EFFICIENT AND SECURE SYSTEM DESIGN IN WIRELESS COMMUNICATIONS

By

Tianlong Song

A DISSERTATION

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

Electrical Engineering - Doctor of Philosophy

2016

ABSTRACT

EFFICIENT AND SECURE SYSTEM DESIGN IN WIRELESS COMMUNICATIONS

By

Tianlong Song

Efficient and secure information transmission lies in the core part of wireless system design and networking. Comparing with its wired counterpart, in wireless communications, the total available spectrum has to be shared by different services. Moreover, wireless transmission is more vulnerable to unauthorized detection, eavesdropping and hostile jamming due to the lack of a protective physical boundary.

Today, the two most representative highly efficient communication systems are CDMA (used in 3G) and OFDM (used in 4G), and OFDM is regarded as the most efficient system. This dissertation will focus on two topics: (1) Explore more spectrally efficient system design based on the 4G OFDM scheme; (2) Investigate robust wireless system design and conduct capacity analysis under different jamming scenarios. The main results are outlined as follows.

First, we develop two spectrally efficient OFDM-based multi-carrier transmission schemes: one with message-driven idle subcarriers (MC-MDIS), and the other with message-driven strengthened subcarriers (MC-MDSS). The basic idea in MC-MDIS is to carry part of the information, named carrier bits, through idle subcarrier selection while transmitting the ordinary bits regularly on all the other subcarriers. When the number of subcarriers is much larger than the adopted constellation size, higher spectral and power efficiency can be achieved comparing with OFDM. In MC-MDSS, the idle subcarriers are replaced by strengthened ones, which, unlike idle ones, can carry both carrier bits and ordinary bits. Therefore, MC-MDSS achieves even higher spectral efficiency than MC-MDIS.

Second, we consider jamming-resistant OFDM system design under full-band disguised jamming, where the jamming symbols are taken from the same constellation as the infor-

mation symbols over each subcarrier. It is shown that due to the symmetricity between the authorized signal and jamming, the BER of the traditional OFDM system is lower bounded by a modulation specific constant. We develop an optimal precoding scheme, which minimizes the BER of OFDM systems under full-band disguised jamming. It is shown that the most efficient way to combat full-band disguised jamming is to concentrate the total available power and distribute it uniformly over a particular number of subcarriers instead of the entire spectrum. The precoding scheme is further randomized to reinforce the system jamming resistance.

Third, we consider jamming mitigation for CDMA systems under disguised jamming, where the jammer generates a fake signal using the same spreading code, constellation and pulse shaping filter as that of the authorized signal. Again, due to the symmetricity between the authorized signal and jamming, the receiver cannot really distinguish the authorized signal from jamming, leading to complete communication failure. In this research, instead of using conventional scrambling codes, we apply advanced encryption standard (AES) to generate the security-enhanced scrambling codes. Theoretical analysis shows that: the capacity of conventional CDMA systems without secure scrambling under disguised jamming is actually zero, while the capacity can be significantly increased by secure scrambling.

Finally, we consider a game between a power-limited authorized user and a power-limited jammer, who operate independently over the same spectrum consisting of multiple bands. The strategic decision-making is modeled as a two-party zero-sum game, where the payoff function is the capacity that can be achieved by the authorized user in presence of the jammer. We first investigate the game under AWGN channels. It is found that: either for the authorized user to maximize its capacity, or for the jammer to minimize the capacity of the authorized user, the best strategy is to distribute the power uniformly over all the available spectrum. Then, we consider fading channels. We characterize the dynamic relationship between the optimal signal power allocation and the optimal jamming power allocation, and propose an efficient two-step water pouring algorithm to calculate them.

Dedicated to my dear parents and to my beloved wife.

ACKNOWLEDGMENTS

I would like to express my sincere appreciation and gratitude to my advisor, Dr. Tongtong Li, for her guidance and support throughout the years of my PhD studies at Michigan State University. It is a great honor to have worked with Dr. Li, from whom I learned far more beyond the rich knowledge only, but also including a great attitude towards research and life. Since years ago, she has become an important influencer of my life, and she will continue to be the one along my lifelong career path.

I would also like to thank Dr. Selin Aviyente, Dr. Guoliang Xing and Dr. Hayder Radha on my committee for their helpful comments and insightful discussions throughout my PhD program. Special gratitude should also be shown to Dr. Jian Ren, who helped me by both insightful academic inputs and precious daily life advices.

Besides, I would not have enjoyed my PhD life without my labmates: Mai Abdelhakim, Xiaochen Tang, Zhe Wang, Ahmed Alahmadi, Zhaoxi Fang, Kai Zhou, Yuan Liang and Run Tian. It was those guys who accompanied me through the last few years with their academic inputs and sincere laughter.

My profound gratitude is to my parents. I could not be more grateful to them for their endless love, care, and encouragement. They have always been motivating me to advance in both my study and becoming their "bigger" boy.

I could not be more grateful to my wife, Jing, for being always standing aside and supporting me. We met and married in this small town, have been caring and loving each other ever since. She helped and supported me through many difficult times, and I could not have accomplished all these things without her. I wish our love which started during my PhD study will continue to flourish in the future anywhere we stay.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

Along with the global wise commercialization of the third generation (3G) and fourth generation (4G) standards in the 21st century, wireless communications have moved into a new era of high-speed multimedia connections with seamless coverage and excellent mobility support. Comparing with its wired counterpart, in wireless communications, the total available spectrum has to be shared by different services. Moreover, wireless transmission is more vulnerable to unauthorized detection, eavesdropping, and hostile jamming due to the lack of a protective physical boundary. As a result, efficient and secure information transmission lies in the core part of wireless system design and networking.

Today, the two most representative highly efficient communication systems are code division multiple access (CDMA, used in 3G) and orthogonal frequency division multiplexing (OFDM, used in 4G), and OFDM is regarded as the most efficient system. Motivated by these observations, this dissertation will focus on two topics: (1) Explore more spectrally efficient system design based on the 4G OFDM scheme; (2) Investigate robust wireless system design and conduct capacity analysis under different jamming scenarios.

In this chapter, first, we will revisit the design principle of the OFDM system, which is considered to be the most efficient system today, and discuss the possibility of achieving higher efficiency than ODFM through innovative transceiver design. Second, we will review the limitations of existing systems under hostile jamming, and explore possible approaches to address these limitations. Third, we provide an overview to the major contributions of

this dissertation.

1.1 Spectral Efficiency of Traditional OFDM Systems

Formally, the spectral efficiency η is defined as the ratio of the information bit rate R_b (bits/s) to the transmission bandwidth W (Hz), i.e., $\eta = \frac{R_b}{W}$ (bits/s/Hz). Given the fact that the total available spectrum remains constant, to accommodate more users and services without compromising the service quality, it is critical to increase the spectral efficiency of wireless communication systems.

In conventional multicarrier transmission systems, spectral overlaps between neighboring carriers are usually avoided to eliminate inter-carrier interference (ICI). When it was realized that the spectral efficiency could be significantly increased by allowing spectral overlaps between orthogonal subcarriers [1], especially after a low-cost implementation using inverse fast Fourier transform/fast Fourier transform (IFFT/FFT) blocks was proposed [2], OFDM has become one of the most effective ways in modern communications and is adopted by many recent standards [3], e.g., long term evolution (LTE) [4] and worldwide interoperability for microwave access (WiMAX) [5]. Besides the robustness to multipath fading over frequency selective channels [6], the very first advantage making OFDM prevalent is its high spectral efficiency, which is so far believed to be the highest due to the wisely introduced spectral overlap. However, there is always a question which greatly attracts the interest of many researchers: can the efficiency of a system be even higher than OFDM?

In this research, we will provide a positive answer to the question above. More specifically, we will incorporate the idea of message-driven frequency hopping (MDFH) [7] into OFDM systems by transmitting extra information through message-driven subcarrier selection.

1.2 Limitations of Existing Systems under Hostile Jamming

The malicious jammer can intentionally interfere the legitimate user's communication by saturating the receiver with noise or false information through deliberate radiation of radio signals [8, 9]. Hostile jamming is an effective way to carry out denial-of-service (DoS) attack and is often used in military fields. However, with the advent of reconfigurable cognitive radios widely available, hostile jamming attack is much easier to launch and has become an urgent and serious threat to civilian communications as well [10–12]. In the following, we will: (i) examine the jamming resistance of traditional OFDM systems; (ii) identify the limitations of traditional CDMA systems; and (iii) discuss the challenges from an even more severe jamming case - cognitive jamming.

1.2.1 Jamming Resistance of Traditional OFDM Systems

For a long time, research on communication system design has been focused on capacity improvement under non-intentional interference, such as intersymbol interference, multiuser interference and noise. Most of the communication systems today, such as OFDM, do not really have anti-jamming features. Their jamming resistance mainly relies on the diversity introduced by error control coding. On the other hand, jamming has widely been modeled as Gaussian noise. Based on the noise jamming model and the Shannon capacity formula, $C = B\log_2(1 + SNR)$, an intuitive impression is that jamming is really harmful only when the jamming power is much higher than the signal power.

However, this is only partially true. To show it, we need to take a look at disguised jamming [13–15], where the jamming is highly correlated with the signal, and has a power

level close or equal to the signal power. Disguised jamming can be much more harmful than noise jamming, since it can reduce the system capacity to zero even when the jamming power equals the signal power. Consider the example, for each subcarrier in OFDM transmission, $y = s + j + n$, where s is the authorized signal, j is the jamming, n is the noise independent of j and s, and y is the received signal. If j and s are taken randomly and independently from the same constellation Ω, then it can be proved [16] that *the capacity of the system is zero*! The reason behind it is that: due to the symmetricity between the jamming and the authorized signal, the receiver is fully confused and cannot really distinguish the authorized signal from jamming. Moreover, the result cannot be changed by applying the conventional bit-level channel coding. From this example, we can see that *the traditional OFDM systems are facing much more serious threats from hostile jamming than we had thought.*

In this research, we will develop an optimal precoding scheme to minimize the BER of OFDM systems under full-band disguised jamming. Furthermore, the precoding scheme is randomized to protect the OFDM transmission from a follower fashion of disguised jamming.

1.2.2 Limitations of Traditional CDMA Systems

Existing work on anti-jamming system design or jamming mitigation is mainly based on spread spectrum techniques [17–25]. Two techniques are often employed for spread spectrum systems: direct sequence spread spectrum (DSSS, also known as CDMA) and frequency hopping spread spectrum (FHSS). The CDMA systems have been successfully incorporated into the 3G wireless communication standards, while FH systems are widely adopted in military applications. There are a lot of variants and hybrids of these two techniques that have been developed, but their performances generally do not differ significantly from the two basic techniques. Both FH and CDMA systems gain anti-jamming features by exploiting

frequency diversity over large spectrum [26]. The FH systems have been extensively studied in [7, 10, 15, 27], where several effective approaches were proposed to improve the spectral efficiency and anti-jamming features of FH systems. As a result, we will focus on CDMA systems hereinafter.

In CDMA, each user is assigned a specific pseudo-random code (also known as the signature) to spread its signal energy over a bandwidth N times larger. Due to the spread spectrum, CDMA is especially robust under narrow band jamming. CDMA signals cannot be recovered unless the user signature is known at the receiver, and can be hidden within the noise floor, making it difficult to be detected. The security of CDMA relies on the randomness in the PN sequence used for scrambling after the spreading process. The spreading code of each user is obtained through the modulo 2 sum of the Walsh code and the PN sequence, and thus is varying in every symbol period. So how safe is the PN sequence? What would be the result if it is broken?

According to the Berlekamp-Massey algorithm [28], for a sequence generated from an n-stage linear feedback shift register (LFSR), the characteristic polynomial and the entire sequence can be reconstructed if an eavesdropper can intercept a $2n$-bit sequence segment. Note that the characteristic polynomial is generally available to the public, then PN sequence can be recovered if an n-bit sequence segment is intercepted. That is, it is possible to break the PN sequence used in conventional CDMA systems in real time with today's high speed computing techniques [29].

Once the PN sequence is recovered or broken, the jammer can then launch disguised jamming. More specifically, the jammer can transmit a different signal from the same constellation using the recovered spreading code of the authorized user. As a result, the authorized user's signal is completely jammed. In summary, due to the security weakness of the PN

sequences, existing CDMA systems are fragile under hostile jamming, especially disguised jamming.

In this research, we will propose two approaches to make CDMA systems robust against disguised jamming: (i) Robust receiver design by exploiting the small timing differences between the authorized signal and the jamming; (ii) Secure scrambling by encrypting the PN sequence using advanced encryption standard (AES).

1.2.3 Challenges from Cognitive Jamming

When a jammer applies a constant jamming strategy, the jamming is said to be *static*. However, a smart jammer equipped with a receiver can capture the transmitted signal of the authorized user. With sufficient intelligence, the smart jammer can determine the transmission scheme used by the authorized user in real time, and adjust the jamming strategy accordingly to maximize the jamming effect. The jamming generated by the smart jammer is called *cognitive jamming*, also known as adaptive jamming or time-varying jamming [10].

In traditional research on jamming mitigation, there is generally an assumption that the jamming either is static or varies slowly such that the authorized user has sufficient time to track and react to the jamming. However, if the jammer is intelligent and can switch its patterns fast enough, then it would be impossible for the authorized user to detect and react in real time. In this case, the authorized user and the jammer are actually acting independently of each other. Regarding this scenario, there has been a surge in research that applies game theory to characterize and analyze the uncertainties in communication systems with cognitive jamming or interference.

Motivated by these observations, in this research, we will consider multiband communications under the presence of fast cognitive jamming, and investigate the optimal transmission

strategy (as well as jamming strategy) using game theory.

1.3 Overview of the Dissertation

In this dissertation, there are three major contributions: (1) To improve the spectral efficiency of the OFDM systems, we incorporate the idea of message-driven frequency hopping [7] into OFDM systems by transmitting extra information through message-driven subcarrier selection; (2) To enhance the anti-jamming features of OFDM and CDMA systems, we introduce security-enhanced shared randomness between transmitters and receivers by integrating cryptographic techniques into the physical layer transceiver design; (3) To combat fast cognitive jamming in multiband communications, taking jamming and jamming mitigation as a two-party zero-sum game, we investigate the optimal transmission and jamming strategies using game theory. More specifically, this dissertation is organized as follows.

Chapter 2 develops two spectrally efficient OFDM-based multi-carrier transmission schemes: one with message-driven idle subcarriers (MC-MDIS), and the other with message-driven strengthened subcarriers (MC-MDSS). The basic idea in MC-MDIS is to carry part of the information, named carrier bits, through idle subcarrier selection while transmitting the ordinary bits regularly on all the other subcarriers. When the number of subcarriers is much larger than the adopted constellation size, higher spectral and power efficiency can be achieved comparing with OFDM. The reason is that each idle subcarrier carries more bits than a regular symbol, with no power consumption. Moreover, the existence of idle subcarriers can also decrease possible inter-carrier interference (ICI) between their neighboring subcarriers. In MC-MDSS, the idle subcarriers are replaced by strengthened ones, which, unlike idle ones, can carry both carrier bits and ordinary bits. Therefore, MC-MDSS

achieves even higher spectral efficiency than MC-MDIS. We further enhance the security of these two schemes under eavesdropping and partial-band jamming through secure subcarrier assignment and secure symbol mapping, which actually perform symbol-level encryption.

Chapter 3 considers jamming-resistant OFDM system design under full-band disguised jamming, where the jamming symbols are taken from the same constellation as the information symbols over each subcarrier. First, we analyze the impact of disguised jamming on OFDM systems. It is shown that due to the symmetricity between the authorized signal and jamming, the BER of OFDM systems without symbol-level precoding or only with repeated symbol-level coding is lower bounded by a modulation specific constant, which cannot be improved by increasing SNR. Second, we develop an optimal precoding scheme, which minimizes the BER of OFDM systems under full-band disguised jamming. It is shown that the most efficient way to combat full-band disguised jamming in OFDM systems is to concentrate the total available power and distribute it uniformly over a particular number of subcarriers instead of the entire spectrum. The precoding scheme is further randomized to protect the OFDM communication from a follower fashion of disguised jamming.

Chapter 4 considers jamming mitigation for CDMA systems under disguised jamming, where the jammer generates a fake signal using the same spreading code, constellation and pulse shaping filter as that of the authorized signal. First, we analyze the performance of conventional CDMA systems under disguised jamming, and show that due to the symmetricity between the authorized signal and the jamming interference, the receiver cannot really distinguish the authorized signal from jamming, leading to complete communication failure. Second, for CDMA systems with public codes which cannot be concealed for some reason, we mitigate the disguised jamming through robust receiver design. By exploiting the small time difference between the authorized signal and the jamming interference, the conventional

CDMA receiver can be re-designed to achieve robust performance under disguised jamming. Third, for CDMA systems which allow code concealment, we mitigate disguised jamming using secure scrambling. Instead of using conventional scrambling codes, we apply AES to generate the security-enhanced scrambling codes. Theoretical analysis shows that: the capacity of conventional CDMA systems without secure scrambling under disguised jamming is actually zero; however, the capacity can be significantly increased when the CDMA systems are protected using secure scrambling.

Chapter 5 considers a game between a power-limited authorized user and a power-limited jammer, who operate independently over the same spectrum consisting of multiple bands. The strategic decision-making of the authorized user and the jammer is modeled as a two-party zero-sum game, where the payoff function is the capacity that can be achieved by the authorized user in presence of the jammer. First, we investigate the game under additive white Gaussian noise (AWGN) channels. We explore the possibility for the authorized user or the jammer to randomly utilize part (or all) of the available spectrum and/or apply nonuniform power allocation. It is found that: under AWGN channels, either for the authorized user to maximize its capacity, or for the jammer to minimize the capacity of the authorized user, the best strategy is to distribute the transmission power or jamming power uniformly over all the available spectrum. The minimax capacity can be calculated based on the channel bandwidth and the signal-to-jamming and noise ratio, and it matches with the Shannon channel capacity formula. Second, we consider frequency selective fading channels. We characterize the dynamic relationship between the optimal signal power allocation and the optimal jamming power allocation in the minimax game, and propose an efficient two-step water pouring algorithm to find the optimal power allocation schemes for both the authorized user and the jammer.

Chapter 6 summarizes the contributions and concludes the dissertation. An outline of future work is also provided.

Chapter 2

Spectrally Efficient Multicarrier Transmission with Message-Driven Subcarrier Selection

In this chapter, we develop two spectrally efficient OFDM-based multicarrier transmission schemes: one with message-driven idle subcarriers (MC-MDIS), and the other with message-driven strengthened subcarriers (MC-MDSS). The basic idea in MC-MDIS is to carry part of the information, named carrier bits, through idle subcarrier selection while transmitting the ordinary bits regularly on all the other subcarriers. When the number of subcarriers is much larger than the adopted constellation size, higher spectral and power efficiency can be achieved comparing with OFDM. In MC-MDSS, the idle subcarriers are replaced by strengthened ones, which, unlike idle ones, can carry both carrier bits and ordinary bits. Therefore, MC-MDSS achieves an even higher spectral efficiency than MC-MDIS. We further enhance the security of these two schemes under eavesdropping and partial-band jamming through secure subcarrier assignment and secure symbol mapping, which actually perform symbol-level encryption.

2.1 Introduction

In conventional multicarrier transmission systems, spectral overlaps between neighboring carriers are usually avoided to eliminate inter-carrier interference (ICI). When it was realized that the spectral efficiency could be significantly increased by allowing spectral overlaps between orthogonal subcarriers [1], especially after a low-cost implementation using IFFT/FFT blocks was proposed [2], orthogonal frequency division multiplexing (OFDM) has become one of the most effective ways in modern communications and is adopted by many recent standards [3], e.g., LTE [4] and WiMAX [5]. Besides the robustness to multipath fading over frequency selective channels [6], the very first advantage making OFDM prevalent is its high spectral efficiency, which is so far believed to be the highest due to the wisely introduced spectral overlap. However, there is always a question which greatly attracts the interest of many researchers: can the efficiency of a system be even higher than OFDM?

In literature, researchers have proposed to improve the efficiency of OFDM through cyclic prefix (CP) optimization [30–33]. Here we take a different perspective and introduce two highly efficient OFDM-based multicarrier transmission schemes, which offer a positive answer to the question above. Our approaches are motivated by the idea of embedding information in channel state control [7,34–36], of which the concept of message-driven frequency hopping (MDFH) [7] gives us the most direct inspiration. In MDFH, besides carrying ordinary bits as usual, the active hopping carrier itself is specified by additional information bits and recovered by a filter bank at the receiver. Refined versions of MDFH were proposed and analyzed in [15,27,37,38]. For MDFH, transmission through hopping frequency control adds another dimension to the signal space, and the resulted coding gain can increase the spectral efficiency of conventional frequency hopping (FH) systems [39] by multiple times. This

motivates us to improve the spectral efficiency of OFDM by allowing part of the information bits being transmitted through carrier frequency selection.

First, we propose a multicarrier transmission scheme with message-driven idle subcarriers (MC-MDIS). The basic idea is to use part of the information bits, named carrier bits, to specify idle subcarriers while transmitting ordinary bits regularly on all the other subcarriers. In this way, if the number of subcarriers is much larger than the adopted constellation size (e.g., in most OFDM systems), we can transmit more information bits at an even lower power consumption. This is because the number of carrier bits transmitted through each idle subcarrier is more than that of the ordinary bits carried by each regular symbol, and all the carrier bits are transmitted with no power consumption through idle subcarrier selection. When applied to the OFDM framework, i.e., using orthogonal subcarriers and IFFT/FFT blocks, MC-MDIS can achieve an even higher spectral efficiency than OFDM, while keeping a higher power efficiency. The existence of idle subcarriers can also decrease possible inter-carrier interference (ICI) between their neighboring subcarriers. We would like to point out that, under very low SNRs, an error in idle subcarrier detection may lead to possible bit vector disorder, since the location of the idle subcarrier has a great impact on bit vector reorganization. However, this issue is properly resolved by a bit vector rearrangement (BVR) algorithm, which can be implemented with no sacrifice on spectral efficiency.

An alternative scheme, with message-driven strengthened subcarriers (MC-MDSS), is proposed simply by replacing the idle subcarriers in MC-MDIS with strengthened ones. In MC-MDSS, different from MC-MDIS, the strengthened subcarriers selected by the carrier bits can also carry ordinary bits. This leads to two advantages: 1) Higher spectral efficiency can be achieved than MC-MDIS due to the additional ordinary bits transmitted on the strengthened subcarriers; 2) The bit-vector-disorder issue is automatically resolved, resulting

in simpler transceiver design.

To enhance the security of the proposed schemes under eavesdropping and partial-band jamming, we further implement secure subcarrier assignment (SSA) and secure symbol mapping (SSM) in both MC-MDIS and MC-MDSS. Besides working as an effective way in subcarrier grouping to maximize the two schemes' spectral efficiency, SSA shuffles and groups all the available subcarriers dynamically and secretly such that: 1) The eavesdroppers cannot recover the carrier bits, even if they successfully locate the idle subcarriers. For the ordinary bits, they cannot sort the bits in the right order, even if they can recover them from the symbols correctly. 2) Burst errors caused by partial-band jamming can be randomized by SSA and thus reduced to the correction range of the error-control coding. 3) No follower jamming can be launched toward any particular users.

In addition to secure subcarrier assignment (SSA), secure symbol mapping (SSM) offers a dynamic and secret symbol mapping scheme, which further prevents the eavesdroppers from trying to sort the ordinary bits correctly or break SSA reversely by exploiting information redundancy [40]. Both SSM and SSA can be viewed as symbol-level encryption, which performs encryption in symbol generation and subcarrier grouping rather than conducting bit-level encryption. Compared with bit-level encryption, symbol-level encryption using SSA and SSM results in smaller processing delays. The underlying argument is that, with SSA and SSM, encryption/decryption can be performed in parallel, rather than in series, with modulation/demodulation.

This chapter is organized as follows. In Section 2.2, the system structure of MC-MDIS is provided. In Section 2.3, we introduce MC-MDSS. Secure subcarrier assignment and secure symbol mapping are discussed in Section 2.4. Analytical performance evaluation is presented in Section 2.5. Simulation results are provided in Section 2.6 and we conclude in Section 2.7.

2.2 Multicarrier Transmission with Message-Driven Idle Subcarriers (MC-MDIS)

The main idea of MC-MDIS, which distinguishes itself from MDFH [7, 15, 27, 37, 38], is that part of the information bits are used to select the idle subcarriers instead of active subcarriers. The active subcarriers carry ordinary bits as usual, while for the idle ones, we transmit the carrier bits without power consumption. The essential difference between MC-MDIS and MDFH lies in: 1) MDFH only transmits information through a few selected subcarriers while keeping most subcarriers idle, leading to a lower spectral efficiency; 2) MC-MDIS is actually a "flipped" version of MDFH, which activates most of the subcarriers to transmit regular information with even the remaining idle ones carrying extra information through idle subcarrier selection, and therefore achieving a high spectral efficiency. We implement MC-MDIS through the OFDM framework to maximize the spectral efficiency.

2.2.1 Transmitter Design

Let N_c be the total number of available subcarriers, with $\{f_0, f_1, ..., f_{N_c-1}\}$ being the set of all available subcarrier frequencies. Here we assume N_c is exactly a power of 2 for the convenience of OFDM implementation. All the N_c subcarriers are uniformly divided into N_g groups[1]. Within each group, there is only one idle subcarrier and the rest will carry regular symbols as usual. The number of subcarriers in each group would be $N_f = \frac{N_c}{N_g}$, and the number of bits required to specify the idle subcarrier in each group is $B_c = \log_2 N_f = \log_2 \frac{N_c}{N_g}$. We name the bits used to specify idle subcarriers as *carrier bits*, and then the total

[1]It is shown in Section 2.5.1 and Appendix A how to properly choose N_g and why the uniform grouping strategy is optimal in terms of spectral efficiency maximization.

number of carrier bits in all groups would be $N_g B_c = N_g \log_2 \frac{N_c}{N_g}$.

Let Ω be the selected constellation that contains M symbols, and each symbol in the constellation represents $B_s = \log_2 M$ bits. We name the bits carried in regular symbols as *ordinary bits*, and the total number of ordinary bits carried on all the active subcarriers is $(N_c - N_g)B_s = (N_c - N_g)\log_2 M$.

We divide the data stream into blocks of length $L = N_g B_c + (N_c - N_g)B_s$. Each block is partitioned into N_g groups and each group contains $B_c + (N_f - 1)B_s$ bits. The information block structure is shown in Fig. 2.1. We will transmit the entire block I_n, which contains L bits, in one single OFDM symbol period.

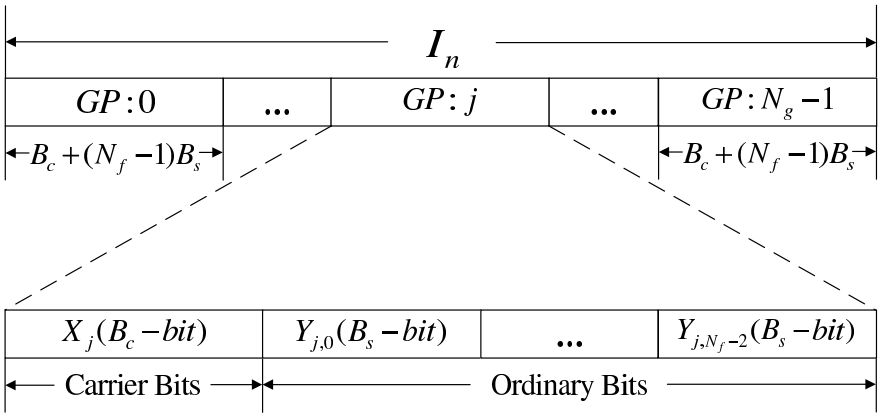


Figure 2.1: Information block structure for MC-MDIS.

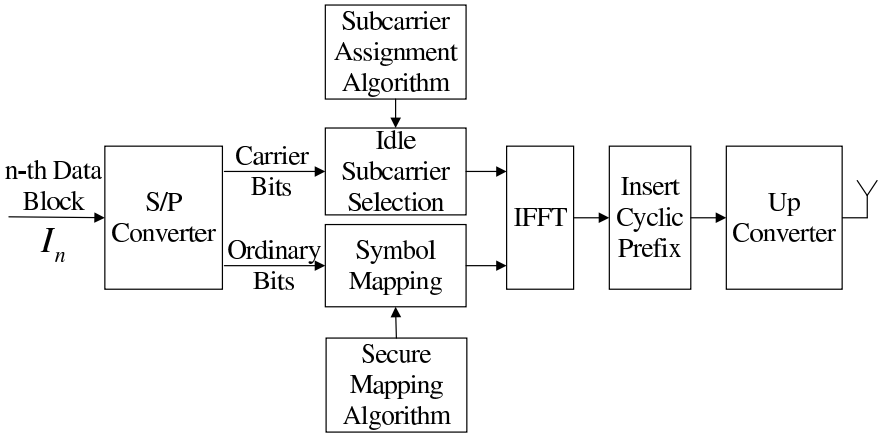


Figure 2.2: Transmitter structure of MC-MDIS.

The transmitter structure is shown in Fig. 2.2. According to the information block structure, the Serial-to-Parallel (SP) converter fetches carrier bits and ordinary bits from the information block. The carrier bits are used to determine the idle subcarrier in each subcarrier group. The index of the idle subcarrier in the jth group, k_j, can be calculated by converting the carrier bit vector, X_j, into a decimal value, where X_j is the carrier bit vector corresponding to the idle subcarrier in the jth group. The ordinary bits are mapped to symbols which are carried by the active subcarriers.

Once the idle subcarriers and regular symbols are determined, we transmit the carrier bits and ordinary bits using the OFDM framework [2]. For each subcarrier, assign a zero symbol if it is idle; otherwise assign a regular symbol obtained through the bit-to-symbol mapping. If the subcarrier grouping is a direct segmentation of $\{0, 1, ..., N_c - 1\}$, the subcarrier index of the kth subcarrier in the jth group would be $G_{j,k} = jN_f + k$. For $i = 0, 1, ..., N_c - 1$, the symbol corresponding to subcarrier i is

$$d_i = d_{G_{j,k}} = \begin{cases} \mathcal{M}(Y_{j,k}), & k < k_j, \\ \mathcal{M}(Y_{j,k-1}), & k > k_j, \\ 0, & k = k_j, \end{cases} \tag{2.1}$$

where $\mathcal{M}(Y_{j,k})$ and $\mathcal{M}(Y_{j,k-1})$ are symbols mapped from the ordinary bit vectors $Y_{j,k}$ and $Y_{j,k-1}$, respectively. In the jth group, since the idle subcarrier indexed by k_j cannot carry an ordinary bit vector, for any $k > k_j$, subcarrier k should carry the ordinary bit vector indexed by $k - 1$ (one-vector forward). Let $d_{n,i}$ denote the ith symbol corresponding to the

nth information block I_n, the OFDM symbol corresponding to I_n can then be written as [2]

$$s_n(t) = \sum_{i=0}^{N_c-1} d_{n,i} e^{j2\pi f_i t}, \quad t \in [nT_s, (n+1)T_s), \tag{2.2}$$

where $f_i = \frac{i}{T_s}$ and T_s is the OFDM symbol period. Note that the discrete version of (2.2) can be efficiently computed by the IFFT block in Fig. 2.2.

2.2.2 Receiver Design

The receiver structure is shown in Fig. 2.3. The nth received OFDM symbol can be written as

$$r_n(t) = s_n(t) * h(t) + n(t), \tag{2.3}$$

where $*$ stands for convolution, $h(t)$ is the channel impulse response, and $n(t)$ denotes additive white Gaussian noise (AWGN). Sample the OFDM symbol and remove the cyclic prefix, we get

$$r_{n,l} = r_n(t_l), \quad t_l = nT_s + l\frac{T_s}{N_c}, \quad l = 0, 1, ..., N_c - 1. \tag{2.4}$$

Performing FFT, we have

$$R_{n,i} = \sum_{l=0}^{N_c-1} r_{n,l} e^{-j2\pi f_i t_l}, \quad i = 0, 1, ..., N_c - 1. \tag{2.5}$$

Let $\mathbf{H} = [H(0), ..., H(N_c - 1)]$ be the frequency domain channel response vector. After channel estimation, the nth symbol for the ith subcarrier can be estimated as [41]

$$\hat{d}_{n,i} = \frac{R_{n,i}}{H(i)}. \tag{2.6}$$

Without loss of generality, the subindex n in $\hat{d}_{n,i}$ is omitted in the following discussions.

Next we look at the recovery of the carrier bits and the ordinary bits. For each subcarrier group, the idle subcarrier can be detected as

$$\hat{k}_j = \underset{0 \le k \le N_f - 1}{\arg\min} \; |\hat{d}_{G_{j,k}}|^2, \tag{2.7}$$

where $\hat{k}_j$ is the estimated index of the idle subcarrier in the jth group and $G_{j,k}$ is the shared subcarrier grouping information between the transmitter and receiver. Now the carrier bit vector, $\hat{X}_j$, can be obtained by converting the estimated idle subcarrier index, $\hat{k}_j$, into a binary carrier bit vector. After the idle subcarriers are determined, ordinary bit vectors can be estimated as

$$\begin{cases} \hat{Y}_{j,k} \quad = \mathcal{M}^{-1}(\hat{d}_{G_{j,k}}), & k < \hat{k}_j, \\ \hat{Y}_{j,k-1} = \mathcal{M}^{-1}(\hat{d}_{G_{j,k}}), & k > \hat{k}_j, \end{cases} \tag{2.8}$$

where $\mathcal{M}^{-1}(\cdot)$ represents the demapping operator, $\hat{Y}_{j,k}$ and $\hat{Y}_{j,k-1}$ denote the recovered ordinary bit vectors. Hence, the entire block $\hat{I}_n$ is recovered.

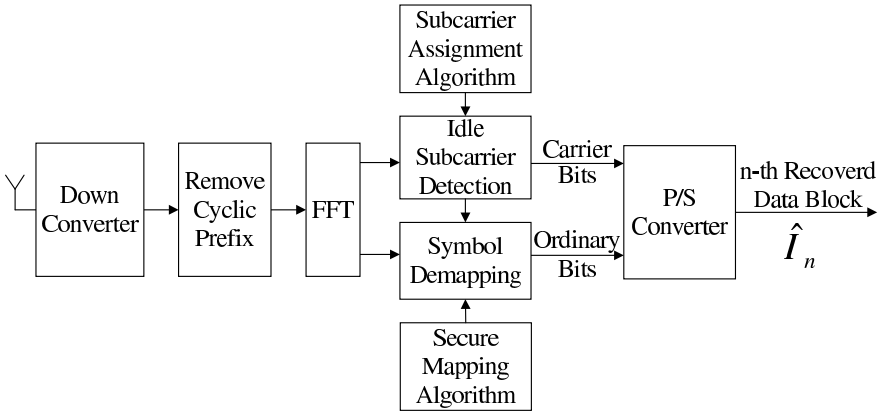


Figure 2.3: Receiver structure of MC-MDIS.

2.2.3 Bit Vector Rearrangement (BVR)

One possible issue with MC-MDIS is that under low SNRs, an error in idle subcarrier detection may occur and lead to bit vector disorder in the whole subcarrier group, even if each symbol is recovered correctly from its corresponding subcarrier. To solve this problem, we develop a bit vector rearrangement (BVR) algorithm, which is described as follows and graphically illustrated in Fig. 2.4. Note that each information block contains N_g groups, and BVR is performed group by group rather than block by block.

Rearrangement in the transmitter:

1. Fetch $B_c + N_f B_s$ bits and determine the idle subcarrier in the current group using the first B_c bits;

2. Evacuate the B_s bits at the location of the idle subcarrier and place them at the beginning of next group;

3. Transmit the remaining $(N_f - 1)B_s$ ordinary bits on the active subcarriers of the current group;

4. Repeat the above procedures till the end of the bit stream.

Restoration in the receiver:

1. Recover both the carrier bits and ordinary bits from the current group;

2. Reserve a B_s-bit space at the location of the idle subcarrier according to the carrier bit vector in the current group;

3. Recover the next bit group and fill its first B_s bits into the reserved space in the current one;

4. Make the new group the current one and repeat from 2).

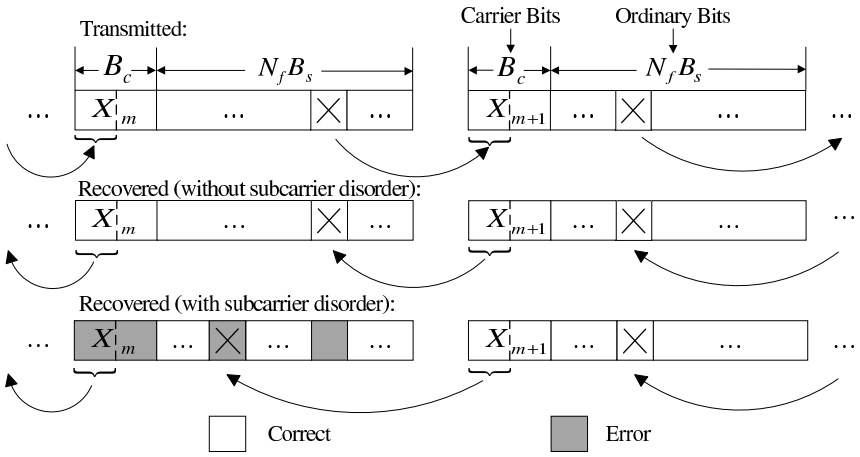


Figure 2.4: Illustration of the bit vector rearrangement (BVR) algorithm.

BVR is designed to keep the order of most ordinary bits from being influenced by an error in idle subcarrier detection. Note that the evacuated B_s bits in the current group will be placed at the beginning of the next one and form a carrier bit vector together with the successive $B_c - B_s$ bits. At the receiver side, each group removes its first B_s bits and fills them into the previous group, simultaneously acquiring B_s bits from the next group. As a result, the length of each group remains unchanged as $B_c + (N_f - 1)B_s$ bits. Unlike channel coding, no redundancy is introduced here, so no spectral efficiency is sacrificed. However, as in most coding methods, a mild delay will be introduced at the receiver side, since the reconstruction for the current group cannot be completed until the carrier bit vector of the next group arrives.

As shown in Fig. 2.4, with BVR, if an error in idle subcarrier detection occurs, only one[2] of the ordinary bit vectors in the group will be influenced, but the remaining would not. This contributes a lot to save the ordinary bits under possible idle subcarrier detection

[2]Note that in Fig. 2.4, only the middle shaded box is counted as ordinary bit errors, while the other two shaded ones are counted as carrier bit errors.

errors, especially when the group size is large. Please refer to the error probability analysis on the ordinary bits in Section 2.5.2 for a quantitative evaluation on how much ordinary bits can be saved by BVR. In the worst case, if the carrier bits of the current group is corrupted, the first B_s bits of the next group will be placed at a wrong location. As a result, it will also lead to errors, even if they themselves are correctly recovered. However, when the group size is relatively large, the impact is insignificant comparing with the saved ordinary bits. In the case of a small group size $N_f = 2$, this approach is not recommended since no ordinary bits can be saved.

Remark 2.1 *BVR is designed to enable MC-MDIS to work in the worst case (i.e., at low SNRs), but we would like to point out that idle subcarrier detection errors are very unlikely to occur at reasonable or high SNRs.*

2.3 Multicarrier Transmission with Message-Driven Strengthened Subcarriers (MC-MDSS)

In this section, we introduce an alternative scheme, MC-MDSS, by replacing the idle subcarriers in MC-MDIS with strengthened ones, which transmits both carrier bits and ordinary bits. Comparing with MC-MDIS, MC-MDSS can achieve higher spectral efficiency without suffering from the bit-vector-disorder issue.

2.3.1 Transmitter Design

We use the same notations as in Section 2.2. The first change resulted from MC-MDSS would be the information block structure. The total number of carrier bits to determine

strengthened subcarriers in all groups remains unchanged as $N_g B_c = N_g \log_2 \frac{N_c}{N_g}$, but the total number of ordinary bits will be increased to $N_c B_s = N_c \log_2 M$. Accordingly, in Fig. 2.1, the number of bits corresponding to each subcarrier group would be $B_c + N_f B_s$, and the length of the information block for MC-MDSS will be increased to $L = N_g B_c + N_c B_s$.

The power enhancement of several subcarriers make it difficult to employ non-constant-modulus[3] constellations (e.g. QAM), because under a modest amplitude-strengthening ratio, it is hard for the receiver to distinguish unamplified high-power-level symbols and amplified low-power-level symbols. For this reason, in MC-MDSS, we assume constant-modulus modulations, which can potentially be applied in digital video broadcasting [42] and optical communications [43].

Second, the idle subcarrier generation block in Fig. 2.2 is now replaced by the strengthened subcarrier generation block. The index of the strengthened subcarrier in the jth group, k_j, can be similarly calculated as that of idle subcarriers in MC-MDIS. A regular symbol will be assigned to each subcarrier; whereas, for each strengthened subcarrier indexed by k_j, the corresponding symbol will be amplified by a fixed amplitude-strengthening ratio, γ ($\gamma > 1$). Namely, for $i = 0, 1, ..., N_c - 1$, the symbol corresponding to subcarrier i is

$$d_i = d_{G_{j,k}} = \begin{cases} \gamma \mathcal{M}(Y_{j,k}), & k = k_j, \\ \mathcal{M}(Y_{j,k}), & otherwise, \end{cases} \tag{2.9}$$

where $\mathcal{M}(Y_{j,k})$ is the symbol mapped from the ordinary bit vector $Y_{j,k}$, and $G_{j,k}$ has the same definition as in Section 2.2. Except the differences above, the other parts of the transmitter for MC-MDSS are exactly the same as in MC-MDIS.

