(x_1, x_4) &= \sum_{j=1}^{n_R} \Bigg[\Big(\sum_{i=1}^{4} |h_{j,i}|^2 \Big) (|x_1|^2 + |x_4|^2) \\ &+ 2\mathrm{Re}\Big(x_1(-h_{j,1} r_1^{(j)*} - h_{j,2}^* r_2^{(j)} - h_{j,3}^* r_3^{(j)} - h_{j,4} r_4^{(j)*}) \\ &+ x_4(-h_{j,4} r_1^{(j)*} + h_{j,3}^* r_2^{(j)} + h_{j,2}^* r_3^{(j)} - h_{j,1} r_4^{(j)*}) \\ &+ x_1 x_4^* \times 2\mathrm{Re}(h_{j,1} h_{j,4}^* - h_{j,2} h_{j,3}^*) \Big) \Bigg], \end{aligned} \tag{2.36}$$

$$\begin{aligned} f_{23}(x_2, x_3) &= \sum_{j=1}^{n_R} \Bigg[\Big(\sum_{i=1}^{4} |h_{j,i}|^2 \Big) (|x_2|^2 + |x_3|^2) \\ &+ 2\mathrm{Re}\Big(x_2(-h_{j,2} r_1^{(j)*} - h_{j,1}^* r_2^{(j)} - h_{j,4}^* r_3^{(j)} - h_{j,3} r_4^{(j)*}) \\ &+ x_3(-h_{j,3} r_1^{(j)*} + h_{j,4}^* r_2^{(j)} + h_{j,1}^* r_3^{(j)} - h_{j,2} r_4^{(j)*}) \\ &+ x_2 x_3^* \times 2\mathrm{Re}(h_{j,1} h_{j,4}^* - h_{j,2} h_{j,3}^*) \Big) \Bigg], \end{aligned} \tag{2.37}$$

where $Re\{\cdot\}$ denotes the real part of $\{\cdot\}$.

Although the decoding complexity of the QO-STBC is less than of non-orthogonal designs, the QO-STBCs provided in this subsection do not achieve full diversity. Using the **PF** code (2.35) as an example, we show that QO-STBCs do not provide full diversity.

First we define codeword difference matrix $\mathbf{B}$ as

$$\mathbf{B} = \mathbf{X} - \hat{\mathbf{X}}, \tag{2.38}$$

where $\hat{\mathbf{X}}$ is the estimated codeword matrix, and calculate the codeword distance matrix $\mathbf{A}$ as

$$\begin{aligned}\mathbf{A} &= \mathbf{B}^H\mathbf{B} \\ &= \begin{bmatrix} a & 0 & 0 & b \\ 0 & a & -b & 0 \\ 0 & -b & a & 0 \\ b & 0 & 0 & a \end{bmatrix},\end{aligned} \tag{2.39}$$

where

$$a = \sum_{i=1}^{4} |x_i - \hat{x}_i|^2 \tag{2.40}$$

and

$$b = 2\mathrm{Re}\big((x_1 - \hat{x}_1)(x_4 - \hat{x}_4)^* - (x_2 - \hat{x}_2)(x_3 - \hat{x}_3)^*\big). \tag{2.41}$$

The determinant of codeword distant matrix is

$$\begin{aligned}\mathrm{Det}\big(\mathbf{B}^H\mathbf{B}\big) &= (a+b)^2(a-b)^2 \\ &= \big(|\Delta_1 + \Delta_4|^2 + |\Delta_2 - \Delta_3|^2\big)\big(|\Delta_1 - \Delta_4|^2 + |\Delta_2 + \Delta_3|^2\big),\end{aligned} \tag{2.42}$$

where $\Delta_i = x_i - \hat{x}_i$.

From (2.42), the minimum value occurs when half of the symbols have error, i.e. either $\Delta_1 = \Delta_4 = 0$ (while Δ_2 and Δ_3 are non-zero) or $\Delta_2 = \Delta_3 = 0$ (while Δ_1 and Δ_1 are non-zero). Hence, the minimum determinant value in (2.42), can be simplified as

$$\mathrm{Min}\big[\mathrm{Det}\big(\mathbf{B}^H\mathbf{B}\big)\big] = \big[|\Delta_1 + \Delta_4|^2|\Delta_1 - \Delta_4|^2\big], \tag{2.43}$$

assuming that $\Delta_2 = \Delta_3 = 0$.

From (2.43), when $\Delta_1 = \pm\Delta_4$, the determinant value of the codeword distance matrix would become zero, which implies the codeword distance matrix does not have full rank and cannot achieve full diversity. For example, if a conventional symmetric constellation sets such as phase shift keying (PSK) or quadrature amplitude modulation (QAM) is used, it is easy to see that the determinant of the codeword distance matrix will be zero. If a binary phase shift keying (BPSK) constellation set $\{-1, 1\}$ for all symbols, the possible values of Δ_i are $\{0, 2, -2\}$ for all value of i, therefore $\Delta_1 = \pm\Delta_4$ can easily be zero.

2.4.2 Quasi-Orthogonal Space-Time Block Codes with Constellation Rotation

Although QO-STBC can achieve higher code rates than orthogonal STBC, QO-STBCs generally does not provide full diversity. As a result, QO-STBC suffer from poor bit-error rate (BER) performance in high SNR levels. In an interest of achieving full diversity, QO-STBCs with constellation rotation were proposed in [52–56]. Specifically, the constellation rotation QO-STBC [55, 56] proposes that half of the symbols in the quasi-orthogonal design be chosen from a signal constellation $\mathcal{A}$ and the other half of the symbols be chosen from a rotated constellation $e^{j\phi}\mathcal{A}$.

Considering the BPSK and the **PF** code (2.35) as an example, it can be shown that the rotated constellation achieves full diversity. If x_1 is chosen from signal constellation $\mathcal{A}$ (hence Δ_1 takes values $\{0, 2, -2\}$), while symbol x_4 is chosen from a rotated signal constellation $e^{j\phi}\mathcal{A}$ (hence Δ_4 takes $\{0, 2\exp(j\phi), -2\exp(j\phi)\}$), then a non-zero value for $|\Delta_1 \pm \Delta_4|$ can always be obtained, assuming $\Delta_2 = \Delta_3 = 0$. Similarly, the constellation rotation can be applied to symbols pair (x_2, x_3).

In addition to providing full diversity, the constellation rotation gives an extra degree to maximize the minimum determinant value in (2.43) to achieve maximum coding gain for QO-STBC. Again, using the **PF** code (2.35) as an example, we illus-

trate constellation rotation code structure as follows

$$\mathbf{X}_{\mathbf{PF}_{CR}} = \begin{bmatrix} x_1 & x_2 & e^{j\phi}x_3 & e^{j\phi}x_4 \\ x_2^* & -x_1^* & (e^{j\phi}x_4)^* & (e^{j\phi}x_3)^* \\ e^{j\phi}x_3 & -e^{j\phi}x_4 & -x_1 & x_2 \\ (e^{j\phi}x_4)^* & (e^{j\phi}x_3)^* & -x_2^* & -x_1^* \end{bmatrix}. \tag{2.44}$$

2.4.3 Performance of Quasi-Orthogonal Space-Time Block Codes

In this subsection, the BER performance of the QO-STBC with and without constellation rotation on Rayleigh fading channels are evaluated by simulation. For comparison, the BER performance of the OSTBC is also simulated over Rayleigh fading channels. Each system is equipped with four transmit antennas and one receive antenna. The OSTBC scheme is rate-$\frac{1}{2}$ and the QO-STBCs are rate-1. In order to for all schemes to have the same spectral efficiency of 2 bps/Hz for fair comparison, the rate-$\frac{1}{2}$ transmits 16-QAM systems, while the rate-1 QO-STBCs transmits QPSK symbols. It can be seen from Figure 2.5 that both QO-STBCs perform better than the OSTBC scheme at low SNR levels. This is due to the fact that QO-STBCs have a higher code rate and the QPSK constellation that has a larger Euclidean distance than 16-QAM constellation. However, as the SNR increases, the OSTBC scheme begins to outperform the QO-STBC without constellation rotation due to the lack of full diversity. On the other hand, the QO-STBC with constellation rotation performs consistently better than OSTBC.

2.5 Summary

In summary, space-time coding is a signal technique design aimed at approaching the information theoretic capacity limit of MIMO systems. Space-time block codes were pioneered by Siavash Alamouti, who developed a full transmit diversity scheme for two transmit antennas. Alamouti's work motivated Vahid Tarok *et al.* to generalize

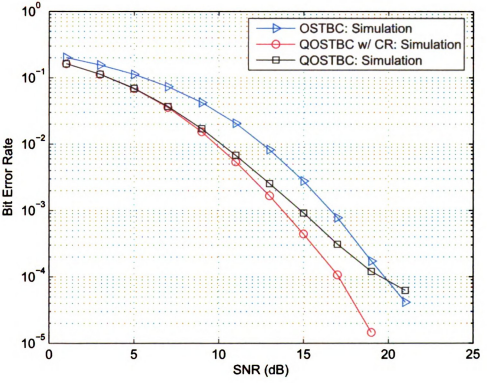

Figure 2.5. BER performance of OSTBC vs. QO-STBC schemes with and without constellation rotation.

space-time block codes to accommodate the use of more than two transmit antennas. However, generalize space-time block codes for more than two antennas do not provide full-rate transmission. In an effort to provide full-rate transmission for space-time block codes with more than two transmit antennas, quasi-orthogonal space-time block codes were proposed, where the orthogonality of the code is relaxed to provide a higher symbol transmission.

CHAPTER 3

Spectrally Efficient Space-Time Coding

In this chapter, we introduce a spectrally efficient Alamouti scheme. First, we investigate the code efficiency of the Alamouti code from a bit-level perspective by introducing the concepts of *Alamouti patterns* and *irregular partitioning*. Our investigation reveals the possibility of spectral efficiency enhancement. Second, we propose a novel spectrally efficient Alamouti code. The proposed scheme improves the code efficiency of the traditional Alamouti scheme by increasing the number of information bits transmitted in each Alamouti block. Finally, we provide simulation examples to demonstrate the effectiveness of the proposed spectrally efficient Alamouti code.

3.1 Introduction

Theoretical and experimental results of multiple-input multiple- output (MIMO) systems promise dramatic improvements in spectral efficiency. Pioneering research of Foschini and Telatar [30, 31] shows that the channel capacity grows linearly as the number of transmit and receive antennas grow simultaneously. As a result, multiple transmit and receive antennas with space-time coding has been the subject of many works [30, 39, 42, 43, 48, 57–65] to achieve high data rates.

Schemes such as BLAST [30] and V-BLAST [48] have been proposed to exploit the spatial multiplexing to transmit independent data streams over MIMO channels. Although BLAST can handle high data rates, there are some drawbacks against its use for downlink communications. First, the data stream suffers from deep fades

during the transmission due to the lack of spatial coding. Second, the receiver relies on powerful signal processing techniques, e.g., a sequence of nulling and canceling steps, to detect the desired signals. Third, the performance is subject to degradation for the V-BLAST decoding scheme, when the number of receive antennas is less than the number of transmit antennas.

Space-time codes that use algebraic designs have recently been proposed to simultaneously achieve full rate and maximum diversity [62,63]. The full diversity of these codes are achieved by extending the block length. Consequently, more data symbols need to be jointly decoded than with V-BLAST, leading to a dramatic increase in complexity.

Unlike most of the existing methods which are designed to maximize the diversity or rate for space-time block codes, the proposed scheme aims to improve the code efficiency of the Alamouti codes, while achieving full transmit diversity and retaining the decoding simplicity. For example, even the so-called full-rate orthogonal codes [39, 42,43] are low-efficient codes. Defining the code efficiency as the ratio of information bits to the total number of bits transmitted in a space-time block, we find out that the full-rate Alamouti code, only achieves a code efficiency of 0.5. As a matter of fact, all other full-rate space-time block codes have a code efficiency of 0.5, and non full-rate space-time block codes have a code efficiency less than 0.5.

As an effort to increase the code efficiency of space-time block codes, we investigate the traditional Alamouti space-time code from a bit-level perspective and propose a spectrally efficient Alamouti scheme. The proposed scheme enhances the spectral efficiency by increasing the number of information bits transmitted in each Alamouti block. Furthermore, the proposed scheme achieves high transmit diversity and retains the decoding simplicity of the maximum likelihood decoder.

The rest of the chapter is organized as follows: In Section 3.2 we review the system model for the Alamouti code. In Section 3.3, we investigate the code efficiency of the Alamouti code from a bit-level perspective by introducing the concepts of *Alamouti patterns* and *irregular partitioning*. In Section 3.4, we propose a spectrally efficient Alamout code design. We provide illustrative simulation examples of the proposed

scheme in Section 3.5. Finally, in Section 3.6, we provide a summary.

3.2 System Model of Alamouti Scheme

In this section, we briefly review the Alamouti code and investigate the Alamouti code from a symbol-level perspective. Our investigation reveals that the traditional Alamouti scheme has a low code efficiency.

Recall, the Alamouti scheme is a full-rate full-diversity orthogonal code for a system with two transmit antennas and one receive antenna. From a symbol-level perspective, the input binary stream is first mapped into symbols based on a particular constellation $\mathcal{A}$. In each encoding operation, two symbols x_1 and x_2 are encoded into the *Alamouti matrix*, which is expressed as

$$\begin{array}{c} \text{Time} \\ \rightarrow \\ \begin{bmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{bmatrix} \downarrow \text{Space}, \end{array} \tag{3.1}$$

where the complex scalars x_1 and x_2 are chosen from a particular (M-PSK or M-QAM) constellation, and x_1^* and x_2^* are the complex conjugates of x_1 and x_2, respectively. The bits related to $\{x_1^*, -x_2^*\}$ depends only on $\{x_1, x_2\}$ once the signal constellation is fixed. As a matter of fact, only the bits corresponding to $\{x_1, x_2\}$ carry the useful information and the others are redundancy bits. In other words, there is room for spectral efficiency enhancement.

Assuming that one receive antenna is employed at the receiver and the fading coefficients, i.e., $\{h_1, h_2\}$, are invariant across two consecutive symbols, the received signals can then be expressed as,

$$\begin{bmatrix} r_1 & r_2 \end{bmatrix} = \begin{bmatrix} h_1 & h_2 \end{bmatrix} \begin{bmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{bmatrix} + \begin{bmatrix} n_1 & n_2 \end{bmatrix}, \tag{3.2}$$

where r_1 and r_2 are the received signals at time t and $t+T$ and n_1 and n_2 are complex random variables representing receiver noise. Rewrite (3.2) as

$$\underbrace{\begin{bmatrix} r_1 \\ r_2^* \end{bmatrix}}_{\triangleq \mathbf{R}} = \underbrace{\begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix}}_{\triangleq \mathbf{H}} \underbrace{\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}}_{\triangleq \mathbf{X}} + \underbrace{\begin{bmatrix} n_1 \\ n_2^* \end{bmatrix}}_{\triangleq \mathbf{N}}. \tag{3.3}$$

Note that $\mathbf{H}^{\mathcal{H}}\mathbf{H} = \mathbf{H}\mathbf{H}^{\mathcal{H}} = (|h_1|^2 + |h_2|^2)\mathbf{I}_2$, where I_2 is 2×2 identity matrix and $\mathcal{H}$ is the Hermitian conjugate. It follows that

$$\mathbf{Z} = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} \triangleq \mathbf{H}^{\mathcal{H}}\mathbf{R} = (|h_1|^2 + |h_2|^2)\mathbf{I}_2\mathbf{X} + \mathbf{H}^{\mathcal{H}}\mathbf{N}, \tag{3.4}$$

therefore, maximum-likelihood decoding of x_1 and x_2 can be decoupled:

$$\hat{x}_1 = \arg \min_{x_k \in \mathcal{A}} \{|z_1 - x_k|^2 + (|h_1|^2 + |h_2|^2 - 1)|x_k|^2\}, \tag{3.5}$$

$$\hat{x}_2 = \arg \min_{x_k \in \mathcal{A}} \{|z_2 - x_k|^2 + (|h_1|^2 + |h_2|^2 - 1)|x_k|^2\}. \tag{3.6}$$

For PSK signals, the decision rule in (3.5) and (3.6) can be further simplified as follows:

$$\hat{x}_1 = \arg \min_{x_k \in \mathcal{A}} \{|z_1 - x_k|^2\}, \tag{3.7}$$

$$\hat{x}_2 = \arg \min_{x_k \in \mathcal{A}} \{|z_2 - x_k|^2\}. \tag{3.8}$$

3.3 Bit-Level Inspection of the Alamouti Code

In this section, we introduce the concepts of *Alamouti patterns* and *irregular partitioning* to investigate the code efficiency of the Alamouti scheme from a bit-level perspective.

3.3.1 The Alamouti Patterns

Assume that all the symbols in the Alamouti transmission matrix (3.1) are drawn from a quadrature phase shift keying (QPSK) constellation with Gray code mapping, as shown in Figure 3.1.

Define *Alamouti patterns* to be all possible matrices with bit representation of (3.1). For example, if $x_1 = e^{(j\frac{\pi}{4})}$ and $x_2 = e^{(j\frac{3\pi}{4})}$, then $x_1^* = e^{(j\frac{7\pi}{4})}$ and $-x_2^* = e^{(j\frac{\pi}{4})}$. The corresponding bit representations of the four signals are 00, 01, 10 and 00, respectively. If we replace each symbol with its bit representation in (3.1) we get an Alamouti pattern, $\begin{bmatrix} 0000 \\ 0110 \end{bmatrix}$.

By computing all combinations of $\{x_1, x_2\}$ through the constellation points, we find all Alamouti patterns, which are listed in (3.9). Obviously, bits in each Alamouti pattern are not independent. Define *crucial bits* to be the necessary bits uniquely determining the Alamouti pattern, and *auxiliary bits* to be the bits totally dependent on crucial bits. In fact, only crucial bits contain useful information and auxiliary bits are redundant in some sense. In this case, crucial bits can be chosen to be bit representations of x_1 and x_2, i.e., the first two columns of each Alamouti pattern.

Define the *code efficiency* (η) as the ratio of the number of crucial bits to the total number of bits in each Alamouti pattern, such that η is bounded by $0 \leq \eta \leq 1$. Due to the use of auxiliary bits, in this particular case, $\eta = 0.5$. In fact, for all the other full-rate space-time block codes, the efficiency is also 0.5, and even worse for non full-rate codes.

$$\text{Alamouti patterns for QPSK}: \left\{ \begin{array}{l} \begin{bmatrix} 0001 \\ 0010 \end{bmatrix}, \begin{bmatrix} 0000 \\ 0110 \end{bmatrix}, \begin{bmatrix} 0011 \\ 1010 \end{bmatrix}, \begin{bmatrix} 0010 \\ 1110 \end{bmatrix}, \\ \begin{bmatrix} 0101 \\ 0011 \end{bmatrix}, \begin{bmatrix} 0100 \\ 0111 \end{bmatrix}, \begin{bmatrix} 0111 \\ 1011 \end{bmatrix}, \begin{bmatrix} 0110 \\ 1111 \end{bmatrix}, \\ \begin{bmatrix} 1001 \\ 0000 \end{bmatrix}, \begin{bmatrix} 1000 \\ 0100 \end{bmatrix}, \begin{bmatrix} 1011 \\ 1000 \end{bmatrix}, \begin{bmatrix} 1010 \\ 1100 \end{bmatrix}, \\ \begin{bmatrix} 1101 \\ 0001 \end{bmatrix}, \begin{bmatrix} 1100 \\ 0101 \end{bmatrix}, \begin{bmatrix} 1111 \\ 1001 \end{bmatrix}, \begin{bmatrix} 1110 \\ 1101 \end{bmatrix}. \end{array} \right\} \tag{3.9}$$

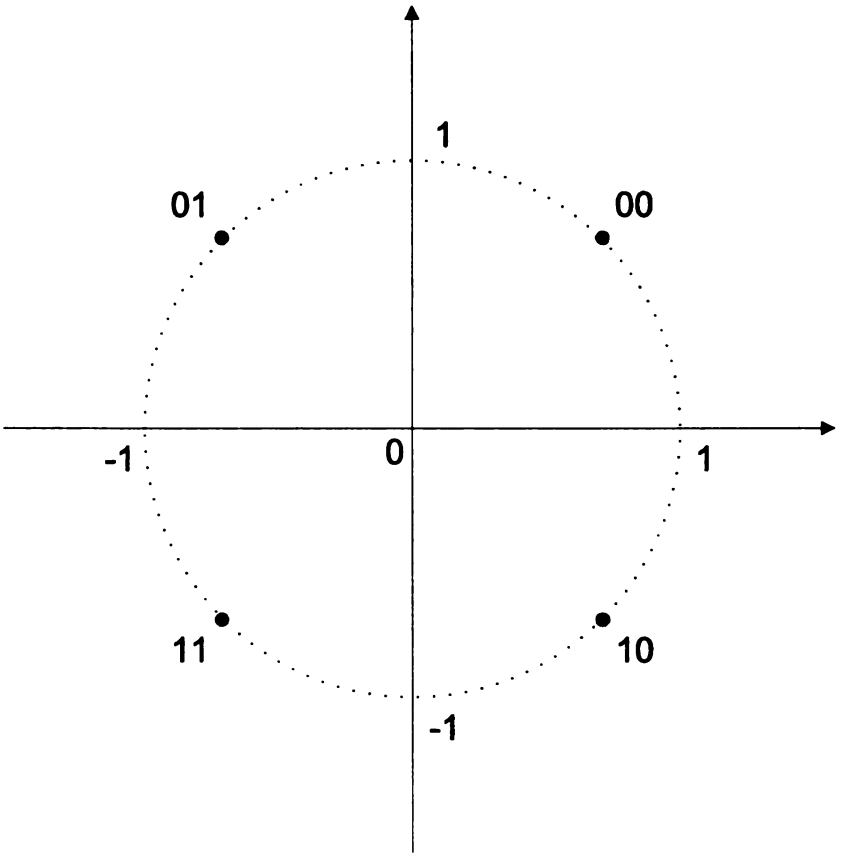

Figure 3.1. QPSK constellation with Gray mapping.

On the other hand, if we partition the original bit stream into groups of size 2×4 like the Alamouti patterns, and each group consists of one Alamouti pattern, then no extra bits need to be inserted into data stream in order to form the Alamouti matrix before transmission. In other words, the data rate is really "full" in this situation and the efficiency is at its maximum, i.e., $\eta = 1$. However, since the original data stream is random, the probability of each group being a Alamouti pattern is only $\frac{2^4}{2^8} = 6.25\%$. Suppose that the number of groups is N and the groups are independent of one another, it turns out that the probability of achieving $\eta = 1$ for the random data stream is $(6.25\%)^N$, which is a very small number if $N > 2$. In other words, practical systems using the Alamouti code achieves $\eta = 1$ with nearly zero probability.

