PHYSICAL LAYER TECHNIQUES FOR WIRELESS COMMUNICATION SECURITY

By

YOUNGHO JO

A DISSERTATION PRESENTED TO THE GRADUATE SCHOOL
OF THE UNIVERSITY OF FLORIDA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA

2009

To my father, Sanghyun Jo, in heaven for his tears and love

ACKNOWLEDGMENTS

I would like to express my sincere appreciation to several people for their continuous support and guidance over the course of my degree. First, I would like to express my deepest gratitude to my advisor Professor Dapeng Oliver Wu for his excellent guidance and continual support during the course to my degree. Without his deep insight, advice, and willingness to provide support, this work would not have been possible. His extensive knowledge and commitment to the excellence of research and teaching are truly a treasure for me. He has always provided needed assistance at any time.

I also would like to thank Professor Liuqing Yang, Professor Tao Li, and Professor Shigang Chen for serving on my dissertation committee and providing valuable advice on my research. I am also grateful to Professor Clint Slatton for mentoring my research during my first year at the University of Florida.

My fellow graduate students have made my life at UF enjoyable and memorable. I would like to thank the students at the Multimedia Communications and Networking Laboratory (MCN) at the Electrical and Computer Department of the University of Florida, who have made my doctoral program experience all the more rewarding to me.

I want to take this opportunity to thank my colleagues and friends at the Department of Electrical and Computer Engineering and at the University of Florida. In particular, special thanks to Changhwan Ko and his wife Jungmin for their deepest friendship toward me and my family at Gainesville, Florida.

As always, I am deeply indebted to my lovely mother, my parents-in-law, and the rest of my family for their love and support throughout this degree program and my life. I would like to thank my wife Jeunghee for her love, understanding, and unwavering belief in me, and would like to express my great love to my sons Sungbin and Anthony. Finally, this dissertation is dedicated to my father, in heaven, for his tears and love.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Abstract of Dissertation Presented to the Graduate School
of the University of Florida in Partial Fulfillment of the
Requirements for the Degree of Doctor of Philosophy

PHYSICAL LAYER TECHNIQUES FOR WIRELESS COMMUNICATION SECURITY

By

Youngho Jo

December 2009

Chair: Dapeng Oliver Wu
Major: Electrical and Computer Engineering

In this dissertation, we consider physical layer techniques in wireless communication security. We study how to crack an adversary's communication which uses direct-sequence spread-spectrum (DS-SS), and how to protect wireless communication systems against interference. These security measures are classified as electronic protection (EP) and electronic attack (EA) among electronic warfare (EW), respectively. EW is the use of the electromagnetic spectrum to effectively deny the use of this medium by an adversary, while optimizing its use by friendly forces.

We investigate the performance of the physical layer of wireless communication systems considered in this dissertation. On the topic of eavesdropping on an adversary's secure communication, we discuss how to crack a DS-SS system. The DS-SS is a covert technique resistant to interference, interception and multipath fading. Identifying spread-spectrum signals or cracking DS-SS systems by an unintended receiver (or eavesdropper) without a priori knowledge is a challenging problem. To address this problem, we first search for the start position of data symbols in the spread signal (for symbol synchronization). After synchronization, we remove a spread sequence by a less-expensive and more accurate cross-correlation based method, and identify the spread sequence by using a matched filter. We also propose a zigzag searching method to identify a generator polynomial that reduces memory requirement and is capable of correcting

polarity errors existing in the previous methods. In addition, we analyze the bit error performance of our proposed method.

With regard to protecting wireless communication systems against interference, we propose an enhanced transform domain communication system (ETDCS) with narrow band interference (NBI) avoidance capability as a countermeasure for a single-carrier single-input single-output (SC-SISO) communication system, a vertical-Bell Laboratories layered space-time (V-BLAST) architecture with non-stationary interference avoidance capability as a countermeasure for a single-carrier multi-input multi-output (SC-MIMO), and a multi-carrier transform domain communication system (MC-TDCS) as a countermeasure for multi-carrier multi-input single-output (MC-MISO) systems, respectively.

The TDCS is a viable solution for interference avoidance. An interference avoiding fundamental modulation waveform is synthesized at the transmitter to avoid intentional interference, and the receiver adapts its matched filter to match the transmitted fundamental modulation waveform in the frequency domain. By doing so, spectrally interfered regions are avoided altogether via adaptive spectral notching.