[3]For constant-modulus constellations, $\|s\|^2 = P_s$ holds for each symbol $s \in \Omega$, e.g., PSK modulation; whereas, the non-constant-modulus ones do not satisfy this requirement, e.g., QAM modulation.

2.3.2 Receiver Design

At the receiver side, we also need to make two changes for MC-MDSS accordingly. First, the block of idle subcarrier detection in Fig. 2.3 will be replaced by strengthened subcarrier detection. Namely, the index of the strengthened subcarrier can be determined by

$$\hat{k}_j = \underset{0 \le k \le N_f - 1}{\arg\max} \; |\hat{d}_{G_{j,k}}|^2. \tag{2.10}$$

Second, without the bit-vector-disorder issue, the ordinary bit estimation can be simplified as

$$\hat{Y}_{j,k} = \mathcal{M}^{-1}(\hat{d}_{G_{j,k}}), \tag{2.11}$$

where $\mathcal{M}^{-1}(\cdot)$ represents the demapping operator, and $\hat{Y}_{j,k}$ is the kth recovered ordinary bit vector in the jth subcarrier group.

2.4 Secure Subcarrier Assignment and Secure Symbol Mapping

In this section, we enhance the security of the proposed schemes under two commonly encountered attacks, eavesdropping and partial-band jamming. Eavesdropping is a passive attack, in which malicious users try to detect and recover the information of the authorized user. Whereas, partial-band jamming is an active attack, in which certain bands or subcarriers are deliberately interfered with strong jamming signals by the adversary. The worst case is often the follower jamming, in which the jammer follows the transmission pattern of a particular user and destroy its effective communication. Our approaches here are Advanced

Encryption Standard (AES) based secure subcarrier assignment and secure symbol mapping.

2.4.1 Secure Subcarrier Assignment (SSA)

The basic idea of secure subcarrier assignment is to shuffle and group all the available subcarriers secretly and dynamically, so that the jammers and eavesdroppers cannot follow the transmission pattern of the authorized users. More specifically, the secure subcarrier assignment scheme should satisfy the following requirements:

1) All available subcarriers should be involved, and there are no frequency overlaps in any grouping period;

2) The secure grouping information is shared only by the authorized transmitter and receiver, and should be secure under all known attacks;

3) The implementation cost should be low enough to allow frequent subcarrier regrouping.

In [44], we proposed a secure subcarrier assignment (SSA) algorithm to avoid frequency collisions in OFDM-based FH systems. Its security is guaranteed by the Advanced Encryption Standard (AES) [45], which has been proven to be secure under all known attacks [46]. Although this algorithm was originally designed to assign subcarriers randomly to different users in multi-user FH systems, we find that it meets all the aforementioned requirements. The core part of the secure subcarrier assignment is a secure permutation algorithm. The details of this algorithm is omitted here, please refer to [44]. However, we would like to illustrate what we can finally obtain from the algorithm through the following simple example.

Example 1: Assume that the total number of available subcarriers is $N_c = 8$, and they are supposed to equally divided into $M = 2$ groups. The algorithm actually performs a secret and random permutation among the subcarrier indexes $\{0, 1, 2, 3, 4, 5, 6, 7\}$. Suppose we get the final permutation as $\{3, 7, 0, 4, 2, 5, 6, 1\}$. In this case, the subcarrier groups are

$\{3, 7, 0, 4\}$ and $\{2, 5, 6, 1\}$, respectively. For instance, for the first group, if the specified idle subcarrier index is 1 (note that we start from 0), then subcarrier 7 will be the one unused and the rest $\{3, 0, 4\}$ will work as active subcarriers.

The features of SSA can be summarized as follows: 1) Due to the secured randomness introduced by SSA, the malicious users cannot follow the transmission pattern/bands of the authorized users, not to mention recovering the information. 2) For the authorized users, burst errors caused by partial-band jamming are randomized and largely reduced within the correction range of error control coding. As a result, the system becomes robust under partial-band jamming.

2.4.2 Secure Symbol Mapping (SSM)

To further enhance the system security such that the eavesdroppers cannot even recover the bits from an individual subcarrier, here we develop a secure symbol mapping algorithm to hide the ordinary bits.

To secure the mapping operation, we can simply make the constant mapping table dynamic and secret. For a constellation of size M, keeping a fixed-order symbol list $\mathcal{D} = \{d_0, d_1, ..., d_{M-1}\}$, we randomly and secretly adjust the corresponding bit vectors of these symbols. More specifically, define $\mathcal{A} = \{0, 1, ..., M-1\}$, and denote the AES-based secure permutation operation in [44] as $\mathcal{P} : \mathcal{A} \to \mathcal{A}$. Then for any $l \in \mathcal{A}$, the bit vector obtained from $dec2bin(\mathcal{P}(l))$ is mapped to symbol d_l. The demapping operation can be performed accordingly.

With SSM, the eavesdroppers would not be able to recover the bits from an individual subcarrier, even if they can extract the symbols correctly.

Remark 2.2 *Both SSM and SSA can be viewed as symbol-level encryption, which performs encryption in symbol generation and subcarrier grouping rather than conducting bit-level encryption. Compared with bit-level encryption, symbol-level encryption using SSA and SSM can achieve smaller processing delays. The underlying argument is that, with SSA and SSM, encryption/decryption can be performed in parallel with modulation/demodulation. While in traditional bit-level encryption, modulation can only be performed after the encryption, and decryption cannot start until the entire information block arrives.*

2.5 Analysis on Spectral Efficiency and Probability of Error

In this section, we analyze the performance of the two proposed schemes, MC-MDIS and MC-MDSS, in terms of spectral efficiency, power efficiency and error probability.

2.5.1 Spectral and Power Efficiency

The spectral efficiency η is defined as the ratio of the information bit rate R_b (bits/s) to the transmission bandwidth W (Hz), i.e., $\eta = \frac{R_b}{W}$ (bits/s/Hz). Since the proposed schemes are implemented on the OFDM framework, both of them, as well as OFDM, have the same total bandwidth $W = (N_c + 1)R_s$, where R_s is the OFDM symbol rate. To evaluate the power efficiency, we define the power ratio ρ as the ratio of the power consumed by MC-MDIS/MC-MDSS to that of OFDM.

For comparison, we first derive the bit rate ($R_{b,OFDM}$) and spectral efficiency (η_{OFDM})

of OFDM,

$$R_{b,OFDM} = R_s N_c \log_2 M, \tag{2.12}$$

$$\eta_{OFDM} = \frac{N_c}{N_c + 1} \log_2 M \approx \log_2 M. \tag{2.13}$$

2.5.1.1 MC-MDIS

Considering both the carrier bits and the ordinary bits, the bit rate of MC-MDIS can be calculated as

$$R_{b,MDIS} = R_s[N_g \log_2 \frac{N_c}{N_g} + (N_c - N_g) \log_2 M]. \tag{2.14}$$

To maximize the bit rate, we differentiate (2.14) over N_g,

$$\frac{dR_{b,MDIS}}{dN_g} = R_s \log_2 \frac{N_c}{N_g M e}, \tag{2.15}$$

where e is the Euler's number. Set (2.15) to zero, we get $N_g^* = \frac{N_c}{Me}$. Note that N_g can only be a power of 2, so we select two valid candidates nearest to N_g^*: $N_{g,1}^* = \frac{N_c}{2M}$ and $N_{g,2}^* = \frac{N_c}{4M}$. Substituting them into (2.14), we obtain exactly the same value, which forms the maximum bit rate for MC-MDIS,

$$R_{b,MDIS}^* = R_s N_c[\log_2 M + \frac{1}{2M}]. \tag{2.16}$$

Although both $N_{g,1}^*$ and $N_{g,2}^*$ maximize the bit rate, we choose $N_g = N_{g,1}^* = \frac{N_c}{2M}$ (i.e., more subcarrier groups) due to the following two reasons: 1) For a fixed number of available subcarriers, N_c, if we choose the number of groups to be $\frac{N_c}{2M}$ instead of $\frac{N_c}{4M}$, in each group there will be only $2M$ subcarriers instead of $4M$ ones; since the idle subcarrier detection can be considered as a flipped FSK, the $2M$-ary flipped FSK would outperform the $4M$-ary one in BER performance. 2) More subcarrier groups implies more subcarriers will be left idle,

which would result in further power savings and ICI suppression. With the maximized bit rate, it then follows that the maximum spectral efficiency of MC-MDIS is given by

$$\eta^*_{MDIS} = \frac{N_c}{N_c+1}[\log_2 M + \frac{1}{2M}] \approx \log_2 M + \frac{1}{2M}. \tag{2.17}$$

With $\frac{N_c}{2M}$ out of N_c subcarriers left idle in each group, the power ratio for MC-MDIS would be

$$\rho_{MDIS} = \frac{N_c - \frac{N_c}{2M}}{N_c} = 1 - \frac{1}{2M}. \tag{2.18}$$

2.5.1.2 MC-MDSS

Similarly, the bit rate of MC-MDSS can be calculated as

$$R_{b,MDSS} = R_s[N_g \log_2 \frac{N_c}{N_g} + N_c \log_2 M]. \tag{2.19}$$

Using the same methodology as in MC-MDIS, by setting $N_g = \frac{N_c}{4}$, we obtain the maximum bit rate for MC-MDSS,

$$R^*_{b,MDSS} = R_s N_c[\log_2 M + \frac{1}{2}], \tag{2.20}$$

and the maximum spectral efficiency of MC-MDSS,

$$\eta^*_{MDSS} = \frac{N_c}{N_c+1}[\log_2 M + \frac{1}{2}] \approx \log_2 M + \frac{1}{2}. \tag{2.21}$$

With $\frac{N_c}{4}$ out of N_c subcarriers whose symbols will be amplified by γ in amplitude, the

power ratio for MC-MDSS can be obtained as

$$\rho_{MDSS} = \frac{N_c - \frac{N_c}{4} + \gamma^2 \frac{N_c}{4}}{N_c} = \frac{\gamma^2 + 3}{4}. \tag{2.22}$$

For clarity, we summarize the analysis above in Table 2.1. It can be seen that comparing with OFDM, the improvement achieved by MC-MDIS in both spectral efficiency and power efficiency only depends on the constellation size M, while MC-MDSS can achieve a fixed but even larger improvement in spectral efficiency than MC-MDIS at a slight cost on power efficiency.

Table 2.1: Comparison of Spectral and Power Efficiency.

	Maximum Bit Rate	Maximum Efficiency	Efficiency Gap	Power Ratio
OFDM	$R_s N_c \log_2 M$	$\log_2 M$	N/A	N/A
MC-MDIS	$R_s N_c [\log_2 M + \frac{1}{2M}]$	$\log_2 M + \frac{1}{2M}$	$\frac{1}{2M}$	$1 - \frac{1}{2M}$
MC-MDSS	$R_s N_c [\log_2 M + \frac{1}{2}]$	$\log_2 M + \frac{1}{2}$	$\frac{1}{2}$	$\frac{\gamma^2+3}{4}$

2.5.2 Probability of Error for MC-MDIS

2.5.2.1 Carrier Bits

Given the average bit-level SNR, $\frac{E_b}{N_0}$, for MC-MDIS, the average symbol-level SNR, $\frac{E_s}{N_0}$, for each active subcarrier can be obtained as

$$\frac{E_s}{N_0} = \frac{L}{N_c - N_g} \frac{E_b}{N_0}, \tag{2.23}$$

where $L = N_g B_c + (N_c - N_g) B_s$ is the information block length and $N_c - N_g$ is the number of active subcarriers. It should be noted that E_s defined here corresponds to the average symbol energy in each active subcarrier.

The carrier bit modulation in MC-MDIS can be roughly considered as a "flipped" N_f-ary FSK, by which we mean an idle subcarrier is used to represent the carrier bits instead of an active one as in conventional FSK. Another difference is that, in MC-MDIS, when a non-constant-modulus constellation is employed, the active subcarriers may carry symbols with different power levels.

Let $E_1, ..., E_T$ be all the possible power levels in constellation Ω, and p_i the probability that the power level of an arbitrary symbol is E_i, then the average symbol power is given by

$$\bar{E}_s = \sum_{i=1}^{T} p_i E_i, \quad where \ \sum_{i=1}^{T} p_i = 1. \tag{2.24}$$

In this case, to achieve an overall SNR of $\frac{E_s}{N_0}$, the actual symbol-level SNR in MC-MDIS, $\frac{E_{s,i}}{N_0}$, would be

$$\frac{E_{s,i}}{N_0} = \frac{E_i}{\bar{E}_s} \frac{E_s}{N_0} = \frac{L}{N_c - N_g} \frac{E_i}{\bar{E}_s} \frac{E_b}{N_0}. \tag{2.25}$$

We can calculate the symbol error probability corresponding to the carrier bits for MC-MDIS as (see Appendix B for the details)

$$P_s^{(c)} \left(\frac{E_b}{N_0} \right) = 1 - \int_0^{\infty} \bar{Q}_1^{N_f - 1} x e^{-\frac{x^2}{2}} dx, \tag{2.26}$$

in which

$$\bar{Q}_1 = \sum_{i=1}^{T} p_i Q_1 \left(\sqrt{2 \frac{E_{s,i}}{N_0}}, x \right), \tag{2.27}$$

where $Q_1(a,b) = \int_b^\infty x \exp\left(-\frac{x^2+a^2}{2}\right) I_0(ax)dx$ is the Marcum Q-function [47], in which $I_0(\cdot)$ is the zero-order modified Bessel function.

Let $P_{e,\mathrm{I}}^{(c)}$ and $P_{e,\mathrm{II}}^{(c)}$ denote the bit error probabilities for carrier bits without and with BVR, respectively. According to [48, eqn. (5.2-24), page 260],

$$P_{e,\mathrm{I}}^{(c)}\left(\frac{E_b}{N_0}\right) = \frac{2^{B_c-1}}{2^{B_c}-1} P_s^{(c)}\left(\frac{E_b}{N_0}\right). \tag{2.28}$$

If BVR is employed, an error in idle subcarrier detection in the current bit block will lead to an incorrect replacement of the first B_s bits within the B_c carrier bits in the successive block. If an error occurs in idle subcarrier detection for the current bit block, there are two possible results for the idle subcarrier detection in the successive block: (i) an error occurs with a probability of $P_s^{(c)}\left(\frac{E_b}{N_0}\right)$; or (ii) it is correctly detected with a probability of $1 - P_s^{(c)}\left(\frac{E_b}{N_0}\right)$. In the first case, the bit error probability would still roughly be $P_{e,\mathrm{I}}^{(c)}\left(\frac{E_b}{N_0}\right)$, since the B_s bits that are incorrectly replaced originally contains errors; whereas in the second case, the bit error probability will approximately become $\left(1+\frac{B_s}{B_c}\right) P_{e,\mathrm{I}}^{(c)}\left(\frac{E_b}{N_0}\right)$, considering the newly introduced errors resulting from the incorrectly replaced B_s bits. Combining these two cases, the bit error probability of carrier bits with BVR can be estimated as

$$P_{e,\mathrm{II}}^{(c)}\left(\frac{E_b}{N_0}\right) \approx P_s^{(c)}\left(\frac{E_b}{N_0}\right) P_{e,\mathrm{I}}^{(c)}\left(\frac{E_b}{N_0}\right) + \left(1 - P_s^{(c)}\left(\frac{E_b}{N_0}\right)\right)\left(1+\frac{B_s}{B_c}\right) P_{e,\mathrm{I}}^{(c)}\left(\frac{E_b}{N_0}\right). \tag{2.29}$$

2.5.2.2 Ordinary Bits

The bit error probability of the ordinary bits depends on the modulation scheme exploited by the active subcarriers. We consider the case of transmitting the ordinary bits through M-ary QAM. Recall that $M = 2^{B_s}$, and the symbol error probability for M-ary QAM can

be represented as[4] [48, eqn. (5.2-78) & (5.2-79), page 278]

$$P_{s,QAM}\left(\frac{E_b}{N_0}\right) = 1 - \left[1 - 2(1 - \frac{1}{\sqrt{M}})Q\left(\sqrt{\frac{3}{M-1}\frac{E_s}{N_0}}\right)\right]^2, \tag{2.30}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{t^2}{2}}dt$, and $\frac{E_s}{N_0}$ can be found in (2.23). The bit error probability of the ordinary bits on each active subcarrier can then be approximated as

$$P_{e,QAM}\left(\frac{E_b}{N_0}\right) \approx \frac{1}{B_s}P_{s,QAM}\left(\frac{E_b}{N_0}\right). \tag{2.31}$$

Without BVR, if an error occurs in idle subcarrier detection, there will be a bit vector disorder on all the subcarriers between the truly idle one and the incorrectly detected one, which leads to a random guess in terms of error probability. Namely, if the idle subcarrier indices selected at the transmitter and estimated at the receiver are i and j, respectively, the bit error probabilities of the ordinary bits carried on subcarrier from i through j ($|i-j|$ out of $N_f - 1$ subcarriers) would be $\frac{1}{2}$, while the bit error probabilites of those carried on the other subcarriers will not be influenced and can thus be estimated by (2.31). The bit error probability of the ordinary bits with an error in idle subcarrier detection (with a probability of $P_s^{(c)}\left(\frac{E_b}{N_0}\right)$, in (2.26)) can therefore be calculated as

$$P_{e,\mathrm{I}}\left(\frac{E_b}{N_0}\right) = \sum_{i,j=0,i\neq j}^{N_f-1}\frac{1}{(N_f)_2}\left[\frac{|i-j|}{2(N_f-1)} + \left(1 - \frac{|i-j|}{N_f-1}\right)P_{e,QAM}\left(\frac{E_b}{N_0}\right)\right], \tag{2.32}$$

where $(n)_k$ denotes the number of k-permutations out of n.

With BVR, only one subcarrier carrying ordinary bits in each subcarrier group will be

[4]Note that (2.30) applies only when B_s is even and a rectangular constellation is employed. For cases with odd B_s or non-rectangular constellations, please refer to [48, page 278-279].

influenced and the remaining would remain uninfluenced, so the corresponding bit error probability with an error in idle subcarrier detection in this case would be

$$P_{e,\mathrm{II}}\left(\frac{E_b}{N_0}\right) = \frac{1}{2(N_f-1)} + \left(1 - \frac{1}{N_f - 1}\right) P_{e,QAM}\left(\frac{E_b}{N_0}\right). \tag{2.33}$$

If the idle subcarrier is correctly detected, the bit error probability of the ordinary bits can also be estimated by (2.31). Taking all the cases into account, the bit error probability of the ordinary bits can be calculated as

$$P_{e,\kappa}^{(o)}\left(\frac{E_b}{N_0}\right) = P_s^{(c)}\left(\frac{E_b}{N_0}\right) P_{e,\kappa}\left(\frac{E_b}{N_0}\right) + \left(1 - P_s^{(c)}\left(\frac{E_b}{N_0}\right)\right) P_{e,QAM}\left(\frac{E_b}{N_0}\right), \tag{2.34}$$

where $\kappa \in \{\mathrm{I}, \mathrm{II}\}$ denotes whether BVR is employed or not.

2.5.2.3 Overall

Following the discussions above, the overall bit error probability for MC-MDIS can be calculated as

$$P_e\left(\frac{E_b}{N_0}\right) = \frac{N_g B_c}{L} P_{e,\kappa}^{(c)}\left(\frac{E_b}{N_0}\right) + \frac{(N_c - N_g)B_s}{L} P_{e,\kappa}^{(o)}\left(\frac{E_b}{N_0}\right), \tag{2.35}$$

where $L = N_g B_c + (N_c - N_g)B_s$ is the number of bits in each information block for MC-MDIS, and $\kappa \in \{\mathrm{I}, \mathrm{II}\}$ denotes whether BVR is employed or not.

Remark 2.3 *Although we analyze the error probability of MC-MDIS theoretically with QAM modulation, the constant-modulus modulation (M-ary PSK) can also be used in MC-MDIS. Using the constant-modulus modulation instead of QAM would lead to two differences: 1) The power of each active subcarrier would become identical to each other, which works as a special case of nonuniform power distribution and actually makes the calculation much*

easier; 2) M-ary PSK has a different representation on the error probability from that of QAM; however, concerning the error probability analysis, the only thing we need to do is to replace $P_{s,QAM}\left(\frac{E_b}{N_0}\right)$ *with* $P_{s,PSK}\left(\frac{E_b}{N_0}\right)$*, which can be found in [48, eqn. (5.2-56), page 268].*

2.5.3 Probability of Error for MC-MDSS

2.5.3.1 Carrier Bits

We consider the case with constant modulus constellations only. Given the average bit-level SNR, $\frac{E_b}{N_0}$, for the MC-MDSS scheme, the average symbol-level SNR, $\frac{E_s}{N_0}$, would be

$$\frac{E_s}{N_0} = L\frac{E_b}{N_0} = (N_g B_c + N_c B_s)\frac{E_b}{N_0}, \tag{2.36}$$

where $L = N_g B_c + N_c B_s$ is the information block length. Note that different from the definition in MC-MDIS where E_s is averaged to each active subcarrier, E_s defined here takes into account the symbols transmitted through all the subcarriers, which contains N_g strengthened subcarriers and $N_c - N_g$ regular ones. Let $\frac{E_{s,1}^{(o)}}{N_0}$ be the symbol-level SNR of the strengthened subcarriers, and $\frac{E_{s,2}^{(o)}}{N_0}$ the symbol-level SNR corresponding to those regular ones, then we have

$$N_g\frac{E_{s,1}^{(o)}}{N_0} + (N_c - N_g)\frac{E_{s,2}^{(o)}}{N_0} = \frac{E_s}{N_0}. \tag{2.37}$$

The power relation of the strengthened subcarriers and the regular ones can be represented as

$$\frac{E_{s,1}^{(o)}}{N_0} = \gamma^2\frac{E_{s,2}^{(o)}}{N_0}, \tag{2.38}$$

where γ is the amplitude-strengthening ratio which is defined in Section 2.3. Combining (2.36)-(2.38), the SNRs for the two different kinds of subcarriers can be obtained as

$$\begin{cases} \dfrac{E_{s,1}^{(o)}}{N_0} = \dfrac{\gamma^2 L}{N_c + (\gamma^2 - 1)N_g} \dfrac{E_b}{N_0}, \\ \dfrac{E_{s,2}^{(o)}}{N_0} = \dfrac{L}{N_c + (\gamma^2 - 1)N_g} \dfrac{E_b}{N_0}. \end{cases} \tag{2.39}$$

The carrier bit demodulation in MC-MDSS can largely be viewed as a non-coherent N_f-ary FSK demodulation as well. What makes it slightly different from conventional FSK is that we have one strengthened subcarrier and several other regular ones (with non-zero power but less than the strengthened one), while in conventional FSK only one subcarrier has non-zero power. We can calculate the symbol error probability corresponding to the carrier bits for MC-MDSS as (see Appendix C for the details)

$$P_s^{(c)}\left(\frac{E_b}{N_0}\right) = \sum_{k=1}^{N_f-1} (-1)^{k+1} \binom{N_f - 1}{k} \int_0^\infty \left[Q_1\left(\sqrt{2\frac{E_{s,2}^{(o)}}{N_0}}, x \right) \right]^k f\left(x | \sqrt{2\frac{E_{s,1}^{(o)}}{N_0}}, 1 \right) dx, \tag{2.40}$$

where $Q_1(a,b) = \int_b^\infty x \exp\left(-\frac{x^2+a^2}{2}\right) I_0(ax) dx$ is the Marcum Q-function, and $f(x|\nu,\sigma) = \frac{x}{\sigma^2} \exp\left(-\frac{x^2+\nu^2}{2\sigma^2}\right) I_0(\frac{\nu x}{\sigma^2})$ denotes the probability density function of a Rician distribution. Accordingly, the bit error probability of the carrier bits can be calculated as

$$P_e^{(c)}\left(\frac{E_b}{N_0}\right) = \frac{2^{B_c - 1}}{2^{B_c} - 1} P_s^{(c)}\left(\frac{E_b}{N_0}\right). \tag{2.41}$$

2.5.3.2 Ordinary Bits

The symbol error probability of the constant-modulus modulation (PSK), $P_{s,PSK}\left(\frac{E_b}{N_0}\right)$, can be found in [48, eqn. (5.2-56), page 268]. What makes it different in MC-MDSS is

that among all the subcarriers, N_g of them are carrying ordinary bits at the SNR of $\frac{E_{s,1}^{(o)}}{N_0}$, while the other $N_c - N_g$ ones work at $\frac{E_{s,2}^{(o)}}{N_0}$. Consequently, the symbol error probability corresponding to the ordinary bits would be

$$P_s^{(o)}\left(\frac{E_b}{N_0}\right) = \frac{N_g}{N_c} P_{s,PSK}\left(\frac{1}{B_s}\frac{E_{s,1}^{(o)}}{N_0}\right) + \frac{N_c - N_g}{N_c} P_{s,PSK}\left(\frac{1}{B_s}\frac{E_{s,2}^{(o)}}{N_0}\right). \tag{2.42}$$

Similarly, the bit error probability of the ordinary bits can be approximated as

$$P_e^{(o)}\left(\frac{E_b}{N_0}\right) \approx \frac{1}{B_s} P_s^{(o)}\left(\frac{E_b}{N_0}\right). \tag{2.43}$$

2.5.3.3 Overall

Following the discussions above, the overall bit error probability for MC-MDSS can be calculated as

$$P_e\left(\frac{E_b}{N_0}\right) = \frac{N_g B_c}{L} P_e^{(c)}\left(\frac{E_b}{N_0}\right) + \frac{N_c B_s}{L} P_e^{(o)}\left(\frac{E_b}{N_0}\right), \tag{2.44}$$

where $L = N_g B_c + N_c B_s$ is the number of bits in each information block for MC-MDSS.

2.6 Numerical Results

In this section, the performance of both MC-MDIS and MC-MDSS is evaluated and compared with that of OFDM and some other most related schemes through simulation examples. We consider both AWGN and frequency selective channels, as well as the presence of inter-carrier interference (ICI). In the following, we assume $N_c = 64$, $R_s = 100$ and N_g is properly chosen according to the optimal subcarrier grouping strategy derived in Section

2.5.1. Unless otherwise stated, 16-QAM is used in MC-MDIS to exploit the general case of non-constant-modulus constellations, while QPSK is employed in MC-MDSS where the amplitude-strengthening ratio (γ) is set to 2. In addition, we provide the evaluation of the peak-to-average power ratio (PAPR) in Appendix D.

2.6.1 Spectral Efficiency

In Table 2.2, for different constellation size M, we compare the spectral efficiency of the proposed MC-MDIS and MC-MDSS with that of OFDM, as well as the other most related systems in literature, including collision-free frequency hopping (CFFH) [44], message-driven frequency hopping (MDFH) [7] and anti-jamming message-driven frequency hopping (AJ-MDFH) [15]. Both MC-MDIS and MC-MDSS, with maximized efficiency, are always more efficient than the other schemes. It is also observed that the efficiency gap between MC-MDIS and OFDM decreases as the constellation size increases. It should be pointed out that the increase in bit rate achieved by MC-MDIS and MC-MDSS can be significant and of great commercial value when the baud rate is large, which is generally the case in broadband communications.

2.6.2 Bit Error Rate

In this section, we numerically evaluate the BER performance of the proposed schemes under different scenarios.

1) Experimental Validation of Theoretical Results Fig. 2.5 and Fig. 2.6 compare the theoretical and simulation BERs of both carrier bits and ordinary bits for MC-MDIS without and with BVR, respectively. Fig. 2.7 depicts the BERs for MC-MDSS accordingly.

Table 2.2: Comparison of Spectral Efficiency with Different M.

Constellation Size	M	M=2	M=4	M=8	M=16
OFDM(bits/s/Hz)	$\log_2 M$	1	2	3	4
MC-MDIS(bits/s/Hz) (Compared to OFDM)	$\log_2 M + \frac{1}{2M}$	1.25 (+25%)	2.125 (+6.25%)	3.0625 (+2.08%)	4.03125 (+0.78%)
MC-MDSS(bits/s/Hz) (Compared to OFDM)	$\log_2 M + \frac{1}{2}$	1.5 (+50%)	2.5 (+25%)	3.5 (+16.7%)	4.5 (+12.5%)
CFFH(bits/s/Hz) (Compared to OFDM)	$\frac{1}{2}\log_2 M$	0.5 (-50%)	1 (-50%)	1.5 (-50%)	2 (-50%)
MDFH(bits/s/Hz) (Compared to OFDM)	$\frac{1}{2}\log_2 M + \frac{1}{2}$	1 (0%)	1.5 (-25%)	2 (-33.3%)	2.5 (-37.5%)
AJ-MDFH(bits/s/Hz) (Compared to OFDM)	$\frac{1}{2}$	0.5 (-50%)	0.5 (-75%)	0.5 (-83.3%)	0.5 (-87.5%)

It can be seen that the simulation results match well with the theoretical derivation.

2) Improvement on BER by BVR for MC-MDIS The improvement on BER by BVR for MC-MDIS is demonstrated in Fig. 2.8. We can see that the BER of MC-MDIS is considerably reduced by BVR, which is designed to eliminate the bit vector disorder.

3) Improvement on BERs by SSA under Partial-Band Jamming The improvements on BERs for MC-MDIS and MC-MDSS achieved by SSA under partial-band jamming are demonstrated in Fig. 2.9, in which the jamming occupancy (ρ) indicates the ratio of jammed subcarriers. We can see that SSA largely randomizes the burst errors such that they can be corrected by BCH coding.

4) BER Comparison of Different Schemes A comprehensive BER comparison is performed involving all the schemes listed in Table 2.2. For fair comparison, all the schemes employ QPSK and work at their maximum bit rates, i.e., $128R_s$ for OFDM, $136R_s$ for MC-

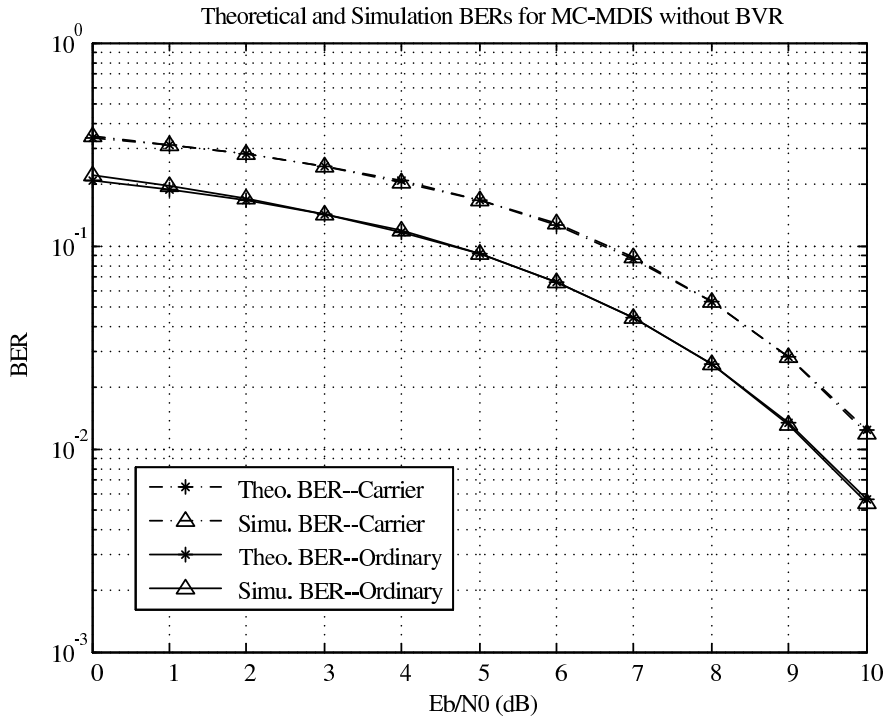


Figure 2.5: Theoretical and simulation BERs for MC-MDIS without BVR.

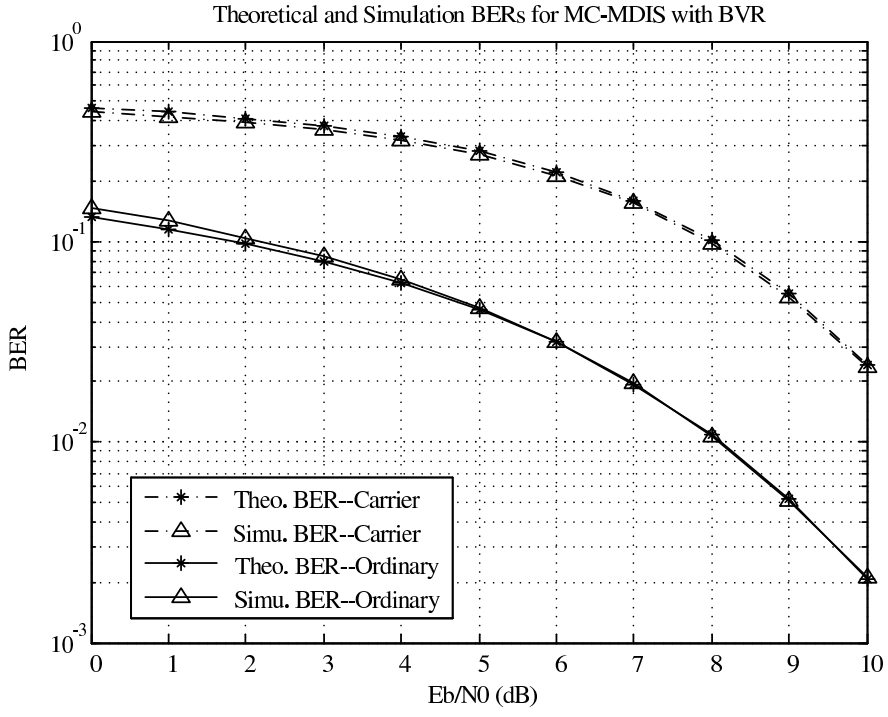


Figure 2.6: Theoretical and simulation BERs for MC-MDIS with BVR.

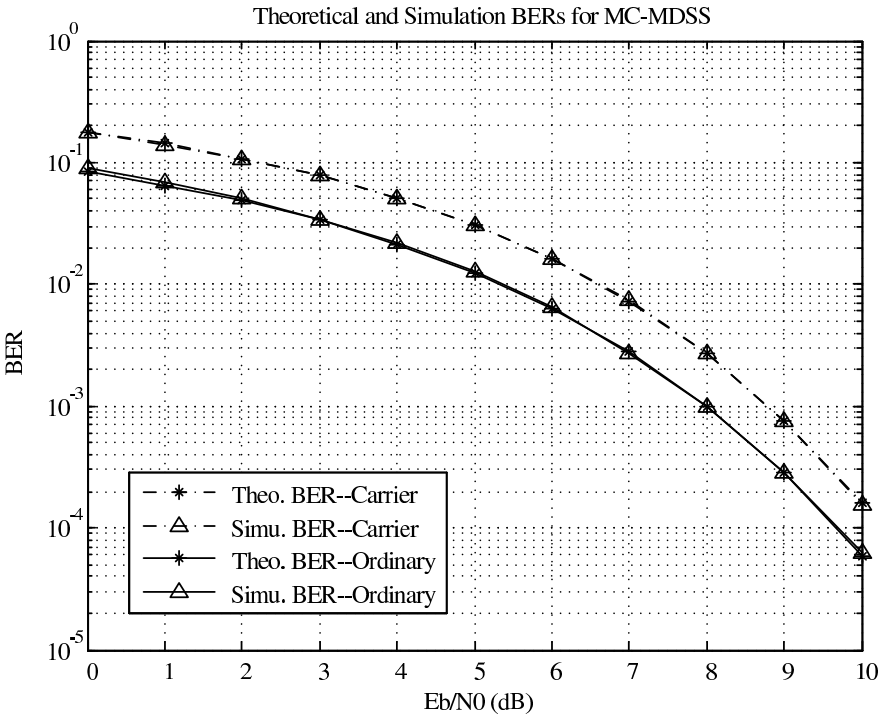


Figure 2.7: Theoretical and simulation BERs for MC-MDSS.

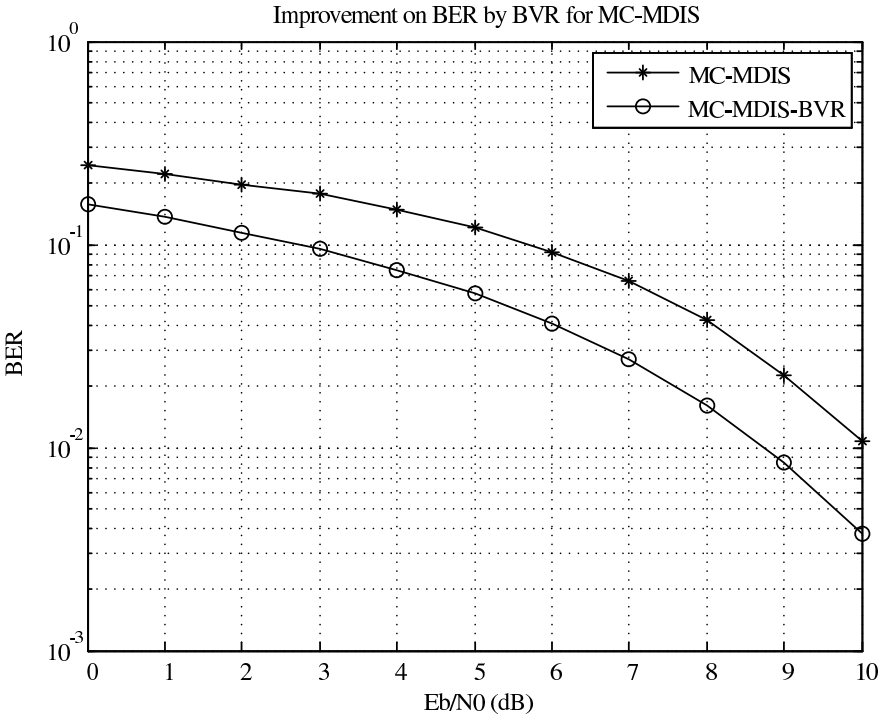


Figure 2.8: Improvement on BER by BVR for MC-MDIS.

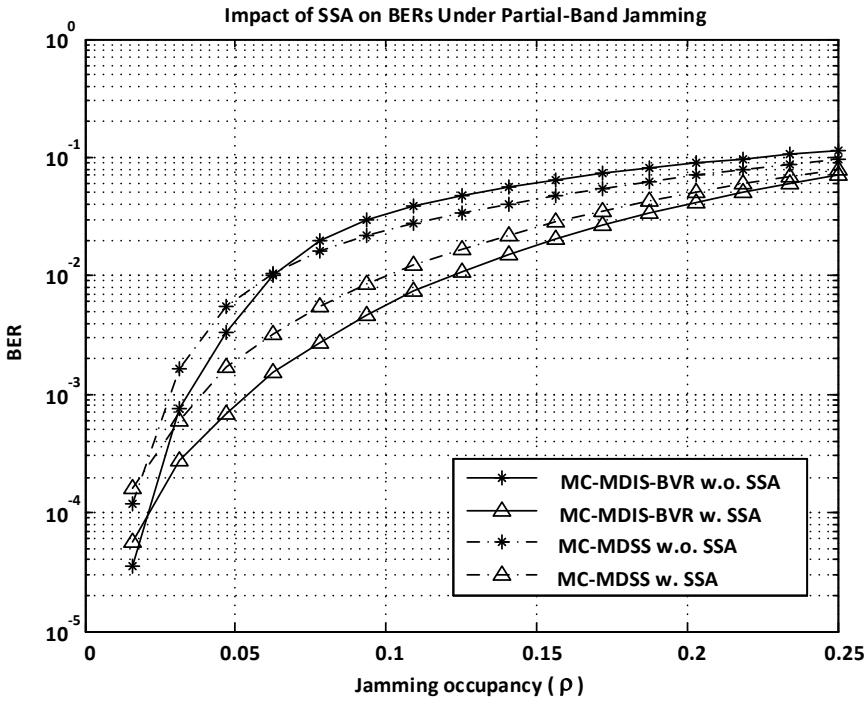


Figure 2.9: Impact of SSA on BERs under partial-band jamming. Coded with (31,11) BCH coding, SNR=10dB, and JSR=10dB.

MDIS, $160R_s$ for MC-MDSS, $64R_s$ for CFFH, $96R_s$ for MDFH and $32R_s$ for AJ-MDFH, where R_s is the OFDM symbol rate.

The BER comparison under AWGN channels is shown in Fig. 2.10. As expected, the proposed MC-MDIS and MC-MDSS achieve higher spectral efficiency at a slight cost on BER performance, which is mainly caused by the carrier bits. It can also be observed that: 1) MC-MDSS delivers better BER performance at lower SNRs, while MC-MDIS performs better at higher SNRs (very close to OFDM), where bit vector disorder is unlikely to happen; 2) MDFH and CFFH outperform MC-MDIS and MC-MDSS in BER performance, but at the cost of considerable spectral efficiency loss (shown in Table 2.2); 3) AJ-MDFH has an even worse BER performance, which is sacrificed together with spectral efficiency to gain the anti-jamming ability [15].