3.3.2 Irregular Partitioning of the Alamouti Code

To generalize the concept of grouping Alamouti patterns, we introduce *irregular partitioning*. Assume that the original bit stream is partitioned into groups of size $2 \times M$ matrix, denoted by B.

In *irregular partitioning*, the input bit stream is first partitioned into a 2×4 matrix. If the 2×4 matrix matches a valid Alamouti pattern, then the corresponding matrix has maximum efficiency. In the case that the 2×4 matrix does not match any valid Alamouti patterns, the matrix is reduced to a 2×3 matrix. If the 2×3 matrix matches the prefix of a valid Alamouti pattern, then a suffix *auxiliary bits* are appended to the 2×3 matrix, yielding a full 2×4 Alamouti pattern. Note, a 2×3 partition has $\eta = 0.75$. In the case that the 2×3 partition does not match the prefix of any valid Alamouti patterns, the partition is reduced to a 2×2 matrix. At this point, there is always a 2×2 partition prefix match of a valid Alamouti pattern. As a result, the 2×2 partition has $\eta = 0.5$. The pseudo-code of this *irregular partitioning* is listed as follows:

According to the above irregular partitioning, the probabilities of resulting 2×4 matrix, 2×3 matrix or 2×2 matix, in theory, are $\frac{2^4}{2^8} = 6.25\%$, $(1-6.25\%)\frac{2^4}{2^6} = 23.44\%$ and $(1 - 6.25\% - 23.44\%)\frac{2^4}{2^4} = 68.75\%$, respectively. Assuming that the receiver has

```
                    Irregular Partitioning
Initialize i = 1, j = 4.
While i < M
    If B(:, i : j) doesn't match any Alamouti patterns
        j = j − 1
        If B(:, i : j) doesn't match any Alamouti patterns'
                first three columns
            j = j − 1
        End if
    End if
    Record j
    i = j + 1
    j = j + 4
End while
```

the knowledge of the partitioning strategy, the theoretical code efficiency is given by

$$\eta = 1 \cdot 6.25\% + 0.75 \cdot 23.44\% + 0.5 \cdot 68.75\% = 0.5820, \tag{3.9}$$

which is pretty close to the simulation results, $\eta = 0.5796$.

On the other hand, the Alamouti code can be regarded as a *regular partitioning* of the input. Each partitioned block is always a 2×2 matrix, which are treated as crucial bits. The other 2×2 matrix of auxiliary bits are appended to crucial bits in each block. Thus, $\eta = 0.5$.

Although the code efficiency is slightly improved by the irregular partitioning scheme, it introduces extra complexity to the transmitter. Furthermore, it is not realistic to assume that the knowledge of the data-dependent partitioning strategy is available at the receiver.

3.4 The Spectrally Efficient Alamouti Scheme

Our goal is to enhance the efficiency of the Alamouti code, and at the same time achieve high transmit diversity and retain the decoding simplicity.

3.4.1 Encoding Algorithm Design

Starting with Alamouti patterns of QPSK, we try to increase the number of crucial bits by one. Since there are 16 valid Alamouti patterns, each pattern can be uniquely determined by four crucial bits. How do we increase the number of crucial bits by one? We propose to use dual constellations, and the fifth crucial bit can be utilized to indicate a specific constellation for transmission. In this particular case, two constellations, A_0 and A_1 are illustrated in Figure 3.2, where A_1 is obtained by rotating A_0 clockwise by $\pi/4$. The constellations are coded for minimum BER by minimizing the number of nearest neighbors.

At the transmitter, the binary data stream is first divided into 5-bit groups. The first four bits are used to select one of the Alamouti pattern from (3.9). The fifth bit chooses one of two constellations, which are depicted in Figure 3.2. In particular, the fifth bit equal to "0" indicates the use of A_0 constellation, while the fifth bit equal to "1" indicates the use of A_1 constellation as an alternative. It turns out that the transmission matrix has the same format of the Alamouti matrix, but each Alamouti block now contains 5 information bits rather than 4 bits in the original Alamouti code.

Let $b_5 \in \{0, 1\}$ denote the fifth bit. The transmission matrix can be represented as

$$\begin{bmatrix} x_1 \cdot e^{-j\frac{\pi}{4}b_5} & -x_2^* \cdot e^{-j\frac{\pi}{4}b_5} \\ x_2 \cdot e^{-j\frac{\pi}{4}b_5} & x_1^* \cdot e^{-j\frac{\pi}{4}b_5} \end{bmatrix}. \tag{3.10}$$

3.4.2 Decoding Algorithm Design

Assuming the receiver is equipped with one receive antenna and the channel coefficients are invariant across two consecutive symbols, it follows that the received signal in (3.3) becomes

$$\underbrace{\begin{bmatrix} r_1 \\ r_2^* \end{bmatrix}}_{\triangleq \mathbf{R}} = \underbrace{\begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix}}_{\triangleq \mathbf{H}} \underbrace{\begin{bmatrix} x_1 \cdot e^{-j\frac{\pi}{4}b_5} \\ x_2 \cdot e^{-j\frac{\pi}{4}b_5} \end{bmatrix}}_{\triangleq \mathbf{X}} + \underbrace{\begin{bmatrix} n_1 \\ n_2^* \end{bmatrix}}_{\triangleq \mathbf{N}}, \tag{3.11}$$

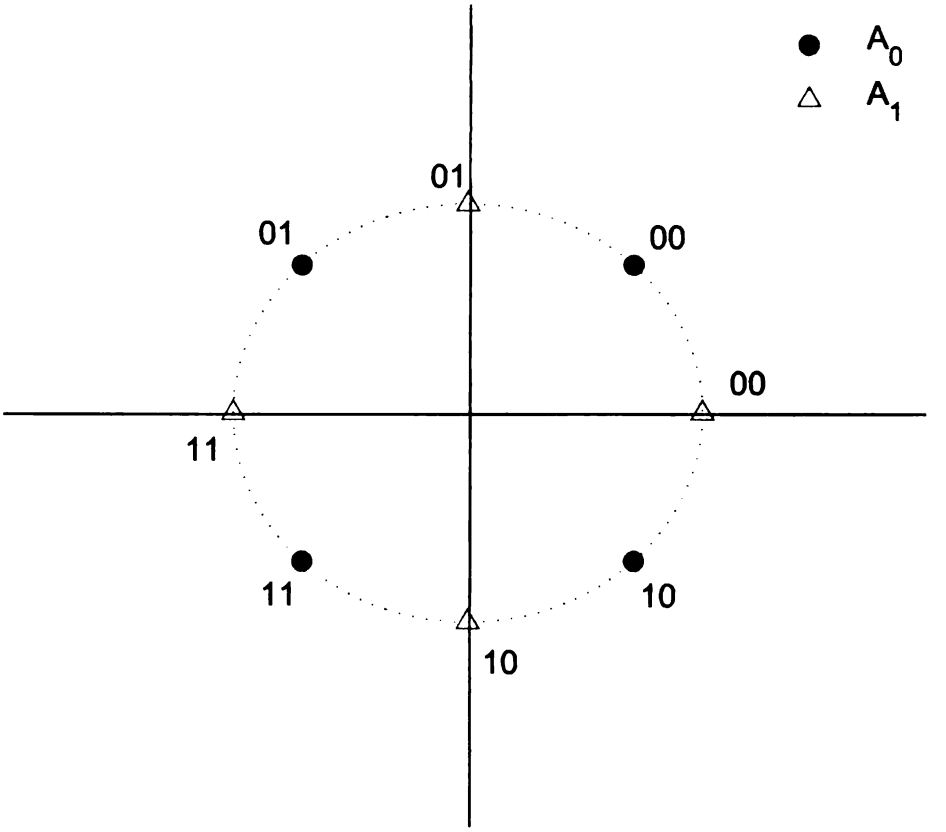

Figure 3.2. Constellation design for the spectrally efficient Alamouti code.

and (3.4) becomes

$$\mathbf{Z} = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} \triangleq \mathbf{H}^{\mathcal{H}}\mathbf{R} = (|h_1|^2 + |h_2|^2)\mathbf{I}_2\mathbf{X} + \mathbf{H}^{\mathcal{H}}\mathbf{N}. \tag{3.12}$$

The fifth bit b_5 is decided by the locations of z_1 and z_2. Assuming that all the signals in the A_0 and A_1 constellations are equiprobable, the signals $\hat{z}_1$ and $\hat{z}_2$ are

chosen from the constellations to minimize the distance metric

$$\begin{aligned}
\hat{z}_1 &= \arg \min_{\hat{z}_1 \in A_0, A_1} \left(d^2(z_1, (|h_1|^2 + |h_2|^2)\hat{z}_1) + d^2(z_2, (|h_1|^2 + |h_2|^2)\hat{z}_1) \right) \\
&= \arg \min_{\hat{z}_1 \in A_0, A_1} \left(|z_1 - (|h_1|^2 + |h_2|^2)\hat{z}_1|^2 + |z_2 - (|h_1|^2 + |h_2|^2)\hat{z}_1|^2 \right) \quad (3.13) \\
\hat{z}_2 &= \arg \min_{\hat{z}_1 \in A_0, A_1} \left(d^2(z_1, (|h_1|^2 + |h_2|^2)\hat{z}_2) + d^2(z_2, (|h_1|^2 + |h_2|^2)\hat{z}_2) \right) \\
&= \arg \min_{\hat{z}_1 \in A_0, A_1} \left(|z_1 - (|h_1|^2 + |h_2|^2)\hat{z}_2|^2 + |z_2 - (|h_1|^2 + |h_2|^2)\hat{z}_2|^2 \right) \quad (3.14)
\end{aligned}$$

over all possible values of $\hat{z}_1$ and $\hat{z}_2$. If $\hat{z}_1 < \hat{z}_2$, then $b_5 = 0$, else if, $\hat{z}_1 > \hat{z}_2$, then $b_5 = 1$.

Once b_5 is determined, maximum-likelihood decoding of x_1 and x_2 can still be decoupled as:

$$\hat{x}_1 = \arg \min_{x_1 \in A_{b_5}} \{|z_1 - x_1 e^{-j\frac{\pi}{4}b_5}|^2\}, \quad (3.15)$$

$$\hat{x}_2 = \arg \min_{x_2 \in A_{b_5}} \{|z_2 - x_2 e^{-j\frac{\pi}{4}b_5}|^2\}. \quad (3.16)$$

Discussions: It can be seen that the proposed scheme increases the spectral efficiency in systems with two transmit antennas and QPSK modulation. Modulation schemes other than QPSK will produce different Alamouti patterns, thus yielding different performance. Furthermore, the proposed scheme does not change the code structure, therefore the same idea can be extended to space-time block codes for more than two transmit antennas.

3.5 Simulation Examples

In this section, simulation results are provided to demonstrate the performance of the proposed spectrally efficient Alamouti code. The proposed scheme with QPSK modulation is compared with Alamouti codes with QPSK and 8PSK modulations. Note that the traditional Alamouti codes with QPSK modulation (*Alamouti-QPSK*)

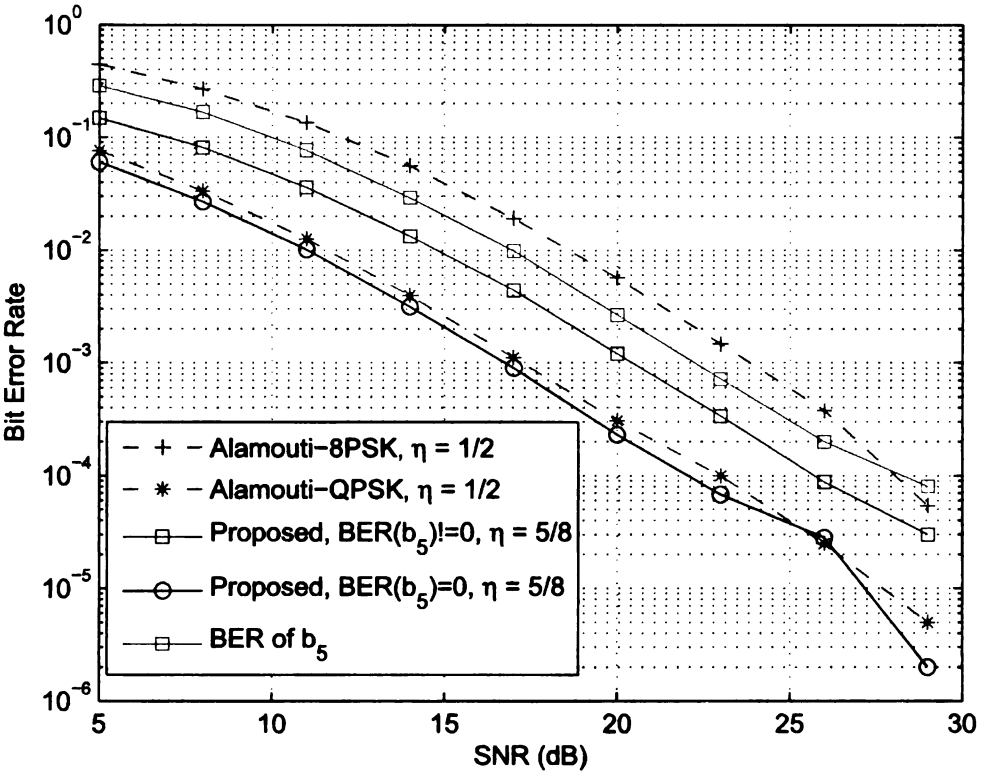

Figure 3.3. The BER performance comparison of the proposed scheme and the Alamouti code in Rayleigh flat fading, $n_T = 2$, $n_R = 1$.

and 8PSK modulation (*Alamouti-8PSK*) are considered full-rate space-time block codes. As a result, their code efficiency is only 0.5. On the other hand, the proposed scheme, increases the number of information bits by one per Alamouti block, resulting in an increase of code efficiency to 0.625. In Figure 3.3, the bit error rate (BER) performance of the three schemes are evaluated in Rayleigh flat fading and equipped with $n_T = 2$ and $n_R = 1$ antennas. In addition, we plot the BER performance of the fifth bit b_5 and the proposed scheme with perfect recovery of b_5 i.e., the number of errors related to b_5 is zero ($BER(b_5) = 0$). The minimum Euclidean distance between two QPSK constellations in Figure 3.2 is the same as that of a 8PSK constellation. Therefore, in the worst case, the BER performance of the proposed scheme will be slightly worse than Alamouti-8PSK, due to additional b_5 errors. On the contrary,

if the recovery of b_5 is perfect, then the selection of the QPSK constellation at the receiver is always correct. Correspondingly, the minimum Euclidean distance turns out to be the same as that of a QPSK constellation. Thus, in the best case (perfect recovery of b_5), the BER performance of the proposed scheme will outperform the Alamouti-QPSK due to the perfect reconstruction of b_5.

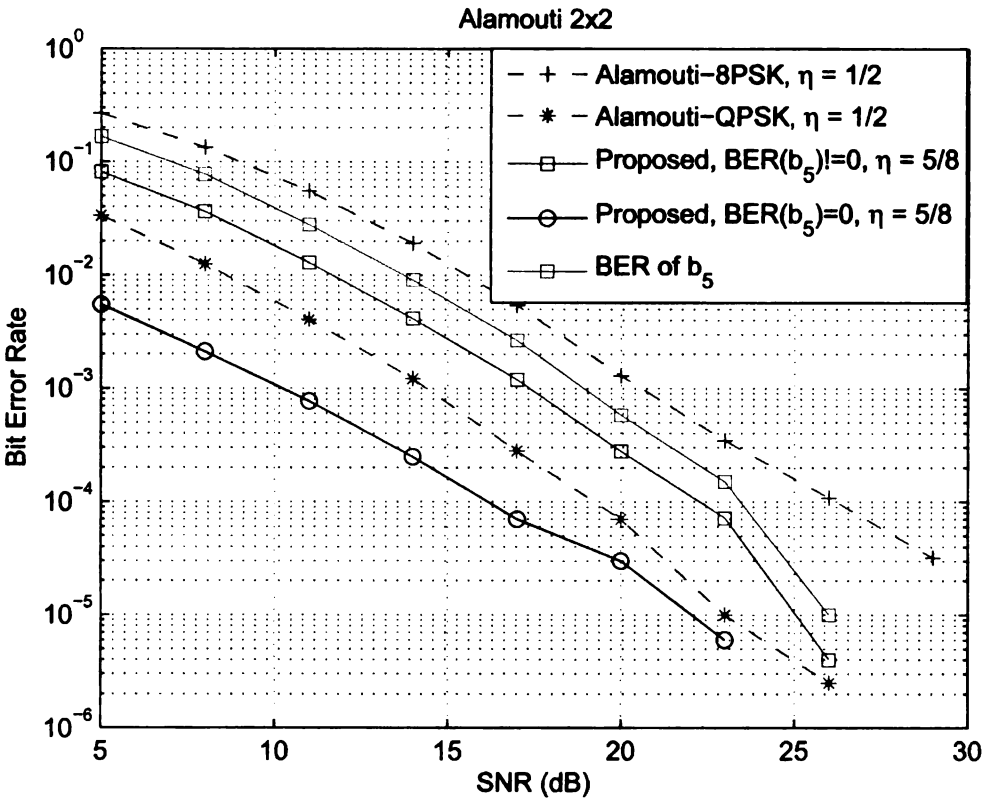

Figure 3.4. The BER performance comparison of the proposed scheme and the Alamouti code in Rayleigh flat fading, $n_T = 2$, $n_R = 2$.

In Figure 3.4, we consider the BER performance of the three schemes with $n_T = 2$ and $n_R = 2$ antennas. From the figure, it is shown that the additional antenna at the receiver significantly improves the performance proposed scheme with perfect recovery of b_5. At 10^{-3} the proposed scheme with perfect recovery outperforms the Alamouti-QPSK by 4dB. In Figure 3.5, performance of the proposed scheme with $n_T = 2$, $n_R = 1$ and $n_T = 2$, $n_R = 2$ antennas is shown to demonstrate the effectiveness of

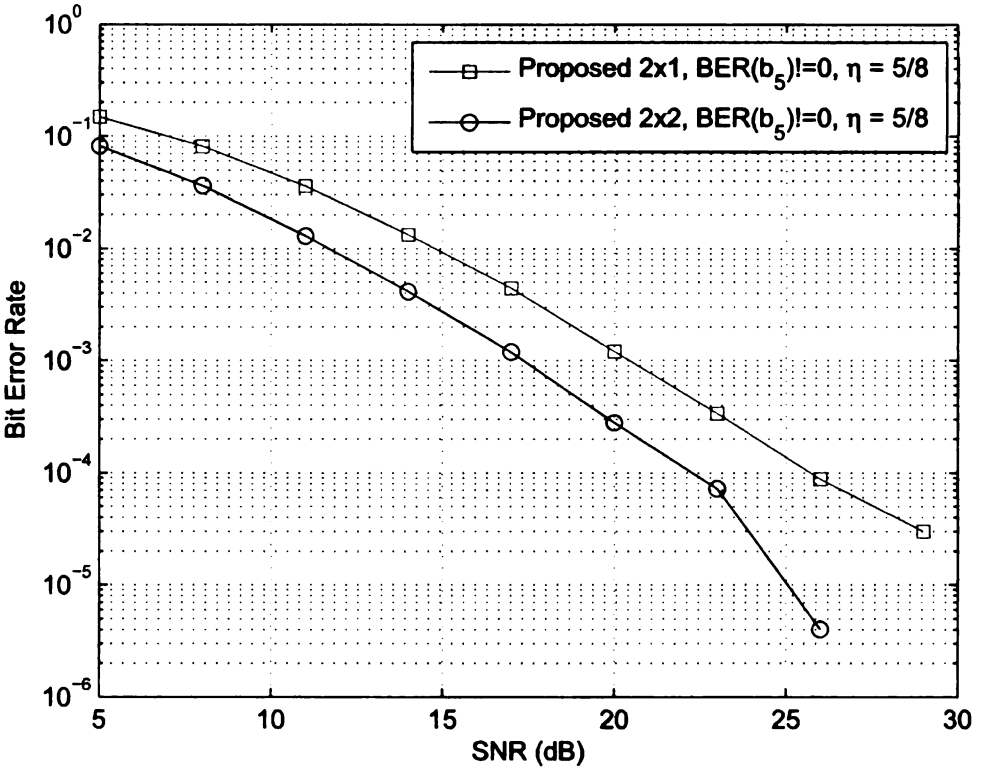

Figure 3.5. The BER performance comparison of the proposed scheme with $n_T = 2$, $n_R = 1$ and $n_T = 2$, $n_R = 2$ in Rayleigh flat fading

additional receive antenna.

In Table 3.1, a comparison of the three Alamouti codes is provided in terms of code efficiency, bit-rate and BER.

Table 3.1. Comparison of three Alamouti codes.

Schemes	η	R $(bit/s/Hz)$	BER
Alamouti-QPSK	0.5	2	low
Proposed-Alamouti	0.625	2.5	↓
Alamouti-8PSK	0.5	3	high

3.6 Summary

In summary, we investigated the efficiency of the Alamouti code from a bit level perspective, and introduced a spectrally efficient Alamouti scheme. The proposed scheme enhances the spectral efficiency by transmitting more information bits than redundancy bits per Alamouti block. Moreover, the proposed scheme preserves the high transmit diversity and simple receiver design of the Alamouti code. Finally, the proposed scheme has no specific constraints, therefore can be directly extended to any space-time block codes with more than two transmit antennas. Simulation results verify the effectiveness of the proposed scheme.

CHAPTER 4

Secure Space-Time Coded Collision-Free Frequency Hopping System

In this chapter, we propose an innovative spectrally efficient, jamming-resistant wireless scheme by exploiting the joint space-time and frequency diversity. First, we develop a collision-free frequency hopping (CFFH) system based on the orthogonal frequency division multiplexing (OFDM) framework. Second, we investigate the limitations of the recently proposed subcarrier assignment algorithm [66,67] and propose a new subcarrier assignment algorithm based on the secure permutation scheme [68,69]. The new secure subcarrier assignment algorithm is designed to ensure that: (i) Each user hops to a new set of subcarriers in a pseudo-random manner at the beginning of each hopping period; (ii) Different users always transmit on non-overlapping sets of subcarriers; (iii) Malicious users cannot predict or repeat the hopping pattern of the authorized users, and hence cannot launch follower jamming attacks. Third, we enhance the anti-jamming property of the CFFH scheme by incorporating space-time coding. Our analysis indicates that the enhanced system, referred to as STC-CFFH, is particularly powerful in eliminating channel interference and hostile jamming interference, especially random jamming. Finally, simulation examples are provided to illustrate the performance of the proposed schemes.