The basic idea for the ETDCS is to synthesize an adaptive fundamental modulation waveform by a non-parametric spectral estimator, called Capon's method. The advantages of the ETDCS and a V-BLAST with the minimum mean square error (MMSE) detector are integrated to enhance bit error performance in narrow band interference (NBI) environment. The concepts of ETDCS and multi-carrier modulation are combined together in the MC-TDCS to combat multipath fading and to avoid intentional interference.

In code division multiple access (CDMA) or multi-carrier CDMA (MC-CDMA) systems, because users do not use completely orthogonal spreading codes or orthogonality of the spreading codes are destroyed by multipath fading, there is residual multiple-access interference (MAI) present at the output of a matched filter. Transmitter pre-filtering techniques can be employed to mitigate the MAI and channel distortions in the downlink of the MC-CDMA. We analyze the bit error rate performance of a downlink time division

duplex MC-CDMA with a pre-filtering transmitter antenna array at the base station (BS), rather than at the mobile terminals (MTs). We also incorporate a pre-filtering approach at the MC-TDCS to mitigate the MAI.

In summary, this research studies physical layer measures in wireless communication security. We provide countermeasures for SISO and MIMO communication systems against jamming and unintentional interference, while we also study vulnerabilities of DS-SS systems as well as how to crack the DS-SS system.

CHAPTER 1
INTRODUCTION

Wireless communications are very common both for military and commercial parties. The ability to use communication while mobile has great benefits to both parties. However, wireless communication has many security issues, since communication takes place over a wireless channel while the users are usually mobile.

Such a wireless channel suffers from a number of vulnerabilities: 1) The channel is vulnerable to eavesdropping. 2) The data can be altered. 3) The absence of a wired link makes it much easier to cheat on identities. 4) The channel can be overused. 5) Finally, the channel can be jammed, notably in order to a perpetrate a denial-of-service (DoS) attack [13].

Mobility also brings us several implications: 1) A device can jeopardize privacy. 2) Mobility means that a given device must be able to roam across wireless networks controlled by different operators. 3) Mobile devices have limited storage, computing power, and energy. 4) A mobile device can be easily stolen so that it can be misused or reverse engineered [13][1] .

Due to vulnerabilities by the characteristics of wireless communications, we have several requirements usually to be met by a secure system: 1) The most obvious requirement is authentication. 2) Access control is the ability of an organization to grant appropriate access to resources. 3) Confidentiality of the exchanged information is also an important requirement since the wireless channel can be vulnerable to eavesdropping. 4) The integrity of data must be appropriately protected. 5) Another requirement is privacy. 6) Non-repudiation is also an important requirement. 7) Finally, the network must provide

[1] In this dissertation, we do not consider the problem of mobility of wireless communications for the sake of simplicity.

a certain level of availability [13]. Next, we will describe our motivation for studying these problems.

1.1 Motivation

In this dissertation, we consider physical layer techniques in wireless communication security: We study both how to protect wireless communication systems against interference and how to attack (or crack) the adversary's communication systems, which uses direct-sequence spread-spectrum (DS-SS). These security measures belong to electronic protection (EP) and electronic attack (EA) among electronic warfare (EW), respectively. EW is the use of the electromagnetic spectrum to effectively deny the use of this medium by an adversary, while optimizing its use by friendly forces [14].

1.1.1 Crack Direct-Sequence Spread-Spectrum Systems

In DS-SS systems, the information signal is modulated by a pseudo-random (PN) sequence prior to transmission resulting in a wide-band signal resistant to narrow band jamming and multipath fading. The spreading sequence is typically known to the receiver, which uses a matched filtering operation and recovers the transmitted data [2, 15, 16]. The DS-SS signal has the characteristics of pseudo-randomness and correlation processing, which lead to many advantages such as anti-noise, anti-interference, and anti-multipath fading.