The BER comparison under a typical frequency selective channel is shown in Fig. 2.11. It

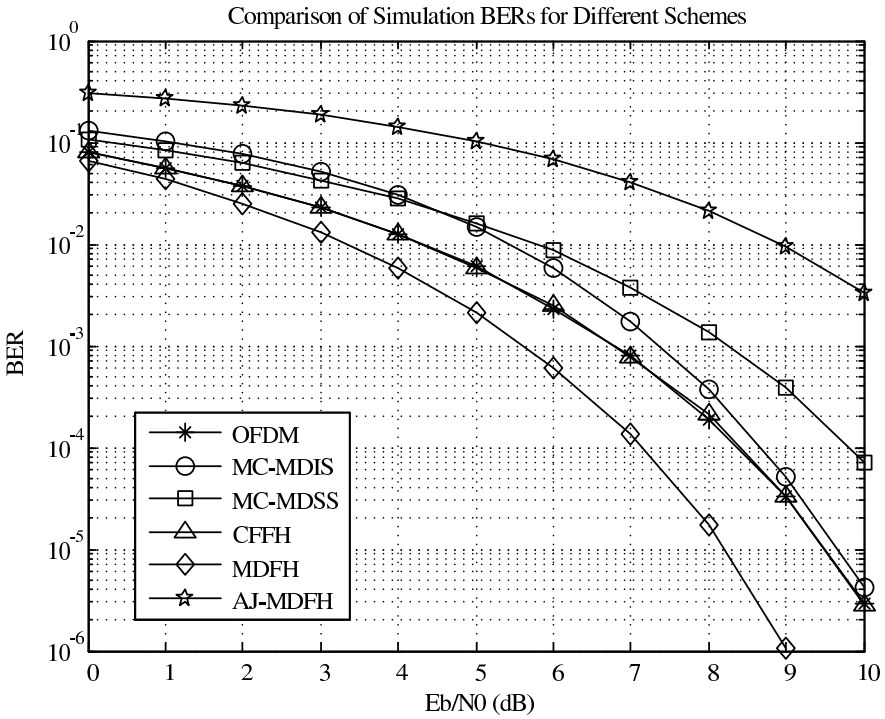


Figure 2.10: Comparison of simulation BERs under AWGN channels.

can be observed that under frequency selective channels, neither MC-MDIS nor MC-MDSS has a larger gap to OFDM than that under AWGN channels. There is still roughly 1.0dB gap between MC-MDIS and OFDM as under AWGN channels, and the BER performance of MC-MDSS comes even closer to OFDM than the AWGN case.

The BER comparison in the presence of inter-carrier interference (ICI) is shown in Fig. 2.12. The residual carrier frequency offset after proper frequency synchronization/tracking [49,50] is set to be 5Hz, which acts as a source of ICI. It can be observed that *in the presence of ICI, MC-MDIS outperforms OFDM in terms of BER, due to the ICI suppression effect contributed by the existence of idle subcarriers.* It is expected as well as demonstrated in Fig. 2.12 that MC-MDSS cannot yield a better result with ICI, since it uses strengthened subcarriers instead of idle ones.

We would like to point out that the loss in BER performance of the proposed schemes

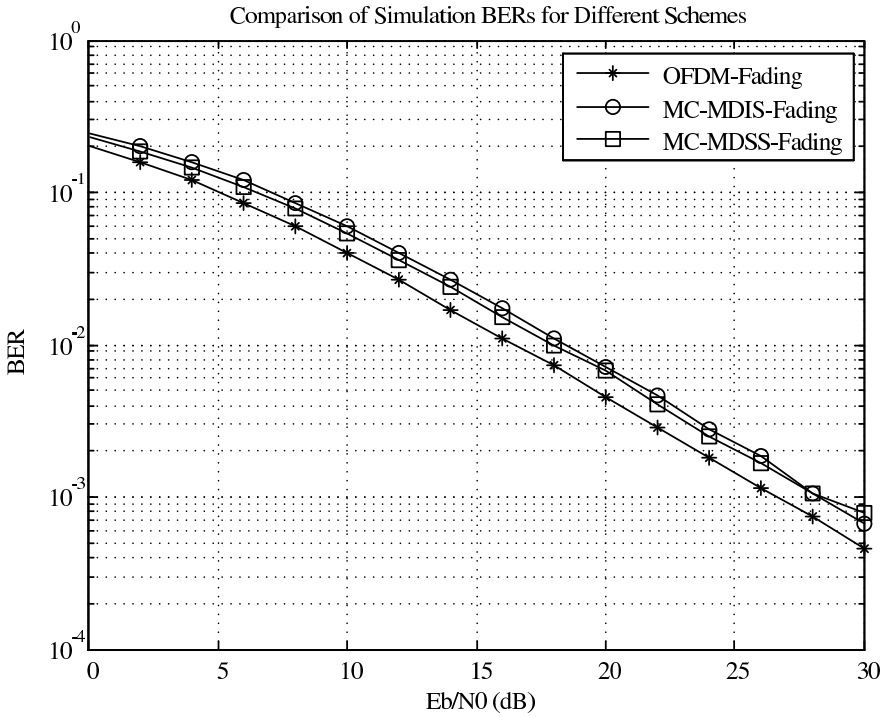


Figure 2.11: Comparison of simulation BERs under frequency selective channels.

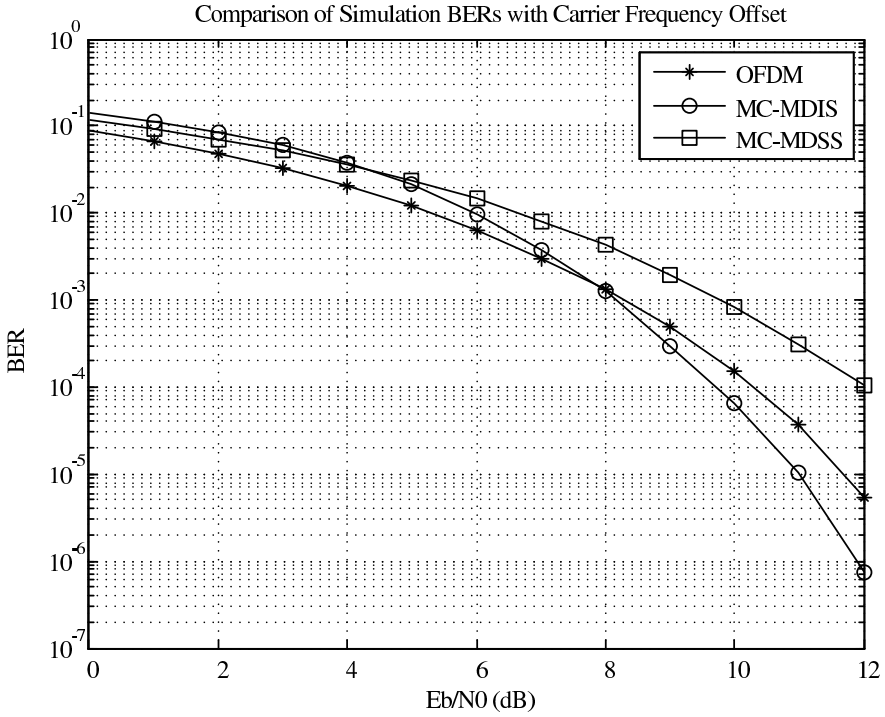


Figure 2.12: Comparison of simulation BERs in the presence of ICI.

(MC-MDIS/MC-MDSS), not significant though, may make them less favorable under low-SNR channels; however, the higher spectral efficiency achieved by MC-MDIS/MC-MDSS, as well as the ICI suppression effect of MC-MDIS, will make one or both of them popular under reasonable-SNR channels and/or in the presence of ICI.

2.7 Summary

In this chapter, we proposed two highly efficient OFDM-based multicarrier transmission schemes, MC-MDIS and MC-MDSS. In MC-MDIS, we specify one idle subcarrier in each group using the carrier bits, while transmits ordinary bits regularly on all the other subcarriers. Comparing with OFDM, MC-MDIS imposes no extra cost on bandwidth but resulting in higher spectral and power efficiency, as well as better ICI suppression. In MC-MDSS, the idle subcarriers are replaced by strengthened ones, which, unlike idle ones, can carry both carrier bits and ordinary bits. As a result, MC-MDSS achieves an even higher spectral efficiency than MC-MDIS with simpler transceiver design. The higher spectral efficiency achieved by MC-MDIS and MC-MDSS can be of great commercial value for broadband communications, where the baud rate is large. With symbol-level encryption (SSA and SSM), both MC-MDIS and MC-MDSS can prevent follower jamming, and are more robust than the traditional OFDM under eavesdropping and partial-band jamming.

Chapter 3

Precoding for OFDM under Disguised Jamming

In this chapter, we consider jamming-resistant OFDM system design under full-band disguised jamming, where the jamming symbols are taken from the same constellation as the information symbols over each subcarrier. *First*, we analyze the impact of disguised jamming on OFDM systems. It is shown that due to the symmetricity between the authorized signal and jamming, the BER of OFDM systems without symbol-level precoding or only with repeated symbol-level coding is lower bounded by a modulation specific constant, which cannot be improved by increasing SNR. *Second*, we develop an optimal precoding scheme which minimizes the BER of OFDM systems under full-band disguised jamming. It is shown that the most efficient way to combat full-band disguised jamming in OFDM systems is to concentrate the total available power and distribute it uniformly over a particular number of subcarriers instead of the entire spectrum. The precoding scheme is further randomized to protect the OFDM communication from a follower fashion of disguised jamming.

3.1 Introduction

Conventionally, research on communication system design has been focused on capacity improvement under non-intentional interference, such as intersymbol interference, multiuser

interference and noise. The jamming resistance of most communication systems today mainly relies on the diversity introduced by error control coding. On the other hand, jamming has widely been modeled as Gaussian noise. Based on the noise jamming model and the Shannon capacity formula, $C = \log_2(1 + SNR)$, an intuitive impression is that jamming is really harmful only when the jamming power is much higher than the signal power. However, this is only partially true. To show it, we need to look at disguised jamming [13–15], where the jamming is highly correlated with the signal, and has a power level close or equal to the signal power. Consider the example, $y = s + j + n$, where s is the authorized signal, j is the jamming, n is the noise independent of j and s, and y is the received signal. If j and s are taken randomly and independently from the same constellation, then due to the symmetricity between the jamming and the authorized signal, the receiver is fully confused and cannot really distinguish the authorized signal from jamming. As can be seen, the symbol error rate cannot be easily changed based only on the conventional bit-level channel coding. This observation motivates us to revisit the importance of symbol-level coding, generally known as precoding. In this chapter, we first explore the impact of disguised jamming, and then investigate how precoding can be exploited to combat disguised jamming.

As an important multi-carrier transmission system, orthogonal frequency division multiplexing (OFDM) has been identified as a core technique by many recent standards [3], e.g., LTE and WiMAX, mainly due to its high spectral efficiency and robustness under frequency selective channels. For jamming-resistant OFDM system design, a majority of literature [51, 52] primarily focuses on partial-band jamming, which jams only part of all the subcarriers. The basic strategies include: 1) avoiding the jammed bands, but only transmitting on the jamming-free bands; 2) randomizing the jamming effect through carefully designed interleaving, such that the burst errors caused by partial-band jamming can be

properly corrected. However, we observed that under the same jamming power constraint, full-band jamming could be more harmful for these systems [44].

In this chapter, we consider the jamming-resistant OFDM system design under full-band disguised jamming, where the jamming symbols are taken from the same constellation as the information symbols over each subcarrier. *First*, we analyze the impact of disguised jamming on OFDM systems. It is shown that due to the symmetricity between the authorized signal and jamming, the BER of OFDM systems without symbol-level precoding or only with repeated symbol-level coding is lower bounded by a modulation specific constant, which cannot be improved by simply increasing the SNR. *Second*, we develop an optimal precoding scheme which minimizes the BER of OFDM systems under full-band disguised jamming. It is shown that the most efficient way to combat full-band disguised jamming in OFDM systems is to concentrate the total available power and distribute it uniformly over a particular number of subcarriers instead of the entire spectrum. The underlying argument is that for a particular subcarrier, when the signal-to-jamming ratio is large enough, then the receiver can distinguish the authorized signal from disguised jamming under the presence of noise. The precoding scheme is further randomized to protect the OFDM communication from a follower fashion of disguised jamming. Our theoretical analysis and numerical results show that the BER performance of OFDM systems under full-band disguised jamming can be improved significantly with the proposed precoding scheme.

This chapter is organized as follows. In Section 3.2, the system model of precoded OFDM systems is provided. The impact of disguised jamming on OFDM is analyzed in Section 3.3. The optimal precoding scheme as well as the minimum BER of OFDM systems under full-band disguised jamming is derived in Section 3.4. The precoding scheme is further randomized in 3.5. Numerical evaluation is conducted in Section 3.6 and we conclude in

Section 3.7.

3.2 System Model

We consider the OFDM system equipped with a precoder as shown in Fig. 3.1. In our model, the input data block is first mapped to symbols. Let Ω represent the constellation we use and $\mathbf{x} = [x_0, x_1, ..., x_{K-1}]^T$ the symbol vector after symbol mapping, where $x_i \in \Omega$, K is the length of the symbol vector, and $(\cdot)^T$ denotes the transpose of a vector.

The $N_c \times K$ precoder matrix is denoted by $\mathbf{P}$, where N_c is the number of subcarriers for OFDM transmission. To allow some redundancy, we choose $N_c \geq K$. After symbol mapping, the precoder is applied to the symbol vector $\mathbf{x}$, which results in an $N_c \times 1$ vector $\mathbf{s}$, i.e.,

$$\mathbf{s} = \mathbf{P}\mathbf{x}. \tag{3.1}$$

The entire OFDM symbol can then be generated by performing inverse fast fourier transform (IFFT). This is followed by cyclic prefix (CP) insertion, which adds a guard time to eliminate intersymbol interference caused by multipath signals.

The obtained signal is then transmitted through an additive white Gaussian noise (AWGN) channel, and simultaneously interfered by full-band disguised jamming. The AWGN noise vector $\tilde{\mathbf{n}}$ has zero means and covariance matrix $E(\tilde{\mathbf{n}}^H\tilde{\mathbf{n}}) = \sigma_n^2\mathbf{I}$, where $(\cdot)^H$ denotes the Hermitian of a matrix. The frequency domain representation of $\tilde{\mathbf{n}}$ is actually a noise vector whose elements correspond to the AWGN noise associating to each OFDM subcarrier. If we denote it by $\mathbf{n} = [n_0, n_1, ..., n_{N_c-1}]^T$, then $\mathbf{n} = \mathbf{F}^H\tilde{\mathbf{n}}$, where $\mathbf{F}$ is the $N_c \times N_c$ IFFT unitary matrix with $[\mathbf{F}]_{n,k} = \frac{1}{\sqrt{N_c}}e^{j2\pi nk/N_c}$. It is noted that, since $\mathbf{F}^H$ is a unitary matrix, $\mathbf{n}$ continues to be a Gaussian random vector with zero means and covariance

matrix $E(\mathbf{n}^H\mathbf{n}) = \sigma_n^2\mathbf{I}$ [51]. Hence, the noise power corresponding to each subcarrier is σ_n^2.

The disguised jamming is typically launched by generating a signal which mimics the legally transmitted signal to confuse the receiver [13]. More specifically, in the OFDM case, the disguised jammer randomly choose one symbol out of the same constellation Ω for each subcarrier and transmit them exactly as the same way in the authorized OFDM transmitter. Namely, if the jamming vector is denoted by $\mathbf{j} = [j_0, j_1, ..., j_{N_c-1}]^T$, where $j_i \in \Omega$ is the disguised symbol associating to the ith subcarrier, then $\tilde{\mathbf{j}} = \mathbf{Fj}$.

At the receiver side, the cyclic prefix is first removed, followed by an FFT operation, which yields

$$\mathbf{y} = \mathbf{s} + \mathbf{j} + \mathbf{n}, \tag{3.2}$$

in which all the vectors have a dimension of $N_c \times 1$ and their elements correspond to N_c OFDM subcarriers, repectively.

The $K \times N_c$ decoder matrix $\mathbf{D}$ is then applied to $\mathbf{y}$ to recover the transmitted symbols. Hence, the estimated symbol vector, $\hat{\mathbf{x}}$, can be obtained as

$$\hat{\mathbf{x}} = \mathbf{Ds} + \mathbf{Dj} + \mathbf{Dn}. \tag{3.3}$$

The basic idea of precoding is to optimally exploit the channel information, including that on noise and jamming, at the transmitter to assign symbols, or their linear combination, over different subcarriers. If some redundancy is allowed (i.e., $K < N_c$), an optimal precoder should be able to wisely exploit the introduced redundancy to combat the distortion and interference. In this chapter, we aim to find the optimal precoder that can minimize the BER of OFDM systems under full-band disguised jamming, subject to the constraint on transmit power.

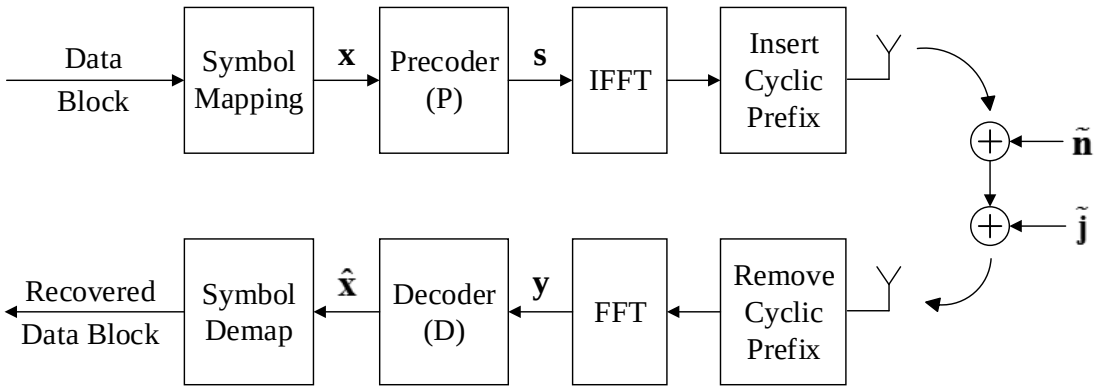


Figure 3.1: The system model of OFDM with precoding.

3.3 Conventional OFDM under Disguised Jamming

3.3.1 OFDM without Precoding

When there is no precoding employed, a channel with disguised jamming can be modeled as an arbitrarily varying channel (AVC) [13]. It has been proven in [13] that, due to the symmetricity between the authorized signal and jamming, the symbol error rate (SER) of a transmission under disguised jamming is lower bounded by

$$\mathcal{P}_s \geq \frac{M-1}{2M}, \tag{3.4}$$

where M is the constellation size. An intuitive explanation is that under disguised jamming, the receiver has to guess between the truly transmitted symbol and the fake symbol sent by the disguised jammer, if the two symbols are distinct. Note that the error probability of a random guess between two symbols is $\frac{1}{2}$, and the two symbols randomly and independently selected out of Ω by the authorized transmitter and disguised jammer differ in a probability of $\frac{M-1}{M}$. The additional noise would make the error probability even larger.

The lower bounded SER would naturally result in a lower bounded BER, where the

relationship is determined by the constellation used. When a binary modulation scheme (e.g., BPSK with M=2) is used, the BER coincides with the SER, and it would be lower bounded by

$$\mathcal{P}_{b,BPSK} \geq \frac{1}{4}, \qquad \textit{without precoding.} \tag{3.5}$$

The derived lower bounds above point to an important fact that under disguised jamming, bit-level coding can no longer decrease the error probability. The reason is that the bit stream with any bit-level coding ultimately has to be mapped to symbols, which unfortunately have an error probability lower bounded by (3.4) under disguised jamming.

3.3.2 MC-CDMA: OFDM with Repeated Coding

Considering that the disguised jamming disenables bit-level coding from improving the error probability performance, it becomes an option to exploit the symbol-level coding, which performs the coding directly on symbols instead of the bit stream. Let us consider MC-CDMA [53], which actually exploits repeated symbol-level coding. In repeated coding, each symbol is transmitted for L times, and it will be estimated at the receiver by averaging all the distorted copies. Take BPSK as an example, with a probability of $\frac{1}{2^L}$, the disguised symbols are all coincidentally opposite to the one sent by the authorized transmitter, in which case the receiver would still have to randomly guess which one out of the two symbols is transmitted. Hence, considering the noise as an additional impact, the BER under disguised jamming is lowered bounded by

$$\mathcal{P}_{b,BPSK} \geq \frac{1}{2^{L+1}}, \qquad \textit{repeated coding.} \tag{3.6}$$

It can be observed from (3.5) and (3.6) that disguised jamming is a significant threat to OFDM without precoding or only equipped with repeated coding, since the BERs cannot be

reduced below the lower bounds no matter how high the SNR is. The significant performance degradation of OFDM under disguised jamming motivates us to design an effective jamming-resistant symbol-level precoding scheme, as will be illustrated in Section 3.4.

3.4 Precoding for OFDM under Disguised Jamming

In this section, we derive the optimal precoder and decoder matrices using the minimum BER criterion. We start with BPSK modulation and AWGN channels, and then discuss other modulation schemes and frequency selective channels.

Let $\mathcal{P}_{\mathbf{P},\mathbf{D}}$ denote the BER with a precoder matrix $\mathbf{P}$ and decoder matrix $\mathbf{D}$ under full-band disguised jamming, and the problem can then be formulated as

$$\min_{\mathbf{P},\mathbf{D}} \mathcal{P}_{\mathbf{P},\mathbf{D}}; \tag{3.7a}$$

$$s.t. \;\; tr(\mathbf{P}\mathbf{P}^H) = P_c, \tag{3.7b}$$

$$\mathbf{D}\mathbf{P} = \mathbf{I}, \tag{3.7c}$$

where $tr(\cdot)$ is the trace operation. More specifically, (3.7b) is the constraint on the total available transmit power, and (3.7c) ensures perfect recovery for the precoding and decoding.

Under the constraint in (3.7c), the estimated symbol vector in (3.3) can be further simplified as

$$\hat{\mathbf{x}} = \mathbf{x} + \mathbf{D}\mathbf{j} + \mathbf{D}\mathbf{n}, \tag{3.8}$$

which is equivalent to

$$\hat{x}_k = x_k + \sum_{i=0}^{N_c-1} d_{k,i} j_i + \sum_{i=0}^{N_c-1} d_{k,i} n_i, \quad k = 0, 1, ..., K-1, \tag{3.9}$$

where we can see that with respect to $\mathbf{D}$, the estimation of the kth symbol in the transmitted symbol vector only depends on the kth row of $\mathbf{D}$. *This allows us to divide the optimization into two steps: 1) Minimizing the BER independently for each symbol under a parameterized constraint; 2) Minimizing the overall BER including all the symbols by finding the optimal parameters in the constraints.*

3.4.1 Independent BER Minimization for Each Symbol

To facilitate the analysis, we present two propositions first.

Proposition 3.1 *If a BPSK symbol with unit power is distorted by a deviation z and a Gaussian noise with a variance σ^2, the BER can be calculated by*

$$\mathcal{P}_{b,BPSK}(\sigma, z) = \frac{1}{2} Q\left(\frac{1-|z|}{\sigma}\right) + \frac{1}{2} Q\left(\frac{1+|z|}{\sigma}\right), \tag{3.10}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt$.

Proof: If the symbol $s = -1$ is transmitted, with a fixed deviation z, the received symbol would obey a Gaussian distribution $\hat{s} \sim \mathcal{N}(z-1, \sigma^2)$. The BER with $s = -1$ would be

$$\mathcal{P}(\hat{s} > 0 | s = -1) = Q\left(\frac{1-z}{\sigma}\right). \tag{3.11}$$

Similarly, the BER with $s = 1$ can be calculated as

$$\mathcal{P}(\hat{s} < 0 | s = 1) = Q\left(\frac{1+z}{\sigma}\right). \tag{3.12}$$

Assuming that $s = -1$ and $s = 1$ are equally probable, the overall BER can be obtained as shown in (3.10). □

Proposition 3.2 *Under the condition that $\sigma^2 < \beta - 1$, the constrained objective function*

$$J = \sum_{l=0}^{L-1} Q\left(\frac{\beta \pm w_l}{\sigma}\right), \quad s.t. \ \sum_{l=0}^{L-1} w_l^2 = L \& w_l \geq 0, \ \forall l, \tag{3.13}$$

achieves its minimum

$$J_{min} = LQ\left(\frac{\beta \pm 1}{\sigma}\right), \tag{3.14}$$

at $w_l = 1, \ \forall l$. Note that "+" and "−" in (3.14) correspond to those in (3.13), respectively.

Proof: We start from the problem with the "−" sign. Using the Lagrange multiplier, we define

$$F = \sum_{l=0}^{L-1} Q\left(\frac{\beta - w_l}{\sigma}\right) + \lambda\left(\sum_{l=0}^{L-1} w_l^2 - L\right). \tag{3.15}$$

Differentiating (3.15) with respect to each w_l,

$$\frac{\partial F}{\partial w_l} = \frac{1}{\sqrt{2\pi}\sigma} \exp\left\{-\frac{(\beta - w_l)^2}{2\sigma^2}\right\} + 2\lambda w_l, \quad \forall l. \tag{3.16}$$

By setting $\frac{\partial F}{\partial w_l} = 0$ and considering the constraint in (3.13), we have $w_l = 1,\ \forall l$. To ensure that this is the minimum point, we calculate the second-order differentiation at this point,

$$\frac{\partial^2 F}{\partial w_l^2} = \frac{1}{\sqrt{2\pi}\sigma}\left(\frac{\beta-1}{\sigma^2} - 1\right)\exp\left\{-\frac{(\beta-1)^2}{2\sigma^2}\right\},\quad \forall\ l. \tag{3.17}$$

Let $\frac{\partial^2 F}{\partial w_l^2} > 0$, we obtain the condition for the derived point being the minimum, $\sigma^2 < \beta - 1$. The problem with the "+" sign can be proved similarly. □

If we define $\sum_{i=0}^{N_c-1} d_{k,i}^2 \triangleq \frac{1}{\beta_k^2}$, the exclusive dependency on the kth row of $\mathbf{D}$ for the kth symbol estimation enables us to find the minimum BER for the kth symbol with respect to β_k, and we have the following theorem.

Theorem 3.1 *Under the condition that $\sigma_n^2 < \beta_k - 1$, the minimum BER of the kth symbol estimation in (3.9) can be obtained as*

$$\mathcal{P}_{k,min} = \frac{1}{2}Q\left(\frac{\beta_k - 1}{\sigma_n}\right) + \frac{1}{2}Q\left(\frac{\beta_k + 1}{\sigma_n}\right), \tag{3.18}$$

where $\beta_k = \sqrt{1/\sum_{i=0}^{N_c-1} d_{k,i}^2}$ and (3.18) is achieved when

$$d_{k,i} = \begin{cases} \frac{1}{\beta_k}, & i = i_k, \\ 0, & elsewhere, \end{cases} \tag{3.19}$$

where i_k differs from each other for different k.

Proof: Define $\mathcal{J} \triangleq \{\mathbf{j} = [j_0, j_1, ..., j_{N_c-1}]^T | j_i \in \Omega, i = 0, 1, ..., N_c - 1\}$, and the size of $\mathcal{J}$ would be $|\mathcal{J}| = 2^{N_c}$, since $\Omega = \{-1, +1\}$. According to (3.9), with a particular jamming vector $\mathbf{j} = [j_0, j_1, ..., j_{N_c-1}]^T$, the kth BPSK symbol x_k is distorted by a deviation

$z = \sum_{i=0}^{N_c-1} d_{k,i} j_i$ and a Gaussian noise with a variance $\sigma^2 = \sigma_n^2 \sum_{i=0}^{N_c-1} d_{k,i}^2 = \sigma_n^2/\beta_k^2$. Considering all the 2^{N_c} possible jamming vectors and applying Proposition 3.1, the BER of the kth symbol can be obtained as

$$\begin{aligned}\mathcal{P}_k &= \frac{1}{2^{N_c}} \sum_{\mathbf{j}\in\mathcal{J}} \left[\frac{1}{2} Q\left(\frac{1 - |\sum_{i=0}^{N_c-1} d_{k,i} j_i|}{\sigma_n/\beta_k} \right) + \frac{1}{2} Q\left(\frac{1 + |\sum_{i=0}^{N_c-1} d_{k,i} j_i|}{\sigma_n/\beta_k} \right) \right] \\ &= \frac{1}{2^{N_c+1}} \left[\sum_{\mathbf{j}\in\mathcal{J}} Q\left(\frac{\beta_k - \beta_k |\sum_{i=0}^{N_c-1} d_{k,i} j_i|}{\sigma_n} \right) + \sum_{\mathbf{j}\in\mathcal{J}} Q\left(\frac{\beta_k + \beta_k |\sum_{i=0}^{N_c-1} d_{k,i} j_i|}{\sigma_n} \right) \right].\end{aligned} \tag{3.20}$$

For any jamming vector $\mathbf{j} = [j_0, j_1, ..., j_{N_c-1}]^T \in \mathcal{J}$, we define $l \triangleq bin2dec([\frac{1-j_0}{2}, \frac{1-j_1}{2}, ..., \frac{1-j_{N_c-1}}{2}])$ and let $w_l \triangleq \beta_k |\sum_{i=0}^{N_c-1} d_{k,i} j_i|$, for $l = 0, 1, ..., 2^{N_c} - 1$. Then (3.20) can be rewritten as

$$\mathcal{P}_k = \frac{1}{2^{N_c+1}} \left[\sum_{l=0}^{2^{N_c-1}} Q\left(\frac{\beta_k - w_l}{\sigma_n} \right) + \sum_{l=0}^{2^{N_c-1}} Q\left(\frac{\beta_k + w_l}{\sigma_n} \right) \right], \tag{3.21}$$

with

$$\sum_{l=0}^{2^{N_c-1}} w_l^2 = 2^{N_c} \beta_k^2 \sum_{i=0}^{N_c-1} d_{k,i}^2 = 2^{N_c}. \tag{3.22}$$

Applying Proposition 3.2, we can obtain the minimum of (3.21) as shown in (3.18), under the condition that $\sigma_n^2 < \beta_k - 1$ and the minimum is achieved at $w_l = 1$, $\forall l$. To achieve this minimum point, only one non-zero element, $\frac{1}{\beta_k}$, can exist among $d_{k,i}$, $\forall i$. There is another requirement that the only non-zero element in each row needs to be located in different columns, which guarantees that (3.7c) is satisfied. To sum up, the decoder matrix $\mathbf{D}$ that minimizes the BER for each symbol should be formed as shown in (3.19). □

3.4.2 Minimization for the Overall BER

With the BER of each symbol minimized, we try to minimize the overall BER including all the symbols, by finding the optimal β_k for each k. Following the pattern in (3.19), and without loss of generality, we assume the non-zeros of $\mathbf{D}$ locate in the first k columns, i.e.,

$$\mathbf{D} = \begin{bmatrix} \frac{1}{\beta_0} & 0 & \cdot & \cdot & 0 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & \frac{1}{\beta_1} & \cdot & \cdot & 0 & 0 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \frac{1}{\beta_{K-1}} & 0 & 0 & \cdot & \cdot & 0 \end{bmatrix}_{K \times N_c}.$$

Applying the constraint in (3.7c), the precoding matrix needs to be

$$\mathbf{P} = \begin{bmatrix} \beta_0 & 0 & \cdot & \cdot & 0 \\ 0 & \beta_1 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \beta_{K-1} \\ 0 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & 0 \end{bmatrix}_{N_c \times K}.$$

Applying the constraint in (3.7b), the constraint on β_k can be obtained as $\sum_{k=0}^{K-1} \beta_k^2 = P_c$.

Taking into account all the symbols in the transmitted symbol vector and applying Theorem 3.1, the overall BER can be calculated as

$$\begin{aligned}\mathcal{P}_{\mathbf{P},\mathbf{D}} &= \frac{1}{K}\sum_{k=0}^{K-1}\mathcal{P}_{k,min} \\ &= \frac{1}{2K}\sum_{k=0}^{K-1}\left[Q\left(\frac{\beta_k-1}{\sigma_n}\right)+Q\left(\frac{\beta_k+1}{\sigma_n}\right)\right].\end{aligned} \tag{3.23}$$

Due to the convexity of the Q function,

$$\mathcal{P}_{\mathbf{P},\mathbf{D}} \geq \frac{1}{2}Q\left(\frac{\frac{1}{K}\sum_{k=0}^{K-1}\beta_k-1}{\sigma_n}\right)+\frac{1}{2}Q\left(\frac{\frac{1}{K}\sum_{k=0}^{K-1}\beta_k+1}{\sigma_n}\right), \tag{3.24}$$

where the equality holds if and only if each β_k equals each other for all k.

Simultaneously, using the Lagrange multiplier, we have

$$\frac{1}{K}\sum_{k=0}^{K-1}\beta_k \leq \sqrt{\frac{P_c}{K}}, \quad s.t. \sum_{k=0}^{K-1}\beta_k^2 = P_c, \tag{3.25}$$

in which the equality holds if and only if

$$\beta_k = \sqrt{\frac{P_c}{K}},\ \forall k. \tag{3.26}$$

Considering the equality of both (3.24) and (3.25) holds with the same condition as in (3.26), the minimum overall BER can be obtained as

$$\mathcal{P}_{\mathbf{P},\mathbf{D}} \geq \frac{1}{2}Q\left(\frac{\sqrt{\frac{P_c}{K}}-1}{\sigma_n}\right)+\frac{1}{2}Q\left(\frac{\sqrt{\frac{P_c}{K}}+1}{\sigma_n}\right), \tag{3.27}$$

where the equality holds when $\beta_k = \sqrt{\frac{P_c}{K}},\ \forall k$.

The above result is summarized in the following theorem.

Theorem 3.2 *Under the condition that* $\sigma_n^2 < \sqrt{\frac{P_c}{K}} - 1$*, the BER minimization problem in (3.7) has a solution,*

$$\min_{\boldsymbol{P},\boldsymbol{D}} \mathcal{P}_{\boldsymbol{P},\boldsymbol{D}} = \frac{1}{2}Q\left(\frac{\sqrt{\frac{P_c}{K}} - 1}{\sigma_n}\right) + \frac{1}{2}Q\left(\frac{\sqrt{\frac{P_c}{K}} + 1}{\sigma_n}\right), \tag{3.28}$$

where the minimum is achieved with

$$\boldsymbol{P} = \begin{bmatrix} \sqrt{\frac{N_c}{K}} & 0 & \cdot & \cdot & 0 \\ 0 & \sqrt{\frac{N_c}{K}} & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \sqrt{\frac{N_c}{K}} \\ 0 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & 0 \end{bmatrix}_{N_c \times K},$$

and

$$\boldsymbol{D} = \begin{bmatrix} \sqrt{\frac{K}{N_c}} & 0 & \cdot & \cdot & 0 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & \sqrt{\frac{K}{N_c}} & \cdot & \cdot & 0 & 0 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \sqrt{\frac{K}{N_c}} & 0 & 0 & \cdot & \cdot & 0 \end{bmatrix}_{K \times N_c}.$$

Theorem 3.2 indicates that the most efficient way to combat full-band disguised jamming in OFDM systems is to concentrate all the available power and distribute it uniformly on a particular number of subcarriers instead of the entire spectrum. The underlying argument is that for a particular subcarrier, when the signal-to-jamming ratio is large enough, then the receiver can distinguish the authorized signal from disguised jamming under the presence of noise.

Discussions: a) *Other Modulation Schemes* Though Theorems 3.1 and 3.2 are proved for BPSK at this point, these results shed light on precoder design for other modulations as well. The effectiveness of the proposed precoding scheme on other modulation schemes is demonstrated in Section 3.6.2 through simulation results.

b) *Frequency Selective Channels* A typical way to cope with frequency selective channels is to perform a channel equalization after estimation, which is also indispensable in conventional OFDM systems without precoding. Let $\mathbf{h} = [h_0, h_1, ..., h_{N_c-1}]$ denote the frequency domain channel impulse response vector. We perform an equalization on the received symbol vector $\mathbf{y}$ before feeding it to the decoder matrix $\mathbf{D}$. Nothing changes but the symbol estimation in (3.3) would become $\hat{\mathbf{x}} = \mathbf{D}\tilde{\mathbf{y}}$, where the ith element of $\tilde{\mathbf{y}}$, $\tilde{y}_i$, can be obtained by $\tilde{y}_i = \frac{y_i}{h_i},\ i = 0, 1, ..., N_c - 1$. In this case, for best performance, the K subcarriers with the largest SNRs should be selected out of all N_c subcarriers. A numerical evaluation on frequency selective channels is provided in Section 3.6.3.

3.5 Randomized Precoding

In section 3.4, we learned that the most efficient way to combat full-band disguised jamming in OFDM systems is to concentrate all the available power and distribute it uniformly on a

particular number of subcarriers instead of the entire spectrum. However, if the authorized user transmits over a fixed set of subcarriers, the jammer could still easily identify these active subcarriers (e.g., by power estimation), and then launch a follower fashion of disguised jamming that will eventually lead to complete communication again. To address this issue, we need to introduce some secured randomness to the proposed precoding scheme, which essentially hides the precoding pattern from being followed by the jammer.

To generate a random precoding pattern, we need to first determine the number of subcarriers that should be activated, and then randomly select the exact number of subcarriers out of the entire spectrum. Determining the desired number of active subcarriers involves a tradeoff between spectral efficiency and error probability. It is observed from Theorem 3.2 that given the power constraint P_c, the minimized error probability decreases with a decreasing number of active subcarriers, K, which, however, will inevitably lead to lower spectral efficiency, since fewer symbols can be transmitted for each symbol period. In view of this observation, the desired number of active subcarriers, K, should be chosen as small as to deliver a satisfying error probability.

Once the number of active subcarriers, K, is determined, for each symbol period, the authorized transmitter randomly select K out of N_c subcarriers and share this secret information with the authorized receiver(s) only. The secret randomness exclusively shared between the authorized user and the authorized receiver(s) makes it difficult for any follower jamming being launched. There might be many approaches to generate the secured randomness, but any approach with guaranteed security would apply. For instance, we can adapt the idea that applies AES to secure the randomness in Chapter 2 here to generate the secure and random precoding patterns.

Taking a closer look at the randomized precoding, we can observe that frequency hopping

(FH) is actually a special case of randomized precoding with $K = 1$. Comparing with traditional FH systems, OFDM with randomized precoding provides more flexibility in balancing spectral efficiency and error probability, and meanwhile, as we see throughout this chapter, works as an effective scheme that is robust against full-band disguised jamming as well as follower jamming.

3.6 Numerical Results

In this section, the BER performance of the precoded OFDM system under full-band disguised jamming is evaluated and compared with that without precoding and with repeated coding through simulation examples. We consider both AWGN and frequency selective channels. In the following, we assume $N_c = 64$, $R_s = 100$, $P_c = 64$, and the signal-to-jamming ratio is 0dB over the entire spectrum.

3.6.1 BPSK under AWGN Channels

In this scenario, under AWGN channels, BPSK is used and we set $K = 16 < N_c$, which provides redundancy for the precoding to combat disguised jamming. In Fig. 3.2, it is observed that: 1) Uncoded OFDM completely fails under full-band disguised jamming, since the BER maintains at approximately $\frac{1}{4}$ (lower bound in (3.5)) no matter how high the SNR is; 2) OFDM with repeated coding improves a little on the BER, but is still far away from being satisfactory, since the BER cannot be reduced beneath $\frac{1}{32}$ (lower bound in (3.6)) no matter how high the SNR is; 3) OFDM with optimal precoding considerably reduces the BER with reasonable SNRs, resulting from the optimal utilization of the introduced redundancy.

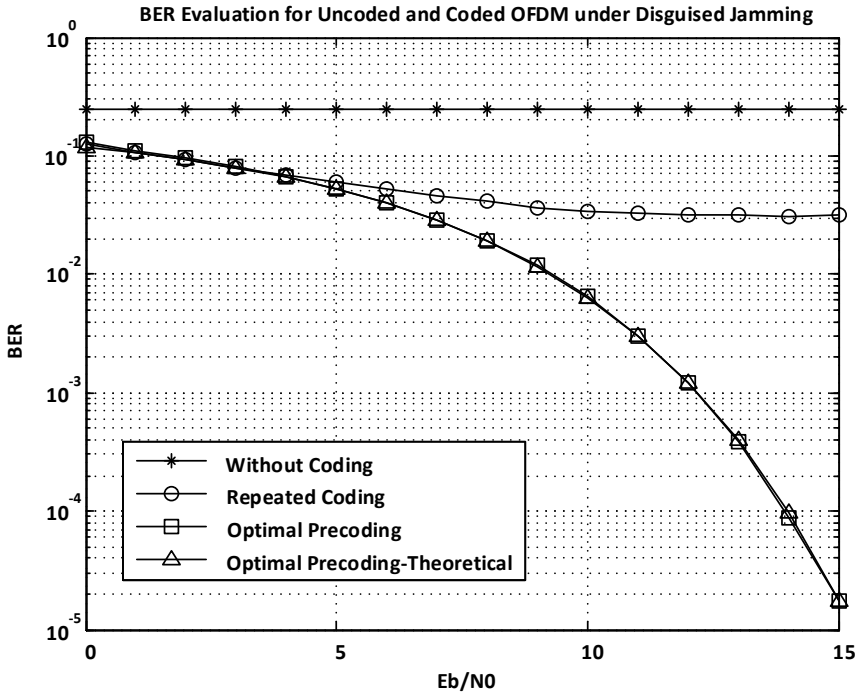


Figure 3.2: BER evaluation for BPSK-modulated OFDM with full-band disguised jamming under AWGN channels.

3.6.2 16QAM under AWGN Channels

In this scenario, still under AWGN channels, 16QAM is used to evaluate the performance of the optimal precoding with high-order modulation. K is further reduced to 4 to provide more redundancy. In Fig. 3.3, we observe the similar results as in Section 3.6.1, which demonstrate that the precoding scheme in Theorem 3.2 works with high-order modulation as well. However, the increased redundancy and the higher SNR requirement prove that high-order modulation is more fragile to disguised jamming.