4.1 Introduction

Mainly due to the lack of a protective physical boundary, wireless communication is facing much more serious security challenges than its wirelined counterpart. In addition to the time and frequency dispersions caused by multipath propagation and Doppler shift, wireless signals are subjected to hostile jamming, interference and interception.

Existing anti-jamming and anti-interception systems, including both code-division multiple access (CDMA) systems and frequency hopping (FH) systems, rely heavily on rich time-frequency diversity over large, spread spectrum. Mainly limited by multiuser interference (caused by multipath propagation and asynchronization in CDMA systems and by collision effects in FH systems), the spectral efficiency of existing jamming resistant systems are very low due to inefficient use of the large bandwidth. While these systems work reasonably well for voice centric communications which only requires relatively narrow bandwidth, their low spectral efficiency can no longer provide sufficient capacity for today's high speed multimedia wireless services. This turns out to be the most significant obstacle in developing anti-jamming features for high speed wireless communication systems, for which spectrum is one of the most precious resources. On the other hand, along with the development of wireless communications, especially cognitive radios, hostile jamming and interception are no longer limited to military applications. Therefore, a major challenge in today's wireless communications is: how to design wireless systems which are highly efficient but at the same time have excellent jamming resistance properties?

As an effort to address this problem, we propose to integrate the *frequency hopping* technique into highly efficient communication systems through a network-centric perspective. Our approach is motivated by the following observations:

- Orthogonal frequency division multiple access (OFDMA) is an efficient multiple user scheme that divides the entire channel into mutually orthogonal parallel sub-channels. The OFDMA technique transforms a frequency-selective fading channel into parallel flat fading channels. As a result, OFDMA can effectively

eliminate the intersymbol interference (ISI) caused by the multipath environment and can achieve high spectral efficiency. For this reason, OFDMA has emerged as one of the prime multiple access schemes for broadband wireless networks [70, 71]. However, OFDMA does not posses any inherent security features and is fragile to hostile jamming.

- FH is originally designed for jamming resistant communications. In traditional FH systems, the transmitter hops in a pseudo-random manner among available frequencies according to a pre-specified algorithm, the receiver then operates in a strict synchronization with the transmitter and remains tuned to the same center frequency. Two major limitations with the conventional FH scheme are: (i) *Strong requirement on frequency acquisition.* In existing FH systems, exact frequency synchronization has to be kept between the transmitter and the receiver. The strict requirement on synchronization directly influences the complexity, design and performance of the system [72], and turns out to be a significant challenge in fast hopping system design. (ii) *Low spectral efficiency over large bandwidth.* Typically, FH systems require large bandwidth, which is proportional to the hopping rate and the number of all the available channels. In conventional frequency hopping multiple access (FHMA), each user hops independently based on its own pseudo-random number (PN) sequence, a collision occurs whenever there are two users over the same frequency band. Mainly limited by the collision effect, the spectral efficiency of conventional FH systems is very low.

- In literature, considerable efforts have been devoted to increasing the spectral efficiency of FH systems by applying high-dimensional modulation schemes [23–29]. More recently, a combination of the FH technique and the OFDMA system, called FH-OFDMA, has been proposed [34,35]. However, as the system is based on the conventional FH techniques, the spectral efficiency is seriously limited by the collision effect. Along with the ever increasing demand on inherently secure high data-rate wireless communications, new techniques that are more

efficient and reliable have to be developed.

We consider highly efficient anti-jamming system design using secure dynamic spectrum access control. First, we develop a collision-free frequency hopping (CFFH) system based on the orthogonal frequency division multiplexing (OFDM) framework. Second, we investigate the limitations of the recently proposed subcarrier assignment algorithm and propose a new subcarrier assignment algorithm based on the secure permutation scheme. The new secure subcarrier assignment is achieved through an advanced encryption standard (AES) [73] based secure permutation algorithm, which is designed to ensure that: (i) Each user hops to a new set of subcarriers in a pseudo-random manner at the beginning of each hopping period; (ii) Different users always transmit on non-overlapping sets of subcarriers; (iii) Malicious users cannot determine the hopping pattern of the authorized users, and hence cannot launch follower jamming attacks.[1] Moreover, using the fast Fourier transform (FFT) based OFDMA framework, CFFH has the same high spectral efficiency as that of OFDM, and at the same time can relax the complex frequency synchronization problem suffered by conventional FH systems. Third, we observe that CFFH is sensitive to random jamming and propose an enhanced CFFH scheme by incorporating space-time coding. Space-time block coding, which was first proposed by Alamouti [42] and refined by Tarokh *et al.* [43, 45], is a technique that exploits antenna array spatial diversity to provide gains against fading environments. When incorporated with OFDM, the space-time diversity in space-time coding is then converted to space-frequency diversity. The enhanced scheme, referred to as space-time coded collision-free frequency hopping (STC-CFFH), is found to be particularly powerful in eliminating both channel interference and hostile jamming interference, especially random jamming. In this chapter, we analyze the performance of the proposed STC-CFFH system through the following aspects: (i) Comparing the spectral efficiency of the proposed scheme with that of the conventional FH-OFDMA system; (ii) Investigating the performance of

[1]Follower jamming is the worst jamming scenario, in which the attacker is aware of the carrier frequency or the frequency hopping pattern of an authorized user, and can destroy the user's communication by launching jamming interference over the same frequency bands.

the STC-CFFH system under Rayleigh fading with hostile jamming. Our analysis indicates that the proposed system is both highly efficient and very robust under various jamming environments.

The rest of the chapter is organized as follows: In Section 4.2, the proposed CFFH system is discussed. In Section 4.3, the limitations of the recently proposed subcarrier assignment algorithm is investigated. In Section 4.4, the new secure subcarrier assignment algorithm based on the secure permutation scheme is introduced. The anti-jamming features of the new CFFH scheme is enhanced with space-time coding in Section 4.5. The spectral efficiency and jamming resistant properties of the proposed systems are analyzed in Section 4.6. Simulation examples are provided in Section 4.7. Finally, a summary is provided in Section 4.8.

4.2 The Collision-Free Frequency Hopping Scheme

The CFFH system is essentially an OFDMA system equipped with secure FH-based dynamic spectrum access control, where the hopping pattern is determined by the secure subcarrier assignment algorithm described in Section 4.4.

4.2.1 Signal Transmission

Consider a system with M users, utilizing an OFDM system with N_c subcarriers, $\{f_0, \cdots, f_{N_c-1}\}$. At each hopping period, each user is assigned a specific subset of the total available subcarriers. One hopping period may last one or more OFDM symbol periods. Assuming that at the nth symbol, user i has been assigned a set of sub-carriers $C_{n,i} = \{f_{n,i_0}, \cdots, f_{n,i_{N_u^i-1}}\}$, that is, user i will transmit and only transmit on these subcarriers. Here N_u^i is the total number of subcarrier assigned to user i. Note that for any n,

$$C_{n,i} \bigcap C_{n,j} = \emptyset, \quad \text{if} \quad i \neq j. \tag{4.1}$$

That is, users transmit on non-overlapping subcarriers. In other words, there is no collision between the users. Ideally, for full capacity of the OFDM system,

$$\bigcup_{i=0}^{M-1} C_{n,i} = \{f_0, \cdots, f_{N_c-1}\}. \tag{4.2}$$

For the ith user, if $N_u^i > 1$, then the ith users information symbols are first fed into a serial-to-parallel converter. Assuming that at the nth symbol period, user i transmits the information symbols $\{u_{n,0}^{(i)}, \cdots, u_{n,N_u^i-1}^{(i)}\}$ (which are generally QAM symbols) through the subcarrier set $C_{n,i} = \{f_{n,i_0}, \cdots, f_{n,i_{N_u^i-1}}\}$. User i's transmitted signal at the nth OFDM symbol can then be written as:

$$s_n^{(i)}(t) = \sum_{l=0}^{N_u^i-1} u_{n,l}^{(i)} e^{j2\pi f_{n,i_l} t}. \tag{4.3}$$

Note that each user does not transmit on subcarriers which are not assigned to them, by setting the symbols to zeros over these subcarriers. This process ensures collision-free transmission among the users.

4.2.2 Signal Detection

At the receiver, the received signal is a superposition of the signals transmitted from all users

$$r(t) = \sum_{i=0}^{M-1} r_n^{(i)}(t) + n(t), \tag{4.4}$$

where

$$r_n^{(i)}(t) = s_n^{(i)}(t) * h_i(t), \tag{4.5}$$

and $n(t)$ is the additive noise. In (4.5), $h_i(t)$ is the channel impulse response corresponding to user i. Note that in OFDM systems, guard intervals are inserted between symbols to eliminate intersymbol interference (ISI), so it is reasonable to study the signals in a symbol-by-symbol manner. Equations (4.3)-(4.5) represent an uplink system. The downlink system can be formulated in a similar manner.

As is well known, the OFDM transmitter and receiver is implemented through IFFT and FFT, respectively. Denote the $N_c \times 1$ symbol vector corresponding to user i's nth OFDM symbol as $\mathbf{u}_n^{(i)}$, we have

$$\mathbf{u}_n^{(i)}(l) = \begin{cases} 0, & l \notin \{i_0, \cdots, i_{N_u^i - 1}\} \\ u_{n,l}^{(i)}, & l \in \{i_0, \cdots, i_{N_u^i - 1}\}. \end{cases} \tag{4.6}$$

Let T_s denote the OFDM symbol period. The discrete form of the transmitted signal $s_n^{(i)}(t)$ (sampled at $\frac{lT_s}{N_c}$) is

$$\mathbf{s}_n^{(i)} = \mathbf{F}\mathbf{u}_n^{(i)}, \tag{4.7}$$

where $\mathbf{F}$ is the IFFT matrix defined as

$$\mathbf{F} = \frac{1}{\sqrt{N_c}} \begin{pmatrix} W_{N_c}^{00} & \cdots & W_{N_c}^{0(N_c-1)} \\ \vdots & \ddots & \vdots \\ W_{N_c}^{(N_c-1)0} & \cdots & W_{N_c}^{(N_c-1)(N_c-1)} \end{pmatrix},$$

with $W_{N_c}^{nk} = e^{j2\pi nk/N_c}$. As we only consider one OFDM symbol at a time, for notation simplification, here we omit the insertion of the guard interval (i.e. the cyclic prefix which is used to ensure that there is no ISI between two successive OFDM symbols).

Let $\mathbf{h}_i = [h_i(0), \cdots, h_i(N_c - 1)]$ be the discrete channel impulse response vector, and let

$$\mathbf{H}_i = \mathbf{F}\mathbf{h}_i \tag{4.8}$$

be the Fourier transform of $\mathbf{h}_i$. Then the received signal corresponding to user i is

$$\mathbf{r}_n^{(i)}(l) = \mathbf{u}_n^{(i)}(l)\mathbf{H}_i(l). \tag{4.9}$$

The overall received signal is then given by

$$\mathbf{r}_n(l) = \sum_{i=0}^{M-1} \mathbf{r}_n^{(i)}(l) + \mathbf{N}_n(l) \tag{4.10}$$

$$= \sum_{i=0}^{M-1} \mathbf{u}_n^{(i)}(l)\mathbf{H}_i(l) + \mathbf{N}_n(l). \tag{4.11}$$

where $\mathbf{N}_n(l)$ is the Fourier transform of the noise corresponding to the nth OFDM symbol.

Note that due to the collision-free subcarrier assignment, for each l, there is at most one non-zero item in the sum $\sum_{i=0}^{M-1} \mathbf{u}_n^{(i)}(l)\mathbf{H}_i(l)$. As a result, standard channel estimation algorithms and signal detection algorithms for OFDM systems can be implemented. In fact, each user can send pilot symbols on its subcarrier set to perform channel estimation. It should be pointed out that instead of estimating the whole frequency domain channel vector $\mathbf{H}_i$, for signal recovery, user i only need to estimate the entries corresponding to its subcarrier set, that is the values of $\mathbf{H}_i(l)$ for $l \in \{i_0, \cdots, i_{N_u^i-1}\}$. After channel estimation, user i's information symbols can be estimated from

$$\mathbf{u}_n^{(i)}(l) = \frac{\mathbf{r}_n^{(i)}(l)}{\mathbf{H}_i(l)}, \quad l \in \{i_0, \cdots, i_{N_u^i-1}\}. \tag{4.12}$$

It is also interesting to note that we can obtain adequate channel information from all the users simultaneously, which can be exploited for dynamic resource reallocation to achieve better BER performance and real-time jamming prevention.

4.3 The Subcarrier Assignment Algorithm and Its Limitations

In this section, we briefly discuss the recently proposed subcarrier assignment algorithm [66,67].

4.3.1 The Subcarrier Assignment Algorithm

The secure subcarrier assignment is described in the following steps.

Step 1 A pseudo-random binary sequence is generated using a 42-bit linear feedback shift register (LFSR), which is initialized by an initialization vector to ensure randomness. The LFSR has the following characteristic polynomial:

$$\begin{aligned} & x^{42}+x^{35}+x^{33}+x^{31}+x^{27}+x^{26}+x^{25} \\ & +x^{22}+x^{21}+x^{19}+x^{18}+x^{17}+x^{16} \\ & +x^{10}+x^{7}+x^{6}+x^{5}+x^{3}+x^{2}+x+1. \end{aligned} \tag{4.13}$$

Assuming that the total number of subcarriers is $K = 128$, the sequence output is grouped into blocks of length 128 bits. The kth block is denoted as X_k and is used to generate the subcarrier index for the kth OFDM symbol.

Step 2 The AES algorithm is used to encrypt the plaintext X_k with a specify 128-bit key. The resulting 128-bit ciphertext is denoted as $\{pc_0, pc_1, \cdots, pc_{127}\}$.

Step 3 Each subcarrier position is represented by $log_2(128) = 7$ bits. A 1×134 vector is formed by cyclic padding $[pc_0, pc_1, \cdots, pc_{127}, pc_0, pc_1, \cdots, pc_5]$. The vector is then divided into 128 7-bit groups:

$$[pc_0, pc_1, \cdots, pc_6], [pc_1, pc_2, \cdots, pc_7] \cdots, [pc_{127}, pc_0, \cdots, pc_5].$$

Step 4 For $i = 0, 1, \cdots, 127$, denote $P(i)$ as the decimal number corresponding to the ith 7-bit vector, such that

$$\begin{aligned} P(i) &= pc_i \cdot 2^6 + pc_{(i+1 \ mod \ 128)} \cdot 2^5 \\ &+ pc_{(i+2 \ mod \ 128)} \cdot 2^4 + pc_{(i+3 \ mod \ 128)} \cdot 2^3 \\ &+ pc_{(i+4 \ mod \ 128)} \cdot 2^2 + pc_{(i+5 \ mod \ 128)} \cdot 2^1 \\ &+ pc_{(i+6 \ mod \ 128)} \cdot 2^0. \end{aligned}$$

Note that vector $P = [P(0) \ P(1) \cdots \ P(127)]$ does not necessarily contain all the

numbers from 0 to 127 and may contain repeated numbers. To replace the repeated numbers with the missing numbers:

a) Stack all of the M missing numbers in matrix P from $0, 1, \cdots, 127$ into a vector A such that $A = [A(0), A(1), \cdots, A(M-1)]$.

b) Find the index of each repeated number in P and stack them to formulate a vector B, such that $B = [B(0), B(1), \cdots, B(M-1)]$. Note, the length of A is equal to B.

c) For $j = 0, 1, \cdots, M-1$, substitute A(j) for the B(j)'s entry in P. The updated vector P contains all the numbers from 0 to 127 and each number occurs only once.

Finally, assign the subcarriers with indexes $\{P(0), P(1), \cdots, P(N_1 - 1)\}$ to user 0, assign the subcarriers with indexes $\{P(N_1), \cdots, P(N_1 + N_2 - 1)\}$ to user 1 and so on. Recall that, for user $i = 0, 1 \cdots, U-1$, the total number of subcarriers assigned to the ith user is N_i.

4.3.2 Limitations of The Subcarrier Assignment Algorithm

Although the concept of the recently proposed subcarrier assignment algorithm is innovative, the recently proposed scheme has numerous limitations. The primary drawback of the recently proposed scheme materializes in Step 3 of the secure subcarrier assignment algorithm, where additional bits are appended to the ciphertext bit vector via cyclic padding. The cyclic padding operation introduces bit redundancy and eliminates bit independence and the strong security properties of the ciphertext bit vector. Furthermore, in Step 3 the overlapping partition of the ciphertext bit vector creates strong correlation between partitions.

Another limitation of the recently proposed subcarrier assignment scheme is the replacement algorithm in Step 4. Simply replacing the repeated numbers with the missing numbers does not guarantee a secure subcarrier assignment. For example,

the strong correlation between the partitions in Step 3 can result in many repeated numbers, leading to a sequential non-random subcarrier allocation.

In all, the secure subcarrier assignment algorithm recently proposed is clever, but lacks strong security properties due to the cyclic padding and overlapping partition of the ciphertext bit vector. Furthermore, the replacement algorithm in Step 4 can lead to non-random subcarrier allocation.

In the following section, we introduce a new subcarrier assignment scheme based on the secure permutation algorithm. The new subcarrier assignment scheme enhances the security features of the previous subcarrier assignment algorithm and possess strong cryptographic properties.

4.4 Secure Subcarrier Assignment Based on Secure Permutation

In this section, we present the proposed secure subcarrier assignment scheme [68,69], for which the major component is an AES based secure permutation algorithm. AES is chosen because of its simplicity of design, variable block and key sizes, feasibility in both hardware and software, and resistance against all known attacks [74]. Note that, the secure subcarrier assignment is not limited to any particular cryptographic algorithm, but is highly recommended that only thoroughly analyzed cryptographic algorithms be applied.

The AES-based permutation algorithm is used to securely select the frequency hopping pattern for each user so that: (i) Different users always transmit on non-overlapping sets of subcarriers; (ii) Malicious users cannot determine the frequency hopping pattern and therefore cannot launch follower jamming attacks.

We assume there is a total of N_c available subcarriers and there are M users in the system. For $i = 0, 1, \cdots, M-1$, the number of subcarriers assigned to user i is denoted as N_u^i. We assume that different users transmit over non-overlapping set of subcarriers and we have $\sum_{i=0}^{M-1} N_u^i = N_c$. The secure subcarrier algorithm is described

in the following subsections.

4.4.1 Secure Permutation Index Generation

A pseudo-random binary sequence is generated using a 32-bit linear feedback shift register (LFSR), which is initialized by a secret sequence chosen by the base station. The LFSR has the following characteristic polynomial:

$$\begin{aligned} & x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} \\ & + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1. \end{aligned} \tag{4.14}$$

Use the pseudo-random binary sequence generated by the LFSR as the plaintext. Encrypt the plaintext using the AES algorithm and a secure key. The key size can be 128, 192, or 256. The encrypted plaintext is known as the ciphertext. Assume N_c is a power of 2, pick an integer $L \in [\frac{N_c}{2}, N_c]$. Note that a total of $N_b = log_2 N_c$ bits are required to represent each subcarrier, let $q = Llog_2 N_c$. Take q bits from the ciphertext and place them in a q-bit vector $\mathbf{e} = [e_1, e_2, \cdots, e_q]$.

Partition the ciphertext sequence $\mathbf{e}$ into L groups, such that each group contains N_b bits. For $k = 1, 2, \cdots, L$, the partition of the ciphertext is as follows

$$\mathbf{p_k} = [e_{(k-1)*N_b+1}, e_{(k-1)*N_b+2}, \cdots, e_{(k-1)*N_b+N_b}], \tag{4.15}$$

where $\mathbf{p_k}$ corresponds to the kth N_b-bit vector.

For $k = 1, 2, \cdots, L$, denote P_k as the decimal number corresponding to $\mathbf{p_k}$, such that

$$\begin{aligned} P_k &= e_{(k-1)*N_b+1} \cdot 2^{N_b-1} + e_{(k-1)*N_b+2} \cdot 2^{N_b-2} \\ &+ \cdots + e_{(k-1)*N_b+N_b-1} \cdot 2^1 \\ &+ e_{(k-1)*N_b+N_b} \cdot 2^0. \end{aligned} \tag{4.16}$$

Finally, we denote $P = [P_1, P_2, \cdots, P_L]$ as the permutation index vector. Here

the largest number in P is $N_c - 1$. In the following subsection, we will discuss the secure permutation algorithm.

4.4.2 Secure Permutation Algorithm and Subcarrier Assignment

For $k = 0, 1, 2, \cdots, L$, denote $I_k = [I_k(0), I_k(1), \cdots, I_k(N_c-1)]$ as the index vector at the kth step. The secure permutation scheme of the index vector is achieved through the following steps:

0. Initially, the index vector is $I_0 = [I_0(0), I_0(1), \cdots, I_0(N_c - 1)]$ and the permutation index is $P = [P_1, P_2, \cdots, P_L]$. We start with $I_0 = [0, 1, \cdots, N_c - 1]$.

1. For $k = 1$, switch $I_0(0)$ and $I_0(P_1)$ in index vector I_0 to obtain I_1. In other words, $I_1 = [I_1(0), I_1(1), \cdots, I_1(N_c-1)]$, where $I_1(0) = I_0(P_1)$, $I_1(P_1) = I_0(0)$, and $I_1(m) = I_0(m)$ for $m \neq 0, P_1$.

2. Repeat the previous step for $k = 2, 3, \cdots, L$. In general, if we already have $I_{k-1} = [I_{k-1}(0), I_{k-1}(1), \cdots, I_{k-1}(N_c - 1)]$, then we can obtain $I_k = [I_k(0), I_k(1), \cdots, I_k(N_c - 1)]$ through the permutation defined as $I_k(k-1) = I_{k-1}(P_k)$, $I_k(P_k) = I_{k-1}(k-1)$, and $I_k(m) = I_{k-1}(m)$ for $m \neq k-1, P_k$.

3. After L steps, we obtain the subcarrier frequency vector as $F_L = [f_{I_L(0)}, f_{I_L(1)}, \cdots, f_{I_L(N_c-1)}]$.

4. The subcarrier frequency vector F_L is used to assign subcarriers to the users. Recall, for user $i = 0, 1 \cdots, M-1$, the total number of subcarriers assigned to the ith user is N_u^i. We assign subcarriers $\{f_{I_L(0)}, f_{I_L(1)}, \cdots, f_{I_L(N_u^0-1)}\}$ to user 0; Assign $\{f_{I_L(N_u^0)}, f_{I_L(N_u^0+1)}, \cdots, f_{I_L(N_u^0+N_u^1-1)}\}$ to user 1, and so on.