In the area of non-cooperative communication systems, an interceptor does not have a priori knowledge about the PN sequence. To eavesdrop on the adversary's communication which uses DS-SS, the estimation of the spread sequence from the intercepted signal is a key to cracking these DS-SS systems and is a challenging problem. The literature on this subject is not rich. [2]

To eavesdrop on the adversary's communication, one needs to (a) identify the start position of data symbols in the intercepted signal for the purpose of symbol

[2] Please refer to Section 3.2.

synchronization, (b) estimate data symbols, (c) estimate the PN sequence, and (d) estimate the code generator polynomial of the PN sequence. There is an erroneous reversal of polarity of each chip in the estimated PN sequence compared to the true PN sequence, which is a major source of the performance degradation of an eavesdropper. Therefore, we need to estimate a code generator polynomial to mitigate this polarity problem. In addition to this problem, saving hundreds or thousands of sequence bits in the memory of an eavesdropper is very expensive.

These observations motivate us to investigate the following problems:

1. Can we crack a DS-SS system without a priori knowledge about that system?
2. Can we correct polarity errors as well as reduce memory requirements of an eavesdropper?
3. If such a method is feasible, can we predict the performance of the eavesdropper without massive simulations?

We will address these questions in this dissertation.

1.1.2 Protect Wireless Communication Systems Against Interference

Both military and civilian parties desire reliable communication, and it is very important to be able to operate in the presence of both intentional and unintentional interference. The primary objective of an interferer (jammer) is to degrade or disrupt communication system performance to the point where it is no longer considered reliable. Therefore, an important goal of communication research is to mitigate or avoid intentional interference (jamming). We consider only narrow band interference (NBI) in this dissertation.

Intentional electromagnetic interference (IEME) can be categorized into four categories, based on the frequency content of their spectral densities as “narrow band”, “moderate band”, “ultra-moderate band”, and “hyperband” [1].

The DS-SS is a radio transmission technology that has resistance to intentional or unintentional interference [2, 16]. Therefore, spread-spectrum, in general, has been used

by the military. The DS-SS can also be used as a multiple access technique with different PN sequences. This multiple access technique is called direct-sequence code division multiple access (DS-CDMA) [17, 18]. The DS-SS does not avoid interfered regions, since the information-bearing signal is still transmitted at those regions.

However, a single-carrier transform domain communication system (SC-TDCS) can avoid altogether spectrally crowded regions via generation of an adaptive interference avoiding fundamental modulation waveform (FMW) at both the transmitter and receiver. The TDCS [9, 11] provides a viable solution for interference avoidance. Therefore, the foremost research problem in the SC-TDCS is accurate estimation of the spectral environment. The more accurate the estimation of the spectral content, the better the performance the TDCS will achieve.

For single-input single-output (SISO) communication systems, there were several approaches which incorporated the SC-TDCS with different methods of estimation of the spectral environment in the literature [9, 10, 19]. The SC-TDCS [9, 11] utilized a parametric 10th-order autoregressive (AR) method to estimate the power spectral density (PSD) of the spectral environment. However, the AR-estimator failed to provide accurate estimation under non-stationary interference. The wavelet domain communication system (WDCS) [10] and the enhanced WDCS (EWDCS) [19] utilized a concept of a wavelet periodogram and an evolutionary wavelet spectrum (EWS) for spectral estimation, respectively. The wavelet periodogram is not an accurate estimation of environmental power spectral density (PSD) and is not able to estimate a non-stationary interference, while the bit error rate (BER) performance of the EWDCS under a non-stationary interference was relatively sub-optimal compared to that under stationary interferences with respect to non-stationary interference. Therefore, we need to mitigate the problem of the TDCS [9, 11], WDCS [10], and EWDCS [19] for SC-TDCS systems.

Multiple-input and multiple-output (MIMO) systems that use multiple antennae at both the transmitter and receiver are a promising development in wireless communication

technology for a higher data rate, a higher spectral efficiency, better quality of service, and a high network capacity. The vertical-Bell Laboratories layered space-time (V-BLAST) is one such MIMO system for realizing very high data rates over the rich-scattering wireless channel [7, 20].

The fundamental concepts of transform domain processing (TDP) of the SC-TDCS and V-BLAST based on zero-forcing (ZF) detector was combined in the work of [12] to mitigate NBI. However, it failed to mitigate non-stationary interference, like swept-tone interference. The lack of stationarity of a non-stationary interference affected the performance of the spectral estimator, therefore the system proposed in [12] did not work well for non-stationary interferences. Moreover, the ZF detector can suffer from noise enhancement at early stages of the V-BLAST scheme. Therefore, we also need to provide non-stationary as well as stationary interference avoidance capability to the V-BLAST system for highly reliable communication.