3.6.3 BPSK under Frequency Selective Channels

To evaluate the impact of fading on the proposed precoding scheme, in this scenario, we move the simulation in Section 3.6.1 to a typical frequency selective channel. In Fig. 3.4,

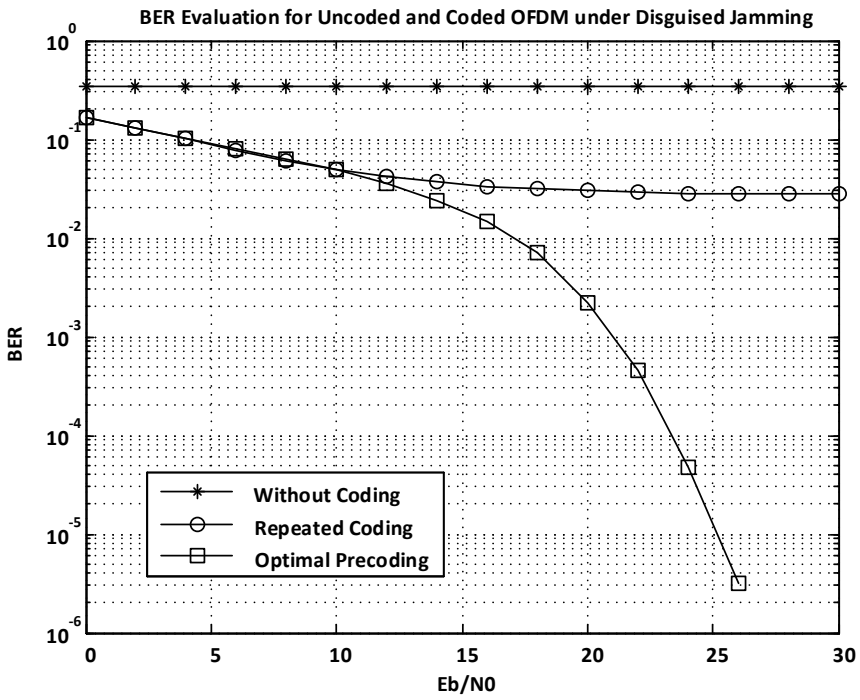


Figure 3.3: BER evaluation for 16QAM-modulated OFDM with full-band disguised jamming under AWGN channels.

it is observed that under frequency selective channels, OFDM with optimal precoding still outperforms the others, which demonstrates the effectiveness of the precoding scheme under frequency selective channels.

3.7 Summary

In this chapter, we analyzed the impact of disguised jamming on OFDM systems, and developed an optimal precoding scheme which minimizes the BER of OFDM systems under full-band disguised jamming. It is shown that the most efficient way to combat full-band disguised jamming in OFDM systems is to concentrate all the available power and distribute it uniformly on a particular number of subcarriers instead of the entire spectrum. The precoding scheme was further randomized to protect the OFDM communication from a follower

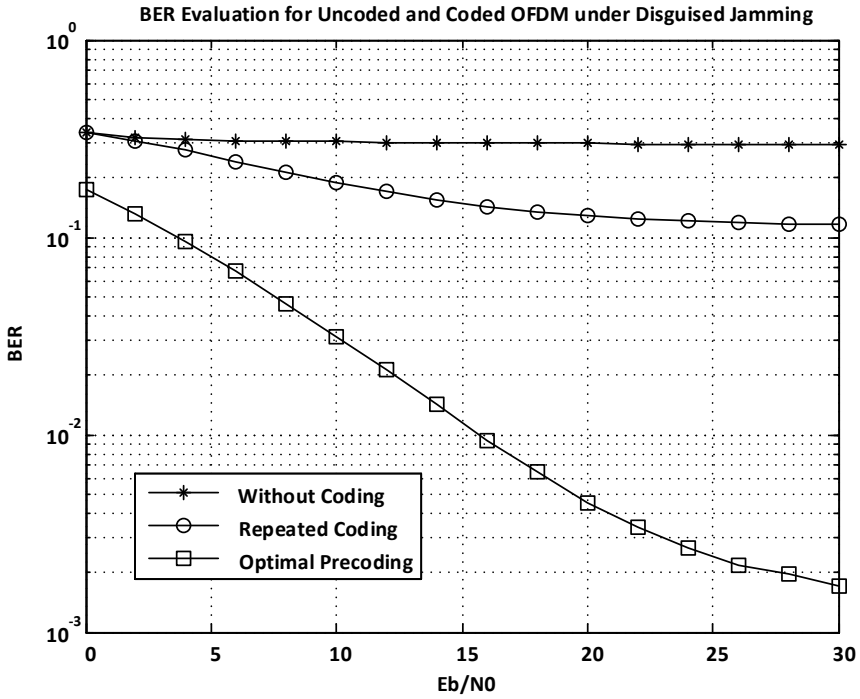


Figure 3.4: BER evaluation for BPSK-modulated OFDM with full-band disguised jamming under frequency selective channels.

fashion of disguised jamming. Both theoretical analysis and numerical results demonstrated that the BER performance of OFDM systems under full-band disguised jamming can be improved significantly with the proposed precoding scheme.

Chapter 4

CDMA System Design and Capacity Analysis under Disguised Jamming

In this chapter, we consider jamming mitigation for CDMA systems under disguised jamming, where the jammer generates a fake signal using the same spreading code, constellation and pulse shaping filter as that of the authorized signal. *First*, we analyze the performance of conventional CDMA systems under disguised jamming, and show that due to the symmetricity between the authorized signal and the jamming interference, the receiver cannot really distinguish the authorized signal from jamming, leading to complete communication failure. *Second*, for CDMA systems with public codes which cannot be concealed for some reason, we mitigate the disguised jamming through robust receiver design. By exploiting the small time difference between the authorized signal and the jamming interference, the conventional CDMA receiver can be re-designed to achieve robust performance under disguised jamming. *Third*, for CDMA systems which allow code concealment, we mitigate disguised jamming using secure scrambling. Instead of using conventional scrambling codes, we apply advanced encryption standard (AES) to generate the security-enhanced scrambling codes. Assuming ideal synchronization between the authorized user and the jammer, we prove that: the capacity of the conventional CDMA systems without secure scrambling under disguised jamming is actually zero; however, the capacity can be significantly increased when CDMA

systems are protected using secure scrambling.

4.1 Introduction

Existing work on anti-jamming system design or jamming mitigation is mainly based on spread spectrum techniques [54, 55]. The spread spectrum systems, including code division multiple access (CDMA) and frequency hopping (FH), were originally developed for secure communications in military applications. Both CDMA and FH systems possess anti-jamming and anti-interception features by exploiting frequency diversity over large spectrum.

In CDMA, each user is assigned a specific pseudo-random code (also known as the signature waveform) to spread its signal over a bandwidth N times larger. Due to the processing gain resulted from the spread spectrum technique, CDMA is especially robust under narrow band jamming and works well under low SNR levels [56]. Hidden within the noise floor, CDMA signals are difficult to be detected, and cannot be recovered unless the user signature is known at the receiver. For these reasons, CDMA has been widely used in both civilian and military applications, such as 3GPP UMTS [57] and GPS [58].

The security of CDMA largely relies on the randomness in the PN sequence. For CDMA, the spreading code of each user is obtained through the modulo 2 sum of the Walsh code and the long code, and thus is varying in every symbol period. However, according to the Berlekamp-Massey algorithm [28], for a sequence generated from an n-stage linear feedback shift register, the characteristic polynomial and the entire sequence can be reconstructed if an eavesdropper can intercept a $2n$-bit sequence segment. Note that the characteristic polynomial is generally available to the public, then PN sequence can be recovered if an n-bit sequence segment is intercepted. That is, it is possible to break the PN sequence

used in the conventional CDMA systems in real time with today's high speed computing techniques [29]. Once the PN sequence is recovered or broken, the jammer can generate a fake signal using the same spreading code, constellation and pulse shaping filter as that of the authorized signal. This is known as the *disguised jamming* [13–15] for CDMA.

In this chapter, we first analyze the performance of conventional CDMA systems under disguised jamming, and show that due to the symmetricity between the authorized signal and the jamming interference, the receiver cannot really distinguish the authorized signal from jamming, leading to complete communication failure. To combat disguised jamming for CDMA, we treat the problem in two separate cases: (i) For CDMA systems with public codes which cannot be concealed for some reason (e.g., in civilian GPS), we propose to mitigate the disguised jamming through robust receiver design; (ii) For CDMA systems which allow code concealment, we propose to combat disguised jamming using secure scrambling.

For CDMA systems that fall into the first category, it is impossible to hide the applied codes while simultaneously providing public access. For example, the civilian GPS provides global positioning service by making its civilian codes public to everyone. Hence, hiding the codes from public implies termination of its service. With public codes readily available, a jammer can launch disguised jamming easily and it would be a great hazard to the authorized users. However, we observe that while malicious user can get complete information about the spreading code and pulse shaping filter, they cannot capture the exact timing information of the authorized signal. By exploiting this small time difference between the authorized signal and the jamming interference, the conventional CDMA receiver can be re-designed to achieve robust performance under disguised jamming. More specifically, we propose to estimate the authorized signal, the phase and power level or range of the jamming interference by minimizing the MSE between the received signal and the jammed signal, which is the

sum of the authorized signal and the disguised jamming. The effectiveness of the proposed approach is demonstrated through simulation examples. It is shown that with the proposed receiver design, the BER performance of CDMA can be improved significantly under disguised jamming. At the same time, we can get a good evaluation on how severe the jamming is.

For CDMA systems that fall into the second category, we propose to combat disguised jamming using secure scrambling. More specifically, instead of using conventional scrambling codes, we apply advanced encryption standard (AES) to generate the security-enhanced scrambling codes. Its security is guaranteed by AES, which has been proved to be secure under all known attacks [46]. Assuming ideal synchronization between the authorized user and the jammer, we prove that: the capacity of the conventional CDMA systems without secure scrambling under disguised jamming is actually zero; however, the capacity can be significantly increased when CDMA systems are protected using secure scrambling. The underlying argument is that: the secure scrambling process results in security-enhanced PN codes which are intractable for the malicious user; hence it breaks the symmetricity between the authorized user and the jammer, and ensures positive transmission capacity under disguised jamming.

This chapter is organized as follows. In Section 4.2, the system model is provided together with problem identification. The first jamming mitigation approach with robust receiver design is analyzed in Section 4.3. The second jamming mitigation approach with secure scrambling is elaborated in Section 4.4. Analytical capacity and error probability analysis for CDMA systems with and without secure scrambling is detailed in Section 4.5. Numerical evaluation is conducted in Section 4.6 and we conclude in Section 4.7.

4.2 System Model and Problem Identification

4.2.1 System Model

We consider an individual user in a typical CDMA system. Assuming the processing gain is N, namely, there are N chips per symbol. Let

$$\mathbf{c} = [c_0, c_1, ..., c_{N-1}] \tag{4.1}$$

denote the spreading code, in which $c_n = \pm 1,\ \forall n$. In the isolated pulse case, the general baseband signal of the spreading sequence can be represented as

$$c(t) = \sum_{n=0}^{N-1} c_n g(t - nT_c), \tag{4.2}$$

where $g(t)$ is the pulse shaping filter, T_c the chip period, and we assume

$$\frac{1}{T}\int_0^T c^2(t)dt = 1, \tag{4.3}$$

where $T = NT_c$ is the symbol period.

Let Ω be the constellation, and $u_k \in \Omega$ the kth symbol to be transmitted. The spread chip-rate signal can be expressed as

$$q_n = u_k c_{n-kN}, \tag{4.4}$$

where $k = \lfloor \frac{n}{N} \rfloor$. The successive scrambling process is achieved by

$$z_n = q_n e_n = u_k c_{n-kN} e_n, \tag{4.5}$$

where $e_n = \pm 1$ is a pseudorandom chip-rate scrambling sequence. After pulse shaping, the transmitted signal would then be

$$s(t) = \sum_{n=-\infty}^{\infty} u_k c_{n-kN} e_n g(t - nT_c). \tag{4.6}$$

Note that c_n, e_n and $g(t)$ are real-valued, while u_k can be complex depending on the constellation Ω.

For an AWGN channel, the received signal can be written as

$$y(t) = s(t) + n(t) = \sum_{n=-\infty}^{\infty} u_k c_{n-kN} e_n g(t - nT_c) + n(t), \tag{4.7}$$

where $n(t)$ is the white Gaussian noise.

To recover the transmitted symbols, the CDMA receiver first descrambles the received signal by multiplying a locally generated and synchronized copy of the scrambling sequence, e_n. Afterwards, the received signal will be reduced to

$$y(t) = \sum_{n=-\infty}^{\infty} u_k c_{n-kN} g(t - nT_c) + n(t). \tag{4.8}$$

Without loss of generality, we consider the recovery of the symbol indexed by $k = 0$ and omit the subscript k in u_k. The corresponding signal of interest would be constrained within

$t = [0, T)$, and following the definition in (4.2), we have

$$r(t) = \sum_{n=0}^{N-1} uc_n g(t - nT_c) + n(t) = uc(t) + n(t). \tag{4.9}$$

Performing the despreading process, and following (4.3), the CDMA receiver estimates the transmitted symbol as

$$\hat{u} = \frac{1}{T}\int_0^T r(t)c(t)dt = u + \frac{1}{T}\int_0^T n(t)c(t)dt. \tag{4.10}$$

We can observe from the process above that it is impossible to recover the transmitted symbols without knowing the user's spreading code and scrambling code. This is known as a *built-in security* feature of the CDMA systems. In the following subsection, we will discuss the security level of several typical CDMA systems, and show that: disguised jamming, which mimics the authorized signal, can severely jeopardize the CDMA systems, and in the worst case, leads to complete communication failure.

4.2.2 Problem Identification

Since the spreading codes are generally short and easy to generate, the physical layer built-in security of typical CDMA systems mainly relies on the long pseudorandom scrambling sequence, also known as long code, e.g., in IS-95, 3GPP as well as the military GPS. However, it was shown in [29] that the long scrambling codes used by IS-95 or 3GPP UMTS can be cracked with reasonably high computational complexity. In fact, the maximum complexity to recover the long scrambling codes in IS-95 and 3GPP UMTS is only $O(2^{42})$ and $O(2^{36})$ [29], respectively. As another example, the civilian GPS even makes its codes public to attract

potential users for global competitiveness.

The weakly secured or even public spreading/scrambling codes leave considerable room for malicious users to launch disguised jamming [13–15] towards the authorized signal. The jammer can mimic the authorized signal by generating fake symbols over the cracked or already known codes. With complete knowledge of the code information and the pulse shaping filter, the jammer can launch disguised jamming, which has the similar characteristics as the authorized signal, except that the fake symbol can only be randomly chosen out of Ω. Moreover, there may be small timing and amplitude differences between the authorized signal and the disguised jamming due to non-ideal estimation at the jammer side.

Let $v \in \Omega$ denote the fake symbol, τ the small timing difference, and γ the amplitude ratio of the disguised jamming to the authorized signal. Then, the disguised jamming can be modeled as

$$j(t) = v\gamma c(t-\tau). \tag{4.11}$$

Taking both the noise and disguised jamming into account, and following (4.9), the received signal can be written as

$$r(t) = s(t) + j(t) + n(t) = uc(t) + v\gamma c(t-\tau) + n(t), \tag{4.12}$$

where $n(t)$ is the noise.

An important observation is that: *the conventional CDMA receiver as indicated in (4.10) would fail under disguised jamming.* In fact, replacing the received signal $r(t)$ in (4.10) with (4.12), and following (4.3), we have

$$\hat{u} = u + v\gamma\frac{1}{T}\int_0^T c(t-\tau)c(t)dt + \frac{1}{T}\int_0^T n(t)c(t)dt. \tag{4.13}$$

As can be seen, the symbol estimation would be considerably influenced by the second term in the RHS of (4.13), which is introduced by disguised jamming, especially when τ is small (e.g., $|\tau| < T_c$) and $\gamma \approx 1$. In the worst case, when $\tau = 0$ and $\gamma = 1$, (4.13) is reduced to a very simple form:

$$\hat{u} = u + v + \frac{1}{T}\int_0^T n(t)c(t)dt. \tag{4.14}$$

We can now apply the error probability analysis result in [13], in which it was shown that in this case, the probability of symbol error, $\mathcal{P}_s$, would be lower bounded by

$$\mathcal{P}_s \geq \frac{M-1}{2M}, \tag{4.15}$$

where M is the constellation size of Ω. An intuitive explanation is that: if the authorized symbol "u" and the fake one "v" are distinct, the receiver would have to guess between them as indicated in (4.14). Note that: (i) the error probability of a random guess between two symbols is $\frac{1}{2}$; (ii) the two symbols randomly and independently selected out of Ω by the authorized transmitter and disguised jammer differ with a probability of $\frac{M-1}{M}$. Combining (i) and (ii), it then follows that $\mathcal{P}_s \geq \frac{M-1}{2M}$.

The lower bound in (4.15) sets up a limit for the error probability performance of CDMA systems under the worst-case disguised jamming (i.e., $\tau = 0$ and $\gamma = 1$), which implies that the CDMA communication is completely paralyzed. We intend to solve this problem in two separate cases: (i) For CDMA systems with public codes which cannot be concealed for some reason (e.g., in civilian GPS), in Section 4.3, we propose to mitigate the disguised jamming through robust receiver design. The underlying idea is that the worst disguised jamming can hardly be launched, since the disguised jammer cannot really capture the exact timing and amplitude information of the authorized signal. In a more practical case with regular

disguised jamming, we found that it is possible to mitigate the jamming considerably by taking the timing difference τ and amplitude ratio γ into account in the receiver design. (ii) For CDMA systems which allow code concealment, in Section 4.4, we propose to combat disguised jamming using secure scrambling, which essentially enhances the security of the scrambling codes and hence breaks the symmetricity between the authorized user and the jammer.

4.3 Jamming Mitigation with Robust Receiver Design

For CDMA systems in which the codes cannot be concealed (e.g., civilian GPS) or the transmitters can hardly be upgraded (e.g., satellites in sky), we propose an efficient way to mitigate disguised jamming by robust receiver design. With the public or easily accessed codes, disguised jamming can hardly be prevented. However, the disguised jammer cannot really capture the exact timing and amplitude information of the authorized signal, so small timing and amplitude differences between the authorized signal and disguised jamming may exist. As a result, it is possible to recover the transmitted symbols aided by proper jamming estimation. In this section, we estimate the jamming parameters as well as the authorized symbol using the minimum mean square error (MMSE) criterion. Unlike traditional MSE between the received signal and transmitted signal, the MSE here is calculated between the received signal and jammed signal, which is the sum of the authorized signal and the disguised jamming.

Following (4.6)-(4.7), the aforementioned MSE can be calculated as

$$\begin{aligned}
&J(u,v,\tau,\gamma)\\
=&\frac{1}{T}\int_0^T |r(t)-s(t)-j(t)|^2 dt\\
=&\frac{1}{T}\int_0^T |r(t)-uc(t)-v\gamma c(t-\tau)|^2 dt\\
=&\frac{1}{T}\int_0^T |r(t)-uc(t)|^2 dt - \frac{\gamma v^*}{T}\int_0^T [r(t)-uc(t)]c(t-\tau)dt\\
&-\frac{\gamma v}{T}\int_0^T [r(t)-uc(t)]^* c(t-\tau)dt + \frac{\gamma^2|v|^2}{T}\int_0^T c^2(t-\tau)dt,
\end{aligned} \tag{4.16}$$

where $(\cdot)^*$ denotes the complex conjugate. Since $c(t)$ is T-periodic, following (4.3), we have $\frac{1}{T}\int_0^T c^2(t-\tau)dt = \frac{1}{T}\int_0^T c^2(t)dt = 1$. If we further denote

$$A(u,\tau) = \frac{1}{T}\int_0^T [r(t)-uc(t)]c(t-\tau)dt, \tag{4.17}$$

the MSE can be rewritten as

$$J(u,v,\tau,\gamma) = \frac{1}{T}\int_0^T |r(t)-uc(t)|^2 dt - \gamma v^* A(u,\tau) - \gamma v A^*(u,\tau) + \gamma^2|v|^2. \tag{4.18}$$

Thus, the problem can be formulated as minimizing (4.18) by finding the optimal u, v, τ and γ, i.e.,

$$\{\hat{u},\hat{v},\hat{\tau},\hat{\gamma}\} = \arg\min_{u,v,\tau,\gamma} J(u,v,\tau,\gamma). \tag{4.19}$$

To minimize (4.18), one necessary condition is that its partial derivatives regarding v and γ are zero. Note that when z is a complex variable, we have $\frac{\partial z}{\partial z} = 0$, $\frac{\partial z^*}{\partial z} = 2$ and $\frac{\partial |z|^2}{\partial z} = 2z$.

Hence,

$$\begin{cases} \dfrac{\partial J}{\partial v} = -2\gamma A(u,\tau) + 2\gamma^2 v = 0, & \text{(4.20a)} \\ \dfrac{\partial J}{\partial \gamma} = -v^* A(u,\tau) - v A^*(u,\tau) + 2\gamma |v|^2 = 0, & \text{(4.20b)} \end{cases}$$

from which we can get

$$\gamma = \frac{A(u,\tau)}{v} = \frac{A^*(u,\tau)}{v^*}. \tag{4.21}$$

Substituting (4.21) into (4.18), the MSE can be reduced to

$$J = \frac{1}{T}\int_0^T |r(t) - uc(t)|^2 dt - |A(u,\tau)|^2, \tag{4.22}$$

which is a function depending only on u and τ.

In numerical solution search, limited by the time resolution, τ becomes discrete and thus has only finite possible values with $|\tau| < T_c$. In this way, an exhaustive search[1] on τ and u would be feasible and also an effective approach to minimize (4.22). Let $\hat{u}$ and $\hat{\tau}$ be the solution pair that minimizes (4.22), following (4.21), the amplitude ratio can be estimated as

$$\hat{\gamma} = \frac{|A(\hat{u},\hat{\tau})|}{|v|}. \tag{4.23}$$

For a constant-modulus constellation (e.g., PSK), $|v|$ is readily available since it holds constant for all $v \in \Omega$. For non-constant-modulus constellation, the amplitude ratio cannot be exactly drawn. This is because that from (4.21), we can only determine $\hat{v}\hat{\gamma} = A(\hat{u},\hat{\tau})$, which cannot yield a specific $\hat{\gamma}$ when the amplitude of the jamming symbol is not specifically available. However, in this case, we can obtain a range for $\hat{\gamma}$. More specifically, if $B_1 \leq |v| \leq B_2$

[1]Generally it would be sufficient to perform an exhaustive search for regular time resolution with a practical sampling rate; however, for high time resolution, we suggest the usage of state-of-the-art iterative optimization methods, e.g., Newton's method.

for $v \in \Omega$, then we have

$$\frac{|A(\hat{u},\hat{\tau})|}{B_2} \leq \hat{\gamma} \leq \frac{|A(\hat{u},\hat{\tau})|}{B_1}. \tag{4.24}$$

Discussions: (1) The major differences between the estimation of disguised jamming and that of multipath signals [59,60] lie in: i) Multipath signals always contain the same symbol as the primary signal (which is the signal going through the line-of-sight path), while the symbol carried by disguised jamming is chosen independently from the authorized signal; ii) Multipath signals are generally much weaker than the primary signal, while disguised jamming maintains a similar power level as the authorized signal; iii) Multipath signals always arrive at the receiver after the primary signal, while disguised jamming can have either a leading or lagging phase compared with the authorized signal.

(2) Although we primarily focus on recovering the authorized symbols under disguised jamming here; however, the information obtained from the MMSE receiver can be used for jamming detection and evaluation. The estimated amplitude ratio can be used as a metric to determine whether a disguised jammer is present or not by comparing it with an appropriate threshold. Through cooperation of multiple receivers, it is also possible to locate the disguised jammer by exploiting the estimated timing differences between the jamming interference and the authorized signal.

4.4 Jamming Mitigation with Secure Scrambling

As can be seen in Section 4.2, the physical layer security of most CDMA systems largely relies on the scrambling process. For CDMA systems whose scrambling codes are not adequately secured, to prevent the disguised jamming, we propose to generate the scrambling sequence using the advanced encryption standard (AES), also known as Rijndael.

4.4.1 AES-based Secure Scrambling

Rijndael was identified as the new AES in October 2, 2000. Rijndael's combination of security, performance, efficiency, ease of implementation, and flexibility make it an appropriate selection for the AES. Rijndael is a good performer in both hardware and software across a wide range of computing environments. Its low memory requirements make it very well suited for restricted-space environments such as mobile handset to achieve excellent performance. More details on AES can be found in [45].

The proposed secure scrambling scheme aims to increase the physical layer built-in security of CDMA systems and prevent exhaustive key search attack, while minimizing the changes required to the existing standards. As shown in Fig. 4.1, the secure scrambling sequence is generated through two steps: first, generate a pseudo-noise (PN) sequence, then encrypt the sequence with the AES algorithm. More specifically, a PN sequence is first generated using a PN sequence generator with a secure initialization vector (IV), where the PN sequence generator is typically a linear feedback shift register (LFSR) or Gold sequence generator; subsequently the PN sequence is encrypted by the AES algorithm block by block secured by a secret encryption key, which is shared between the legitimate communication parties.

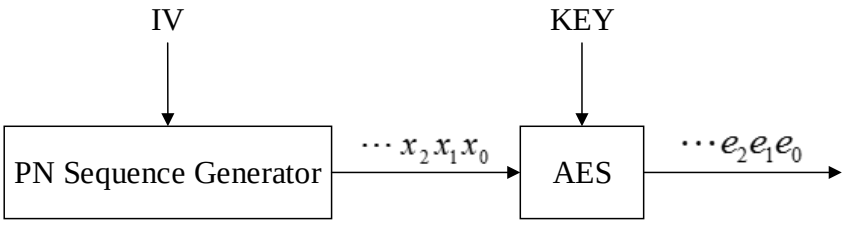


Figure 4.1: Secure scrambling sequence generation.

The secure scrambling process can be summarized as follows:

1. The communication parties share a common initial vector (IV) for the PN sequence generator and an L-bit (L=128, 192, or 256) common secret encryption key;

2. The long scrambling sequence is generated through encryption of a particular segment of the sequence generated from the PN sequence generator using the shared secret key;

3. The scrambling process is realized by adding the scrambling sequence to the chip-rate spread signal.

4.4.2 Security and Implementation Analysis

To eavesdrop the transmitted data or launch disguised jamming, the malicious user has to intercept the secure scrambling sequence used by the legitimate users. Hence, the security of the proposed scrambling process lies in how difficult it is to crack the encrypted scrambling sequence. In this subsection, we use data encryption standard (DES) [61] as a benchmark to evaluate the security of the proposed secure scrambling, which is essentially ensured by AES. We compare the number of possible keys of AES, DES and that of the typical CDMA scrambling sequences. The number of keys determines the effort required to crack the cryptosystem by trying all possible keys.

The most important reason for DES to be replaced by AES is that it is becoming possible to crack DES through exhaustive key search. Single DES uses 56-bit encryption key, which means that there are approximately 7.2×10^{16} possible DES keys. In the late 1990s, specialized "DES cracker" machines were built and they could recover a DES key after a few hours. In other words, by trying all possible keys, the hardware could determine which key was used to encrypt a message. Compared with DES, IS-95 has only 42-bit shared secret (approximately 4.4×10^{12} possible keys), and 3GPP UMTS has even lower security with

36-bit shared secret (approximately 6.9×10^{10} possible keys). This makes it possible to break these low-security scrambling sequences almost in real time through exhaustive key search.

On the other hand, AES specifies three key sizes: 128, 192, and 256 bits. In decimal terms, this means that approximately there are

1. 3.4×10^{38} possible 128-bit keys;
2. 6.2×10^{57} possible 192-bit keys;
3. 1.1×10^{77} possible 256-bit keys.

Thus, if we choose $L = 128$, then there are on the order of 10^{21} times more AES 128-bit keys than DES 56-bit keys. Assuming that one could build a machine that could recover a DES key in a second (i.e., try 2^{56} keys per second), as we can see, this is a very ambitious assumption and far from what we can do today, then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key.

Security measurement through the number of all possible keys is based on the assumption that the attacker has no easy access to the secret encryption key, therefore, the attacker has to perform an exhaustive key search in order to break the system. As is well known, the security of AES is based on the infeasible complexity in recovering the encryption key. Currently, no weakness has been detected for AES, thus, exhaustive key search is still being recognized as the most effective method in recovering the encryption key and breaking the cryptosystem. Based on the calculation above, as long as the encryption key is kept secret, it is impossible for the malicious user to recover the scrambling sequence, and thus disguised jamming can hardly be launched. In this case, the best jamming strategy for the malicious

user would be distributing its total available power uniformly on the spread spectrum by randomly generating a PN sequence as the scrambling sequence.

As will be seen in Section 4.5, under the condition that the jammer has comparable power as the authorized user, the harm of this kind of jamming without knowing the secure scrambling sequence will actually become trivial.

Feasibility: The AES algorithm is one of the block ciphers that can be implemented in different operational modes to generate stream data [62]. High-throughput (3.84 Gbps and higher) AES chips can be found in [63, 64]. In [65], an experiment was performed to measure the AES algorithm performance, where several file sizes from 100 KB to 50 MB were encrypted using a laptop with 2.99 GHz CPU and 2 GB RAM. Based on the results of the experiment, when the AES operates in the cipher feedback (CFB) mode, 554 bytes can be encrypted using 256-bit AES algorithm in 77.3 μs, which is equivalently as high as 57 Mbps. Comparing with the chip rates of regular CDMA systems which are typically below 10 Mbps, the existing hardware would be more than adequate in performing a real-time AES-based secure scrambling sequence generation.

4.5 Capacity Analysis of CDMA Systems with and without Secure Scrambling under Disguised Jamming

Without secure scrambling, the jammer can launch disguised jamming towards the CDMA systems by exploiting the known code information and mimicking the authorized signal. In this case, it has been shown in Section 4.2.2 that the error probability of the symbol

transmission is lower bounded by $\frac{M-1}{2M}$, where M is the constellation size. In this section, by applying the arbitrarily varying channel (AVC) model, we will show that: due to the symmetricity between the authorized signal and jamming interference, the capacity of the traditional CDMA system (i.e., without secure scrambling) under worst disguised jamming is actually zero; on the other hand, with secure scrambling, the shared secure randomness between the transmitter and the receiver breaks the symmetricity between the authorized signal and jamming, and hence ensures positive capacity under worst disguised jamming.

4.5.1 Revisit of the AVC Model

Before proceeding to the analysis of any specific systems, we first briefly revisit the general AVC model and some well-known results corresponding to it. An AVC channel model is generally characterized using a kernel $W : \mathcal{S} \times \mathcal{J} \to \mathcal{Y}$, where $\mathcal{S}$ is the transmitted signal space, $\mathcal{J}$ is the jamming space (i.e., the jamming is viewed as the arbitrarily varying channel states) and $\mathcal{Y}$ is the estimated signal space. For any $\mathbf{s} \in \mathcal{S}$, $\mathbf{j} \in \mathcal{J}$ and $\mathbf{y} \in \mathcal{Y}$, $W(\mathbf{y}|\mathbf{s},\mathbf{j})$ denotes the conditional probability that $\mathbf{y}$ is detected at the receiver, given that $\mathbf{s}$ is the transmitted signal and $\mathbf{j}$ the jamming.

Definition 4.1 ([66]) *The AVC is said to have a symmetric kernel, if* $\mathcal{S} = \mathcal{J}$ *and* $W(\boldsymbol{y}|\boldsymbol{s},\boldsymbol{j}) = W(\boldsymbol{y}|\boldsymbol{j},\boldsymbol{s})$ *for any* $\boldsymbol{s},\boldsymbol{j} \in \mathcal{S}, \boldsymbol{y} \in \mathcal{Y}$.

Definition 4.2 ([66]) *Define* $\hat{W} : \mathcal{S} \times \mathcal{S} \to \mathcal{Y}$ *by* $\hat{W}(\boldsymbol{y}|\boldsymbol{s},\boldsymbol{s}') \triangleq \sum_{\boldsymbol{j}\in\mathcal{J}'} \pi(\boldsymbol{j}|\boldsymbol{s}')W(\boldsymbol{y}|\boldsymbol{s},\boldsymbol{j})$, *where* $\pi : \mathcal{S} \to \mathcal{J}'$ *is a probability matrix and* $\mathcal{J}' \subseteq \mathcal{J}$. *If there exists a* $\pi : \mathcal{S} \to \mathcal{J}'$ *such that* $\hat{W}(\boldsymbol{y}|\boldsymbol{s},\boldsymbol{s}') = \hat{W}(\boldsymbol{y}|\boldsymbol{s}',\boldsymbol{s}), \forall \boldsymbol{s},\boldsymbol{s}' \in \mathcal{S}, \forall \boldsymbol{y} \in \mathcal{Y}$, *then* W *is said to be symmetrizable.*

To help elaborate the physical meaning of these concepts, symmetric and symmetrizable AVC kernels are depicted in Fig. 4.2. In an AVC with a symmetric kernel, jamming

is generated from exactly the same signal space as that of the authorized signal. Even if the roles of the authorized signal and the jamming are switched, the receiver cannot detect any differences, i.e., $W(\mathbf{y}|\mathbf{s},\mathbf{j}) = W(\mathbf{y}|\mathbf{j},\mathbf{s})$. In an AVC with a symmetrizable kernel, jamming is generated or can be viewed as: the jammer excites the main channel via an auxiliary channel $\pi : \mathcal{S} \to \mathcal{J}$, where π is essentially a probability matrix. More specifically, the input of the auxiliary channel comes from exactly the same signal space as that of the authorized signal, and it is transformed by the auxiliary channel and then imposed to the main channel. An AVC kernel is said to be symmetrizable, if there exist an auxiliary channel π, such that even if we switch the authorized signal and the input signal of the auxiliary channel, the receiver cannot tell any differences, i.e., $\hat{W}(\mathbf{y}|\mathbf{s},\mathbf{s}') = \hat{W}(\mathbf{y}|\mathbf{s}',\mathbf{s})$ with $\hat{W}(\mathbf{y}|\mathbf{s},\mathbf{s}') \triangleq \sum_{\mathbf{j}\in\mathcal{J}'} \pi(\mathbf{j}|\mathbf{s}')W(\mathbf{y}|\mathbf{s},\mathbf{j})$. In both cases, the receiver will be confused by the disguised jamming (either generated directly or via an auxiliary channel), which is indistinguishable from the authorized signal. An interesting observation is that: for an AVC kernel, being symmetric is actually a special case of being symmetrizable, where the output of the auxiliary channel equals its input.

Remark 4.1 *In Definition 4.2, $\mathcal{J}'$ can be any finite subset of $\mathcal{J}$. Note that the probability matrix $\pi : \mathcal{S} \to \mathcal{J}'$ can be viewed as a special case of $\pi : \mathcal{S} \to \mathcal{J}$ with zero entries corresponding to the elements that are in $\mathcal{J}$ but not in $\mathcal{J}'$, i.e., $\pi(\boldsymbol{j}|\boldsymbol{s}') = 0,\ \forall \boldsymbol{s}' \in \mathcal{J}\backslash\mathcal{J}'$. Hence, in addressing the existence of the probability matrix, we will hereinafter focus on the case associating to the full set, namely, $\pi : \mathcal{S} \to \mathcal{J}$.*

Concerning the capacity of the AVC channel, it was shown in [66] that: *the deterministic code capacity*[2] *of an AVC for the average probability of error is positive if and only if the*

[2]A deterministic code capacity is defined by the capacity that can be achieved by a communication system, when it applies only one code pattern during the information transmission. In other words, the coding scheme is deterministic and can be readily repeated by other users [66].

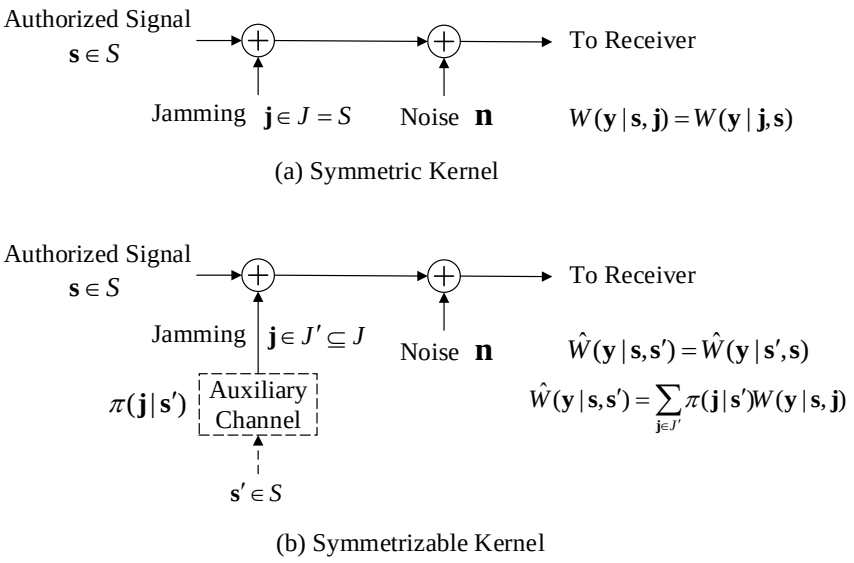


Figure 4.2: An illustration of symmetric and symmetrizable AVC kernels.

AVC is neither symmetric nor symmetrizable.

Next we will analyze the CDMA systems with and without secure scrambling under disguised jamming, by applying the AVC model.

4.5.2 Capacity of CDMA Systems without Secure Scrambling under Disguised Jamming

Without secure scrambling, the codes employed by the authorized user can be regenerated by the jammer, and disguised jamming can thus be generated by applying the same codes but with a fake symbol. If we denote the fake symbol by $v \in \Omega$, in an isolated symbol period, the chip-rate disguised jamming can be represented as

$$\mathbf{j} = v\mathbf{c} = [vc_0, vc_1, ..., vc_{N-1}], \tag{4.25}$$

where $\mathbf{c} = [c_0, c_1, ..., c_{N-1}]$ is the spreading code, and $v \in \Omega$ the fake symbol. The authorized signal can similarly be written as

$$\mathbf{s} = u\mathbf{c} = [uc_0, uc_1, ..., uc_{N-1}], \tag{4.26}$$

where $u \in \Omega$ is the authorized symbol. Taking both the noise and jamming into account, the received chip-rate signal can be written as

$$\mathbf{r} = \mathbf{s} + \mathbf{j} + \mathbf{n}, \tag{4.27}$$

in which $\mathbf{n} = [n_0, n_1, ..., n_{N-1}]$ and $\mathbf{r} = [r_0, r_1, ..., r_{N-1}]$ denote the AWGN noise vector and received signal vector, respectively.

Define the authorized signal space as $\mathcal{S} = \{u\mathbf{c}|u \in \Omega\}$, where $\mathbf{c} = [c_0, c_1, ..., c_{N-1}]$ is the spreading code. It follows immediately that the disguised jamming space

$$\mathcal{J} = \{v\mathbf{c}|v \in \Omega\} = \mathcal{S}. \tag{4.28}$$

Let $\hat{u} \in \Omega$ be the estimated version of the authorized symbol "u" at the receiver, and $W_0(\hat{u}|\mathbf{s}, \mathbf{j})$ the conditional probability that $\hat{u}$ is estimated given that the authorized signal is $\mathbf{s} \in \mathcal{S}$, and the disguised jamming is $\mathbf{j} \in \mathcal{S}$. Thus, the CDMA system under disguised jamming can be modeled as an AVC channel characterized by the probability matrix

$$W_0 : \mathcal{S} \times \mathcal{S} \to \Omega, \tag{4.29}$$

where W_0 is the kernel of the AVC.

As indicated in (4.28), the jamming and the authorized signal are fully symmetric as they are generated from exactly the same space $\mathcal{S}$. Note that the recovery of the authorized symbol is completely based on $\mathbf{r}$ in (4.27), so we further have

$$W_0(\hat{u}|\mathbf{s},\mathbf{j}) = W_0(\hat{u}|\mathbf{j},\mathbf{s}). \tag{4.30}$$

Combining (4.28) and (4.30), and following Definition 4.1, we have the proposition below.

Proposition 4.1 *Under disguised jamming, the kernel of the AVC corresponding to a CDMA system without secure scrambling, W_0, is symmetric.*

The symmetricity of the AVC kernel explains why the error probability of the symbol transmission in CDMA systems without secure scrambling is lower bounded under disguised jamming, as indicated in (4.15). Applying the result in [66] that the deterministic code capacity of an AVC with a symmetric or symmetrizable kernel is zero, the proposition below follows immediately.

Proposition 4.2 *Under disguised jamming, the deterministic code capacity of a CDMA system without secure scrambling is zero.*

4.5.3 Symmetricity Analysis of CDMA Systems with Secure Scrambling under Disguised Jamming

From the discussions above, it can be seen that disguised jamming is destructive to CDMA systems without secure scrambling, as zero capacity implies a complete failure in information transmission. In what follows, we will show how secure scrambling breaks the symmetricity

between the authorized signal and jamming interference, and evaluate the resulted performance gain in terms of error probability and capacity.

When the coding information of the authorized user is securely hidden from the jammer by the proposed secure scrambling scheme, the best strategy for the jammer would be distributing its total available power uniformly over the entire spectrum, since CDMA systems are well known to be resistant to narrowband jamming. To this end, the jammer can spread its power by using a randomly generated spreading sequence. More specifically, if we define $\mathcal{D} = \{[d_0, d_1, ..., d_{N-1}] | d_n = \pm 1, \ \forall n\}$, and denote the randomly generated spreading sequence by $\mathbf{d} \in \mathcal{D}$, the chip-rate jamming sequence can be represented as

$$\mathbf{j} = v\mathbf{d} = [vd_0, vd_1, ..., vd_{N-1}], \tag{4.31}$$

where $v \in \Omega$ is the fake symbol. The jamming space now becomes

$$\mathcal{J} = \{v\mathbf{d} | v \in \Omega, \mathbf{d} \in \mathcal{D}\}. \tag{4.32}$$

We can see that without the coding information $\mathbf{c}$, the jamming, $\mathbf{j}$, can only be generated from a space much larger than the authorized signal space. More specifically, $\mathcal{J} \supset \mathcal{S}$. For any $\mathbf{j} \in \mathcal{J}$, the probability that $\mathbf{j} \in \mathcal{S}$ (i.e., the jamming falls into the authorized signal space by coincidentally repeating the authorized code $\mathbf{c}$ or its negative) is $\frac{1}{2^{N-1}}$, which approaches zero when N is reasonably large.