Proposition 1 *The proposed secure subcarrier assignment scheme ensures non-overlapping transmission among all the users in the system.*

Proof: In fact, after L steps, we obtain the subcarrier frequency vector as $F_L = [f_{I_L(0)}, f_{I_L(1)}, \cdots, f_{I_L(N_c-1)}]$. We can rewrite the subcarrier frequency vector F_L as $F_L = [F_L(0), F_L(1), \cdots, F_L(N_c-1)]$ by defining $F_L(j) = f_{I_L(j)}$ for $j = 0, 1, \cdots, N_c - 1$, where N_c is the total number of subcarriers. Assume that we have M users in the system, and for $i = 0, 1 \cdots, M-1$, the total number of subcarriers assigned to the ith user is N_u^i. The subcarrier assignment process described in step 4 of the secure subcarrier algorithm above is equivalent to assigning subcarriers $\{F_L(0), F_L(1), \cdots, F_L(N_u^0 - 1)\}$ to user 0, and subcarriers $\{F_L(N_u^0), F_L(N_u^0+1), \cdots, F_L(N_u^0+N_u^1-1)\}$ to user 1, and so on.

Because each frequency index appears in F_L once and only once, the proposed algorithm ensures that: (i) All the users are transmitting on non-overlapping sets of subcarriers; (ii) No subcarrier is left idle. That is, all the subcarriers are active. □

The secure permutation algorithm is performed at the base station. The base station sends encrypted channel assignment information to each user periodically through the control channels. Details of how the base station transmits the channel assignments to each user is provided in Section 4.4.3.

The proposed scheme addresses the problem of securely allocating subcarriers in the presence of hostile jamming. This algorithm can be combined with existing resource allocation techniques. First, the number of subcarriers assigned to each user can be determined through power and bandwidth optimization, see [34, 75], for example. Then, we use the secure subcarrier assignment algorithm to select the group of subcarriers for each user at each hopping period. In the following, we illustrate the secure subcarrier assignment algorithm though a simple example.

Example: Assume the total number of available subcarriers is N_c=8, to be equally divided among M=2 users; the permutation index vector $P = [4, 7, 4, 0]$, and the initial index vector $I_0 = [0, 1, 2, 3, 4, 5, 6, 7]$, as shown in Fig. 4.1. Note that, the initial index vector I_0 can contain any random permutation of the sequence $\{0, 1, \cdots, N_c - 1\}$, and $L \in [\frac{N_c}{2}, N_c]$. In this example, we choose $L = \frac{N_c}{2}$.

At Step 1, $k = 1$, and $P_k = 4$, thus we switch $I_0(P_k)$ and $I_0(k-1)$ of the index vector I_0. After the switching, we obtain a new index vector $I_1 = [4, 1, 2, 3, 0, 5, 6, 7]$.

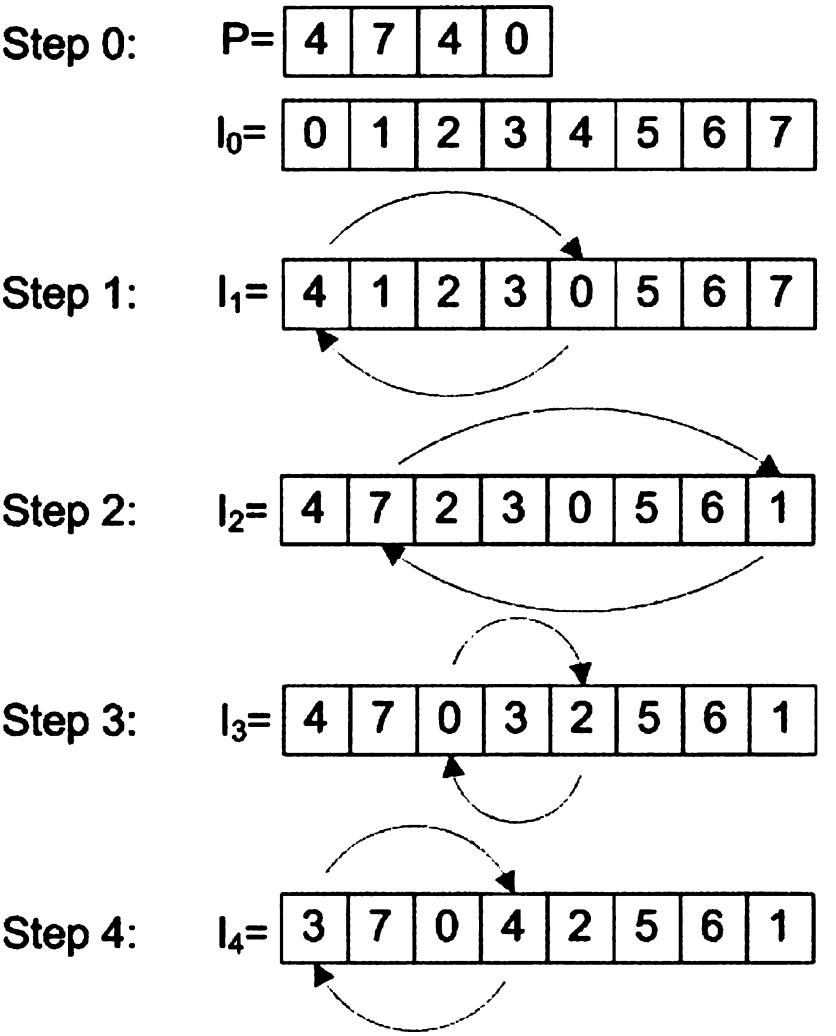

Figure 4.1. Example of the Secure Permutation Algorithm for N_c=8 subcarriers and M=2 users.

At Step 2, $k = 2$, and $P_k = 7$, thus we switch $I_1(P_k)$ and $I_1(k-1)$ of the index vector I_1. We obtain the new index vector $I_2 = [4, 7, 2, 3, 0, 5, 6, 1]$. Below are the remaining index vectors for $k = 3, 4$:

$$I_3 = [4, 7, 0, 3, 2, 5, 6, 1], \; I_4 = [3, 7, 0, 4, 2, 5, 6, 1].$$

The subcarrier frequency vector is $F_4 = [f_{I_4(0)}, f_{I_4(1)}, \cdots, f_{I_4(N_c-1)}]$. Frequencies $\{f_3, f_7, f_0, f_4\}$ are assigned to user 0 and frequencies $\{f_2, f_5, f_6, f_1\}$ are assigned to user 1.

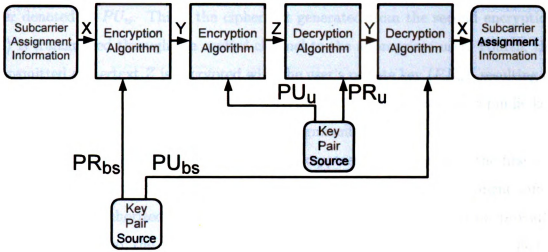

Figure 4.2. Public/Private Key Cryptosystem

4.4.3 Secure Subcarrier Assignment Distribution

In this subsection, we will discuss how the subcarriers assignments are distributed to the users. Recall that the secure permutation algorithm is performed at the based station and the subcarrier assignment information is encrypted then transmitted through a control channel to the users.

The channel assignment information is securely transmitted to each user through a public/private key cryptosystem. The public/private key cryptosystem is known as an asymmetric algorithm, where one key is used for encryption and a different, but related key is used for decryption. Typically, the public key (stored at a public register) is used to encrypt messages, and the private key is used to decrypt the message. The public and private key pair are generated by a cryptographic algorithm developed by Ron Rivest, Adi Shamir, and Len Adleman, which is known as the RSA algorithm [76].

Figure 4.2 is a depiction of the secure public/private key cryptosystem algorithm for the subcarrier assignment distribution. First, the subcarrier assignment information (X) is encrypted with the private key of the base station denoted as PR_{bs}.

Second, the following ciphertext (Y) is encrypted again using the public key of the user denoted as PU_u. Third, the ciphertext generated from the second encryption (Z) is transmitted through the control channel to the appropriate user. Fourth, the transmitted ciphertext Z is decrypted with the user's private key (PR_u), resulting in ciphertext Y. Fifth, the ciphertext Y is decrypted with the base station's public key (PU_{bs}), resulting in the original subcarrier assignment information.

Note that in the secure public/private key cryptosystem algorithm, the first encryption process provides a digital signature (ensures subcarrier assignment information is from authorized base station) and the second encryption process provides confidentiality. Also, the transmitted ciphertext Z can only be decrypted by the intended user who has the matching private key. Finally, the encryption algorithm in the public/private cryptosystem is not limited to any particular encryption algorithm, but is highly recommended that only thoroughly analyzed cryptographic algorithms be applied.

4.5 Secure Space-Time Coded Collision-Free Frequency Hopping

In this section, we enhance the anti-jamming features of the CFFH scheme by using space-time coding. Here we present the transmitter and receiver design of the proposed STC-CFFH system from the downlink perspective. The uplink can be designed in a similar manner.

4.5.1 Transmitter Design

We assume that during each hopping period, the number of subcarriers assigned to each user in the CFFH system is fixed. Recall that one hopping period may contain one or more OFDM symbol periods. In the following we illustrate the transmitter design over one OFDM symbol.

Assume the transmitter at the base station has n_T antennas and there are M

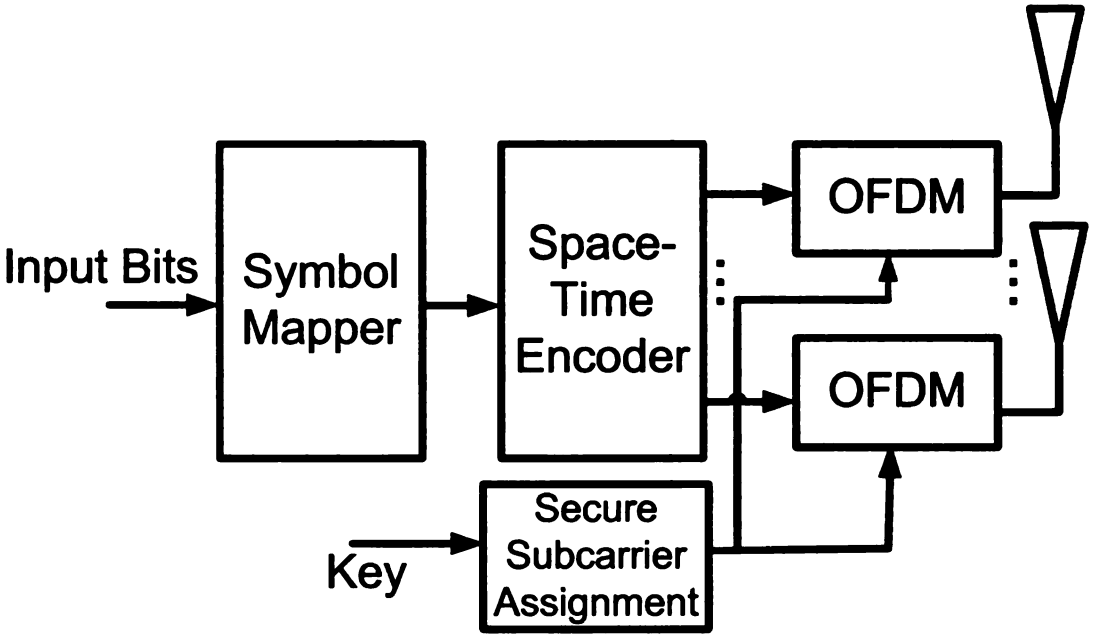

Figure 4.3. Block diagram of the STC-CFFH transmitter.

users in the system. Over each OFDM symbol period, the ith user is assigned N_u^i subcarriers, which do not need to be contiguous. The transmitter structure at the base station is illustrated in Fig.4.3.

Initially, the input bit stream corresponding to each user is mapped to symbols based on a selected constellation. The constellation could be different for different users based on the channel condition and user data-rate [77, 78]. Assume the base station uses a $n_T \times n_T$ space-time block code (STBC). Note that non-square STBC codes [43, 45] exists, but for notation simplicity, here we adopt the $n_T \times n_T$ square code. For each user, divide the N_u^i subcarriers into $G_i = \frac{N_u^i}{n_T}$ groups, where each group contains n_T subcarriers, which is of the same length as that of the STBC. For simplicity, we assume G_i is an integer, that is, each user transmits G_i space-time blocks in one OFDM symbol period. (Otherwise, if G_i is not an integer, the symbols can be broken down and transmitted over two successive OFDM symbol periods.)

For each $n \in \{1, 2, \cdots, G_i\}$, the base station takes a block of n_T complex symbols and maps them to a $n_T \times n_T$ STBC code matrix $X_i(n)$. In other words, for $n =$

$1, 2, \cdots, G_i$, $m = 1, 2, \cdots, n_T$, the mth row of the code matrix $X_i(n)$ is merged with the corresponding symbols from other users and transmitted through the mth transmit antenna, and all symbols within each column ($m = 1, 2, \cdots, n_T$) of the code matrix $X_i(n)$ is transmitted over the same subcarrier. The code matrix $X_i(n)$ is given by

$$X_i(n) = \begin{array}{c} \text{Subcarrier} \rightarrow \\ \begin{bmatrix} x_{i,1}^{1}(n) & \cdots & x_{i,n_T}^{1}(n) \\ \vdots & \ddots & \vdots \\ x_{i,1}^{n_T}(n) & \cdots & x_{i,n_T}^{n_T}(n) \end{bmatrix} \end{array} \begin{array}{l} \\ \\ \downarrow \text{Antenna} \end{array}, \tag{4.17}$$

where $x_{i,t}^{m}(n)$ is the tth symbol of the nth block for user i in transmit antenna m.

Note that, since each user is assigned multiple frequency bands, we are transmitting symbols over multiple subcarriers instead of multiple time slots. Thus the time diversity of the space-time coder is converted to frequency diversity and this structure is referred to as space-frequency coding [79].

STC-CFFH Transmitter Design Example: We provide an example to illustrate the transmitter structure of STC-CFFH, in which the subcarrier assignment is based on the example in Section 4.4. Assume an Alamouti space-time coded system with n_T=2 and we have M=2 users. A total of N_c=8 subcarriers are available and each user is assigned $N_u^0 = N_u^1 = 4$ subcarriers. For this example, each user transmit $G_i = \frac{N_u^i}{n_T} = 2$ code matrices in one OFDM symbol period. Consider the nth block for the ith user, where $n = 1, 2$ in this case. The space-time encoder takes n_T=2 complex symbols $x_{i,1}(n)$, $x_{i,2}(n)$ in each encoding operation and maps them to the code matrix $X_i(n)$. In this example, the first and second column of $X_i(n)$ will be sent from the first and second transmit antenna, respectively.

In this example, we can drop the superscript m in $x_{i,t}^{m}(n)$ by representing $X_i(n)$ with the Alamouti space-time code block structure [42]. Then the code matrices

Table 4.1. STC-CFFH Transmitter Example.

freq. / *Tx*	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
1	$x_{0,1}(1)$	$x_{1,1}(1)$	$-x^*_{1,2}(1)$	$-x^*_{0,2}(1)$	$x_{0,1}(2)$	$x_{1,1}(2)$	$-x^*_{1,2}(2)$	$-x^*_{0,2}(2)$
2	$x_{0,2}(1)$	$x_{1,2}(1)$	$x^*_{1,1}(1)$	$x^*_{0,1}(1)$	$x_{0,2}(2)$	$x_{1,2}(2)$	$x^*_{1,1}(2)$	$x^*_{0,1}(2)$

$X_i(n)$ are given by

$$X_i(n) = \begin{array}{c} \text{Subcarrier} \rightarrow \\ \begin{bmatrix} x_{i,1}(n) & -x^*_{i,2}(n) \\ x_{i,2}(n) & x^*_{i,1}(n) \end{bmatrix} \end{array} \downarrow \text{Antenna}, \tag{4.18}$$

where * is the complex conjugate operator. Specifically, User 0's two code matrices are represented as

$$X_0(1) = \begin{bmatrix} x_{0,1}(1) & -x^*_{0,2}(1) \\ x_{0,2}(1) & x^*_{0,1}(1) \end{bmatrix}, \; X_0(2) = \begin{bmatrix} x_{0,1}(2) & -x^*_{0,2}(2) \\ x_{0,2}(2) & x^*_{0,1}(2) \end{bmatrix}, \tag{4.19}$$

and user 1's two code matrices are represented as

$$X_1(1) = \begin{bmatrix} x_{1,1}(1) & -x^*_{1,2}(1) \\ x_{1,2}(1) & x^*_{1,1}(1) \end{bmatrix}, \; X_1(2) = \begin{bmatrix} x_{1,1}(2) & -x^*_{1,2}(2) \\ x_{1,2}(2) & x^*_{1,1}(2) \end{bmatrix}. \tag{4.20}$$

Recall that the secure subcarrier assignment from the example in Section 4.4. User 0 is assigned to subcarriers $\{f_0, f_3, f_4, f_7\}$. User 1 is assigned to subcarriers $\{f_1, f_2, f_5, f_6\}$. A depiction of the subcarrier allocation for this example is provided in Table 4.1.

For user 0, $[x_{0,1}(1), -x^*_{0,2}(1), x_{0,1}(2), -x^*_{0,2}(2)]$ is transmitted through antenna 1 over subcarriers $\{f_0, f_3, f_4, f_7\}$, respectively; $[x_{0,2}(1), x^*_{0,1}(1), x_{0,2}(2), x^*_{0,1}(2)]$ is transmitted through antenna 2 over the same group of subcarriers. User 1's subcarrier allocation can be achieved in the same manner as User 0.

4.5.2 Receiver Design

Assuming user i has n_R antennas. Recall that the secure permutation index generation is performed at the base station and the base station sends encrypted channel assignment information to each user periodically through the control channels. After cyclic prefix removal and FFT, the receiver will only extract the symbols on the subcarriers assigned to itself and discard the symbols on the rest of subcarriers. The extracted symbols are reorganized into a $n_R \times n_T$ matrix $R_i(n)$, which corresponds to the transmitted code matrix $X_i(n)$. Thus the space-time decoding can be performed for each symbol matrix $R_i(n)$ individually and the estimated symbols are mapped back into bits by the symbol de-mapper.

Here we consider the space-time decoding algorithm for a single symbol matrix $R_i(n)$ given as

$$R_i(n) = \begin{array}{c} \text{Subcarrier} \rightarrow \\ \begin{bmatrix} r_{i,1}^{1}(n) & \cdots & r_{i,n_T}^{1}(n) \\ \vdots & \ddots & \vdots \\ r_{i,1}^{n_R}(n) & \cdots & r_{i,n_T}^{n_R}(n) \end{bmatrix} \downarrow \text{Antenna} \end{array}, \tag{4.21}$$

where $r_{i,t}^{j}(n)$ is the tth symbol of group n for user i from jth receive antenna. Each symbol in the matrix $R_i(n)$ can be obtained as

$$r_{i,t}^{j}(n) = \sum_{m=1}^{n_T} H_{i,t}^{j,m}(n) x_{i,t}^{m}(n) + n_{i,t}^{j}(n), \tag{4.22}$$

where $H_{i,t}^{j,m}(n)$ is the channel frequency response for the path from the mth transmit antenna to the jth receive antenna corresponding to tth symbol of group n for user i. It is assumed that the channels between the different antennas are uncorrelated. Here, $n_{i,t}^{j}(n)$ is the OFDM demodulated version of the additive white Gaussian noise (AWGN) at the jth receive antenna for tth symbol of the nth group for ith user. The noise is assumed to be zero-mean with variance σ_N^2.

Table 4.2. STC-CFFH Receiver Example.

Rx \ freq.	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
1	$r^1_{0,1}(1)$	$r^1_{1,1}(1)$	$r^1_{1,2}(1)$	$r^1_{0,2}(1)$	$r^1_{0,1}(2)$	$r^1_{1,1}(2)$	$r^1_{1,2}(2)$	$r^1_{0,2}(2)$
2	$r^2_{0,1}(1)$	$r^2_{1,1}(1)$	$r^2_{1,2}(1)$	$r^2_{0,2}(1)$	$r^2_{0,1}(2)$	$r^2_{1,1}(2)$	$r^2_{1,2}(2)$	$r^2_{0,2}(2)$

The space-time ML decoder is obtained as

$$\hat{X}_i(n) = \arg \min_{X_i(n)} \sum_{j=1}^{n_R} \sum_{t=1}^{n_T} \left| r^j_{i,t}(n) - \sum_{m=1}^{n_T} H^{j,m}_{i,t}(n) x^m_{i,t}(n) \right|^2, \tag{4.23}$$

where $\hat{X}_i(n)$ denotes the recovered symbols of group n for user i. Note that the minimization is performed over all possible space-time codewords.

STC-CFFH Receiver Design Example: We continue with the transmitter example in the previous subsection. Assuming each user is equipped with $n_R = 2$ receive antenna, the received symbols are illustrated in Table 4.2. Arranging the extracted symbols according to the users and the groups, the extracted symbol matrix $R_i(n)$ is given as

$$R_i(n) = \begin{matrix} \text{Subcarrier} \rightarrow \\ \begin{bmatrix} r^1_{i,1}(n) & r^1_{i,2}(n) \\ r^2_{i,1}(n) & r^2_{i,2}(n) \end{bmatrix} \end{matrix} \begin{matrix} \\ \downarrow \text{Antenna.} \end{matrix} \tag{4.24}$$

Specifically, User 0's two extracted symbol matrices can be represented as

$$R_0(1) = \begin{bmatrix} r^1_{0,1}(1) & r^1_{0,2}(1) \\ r^2_{0,1}(1) & r^2_{0,2}(1) \end{bmatrix}, \; R_0(2) = \begin{bmatrix} r^1_{0,1}(2) & r^1_{0,2}(2) \\ r^2_{0,1}(2) & r^2_{0,2}(2) \end{bmatrix}, \tag{4.25}$$

and User 1's two extracted symbol matrices can be represented as

$$R_1(1) = \begin{bmatrix} r^1_{1,1}(1) & r^1_{1,2}(1) \\ r^2_{1,1}(1) & r^2_{1,2}(1) \end{bmatrix}, \; R_1(2) = \begin{bmatrix} r^1_{1,1}(2) & r^1_{1,2}(2) \\ r^2_{1,1}(2) & r^2_{1,2}(2) \end{bmatrix}. \tag{4.26}$$

Then, the ML space-time decoding is performed for each $R_i(n)$.