With the jamming space $\mathcal{J}$ as defined in (4.32), the AVC corresponding to the CDMA system with secure scrambling can be characterized by

$$W : \mathcal{S} \times \mathcal{J} \to \Omega. \tag{4.33}$$

Based on the discussion above, $\mathcal{J} \neq \mathcal{S}$. That is, the jamming and the authorized signal are no longer symmetric. Following Definition 4.1, we have the proposition below.

Proposition 4.3 *Under disguised jamming, the kernel of the AVC corresponding to a CDMA system with secure scrambling, W, is nonsymmetric.*

Next, we will prove a stronger result: *W is actually nonsymmetrizable.* According to Definition 4.2, we need to show that for any probability matrix $\pi : \mathcal{S} \to \mathcal{J}$, there exists some $\mathbf{s}_0, \mathbf{s}_0' \in \mathcal{S}$ and $\hat{u}_0 \in \Omega$, such that

$$\hat{W}(\hat{u}_0|\mathbf{s}_0, \mathbf{s}_0') \neq \hat{W}(\hat{u}_0|\mathbf{s}_0', \mathbf{s}_0), \tag{4.34}$$

where $\hat{W}(\hat{u}|\mathbf{s}, \mathbf{s}') \triangleq \sum_{\mathbf{j}\in\mathcal{J}} \pi(\mathbf{j}|\mathbf{s}')W(\hat{u}|\mathbf{s}, \mathbf{j})$. To prove it, we present three lemmas first.

Lemma 4.1 *In a complex plane, there are two pairs of symmetric points, (u_1, u_2) and (v_1, v_2), which share the same axis of symmetry. Suppose u_1 and v_1 are located on one side of the axis of symmetry, while u_2 and v_2 reside on the other side. For any point p, if $|p - u_1| \leq |p - u_2|$, then $|p - v_1| \leq |p - v_2|$, where the equality holds if and only if $|p - u_1| = |p - u_2|$.*

Proof: From $|p - u_1| \leq |p - u_2|$, we know that p is either on the same side with u_1 or exactly on the axis of symmetry. If p is on the same side with u_1, i.e., $|p - u_1| < |p - u_2|$, since u_1 and v_1 are on the same side, hence p and v_1 are on the same side. Since v_2 is on the other side, it follows immediately that $|p - v_1| < |p - v_2|$. If p is exactly on the axis of symmetry, i.e., $|p - u_1| = |p - u_2|$, then $|p - v_1| = |p - v_2|$. Similarly, if $|p - v_1| = |p - v_2|$, then $|p - u_1| = |p - u_2|$. □

Define $R(u)$ as the region of detection for symbol $u \in \Omega$ in the complex plane, which means that any received symbol located in this region will be decided as "u" by a minimum distance detector. That is, for any point $p \in R(u)$, any symbol $v \in \Omega$ and $v \neq u$, we always have $|p-u| < |p-v|$. Furthermore, for a pair of symmetric symbols from a symmetric constellation[3], $(u, -u)$, their regions of detection, $R(u)$ and $R(-u)$, are said to be axial symmetric, if for any point $p \in R(u)$, there always exists a point $M(p) \in R(-u)$, such that $(p, M(p))$ and $(u, -u)$ share the same axis of symmetry. Such a point, $M(p)$, is called the *symmetric point* of p with respect to the axis of symmetry for $(u, -u)$. The shaded areas of Fig. 4.3 illustrate the regions of detection for two symmetric symbols, which are axial symmetric with respect to the axis of symmetry given in the figure.

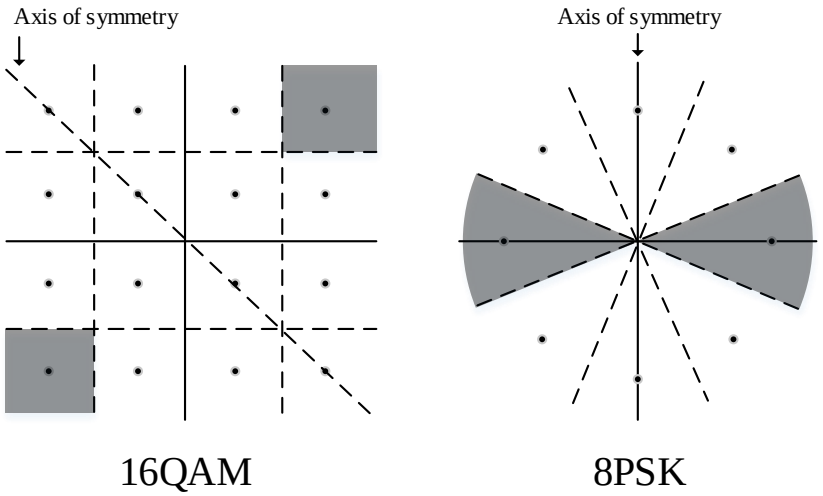


Figure 4.3: Illustration of symmetric symbols with axial symmetric regions of detection.

Lemma 4.2 *Assume the received symbol is $r = u + z + n$, where $u \in \Omega$ is the transmitted symbol, z a fixed complex deviation with $|z| \leq |u|$, and $n \sim \mathcal{CN}\left(0, \sigma^2\right)$ the complex Gaussian noise. If the regions of detection, $R(u)$ and $R(-u)$, are axial symmetric, then we have $W(u|u,z) \geq W(-u|u,z)$, where the equality holds if and only if $z = -u$.*

[3]A constellation Ω is said to be symmetric, if for any $u \in \Omega$, we always have $-u \in \Omega$. For maximum power efficiency, traditional constellations in use are generally symmetric, e.g., PSK and QAM.

Proof: For the received symbol $r = u + z + n$, where "u" is the transmitted symbol, "z" is the fixed deviation and $n \sim \mathcal{CN}\left(0, \sigma^2\right)$, r follows a complex Gaussian distribution, $r \sim \mathcal{CN}\left(u + z, \sigma^2\right)$. Hence, the conditional probability that the received symbol will be decided as "u" given that the actually transmitted symbol is "u" and the fixed deviation is "z" can be calculated as

$$W(u|u, z) = \int_{r \in R(u)} f_R(r) dr, \tag{4.35}$$

where $f_R(r) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left\{-\frac{|r-(u+z)|^2}{2\sigma^2}\right\}$ is the probability density function of r. Similarly, the probability that the received symbol will be decided as "$-u$" given that the actually transmitted symbol is "u" and the fixed deviation is "z" can be calculated as

$$W(-u|u, z) = \int_{r \in R(-u)} f_R(r) dr = \int_{r \in R(u)} f_R(M(r)) dr. \tag{4.36}$$

Note that the two regions of detection, $R(u)$ and $R(-u)$, are axial symmetric, and $M(r)$ is the symmetric point of r with respect to the axis of symmetry for $(u, -u)$.

Let $p = u + z$, $u_1 = u$ and $u_2 = -u$. Since $|z| \leq |u|$,

$$|p - u_1| - |p - u_2| = |z| - |2u + z| \leq 0, \tag{4.37}$$

where the equality holds if and only if $z = -u$. For any $r \in R(u)$, r must be on the same side with $u_1 = u$ relative to the axis of symmetry for $(u, -u)$, and $M(r)$ must be on the same side with $u_2 = -u$, as illustrated in Fig. 4.3. Applying Lemma 4.1, it follows from (4.37) that

$$|p - r| - |p - M(r)| = |r - (u + z)| - |M(r) - (u + z)| \leq 0, \ \forall r \in R(u), \tag{4.38}$$

where the equality holds if and only if $z = -u$. Thus, we have

$$\begin{aligned} & W(u|u,z) - W(-u|u,z) \\ &= \int_{r \in R(u)} [f_R(r) - f_R(M(r))] dr \\ &= \int_{r \in R(u)} \frac{1}{\sqrt{2\pi}\sigma} \left[\exp\left\{ -\frac{|r-(u+z)|^2}{2\sigma^2} \right\} - \exp\left\{ -\frac{|M(r)-(u+z)|^2}{2\sigma^2} \right\} \right] dr. \end{aligned} \tag{4.39}$$

Applying (4.38) to (4.39), we have

$$W(u|u,z) - W(-u|u,z) \geq 0, \tag{4.40}$$

where the equality holds if and only if $z = -u$. □

Lemma 4.3 *Assume the received signal is $\boldsymbol{r} = \boldsymbol{s} + \boldsymbol{j} + \boldsymbol{n}$, where $\boldsymbol{s} = u\boldsymbol{c}$ is the signal vector with $u \in \Omega$ as the transmitted symbol and $\boldsymbol{c}$ as the spreading code, $\boldsymbol{j} \in \mathcal{J} = \{v\boldsymbol{d} | v \in \Omega, \boldsymbol{d} \in \mathcal{D}\}$ is the jamming vector, and $\boldsymbol{n}$ is the noise vector. If the regions of detection, $R(u)$ and $R(-u)$, are axial symmetric, and $|u| \geq |v|$, $\forall v \in \Omega$, then we have $W(u|\boldsymbol{s}, \boldsymbol{j}) \geq W(-u|\boldsymbol{s}, \boldsymbol{j})$, where the equality holds if and only if $\boldsymbol{j} = -\boldsymbol{s}$.*

Proof: With $\mathbf{r} = \mathbf{s} + \mathbf{j} + \mathbf{n}$, the despread signal at the receiver would be

$$r = \frac{1}{N} \sum_{n=0}^{N-1} r_n c_n = u + \frac{v}{N} \sum_{n=0}^{N-1} c_n d_n + \frac{1}{N} \sum_{n=0}^{N-1} c_n n_n. \tag{4.41}$$

Let $z = \frac{v}{N} \sum_{n=0}^{N-1} c_n d_n$ and $n = \frac{1}{N} \sum_{n=0}^{N-1} c_n n_n$. Note that for all n, $c_n = \pm 1$, so the despread noise n would follow a complex Gaussian distribution, i.e., $n \sim \mathcal{CN}(0, \frac{\sigma_n^2}{N})$, where σ_n^2 is the original noise power before despreading. Hence, the recovered symbol, $r = u + z + n$, is

actually the transmitted symbol "u" distorted by a fixed deviation z and a complex Gaussian noise n.

Since $|v| \leq |u|$, and for all n, $c_n = \pm 1$, $d_n = \pm 1$, we know that $|z| = |\frac{v}{N} \sum_{n=0}^{N-1} c_n d_n| \leq |u|$. Applying Lemma 4.2, we have $W(u|u,z) \geq W(-u|u,z)$, where the equality holds if and only if $z = \frac{v}{N} \sum_{n=0}^{N-1} c_n d_n = -u$. We then prove that $z = -u$ is equivalent to $\mathbf{j} = -\mathbf{s}$. On one hand, if $z = -u$, then $|z| = |u|$. Considering $|v| \leq |u|$ and $|\frac{1}{N} \sum_{n=0}^{N-1} c_n d_n| \leq 1$, we must have $|v| = |u|$ and $|\frac{1}{N} \sum_{n=0}^{N-1} c_n d_n| = 1$. There are only two cases that satisfy $z = -u$: (1) $v = -u$ and $d_n = c_n$, $\forall n$; (2) $v = u$ and $d_n = -c_n$, $\forall n$. Both cases lead to $\mathbf{j} = v\mathbf{d} = -u\mathbf{c} = -\mathbf{s}$. On the other hand, if $\mathbf{j} = -\mathbf{s}$, then it leads to the same two cases as above, both of which satisfy $z = -u$.

Due to the equivalence between the signals before and after despreading as shown in (4.41), we have $W(u|u,z) = W(u|\mathbf{s},\mathbf{j})$ and $W(-u|u,z) = W(-u|\mathbf{s},\mathbf{j})$. It then follows immediately that $W(u|\mathbf{s},\mathbf{j}) \geq W(-u|\mathbf{s},\mathbf{j})$, where the equality holds if and only if $\mathbf{j} = -\mathbf{s}$. □

Proposition 4.4 *Under disguised jamming, the kernel of the AVC corresponding to a CDMA system with secure scrambling, W, is nonsymmetrizable.*

Proof: We will show that for any probability matrix $\pi : \mathcal{S} \to \mathcal{J}$, there exists some $\mathbf{s}_0, \mathbf{s}_0' \in \mathcal{S}$ and $\hat{u}_0 \in \Omega$, such that

$$\hat{W}(\hat{u}_0|\mathbf{s}_0,\mathbf{s}_0') \neq \hat{W}(\hat{u}_0|\mathbf{s}_0',\mathbf{s}_0), \tag{4.42}$$

where $\hat{W}(\hat{u}|\mathbf{s},\mathbf{s}') \triangleq \sum_{\mathbf{j}\in\mathcal{J}} \pi(\mathbf{j}|\mathbf{s}') W(\hat{u}|\mathbf{s},\mathbf{j})$. To this end, we pick $\mathbf{s}_0 = u\mathbf{c}$, $\mathbf{s}_0' = -u\mathbf{c}$, $\hat{u}_1 = u$ and $\hat{u}_2 = -u$. Note that "u" is picked such that $R(u)$ and $R(-u)$ are axial symmetric, and

$|u| \geq |v|$, $\forall v \in \Omega$, as illustrated in Fig. 4.3. We will prove that $\hat{W}(\hat{u}_1|\mathbf{s}_0, \mathbf{s}_0') = \hat{W}(\hat{u}_1|\mathbf{s}_0', \mathbf{s}_0)$ and $\hat{W}(\hat{u}_2|\mathbf{s}_0, \mathbf{s}_0') = \hat{W}(\hat{u}_2|\mathbf{s}_0', \mathbf{s}_0)$ cannot hold simultaneously, by showing that

$$\hat{W}(\hat{u}_1|\mathbf{s}_0, \mathbf{s}_0') - \hat{W}(\hat{u}_2|\mathbf{s}_0, \mathbf{s}_0') > \hat{W}(\hat{u}_1|\mathbf{s}_0', \mathbf{s}_0) - \hat{W}(\hat{u}_2|\mathbf{s}_0', \mathbf{s}_0). \tag{4.43}$$

Following the definition of $\hat{W}$, we have

$$\begin{aligned} &\hat{W}(\hat{u}_1|\mathbf{s}_0, \mathbf{s}_0') - \hat{W}(\hat{u}_2|\mathbf{s}_0, \mathbf{s}_0') \\ =&\sum_{\mathbf{j}\in\mathcal{J}} \pi(\mathbf{j}|\mathbf{s}_0') W(\hat{u}_1|\mathbf{s}_0, \mathbf{j}) - \sum_{\mathbf{j}\in\mathcal{J}} \pi(\mathbf{j}|\mathbf{s}_0') W(\hat{u}_2|\mathbf{s}_0, \mathbf{j}) \\ =&\sum_{\mathbf{j}\in\mathcal{J}} \pi(\mathbf{j}|\mathbf{s}_0')[W(\hat{u}_1|\mathbf{s}_0, \mathbf{j}) - W(\hat{u}_2|\mathbf{s}_0, \mathbf{j})]. \end{aligned} \tag{4.44}$$

Note that $W(\hat{u}_1|\mathbf{s}_0, \mathbf{j})$ and $W(\hat{u}_2|\mathbf{s}_0, \mathbf{j})$ denote the probabilities that the received symbol is decided as $\hat{u}_1 = u$ and $\hat{u}_2 = -u$, respectively, given that the transmitted signal is $\mathbf{s}_0$ and the jamming is $\mathbf{j}$. Applying Lemma 4.3, we have

$$W(\hat{u}_1|\mathbf{s}_0, \mathbf{j}) \geq W(\hat{u}_2|\mathbf{s}_0, \mathbf{j}), \tag{4.45}$$

where the equality holds if and only if $\mathbf{j} = -\mathbf{s}_0$. Substituting (4.45) into (4.44), it follows immediately that

$$\hat{W}(\hat{u}_1|\mathbf{s}_0, \mathbf{s}_0') - \hat{W}(\hat{u}_2|\mathbf{s}_0, \mathbf{s}_0') \geq 0, \tag{4.46}$$

where the equality holds if and only if $\pi(\mathbf{j}|\mathbf{s}_0') = 0$, $\forall \mathbf{j} \neq -\mathbf{s}_0$. This means that $\hat{W}(\hat{u}_1|\mathbf{s}_0, \mathbf{s}_0') = \hat{W}(\hat{u}_2|\mathbf{s}_0, \mathbf{s}_0')$ occurs only when the jammer can *always* generate the jamming exactly as the opposite to the authorized signal, which is impossible since the jammer has no knowledge how the spreading sequence $\mathbf{c}$ is encrypted and changes at each symbol period. Based on

the observation above, we further have

$$\hat{W}(\hat{u}_1|\mathbf{s}_0, \mathbf{s}_0') - \hat{W}(\hat{u}_2|\mathbf{s}_0, \mathbf{s}_0') > 0. \tag{4.47}$$

Applying the same methodology, we can show that

$$\hat{W}(\hat{u}_1|\mathbf{s}_0', \mathbf{s}_0) - \hat{W}(\hat{u}_2|\mathbf{s}_0', \mathbf{s}_0) < 0. \tag{4.48}$$

Combining (4.47) and (4.48), we have

$$\hat{W}(\hat{u}_1|\mathbf{s}_0, \mathbf{s}_0') - \hat{W}(\hat{u}_2|\mathbf{s}_0, \mathbf{s}_0') > \hat{W}(\hat{u}_1|\mathbf{s}_0', \mathbf{s}_0) - \hat{W}(\hat{u}_2|\mathbf{s}_0', \mathbf{s}_0), \tag{4.49}$$

which shows that $\hat{W}(\hat{u}_1|\mathbf{s}_0, \mathbf{s}_0') = \hat{W}(\hat{u}_1|\mathbf{s}_0', \mathbf{s}_0)$ and $\hat{W}(\hat{u}_2|\mathbf{s}_0, \mathbf{s}_0') = \hat{W}(\hat{u}_2|\mathbf{s}_0', \mathbf{s}_0)$ cannot hold simultaneously. □

Since the kernel corresponding to a CDMA system with secure scrambling under disguised jamming, W, is neither symmetric (Proposition 4.3) nor symmetrizable (Proposition 4.4), we have the proposition below.

Proposition 4.5 *Under disguised jamming, the deterministic code capacity of a CDMA system with secure scrambling is not zero.*

Discussions: Proposition 4.4 shows that the kernel of the AVC corresponding to a CDMA system with secure scrambling is nonsymmetrizable, except when the jammer can always generate the jamming as exactly as the negative of the authorized signal. However, this is computationally impossible, since it is equivalent to break AES applied in secure

scrambling, which has been proved to be secure under all known attacks.

An aggressive jammer can probably launch jamming consisting of multiple spreading codes, in order to increase the probability that one of its applied codes coincides with the one applied by the authorized user. When the number of spreading codes covered by the jammer is small, the harm to the authorized communication would be negligible. While using multiple spreading codes produces more effective jamming, the power consumption can be forbiddingly high. However, it does indicate that: when the user information (including both symbol and codes) is unknown, the most effective jamming is still Gaussian, resulting from accumulation of a large number of spreading codes and the central limit theorem (CLT).

4.5.4 Capacity Calculation of CDMA Systems with Secure Scrambling under Disguised Jamming

So far we have shown that: in CDMA systems with secure scrambling, the symmetricity between the authorized signal and the disguised jamming is broken, and hence the capacity is no longer zero. A natural question is: what is the capacity then? Although it is difficult to derive a modulation-specific capacity, we manage to provide a general analysis on the capacity by applying the Shannon Formula as stated below. For particular modulation schemes like QAM and PSK, the error probabilities of symbol transmission will also be provided.

Recall that at the receiver, the despread symbol under disguised jamming can be calculated as

$$r = \frac{1}{N}\sum_{n=0}^{N-1} r_n c_n = u + \frac{v}{N}\sum_{n=0}^{N-1} c_n d_n + \frac{1}{N}\sum_{n=0}^{N-1} c_n n_n. \tag{4.50}$$

Note that for all n, $c_n = \pm 1$ are constant, while $d_n = \pm 1$ are statistically independent and identically distributed (i.i.d.) binary random variables with zero mean and variance 1.

Applying the central limit theorem (CLT), $\frac{1}{N}\sum_{n=0}^{N-1} c_n d_n$ would follow a complex Gaussian distribution with zero mean and variance $\frac{1}{N}$, i.e.,

$$\frac{1}{N}\sum_{n=0}^{N-1} c_n d_n \sim \mathcal{CN}\left(0, \frac{1}{N}\right). \tag{4.51}$$

Similarly, we have

$$\frac{1}{N}\sum_{n=0}^{N-1} c_n n_n \sim \mathcal{CN}\left(0, \frac{\sigma_n^2}{N}\right), \tag{4.52}$$

where σ_n^2 is the original noise power before despreading. It then follows that r is also a complex Gaussian variable, whose distribution can be characterized by

$$r \sim \mathcal{CN}\left(u, \frac{|v|^2}{N} + \frac{\sigma_n^2}{N}\right), \tag{4.53}$$

which implies that for an arbitrary transmitted symbol $u \in \Omega$ and an arbitrary fake symbol $v \in \Omega$ in (4.50), the received symbol is actually the transmitted symbol "u" polluted by a complex Gaussian noise, $n \sim \mathcal{CN}\left(0, \frac{|v|^2}{N} + \frac{\sigma_n^2}{N}\right)$.

Let σ_s^2 denote the average symbol power, namely, $\mathcal{E}\{|u|^2\} = \sigma_s^2$, where $u \in \Omega$. Based on (4.53), for a specific fake symbol $v \in \Omega$, the corresponding signal-to-jamming-and-noise ratio (SJNR) can be calculated as

$$\gamma(v) = \frac{\sigma_s^2}{|v|^2/N + \sigma_n^2/N} = \frac{N\sigma_s^2}{|v|^2 + \sigma_n^2}. \tag{4.54}$$

The symbol error probability largely depends on the employed constellation Ω. However, with SJNR available, and considering all possible $v \in \Omega$, the average symbol error probability

can be calculated as

$$\mathcal{P}_s = \frac{1}{|\Omega|}\sum_{v\in\Omega}\mathcal{P}_\Omega(\gamma(v)) = \frac{1}{|\Omega|}\sum_{v\in\Omega}\mathcal{P}_\Omega\left(\frac{N\sigma_s^2}{|v|^2+\sigma_n^2}\right), \tag{4.55}$$

where $|\Omega|$ denotes the constellation size, and $\mathcal{P}_\Omega(\cdot)$ is readily available in [48, eqn. (5.2-78) & (5.2-79), page 278] for QAM and [48, eqn. (5.2-56), page 268] for PSK, respectively.

To calculate the capacity, a CDMA system which operates over a spectrum of B Hz can be equivalently viewed as a narrowband transmission with a bandwidth of $\frac{B}{N}$, while simultaneously having its SJNR level increased to (4.54) as a result of the processing gain. Hence, the capacity can be obtained as

$$C = \frac{B}{N}\frac{1}{|\Omega|}\sum_{v\in\Omega}\log_2(1+\gamma(v)) = \frac{B}{N}\frac{1}{|\Omega|}\sum_{v\in\Omega}\log_2\left(1+\frac{N\sigma_s^2}{|v|^2+\sigma_n^2}\right). \tag{4.56}$$

For clarity, we summarize the analysis above in Table 4.1. It can be seen that: 1) The symbol error probability of a CDMA system under disguised jamming can be decreased significantly using the secure scrambling scheme, compared with the lower-bounded error probability without secure scrambling, especially when the processing gain, N, is large. 2) With secure scrambling, the capacity of a CDMA system will no longer be zero.

Overall, we would like to point out that: based on the shared secret between the authorized transmitter and receiver, secure scrambling enhances the randomness in the CDMA spreading process and makes it forbiddingly difficult for the malicious user to launch disguised jamming. Our results echo the observations in [13, 16, 66–68], where random coding is viewed as a promising solution in combating disguised jamming.

Table 4.1: Comparison of CDMA Systems with and without Secure Scrambling under Disguised Jamming.

	Without Secure Scrambling	With Secure Scrambling
Symmetric	Yes	No
Symmetrizable	N/A	No
SJNR	N/A	$\frac{N\sigma_s^2}{\lvert v\rvert^2+\sigma_n^2},\ v \in \Omega$
Error Probability	$\geq \frac{M-1}{2M}$	$\frac{1}{\lvert\Omega\rvert}\sum_{v\in\Omega}\mathcal{P}_\Omega\left(\frac{N\sigma_s^2}{\lvert v\rvert^2+\sigma_n^2}\right)$
Capacity	0	$\frac{B}{N}\frac{1}{\lvert\Omega\rvert}\sum_{v\in\Omega}\log_2\left(1+\frac{N\sigma_s^2}{\lvert v\rvert^2+\sigma_n^2}\right)$

4.6 Numerical Results

In this section, we numerically evaluate the effectiveness of the proposed jamming mitigation schemes: robust receiver design and secure scrambling. In what follows, we assume AWGN channels, and launch two separate simulation settings from practical CDMA systems, which, we believe, provide good examples in potential applications of the proposed schemes.

4.6.1 Jamming Mitigation with Robust Receiver Design

In this subsection, through several simulation examples, we first evaluate the performance degradation of CDMA systems under disguised jamming, and then demonstrate the effectiveness of the proposed receiver design in jamming estimation and BER performance improvement. In the simulation, we adopt the settings as in civilian GPS, where BPSK modulation is applied and the spreading code is a Gold sequence with a processing gain $N = 1023$. Note that the civilian GPS has public spreading codes, and it is exactly one of the scenarios where the robust receiver design is needed in order to avoid the code concealment. Moreover, we set the oversampling factor to 32, which means that there are 32 samples in

each chip with a T_c duration. Note that the oversampling factor determines the resolution of the timing difference estimation, i.e., $\frac{1}{32}T_c$, for the current setting.

1) Performance Degradation of Conventional CDMA Systems under Disguised Jamming In this simulation example, we evaluate the impact of disguised jamming with different timing differences on the BER performance of the conventional CDMA system. The amplitude ratio γ is set to 1, and we apply the conventional CDMA receiver as in (4.10) without any jamming estimation. It is observed from Fig. 4.4 that comparing with jamming-free case, the BER performance is severely degraded by the disguised jamming, especially when the timing difference τ is small. In the worst case with $\tau = 0$, the BER maintains at approximately $\frac{1}{4}$ no matter how high the SNR is, which agrees with the lower bound in (4.15).

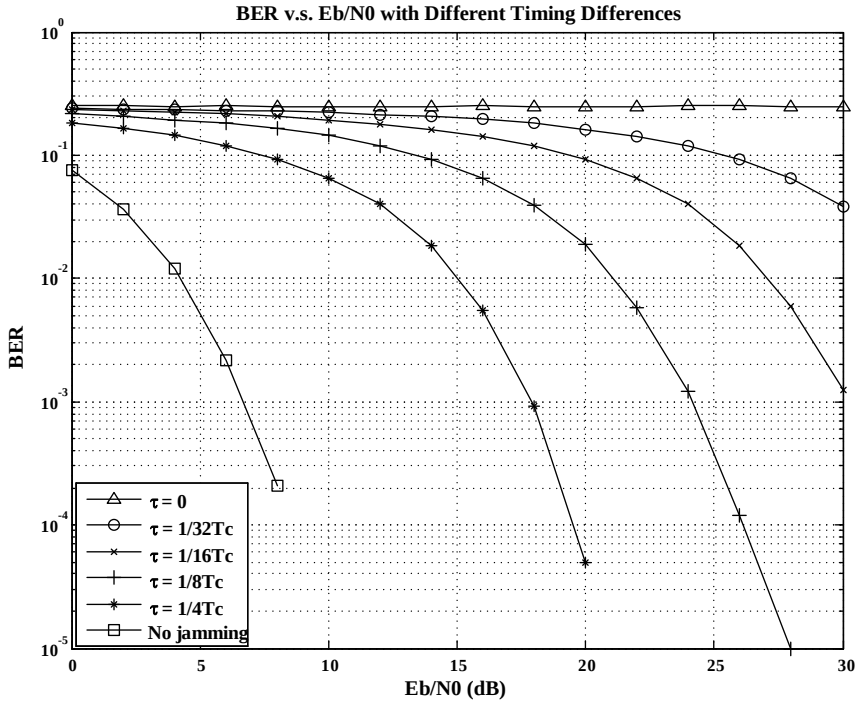


Figure 4.4: BER v.s. Eb/N0 for the conventional CDMA receiver under various disguised jamming.

2) Timing Difference and Amplitude Ratio Estimation In this simulation exam-

ple, we provide the estimation results of the timing difference τ and amplitude ratio γ by applying the proposed CDMA receiver. Here we set $\tau = \frac{1}{4}T_c$ and $\gamma = 1.2$. In Fig. 4.5, we can observe that both the timing difference and amplitude ratio can be accurately estimated with reasonable SNRs, and the accuracy improves as the SNR increases.

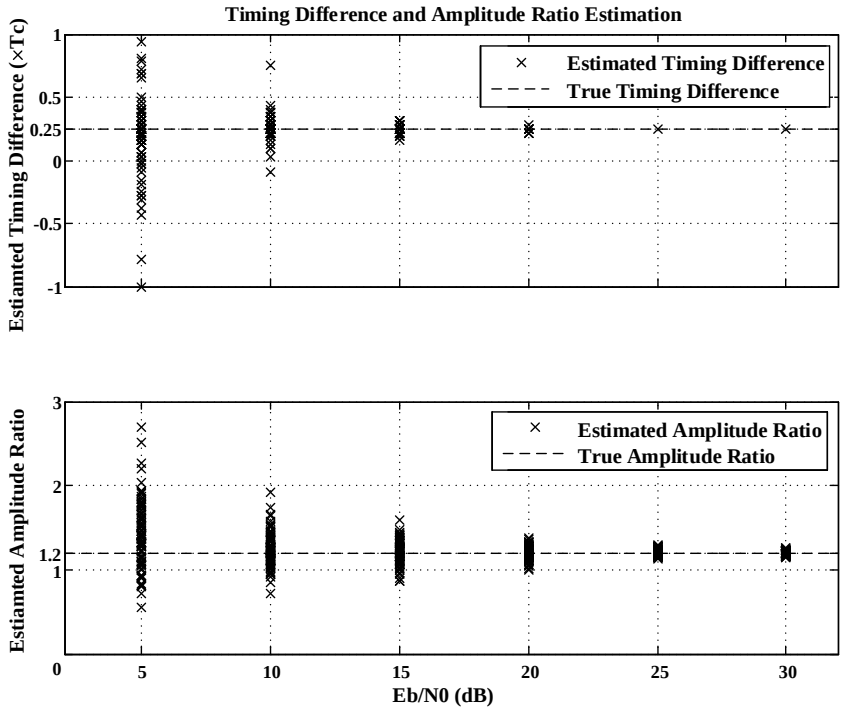


Figure 4.5: Timing difference and amplitude ratio estimation.

3) BER Performance Improvement with Jamming Estimation In this simulation example, we compare the BER performance of the proposed CDMA receiver with that of the conventional receiver. To explore a time-varying jamming scenario, the timing difference τ is set to be uniformly distributed on $[-\frac{1}{4}T_c, 0) \cup (0, \frac{1}{4}T_c]$, and the amplitude ratio γ follows a normal distribution $\mathcal{N}(1, \sigma^2)$, where $\sigma = \frac{1}{6}$. Note that we do not take into account $\tau = 0$, in which case the BER cannot be decreased because of the lower bound in (4.15). In Fig. 4.6, it is observed that the BER is decreased significantly by the proposed CDMA receiver with reasonable SNRs. With low SNRs, the BER cannot be decreased due to

the inaccurate jamming estimation, which demonstrates that it is more difficult to combat disguised jamming under poor channel conditions.

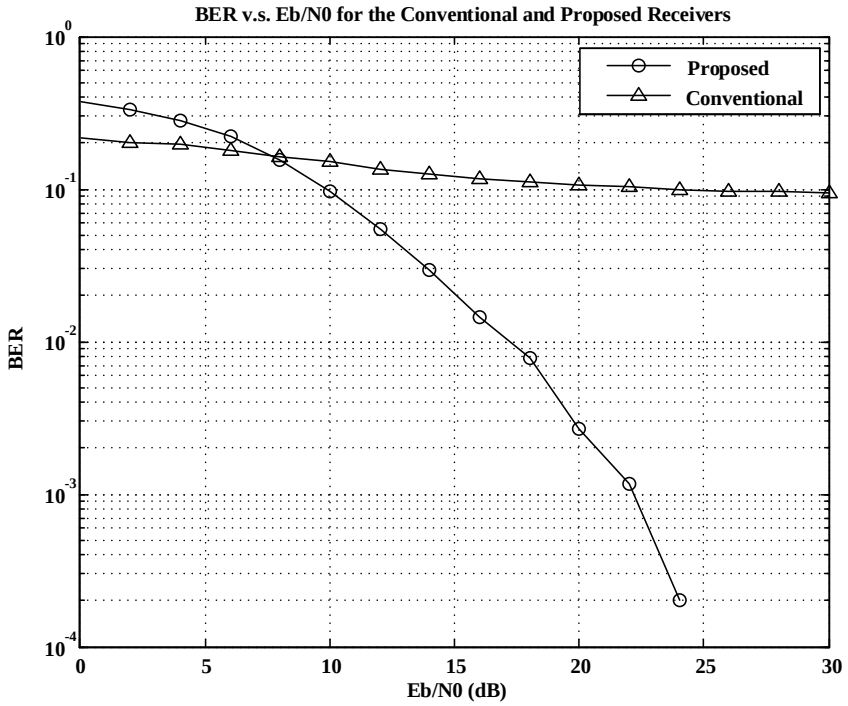


Figure 4.6: Performance comparison of the conventional receiver and the proposed receiver under disguised jamming.

To evaluate how well the proposed receiver works with different but fixed timing differences, we compare the performance of the conventional receiver with that of the proposed receiver regrading different timing differences in Fig. 4.7, where the amplitude ratio γ is set to 1. It is observed that: (i) For nonzero timing differences, the BER is decreased significantly by the proposed CDMA receiver with reasonable SNRs; (ii) For the worst disguised jamming with zero timing difference, the proposed receiver design cannot help at all, in which case we should consider using secure scrambling to break the symmetricity.

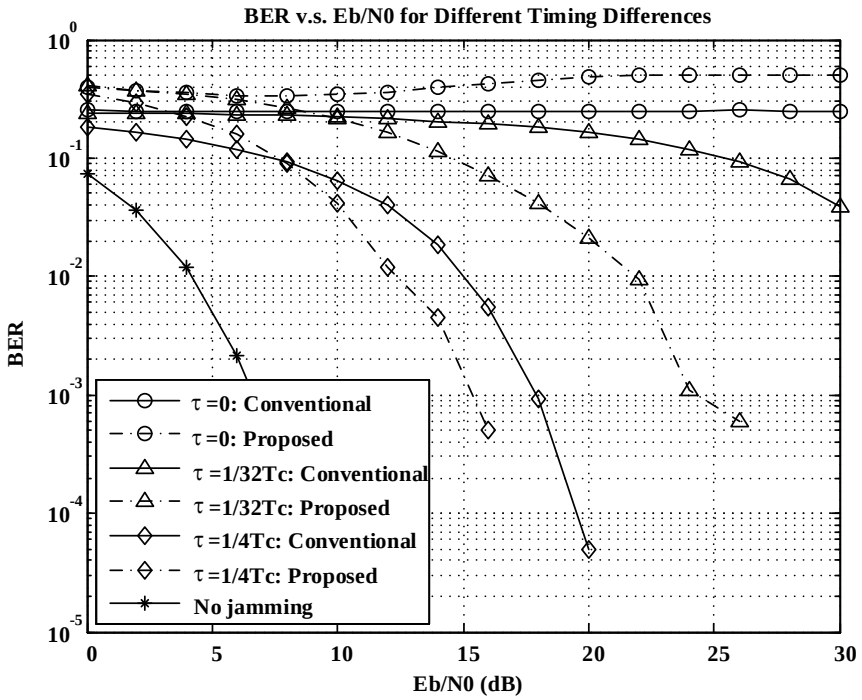


Figure 4.7: BER v.s. Eb/N0 for different timing differences.

4.6.2 Jamming Mitigation with Secure Scrambling

In this subsection, we numerically show the effectiveness of the secure scrambling in combating disguised jamming for CDMA systems whose scrambling codes can potentially be protected. In the simulation, we adopt Walsh codes with a processing gain $N = 64$ as the spreading codes, and apply 16QAM modulation. The symbol error rates (SERs) of CDMA systems are shown in Fig. 4.8 associating with the following four conditions: a) jamming-free case as the benchmark; b) under disguised jamming but without secure scrambling; c) under disguised jamming and with secure scrambling; d) the theoretical result for the case in c) as a verification.

In Fig. 4.8, it is observed that: 1) Without secure scrambling, the symbol error rate of CDMA communication under disguised jamming maintains at a extremely high level no matter how high the SNR is, which shows that the CDMA communication is severely

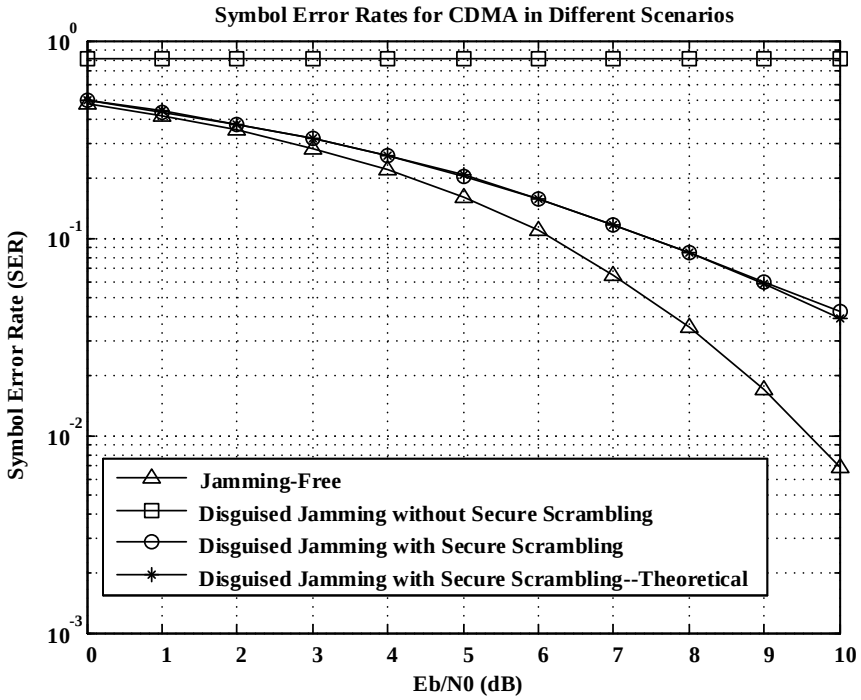


Figure 4.8: Symbol error rates (SERs) for CDMA in Different Scenarios.

paralyzed by disguised jamming; 2) The secure scrambling scheme significantly improves the performance of CDMA communication under disguised jamming, where the SER curve matches the theoretical result as indicated in (4.55) as well; 3) The SER curve using secure scrambling under disguised jamming is quite close to that of the jamming-free case, and it can be expected that the gap will become even smaller if we have a larger processing gain N.

4.7 Summary

In this chapter, we analyzed the impact of disguised jamming on conventional CDMA systems, and developed two effective approaches to mitigate the jamming effect for two different categories of CDMA systems. *For CDMA systems with public codes which cannot be concealed for some reason*, we mitigated the disguised jamming through robust receiver design.

The proposed approach exploited the small timing difference between the authorized signal and the jamming interference. We estimated the authorized symbols as well as the jamming parameters by finding the minimum mean square error (MMSE) between the received signal and jammed signal, which is the sum of the authorized signal and the disguised jamming. The numerical results demonstrated that with reasonable SNRs, the proposed receiver significantly improves the BER performance of CDMA systems under disguised jamming, and also provides a good evaluation about jamming. *For CDMA systems which allow code concealment*, we mitigated disguised jamming using secure scrambling. Instead of using conventional scrambling codes, we applied advanced encryption standard (AES) to generate the security-enhanced scrambling codes. Theoretical analysis shows that: the capacity of the conventional CDMA systems without secure scrambling under disguised jamming is actually zero; however, the capacity can be significantly increased when the CDMA systems are protected using secure scrambling. Numerical examples were provided to demonstrate the effectiveness of secure scrambling in combating disguised jamming.

Chapter 5

Multiband Transmission Under Jamming: A Game Theoretic Perspective

In this chapter, we consider a game between a power-limited authorized user and a power-limited jammer, who operate independently over the same spectrum consisting of multiple bands. The strategic decision-making of the authorized user and the jammer is modeled as a two-party zero-sum game, where the payoff function is the capacity that can be achieved by the authorized user in presence of the jammer. *First*, we investigate the game under AWGN channels. We explore the possibility for the authorized user or the jammer to randomly utilize part (or all) of the available spectrum and/or apply nonuniform power allocation. It is found that: under AWGN channels, either for the authorized user to maximize its capacity, or for the jammer to minimize the capacity of the authorized user, the best strategy is to distribute the transmission power or jamming power uniformly over all the available spectrum. The minimax capacity can be calculated based on the channel bandwidth and the signal-to-jamming and noise ratio, and it matches with the Shannon channel capacity formula. *Second*, we consider frequency selective fading channels. We characterize the dynamic relationship between the optimal signal power allocation and the optimal jamming power allocation in

the minimax game, and propose an efficient two-step water pouring algorithm to find the optimal power allocation schemes for both the authorized user and the jammer.

5.1 Introduction

In traditional research on jamming strategy and jamming mitigation, there is generally an assumption that the jammer or the authorized user can access at least part of the information about the transmission pattern of its adversary. As such, the jammer can launch more effective jamming by exploiting the information it has about the authorized user, e.g., correlated jamming [14, 69, 70] or disguised jamming [15, 71]. For jamming mitigation, the authorized user can mitigate the jammer's effect by applying a particular anti-jamming scheme that is robust against a specific jamming pattern [11, 12]. The underlying assumption is that the jamming varies slowly such that the authorized user has sufficient time to track and react to the jamming. However, if the jammer is intelligent and can switch its patterns fast enough, then it would be impossible for the authorized user to detect and react in real time. In this case, the authorized user and the jammer are actually acting independently of each other. Regarding this scenario, there has been a surge in research that applies game theory to characterize and analyze the uncertainties in communication systems with cognitive jamming or interference.

A lot of work on game theory in communications has been focused on *the single user and single band case* [72–76]. The optimal jamming strategy under the Gaussian test channel was investigated in [72], and the worst additive noise for a communication channel under a covariance constraint was studied in [73]. The capacity of channels with block memory was investigated in [74], which showed that both the optimal coding strategy and the optimal

jamming strategy are independent from symbol to symbol within a block. The authors in [75] discussed the minimax game between an authorized user and a jammer for any combinations of "hard" or "soft" input and output quantization with additive noise and average power constraints. In [76], a dynamic game between a communicator and a jammer was considered, where the participants choose their power levels randomly from a finite space subject to temporal energy constraints.

Application of game theory to *multiuser and multiband/multicarrier communications* has been brought to attention in recent years [77–80]. In [77], the authors proposed a decentralized strategy to find out the optimal precoding/multiplexing matrices for a multipoint-to-multipoint communication system composed of a set of wideband links sharing the same physical resources. In [78], a scheme aiming for fair allocation of subcarriers, rates, and power for multiuser orthogonal frequency-division multiple-access (OFDMA) systems was proposed to maximize the overall system rate, subject to each user's maximal power and minimal rate constraints. In [79], jamming mitigation was carried out by maximizing the sum signal-to-interference and noise ratio (SINR) for multichannel communications. In [80], the authors considered a particular scenario where K users and a jammer share a common spectrum of N orthogonal tones, and examined how each user could maximize its own total sum rate selfishly.

Game theory has also been applied to *cognitive radios and ad hoc networks* [81–85]. New techniques for analyzing networks of cognitive radios that can alter either their power levels or their signature waveforms through the use of game models were introduced in [81]. In [82], a game theoretic overview of dynamic spectrum sharing was provided regarding analysis of network users' behaviors, efficient dynamic distributed design, and performance optimality. A game theoretic power control framework for spectrum sensing in cognitive radio networks

was proposed in [83], and the minimax game for cooperative spectrum sensing in centralized cognitive radio networks was investigated in [84]. In [85], the authors developed a game theoretic framework to construct convergent interference avoidance (IA) algorithms in ad hoc networks with multiple distributed receivers.

For spectrum and power utilization in multiband communications, an open while interesting question is: in presence of a random and intractable opponent, can the authorized user or the jammer benefit from utilizing part instead of the entire spectrum and/or applying nonuniform power allocation?

In this research, we try to address this question from a game theoretic perspective, taking jamming and jamming mitigation as a game between a power-limited jammer and a power-limited authorized user, who operate independently over the same spectrum consisting of multiple bands or subchannels. The authorized user is always trying to maximize its capacity under jamming by applying an optimal strategy. Accordingly, the jammer would like to find an optimal strategy that can minimize the capacity of the authorized user. To apply a chosen strategy, the authorized user or the jammer selects a particular number of subchannels and applies a particular power allocation scheme over the selected subchannels. For both the authorized user and the jammer, the subchannels may not be chosen with equal probability. The strategic decision-making of the authorized user and the jammer can be modeled as a two-party zero-sum game, where the payoff function is the capacity that can be achieved by the authorized user in presence of the jammer.

Solving the zero-sum game above is equivalent to locating the saddle point, which produces optimal strategies for both the authorized user and the jammer. That is, the jammer cannot reduce the capacity of the authorized user by applying a jamming strategy different from the optimal one; meanwhile, the authorized user cannot increase its capacity by switch-

ing to another transmission strategy either. We find that: under AWGN channels, either for the authorized user to maximize its capacity, or for the jammer to minimize the capacity of the authorized user, the best strategy is to distribute the signal power or jamming power uniformly over all the available spectrum. The minimax capacity of the authorized user is given by $C = B\log_2(1+\frac{P_s}{P_J+P_N})$, where B is the bandwidth of the overall spectrum, P_N the noise power, P_s and P_J the total power of the authorized user and the jammer, respectively. In other words, the minimax capacity above is the minimal capacity that can be achieved by the authorized user if it utilizes all the available spectrum and applies uniform power allocation, no matter what strategy is applied by the jammer; meanwhile, it is also the maximal capacity that can be achieved by the authorized user if the jammer jams all the available spectrum and applies uniform power allocation, no matter what strategy is applied by the authorized user.

As can be expected, the results we obtained under AWGN channels may no longer be true for frequency selective fading channels. In the jamming-free case, it is well known that the classical water pouring algorithm provides the optimal power allocation scheme that maximizes the capacity of the authorized user under frequency selective fading channels. Naturally, the situation becomes complicated when a jammer is involved in the game.

To identify the saddle point under frequency selective fading channels, we first characterize the dynamic relationship between the optimal signal power allocation and the optimal jamming power allocation in the minimax game. Then we show that under certain conditions, the closed-form solution for the saddle point can be obtained using a two-step water pouring algorithm. As a special case, it is shown that when the channel for the authorized user and the channel for the jammer are relatively flat with respect to each other, i.e., their magnitude spectrum is proportional to each other, the closed-form solution for the saddle

point can be obtained. From the arbitrarily varying channel (AVC) point of view, the correlation between the user channel and the jamming channel can be regarded as an indicator of possible symmetricity between the user and the jammer. It is also observed that as long as the cross-correlation between the user channel and the jammer channel is reasonably high, the two-step water pouring algorithm can still provide a much better solution than uniform power allocation. Simulation examples are provided to illustrate our findings for both the AWGN channels and the frequency selective fading channels.

This chapter is organized as follows. In Section 5.2, the problem is formulated after the system model description. The minimax problem in the zero-sum game with an authorized user and a jammer under AWGN channels is theoretically solved in Section 5.3. The gaming problem under frequency selective fading channels is investigated in Section 5.4. Numerical analysis is provided in Section 5.5 and we conclude in Section 5.6.

5.2 Problem Formulation

5.2.1 System Description

We consider a multiband communication system[1], where there is *an authorized user* and *a jammer* who are operating randomly and independently of each other. Assuming that both the authorized user and the jammer can choose to operate over all or part of the N_c frequency bands or subchannels (not necessarily being consecutive), each of which has a bandwidth $\frac{B}{N_c}$ Hz. We start with the AWGN channel model, where all the subchannels have equal noise power, and then extend to the frequency selective fading scenario. In the AWGN

[1]We assume multiband communications here, but the derivation is readily applicable to multicarrier communications (e.g., OFDM), if the authorized user and the jammer apply the same transceiver structure.

case, assuming the total noise power over the entire spectrum is P_N, then the noise power corresponding to each subchannel is $\frac{P_N}{N_c}$. We assume the jamming is Gaussian over each jammed subchannel, because Gaussian jamming is the worst jamming when the jammer has no knowledge of the authorized transmission [72]. In the following, let P_s denote the total signal power for the authorized user, and P_J the total jamming power.

The authorized user is always trying to maximize its capacity under jamming by applying an optimal strategy on subchannel selection (either all or part) and power allocation. On the other hand, the jammer tries to find an optimal strategy that can minimize the capacity of the authorized user. In this research, we consider the case where both the authorized user and the jammer use random strategies. It is assumed that both the authorized user and the jammer can adjust their subchannel selection and power allocation swiftly and randomly, such that neither of them has sufficient time to learn and react in real time before its opponent switches to new subchannels and/or power levels. In other words, when the authorized user and the jammer apply their own resource allocation strategy, they have no knowledge of the selected subchannels and power levels of their opponent.

5.2.2 Strategy Spaces for the Authorized User and the Jammer

Each random strategy applied by the authorized user is determined by the number of activated subchannels, the subchannel selection process and the power allocation process. More specifically: (1) The authorized user activates K_s ($1 \leq K_s \leq N_c$) out of N_c subchannels each time for information transmission. (2) The subchannel selection process is characterized using a binary indicator vector $\boldsymbol{\alpha} = [\alpha_1, \alpha_2, ..., \alpha_{N_c}]$, where each random variable $\alpha_m = 1$ or 0 indicates whether the mth subchannel is selected or not, and $\sum_{m=1}^{N_c} \alpha_m = K_s$. Let $\boldsymbol{\omega}_s = [\omega_{s,1}, \omega_{s,2}, ..., \omega_{s,N_c}]$ be the corresponding probability vector, where $\omega_{s,m}$ denotes the

probability that the mth subchannel is selected each time. That is, $\omega_{s,m} = Pr\{\alpha_m = 1\}$, and $\sum_{m=1}^{N_c} \omega_{s,m} = K_s$. (A simple strategy for selecting a particular number of subchannels based on a given subchannel selection probability vector, $\boldsymbol{\omega}_s$, is illustrated in Appendix E.) (3) For notation simplicity, the authorized user always specifies the indices of the selected K_s subchannels as $1, 2, ..., K_s$, following the order as they appear in the original spectrum, and performs power allocation over them. The power allocation process is characterized using a vector $\mathbf{P}_s = [P_{s,1}, P_{s,2}, ..., P_{s,K_s}]$, in which $P_{s,n}$ denotes the power allocated to the nth selected subchannel, and $\sum_{n=1}^{K_s} P_{s,n} = P_s$ is the power constraint. Let $\mathcal{W}_{s,K_s} = \{\boldsymbol{\omega}_s = [\omega_{s,1}, \omega_{s,2}, ..., \omega_{s,N_c}] \mid 0 \leq \omega_{s,m} \leq 1, \sum_{m=1}^{N_c} \omega_{s,m} = K_s\}$, and $\mathcal{P}_{s,K_s} = \{\mathbf{P}_s = [P_{s,1}, P_{s,2}, ..., P_{s,K_s}] \mid 0 < P_{s,n} \leq P_s, \sum_{n=1}^{K_s} P_{s,n} = P_s\}$. The strategy space for the authorized user can thus be defined as

$$\mathcal{X} = \{(K_s, \boldsymbol{\omega}_s, \mathbf{P}_s) \mid 1 \leq K_s \leq N_c, \boldsymbol{\omega}_s \in \mathcal{W}_{s,K_s}, \mathbf{P}_s \in \mathcal{P}_{s,K_s}\}. \tag{5.1}$$

The strategy space $\mathcal{X}$ covers all the possible subchannel utilization strategies as K_s varies from 1 to N_c. Here, a strategy $(K_s, \boldsymbol{\omega}_s, \mathbf{P}_s)$ with $K_s = 1$ and $\boldsymbol{\omega}_s = [\frac{1}{N_c}, \cdots, \frac{1}{N_c}]$ and $P_{s,1} = P_s$, corresponds to the conventional frequency hopping (FH) system, while a strategy $(K_s, \boldsymbol{\omega}_s, \mathbf{P}_s)$ with $K_s = N_c$, $\boldsymbol{\omega}_s = [1, \cdots, 1]$ and $P_{s,n} = \frac{P_s}{N_c}$, $\forall n$, would result in a full band transmission with uniform power allocation.

Similarly, the jammer jams K_J ($1 \leq K_J \leq N_c$) out of N_c subchannels each time following a binary indicator vector $\boldsymbol{\beta} = [\beta_1, \beta_2, ..., \beta_{N_c}]$ with $\sum_{m=1}^{N_c} \beta_m = K_J$. The subchannel selection process is characterized using a probability vector $\boldsymbol{\omega}_J = [\omega_{J,1}, \omega_{J,2}, ..., \omega_{J,N_c}]$, where $\omega_{J,m} = Pr\{\beta_m = 1\}$ and $\sum_{m=1}^{N_c} \omega_{J,m} = K_J$. Then the jammer specifies the indices of the K_J jammed subchannels as $1, 2, ..., K_J$ in the same manner as the authorized user, and per-

forms power allocation over them using a power-allocation vector $\mathbf{P}_J = [P_{J,1}, P_{J,2}, ..., P_{J,K_J}]$ constrained by $\sum_{n=1}^{K_J} P_{J,n} = P_J$. Let $\mathcal{W}_{J,K_J} = \{\boldsymbol{\omega}_J = [\omega_{J,1}, \omega_{J,2}, ..., \omega_{J,N_c}] \mid 0 \leq \omega_{J,m} \leq 1, \sum_{m=1}^{N_c} \omega_{J,m} = K_J\}$ and $\mathcal{P}_{J,K_J} = \{\mathbf{P}_J = [P_{J,1}, P_{J,2}, ..., P_{J,K_J}] \mid 0 < P_{J,n} \leq P_J, \sum_{n=1}^{K_J} P_{J,n} = P_J\}$, the strategy space for the jammer can thus be defined as

$$\mathcal{Y} = \{(K_J, \boldsymbol{\omega}_J, \mathbf{P}_J) \mid 1 \leq K_J \leq N_c, \boldsymbol{\omega}_J \in \mathcal{W}_{J,K_J}, \mathbf{P}_J \in \mathcal{P}_{J,K_J}\}. \tag{5.2}$$

5.2.3 The Minimax Problem in the Zero-Sum Game between the Authorized User and the Jammer

From a game theoretic perspective, the strategic decision-making of the authorized user and the jammer can be modeled as a two-party zero-sum game [86], which is characterized by a triplet $(\mathcal{X}, \mathcal{Y}, C)$, where

1. $\mathcal{X}$ is the strategy space of the authorized user;
2. $\mathcal{Y}$ is the strategy space of the jammer;
3. C is a real-valued payoff function defined on $\mathcal{X} \times \mathcal{Y}$.

The interpretation is as follows. Let (x, y) denote the strategy pair, in which $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ are the strategies applied by the authorized user and the jammer, respectively. Note that both x and y are random strategies. The payoff function $C(x, y)$ is therefore defined as the *ergodic* (i.e., expected or average) capacity of the authorized user choosing a strategy $x \in \mathcal{X}$ in presence of the jammer choosing a strategy $y \in \mathcal{Y}$. In other words, $C(x, y)$ is the amount that the authorized user wins and simultaneously the jammer loses in the game with a strategy pair (x, y).

Assuming that with strategy pair (x, y), the authorized user and the jammer activate K_s and K_J channels, respectively. Define $\mathcal{A}_{K_s} = \{\boldsymbol{\alpha} = [\alpha_1, \alpha_2, ..., \alpha_{N_c}] \mid \alpha_m \in \{0, 1\}, \sum_{m=1}^{N_c} \alpha_m = K_s\}$, and $\mathcal{B}_{K_J} = \{\boldsymbol{\beta} = [\beta_1, \beta_2, ..., \beta_{N_c}] \mid \beta_m \in \{0, 1\}, \sum_{m=1}^{N_c} \beta_m = K_J\}$. Let $p(\boldsymbol{\alpha}|x)$ denote the probability that the subchannels selected by the authorized user follow the indicator vector $\boldsymbol{\alpha}$ given that the strategy $x \in \mathcal{X}$ is applied, and $p(\boldsymbol{\beta}|y)$ the probability that the subchannels selected by the jammer follow the indicator vector $\boldsymbol{\beta}$ given that the strategy $y \in \mathcal{Y}$ is applied. Let $T_{s,m}$ and $T_{J,m}$ be the power allocated to the mth subchannel by the authorized user and the jammer, respectively, which are determined by

$$T_{s,m} = \begin{cases} P_{s,g_m}, & \alpha_m = 1, \\ 0, & \alpha_m = 0, \end{cases} \qquad T_{J,m} = \begin{cases} P_{J,q_m}, & \beta_m = 1, \\ 0, & \beta_m = 0, \end{cases} \tag{5.3}$$

where $g_m = \sum_{i=1}^{m} \alpha_i$ is the new index of subchannel m specified by the authorized user in the K_s selected subchannels if it is activated by the authorized user ($\alpha_m = 1$), and $q_m = \sum_{i=1}^{m} \beta_i$ is the new index of subchannel m specified by the jammer in the K_J jammed subchannels if it is activated by the jammer ($\beta_m = 1$). Note that: (i) the subchannel selection processes used by the authorized user and the jammer are independent of each other; and (ii) for each strategy pair (x, y), the subchannel selection choices ($\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$) are not unique for both the authorized user and the jammer. Thus, the ergodic capacity of the authorized user in the game with a strategy pair (x, y) can be calculated as

$$C(x, y) = \sum_{\boldsymbol{\alpha} \in \mathcal{A}_{K_s}} \sum_{\boldsymbol{\beta} \in \mathcal{B}_{K_J}} p(\boldsymbol{\alpha}|x) p(\boldsymbol{\beta}|y) \sum_{m=1}^{N_c} \frac{B}{N_c} \log_2 \left(1 + \frac{T_{s,m}}{T_{J,m} + P_N/N_c} \right). \tag{5.4}$$

Based on the definitions above, the minimax capacity of the authorized user is defined as [16, 27, 68]

$$C(x^*, y^*) = \max_{x \in \mathcal{X}} \min_{y \in \mathcal{Y}} C(x, y) = \min_{y \in \mathcal{Y}} \max_{x \in \mathcal{X}} C(x, y). \tag{5.5}$$

It can be seen from (5.5) that the authorized user tries to choose an optimal transmission strategy $x^* \in \mathcal{X}$ to maximize its capacity, while the jammer tries to minimize it by choosing an optimal jamming strategy $y^* \in \mathcal{Y}$. The capacity $C(x^*, y^*)$ in (5.5) can be achieved when a saddle point strategy pair (x^*, y^*) is chosen, which is characterized by [69, 75]

$$C(x, y^*) \leq C(x^*, y^*) \leq C(x^*, y), \quad \forall x \in \mathcal{X}, y \in \mathcal{Y}. \tag{5.6}$$

This implies that: with strategy x^*, the minimal capacity that can be achieved by the authorized user is $C(x^*, y^*)$, no matter which strategy is applied by the jammer; on the other hand, if the jammer applies strategy y^*, the maximal capacity that can be achieved by the authorized user is also $C(x^*, y^*)$, no matter which strategy is applied by the authorized user. As a result, to find the optimal transmission strategy and the worst jamming strategy under the power constraints P_s and P_J, we need to find the saddle point strategy pair (x^*, y^*).

5.3 Optimal Strategy for Multiband Communications under Jamming over AWGN Channels

Recall that K_s denotes the number of subchannels activated by the authorized user, and K_J the number of subchannels interfered by the jammer. In this section, we derive the

saddle point strategy pair (x^*, y^*) in two steps: (1) For any fixed K_s and K_J with $1 \leq K_s, K_J \leq N_c$, calculate the corresponding minimax capacity and denote it by $\widetilde{C}(K_s, K_J)$. Let $K_s = 1, 2, ..., N_c$ and $K_J = 1, 2, ..., N_c$, we can obtain an $N_c \times N_c$ payoff matrix $\widetilde{\mathbf{C}}$. (2) For the derived payoff matrix $\widetilde{\mathbf{C}}$, locate its saddle point, and then the minimax capacity of the authorized user in (5.5) can be calculated accordingly.

5.3.1 The Minimax Problem for Fixed K_s and K_J

With fixed K_s and K_J, the strategy space for the authorized user becomes $\widetilde{\mathcal{X}}_{K_s} = \{(K_s, \boldsymbol{\omega}_s, \mathbf{P}_s) \mid K_s \text{ Fixed}, \boldsymbol{\omega}_s \in \mathcal{W}_{s,K_s}, \mathbf{P}_s \in \mathcal{P}_{s,K_s}\} \subset \mathcal{X}$, and similarly the strategy space for the jammer becomes $\widetilde{\mathcal{Y}}_{K_J} = \{(K_J, \boldsymbol{\omega}_J, \mathbf{P}_J) \mid K_J \text{ Fixed}, \boldsymbol{\omega}_J \in \mathcal{W}_{J,K_J}, \mathbf{P}_J \in \mathcal{P}_{J,K_J}\} \subset \mathcal{Y}$. It should be noted that the user-activated subchannels and the jammed subchannels may vary from time to time, although the total number of the user-activated or jammed subchannels is fixed.

We first present two lemmas on the concavity/convexity property of two real-valued functions that will be used afterwards. More information on concavity and convexity can be found in [87].

Lemma 5.1 *For any $v \geq 0$ and $a > 0$, the real-valued function, $f(v) = \log_2(1 + \frac{v}{a})$, is concave.*

Proof: The second-order derivative, $f''(v) = -\frac{1}{\ln 2}\frac{1}{(v+a)^2} < 0$, for any $v \geq 0$ and $a > 0$. □

Lemma 5.2 *For any $v \geq 0$, $a > 0$ and $b > 0$, the real-valued function, $f(v) = \log_2(1 + \frac{a}{v+b})$, is convex.*

Proof: The second-order derivative, $f''(v) = \frac{a}{\ln 2}\frac{(2v+a+2b)}{(v+a)^2(v+a+b)^2} > 0$, for any $v \geq 0$, $a > 0$ and $b > 0$. □

The solution to the minimax problem for fixed K_s and K_J is given in Proposition 5.1.

Proposition 5.1 *Let K_s be the number of subchannels activated by the authorized user, and K_J the number of subchannels interfered by the jammer. For any fixed (K_s, K_J) pair, the saddle point of $C(x, y)$ under the power constraints P_s and P_J for $x \in \widetilde{\mathcal{X}}_{K_s}$ and $y \in \widetilde{\mathcal{Y}}_{K_J}$ is reached when both authorized user and the jammer choose to apply uniform subchannel selection and uniform power allocation strategy. That is, for fixed K_s and K_J, the saddle point strategy pair $(\widetilde{x}^*, \widetilde{y}^*)$ that satisfies*

$$C(\widetilde{x}, \widetilde{y}^*) \leq C(\widetilde{x}^*, \widetilde{y}^*) \leq C(\widetilde{x}^*, \widetilde{y}), \quad \forall \widetilde{x} \in \widetilde{\mathcal{X}}_{K_s}, \widetilde{y} \in \widetilde{\mathcal{Y}}_{K_J}, \tag{5.7}$$

is given by $\widetilde{x}^* = (K_s, \boldsymbol{\omega}_s^*, \boldsymbol{P}_s^*)$ with

$$\begin{cases} \omega_{s,m}^* = K_s/N_c, & m = 1, 2, ..., N_c, \\ P_{s,n}^* = P_s/K_s, & n = 1, 2, ..., K_s, \end{cases} \tag{5.8}$$

and $\widetilde{y}^* = (K_J, \boldsymbol{\omega}_J^*, \boldsymbol{P}_J^*)$ with

$$\begin{cases} \omega_{J,m}^* = K_J/N_c, & m = 1, 2, ..., N_c, \\ P_{J,n}^* = P_J/K_J, & n = 1, 2, ..., K_J. \end{cases} \tag{5.9}$$

In this case, the minimax capacity of the authorized user is given by

$$\begin{aligned}\widetilde{C}(K_s, K_J) =& K_s \frac{K_J}{N_c} \frac{B}{N_c} \log_2 \left(1 + \frac{P_s/K_s}{P_J/K_J + P_N/N_c}\right) \\ &+ K_s \left(1 - \frac{K_J}{N_c}\right) \frac{B}{N_c} \log_2 \left(1 + \frac{P_s/K_s}{P_N/N_c}\right).\end{aligned} \tag{5.10}$$

Proof: (1) We first prove that the $(\widetilde{x}^*, \widetilde{y}^*)$ pair defined in (5.8) and (5.9) satisfies the left part of (5.7), $C(\widetilde{x}, \widetilde{y}^*) \leq C(\widetilde{x}^*, \widetilde{y}^*)$. Assume the jammer applies the strategy $\widetilde{y}^*$, which means uniform subchannel selection and uniform power allocation as indicated in (5.9). For the authorized user who applies an arbitrary strategy $\widetilde{x} \in \widetilde{\mathcal{X}}_{K_s}$, we specified the indices of the activated K_s subchannels as $n = 1, 2, ..., K_s$. With any subchannel selection probability vector $\boldsymbol{\omega}_s \in \mathcal{W}_{s,K_s}$, for each subchannel activated by the authorized user, the probability that it is jammed is always $\frac{K_J}{N_c}$, since the jammer jams each subchannel with a uniform probability $\omega^*_{J,m} = \frac{K_J}{N_c}$, for any $m = 1, 2, ..., N_c$. Accordingly, the probability that each subchannel is not jammed is $1 - \frac{K_J}{N_c}$.

Considering all the subchannels activated by the authorized user, when the authorized user applies an arbitrary strategy $\widetilde{x} \in \widetilde{\mathcal{X}}_{K_s}$, and the jammer applies strategy $\widetilde{y}^*$, the ergodic capacity can be calculated as the weighted average of the capacity under jamming and the capacity in the jamming-free case,

$$\begin{aligned}C(\widetilde{x}, \widetilde{y}^*) =& \sum_{n=1}^{K_s} \left[\frac{K_J}{N_c} \frac{B}{N_c} \log_2 \left(1 + \frac{P_{s,n}}{P_J/K_J + P_N/N_c}\right)\right. \\ &\left. + \left(1 - \frac{K_J}{N_c}\right) \frac{B}{N_c} \log_2 \left(1 + \frac{P_{s,n}}{P_N/N_c}\right)\right] \\ =& \frac{K_J}{N_c} \frac{B}{N_c} \sum_{n=1}^{K_s} \log_2 \left(1 + \frac{P_{s,n}}{P_J/K_J + P_N/N_c}\right) \\ &+ \left(1 - \frac{K_J}{N_c}\right) \frac{B}{N_c} \sum_{n=1}^{K_s} \log_2 \left(1 + \frac{P_{s,n}}{P_N/N_c}\right).\end{aligned} \tag{5.11}$$

Note that $\sum_{n=1}^{K_S} P_{s,n} = P_s$, and applying the concavity property proved in Lemma 5.1, we have

$$\begin{aligned} C(\widetilde{x},\widetilde{y}^*) \leq & K_s \frac{K_J}{N_c}\frac{B}{N_c}\log_2\left(1+\frac{P_s/K_s}{P_J/K_J+P_N/N_c}\right) \\ & + K_s\left(1-\frac{K_J}{N_c}\right)\frac{B}{N_c}\log_2\left(1+\frac{P_s/K_s}{P_N/N_c}\right) \\ = & C(\widetilde{x}^*,\widetilde{y}^*), \end{aligned} \tag{5.12}$$

where the equality holds if and only if $P_{s,n} = \frac{P_s}{K_s}, \forall n$.

(2) Proof of the right part of (5.7), $C(\widetilde{x}^*,\widetilde{y}^*) \leq C(\widetilde{x}^*,\widetilde{y})$. In this part of the proof, we will show that applying uniform subchannel selection and uniform power allocation strategy $\widetilde{x}^*$ at the authorized user side guarantees a lower bound on its capacity, no matter what strategy is applied by the jammer. Assume the authorized user applies the strategy $\widetilde{x}^*$ as indicated in (5.8). For the jammer who applies an arbitrary strategy $\widetilde{y} \in \widetilde{\mathcal{Y}}_{K_J}$, we specified the indices of the jammed K_J subchannels as $n = 1, 2, ..., K_J$. With any subchannel selection probability vector $\boldsymbol{\omega}_J \in \mathcal{W}_{J,K_J}$, for each jammed or jamming-free subchannel, the probability that it serves as a subchannel activated by the authorized user is always $\frac{K_S}{N_c}$. Hence, the average number[2] of jammed subchannels which are also activated by the authorized user is $\frac{K_J K_S}{N_c}$, and the average number of jamming-free subchannels which are activated by the authorized user would be $(N_c - K_J)\frac{K_S}{N_c} = K_s(1-\frac{K_J}{N_c})$.

Considering both the jammed and jamming-free subchannels, when the jammer applies an arbitrary strategy $\widetilde{y} \in \widetilde{\mathcal{Y}}_{K_J}$, and the authorized user applies strategy $\widetilde{x}^*$, the ergodic

[2]The ensemble average might not be an integer. Nevertheless, the capacity calculation would still be accurate from a statistical perspective.

capacity can be calculated as

$$\begin{aligned} C(\widetilde{x}^*, \widetilde{y}) = & \sum_{n=1}^{K_J} \frac{K_s}{N_c} \frac{B}{N_c} \log_2 \left(1 + \frac{P_s/K_s}{P_{J,n} + P_N/N_c} \right) \\ & + K_s \left(1 - \frac{K_J}{N_c} \right) \frac{B}{N_c} \log_2 \left(1 + \frac{P_s/K_s}{P_N/N_c} \right). \end{aligned} \tag{5.13}$$

Note that $\sum_{n=1}^{K_J} P_{J,n} = P_J$, and applying the convexity property proved in Lemma 5.2, we have

$$\begin{aligned} C(\widetilde{x}^*, \widetilde{y}) \geq & K_s \frac{K_J}{N_c} \frac{B}{N_c} \log_2 \left(1 + \frac{P_s/K_s}{P_J/K_J + P_N/N_c} \right) \\ & + K_s \left(1 - \frac{K_J}{N_c} \right) \frac{B}{N_c} \log_2 \left(1 + \frac{P_s/K_s}{P_N/N_c} \right) \\ = & C(\widetilde{x}^*, \widetilde{y}^*), \end{aligned} \tag{5.14}$$

where the equality holds if and only if $P_{J,n} = \frac{P_J}{K_J}, \forall n$. □

5.3.2 Capacity Optimization over K_s and K_J

In Section 5.3.1, we derived the closed-form minimax capacity of the authorized user for fixed K_s and K_J. Considering all possible K_s and K_J, we would have an $N_c \times N_c$ matrix $\widetilde{\mathbf{C}}$, in which $\widetilde{C}(K_s, K_J)$ is the minimax capacity of the authorized user for fixed K_s and K_J, as indicated in (5.10). Now finding the minimax capacity in (5.5) can be reduced to finding the saddle point of the matrix $\widetilde{\mathbf{C}}$, that is, the entry $\widetilde{C}(i, j)$, which is simultaneously the minimum of the ith row and the maximum of the jth column.

To locate the saddle point of matrix $\widetilde{\mathbf{C}}$, we need Lemma 5.3.

Lemma 5.3 *For the capacity function*

$$\begin{aligned}\widetilde{C}(K_s, K_J) =& K_s \frac{K_J}{N_c} \frac{B}{N_c} \log_2 \left(1 + \frac{P_s/K_s}{P_J/K_J + P_N/N_c}\right) \\ &+ K_s \left(1 - \frac{K_J}{N_c}\right) \frac{B}{N_c} \log_2 \left(1 + \frac{P_s/K_s}{P_N/N_c}\right),\end{aligned} \tag{5.15}$$

we have

$$\frac{\partial \widetilde{C}}{\partial K_s} > 0, \text{ for any } K_s = 1, 2, ..., N_c, \tag{5.16}$$

and

$$\frac{\partial \widetilde{C}}{\partial K_J} < 0, \text{ for any } K_J = 1, 2, ..., N_c. \tag{5.17}$$

Proof: See Appendix F. □

Following Lemma 5.3, we have Proposition 5.2.

Proposition 5.2 *The saddle point of matrix* $\widetilde{\boldsymbol{C}}$ *is indexed by* $(K_s^*, K_J^*) = (N_c, N_c)$. *Equivalently, for all* $1 \leq K_s, K_J \leq N_c$, *we have*

$$\widetilde{C}(K_s, N_c) \leq \widetilde{C}(N_c, N_c) \leq \widetilde{C}(N_c, K_J). \tag{5.18}$$

Combining *Propositions* 1 and 2, we can obtain the saddle point to the original minimax problem in (5.5) over strategy spaces $\mathcal{X}$ and $\mathcal{Y}$. The result is summarized in Theorem 5.1.

Theorem 5.1 *Assume that an authorized user and a jammer are operating independently over the same AWGN channel consisting of* N_c *subchannels. Either for the authorized user to maximize its capacity, or for the jammer to minimize the capacity of the authorized user, the best strategy is to distribute the signal power or jamming power uniformly over all the*

N_c subchannels. In this case, the minimax capacity of the authorized user is given by

$$C = B \log_2 \left(1 + \frac{P_s}{P_J + P_N} \right), \tag{5.19}$$

where B is the bandwidth of the overall spectrum, P_N the noise power, P_s and P_J the total power for the authorized user and the jammer, respectively.

Proof: The proof follows directly from Propositions 5.1 and 5.2. The minimax capacity in (5.19) can be derived simply by substituting $K_s = K_J = N_c$ into (5.10). □

5.4 Optimal Strategy for Multiband Communications under Jamming over Frequency Selective Fading Channels

In this section, we investigate the optimal strategies for both the authorized user and the jammer in multiband communications under frequency selective fading channels.

Recall that the power allocation for the authorized user is characterized using the vector $\mathbf{P}_s = [P_{s,1}, P_{s,2}, ..., P_{s,N_c}]$, where $P_{s,i}$ denotes the power allocated to the ith subchannel, and $\sum_{i=1}^{N_c} P_{s,i} = P_s$ is the signal power constraint. Similarly, the power allocation vector for the jammer is $\mathbf{P}_J = [P_{J,1}, P_{J,2}, ..., P_{J,N_c}]$, and $\sum_{i=1}^{N_c} P_{J,i} = P_J$ is the jamming power constraint. As in the OFDM systems, here we assume that all the subchannels are narrowband and have flat magnitude spectrum. Let $\mathbf{H}_s = [H_{s,1}, H_{s,2}, ..., H_{s,N_c}]$ be the frequency domain channel response vector for the authorized user, and $\mathbf{H}_J = [H_{J,1}, H_{J,2}, ..., H_{J,N_c}]$ the frequency

domain channel response vector for the jammer, respectively. Under the settings specified above, the capacity of the authorized user can be calculated as

$$\begin{aligned} C(\mathbf{P}_s, \mathbf{P}_J) &= \sum_{i=1}^{N_c} \frac{B}{N_c} \log_2 \left(1 + \frac{|H_{s,i}|^2 P_{s,i}}{|H_{J,i}|^2 P_{J,i} + \sigma_n^2} \right) \\ &= \sum_{i=1}^{N_c} \frac{B}{N_c} \log_2 \left(1 + \frac{P_{s,i}}{\frac{|H_{J,i}|^2}{|H_{s,i}|^2} P_{J,i} + \sigma_{n,i}^2} \right), \end{aligned} \tag{5.20}$$

where $\sigma_n^2 = \frac{P_N}{N_c}$ is the original noise power for each subchannel, and $\sigma_{n,i}^2 = \frac{\sigma_n^2}{|H_{s,i}|^2}$.

Define $\mathcal{P}_s = \{\mathbf{P}_s = [P_{s,1}, P_{s,2}, ..., P_{s,N_c}] \mid 0 \leq P_{s,i} \leq P_s, \sum_{i=1}^{N_c} P_{s,i} = P_s\}$, and $\mathcal{P}_J = \{\mathbf{P}_J = [P_{J,1}, P_{J,2}, ..., P_{J,N_c}] \mid 0 \leq P_{J,i} \leq P_J, \sum_{i=1}^{N_c} P_{J,i} = P_J\}$. The minimax capacity of the authorized user is defined as

$$C(\mathbf{P}_s^*, \mathbf{P}_J^*) = \max_{\mathbf{P}_s^* \in \mathcal{P}_s} \min_{\mathbf{P}_J^* \in \mathcal{P}_J} C(\mathbf{P}_s, \mathbf{P}_J) = \min_{\mathbf{P}_J^* \in \mathcal{P}_J} \max_{\mathbf{P}_s^* \in \mathcal{P}_s} C(\mathbf{P}_s, \mathbf{P}_J). \tag{5.21}$$

As before, the authorized user tries to apply optimal signal power allocation $\mathbf{P}_s^* \in \mathcal{P}_s$ to maximize its capacity, while the jammer tries to minimize it by applying optimal jamming power allocation $\mathbf{P}_J^* \in \mathcal{P}_J$.

Theorem 5.2 *Assume that there are N_c available subchannels. Let $\boldsymbol{H}_s = [H_{s,1}, H_{s,2}, ..., H_{s,N_c}]$ and $\boldsymbol{H}_J = [H_{J,1}, H_{J,2}, ..., H_{J,N_c}]$ denote the frequency domain channel response vector for the authorized user and the jammer, respectively. Assuming zero-mean white Gaussian noise of variance σ_n^2 over the entire band, let $\boldsymbol{\sigma}_n^2 = [\sigma_{n,1}^2, \sigma_{n,2}^2, ..., \sigma_{n,N_c}^2]$, where $\sigma_{n,i}^2 = \frac{\sigma_n^2}{|H_{s,i}|^2}$. The optimal power-allocation pair for the authorized user and the jammer under the signal power constraint $\sum_{i=1}^{N_c} P_{s,i}^* = P_s$ and the jamming power constraint*

$\sum_{i=1}^{N_c} P_{J,i}^* = P_J$, $(\boldsymbol{P}_s^*, \boldsymbol{P}_J^*)$, *which satisfies*

$$C(\boldsymbol{P}_s, \boldsymbol{P}_J^*) \leq C(\boldsymbol{P}_s^*, \boldsymbol{P}_J^*) \leq C(\boldsymbol{P}_s^*, \boldsymbol{P}_J), \ \ \forall \boldsymbol{P}_s \in \mathcal{P}_s, \boldsymbol{P}_J \in \mathcal{P}_J, \tag{5.22}$$

can be characterized by

$$\begin{cases} P_{J,i}^* = sgn(P_{s,i}^*) \left(c_1 - \dfrac{|H_{s,i}|^2}{|H_{J,i}|^2} \sigma_{n,i}^2 \right)^+, \ \forall i, & \text{(5.23a)} \\ P_{s,i}^* = \left(c_2 - \dfrac{|H_{J,i}|^2}{|H_{s,i}|^2} P_{J,i}^* - \sigma_{n,i}^2 \right)^+, \quad \forall i, & \text{(5.23b)} \end{cases}$$

where $(x)^+ = \max\{0, x\}$, *sgn*$(\cdot)$ *is the sign function, and* c_1, c_2 *are constants determined by the power constraints.*

Proof: (1) We first prove that the $(\mathbf{P}_s^*, \mathbf{P}_J^*)$ pair defined in (5.23) satisfies the left part of (5.22), $C(\mathbf{P}_s, \mathbf{P}_J^*) \leq C(\mathbf{P}_s^*, \mathbf{P}_J^*), \ \forall \mathbf{P}_s \in \mathcal{P}_s$. With the jammer applying power allocation $\mathbf{P}_J^*$, the equivalent jamming power for the ith subchannel after fading and equalization would be $\dfrac{|H_{J,i}|^2}{|H_{s,i}|^2} P_{J,i}^*$, as shown in (5.20). Since jamming is assumed to be a Gaussian random process which is independent of the signal and the noise, the overall interference and noise power level for the ith subchannel at the receiver would be $\dfrac{|H_{J,i}|^2}{|H_{s,i}|^2} P_{J,i}^* + \sigma_{n,i}^2$. As a result, the problem now turns to be the capacity maximization problem for multiband communications with nonuniform noise power levels. To this end, it is well known that the classical water pouring algorithm produces the best solution [88]. In this particular case, the water pouring solution for optimal signal power allocation would be

$$P_{s,i}^* = \left(c_2 - \frac{|H_{J,i}|^2}{|H_{s,i}|^2} P_{J,i}^* - \sigma_{n,i}^2 \right)^+, \ \ i = 1, 2, ..., N_c, \tag{5.24}$$

which maximizes the capacity of the authorized user, $C(\mathbf{P}_s^*, \mathbf{P}_J^*)$, while the jammer applying power allocation $\mathbf{P}_J^*$. Note that c_2 is a constant that should be chosen such that the power constraint for the authorized user is satisfied, i.e., $\sum_{i=1}^{N_c} P_{s,i}^* = P_s$.