Remark: In the discussion above, we focused on STC-CFFH system for the downlink case, where the information is transmitted from base station to the multiple users. In the uplink case, the secure permutation index is encrypted and transmitted from base station to each user, prior to the user transmission. Then during the transmission, each user only transmits on the subcarriers assigned to them. The receiver at the base station separates each user's transmitted data. In order for the user to use space-time coding, each user needs to have at least two antennas.

4.6 Performance Analysis of Space-Time Coded Collision-Free Frequency Hopping System

In this section, we investigate the spectral efficiency and the performance of the proposed schemes under jamming interference over frequency selective fading environments. First, the system performance in jamming-free case is analyzed. Second, the system performance under hostile jamming is investigated. Finally, the spectral efficiency comparison of the proposed schemes and the conventional FH-OFDMA system is performed.

4.6.1 System Performance in Jamming-Free Case

First, we analyze the pairwise error probability of the STC-CFFH system under Rayleigh fading. Assume ideal channel state information (CSI) and perfect synchronization between transmitter and receiver. Recall that the ML space-time decoding rule for the extracted symbol matrix $R_i(n)$ is given by (4.23).

Denote the pairwise error probability of transmitting $X_i(n)$ and deciding in favor of another codeword $\hat{X}_i(n)$, given the realizations of the fading channel $H_{i,t}^{j,m}(n)$, as $P(X_i(n), \hat{X}_i(n)|H_{i,t}^{j,m}(n))$. This pairwise error probability is bounded by [80] (see page 255)

$$P(X_i(n), \hat{X}_i(n)|H_{i,t}^{j,m}(n)) \leq \exp\left(-d^2(X_i(n), \hat{X}_i(n))\frac{E_s}{4N_0}\right), \tag{4.27}$$

where E_s is the average symbol energy, N_0 is the noise power spectral density, and $d^2(X_i(n), \hat{X}_i(n))$ is a modified Euclidean distance between the two space-time codewords $X_i(n)$ and $\hat{X}_i(n)$, and is given by

$$d^2(X_i(n), \hat{X}_i(n)) = \sum_{t=1}^{n_T}\sum_{j=1}^{n_R}\left|\sum_{m=1}^{n_T} H_{i,t}^{j,m}(n)(\hat{x}_{i,t}^m(n) - x_{i,t}^m(n))\right|^2, \tag{4.28}$$

where $\hat{x}_{i,t}^m(n)$ is the estimated version of $x_{i,t}^m(n)$.

Let us define a codeword difference matrix $C(X_i(n), \hat{X}_i(n)) = X_i(n) - \hat{X}_i(n)$ and define a codeword distance matrix $B(X_i(n), \hat{X}_i(n))$ with rank r_B as

$$B(X_i(n), \hat{X}_i(n)) = C(X_i(n), \hat{X}_i(n)) \cdot C(X_i(n), \hat{X}_i(n))^H, \tag{4.29}$$

where H denotes the Hermitian operator. Since the matrix $B(X_i(n), \hat{X}_i(n))$ is a nonnegative definite Hermitian matrix, the eigenvalues of $B(X_i(n), \hat{X}_i(n))$ are nonnegative real numbers, denoted as $\lambda_1, \lambda_2, \cdots, \lambda_{r_B}$.

After averaging with respect to the Rayleigh fading coefficients, the upper bound of pairwise error probability can be obtained as [39]

$$\begin{aligned} P(X_i(n), \hat{X}_i(n)|H_{i,t}^{j,m}(n)) &\leq \left(\prod_{j=1}^{r_B}\left(1 + \lambda_j\frac{E_s}{4N_0}\right)\right)^{-n_R} \\ &\leq \left(\prod_{j=1}^{r_B}\lambda_j\right)^{-n_R}\left(\frac{E_s}{4N_0}\right)^{-r_B n_R}. \end{aligned} \tag{4.30}$$

In the case of low signal-to-noise ratio (SNR), the upper bound in (4.30) can be

expressed as [80],

$$P(X_i(n), \hat{X}_i(n)|H_{i,t}^{j,m}(n)) \leq \left(1 + \frac{E_s}{4N_0} \sum_{j=1}^{r_B} \lambda_j\right)^{-n_R}. \quad (4.31)$$

4.6.2 System Performance Under Hostile Jamming

In this subsection, we will first introduce the jamming models, and then analyze the system performance under both full-band jamming and partial-band jamming.

Jamming Models

Jamming interference in the OFDM framework can severely degrade the system performance [81]. Each extracted symbol in the matrix $R_i(n)$ that experiences jamming interference is given as

$$r_{i,t}^{j}(n) = \sum_{m=1}^{n_T} H_{i,t}^{j,m}(n) x_{i,t}^{m}(n) + n_{i,t}^{j}(n) + J_{i,t}^{j}(n), \quad (4.32)$$

where $J_{i,t}^{j}(n)$ is the jamming interference at the jth receive antenna for tth symbol of the nth group for ith user. Assume all jamming interference $J_{i,t}^{j}(n)$ has the same power spectral density N_J, then the signal-to-jamming plus noise ratio (SJNR) at the receiver is represented by SJNR $= \frac{E_s}{N_0+N_J}$. When the noise is dominated by jamming, the SJNR can be represented as the signal-to-jamming ratio (SJR) where SJR $= \frac{E_s}{N_J}$.

Partial-band jamming [18–20] is generally characterized by the additive Gaussian noise interference with flat power spectral density $\frac{N_J}{\rho}$ over a fraction ρ of the total bandwidth and negligible interference over the remaining fraction $(1-\rho)$ of the band. ρ is also referred to as the jammer occupancy and is given as

$$\rho = \frac{W_J}{W_S} \leq 1, \quad (4.33)$$

where W_J is the jamming bandwidth and W_S is the total signal bandwidth. For CFFH, partial-band jamming means that the jamming power is concentrated on a certain group of subcarriers. Let n_J denotes the number of jammed subcarriers, then the jamming ratio ρ is given by $\rho = \frac{n_J}{n_T}$. For a particular code matrix $X_i(n)$, this means that on average, ρn_T subcarriers are jammed out of n_T subcarriers used by $X_i(n)$.

When $\rho = 1$, the jamming power is uniformly distributed over the entire bandwidth. In this case, the partial-band jamming becomes *full-band jamming* [16, 17]. For a CFFH system, full-band jamming means that the jamming power is uniformly distributed over all N_c.

System Performance Under Rayleigh Fading and Full-Band Jamming

In the presence of Rayleigh fading and full-band jamming, the pairwise error probability can be expressed in terms of the jamming power spectral density N_J and average signal power E_s. In the case of high SNR, the upper bound in (4.30) can be expressed as

$$P(X_i(n), \hat{X}_i(n)|H_{i,t}^{j,m}(n)) \leq \left(\prod_{j=1}^{r_B} \lambda_j\right)^{-n_R} \left(\frac{E_s}{4N_J}\right)^{-r_B n_R}. \tag{4.34}$$

From (4.31), the upper bound in the presence of Rayleigh fading and full-band jamming can be expressed as

$$P(X_i(n), \hat{X}_i(n)|H_{i,t}^{j,m}(n)) \leq \left(1 + \frac{E_s}{4(N_0+N_J)} \sum_{j=1}^{r_B} \lambda_j\right)^{-n_R}. \tag{4.35}$$

As will be confirmed in Section 5.7: For the STC-CFFH system, at low SJNR, the space-frequency diversity gain is low; however, at high SJNR, the diversity gain becomes noticeable.

Under Rayleigh Fading and Partial-Band Jamming

Recall that each column of the received symbol matrix $R_i(n)$ is obtained from the same subcarrier in all received antennas. When we have partial-band jamming, most

likely not all columns of $R_i(n)$ are jammed, since each column is transmitted though different subcarriers. Thus the receiver may be able to recover the transmitted signal relying on the jamming-free columns.

Orthogonal space-time codes (OSTC) are capable of perfectly decoding the transmitted symbols under partial-band jamming and noise-free environments when at least one frequency band is not jammed. We consider a $n_T = 4$ space-time orthogonal block code design as an example. Following the same notation convention in the STC-CFFH transmitter example in Section 4.5, the code matrix with transmit symbols $x_{i,t}(n)$ for $t = 1, 2, 3, 4$, is represented as

$$X_i(n) = \begin{bmatrix} x_{i,1}(n) & x_{i,2}(n) & x_{i,3}(n) & x_{i,4}(n) \\ -x_{i,2}(n) & x_{i,1}(n) & -x_{i,4}(n) & x_{i,3}(n) \\ -x_{i,3}(n) & x_{i,4}(n) & x_{i,1}(n) & -x_{i,2}(n) \\ -x_{i,4}(n) & -x_{i,3}(n) & x_{i,2}(n) & x_{i,1}(n) \end{bmatrix}. \tag{4.36}$$

Due to the orthogonality of the code design, each frequency band contains full information about the transmitted symbols. As a result, the transmitted symbols are recovered perfectly when there is at least one un-jammed frequency band.

In this case, the average probability of error P_e can be expressed as

$$P_e = \sum_{i=0}^{4} P_{e,i} \; Pr\{i \; out \; of \; 4 \; bands \; are \; jammed\}, \tag{4.37}$$

where $P_{e,i}$ is the probability of error when i out of 4 bands are jammed.

4.6.3 Spectral Efficiency

One major challenge in the current FH-OFDMA system is collision. In FH-OFDMA, multiple users hop their subcarrier frequencies independently. If two users transmit simultaneously in the same frequency band, a collision, or hit occurs. In this case, the probability of bit error is generally assumed to be 0.5 [82].

If there are N_c available channels and M active users (i.e., $M - 1$ possible inter-

fering users), assuming that all N_c channels are equally probable and all users are independent. Even if each user only transmit over a single carrier, then the probability that a collision occurs is given by

$$P_h = 1 - (1 - \frac{1}{N_c})^{M-1} \tag{4.38}$$

$$\approx \frac{M-1}{N_c} \quad \text{when } N_c \text{ is large.} \tag{4.39}$$

Taking $N_c = 64$ as an example, the relationship between the probability of collision and the number of active users is shown in Figure 4.4. The high collision probability severely limits the number of users that can be simultaneously supported by an FH-OFDMA system.

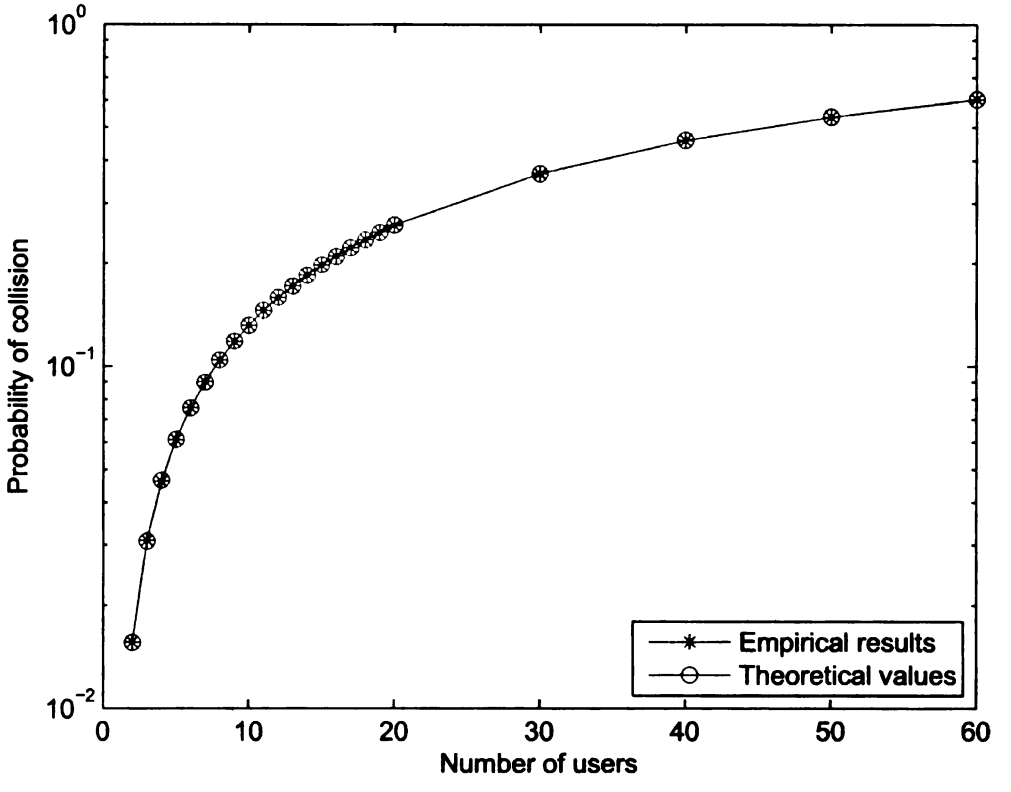

Figure 4.4. Probability of collision (P_h) versus the number of users (starting at the two-user case) for $N_c = 64$.

In this example, $N_c = 64$, for a required BER of 0.04, only 6 users can be supported. That is only 6 out of 64 subcarriers can be used simultaneously, the carrier efficiency is $\frac{6}{64} = 9.38\%$. On the other hand, due to the collision-free design, CFFH has the same spectral efficiency and BER performance as that of OFDM. For CFFH, the carrier efficiency is 100% with a much better BER performance. In this particular case, CFFH is approximately 10.67 times more efficient than the conventional FH-OFDMA system. This fact is further illustrated in simulation example 1 of Section 4.7.

4.7 Simulation Examples

In this section, we provide simulation examples to demonstrate the performance of the proposed schemes. First, the bit-error performance of the proposed CFFH scheme, the conventional FH and FH-OFDMA systems is performed under AWGN channels. Second, the bit-error performance of the proposed CFFH and STC-CFFH schemes, and the STC-OFDM system is performed over a frequency selective fading channel with partial-band jamming.

Simulation Example 1: We consider the conventional FH, the FH-OFDMA and the proposed CFFH systems, each with M=8 users and N_c=128 available subcarriers. The conventional FH system uses four frequency shift keying (4-FSK) modulation, where each user transmits over a single carrier. Both the proposed CFFH and FH-OFDMA systems transmits 16-QAM symbols, and each user is assigned 16 subcarriers. The average bit error rate (BER) versus the signal-to-noise ratio (SNR) performance over AWGN channels of the systems is illustrated in Fig. 4.5. As can be seen, the proposed CFFH scheme delivers excellent results since the multi-user access interference (MAI) is avoided. The conventional FH and FH-OFDMA schemes, on the other hand, is severely limited by collision effect among users.

Simulation Example 2: The BER performance of the STC-OFDM scheme and the proposed STC-CFFH and CFFH schemes are evaluated by simulations. The simulations are carried out over a frequency selective Rayleigh fading channel with

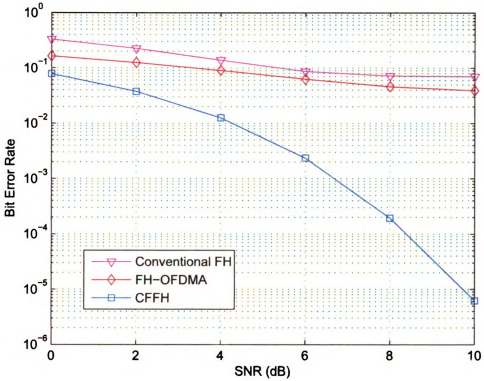

Figure 4.5. BER performance over AWGN channel of the CFFH, FH-OFDMA, and the conventional FH systems with M=8 users and N_c=128 available subcarriers.

partial-band jamming. An Alamouti space-time coding system with two transmit and receive antennas is applied to the proposed STC-CFFH system. We assume perfect timing and frequency synchronization, as well as uncorrelated channels for each antenna. The total number of available subcarriers is N_c=256 and the number of users is M=16; therefore each user is assigned 16 subcarriers.

We consider the performance of three systems that transmits 16-QAM symbols: (i) The proposed CFFH system; (ii) An STC-OFDM system; (iii) The proposed STC-CFFH system. For system (ii), each user transmits on 16 fixed subcarriers. In systems (i), and (iii), each user transmits on 16 pseudo-random secure subcarriers. We assume the jammer intentionally interferes 16 subcarriers out of the whole band.

Figure 4.6 depicts the BER versus SNR over frequency selective fading with

SJR=0dB. The STC-OFDM system outperforms the CFFH scheme due to the lack of space-time diversity. Incorporating space-time coding into CFFH significantly increases the BER performance. The combination of the secure subcarrier assignment and space-time diversity lead to the proposed STC-CFFH system outperforming the STC-OFDM system. The pseudo-random secure subcarrier assignment randomizes each users' channel occupancy at a given time, therefore allowing for multiple access over a wide range of frequencies. We also noticed that at high SNR levels, the performance limiting factor for all systems is the partial-band jamming.

One method of improving the BER performance is incorporating turbo coding into the system design. In Figure 4.7, a rate-$\frac{1}{2}$ turbo code is utilized for forward error control. The generation matrix of the constituent code is given by $[1, \frac{(7)octal}{(5)octal}]$, where $(7)octal$ and $(5)octal$ are the feedback and feedforward polynomials with memory length 2, respectively. At the receiver, tentative soft decisions are made by the symbol demodulation, and then the resulting log-likelihood ratios (LLRs) of the code bits are fed into a turbo decoder. There is no iteration between the demodulator and the turbo decoder. The decoding algorithm is the canonical log-MAP. The number of decoding iterations is 5 and no early termination scheme is applied. From Figure 4.7, we observe a significant BER improvement for each system. Furthermore, the performance limiting of the partial-band jamming is eliminated.

In Figure 4.8, the BER versus the jammer occupancy (ρ) is evaluated with SNR=10dB and SJR=0dB for the three systems. Recall the jammer occupancy is the fraction of subcarriers that experience interference. We can see that the STC-CFFH system outperforms the other systems for all $\rho < 1$. This example shows that STC-CFFH is very robust under jamming interference.

We also observed that due to the randomness in the frequency hopping pattern, as well as the fact that the system ensures collision-free transmission among the users, the performance of the proposed system remains the same as the number of users varies in the system.

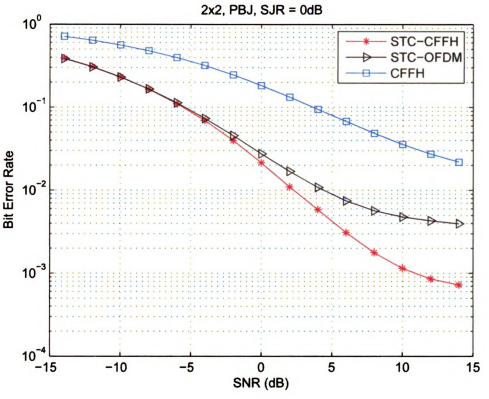

Figure 4.6. Comparison of the BER over frequency selective fading channel with partial-band jamming. Number of subcarriers $N_c = 256$, number of users = 16 and SJR = 0dB.

4.8 Summary

In summary, we introduced a secure collision-free frequency hopping scheme. Based on the OFDMA framework and the new secure subcarrier assignment algorithm, the proposed CFFH system can achieve high spectral efficiency through collision-free multiple access. While keeping the inherent anti-jamming, anti-interception security features of the FH system, CFFH can achieve the same spectral efficiency as that of OFDM, and can relax the strict synchronization requirement suffered by the conventional FH systems. Furthermore, we enhanced the jamming resistance of the CFFH scheme, by incorporating space-time coding to the proposed scheme. Our simulation experiments demonstrated the superior performance of the proposed schemes in terms

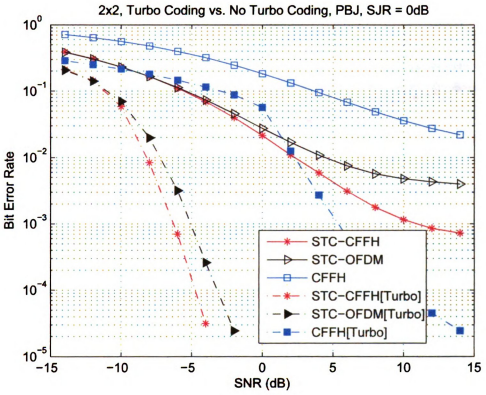

Figure 4.7. BER performance with Turbo Coding over frequency selective fading channel with partial-band jamming. Number of subcarriers $N_c = 256$, number of users = 16 and SJR = 0dB.

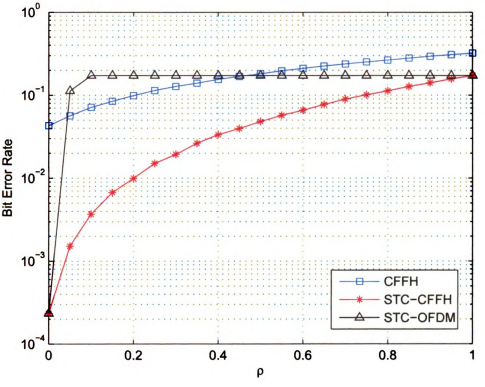

Figure 4.8. BER versus Jammer Occupancy over frequency selective fading channel with partial-band to full-band jamming. Number of subcarriers $N_c = 256$, number of users = 16, SJR = 0dB and SNR = 10dB.

of both spectral efficiency and jamming resistance.

CHAPTER 5

Jamming Mitigation Using Quasi-Orthogonal Space-Time Block Codes

In this chapter, we investigate the use of quasi-orthogonal space-time block codes (QO-STBCs) to mitigate jamming noise. Unlike orthogonal space-time block codes, QO-STBCs are capable of providing full diversity and full-rate transmission for codes designed for more than two transmit antennas. With QO-STBCs, the orthogonality of the code is relaxed and by introducing signal constellation rotation into the QO-STBC design, we can improve the bit error rate performance. First, we derive analytical expressions for the exact pairwise error probability (PEP) of the QO-STBC orthogonal frequency division multiplexing (QO-STBC-OFDM) system using the moment generating function (MGF). Second, we calculate the exact PEP under various situations, and derive the closed-form expressions and union bound for the bit error probability (BEP). Third, we compare the numerical results with the simulation results. Our numerical analysis and simulation results show that union bound is tight and the QO-STBC-OFDM system is effective in mitigating partial-band noise jamming.

5.1 Introduction

Space-time coding [42,43] is an attractive technique to achieve both highly reliable and spectrally efficient communications. Space-time block codes from orthogonal designs

provide full diversity and simple single symbol decoding at the receiver. However, full-rate orthogonal space-time block codes (OSTBCs) with complex elements in its transmission matrix only exist for two transmit antennas, which is the Alamouti scheme [42].