(2) Proof of the right part, $C(\mathbf{P}_s^*, \mathbf{P}_J^*) \leq C(\mathbf{P}_s^*, \mathbf{P}_J), \ \forall \mathbf{P}_J \in \mathcal{P}_J$. To this end, we need to find the optimal jamming power allocation $\mathbf{P}_J^*$, which can minimize the capacity of the authorized user applying power allocation $\mathbf{P}_s^*$. Let $\gamma_i = \frac{|H_{J,i}|^2}{|H_{s,i}|^2}, \ \forall i$. With the authorized user applying power allocation $\mathbf{P}_s^*$, following (5.20), the optimization problem for jamming power allocation can be formulated as

$$\min_{\mathbf{P}_J \in \mathcal{P}_J} \sum_{i=1}^{N_c} \frac{B}{N_c} \log_2 \left(1 + \frac{P_{s,i}^*}{\gamma_i P_{J,i} + \sigma_{n,i}^2} \right); \tag{5.25a}$$

$$s.t. \ \sum_{i=1}^{N_c} P_{J,i} = P_J, \tag{5.25b}$$

$$P_{J,i} \geq 0, \ \forall i. \tag{5.25c}$$

Note that in this optimization problem, we have both equality and inequality constraints. Hence, we need to take the Karush-Kuhn-Tucker (KKT) approach [87], which generalizes the conventional method of Lagrange multipliers by allowing inequality constraints. As observed in (5.24), for $P_{s,i}^* > 0$, $P_{s,i}^* = c_2 - \frac{|H_{J,i}|^2}{|H_{s,i}|^2} P_{J,i}^* - \sigma_{n,i}^2$. In addition, the capacity of any subchannel with zero signal power (i.e., $P_{s,i}^* = 0$) is zero. Define

$$\begin{aligned} J(\mathbf{P}_J, \mathbf{u}, v) =& \sum_{i=1}^{N_c} \frac{B}{N_c} \log_2 \left(1 + \frac{P_{s,i}^*}{\gamma_i P_{J,i} + \sigma_{n,i}^2} \right) - u_i P_{J,i} + v \left(\sum_{i=1}^{N_c} P_{J,i} - P_J \right) \\ =& \sum_{i \in \{i | P_{s,i}^* > 0\}} \frac{B}{N_c} \log_2 \frac{c_2}{\gamma_i P_{J,i} + \sigma_{n,i}^2} - u_i P_{J,i} + v \left(\sum_{i=1}^{N_c} P_{J,i} - P_J \right), \end{aligned} \tag{5.26}$$

where $\mathbf{u} = [u_1, u_2, ..., u_{N_c}]$ and v are Lagrange multipliers that should satisfy the KKT conditions as below:

$$\frac{\partial J}{\partial P_{J,i}} = 0, \;\; u_i P_{J,i} = 0, \;\; u_i \geq 0, \;\; \forall i. \tag{5.27}$$

The first-order partial differentiation with respect to each $P_{J,i}$ can be calculated as

$$\frac{\partial J}{\partial P_{J,i}} = \begin{cases} -\frac{B}{N_c}\frac{1}{\ln 2}\frac{\gamma_i}{\gamma_i P_{J,i}+\sigma_{n,i}^2} - u_i + v, & P_{s,i}^* > 0, \\ -u_i + v, & P_{s,i}^* = 0. \end{cases} \tag{5.28}$$

For each subchannel with nonzero signal power (i.e., $P_{s,i}^* > 0$), applying the KKT conditions and eliminating u_i, we have

$$\begin{cases} v - \frac{B}{N_c}\frac{1}{\ln 2}\frac{\gamma_i}{\gamma_i P_{J,i}+\sigma_{n,i}^2} \geq 0, \\ P_{J,i}\left[v - \frac{B}{N_c}\frac{1}{\ln 2}\frac{\gamma_i}{\gamma_i P_{J,i}+\sigma_{n,i}^2}\right] = 0. \end{cases} \tag{5.29}$$

Solving (5.29), the optimal jamming power for the ith subchannel (with nonzero signal power) can be obtained as

$$P_{J,i}^* = \left(\frac{B}{N_c}\frac{1}{\ln 2}\frac{1}{v} - \frac{1}{\gamma_i}\sigma_{n,i}^2\right)^+. \tag{5.30}$$

Similarly, for each subchannel with zero signal power (i.e., $P_{s,i}^* = 0$), applying the KKT conditions and eliminating u_i, we have $vP_{J,i} = 0$. It is observed from (5.29) that $v > 0$, so the optimal jamming power for the ith subchannel (with zero signal power) is $P_{J,i}^* = 0$. Let

$c_1 = \frac{B}{N_c}\frac{1}{\ln 2}\frac{1}{v}$, and replace γ_i with $\frac{|H_{J,i}|^2}{|H_{s,i}|^2}$, we can summarize the result as

$$P_{J,i}^* = \begin{cases} \left(c_1 - \frac{|H_{s,i}|^2}{|H_{J,i}|^2}\sigma_{n,i}^2\right)^+, & P_{s,i}^* > 0, \\ 0, & P_{s,i}^* = 0, \end{cases} \tag{5.31}$$

where c_1 should be chosen such that the power constraint for the jammer is satisfied, i.e., $\sum_{i=1}^{N_c} P_{J,i}^* = P_J$. This is exactly the optimal jamming power allocation as expressed in (5.23a), which minimizes the capacity of the authorized user, $C(\mathbf{P}_s^*, \mathbf{P}_J^*)$, given that the authorized user applies power allocation $\mathbf{P}_s^*$. □

Theorem 5.2 characterizes the dynamic relationship between the optimal signal power allocation $\mathbf{P}_s^*$ and the optimal jamming power allocation $\mathbf{P}_J^*$. As shown in (5.23), due to the mutual dependency between $\mathbf{P}_s^*$ and $\mathbf{P}_J^*$, it is generally difficult to find an exact solution for them. However, in the following, we will show that under certain conditions, the saddle point, $(\mathbf{P}_s^*, \mathbf{P}_J^*)$, can be calculated explicitly using a two-step water pouring algorithm.

Theorem 5.3 *With the same conditions as in Theorem 5.2, the saddle point, which indicates the optimal signal power allocation and the optimal jamming power allocation, is given by*

$$\begin{cases} P_{J,i}^* = \left(c_1 - \frac{|H_{s,i}|^2}{|H_{J,i}|^2}\sigma_{n,i}^2\right)^+, & \forall i, \quad (5.32a) \\ P_{s,i}^* = \left(c_2 - \frac{|H_{J,i}|^2}{|H_{s,i}|^2}P_{J,i}^* - \sigma_{n,i}^2\right)^+, & \forall i, \quad (5.32b) \end{cases}$$

as long as

$$|H_{J,i}|^2 \le \frac{\sigma_n^2}{c_1} \;\; or \;\; \frac{|H_{J,i}|^2}{|H_{s,i}|^2} < \frac{c_2}{c_1}, \;\; \forall i, \tag{5.33}$$

where $(x)^+ = \max\{0, x\}$*, and* c_1*,* c_2 *are constants that should be chosen such that the power constraints are satisfied, i.e.,* $\sum_{i=1}^{N_c} P_{s,i}^* = P_s$ *and* $\sum_{i=1}^{N_c} P_{J,i}^* = P_J$*.*

Proof: The basic idea here is that given zero signal power for a particular subchannel, it is apparently not necessary to allocate positive jamming power in that subchannel; at the same time, over all the subchannels with nonzero signal power, the optimal jamming power allocation can be formed using the water pouring algorithm. We start by applying the water pouring algorithm over all subchannels,

$$P_{J,i}^* = \left(c_1 - \frac{|H_{s,i}|^2}{|H_{J,i}|^2} \sigma_{n,i}^2 \right)^+, \quad i = 1, 2, ..., N_c. \tag{5.34}$$

For the optimality of (5.34), we further need to ensure that $P_{J,i}^* = 0$, whenever $P_{s,i}^* = 0$.

As can be seen, a violation occurs ($P_{J,i}^* > 0$ and $P_{s,i}^* = 0$), if and only if for some subchannel indexed by i,

$$\begin{cases} P_{J,i}^* = c_1 - \dfrac{|H_{s,i}|^2}{|H_{J,i}|^2} \sigma_{n,i}^2 > 0, \\ c_2 - \dfrac{|H_{J,i}|^2}{|H_{s,i}|^2} P_{J,i}^* - \sigma_{n,i}^2 \leq 0, \end{cases} \tag{5.35}$$

which yields

$$|H_{J,i}|^2 > \frac{\sigma_n^2}{c_1} \text{ and } \frac{|H_{J,i}|^2}{|H_{s,i}|^2} \geq \frac{c_2}{c_1}. \tag{5.36}$$

Note that $\sigma_{n,i}^2 = \frac{\sigma_n^2}{|H_{s,i}|^2}$. Hence, the conditions characterized in (5.33) ensure that no violation occurs, and therefore the saddle point calculated by (5.32) is valid for both capacity maximization by the authorized user and capacity minimization by the jammer. □

In the following, we consider a special case where the channels corresponding to the

authorized user and the jammer are *relatively flat* with respect to each other, that is, their magnitude spectrum is proportional to each other, i.e., $\frac{|H_{J,i}|^2}{|H_{s,i}|^2} = \gamma,\ \forall i$. As will be shown in Corollary 5.1, when the user channel and the jammer channel are relatively flat with respect to each other, the conditions in (5.33) are always satisfied, and the saddle point calculation can be simplified accordingly.

Corollary 5.1 *With the same conditions as in Theorem 5.2, if the magnitude spectrum of the channels for the authorized user and the jammer is proportional to each other, i.e.,* $\frac{|H_{J,i}|^2}{|H_{s,i}|^2} = \gamma,\ \forall i$, *the saddle point, which indicates the optimal signal power allocation and the optimal jamming power allocation, can be calculated as*

$$\begin{cases} P^*_{J,i} = \left(c_1 - \frac{1}{\gamma}\sigma^2_{n,i}\right)^+, & \forall i, \\ P^*_{s,i} = \left(c_2 - \gamma P^*_{J,i} - \sigma^2_{n,i}\right)^+, & \forall i, \end{cases} \tag{5.37}$$

where $(x)^+ = \max\{0, x\}$, *and* c_1, c_2 *are constants that should be chosen such that the power constraints are satisfied, i.e.,* $\sum_{i=1}^{N_c} P^*_{s,i} = P_s$ *and* $\sum_{i=1}^{N_c} P^*_{J,i} = P_J$.

Proof: Note that with $\frac{|H_{J,i}|^2}{|H_{s,i}|^2} = \gamma,\ \forall i$, (5.32) reduces to (5.37). Following Theorem 5.3, we only need to show that the conditions specified in (5.33) are satisfied.

First, we show that the constants $c_1,\ c_2$ resulted from (5.37) and the power constraints always satisfy $\frac{c_2}{c_1} > \gamma$. This is proved by contradiction as follows. Suppose $\frac{c_2}{c_1} \leq \gamma$. Following (5.37), for any $i = 1, 2, ..., N_c,\ P^*_{J,i} \geq c_1 - \frac{1}{\gamma}\sigma^2_{n,i}$. Thus, $c_2 - \gamma P^*_{J,i} - \sigma^2_{n,i} \leq c_2 - \gamma(c_1 - \frac{1}{\gamma}\sigma^2_{n,i}) - \sigma^2_{n,i} = c_2 - \gamma c_1 \leq 0$. This implies that for all subchannels, we always have $P^*_{s,i} = \left(c_2 - \gamma P^*_{J,i} - \sigma^2_{n,i}\right)^+ = 0$, which contradicts with the power constraint that $\sum_{i=1}^{N_c} P^*_{s,i} = P_s$. As a result, we must have $\frac{c_2}{c_1} > \gamma$.

It then follows that for any subchannel, we always have $\frac{|H_{J,i}|^2}{|H_{s,i}|^2} = \gamma < \frac{c_2}{c_1}$. This ensures

that the conditions specified in (5.33) are always satisfied. Hence, the solution calculated by (5.37) must be a valid saddle point. □

Furthermore, if the magnitude spectrum of channels for the authorized user and the jammer is equal to each other, i.e., $\frac{|H_{J,i}|^2}{|H_{s,i}|^2} = \gamma = 1,\ \forall i$, the two-step water pouring algorithm in (5.37) can be graphically illustrated in Fig. 5.1, where the saddle point can simply be obtained by pouring all the signal power after pouring all the jamming power into a tank with given noise power levels. We would like to point out that under AWGN channels, the noise power levels are flat; hence, the water pouring process here would result in uniform power allocation for both the jammer and the authorized user, which echoes the results in Section 5.3.

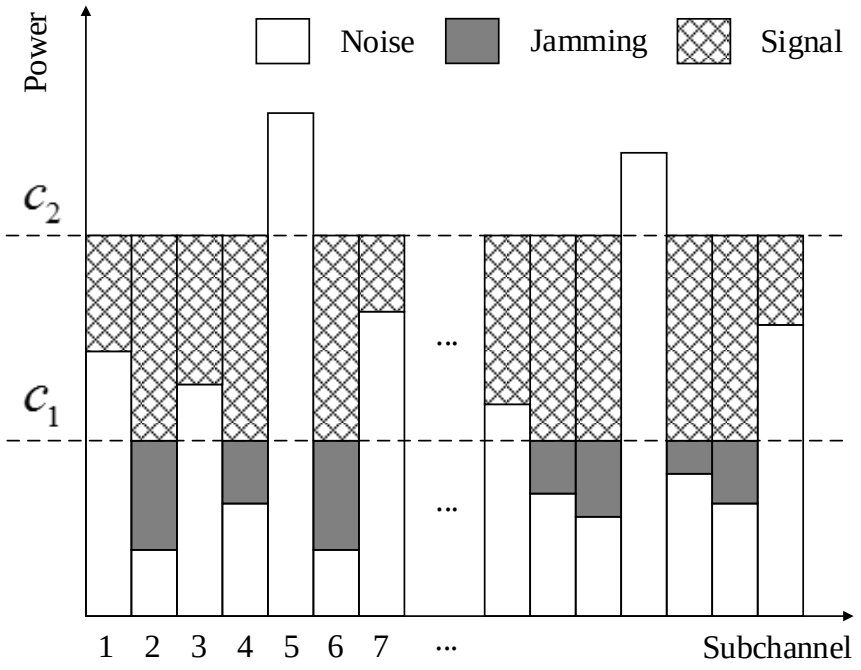


Figure 5.1: Water pouring under jamming with equal channel magnitude spectrum for the authorized user and the jammer (i.e., $\frac{|H_{J,i}|^2}{|H_{s,i}|^2} = \gamma = 1,\ \forall i$).

Discussions: Theorem 5.3 provides an efficient two-step water pouring algorithm to calculate the saddle point of the minimax problem. This algorithm guarantees a valid saddle point under certain conditions as illustrated in (5.33). Corollary 5.1 further shows a sufficient (but may not be necessary) condition for (5.33) being satisfied: the channels for the authorized user and the jammer are relatively flat with respect to each other, i.e., their magnitude spectrum is proportional to each other. From the arbitrarily varying channel (AVC) [15, 71] point of view, the correlation between the user channel and the jamming channel can be regarded as an indicator of possible symmetricity between the user and the jammer. In the case that the user channel and the jammer channel are not relatively flat with respect to each other, as shown in Section 5.5.2, as long as the cross correlation between the two channels is reasonably high, we found that the algorithm in Theorem 5.3 can still provide a much better solution than uniform power allocation.

5.5 Numerical Results

In this section, we evaluate the impact of different strategies applied by the authorized user and the jammer on the capacity of the authorized user through numerical examples. In the following, we assume $N_c = 64$, $B = 1$ MHz, $P_s = P_J = 16$ W. Both AWGN channels and frequency selective fading channels are evaluated.

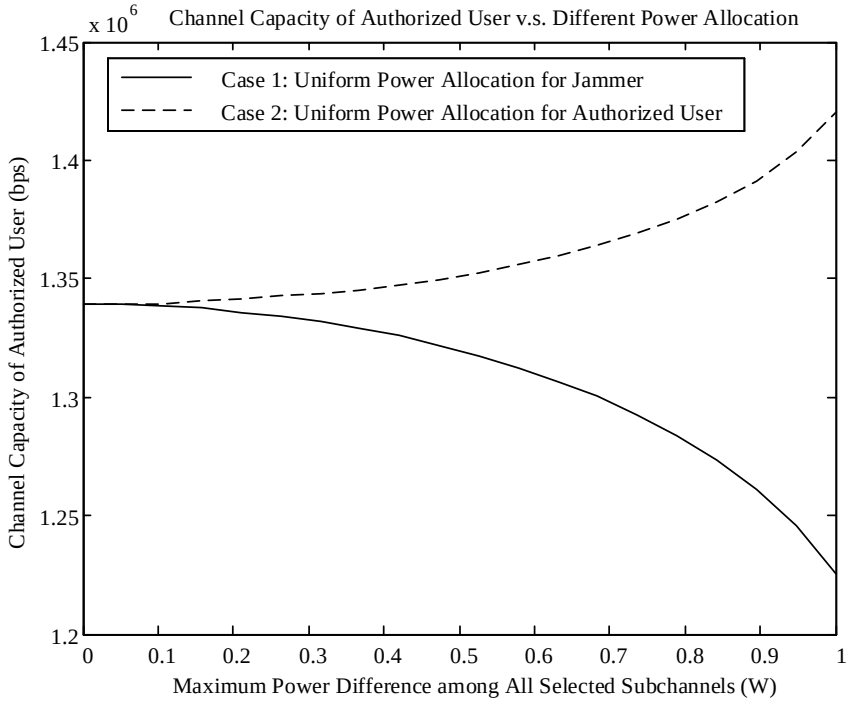
5.5.1 AWGN Channels

In this subsection, we investigate AWGN channels, where the overall signal-to-noise ratio (SNR) is set to 10dB. In light of Proposition 5.1, we assume that both the authorized user and the jammer apply uniform subchannel selection, that is, all subchannels are equally

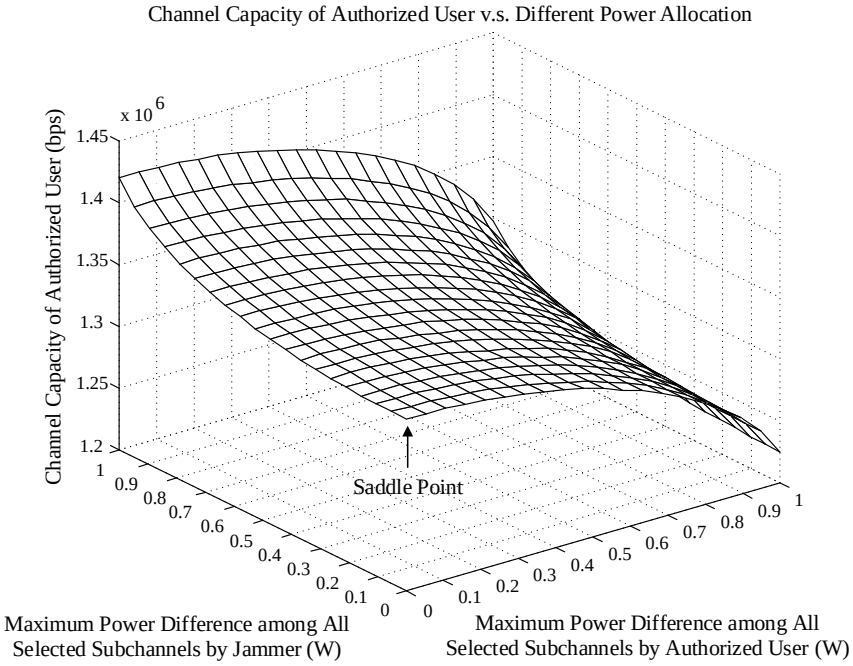
probable to be selected.

1) Capacity v.s. Power Allocation with Fixed K_s and K_J In this example, we evaluate the capacity of the authorized user under different transmit and jamming power allocation schemes. We set the power allocation vector as one whose elements, if sorted, would form an arithmetic sequence, and we use the *maximum power difference* among all the selected subchannels as the metric of uniformity. Hence, the maximum power difference indicates how far the power allocation is away from being uniform, and a zero difference means uniform power allocation. Fig. 5.2 shows the results when both the authorized user and the jammer select half of all the available subchannels each time, while Fig. 5.3 corresponds to the case where both of them select all the available subchannels. In the 2D view, we evaluate the capacity in two scenarios: (1) uniform jamming power allocation, while the power allocation for the authorized user is nonuniform; (2) the case which is exactly opposite to (1). The 3D counterpart in these two figures provides spacial views on the physical meanings of the derived saddle points. Note that the saddle point is reached at one of the vertices, hence the 3D view includes only a quarter portion of a regular saddle-point graph.

From Fig. 5.2 and Fig. 5.3, *it can be seen that*, when the number of user-activated subchannels K_s and the number of jammed subchannels K_J are both fixed: (1) if the jammer applies uniform power allocation, the authorized user maximizes its capacity when it applies uniform power allocation as well; (2) if the authorized user applies uniform power allocation, the jammer minimizes the capacity of the authorized user when it applies uniform power allocation as well; (3) the minimax capacity (the intersections in 2D view and the labeled saddle points in 3D view) serves as a lower bound when the authorized user applies uniform power allocation under all possible jamming power allocation schemes, and simultaneously

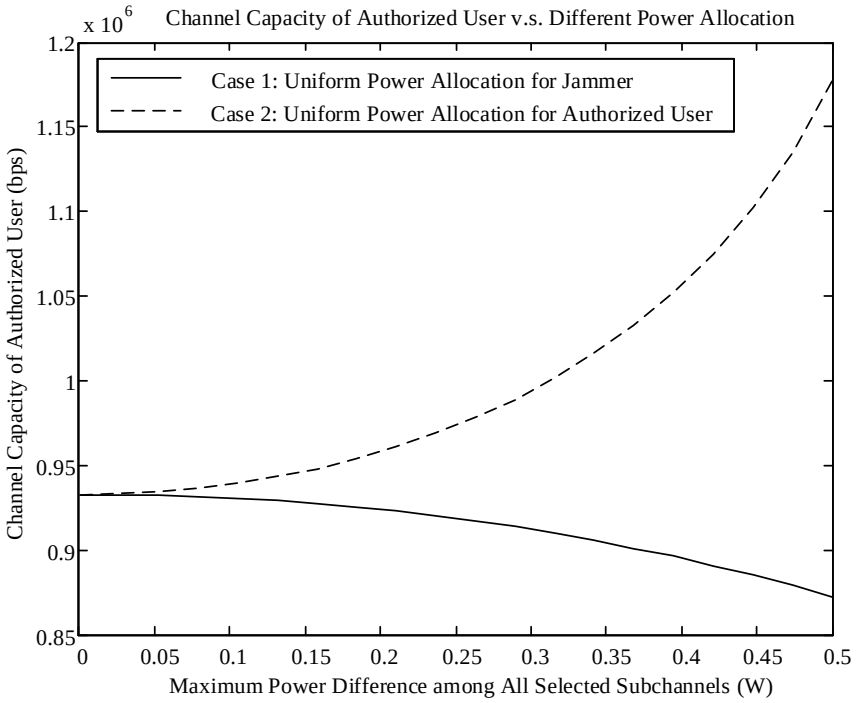


(a) 2D view.

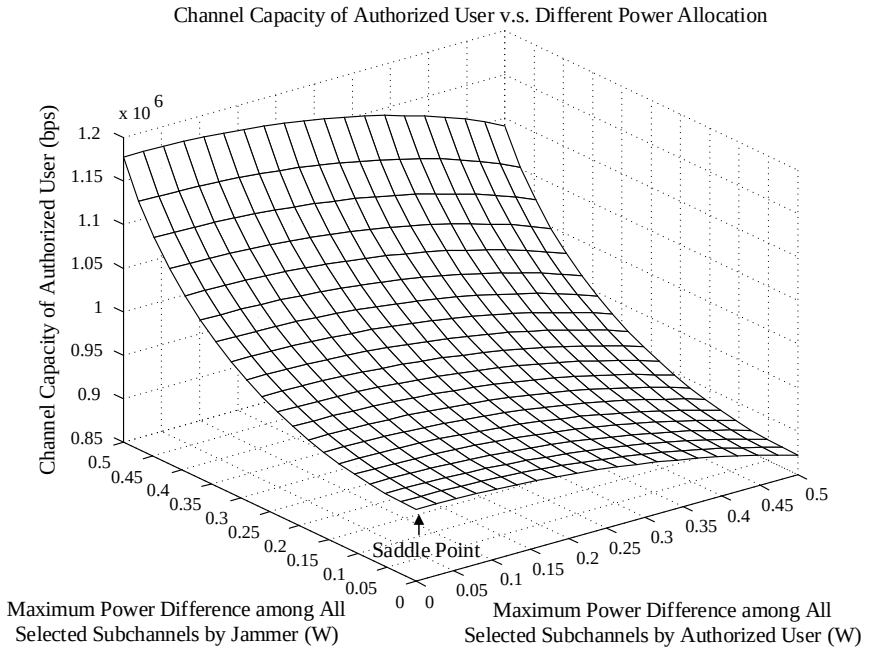


(b) 3D view.

Figure 5.2: AWGN channels: channel capacity of given bandwidth (1 MHz) v.s. different power allocation. Both the authorized user and the jammer select half of all the available subchannels each time.



(a) 2D view.



(b) 3D view.

Figure 5.3: AWGN channels: channel capacity of given bandwidth (1 MHz) v.s. different power allocation. Both the authorized user and the jammer always select all the available subchannels.

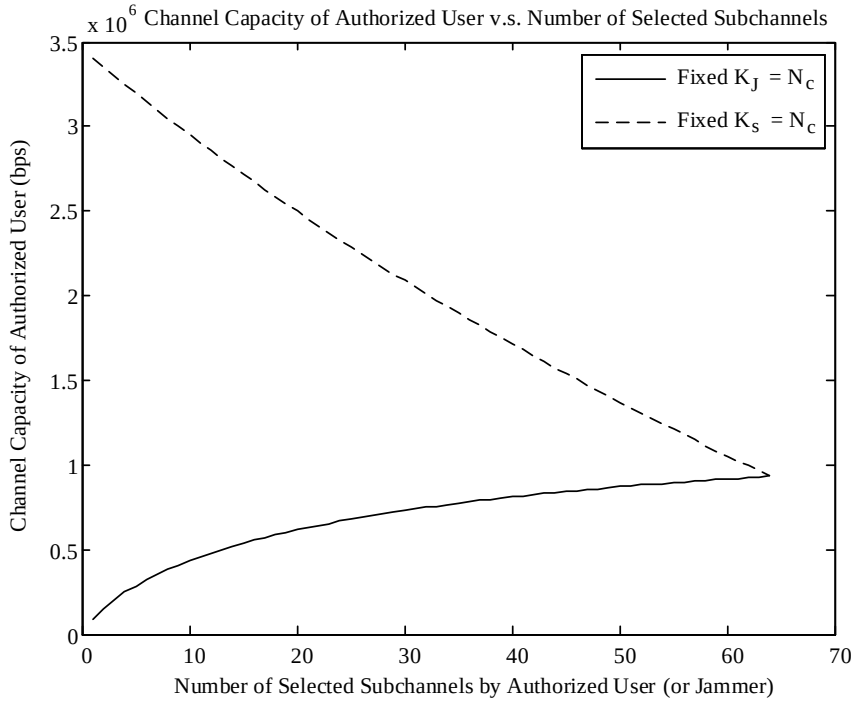
it serves as an upper bound when the jammer applies uniform power allocation under all possible signal power allocation schemes. The results above match well with Proposition 5.1.

2) Capacity v.s. Number of Selected Subchannels In this example, we evaluate the capacity of the authorized user with different number of selected subchannels by the authorized user or the jammer. For each possible pair (K_s, K_J), both the authorized user and the jammer apply uniform power allocation. *It is observed in Fig. 5.4 that* the best strategy is to utilize all the N_c subchannels, either for the authorized user to maximize its capacity, or for the jammer to minimize the capacity of the authorized user. This result matches well with Proposition 5.2.

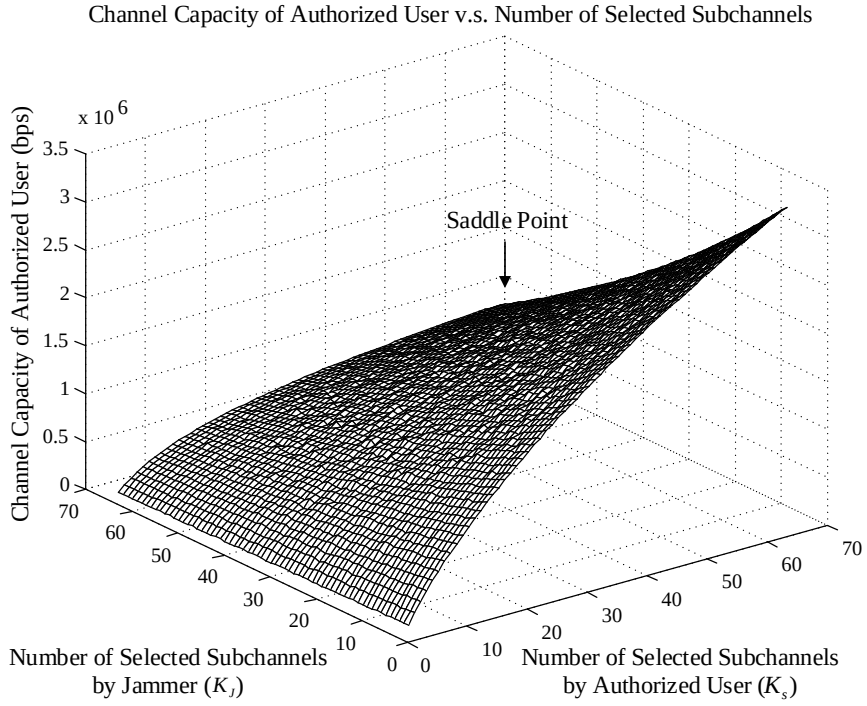
5.5.2 Frequency Selective Fading Channels

In this subsection, we investigate frequency selective fading channels. To address the correlation between channels for the authorized user and the jammer, we introduce a correlation index, $\lambda(0 \leq \lambda \leq 1)$, which characterizes how much dependence the two channels have on each other. More specifically, in this simulation example, we generate the magnitude spectrum of channels in two steps: (1) create two random vectors, $\mathbf{x}_1 = [x_{1,1}, x_{1,2}, ..., x_{1,N_c}]$ and $\mathbf{x}_2 = [x_{2,1}, x_{2,2}, ..., x_{2,N_c}]$, in which all $x_{1,i}$ and $x_{2,i}$ are independent random variables with uniform distribution over (0,1); (2) generate the magnitude spectrum of the channel for the authorized user by assigning $|H_{s,i}|^2 = x_{1,i},\ \forall i$, and that for the jammer as $|H_{J,i}|^2 = \lambda|H_{s,i}|^2 + (1-\lambda)x_{2,i},\ \forall i$. Particularly, $\lambda = 1$ generates equal channel magnitude spectrum for the authorized user and the jammer, while $\lambda = 0$ generates completely independent channel magnitude spectrum.

In Fig. 5.5, with the SNR being set to 10dB, we compare the capacity of the authorized user in three cases with different power allocation strategies: (1) both the authorized user



(a) 2D view.



(b) 3D view.

Figure 5.4: AWGN channels: channel capacity of given bandwidth (1 MHz) v.s. number of selected subchannels.

and the jammer perform power allocation following the algorithm in Theorem 5.3; (2) the authorized user performs power allocation following the algorithm in Theorem 5.3, while the jammer performs uniform power allocation; (3) the jammer performs power allocation following the algorithm in Theorem 5.3, while the authorized user performs uniform power allocation.

There are *four main observations*: (1) the authorized user always has a higher capacity if he performs signal power allocation following the algorithm in Theorem 5.3, compared to uniform signal power allocation; (2) the capacity of the authorized user decreases significantly if the channel of the jammer is more correlated with that of the authorized user, which implies that the jammer can enhance its jamming effect by delivering jamming power through a channel that is correlated with the authorized user's channel; (3) in a more serious case with high channel correlation, the jammer can limit the capacity of the authorized user more effectively by performing jamming power allocation following the algorithm in Theorem 5.3, compared to uniform jamming power allocation; (4) if the jammer is not able to achieve high channel correlation, uniform jamming power allocation is preferred instead of applying the algorithm in Theorem 5.3.

In Fig. 5.6, with the channel correlation index being set to $\lambda = 0.75$, we compare the capacity of the authorized user with different power allocation versus varying SNR. *It is observed that*: (1) with reasonably high correlation between the user channel and the jamming channel, the power allocation strategy given by Theorem 5.3 has notable advantage over uniform power allocation, either for the authorized user to maximize its capacity, or for the jammer to minimize the capacity of the authorized user; (2) when the SNR is sufficiently high, the jamming power allocation produced by Theorem 5.3 converges to uniform.

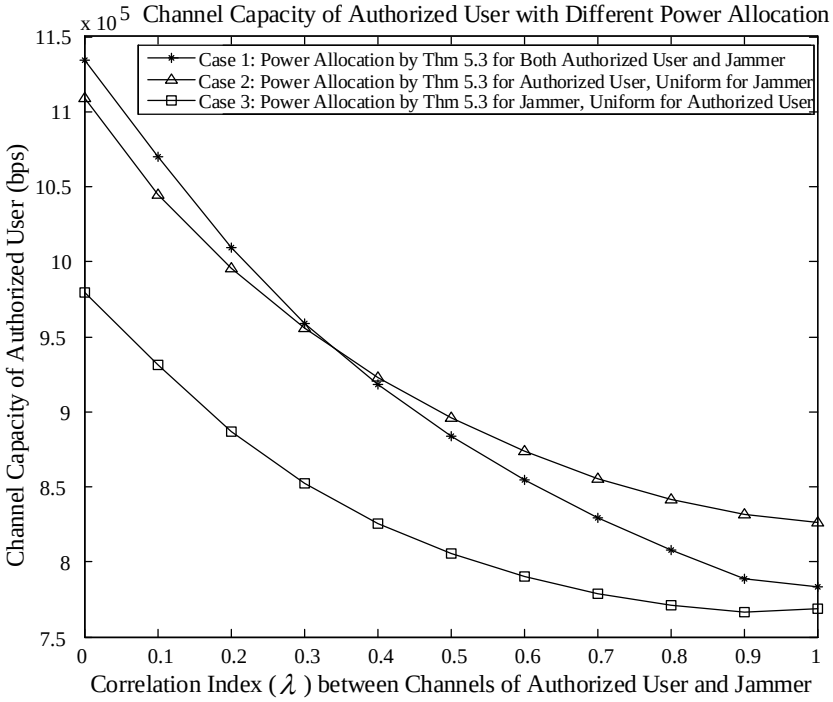


Figure 5.5: Frequency selective fading channels: channel capacity of given bandwidth (1 MHz) with different power allocation v.s. varying channel correlation index λ.

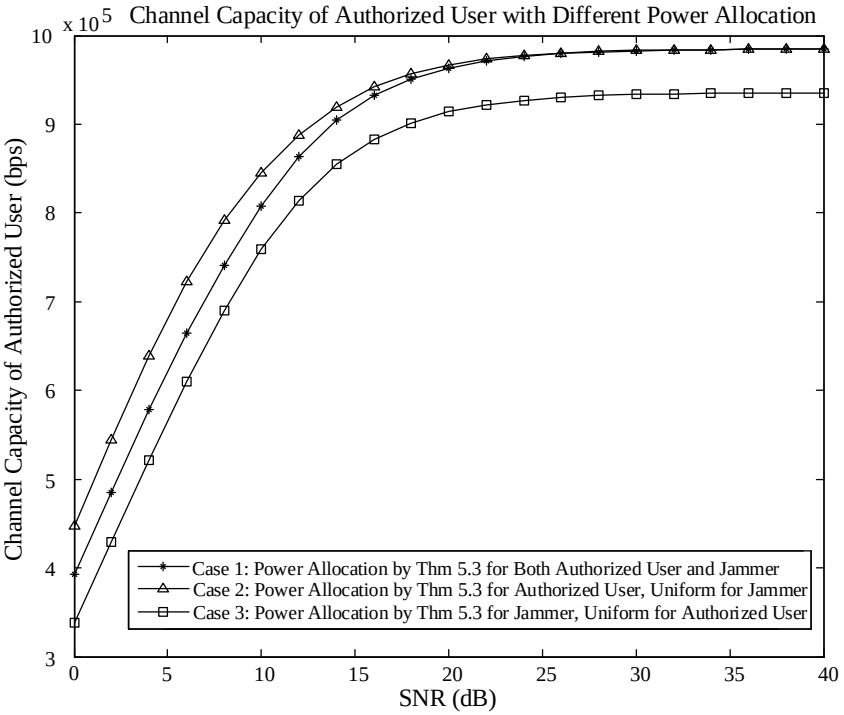


Figure 5.6: Frequency selective fading channels: channel capacity of given bandwidth (1 MHz) with different power allocation v.s. varying SNR.

5.6 Summary

In this chapter, we considered jamming and jamming mitigation as a game between a power-limited jammer and a power-limited authorized user, who operate independently over the same spectrum consisting of multiple bands. The strategic decision-making of the authorized user and the jammer was modeled as a two-party zero-sum game, where the payoff function is the capacity that can be achieved by the authorized user in presence of the jammer. *Under AWGN channels*, we found that either for the authorized user to maximize its capacity, or for the jammer to minimize the capacity of the authorized user, the best strategy is to distribute the signal power or jamming power uniformly over all the available spectrum. *Under frequency selective fading channels*, we characterized the dynamic relationship between the optimal signal power allocation and the optimal jamming power allocation in the minimax game, and proposed an efficient two-step water pouring algorithm to find the optimal power allocation schemes for both the authorized user and the jammer. Numerical results were provided to demonstrate the effectiveness of the proposed strategies for both AWGN and frequency selective fading channels.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

The contributions of this dissertation lie in three aspects: (1) To improve the spectral efficiency of the OFDM systems, we incorporated the idea of message-driven frequency hopping into OFDM systems by transmitting extra information through message-driven subcarrier selection; (2) To enhance the anti-jamming features of OFDM and CDMA systems, we introduced security-enhanced shared randomness between transmitters and receivers by integrating cryptographic techniques into the physical layer transceiver design; (3) To combat fast cognitive jamming in multiband communications, taking jamming and jamming mitigation as a two-party zero-sum game, we investigated the optimal transmission and jamming strategies using game theory. More specifically, the main conclusions are summarized in the following.

On *Spectrally Efficient Multicarrier Transmission with Message-Driven Subcarrier Selection*:

- First, we proposed a multi-carrier transmission scheme with message-driven idle subcarriers (MC-MDIS). The basic idea is to use part of the information bits, named carrier bits, to specify idle subcarriers while transmitting ordinary bits regularly on all the other subcarriers. In this way, if the number of subcarriers is much larger than the

adopted constellation size (e.g., in most OFDM systems), we can transmit more information bits at an even lower power consumption. This is because the number of carrier bits transmitted through each idle subcarrier is more than that of the ordinary bits carried by each regular symbol, and all the carrier bits are transmitted with no power consumption through idle subcarrier selection. When applied to the OFDM framework, i.e., using orthogonal subcarriers and IFFT/FFT blocks, MC-MDIS can achieve even higher spectral efficiency than OFDM, while keeping a higher power efficiency. The existence of idle subcarriers can also decrease possible inter-carrier interference between their neighboring subcarriers.

- An alternative scheme, with message-driven strengthened subcarriers (MC-MDSS), was proposed simply by replacing the idle subcarriers in MC-MDIS with strengthened ones. In MC-MDSS, different from MC-MDIS, the strengthened subcarriers selected by the carrier bits can also carry ordinary bits. This leads to higher spectral efficiency than MC-MDIS due to the additional ordinary bits transmitted on the strengthened subcarriers.

- To enhance the security of the proposed schemes under eavesdropping and partial-band jamming, we further implemented secure subcarrier assignment (SSA) and secure symbol mapping (SSM) in both MC-MDIS and MC-MDSS. Besides working as an effective way in subcarrier grouping to maximize the two schemes' spectral efficiency, SSA shuffles and groups all the available subcarriers dynamically and secretly such that: (i) The eavesdroppers cannot recover the carrier bits, even if they successfully locate the idle subcarriers. For the ordinary bits, they cannot sort the bits in the right order, even if they can recover them from the symbols correctly; (ii) Burst errors caused

by partial-band jamming can be randomized by SSA and thus reduced to the correction range of the error-control coding; (iii) No follower jamming can be launched toward any particular users. In addition to SSA, SSM offers a dynamic and secret symbol mapping scheme, which further prevents the eavesdroppers from trying to sort the ordinary bits correctly or break SSA reversely by exploiting information redundancy.

On *Precoding for OFDM under Disguised Jamming*:

- First, we analyzed the impact of disguised jamming on OFDM systems. It was shown that due to the symmetricity between the authorized signal and jamming, the BER of OFDM systems without symbol-level precoding or only with repeated symbol-level coding is lower bounded by a modulation specific constant, which cannot be improved by simply increasing the SNR.

- Second, we developed an optimal precoding scheme, which minimizes the BER of OFDM systems under full-band disguised jamming. It was shown that the most efficient way to combat full-band disguised jamming in OFDM systems is to concentrate the total available power and distribute it uniformly over a particular number of subcarriers instead of the entire spectrum. The underlying argument is that for a particular subcarrier, when the signal-to-jamming ratio is large enough, then the receiver can distinguish the authorized signal from disguised jamming under the presence of noise. The precoding scheme was further randomized to protect the OFDM communication from a follower fashion of disguised jamming.

On *CDMA System Design and Capacity Analysis under Disguised Jamming*:

- First, we analyzed the performance of conventional CDMA systems under disguised jamming, and showed that due to the symmetricity between the authorized signal and

the jamming interference, the receiver cannot really distinguish the authorized signal from jamming, leading to complete communication failure. To combat disguised jamming for CDMA, we treated the problem in two separate cases: (i) For CDMA systems with public codes which cannot be concealed for some reason (e.g., in civilian GPS), we proposed to mitigate the disguised jamming through robust receiver design; (ii) For CDMA systems which allow code concealment, we proposed to combat disguised jamming using secure scrambling.

- For CDMA systems that fall into the first category, with public codes readily available, a jammer can launch disguised jamming easily and it would be a great threat to the authorized users. However, we observed that while malicious user can get complete information about the spreading code and pulse shaping filter, they cannot capture the exact timing information of the authorized signal. By exploiting this small time difference between the authorized signal and the jamming interference, the conventional CDMA receiver was re-designed to achieve robust performance under disguised jamming. More specifically, we proposed to estimate the authorized signal, the phase and power level or range of the jamming interference by minimizing the MSE between the received signal and the jammed signal, which is the sum of the authorized signal and the disguised jamming. At the same time, we can get a good evaluation on how severe the jamming is.