In an effort to provide full-rate transmission for space-time block codes with more than two transmit antennas, quasi-orthogonal space-time block codes (QO-STBCs) [49, 50] were proposed. With the quasi-orthogonal structure, the orthogonality of the code is relaxed to provide a higher symbol transmission rate and the maximum likelihood (ML) decoding can be done by searching pairs of symbols instead of searching single symbols in orthogonal designs. The tradeoff for the higher transmission rate of QO-STBCs is the inability to achieve full diversity. The performance of QO-STBCs is better than OSTBCs at low signal-to-noise ratio (SNR), but worse at high SNR. In other words, the slope of the QO-STBC is not as steep as the OSTBC because the QO-STBC does not provide full diversity.

In [53,55,56], the authors improve the QO-STBC bit error rate (BER) performance by introducing signal constellation rotation into the QO-STBC design. In particular, the constellation rotation QO-STBC [55, 56] proposes that half of the symbols in the quasi-orthogonal design be chosen from a signal constellation $\mathcal{A}$ and the other half of the symbols be chosen from a rotated constellation $e^{j\phi}\mathcal{A}$. The constellation rotation QO-STBC can achieve full diversity and fast ML decoding.

We consider the combination of constellation rotation QO-STBC with orthogonal frequency division multiplexing (QO-STBC-OFDM) to exploit multipath diversity and achieve high speed high quality transmissions. However, such systems must co-exist with various forms of interference to provide reliable communication [83]. Therefore, there is a need for proper analytical tools to assess the performance of QO-STBC-OFDM systems in the presence of partial-band noise jamming. In partial-band noise (PBN) jamming, the jammer's total power J_{tot} is distributed over T randomly jammed symbol blocks, which are not necessarily contiguous. We define the jammer occupancy $\alpha = T/S$ as the ratio of the symbol blocks jammed, where S is the total number of symbol blocks. We assume there is an integer number of symbol

blocks $S = N_c/n_0$, where N_c is the total number of subcarriers and n_0 is the number of subcarriers required to transmit one encoded symbol block. The PBN jamming acts like a Gaussian noise source with zero-mean and the effective jamming power in any symbol block is J_s.

In this chapter, we consider multiple-input multiple-output (MIMO) communication system that employs a constellation rotated QO-STBC-OFDM and evaluate its performance under frequency-selective fading and partial-band noise jamming [84]. The exact pairwise error probability (PEP) of the constellation rotated QO-STBC with quadrature phase-shift keying (QPSK) modulation is derived by using the moment generating function (MGF). Furthermore, we calculate the PEP under various situations, and derive the closed-form expressions and union bound for the bit error probability (BEP). Our numerical analysis and simulation results show that union bound is tight and the QO-STBC-OFDM system is effective in mitigating partial-band noise jamming.

This chapter is organized as follows. In Section 5.2, the QO-STBC-OFDM system model is outlined. In Section 5.3, the code design of the QO-STBC with constellation rotation is briefly reviewed, and the global minimum Euclidean distance and the diversity product is analyzed. The pairwise error probability of the QO-STBC-OFDM system with and without partial-band noise jamming is derived in Section 5.4. The closed form expressions and the union bound are derived in Section 5.5 and Section 5.6, respectively. Simulation results are provided in Section 5.7. Finally, a summary is provided in Section 5.8.

5.2 System Model

We consider a QO-STBC-OFDM system with N_t transmit antennas and N_r receive antennas, which are assumed to be uncorrelated. The total number of subcarriers N_c are distributed over the $U = N_c/N_u$ users such that each user is assigned N_u subcarriers. Note that each users' subcarriers need not be contiguous. The data symbols are modulated with quadrature phase-shift keying (QPSK).

Initially, a block of L_g information bits are partitioned into groups of 4 bits which are transformed into a stream of complex symbols from the QPSK alphabet $\mathcal{A}$. The resulting complex symbol sequence with elements a_k for $k = 1, \cdots, L_a$ is parsed into S blocks of length k_0 where $L_a = k_0 S$. For $s = 1, 2, \cdots, S$, we can represent each symbol block in vector form as $\mathbf{a}_s = [a_{k_0(s-1)+1}, a_{k_0(s-1)+2}, \cdots, a_{k_0(s-1)+k_0}]^T$. Each block $\mathbf{a}_s$ is then encoded by a QO-STBC encoder, resulting in a $N_t \times n_0$ block matrix $\mathbf{X}_s$ with rate-k_0/n_0. The block matrix $\mathbf{X}_s = [\mathbf{x}_m, \mathbf{x}_{m+1}, \cdots, \mathbf{x}_{m+n_0-1}]$, where $\mathbf{x}_m = [x_{1,m}, x_{2,m}, \cdots, x_{N_t,m}]^T$ and T is the transpose operation. In matrix form, $\mathbf{X}_s$ is represented as

$$\begin{aligned} \mathbf{X}_s &= \begin{bmatrix} \mathbf{x}_m & \mathbf{x}_{m+1} & \cdots & \mathbf{x}_{m+(n_0-1)} \end{bmatrix} \\ &= \begin{bmatrix} x_{1,m} & x_{1,m+1} & \cdots & x_{1,m+(n_0-1)} \\ x_{2,m} & x_{2,m+1} & \cdots & x_{2,m+(n_0-1)} \\ \vdots & \vdots & \ddots & \vdots \\ x_{N_t,m} & x_{N_t,m+1} & \cdots & x_{N_t,m+(n_0-1)} \end{bmatrix}, \end{aligned} \tag{5.1}$$

where $x_{i,m}$ is the symbol transmitted from the mth subcarrier of the ith transmitter, and $m = n_0(s-1)+1$ for each S block. Finally, each symbol block X_s is OFDM modulated with the n_0 subcarriers and transmitted over independent channels.

After OFDM demodulation with perfect channel state information (CSI), the received symbol at the jth receive antenna and mth subcarrier is

$$y_{j,m} = \sum_{i=1}^{N_t} x_{i,m} h_{j,i,m} + n_{j,m} + \rho_{j,m} z_{j,m}, \tag{5.2}$$

for $m = 0, 1, \cdots, N_c - 1$, and where $h_{j,i,m}$ is the channel fading coefficient of the mth subcarrier of the channel between the jth receive antenna and ith transmit antenna, $x_{i,m}$ is the symbol transmitted from mth subcarrier of the ith transmit antenna, $n_{j,m}$ is the zero-mean, complex, additive white Gaussian noise (AWGN) with variance σ_n^2,

$\rho_{j,m}$ is the jammer indicator function defined as

$$\rho_{j,m} = \begin{cases} 0, & \text{No jamming on the } m\text{th subcarrier of the } j\text{th receive antenna;} \\ 1, & \text{Jamming on the } m\text{th subcarrier of the } j\text{th receive antenna,} \end{cases}$$

and $z_{j,m}$ is the zero-mean, complex, jamming Gaussian noise with variance J_s. We denote the set of symbol blocks that experience jamming as $\mathcal{I}$ and the set of symbol blocks that do not experience jamming as $\mathcal{I}'$.

5.3 Quasi-Orthogonal Space-Time Block Codes with Constellation Rotation

In this section, we discuss the code design of the QO-STBC with constellation rotation scheme. In addition, we analyze the performance criteria, namely the global minimum Euclidean distance d_E and the diversity product ζ.

5.3.1 Quasi-Orthogonal Space-Time Block Code with Constellation Rotation Code Design

We consider the Papadias and Foschini (**PF**) [51, 53] scheme in our analysis of the BEP performance in the presence of partial-band noise jamming. The first class of QO-STBCs [49, 50] provides full-rate transmission and outperforms OSTBC at low SNR levels, but is outperformed by the OSTBC at high SNR levels. The loss in performance at the high SNR levels is due to QO-STBC's lack of full diversity. As a result, the constellation rotation (CR) class of QO-STBCs [53, 55, 56] were proposed to provide full-rate and full diversity. Specifically, the constellation rotation scheme proposes that half of the symbols (x_1 and x_2) in the quasi-orthogonal design be selected from a signal constellation set $\mathcal{A}$ and the other half of the symbols (x_3 and x_4) be selected from signal constellation $e^{j\phi}\mathcal{A}$, where ϕ is the rotation angle. The **PF** scheme with rotation angle has the following code structure

$$\mathbf{X_{PF}} = \begin{bmatrix} x_1 & x_2 & e^{j\phi}x_3 & e^{j\phi}x_4 \\ x_2^* & -x_1^* & (e^{j\phi}x_4)^* & (e^{j\phi}x_3)^* \\ e^{j\phi}x_3 & -e^{j\phi}x_4 & -x_1 & x_2 \\ (e^{j\phi}x_4)^* & (e^{j\phi}x_3)^* & -x_2^* & -x_1^* \end{bmatrix}. \tag{5.3}$$

A natural question which arises is what is the optimal rotation angle? In the following subsection, we discuss the performance criteria, specifically the global minimum Euclidean distance and the diversity product.

5.3.2 Global Minimum Euclidean Distance

The first performance criteria for optimizing rotation angle for the QO-STBC with constellation rotation scheme is the global minimum Euclidean distance.

Lets consider the symbols x_1 and x_3 which are selected from constellation $\mathcal{A}$ and $e^{j\phi}\mathcal{A}$, respectively. Furthermore, let us denote the minimum Euclidean distance in $\mathcal{A}$ and $e^{j\phi}\mathcal{A}$ from the pair (x_1,x_3) to all other pairs of symbols as $d_{min}^{\mathcal{A}}$ and $d_{min}^{e^{j\phi}\mathcal{A}}$, respectively. Denoting the global minimum Euclidean distance as

$$d_E = \min_{(x_1,x_3)} [d_{min}^{\mathcal{A}}, d_{min}^{e^{j\phi}\mathcal{A}}]. \tag{5.4}$$

in constellations $\mathcal{A}$ and $e^{j\phi}\mathcal{A}$. The objective is to maximize d_E by choosing the optimum angle ϕ.

5.3.3 Diversity Product

The second performance criteria for optimizing the rotation angle for the QO-STBC with constellation rotation scheme is the diversity product.

The diversity product is important because it determines the slope of the performance curve. In order to achieve the maximum diversity, the difference matrix $\mathbf{X}-\hat{\mathbf{X}}$ has to be full rank for any distinct codewords $\mathbf{X}$ and $\hat{\mathbf{X}}$ [56]. The diversity product

is denoted as

$$\zeta = \frac{1}{\sqrt{N_t}} \min_{\mathbf{X} \neq \hat{\mathbf{X}}} |\det[\mathbf{X} - \hat{\mathbf{X}}]|^{\frac{1}{n_0}}. \tag{5.5}$$

Note that the diversity product is normalized by the factor $\frac{1}{\sqrt{N_t}}$, resulting in $0 \leq \zeta \leq 1$. When all codewords are square matrices ($n_0 = N_t$), the diversity product can be simplified as

$$\zeta = \frac{1}{\sqrt{N_t}} \min_{\mathbf{X} \neq \hat{\mathbf{X}}} |\det[(\mathbf{X} - \hat{\mathbf{X}})]|^{\frac{1}{N_t}}. \tag{5.6}$$

Considering QPSK modulation and (5.3), the diversity product can be rewritten as

$$\begin{aligned} \zeta &= \frac{1}{4} \min_{\mathbf{X} \neq \hat{\mathbf{X}}} |\det[(\mathbf{X} - \hat{\mathbf{X}})]|^{\frac{1}{4}} \\ &= \frac{1}{4} \min_{\mathbf{X} \neq \hat{\mathbf{X}}} |a^2 - b^2|^{\frac{1}{4}}, \end{aligned} \tag{5.7}$$

where,

$$a = \sum_{i=1}^{4} |x_i - \hat{x}_i|^2, \tag{5.8}$$

and

$$\begin{aligned} b &= 2\mathrm{Im}\{(x_{1,m} - \hat{x}_{1,m})^*(x_{3,m} - \hat{x}_{3,m})e^{j\phi} \\ &+ (x_{2,m} - \hat{x}_{2,m})^*(x_{4,m} - \hat{x}_{4,m})e^{-j\phi}\}. \end{aligned} \tag{5.9}$$

Due to the fact that (5.9) decreases monotonically with respect to $|b|^2$, ζ is upper bounded at $|b|^2 = 0$ by

$$\begin{aligned} \zeta \leq \zeta_{ub} &= \min_{\mathbf{X} \neq \hat{\mathbf{X}}} a^{\frac{1}{2}} \\ &= \frac{d_{min}}{4}, \end{aligned} \tag{5.10}$$

where, d_{min} is the minimum Euclidean distance. For the case of $|b|^2 = 0$, a achieves the minimum value $a_{min} = d_{min}^2$. This occurs if all but one of the code symbols of two distinct codewords $\mathbf{X} \neq \hat{\mathbf{X}}$ are identical [85].

For a M-PSK constellation (M>2), the diversity product of QO-STBC as a function of the rotation angle ϕ is given as

$$\zeta = \frac{d_{min}}{4} = \begin{cases} \min\left(\sqrt{2|\sin(\phi - \frac{2k\pi}{M})|}, 1\right), & \text{for } \phi = \phi_1; \\ \min\left(\sqrt{2|\sin(\phi - \frac{2(k+1)\pi}{M})|}, 1\right), & \text{for } \phi = \phi_2, \end{cases} \tag{5.11}$$

where, $\frac{2k\pi}{M} \leq \phi_1 < \frac{(2k+1)\pi}{M}$, $\frac{(2k+1)\pi}{M} \leq \phi_2 < \frac{2(k+1)\pi}{M}$, and k is an integer. Note that, for QPSK constellation, $d_{min} = \sqrt{2}$.

If the diversity product is nonzero, the code has full diversity. Note that, maximizing the diversity product is different from maximizing the Euclidean distance. Two signals with a large Euclidean distance does not translate to a large diversity product. In other words, it is possible for two signals to have a large Euclidean distance, but have a small diversity product.

Figure 5.1 depicts the diversity product ζ and global minimum Euclidean distance d_E for QPSK constellation. From the figure, we observe that for QPSK constellation, ζ achieves the upper bound $d_{min}/4$ between $\phi = \pi/6$ and $\pi/3$ and d_E is maximized at $\phi = \pi/4$. Therefore, the optimal rotation angle for QPSK constellation is $\phi = \pi/4$.

5.4 Analysis of the Pairwise Error Probability

In this section, we discuss and derive the PEP performance of QO-STBC-OFDM system with and without partial-band noise jamming. We assume the jammer interferes all subcarriers transmitted in the sth QO-STBC-OFDM symbol block if the symbol block is jammed.

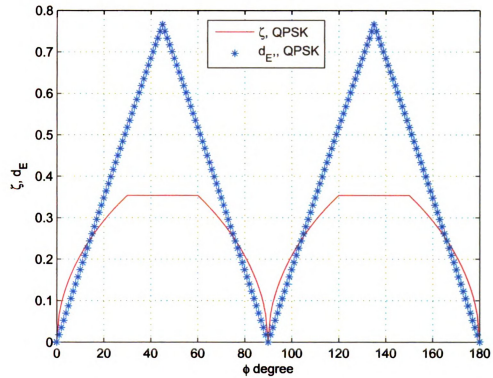

Figure 5.1. Diversity product ζ, and the global minimum Euclidean distance d_E versus the rotation angle ϕ

5.4.1 Pairwise Error Probability Analysis without Jamming

The authors in [86] derived the exact PEP of various QO-STBCs without interference. In this subsection, we adopt the result in [86] and derive the exact PEP for the QO-STBC-OFDM system.

The received signal without jamming can be expressed as

$$\mathbf{y}_s = (\mathbf{I}_{N_r} \otimes \mathbf{X}_s)\mathbf{h}_s + \mathbf{n}_s, \tag{5.12}$$

where $\otimes$ denotes the matrix Kronecker product, $\mathbf{I}_{N_r}$ is the $N_r \times N_r$ identity matrix, $\mathbf{h}_s$ is defined as

$$\begin{aligned}\mathbf{h}_s = {} & [h_{1,1,m}, \cdots, h_{1,N_t,m}, h_{2,1,m}, \cdots, h_{2,N_t,m}, \\ & h_{N_r,1,m}, \cdots, h_{N_r,N_t,m}]^T,\end{aligned} \tag{5.13}$$

and $\mathbf{n}_s$ is defined as

$$\begin{aligned}\mathbf{n}_s = {} & [n_{1,m}, \cdots, n_{N_r,m}, n_{1,m+1}, \cdots, n_{N_r,m+1}, \\ & n_{1,m+(n_0-1)}, \cdots, n_{N_r,m+(n_0-1)}]^T.\end{aligned} \tag{5.14}$$

Assuming channel state information is available at the receiver, then the maximum likelihood (ML) decoding metric becomes

$$m(\mathbf{y}_s, \mathbf{X}_s) = \| \mathbf{y}_s - \mathbf{X}_s\mathbf{h}_s \|^2 = \| \mathbf{y}_s - (\mathbf{I}_{N_r} \otimes \mathbf{X}_s)\mathbf{h}_s \|^2 \tag{5.15}$$

We denote the PEP of the sth symbol block that does not experience jamming as $P_{\mathcal{I}'}(\mathbf{X}_s, \hat{\mathbf{X}}_s|\mathbf{h}_s)$, which is averaged over Rayleigh fading.

The probability that the ML decoder decodes the correct $\mathbf{X}_s$ into the incorrect $\hat{\mathbf{X}}_s \neq \mathbf{X}_s$ is given as

$$P_{\mathcal{I}'}(\mathbf{X}_s, \hat{\mathbf{X}}_s|\mathbf{h}_s) = Pr\{m(\mathbf{y}_s, \mathbf{X}_s) - m(\mathbf{y}_s, \hat{\mathbf{X}}_s) \geq 0|\mathbf{h}_s\} \tag{5.16}$$

After substituting (5.15) into (5.16) and performing some calculations, we obtain

$$\begin{aligned} P_{\mathcal{I}'}(\mathbf{X}_s, \hat{\mathbf{X}}_s|\mathbf{h}_s) &= Pr\{\zeta_{\mathcal{I}'} \geq \eta_s|\mathbf{h}_s\} \\ &= Q\left(\frac{\eta_s}{\sigma^2_{\zeta_{\mathcal{I}'}}}\right) \\ &= Q\left(\sqrt{\frac{\eta_s}{4\sigma_n^2}}\right), \end{aligned} \tag{5.17}$$

where $\eta_s = \|[\mathbf{I}_{N_r} \otimes (\mathbf{X}_s - \hat{\mathbf{X}}_s)]\mathbf{h}_s\|^2$, and $\zeta_{\mathcal{I}'} = 2Re\{\mathbf{n}_s^H[I_{N_r} \otimes (\hat{\mathbf{X}}_s - \mathbf{X}_s)]\mathbf{h}_s\}$ is a zero mean real Gaussian random variable with variance $\sigma^2_{\zeta_{\mathcal{I}'}} = 4\sigma_n^2\eta_s$. Note that $(\cdot)^H$ denotes the complex conjugate transpose, and $Q(\cdot)$ is the Gaussian Q-function defined as $Q(x) = \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \exp(-\frac{x^2}{2\sin\theta})\mathrm{d}\theta$ [87].

5.4.2 Pairwise Error Probability Analysis with Jamming

In this subsection, we derive the PEP of QO-STBC-OFDM system in the presence of partial-band noise jamming.

The received signal that experience jamming can be expressed as

$$\mathbf{y}_s = (\mathbf{I}_{N_r} \otimes \mathbf{X}_s)\mathbf{h}_s + \mathbf{n}_s + \mathbf{z}_s, \tag{5.18}$$

where $\mathbf{z}_s$ is defined as

$$\begin{aligned} \mathbf{z}_s = [&z_{1,m}, \cdots, z_{N_r,m}, z_{1,m+1}, \cdots, z_{N_r,m+1}, \\ &z_{1,m+(n_0-1)}, \cdots, z_{N_r,m+(n_0-1)}]^T. \end{aligned} \tag{5.19}$$

We denote $P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s|\mathbf{h}_s)$ as the PEP of the sth symbol block that experience jamming. Similarly to the jamming-free case we can derive the PEP of the jammed symbol blocks as

$$\begin{aligned} P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s|\mathbf{h}_s) &= Q\left(\frac{\eta_s}{\sigma^2_{\zeta_{\mathcal{I}}}}\right) \\ &= Q\left(\sqrt{\frac{\eta_s}{4(\sigma_n^2+\sigma_z^2)}}\right), \end{aligned} \tag{5.20}$$

where, η_s is defined in Section 5.4.1, and $\zeta_{\mathcal{I}} = 2Re\{(\mathbf{n}_s^H + \mathbf{z}_s^H)[I_{N_r} \otimes (\hat{\mathbf{X}}_s - \mathbf{X}_s)]\mathbf{h}_s\}$ is zero mean real Gaussian random variable with variance $\sigma^2_{\zeta_{\mathcal{I}}} = 4(\sigma_n^2 + \sigma_z^2)\eta_s$.

If we normalize the average transmit symbol energy from each antenna i.e $E|x_{i,m}|^2 = 1$, then the noise variance $\sigma_n^2 = \frac{N_t}{2\gamma}$ and jamming variance $\sigma_z^2 = \frac{N_t}{2\omega}$, where γ is the average signal-to-noise ratio (SNR) and ω is the average signal-to-interference-ratio (SIR). Using Craig's representation of the Gaussian Q-function [87], the conditional PEP of (5.20) can be rewritten as

$$\begin{aligned} P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s|\mathbf{h}_s) &= \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \exp\left[\frac{-\eta_s}{\frac{4(\sigma_n^2+\sigma_z^2)}{2\sin^2\theta}}\right] \mathrm{d}\theta \\ &= \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \exp\left[\frac{-\eta_s}{8(\sigma_n^2+\sigma_z^2)\sin^2\theta}\right] \mathrm{d}\theta \end{aligned} \tag{5.21}$$

Substituting $\sigma_n^2 = \frac{N_t}{2\gamma}$ and $\sigma_z^2 = \frac{N_t}{2\omega}$ into (5.21), we can obtain

$$P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s|\mathbf{h}_s) = \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \exp\left[-\beta\frac{\eta_s}{\sin^2\theta}\right] \mathrm{d}\theta, \tag{5.22}$$

where, $\beta = \frac{1}{4(\frac{N_t}{\gamma}+\frac{N_t}{\omega})}$.

To evaluate the exact PEP, we need to average over the channel. Due to the independence of the channel gain vectors associated with the receivers, the unconditional PEP can be expressed in terms of a single integral whose integrand is the MGF's associated with each of the receivers

$$P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s) = \frac{1}{\pi}\int_0^{\frac{\pi}{2}} M_{\xi_s}\left(\frac{-1}{\sin^2\theta}\right) \mathrm{d}\theta \tag{5.23}$$

where $\xi_s = \beta\mathbf{h}_s^H[\mathbf{I}_{N_r} \otimes (\mathbf{X}_s - \hat{\mathbf{X}}_s)]^H[\mathbf{I}_{N_r} \otimes (\mathbf{X}_s - \hat{\mathbf{X}}_s)]\mathbf{h}_s$ is a quadratic form of complex variables with MGF $M_{\xi_s}(l) = E_{\xi_s}\{\exp(l\xi_s)\}$.

Assuming the channel is Rayleigh distributed, we can make use of a result due

to Turin [88] to evaluate the MGF $M_{\xi_s}(l)$. Furthermore, assuming that the channel gains have identical statistics and making use of the block diagonal structure of $[\mathbf{I}_{N_r} \otimes (\mathbf{X}_s - \hat{\mathbf{X}}_s)]^H [\mathbf{I}_{N_r} \otimes (\mathbf{X}_s - \hat{\mathbf{X}}_s)]$, it is then straightforward to show that

$$P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s) = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \left[\det\Big(\mathbf{I}_{N_t} + \beta \frac{1}{\sin^2\theta} \times (\mathbf{X}_s - \hat{\mathbf{X}}_s)^H (\mathbf{X}_s - \hat{\mathbf{X}}_s) \Big) \right]^{-N_r}. \tag{5.24}$$

Using (5.24), we will find the closed-form expression for the exact PEP of constellation rotation QO-STBC (5.3) under partial-band noise jamming.

In order to find the exact PEP of the **PF** scheme with $N_t = 4$ transmit antennas, we have to calculate the determinant in (5.24). Defining $\kappa_s = (\mathbf{I}_4 + \beta \frac{(\mathbf{X}_s - \hat{\mathbf{X}}_s)^H (\mathbf{X}_s - \hat{\mathbf{X}}_s)}{\sin^2\theta})$ as

$$\begin{aligned} \det\Big[\kappa_s\Big] &= \det \begin{bmatrix} 1+a_s & 0 & jb_s & 0 \\ 0 & 1+a_s & 0 & -jb_s \\ -jb_s & 0 & 1+a_s & 0 \\ 0 & jb_s & 0 & 1+a_s \end{bmatrix} \\ &= [(1+a_s)^2 - b_s^2]^2, \end{aligned} \tag{5.25}$$

where $a_s = \beta \frac{1}{\sin^2\theta} \sum_{i=1}^{4} |x_{i,m} - \hat{x}_{i,m}|^2$ and $b_s = \beta \frac{1}{\sin^2\theta} 2\mathrm{Im}\{(x_{1,m} - \hat{x}_{1,m})^*(x_{3,m} - \hat{x}_{3,m})e^{j\phi} + (x_{2,m} - \hat{x}_{2,m})^*(x_{4,m} - \hat{x}_{4,m})e^{-j\phi}\}$. Recall that the ML decoding of the **PF** scheme is done pair by pair i.e., symbol pairs $(x_{1,m}, x_{3,m})$ are jointly decoded and $(x_{2,m}, x_{4,m})$ are jointly decoded, but each pair is decoded independently. Hence, we consider only symbol pair $(x_{1,m}, x_{3,m})$ to derive the PEP and use the notations $\mathbf{X}_s = (x_{1,m}, x_{3,m})$ and $\hat{\mathbf{X}}_s = (\hat{x}_{1,m}, \hat{x}_{3,m})$. Substituting (5.25) into (5.24) and performing some algebraic simplification, we can express the exact PEP of the **PF** scheme as

$$P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s) = \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \left[1 + \beta\frac{|(x_{1,m}-\hat{x}_{1,m})+je^{j\phi}(x_{3,m}-\hat{x}_{3,m})|^2}{\sin^2\theta}\right]^{-2N_r}$$
$$\times \left[1 + \beta\frac{|(x_{1,m}-\hat{x}_{1,m})-je^{j\phi}(x_{3,m}-\hat{x}_{3,m})|^2}{\sin^2\theta}\right]^{-2N_r} \mathrm{d}\theta. \quad (5.26)$$

Note that the interference-free case $P_{\mathcal{I}'}(\mathbf{X}_s, \hat{\mathbf{X}}_s)$ can be derived in a similar matter. For the interference-free case, replace β with $\delta = \frac{\gamma}{4N_t}$.

5.4.3 Overall Pairwise Error Probability Analysis

The average PEP of a QO-STBC-OFDM system over S blocks can be written as

$$\begin{aligned} P^{QO-STBC-OFDM} &= \frac{1}{S}\left[\sum_{s\in\mathcal{I}'} P_{\mathcal{I}'}(\mathbf{X}_s, \hat{\mathbf{X}}_s|\mathbf{h}_s)\right. \\ &+ \left.\sum_{s\in\mathcal{I}} P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s|\mathbf{h}_s)\right] \\ &= \frac{1}{S}\sum_{s=1}^{S}\left[(1-\alpha)P_{\mathcal{I}'}(\mathbf{X}_s, \hat{\mathbf{X}}_s|\mathbf{h}_s)\right. \\ &+ \left.\alpha P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s|\mathbf{h}_s)\right] \end{aligned} \quad (5.27)$$

where, $\alpha = T/S$ is the fraction of symbol blocks that experience jamming.

5.5 Closed-Form Expressions of the Pairwise Error Probability

In this section, we present the closed-form expressions of the PEP for the sth symbol block of the **PF** scheme with N_t transmit antennas and N_r receive antennas. In our calculations of the closed-form expressions we consider the PEP of the jammed symbol blocks $P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s|\mathbf{h}_s)$, and only consider the symbol pair $(x_{1,m}, x_{3,m})$. The exact PEP expression (5.26) can be simplified by defining variables u_s and v_s as

$$
\begin{aligned}
u_s &= |(x_{1,m} - \hat{x}_{1,m}) + je^{j\phi}(x_{3,m} - \hat{x}_{3,m})|^2, \\
v_s &= |(x_{1,m} - \hat{x}_{1,m}) - je^{j\phi}(x_{3,m} - \hat{x}_{3,m})|^2.
\end{aligned}
$$

Substituting the variables u_s and v_s, (5.26) can be rewritten as

$$
\begin{aligned}
P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s) &= \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \left(\frac{\sin^2\theta}{\sin^2\theta+\beta u_s}\right)^{2N_r} \\
&\times \left(\frac{\sin^2\theta}{\sin^2\theta+\beta v_s}\right)^{2N_r} \mathrm{d}\theta. \qquad (5.28)
\end{aligned}
$$

Depending on the values of u_s and v_s, the exact PEP in (5.28) can be classified into three types. Note that both u_s and v_s cannot be zero because we are considering PEP.

Type I is the case when either u_s or v_s is equal to zero. The exact PEP of Type I can be expressed as

$$
P_I(\mathbf{X}_s, \hat{\mathbf{X}}_s) = \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \left(\frac{\sin^2\theta}{\sin^2\theta+\beta(u_s+v_s)}\right)^{2N_r} \mathrm{d}\theta. \qquad (5.29)
$$

Note that the **PF** scheme with constellation rotation does not have a Type I closed-form expression because symbols $x_{1,m}$ and $x_{3,m}$ are selected from different signal constellations. As a result, neither u_s or v_s can equal to zero. In others words, the **PF** scheme with constellation rotation has full diversity.

Type II is the case when $u_s = v_s \neq 0$. The exact PEP of Type II can be expressed as

$$
P_{II}(\mathbf{X}_s, \hat{\mathbf{X}}_s) = \frac{1}{\pi}\int_0^{\frac{\pi}{2}} \left(\frac{\sin^2\theta}{\sin^2\theta+\beta u_s}\right)^{4N_r} \mathrm{d}\theta. \qquad (5.30)
$$

Type III is the case when u_s and v_s are nonzero and distinct. The exact PEP of

Type III can be expressed as (5.28),

$$P_{III}(\mathbf{X}_s, \hat{\mathbf{X}}_s) = P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s). \tag{5.31}$$

Table 5.1 shows the distribution of u_s and v_s and the corresponding PEP types for the **PF** scheme using QPSK modulation, where b_i is the number of i-bit error cases. From the Table 5.1, it can be easily seen that there are 1-bit, 2-bit or 3-bit errors between $\mathbf{X}_s$ and $\hat{\mathbf{X}}_s$ for Type II and there are 2-bit, 3-bit or 4-bit errors between $\mathbf{X}_s$ and $\hat{\mathbf{X}}_s$ for Type III. Note that when applying QPSK modulation, there are a total of 256 possible (u_s, v_s) pairs. Recall, that if $(u_s, v_s) = (0, 0)$, then there is no error between $\mathbf{X}_s$ and $\hat{\mathbf{X}}_s$. Thus, the 16 (u_s, v_s) pairs resulting in $(u_s, v_s) = (0, 0)$ are excluded from the analysis, and there are a total of 240 possible (u_s, v_s) pairs.

Following the results in [89], the closed-form expressions of the PEPs in the presence of partial-band noise jamming for QO-STBC-OFDM can be derived as

$$\begin{aligned} P_I(\mathbf{X}_s, \hat{\mathbf{X}}_s) &= \frac{1}{2}\left[1 - \sqrt{\frac{\beta(u_s+v_s)}{1+\beta(u_s+v_s)}}\right. \\ &\quad \left. \times \sum_{k=0}^{2N_r-1} \binom{2k}{k} \left(\frac{1-\frac{\beta(u_s+v_s)}{1+\beta(u_s+v_s)}}{4}\right)^k\right], \end{aligned} \tag{5.32}$$

$$\begin{aligned} P_{II}(\mathbf{X}_s, \hat{\mathbf{X}}_s) &= \frac{1}{2}\left[1 - \sqrt{\frac{\beta u_s}{1+\beta u_s}}\right. \\ &\quad \left. \times \sum_{k=0}^{4N_r-1} \binom{2k}{k} \left(\frac{1-\frac{\beta u_s}{1+\beta u_s}}{4}\right)^k\right], \end{aligned} \tag{5.33}$$

$$P_{III}(\mathbf{X}_s, \hat{\mathbf{X}}_s) = \frac{\left(\frac{u_s}{v_s}\right)^{2N_r-1}}{2\left(1-\frac{u_s}{v_s}\right)^{4N_r-1}}\left[\sum_{k=0}^{2N_r-1}\left(\frac{v_s}{u_s}-1\right)^k \times B_k I_k(\beta v_s) - \frac{u_s}{v_s}\sum_{k=0}^{2N_r-1}\left(1-\frac{v_s}{u_s}\right)^k C_k I_k(\beta u_s)\right], \tag{5.34}$$

where,

$$A_k = (-1)^{2N_r-1+k}\frac{\binom{2N_r-1}{k}}{(2N_r-1)!}\prod_{n=1,n\neq k+1}^{2N_r}(4N_r-n),$$

$$B_k = \frac{A_k}{\binom{4N_r-1}{k}},$$

$$C_k = \sum_{n=0}^{2N_r-1}\frac{\binom{k}{n}}{\binom{4N_r-1}{n}}A_n,$$

$$I_k(t) = 1-\sqrt{\frac{t}{1+t}}\left[1+\sum_{n=1}^{k}\frac{(2n-1)!!}{n!2^n(1+t)^n}\right].$$

Note $(2k-1)!!$ denotes the product of only odd integers from 1 to $2k-1$.

Using the closed-form expressions (5.32), (5.33), and (5.34), we can rewrite $P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s)$ as

Table 5.1. Distribution of u_s and v_s for **PF** scheme with QPSK

Type	u_s	v_s	b_1	b_2	b_3	b_4
II	2	2	64	0	0	0
	4	4	0	32	0	0
	6	6	0	0	32	0
III	0.343	11.657	0	0	16	0
	1.172	6.828	0	32	0	0
	2.343	13.657	0	0	0	8
	6.828	1.172	0	32	0	0
	11.657	0.343	0	0	16	0
	13.657	2.343	0	0	0	8

$$P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s) = \sum_{\mathbf{X}_s, \hat{\mathbf{X}}_s \in Type\ I} P_I(\mathbf{X}_s, \hat{\mathbf{X}}_s) + \sum_{\mathbf{X}_s, \hat{\mathbf{X}}_s \in Type\ II} P_{II}(\mathbf{X}_s, \hat{\mathbf{X}}_s) + \sum_{\mathbf{X}_s, \hat{\mathbf{X}}_s \in Type\ III} P_{III}(\mathbf{X}_s, \hat{\mathbf{X}}_s) \tag{5.35}$$

5.6 Union Bound of Bit Error Probability

In this section we will derive the union bound of the bit error probability (BEP) for the **PF** scheme in the presence of partial-band jamming. The union bound technique consists of computing an upper bound of the **PF** scheme error probability, which sums the contributions of the of the pairwise error probabilities over all error events. The BEP of the **PF** scheme in the presence of partial-band jamming is expressed as

$$BEP_{\mathcal{I}} \leq \frac{1}{n_b} \sum_{\mathbf{X}_s} \Big[\sum_{\hat{\mathbf{X}}_s \neq \mathbf{X}_s} P_{\mathcal{I}}(\mathbf{X}_s, \hat{\mathbf{X}}_s) \Big] p(\mathbf{X}_s), \tag{5.36}$$

where n_b is the number of bits of $\mathbf{X}_s$, and $p(\mathbf{X}_s)$ is the probability that $\mathbf{X}_s$ is transmitted.

For simplicity, we only consider symbol pair $\mathbf{X}_m = (x_{1,m}, x_{3,m})$ and assume that each QPSK symbol is equiprobable, such that $n_b = 4$ and $p(\mathbf{X}_s) = \frac{1}{16}$. The union

bound in terms of symbol pair $(x_{1,m}, x_{3,m})$ can be expressed as

$$BEP_{\mathcal{I}} \leq \frac{1}{64} \sum_{x_{1,m}, x_{3,m}} \Big[\sum_{\nu} P_{\mathcal{I}}(\mathbf{X}, \hat{\mathbf{X}}) \Big], \tag{5.37}$$

where $\nu \triangleq (\hat{x}_{1,m}, \hat{x}_{3,m}) \neq (x_{1,m}, x_{3,m})$. Similarly, the union bound can be derived for the BEP for symbols $x_{2,m}$ and $x_{4,m}$.

5.7 Numerical Evaluations and Simulations

In this section, we provide the numerical and the simulation results of the QO-STBC-OFDM system in the presence of partial-band noise jamming and frequency-selective fading.

We consider the QO-STBC with constellation rotation (CR) scheme (5.3), equipped with $N_t = 4$ transmit antennas and $N_r = 2$ receive antennas. QPSK modulation is used for symbol transmissions and $\phi = \pi/4$ is the rotation angle. In all simulations, the channels among different transmit and receive antenna pairs are assumed to be uncorrelated and the channel state information (CSI) of the transmitters and jamming power are perfectly known at the receivers. The channel coefficients are constant during one block of code transmission and independent from block to block. The total number of available subcarriers is $N_c = 256$ and the number of users is 16; therefore each user is assigned 16 subcarriers.

Figures 5.2 and 5.3 shows the BEP versus SNR performance of the numerical results and the simulation results of the QO-STBC with CR scheme. In Figure 5.2, the performance is evaluated in Rayleigh fading. From the figure, we observe that the theoretical performance is very close to the simulation results and serves as an upper bound.

In Figure 5.3, the QO-STBC with CR scheme is evaluated in Rayleigh fading and partial-band noise jamming with SIR=6dB, and $\alpha = 0.5$. Recall that jammer occupancy (α) is the fraction of symbol blocks that experience jamming. From the figure we can see that the performance limiting factor is the partial-band noise jamming and

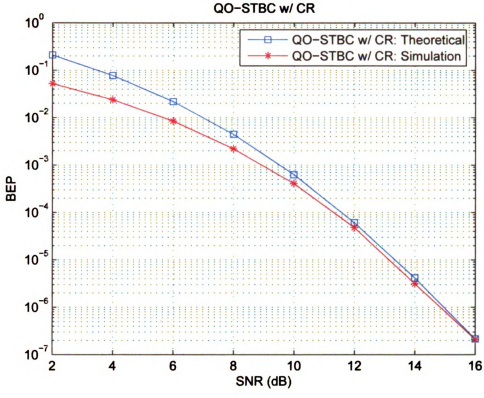

Figure 5.2. Union bound on the BEP and simulation results for QO-STBC with constellation rotation in frequency-selective fading ($N_r = 2$).

the union bound is tight. In Figure 5.4, the performance for various α is evaluated. From the figure, we observed that as α increases the BEP performance degrades.

Finally, in Figure 5.5, we compare the OSTBC scheme and the QO-STBC with constellation rotation scheme. Each scheme is equipped with 4 transmit antennas and 2 receive antennas. The BER performance is evaluated under Rayleigh fading and partial-band jamming with SIR=6dB and $\alpha = 0.5$. As shown in the figure, the QO-STBC with constellation rotation scheme significantly outperforms the OSTBC scheme.

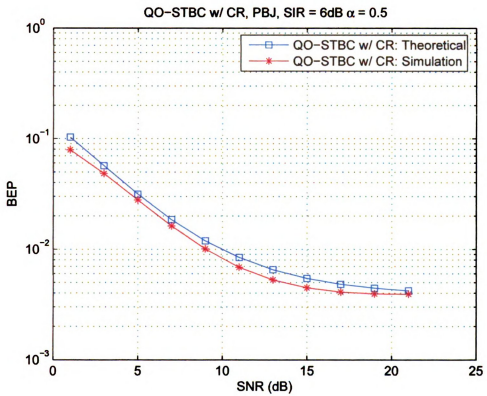

Figure 5.3. Union bound on the BEP and simulation results for QO-STBC with constellation rotation in partial-band noise jamming and frequency-selective fading ($N_r = 2$, $\alpha = 0.5$, SIR=6dB).

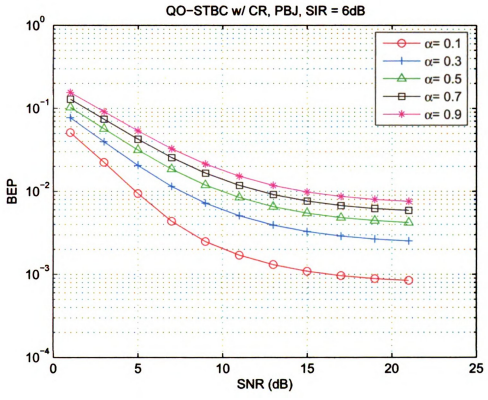

Figure 5.4. Union bound on the BEP for QO-STBC with constellation rotation in partial-band noise jamming and frequency-selective fading ($N_r = 2$, α = [0.1,0.3,0.5,0.7,0.9], SIR=6dB).

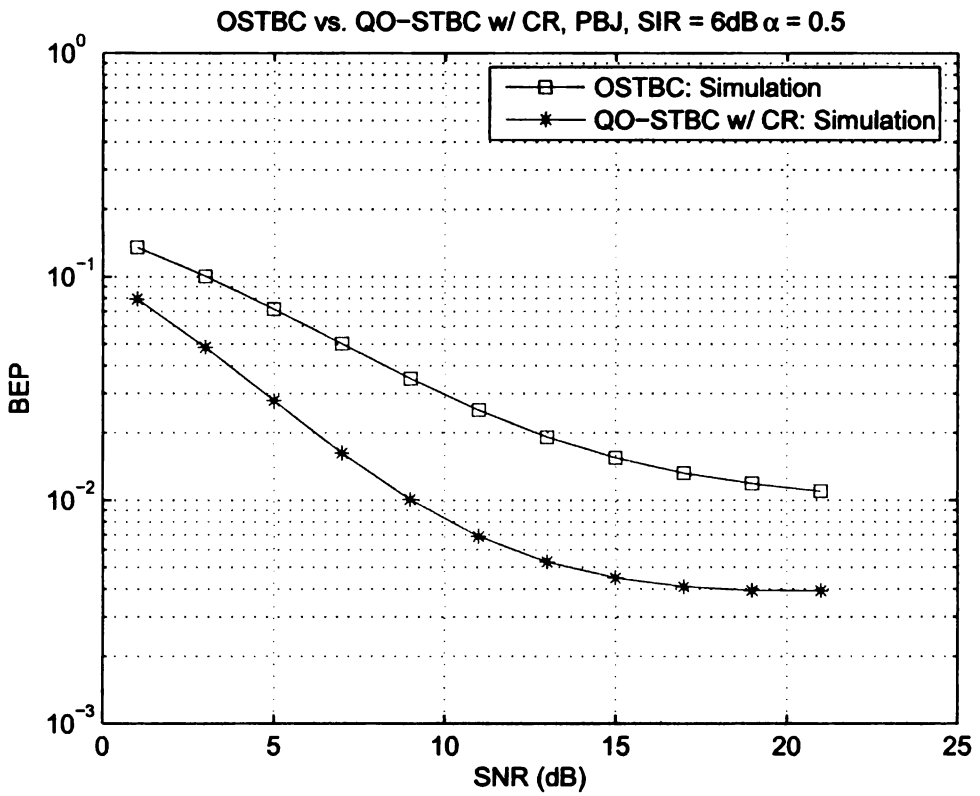

Figure 5.5. Comparison of OSTBC vs. QO-STBC with constellation rotation in rayleigh fading and partial-band noise jamming (SIR=6dB), $\alpha = 0.5$, and $N_r = 2$

5.8 Summary

In summary, the combination of QO-STBCs with OFDM can exploit multipath diversity and achieve spectrally efficient communications. However, future wireless communication systems must be robust against both unintentional and intentional interference. As a result, there is a need for proper analytical tools to assess the performance of QO-STBC-OFDM in the presence of partial-band noise jamming. In this chapter, we derived analytical expressions for the exact PEP of the QO-STBC-OFDM system using the moment generating function. We calculated the exact PEP under various situations, and derived the closed-form expressions and union bound for the bit error probability. Our numerical analysis and simulation results show that union bound is tight and the QO-STBC-OFDM system is effective in mitigating partial-band noise jamming.

CHAPTER 6

Conclusions and Future Work

6.1 Conclusions

In this dissertation, we investigated the efficiency and security of existing work, and enhanced the spectral efficiency and strengthened the inherent security of wireless systems by integrating advanced signal processing techniques and cryptographic techniques into the transmitter-receiver design. In summary, our spectrally efficient Alamouti scheme improves the code efficiency of the traditional Alamouti scheme by increasing the number of information bits transmitted in each Alamouti block; Our highly efficient anti-jamming system design for secure dynamic spectrum access control breaks through the bottleneck in developing high-capacity anti-jamming wireless communication systems.