- For CDMA systems that fall into the second category, we proposed to combat disguised jamming using secure scrambling. More specifically, instead of using conventional scrambling codes, we applied advanced encryption standard (AES) to generate the security-enhanced scrambling codes. Its security is guaranteed by AES, which is proven

to be secure under all known attacks. Assuming ideal synchronization between the authorized user and the jammer, we proved that: the capacity of the conventional CDMA systems without secure scrambling under disguised jamming is actually zero; however, the capacity can be significantly increased when CDMA systems are protected using secure scrambling. The underlying argument is that: the secure scrambling process results in security-enhanced PN codes which are intractable for the malicious user; hence it breaks the symmetricity between the authorized user and the jammer, and ensures positive transmission capacity under disguised jamming.

On *Multiband Transmission Under Jamming - A Game Theoretic Perspective*:

- First, we formulated jamming and jamming mitigation as a game between a power-limited jammer and a power-limited authorized user, who operate independently over the same spectrum consisting of multiple bands or subchannels. The authorized user is always trying to maximize its capacity under jamming by applying an optimal strategy. Accordingly, the jammer would like to find an optimal strategy that can minimize the capacity of the authorized user. To apply a chosen strategy, the authorized user or the jammer selects a particular number of subchannels and applies a particular power allocation scheme over the selected subchannels. For both the authorized user and the jammer, the subchannels may not be chosen with equal probability. The strategic decision-making of the authorized user and the jammer was modeled as a two-party zero-sum game, where the payoff function is the capacity that can be achieved by the authorized user in presence of the jammer.

- Second, we investigated the game under AWGN channels. We explored the possibility for the authorized user or the jammer to randomly utilize part (or all) of the available

spectrum and/or apply nonuniform power allocation. It was found that: under AWGN channels, either for the authorized user to maximize its capacity, or for the jammer to minimize the capacity of the authorized user, the best strategy is to distribute the transmission power or jamming power uniformly over all the available spectrum. The minimax capacity can be calculated based on the channel bandwidth and the signal-to-jamming and noise ratio, and it matches with the Shannon channel capacity formula.

- Third, we considered frequency selective fading channels. We characterized the dynamic relationship between the optimal signal power allocation and the optimal jamming power allocation in the minimax game, and proposed an efficient two-step water pouring algorithm to find the optimal power allocation schemes for both the authorized user and the jammer.

6.2 Future Work

This dissertation is mainly focused on security enhancement for existing communication technologies, like CDMA in 3G and OFDM in 4G. However, the security issues in the upcoming 5G standards remain an open topic. The underlying challenges include: (i) Instead of only handling time and frequency dimensions in 3G and 4G, we need to take the space dimension into consideration due to the application of massive MIMO in 5G; (ii) The network protocols for 5G will possibly become complicated in order to accommodate high-demanding services as well as high density relay distribution.

In the future, we will investigate the potential security issues in 5G communications, and propose new jamming mitigation/prevention techniques to secure the next-generation wireless communication standards.

APPENDICES

Appendix A

Optimality of Uniform Subcarrier Grouping

The proof here is conducted for the MC-MDIS case, but it works similarly for MC-MDSS. Suppose we have a nonuniform subcarrier grouping, and the total N_c available subcarriers are grouped into G groups, i.e.,

$$N_c = \sum_{g=0}^{G-1} N_{c,g}, \tag{A.1}$$

where $N_{c,g}$ denotes the number of subcarriers in the gth group. We assume $N_{c,g} \geq M$; otherwise, the idle subcarrier would not carry more information than an ordinary symbol. Please also note that $N_{c,g}$ should be a power of 2, since this is the most efficient way to carry information bits using idle subcarriers. For the gth subcarrier group, the achievable bit rate (including both carrier bits and ordinary bits) can be written as

$$R_{b,g} = R_s[\log_2 N_{c,g} + (N_{c,g} - 1)\log_2 M] = R_s[N_{c,g}\log_2 M + \log_2 \frac{N_{c,g}}{M}], \tag{A.2}$$

where R_s is the OFDM symbol rate. Under the assumption that $N_{c,g} \geq M$, $\frac{N_{c,g}}{M} = 2^n$ with $n \geq 1$. This leads to the following inequality,

$$\log_2 \frac{N_{c,g}}{M} \leq \frac{N_{c,g}}{2M}. \tag{A.3}$$

Substituting (A.3) into (A.2), we have

$$R_{b,g} \leq R_s N_{c,g} [\log_2 M + \frac{1}{2M}]. \tag{A.4}$$

Taking all the subcarrier groups into account, the total bit rate would be

$$R_b = \sum_{g=0}^{G-1} R_{b,g} \leq R_s N_c [\log_2 M + \frac{1}{2M}]. \tag{A.5}$$

The RHS of (A.5) is exactly the bit rate in (2.16) that the uniform subcarrier grouping can achieve, which is derived in Section 2.5.1. This result demonstrates that *any nonuniform subcarrier grouping would not outperform the uniform one in terms of spectral efficiency.*

Appendix B

Symbol Error Probability of Carrier Bits in MC-MDIS

In conventional FSK, the amplitude of an active subcarrier with a symbol-level SNR of $\frac{E_s}{N_0}$ obeys a Rician distribution [48, eqn. (5.4-39), page 309], and those of the other idle subcarriers follow Rayleigh distributions [48, eqn. (5.4-40), page 309]. Similarly, in MC-MDIS, we can model the amplitudes of the idle subcarrier (indexed by k_j) and the active subcarriers (with an SNR of $\frac{E_s}{N_0}$) through the following distributions,

$$f_{R_{k_j}}(r_{k_j}) = r_{k_j} \exp(-\frac{r_{k_j}^2}{2}), \tag{B.1}$$

$$f_{R_k}\left(r_k|\sqrt{2\frac{E_s}{N_0}}, 1\right) = r_k \exp\left[-\frac{1}{2}\left(r_k^2 + 2\frac{E_s}{N_0}\right)\right] I_0\left(\sqrt{2\frac{E_s}{N_0}} r_k\right), \quad k \neq k_j, \tag{B.2}$$

respectively, where $I_0(\cdot)$ is the zero-order modified Bessel function. The probability of a correct decision, P_c, is the probability that $R_k > R_{k_j}, \forall k \neq k_j$. Hence,

$$\begin{aligned} P_c =& P(R_1 > R_{k_j}, ..., R_{k_j-1} > R_{k_j}, R_{k_j+1} > R_{k_j}, ..., R_{N_f} > R_{k_j}) \\ =& \int_0^\infty P(R_1 > R_{k_j}, ..., R_{k_j-1} > R_{k_j}, R_{k_j+1} > R_{k_j}, ..., R_{N_f} > R_{k_j} | R_{k_j} = x) f_{R_{k_j}}(x) dx. \end{aligned} \tag{B.3}$$

Note that $\forall k \neq k_j$, R_k's are statistically independent and identically distributed (i.i.d.), (B.3) can be further written as

$$P_c = \int_0^\infty [P(R_k > R_{k_j} | R_{k_j} = x)]^{N_f - 1} f_{R_{k_j}}(x) dx, \quad k \neq k_j. \tag{B.4}$$

We define $\bar{Q}_1 = P(R_k > R_{k_j} | R_{k_j} = x)$, and calculate it by considering all the possible power levels. Thus,

$$\begin{aligned} \bar{Q}_1 &= P(R_k > R_{k_j} | R_{k_j} = x) \\ &= \sum_{i=1}^{T} p_i \int_x^\infty f_{R_k}\left(r | \sqrt{2\frac{E_{s,i}}{N_0}}, 1\right) dr \\ &= \sum_{i=1}^{T} p_i Q_1\left(\sqrt{2\frac{E_{s,i}}{N_0}}, x\right), \end{aligned} \tag{B.5}$$

where $Q_1(a,b) = \int_b^\infty x \exp(-\frac{x^2+a^2}{2}) I_0(ax) dx$ is the Marcum Q-function, and the definitions of p_i and $\frac{E_{s,i}}{N_0}$ can be found in (2.24)-(2.25). Combining (B.1), (B.4)-(B.5), the symbol error probability, which is $P_M = 1 - P_c$, becomes

$$P_M = 1 - \int_0^\infty \bar{Q}_1^{N_f - 1} x e^{-\frac{x^2}{2}} dx. \tag{B.6}$$

Appendix C

Symbol Error Probability of Carrier Bits in MC-MDSS

For MC-MDSS, the amplitudes of the power-strengthened subcarrier (indexed by k_j and with an SNR of $\frac{E_{s,1}^{(o)}}{N_0}$) and the regular ones (with an SNR of $\frac{E_{s,2}^{(o)}}{N_0}$) follow Rician distributions, which can be represented as

$$\begin{cases} f_{R_{k_j}}\left(r_{k_j}|\sqrt{2\frac{E_{s,1}^{(o)}}{N_0}},1\right) = r_{k_j}\exp\left[-\frac{1}{2}\left(r_{k_j}^2+2\frac{E_{s,1}^{(o)}}{N_0}\right)\right]I_0\left(\sqrt{2\frac{E_{s,1}^{(o)}}{N_0}}r_{k_j}\right), \\ f_{R_k}\left(r_k|\sqrt{2\frac{E_{s,2}^{(o)}}{N_0}},1\right) = r_k\exp\left[-\frac{1}{2}\left(r_k^2+2\frac{E_{s,2}^{(o)}}{N_0}\right)\right]I_0\left(\sqrt{2\frac{E_{s,2}^{(o)}}{N_0}}r_k\right), \quad k\neq k_j, \end{cases} \tag{C.1}$$

respectively. The probability of a correct decision, P_c, is the probability that $R_{k_j} > R_k, \forall k \neq k_j$. Hence,

$$\begin{aligned} P_c =& P(R_1 < R_{k_j},...,R_{k_j-1} < R_{k_j}, R_{k_j+1} < R_{k_j},...,R_{N_f} < R_{k_j}) \\ =& \int_0^\infty P(R_1 < R_{k_j},...,R_{k_j-1} < R_{k_j}, R_{k_j+1} < R_{k_j},...,R_{N_f} < R_{k_j}|R_{k_j}=x) f_{R_{k_j}}(x)dx. \end{aligned} \tag{C.2}$$

Note that $\forall k \neq k_j$, R_k's are i.i.d., (C.2) can be further written as

$$P_c = \int_0^\infty [P(R_k < R_{k_j}|R_{k_j}=x)]^{N_f-1} f_{R_{k_j}}(x)dx, \quad k\neq k_j, \tag{C.3}$$

where

$$P(R_k < R_{k_j} | R_{k_j} = x) = \int_0^x f_{R_k(r)} dr = 1 - Q_1\left(\sqrt{2\frac{E_{s,2}^{(o)}}{N_0}}, x\right), \tag{C.4}$$

in which $Q_1(a,b) = \int_b^\infty x \exp(-\frac{x^2+a^2}{2}) I_0(ax) dx$ is the Marcum Q-function. The $(N_f - 1)$th power of (C.4) can then be expressed as

$$\left[1 - Q_1\left(\sqrt{2\frac{E_{s,2}^{(o)}}{N_0}}, x\right)\right]^{N_f-1} = \sum_{k=0}^{N_f-1} (-1)^k \binom{N_f - 1}{k} \left[Q_1\left(\sqrt{2\frac{E_{s,2}^{(o)}}{N_0}}, x\right)\right]^k. \tag{C.5}$$

Substituting (C.5) into (C.3), we obtain the probability of a correct decision as

$$P_c = \sum_{k=0}^{N_f-1} (-1)^k \binom{N_f - 1}{k} \int_0^\infty \left[Q_1\left(\sqrt{2\frac{E_{s,2}^{(o)}}{N_0}}, x\right)\right]^k f\left(x | \sqrt{2\frac{E_{s,1}^{(o)}}{N_0}}, 1\right) dx, \tag{C.6}$$

where $f(x|\nu,\sigma) = \frac{x}{\sigma^2} \exp(-\frac{x^2+\nu^2}{2\sigma^2}) I_0(\frac{\nu x}{\sigma^2})$ denotes the probability density function of a Rician distribution, which is specified in (C.1). Then, the symbol error probability, which is $P_M = 1 - P_c$, becomes

$$P_M = \sum_{k=1}^{N_f-1} (-1)^{k+1} \binom{N_f - 1}{k} \int_0^\infty \left[Q_1\left(\sqrt{2\frac{E_{s,2}^{(o)}}{N_0}}, x\right)\right]^k f\left(x | \sqrt{2\frac{E_{s,1}^{(o)}}{N_0}}, 1\right) dx. \tag{C.7}$$

Appendix D

Evaluation on Peak-to-Average Power Ratio (PAPR)

In Fig. D.1, we provide the cumulative density functions of the peak-to-average power ratios (PAPRs) for OFDM, MC-MDIS and MC-MDSS. We can hardly see any difference among the PAPR distributions of these three schemes, which demonstrates that the proposed schemes will not suffer from higher PAPRs than OFDM.

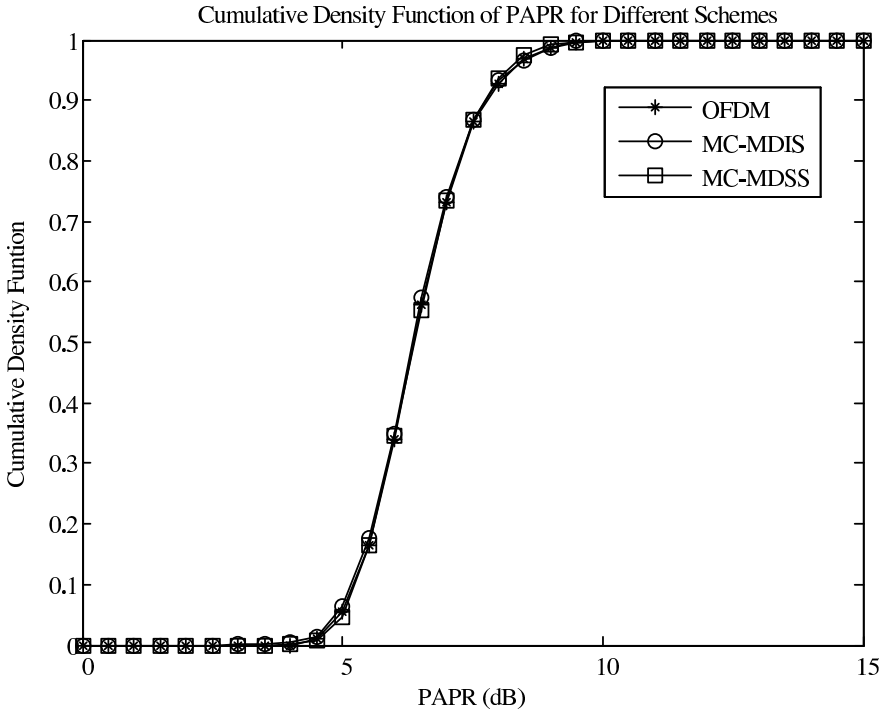


Figure D.1: Cumulative density function of PAPR for different schemes.

Appendix E

Subchannel Selection with Nonuniform Preferences

This appendix provides an approach to select K out of N_c subchannels according to a probability vector $\boldsymbol{\omega} = [\omega_1, \omega_2, ..., \omega_{N_c}]$, where ω_m denotes the probability that the mth subchannel is selected each time, and $\sum_{m=1}^{N_c} \omega_m = K$. Suppose ω_m's are rational numbers, then there exists a finite positive integer M, such that $l_m = M\omega_m$ is a positive integer for all $1 \leq m \leq N_c$. Furthermore, we have $\sum_{m=1}^{N_c} l_m = KM$. The proposed approach works with the following steps:

1. Construct a $K \times M$ matrix, in which the kth ($1 \leq k \leq M$) column represents the kth subchannel selection result; Prepare l_m balls labeled "subchannel m" for all $1 \leq m \leq N_c$, and there are $\sum_{m=1}^{N_c} l_m = KM$ balls in total;

2. Initialization: set $k = 1$ as the current row to be filled, $m = 1$ as the current subchannel to be worked on, and $r = M$ as the number of empty entries for the current row;

3. Select l_1 entries randomly from the 1st ($k = 1$) row of the matrix, and fill them with all the l_1 balls. For $k \geq 1$ and $m \geq 2$, placement of the l_m balls labeled "subchannel m" has two cases:

   - If $l_m \leq r$, the current row has a capacity large enough to accommodate all the l_m

balls. Select l_m entries randomly from the kth row of the matrix, and fill them with all the l_m balls. Update the number of empty entries for the current row by $r \leftarrow (r - l_m)$; if all empty entries of the current row are filled, move to the next row by setting $k \leftarrow (k+1)$ and $r \leftarrow M$.

- If $l_m > r$, the l_m balls have to be split into the current row and the next row. First fill the r empty entries of the kth row with r out of l_m balls; then select $l_m - r$ out of $M - r$ entries randomly from the $(k+1)$th row, and fill them with the remaining $l_m - r$ balls. Note that there are only $M - r$ entries in the new row available here, since the r columns already containing balls labeled "subchannel m" have to be avoided. Update the number of empty entries for the current row by $r \leftarrow [M - (l_m - r)]$, and set the current row by $k \leftarrow (k+1)$.

4. Set $m \leftarrow (m+1)$ and repeat 4) until all KM balls are placed in the $K \times M$ matrix;

5. Fetch each column in the matrix to generate the subchannel selection results for M consecutive time slots, and repeat all the steps above until all information transmission is done.

In the following, we justify that the probability of the mth subchannel being selected each time is exactly the desired ω_m. For each possible $1 \leq m \leq N_c$, the number of balls labeled "subchannel m" is $l_m = M\omega_m \leq M$. According to the approach above, all the l_m balls can be placed into at most two rows in the matrix. Denote $\mathcal{P}_{m,k}$ as the probability that the mth subchannel is chosen in the kth row. Then $\mathcal{P}_{m,k} = \frac{r_k}{M}$, where r_k is the number of balls labeled "subchannel m" that have been placed in the kth row of the matrix, since the mth subchannel would appear r_k times in the kth place out of the total M times of subchannel selection. If the l_m balls are placed into only one row, e.g., the k_0th row, for each subchannel selection,

$\mathcal{P}_{m,k} = \frac{l_m}{M}$ for $k = k_0$, and zero elsewhere. Hence, the probability that the mth subchannel is selected considering all possible places would be $\mathcal{P}_m = \sum_{k=1}^{K} \mathcal{P}_{m,k} = \mathcal{P}_{m,k_0} = \frac{l_m}{M} = \omega_m$. If they are placed into two consecutive rows, e.g., the k_0th row and the $(k_0 + 1)$th row, then $\mathcal{P}_{m,k} = \frac{r}{M}$ for $k = k_0$, $\mathcal{P}_{m,k} = \frac{l_m - r}{M}$ for $k = k_0 + 1$, and zero elsewhere. In this case, $\mathcal{P}_m = \sum_{k=1}^{K} \mathcal{P}_{m,k} = \mathcal{P}_{m,k_0} + \mathcal{P}_{m,k_0+1} = \frac{r}{M} + \frac{l_m - r}{M} = \omega_m$. As a result, we can conclude that the probability that the mth subchannel is selected resulted from the proposed approach is $\mathcal{P}_m = \omega_m$.

Example: Suppose there are $N_c = 8$ subchannels, each time we select $K = 4$ out of $N_c = 8$ subchannels according to a subchannel selection probability vector $\boldsymbol{\omega}_s = [\omega_1, \omega_2, ..., \omega_8] = [0.9, 0.8.0.7, 0.6, 0.4, 0.3, 0.2, 0.1]$. In this case, $M = 10$, and we construct a 4×10 matrix. Furthermore, we prepare 40 balls, in which $M\omega_1 = 9$ balls are labeled "subchannel 1", $M\omega_2 = 8$ balls are labeled "subchannel 2", and so on. As illustrated in Fig. E.1, we first place all the 9 balls labeled "subchannel 1" in 9 entries randomly selected from the first row. Second, place 1 ball labeled "subchannel 2" in the remaining 1 entry of the first row, and the remaining 7 balls labeled "subchannel 2" in 7 entries randomly selected from the second row. Note that the columns already containing a ball labeled "subchannel 2" in the first row need to be avoided, and in the particular case with Fig. E.1 it is column 6. Repeat the procedure above until all the balls are properly placed in the matrix. Then, each column would indicate the selected subchannel indices for one subchannel selection result. The entire matrix provides the subchannel selection results for 10 time slots, and we can repeat all the steps above to generate more subchannel selection results. It can be verified that the probability for each subchannel being selected is exactly the one indicated in the subchannel selection probability vector.

	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	2	1	1	1	1
2	3	2	2	2	2	3	2	3	2	2
3	4	3	4	3	4	4	3	4	4	3
4	7	5	8	5	5	6	6	5	7	6

Figure E.1: Example on subchannel selection with nonuniform preferences.

Appendix F

Proof of Lemma 5.3

To prove Lemma 5.3, we need the following result:

Lemma F.1 *For a real-valued function* $f(v) = \ln(1+v) - \frac{v}{1+v}$, $f(v) > 0$, *for any* $v > 0$.

Proof: When $v > 0$, $f'(v) = \frac{v}{(1+v)^2} > 0$. Thus, $f(v) > f(0) = 0$. □

Now we are ready to prove Lemma 5.3.

(1) The first-order derivative of $\widetilde{C}$ over K_s,

$$\begin{aligned}\frac{\partial \widetilde{C}}{\partial K_s} =& \frac{K_J}{N_c}\frac{B}{N_c}\frac{1}{\ln 2}\left[\ln\left(1+\frac{\frac{P_s}{K_s}}{\frac{P_J}{K_J}+\frac{P_N}{N_c}}\right) - \frac{\frac{P_s}{K_s}}{\frac{P_s}{K_s}+\frac{P_J}{K_J}+\frac{P_N}{N_c}}\right] \\ &+ \left(1-\frac{K_J}{N_c}\right)\frac{B}{N_c}\frac{1}{\ln 2}\left[\ln\left(1+\frac{\frac{P_s}{K_s}}{\frac{P_N}{N_c}}\right) - \frac{\frac{P_s}{K_s}}{\frac{P_s}{K_s}+\frac{P_N}{N_c}}\right].\end{aligned} \tag{F.1}$$

Let $v_1 = \frac{\frac{P_s}{K_s}}{\frac{P_J}{K_J}+\frac{P_N}{N_c}}$, then $\frac{v_1}{1+v_1} = \frac{\frac{P_s}{K_s}}{\frac{P_s}{K_s}+\frac{P_J}{K_J}+\frac{P_N}{N_c}}$. Similarly, let $v_2 = \frac{\frac{P_s}{K_s}}{\frac{P_N}{N_c}}$, then $\frac{v_2}{1+v_2} = \frac{\frac{P_s}{K_s}}{\frac{P_s}{K_s}+\frac{P_N}{N_c}}$. Applying Lemma F.1 to (F.1), we have

$$\frac{\partial \widetilde{C}}{\partial K_s} > 0, \text{ for any } K_s = 1, 2, ..., N_c. \tag{F.2}$$

(2) The first-order derivative of $\widetilde{C}$ over K_J,

$$\begin{aligned}\frac{\partial \widetilde{C}}{\partial K_J} =& \frac{K_s}{N_c}\frac{B}{N_c}\frac{1}{\ln 2}\left[\ln\left(1+\frac{\frac{P_s}{K_s}}{\frac{P_J}{K_J}+\frac{P_N}{N_c}}\right)-\ln\left(1+\frac{\frac{P_s}{K_s}}{\frac{P_N}{N_c}}\right)\right. \\ &\left.+\frac{\frac{P_s}{K_s}\frac{P_J}{K_J}}{\left(\frac{P_s}{K_s}+\frac{P_J}{K_J}+\frac{P_N}{N_c}\right)\left(\frac{P_J}{K_J}+\frac{P_N}{N_c}\right)}\right] \\ <& \frac{K_s}{N_c}\frac{B}{N_c}\frac{1}{\ln 2}\left[\frac{\frac{P_s}{K_s}\frac{P_J}{K_J}}{\frac{P_N}{N_c}\left(\frac{P_s}{K_s}+\frac{P_J}{K_J}+\frac{P_N}{N_c}\right)+\frac{P_s}{K_s}\frac{P_J}{K_J}}\right. \\ &\left.-\ln\left(1+\frac{\frac{P_s}{K_s}\frac{P_J}{K_J}}{\frac{P_N}{N_c}\left(\frac{P_s}{K_s}+\frac{P_J}{K_J}+\frac{P_N}{N_c}\right)}\right)\right].\end{aligned} \tag{F.3}$$

Let $v_0 = \frac{\frac{P_s}{K_s}\frac{P_J}{K_J}}{\frac{P_N}{N_c}\left(\frac{P_s}{K_s}+\frac{P_J}{K_J}+\frac{P_N}{N_c}\right)}$, then $\frac{v_0}{1+v_0} = \frac{\frac{P_s}{K_s}\frac{P_J}{K_J}}{\frac{P_N}{N_c}\left(\frac{P_s}{K_s}+\frac{P_J}{K_J}+\frac{P_N}{N_c}\right)+\frac{P_s}{K_s}\frac{P_J}{K_J}}$. Applying Lemma F.1 to (F.3), we have

$$\frac{\partial \widetilde{C}}{\partial K_J} < 0, \text{ for any } K_J = 1, 2, ..., N_c. \tag{F.4}$$

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] B. Saltzberg, "Performance of an efficient parallel data transmission system," *IEEE Trans. Commun. Technol.*, vol. 15, no. 6, pp. 805–811, Dec. 1967.

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

[3] T. Hwang, C. Yang, G. Wu, S. Li, and G. Li, "OFDM and its wireless applications: A survey," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1673–1694, 2009.

[4] "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 10)," *3GPP TS 36.300 V10.4.0 (2011-06)*, 2011.

[5] "IEEE Standard for Local and metropolitan area networks-Part 16: Air Interface for Fixed Broadband Wireless Access Systems," *IEEE Std 802.16-2004*, 2004.

[6] W. Zou and Y. Wu, "COFDM: An overview," *IEEE Trans. Broadcast.*, vol. 41, no. 1, pp. 1–8, 1995.

[7] Q. Ling and T. Li, "Message-driven frequency hopping: Design and analysis," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1773 –1782, Apr. 2009.

[8] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. McGraw-Hill, 1994.

[9] D. Adamy, *Introduction to electronic warfare modeling and simulation*. Artech House Publishers, 2003.

[10] L. Zhang, "Spectrally efficient anti-jamming system design in wireless networks," Ph.D. dissertation, Michigan State University, 2011.

[11] J. Chiang and Y.-C. Hu, "Cross-layer jamming detection and mitigation in wireless broadcast networks," *IEEE/ACM Transactions on Networking*, vol. 19, no. 1, pp. 286–298, Feb 2011.

[12] R. Di Pietro and G. Oligeri, "Jamming mitigation in cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 10–15, May 2013.

[13] T. Ericson, "The noncooperative binary adder channel," *IEEE Trans. Inform. Theory*, vol. 32, no. 3, pp. 365–374, 1986.

[14] M. Medard, "Capacity of correlated jamming channels," in *Allerton Conference on Communications, Computing and Control*, 1997.

[15] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping-part i: System design," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 70 –79, Jan. 2013.

[16] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2148–2177, 1998.

[17] R. Alred, "Naval radar anti-jamming technique," *Journal of the Institution of Electrical Engineers - Part IIIA: Radiolocation*, vol. 93, no. 10, pp. 1593–1601, 1946.

[18] M. Amin, "Interference mitigation in spread spectrum communication systems using time-frequency distributions," *IEEE Trans. Signal Processing*, vol. 45, no. 1, pp. 90–101, Jan 1997.

[19] W. Sun and M. Amin, "A self-coherence anti-jamming GPS receiver," *IEEE Trans. Signal Processing*, vol. 53, no. 10, pp. 3910–3915, Oct 2005.

[20] I. Bergel, E. Fishler, and H. Messer, "Narrowband interference mitigation in impulse radio," *IEEE Trans. Commun.*, vol. 53, no. 8, pp. 1278–1282, Aug 2005.

[21] H. Sui and J. Zeidler, "A robust coded MIMO FH-CDMA transceiver for mobile ad hoc networks," *IEEE J. Select. Areas Commun.*, vol. 25, no. 7, pp. 1413–1423, September 2007.

[22] Y. Wu, B. Wang, K. Liu, and T. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *IEEE J. Select. Areas Commun.*, vol. 30, no. 1, pp. 4–15, January 2012.

[23] C. Popper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE J. Select. Areas Commun.*, vol. 28, no. 5, pp. 703–715, June 2010.

[24] Q. Wang, P. Xu, K. Ren, and X.-Y. Li, "Towards optimal adaptive UFH-based anti-jamming wireless communication," *IEEE J. Select. Areas Commun.*, vol. 30, no. 1, pp. 16–30, January 2012.

[25] C. Li, H. Dai, L. Xiao, and P. Ning, "Communication efficiency of anti-jamming broadcast in large-scale multi-channel wireless networks," *IEEE Trans. Signal Processing*, vol. 60, no. 10, pp. 5281–5292, Oct 2012.

[26] R. Dixon, *Spread Spectrum Systems with Commercial Applications*, 3rd ed. John Wiley & Son, Inc, 1994.

[27] L. Zhang and T. Li, "Anti-jamming message-driven frequency hopping-Part II: Capacity analysis under disguised jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 80 –88, Jan. 2013.

[28] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. 15, no. 1, pp. 122–127, Jan 1969.

[29] T. Li, Q. Ling, and J. Ren, "Physical layer built-in security analysis and enhancement algorithms for CDMA systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, no. 1, p. 083589, 2007.

[30] L. Dai, J. Wang, Z. Wang, P. Tsiaflakis, and M. Moonen, "Spectrum- and energy-efficient OFDM based on simultaneous multi-channel reconstruction," *IEEE Trans. Signal Processing*, vol. 61, no. 23, pp. 6047–6059, Dec 2013.

[31] J. Kim and Y. H. Lee, "Modified frequency-domain equalization for channel shortening in reduced-CP OFDMA systems," *IEEE Trans. Commun.*, vol. 55, no. 8, pp. 1645–1645, Aug 2007.

[32] S. Deng, X. Yi, M. Deng, Z. Luo, Q. Yang, M. Luo, and K. Qiu, "Reduced-guard-interval OFDM using digital sub-band-demultiplexing," *IEEE Photon. Technol. Lett.*, vol. 25, no. 22, pp. 2174–2177, Nov 2013.

[33] A. Gusmao, P. Torres, R. Dinis, and N. Esteves, "A reduced-CP approach to SC/FDE block transmission for broadband wireless communications," *IEEE Trans. Commun.*, vol. 55, no. 4, pp. 801–809, April 2007.

[34] B. Ahmadi, H. Asnani, O. Simeone, and H. Permuter, "Information embedding on actions," in *IEEE International Symposium on Information Theory Proceedings (ISIT2013)*, 2013, pp. 186–190.

[35] B. Larrousse and S. Lasaulce, "Coded power control: Performance analysis," in *IEEE International Symposium on Information Theory Proceedings (ISIT2013)*, 2013, pp. 3040–3044.

[36] R. Mesleh, H. Haas, C. W. Ahn, and S. Yun, "Spatial modulation - A new low complexity spectral efficiency enhancing technique," in *First International Conference on Communications and Networking in China, 2006. ChinaCom '06.*, Oct 2006, pp. 1–5.

[37] D. Wang, H. Zhao, and Z. Fan, "A new scheme for message-driven FH system," in *Proc. IEEE Intl. Conf. Future Inform. Tech., Manage. Eng.*, vol. 2, Oct. 2010, pp. 395–398.

[38] H. Wang, L. Zhang, T. Li, and J. Tugnait, "Spectrally efficient jamming mitigation based on code-controlled frequency hopping," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 728–732, Mar. 2011.

[39] G. Cooper and R. Nettleton, "A spread-spectrum technique for high-capacity mobile communications," *IEEE Trans. Veh. Technol.*, vol. 27, no. 4, pp. 264–275, Nov. 1978.

[40] C. Swenson, *Modern Cryptanalysis Techniques for Advanced Code Breaking*, 1st ed. Indianapolis: Wiley Publishing, 2008.

[41] L. Hao, T. Li, and Q. Ling, "A highly efficient secure communication interface: Collision-free frequency hopping (CFFH)," in *IEEE Workshop on Signal Processing Applications for Public Security and Forensics*, 2007, pp. 1–4.

[42] L. Dai, Z. Wang, and Z. Yang, "Next-generation digital television terrestrial broadcasting systems: Key technologies and research trends," *IEEE Communications Magazine*, vol. 50, no. 6, pp. 150–158, June 2012.

[43] M. Selvi and K. Murugesan, "Performance of OFDM based FSO communication systems using M-ary PSK modulation," *International Journal of Computer Applications*, vol. 49, no. 7, pp. 41–45, July 2012, published by Foundation of Computer Science, New York, USA.

[44] L. Lightfoot, L. Zhang, J. Ren, and T. Li, "Secure collision-free frequency hopping for OFDMA-based wireless networks," *EURASIP J. Advances in Signal Processing*, vol. 2009, no. 1, p. 361063, 2009.

[45] *Advanced Encryption Standard*, ser. FIPS-197, National Institute of Standards and Technology Std., Nov. 2001. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[46] W. Burr, "Selecting the advanced encryption standard," *IEEE Security Privacy*, vol. 1, no. 2, pp. 43–52, 2003.

[47] P. Cantrell and A. Ojha, "Comparison of generalized Q-function algorithms," *IEEE Trans. Inform. Theory*, vol. 33, no. 4, pp. 591–596, 1987.

[48] J. G. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2000.

[49] M. Luise and R. Reggiannini, "Carrier frequency acquisition and tracking for OFDM systems," *IEEE Trans. Commun.*, vol. 44, no. 11, pp. 1590–1598, Nov 1996.

[50] M. Morelli, C.-C. Kuo, and M.-O. Pun, "Synchronization techniques for orthogonal frequency division multiple access (OFDMA): A tutorial review," *Proceedings of the IEEE*, vol. 95, no. 7, pp. 1394–1427, 2007.

[51] M. Abdelhakim, J. Ren, and T. Li, "Reliable OFDM system design under hostile multi-tone jamming," in *2012 IEEE Global Communications Conference (GLOBECOM)*, Dec 2012, pp. 4290–4295.

[52] J. Luo, J. Andrian, and C. Zhou, "Bit error rate analysis of jamming for OFDM systems," in *2007 Wireless Telecommunications Symposium*, April 2007, pp. 1–8.

[53] R. Prasad and S. Hara, "An overview of multi-carrier CDMA," in *IEEE 4th International Symposium on Spread Spectrum Techniques and Applications Proceedings*, vol. 1, Sep 1996, pp. 107–114.

[54] S. Barbarossa and A. Scaglione, "Adaptive time-varying cancellation of wideband interferences in spread-spectrum communications based on time-frequency distributions," *IEEE Trans. Signal Processing*, vol. 47, no. 4, pp. 957–965, Apr 1999.

[55] S. Aromaa, P. Henttu, and M. Juntti, "Transform-selective interference suppression algorithm for spread-spectrum communications," *IEEE Signal Processing Lett.*, vol. 12, no. 1, pp. 49–51, Jan 2005.

[56] C.-L. Wang and K.-M. Wu, "A new narrowband interference suppression scheme for spread-spectrum CDMA communications," *IEEE Trans. Signal Processing*, vol. 49, no. 11, pp. 2832–2838, Nov 2001.

[57] H. Holma and A. Toskala, *WCDMA for UMTS: HSPA Evolution and LTE.* New York, NY, USA: John Wiley & Sons, Inc., 2007.

[58] E. Kaplan, *Understanding GPS - Principles and applications*, 2nd ed. Artech House, December 2005.

[59] M. Sahmoudi and M. Amin, "Fast iterative maximum-likelihood algorithm (FIMLA) for multipath mitigation in the next generation of GNSS receivers," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4362–4374, November 2008.

[60] Z. Xu and P. Liu, "Code-constrained blind detection of CDMA signals in multipath channels," *IEEE Signal Processing Lett.*, vol. 9, no. 12, pp. 389–392, Dec 2002.

[61] *Data Encryption Standard*, ser. FIPS-46-3, National Institute of Standards and Technology Std., Oct. 1999. [Online]. Available: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[62] T. Good and M. Benaissa, "AES as stream cipher on a small FPGA," in *Circuits and Systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE International Symposium on*, May 2006, pp. 4 pp.–.

[63] A. Hodjat, D. D. Hwang, B. Lai, K. Tiri, and I. Verbauwhede, "A 3.84 gbits/s AES crypto coprocessor with modes of operation in a 0.18-μm CMOS technology," in *Proceedings of the 15th ACM Great Lakes Symposium on VLSI*, ser. GLSVLSI '05. New York, NY, USA: ACM, 2005, pp. 60–63. [Online]. Available: http://doi.acm.org/10.1145/1057661.1057677

[64] S.-Y. Lin and C.-T. Huang, "A high-throughput low-power AES cipher for network applications," in *Design Automation Conference, 2007. ASP-DAC '07. Asia and South Pacific*, Jan 2007, pp. 595–600.

[65] N. Singhal and J.P.S.Raina, "Comparative analysis of AES and RC4 algorithms for better utilization," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 1, no. 3, pp. 259–263, Jul 2011.

[66] T. Ericson, "Exponential error bounds for random codes in the arbitrarily varying channel," *IEEE Trans. Inform. Theory*, vol. 31, no. 1, pp. 42–48, 1985.

[67] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacities of certain channel classes under random coding," *The Annals of Mathematical Statistics*, vol. 31, no. 3, pp. pp. 558–567, 1960.

[68] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Z. Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 44, no. 2, pp. 159–175, 1978.

[69] T. Basar and Y.-W. Wu, "Solutions to a class of minimax decision problems arising in communication systems," in *The 23rd IEEE Conference on Decision and Control*, Dec 1984, pp. 1182–1187.

[70] S. Farahmand, G. Giannakis, and X. Wang, "Max-min strategies for power-limited games in the presence of correlated jamming," in *41st Annual Conference on Information Sciences and Systems*, March 2007, pp. 300–305.

[71] T. Ericson, "The noncooperative binary adder channel," *IEEE Trans. Inform. Theory*, vol. 32, no. 3, pp. 365–374, 1986.

[72] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Trans. Inform. Theory*, vol. 29, no. 1, pp. 152–157, Jan 1983.

[73] S. Diggavi and T. Cover, "The worst additive noise under a covariance constraint," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 3072–3081, Nov 2001.

[74] W. Stark and R. McEliece, "On the capacity of channels with block memory," *IEEE Trans. Inform. Theory*, vol. 34, no. 2, pp. 322–324, Mar 1988.

[75] J. Borden, D. Mason, and R. McEliece, "Some information theoretic saddlepoints," *SIAM Journal on Control and Optimization*, vol. 23, no. 1, pp. 129–143, 1985.

[76] R. Mallik, R. Scholtz, and G. Papavassilopoulos, "Analysis of an on-off jamming situation as a dynamic game," *IEEE Trans. Commun.*, vol. 48, no. 8, pp. 1360–1373, Aug 2000.

[77] G. Scutari, D. Palomar, and S. Barbarossa, "Optimal linear precoding strategies for wideband noncooperative systems based on game theory-part i: Nash equilibria," *IEEE Trans. Signal Processing*, vol. 56, no. 3, pp. 1230–1249, March 2008.

[78] Z. Han, Z. Ji, and K. Liu, "Fair multiuser channel allocation for OFDMA networks using Nash bargaining solutions and coalitions," *IEEE Trans. Commun.*, vol. 53, no. 8, pp. 1366–1376, Aug 2005.

[79] A. Garnaev, Y. Hayel, and E. Altman, "A bayesian jamming game in an OFDM wireless network," in *10th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, May 2012, pp. 41–48.

[80] R. Gohary, Y. Huang, Z.-Q. Luo, and J.-S. Pang, "A generalized iterative water-filling algorithm for distributed power control in the presence of a jammer," *IEEE Trans. Signal Processing*, vol. 57, no. 7, pp. 2660–2674, July 2009.

[81] J. Neel, R. Buehrer, J. Reed, and R. P. Gilles, "Game theoretic analysis of a network of cognitive radios," in *45th Midwest Symposium on Circuits and Systems*, vol. 3, Aug 2002, pp. III–409–III–412 vol.3.

[82] Z. Ji and K. Liu, "Dynamic spectrum sharing: A game theoretical overview," *IEEE Commun. Mag.*, vol. 45, no. 5, pp. 88–94, May 2007.

[83] R. El-Bardan, S. Brahma, and P. Varshney, "A game theoretic power control framework for spectrum sharing in competitive environments," in *Asilomar Conference on Signals, Systems and Computers*, Nov 2013, pp. 1493–1497.

[84] V. Nadendla, H. Chen, and P. Varshney, "Minimax games for cooperative spectrum sensing in a centralized cognitive radio network in the presence of interferers," in *MILITARY COMMUNICATIONS CONFERENCE*, Nov 2011, pp. 1256–1260.

[85] R. Menon, A. MacKenzie, R. Buehrer, and J. Reed, "A game-theoretic framework for interference avoidance in ad hoc networks," in *IEEE Global Telecommunications Conference*, Nov 2006, pp. 1–6.

[86] P. D. Straffin, *Game Theory and Strategy*, 1st ed. Washinton, DC: The Mathematical Association of America, 1993.

[87] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[88] Q. Qi, A. Minturn, and Y. Yang, "An efficient water-filling algorithm for power allocation in OFDM-based cognitive radio systems," in *2012 International Conference on Systems and Informatics (ICSAI)*, May 2012, pp. 2069–2073.