On spectrally efficient Alamouti scheme:

- The code efficiency of the traditional Alamouti code is investigated from a bit-level perspective by introducing the concepts of *Alamouti patterns* and *irregular partitioning*. The investigation reveals room for spectrally efficiency enhancement.

- A novel spectrally efficient Alamouti scheme is proposed to improve the code efficiency of the traditional Alamouti scheme by transmitting more information bits than redundancy bits per Alamouti block, while achieving high transmit diversity. The receiver design of the proposed system allows maximum likelihood decoding for signal decoupling.

- There are no specific constraints of the spectrally efficient Alamouti scheme,

therefore the proposed scheme can be directly extended to any space-time block codes with more than two transmit antennas.

On highly efficient anti-jamming system design for secure dynamic spectrum access control:

- We developed a collision-free frequency hopping (CFFH) system, which is based on the orthogonal frequency division multiple access (OFDMA) framework and a new secure subcarrier assignment scheme, and proposed to enhance the anti-jamming properties of CFFH through joint space-time and frequency diversity.

- First, we analyzed the limitations in the recently proposed subcarrier assignment algorithm, and proposed a new subcarrier assignment scheme based on secure permutation algorithm. From a security perspective, the subcarrier assignment scheme based on secure permutation protects users against follower jamming attacks by preventing adversaries from determining the frequency hopping patterns.

- Second, we observed that although CFFH is very robust under partial-band jamming, it is still sensitive to random jamming. We propose to overcome this deficiency through space-time coding and introduce the space-time coded collision-free frequency hopping (STC-CFFH) system. The proposed STC-CFFH is found to be particularly powerful in eliminating both channel interference and hostile jamming interference.

- Finally, our analysis indicates that the proposed STC-CFFH scheme is both highly efficient and very robust under various jamming scenarios.

On quasi-orthogonal space-time block codes for jamming mitigation:

- The combination of quasi-orthogonal space-time block coding (QO-STBC) with constellation rotation exploits multipath diversity and achieves high speed high quality transmissions. However, such systems must co-exist with various forms of interference to provide reliable communication. Therefore, there is a need

for proper analytical tools to assess the performance of the QO-STBC with constellation rotation scheme in the presence of partial-band noise jamming.

- First, we derived analytical expressions for the exact pairwise error probability (PEP) of the QO-STBC orthogonal frequency division multiplexing (QO-STBC-OFDM) system using the moment generating function (MGF).
- Second, we calculated the exact PEP under various situations, and derived the closed-form expressions and union bound for the bit error probability (BEP).
- Our numerical analysis and simulation results show that the union bound is tight and the QO-STBC-OFDM system is effective in mitigating partial-band noise jamming.

6.2 Future Directions

For future research, we will look at secure communications and dynamic resource allocation in cognitive radio networks.

6.2.1 Cognitive Networks

The rapid increase of wireless networks have led to a shortage of a precious natural resource, radio electromagnetic spectrum. The shortage of spectrum has become more severe due to the outdated way the spectrum is managed. The Federal Communications Commission (FCC) allocates static spectrum to primary users for a fee. The use of static allocations causes spectrum holes. A spectrum hole is defined as a band of frequencies assigned to a primary user, but at a particular time and specific geographic location, the band is not utilized by the user [90]. This inefficient utilization of the spectrum has led to the rise of 802.11-based technologies that uses unlicensed spectrum. However, these unlicensed frequency bands have become over populated and interference among the different networks is the major deployment constraint. All of these factors have led to the need to make dramatic changes in the spectrum

management process, as existing policies are not capable of scaling with demand [91]. Furthermore, these factors have led to the concept of cognitive radio networks.

Cognitive radio network is an intelligent multiuser wireless communication system that is aware of its environment and uses the methodology of understanding-by-building to learn from the environment and adapt to statistical variations in the input stimuli with two primary objectives: (i) highly reliable communications; (ii) efficient utilization of the radio spectrum [92]. In other words, cognitive radio networks improve the spectrum utilization by making it possible for a secondary (unlicensed) user to access spectrum holes unoccupied by the primary users. Furthermore, cognitive radio networks are able to sense and predict interference patterns and adapt their spectrum access accordingly [93].

6.2.2 Major Challenges and Future Research Directions

The major challenges in existing cognitive radio networks are:

- **Spectral Inefficiency Due To Traffic Collisions:** The lack of network-centric scheduling on secondary users may cause collisions between other secondary users as well as collisions between primary users, leading to low efficiency and low system capacity.

- **Security Fragility:** Spectrum sensing enables the secondary user to perform legitimate traffic analysis of the primary user, including spectrum occupation, traffic volume, traffic patterns, and even traffic routing paths. Hostile jamming and privacy compromise can raise serious security problems in cognitive radio networks.

- **High Terminal Cost:** In cognitive radio, every individual terminal needs to perform continuous spectrum sensing, and be able to adapt to the unpredictable, ever changing environment. These operations require expensive hardware and software, which implies that the cost of each radio terminal will be high.

The future research directions are:

- **Architecture And Protocol Design For More Efficient Cognitive Networks:** We propose to increase spectral efficiency and system reliability through network-centric collision-free spectrum sharing, and to increase system flexibility and scalability through both fixed and dynamic base station deployment.

- **Cross-Layer Jamming Mitigation Techniques In Cognitive Networks:** We will consider jamming-resistant system design for both centralized as well as ad hoc networks consisting of cognitive radios. The jamming mitigation techniques will be investigated from both physical layer transceiver design as well as higher layer protocol development.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] I. Wong and B. Evans, *Resource Allocation in Multiuser Multicarrier Wireless Systems.* Springer Science Business Media, New York, NY, 2008.

[2] 3GAmericas, *World Cellular Technology Forecast 2006-2011*, 2007. [Online]. Available: http://www.3gamericas.org/English/Statistics/17.cfm

[3] *Total Midyear Population for the World: 1950-2050*, 2007. [Online]. Available: http://www.census.gov/ipc/www/worldpop.html

[4] *WORLD INTERNET USAGE AND POPULATION STATISTICS*, 2007. [Online]. Available: http://www.Internetworldstats.com/stats.htm

[5] P. Rysavy, *Mobile Broadband: EDGE, HSPA, and LTE*, 2006. [Online]. Available: http://3gamericas.org/pdfs/white_papers/2006_Rysavy_Data_Paper_FINAL_09.15.06.pdf

[6] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking.* Rome, Italy: ACM Press, July 2001, pp. 180–188.

[7] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," in *Proceedings of the Eighth Annual Workshop on Selected Areas in Cryptography*, Aug. 2001, pp. 1–24.

[8] A. Stubblefield, J. Ioannidis, and A. Rubin, "Using the Fluhrer, Mantin, and Shamir attack to break WEP," in *Proceedings of Network and Distributed System Security Symposium (NDSS).* Internet Society, 2002. [Online]. Available: http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/stubbl.pdf

[9] *IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std. 802.11.

[10] S. Houston, "Tone and noise jamming performance of a spread spectrum M-ary FSK and 2, 4-ary DPSK waveforms," in *Proceedings of IEEE National Aeorspace and Electronics Conference*, Dayton, Ohio, June 1975, pp. 51–58.

[11] L. Milstein, S. Davidovici, and D. Schilling, "The effect of multiple-tone interfering signals on a direct sequence spread spectrum communication system," *IEEE Transactions on Communications*, vol. 30, pp. 436–446, March 1982.

[12] K. Raju, T. Ristaniemi, J. Karhunen, and E. Oja, "Jammer suppression in DS-CDMA arrays using independent component analysis," *IEEE Transactions on Wireless Communications*, vol. 5, pp. 1–6, Jan. 2006.

[13] J.-W. Moon, J. Shea, and T. Wong, "Jamming estimation on block-fading channels," in *IEEE Military Communications Conference*, vol. 3, Nov. 2004, pp. 1310–1316.

[14] J. Tan and G. Stuber, "Multicarrier spread spectrum system with constant envelope: Antijamming, jamming estimation, multiuser access," *IEEE Transactions on Wireless Communications*, vol. 4, pp. 1527– 1538, July 2005.

[15] J.-W. Moon, J. Shea, and T. Wong, "Collaborative mitigation of partial-time jamming on nonfading channels," *IEEE Transactions on Wireless Communications*, vol. 5, pp. 1371–1381, June 2006.

[16] R. Pickholtz, D. Schilling, and L.B.Milstein, "Theory of spread spectrum communications - a tutorial," *IEEE Transactions on Communications*, vol. 30, pp. 855–884, May 1982.

[17] C. Cook and H. Marsh, "An introduction to spread spectrum," *IEEE Communications Magazine*, vol. 21, pp. 8–16, Mar. 1983.

[18] P. Crepeau, "Performance of FH/BFSK with generalized fading in worst case partial-band gaussian interference," *IEEE Journal on Selected Areas in Communications*, vol. 8, pp. 884–886, June 1980.

[19] M. Pursley and W. Stark, "Performance of Reed-Solomon coded frequency-hop spread-spectrum communications in partial-band interference," *IEEE Transactions on Communications*, vol. 33, pp. 767–774, Aug. 1985.

[20] W. Stark, "Coding for frequency-hopped spread-spectrum communication with partial-band interference-Part II: Coded performance," *IEEE Transactions on Communications*, vol. 33, pp. 1045–1057, Oct. 1985.

[21] D. Nicholson, *Spread Spectrum Signal Design: LPE and AJ Systems*, ser. Computer Science Press. Maryland: Rockville, 1988.

[22] L. Milstein, D. Schilling, R. Pickholtz, V. Erceg, M. Kullback, E. Kanterakis, D. Fishman, W. Biederman, and D. Salerno, "On the feasibility of a CDMA overlay for personal communication networks," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 10, pp. 655–668, May 1992.

[23] M. Simon, G. Huth, and A. Polydoros, "Differentially coherent detection of QASK for frequency-hopping systems–Part I: Performance in the presence of

a gaussian noise environment," *IEEE Transactions on Communications*, vol. 30, pp. 158–164, Jan. 1982.

[24] Y. Lam and P. Wittke, "Frequency-hopped spread-spectrum transmission with band-efficient modulations and simplified noncoherent sequence estimation," *IEEE Transactions on Communications*, vol. 38, pp. 2184–2196, Dec. 1990.

[25] J. Cho, Y. Kim, and K. Cheun, "A novel FHSS multiple-access network using M-ary orthogonal Walsh modulation," in *Proc. 52nd IEEE Veh. Technol. Conf.*, vol. 3, Sept. 2000, pp. 1134–1141.

[26] S. Glisic, Z. Nikolic, N. Milosevic, and A. Pouttu, "Advanced frequency hopping modulation for spread spectrum WLAN," *IEEE Journal on Selected Areas in Communications*, vol. 18, pp. 16–29, Jan. 2000.

[27] K. Choi and K. Cheun, "Maximum throughput of FHSS multiple-access networks using MFSK modulation," *IEEE Transactions on Communications*, vol. 52, pp. 426–434, Mar. 2004.

[28] K.-C. Peng, C.-H. Huang, C.-J. Li, and T.-S. Horng, "High-performance frequency-hopping transmitters using two-point delta-sigma modulation," *IEEE Transactions on Microwave Theory and Techniques*, vol. 52, pp. 2529–2535, Nov. 2004.

[29] K. Choi and K. Cheun, "Optimum parameters for maximum throughput of FHMA system with multilevel FSK," *IEEE Transactions on Vehicular Technology*, vol. 55, pp. 1485–1492, Sept. 2006.

[30] G. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell labs. Tech. J.*, vol. 1, pp. 41–59, 1996.

[31] I. Telatar, "Capacity of multi-antenna Gaussian channels," *Europ. Trans. Telecommun.*, pp. 585–595, Nov. 1999.

[32] G. Foschini and M. Gans, "On limits of wireless communicationss in a fading environment when using multiple antennas," *Wireless Personal Communications*, pp. 311–335, 1998.

[33] Y. Tsai and J. Chang, "Using frequency hopping spread spectrum technique to combat multipath interference in a multiaccessing environment," *IEEE Transactions on Vehicular Technology*, May 1994.

[34] C. Wong, R. Cheng, K. Letaief, and R. Murch, "Multiuser OFDM with adaptive subcarrier, bit and power allocatioin," *IEEE Journal of Selective Areas on Communications*, Oct 1999.

[35] H. Sari, *Orthogonal frequency-division multiple access with frequency hopping and diversity.* in *Multi-Carrier Spread Spectrum*, K. Fazel and G. P. Fettweis, Editors, Norwell, USA: Kluwer, 1997, pp. 57–68.

[36] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo codes," *in Proc. 1993 International Conference of Communications*, pp. 1064–1070, 1993.

[37] R. Gallager, *Low Density Parity Check Codes.* MIT Press, Cambridge, Massachusets, p. 1963.

[38] D. MacKay, "Near Shannon limit performance of low density parity check codes," *Electronics Letters*, pp. 1645–1646, August 1966.

[39] V. Tarokh, N. Seshadri, and A. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Information Theory*, pp. 744–765, March 1998.

[40] V. Tarokh, A. Naguib, N. Seshadri, and A. Calderbank, "Spacetime codes for high data rate wireless communication: performance criteria in the presence of channel estimation errors, mobility, and multiple paths," *IEEE Transactions on Communications*, p. 199207, February 1999.

[41] A. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Transactions on Information Theory*, p. 260269, April 1967.

[42] S. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, pp. 1451–1458, October 1998.

[43] V. Tarokh, H. Jafarkhani, and A. Calderbank, "Space-time block code from orthogonal designs," *IEEE Trans. Information Theory*, July 1999.

[44] H. Jafarkhani and F. Taherkhani, "Pseudo orghogonal designs as space-time block codes," in *Proc. Int. Symp. Advances in Wireless Communications*, Victoria, BC, Canada, September 2002.

[45] V. Tarokh, H. Jafarkhani, and A. Calderbank, "Space-time codes for high data rate wireless communication: Performance results," *IEEE Journal on Select Areas Communication*, pp. 451–460, March 1999.

[46] L. Dalton and C. Georghiades, "A full-rate, full-diversity four-antenna quasi-orthogonal space-time block code," *IEEE Transactions on Wireless Communications*, vol. 4, pp. 363–366, March 2005.

[47] G. Wang and X.-G. Xia, "On optimal multilayer cyclotomic space-time code designs," *IEEE Transactions on Information Theory*, vol. 51, pp. 1102–1135, March 2005.

[48] G. Golden, G. Foschini, R. Valenzuela, and P. Wolniansky, "Detection algorithm and initial laboratory results using V-BLAST space-time communication architecture," *Electron. Lett.*, vol. 35, pp. 14–16, January 1999.

[49] H. Jafarkhani, "A quasi-orthogonal space-time block code," *IEEE Transactions on Communications*, January 2001.

[50] O. Tirkkonen, A. Boariu, and A. Hottinen, "Minimal nonorthogonal rate 1 space-time block code for 3+ tx antennas," *IEEE International Symposium on Spread-Spectrum Techniques and Applications (ISSSTA)*, September 2000.

[51] C. Papadias and G. Foschini, "Capacity-approaching space-time codes for systems employing four transmitter antennas," *IEEE Transactions on Information Theory*, pp. 726–733, March 2003.

[52] O. Tirkkonen, "Optimizing space-time block codes by constellation rotations," *Finnish Wireless Communication Workshop*, pp. 59–60, 2001.

[53] N. Sharma and C. Papadias, "Improved quasi-orthogonal codes through constellation rotation," *IEEE Transactions on Communications*, pp. 332–335, March 2003.

[54] D. Dao and C. Tellambura, "Optimal rotations for quasi-orthogonal codes through constellation rotation," *IEEE Global Telecommunications Conference (Globecom)*, pp. 2317–2321, 2005.

[55] W. Su and X. Xia, "Quasi-orthogonal space-time block codes with full diversity," *IEEE Global Telecommunication Conference (Globecom)*, pp. 1098–1102, 2002.

[56] ——, "Signal constellations for quasi-orthogonal space-time block codes with full diversity," *IEEE Transactions on Information Theory*, pp. 2331–2347, October 2004.

[57] B. Hassibi and B. Hochwald, "High-rate codes that are linear in space and time," *IEEE Transactions on Information Theory*, pp. 1804–1824, July 2002.

[58] G. Golden, G. Foschini, R. Valenzuela, and P. Wolniansky, "Detection algorithm and initial laboratory results using V-BLAST space-time communication architecture," *Electron. Lett.*, pp. 14–16, Jan. 1999.

[59] G. Foschini, G. Golden, R. Valenzuela, and P. Wolniansky, "Simplified processing for high spectral efficiency wireless communication employing multi-element arrays," *IEEE Journal on Selected Areas in Communications*, pp. 1841–1852, Nov. 1999.

[60] V. Tarokh and H. Jafarkhani, "A differntial detection scheme for transmit diversity," *IEEE Journal on Selected Areas in Communications*, pp. 1169–1174, July 2000.

[61] H. Jafarkhani and V. Tarokh, "Multiple transmit antenna differential detection from generalized orthogonal designs," *IEEE Transactions on Information Theory*, pp. 2626–2631, Sept. 2001.

[62] M. Damen, A. Tewfik, and J. Belfiore, "A construction of space-time code based on number theory," *IEEE Transactions on Information Theory*, pp. 753–760, March 2002.

[63] J. Belfiore, G. Rekaya, and E. Viterbo, "The golden code: A 2 x 2 full-rate space-time code with non-vanishing determinants," *IEEE Transactions on Information Theory*, pp. 1432–1436, April 2005.

[64] H. E. Gamal and M. Damen, "Univeral space-time coding," *IEEE Transactions on Information Theory*, pp. 1097–1119, May 2003.

[65] Z. Chen, J. Yuan, and B. Vucetic, "Improved space-time trellis coded modulation scheme on slow rayleigh fading channels," *Electronics Letters*, pp. 440–441, March 2001.

[66] L. Lightfoot, L. Zhang, and T. Li, "Space-time coded collision-free frequency hopping in hostile jamming," *IEEE Military Communications Conference (MILCOM)*, November 2008.

[67] L. Lightfoot and T. Li, "Jamming mitigation using space-time coded collision-free frequency hopping," *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2717 - 2720, April 2009.

[68] L. Lightfoot, L. Zhang, J. Ren, and T. Li, "Secure collision-free frequency hopping for ofdma based wireless networks," *European Association for Signal Processing (EURASIP) Journal on Advances in Signal Processing*, August 2009.

[69] L. Lightfoot, J. Ren, L. Zhang, and T. Li, "Jamming-resilient subcarrier assignment for OFDMA based space-time coded systems," *IEEE Electro/Information Technology (EIT) Conference*, June 2009.

[70] C. Martin, E. Lemois, F. Buda, and D. Merel, "Description of a complete multi-carrier spread spectrum transmission chain for robust and discrete tactical communications," *IEEE Military Communication Conference*, pp. 942–946, October 2000.

[71] J. Nilsson and T. Giles, "Wideband multi-carrier transmission for military HF communication," *IEEE Military Communication Conference*, pp. 1046–1051, Nov. 1997.

[72] F. Dominique and J. Reed, "Robust frequency hop synchronisation algorithm," *Electronics Letters*, vol. 32, pp. 1450–1451, Aug. 1996.

[73] U. N. I. of Standards and Technology, *Federal Information Processing Standards Publication 197-Announcing the* ADVANCE ENCRYPTION STANDARD (AES), 2001. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[74] W. Burr, "Selecting the advance encryption standard," *IEEE Security and Privacy*, pp. 43–52, April 2003.

[75] J. Jang and K. Lee, "Transmit power adaptation for multiuser ofdm systems," *IEEE Journal of Selective Areas on Communications*, Feb. 2003.

[76] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, Feb. 1978.

[77] M. Ergen, S. Coleri, and P. Varaiya, "QoS aware adaptive resource allocation techniques for fair scheduling in OFDMA based broadband wireless access systems," *in Proceedings of IEEE Transactions on Broadcasting*, pp. 362–370, Dec. 2003.

[78] S. Elayoubi and B. Fourestie, "Performance evaluation of admission control and adaptive modulation in OFDMA WiMax systems," *in Proceedings of IEEE/ACM Transactions on Networking*, pp. 1200–1211, Oct. 2008.

[79] K. Lee and D. Williams, "A space-frequency transmitter diversity technique for ofdm systems," *in Proceedings of IEEE Global Communications Conference*, pp. 1473–1477, Nov. 2000.

[80] B. Vucetic and J. Yuan, *Space Time Coding.* John Wiley and Sons, Ltd., ch. Space Time Coding Peformance Analysis and Code Design, p. 2003.

[81] J. Park, D. Kim, C. Kang, and D. Hong, "Effect of partial band jamming on ODFM-based WLAN in 802.11g," *IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. 560–563, April 2003.

[82] T. Rappaport, *Wireless Communications*, 2nd ed. Prentice Hall, 2002.

[83] C. Esli and H. Delic, "Antijamming performance of space-frequency coding in partial-band noise," *IEEE Transactions on Vehicular Technology*, pp. 466–476, March 2006.

[84] L. Lightfoot, L. Zhang, and T. Li, "Performance of qo-stbc-ofdm in partial-band noise jamming," *Conference on Information Science and Systems (CISS)*, March 2010.

[85] A. Sezgin, E. Jorswieck, and H. Boche, "Performance criteria analysis and further performance results for quasi-orthogonal space-time block codes," *IEEE International Symposium on Signal Processing and Information Technology*, pp. 102–105, December 2003.

[86] J. Yang, X. Jin, J. No, and D. Shin, "On the error probability of quasi-orthogonal space-time block codes," *International Journal Of Communication Systems*, pp. 1033–1045, May 2008.

[87] J. Craig, "A new, simple and exact result for calculating the probability of error for two-dimensional signal constellations," *IEEE Military Communication Conference*, pp. 571–575, October 1991.

[88] G. Turin, "The characteristic function of hermitain quadratic forms in complex normal variables," *Biometrika Trust*, pp. 199–201, 1960.

[89] M. Simon and M. Alouini, *Digital Communication over Fading Channels.* John Wiley and Sons, Ltd., 2005, ch. Appendix 5A.

[90] P. Kolodzy, "Next generation communications: Kickoff meeting," *in Proc. DARPA*, October 2001.

[91] J. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," *IEEE Cognitive Radio Oriented Wireless Networks and Communications*, pp. 1–7, May 2008.

[92] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, pp. 201–220, February 2005.

[93] S. Geirhofer, J. Sun, L. Tong, and B. M. Sadler, "Cognitive frequency hopping based on interference prediction: theory and experimental results," *ACM SIGMOBILE Mobile Computing and Communications Review*, pp. 49–61, April 2009.