A cost effective transmission technique that can use scarce spectral resources is in need for wireless services. Multi-carrier CDMA (MC-CDMA) has been developed as a candidate air-interface, especially for downlink, to provide high bit rates. However, the performance of MC-CDMA is essentially limited by multiple access interference (MAI), and low computational complexity and resource usages are desired at mobile terminals (MTs) [21–23].

To mitigate the MAI, the use of pre-filtering with MC-CDMA systems has also been considered recently. Pre-filtering approaches designed in frequency and space for downlink time division duplex MC-CDMA systems have been proposed in [22, 24–27]. However, not much work has been done to mitigate jamming for the MC-CDMA. The MC-CDMA has anti-jamming capability due to usage of spread sequence, but does not have interference avoidance capability like DS-CDMA.

As mentioned, the TDCS can provide the interference avoidance capability for a SC communication system [9, 11]. Research results aimed at characterizing SC-TDCS

performance in a multiple access environment (MAE) under additive white Gaussian noise (AWGN) channel was presented in [28] and that performance under multipath fading was studied in [29]. However, the mitigation of the MAI was not addressed in [28, 29].

Recently, the TDCS has been applied to cognitive radio (CR) technique [30], since it can utilize the spectrum efficiently by learning and adapting its system to the environmental condition. The development of CR technique has been raised by the fact that the spectrum is not always being used according to the spectral measurement result [31].

An orthogonal frequency division multiplexing (OFDM) based TDCS in CR for control message transmission was proposed in [29]. However, only the SISO antenna configuration was considered and performance under the intentional interference was not investigated. A performance comparison between the SC-TDCS and OFDM-based CR radio for a MIMO system using the V-BLAST receiver architecture to reconstruct the transmitted data in Rayleigh fading channel was presented in [32]. A modification of both the transmitter and the receiver block diagram according to [11] had been made in their systems. The CR with OFDM consistently outperforms the CR with TDCS architecture. Since the zero-forcing equalization at the receiver removed the frequency selectivity of the channel transfer function, there is no room for improvement with the aid of frequency domain diversity. Therefore, we need to enhance the BER performance of the TDCS under Rayleigh fading with the help of the frequency domain diversity combining techniques.

The aforementioned observations motivate us to investigate the following problems:

1. Can we enhance the performance of the SC-TDCS under both stationary and non-stationary interference?

2. If such a method is established, is it applicable to MIMO-TDCS, especially for the V-BLAST, in order to mitigate both stationary and non-stationary interference?

3. Can we enhance the performance of the TDCS under multipath fading with the help of the frequency domain diversity and transmitter diversity?

4. If such a system is possible, can we mitigate intentional interference as well as unintentional interference?

5. Can we predict the bit error performance of the system?

We will address these questions in this dissertation.

1.2 Contributions of this Dissertation

The contribution of this dissertation are the following:

The contributions made toward cracking DS-SS are: (i) a generator polynomial estimator which can identify a code generator polynomial and can correct polarity errors in the estimated PN sequence and estimated data symbols, (ii) a theoretical verification of the probability of error of a code generator estimator with respect to signal-to-noise ratio (SNR), the number of data symbols, and the length of the spread sequence of the intercepted signal, and (iii) the accuracy of performance prediction of an eavesdropper.

As contributions made toward protecting SISO communication systems against jamming, we propose the enhanced TDCS (ETDCS) which is a practical alternative for the SC-TDCS with a non-parametric spectral estimation method [33, 34]. We derive a mathematical model of the TDCS and analyze the BER performance of the TDCS. The proposed ETDCS with Capon's method (CM) can properly estimate the interference environment and offers significant interference avoidance capability for both the stationary and non-stationary interference. Moreover, the ETDCS shows the consistent bit error performance under both the stationary interference and the non-stationary interference.

We extend our previous approach in [34] to provide non-stationary as well as stationary interference avoidance capability to the V-BLAST system [35] as contributions protecting the MIMO communication system against jamming. The TDP by CM and minimum mean square error (MMSE) detector are combined with the V-BLAST to enhance bit error performance in the NBI environment.

To mitigate the multiple access interference (MAI) and intentional interference, we propose the multi-carrier TDCS (MC-TDCS) as an interference avoidance multi-carrier

system. The contributions of MC-TDCS approach are: (i) the performance improvement of TDCS under multipath fading with help of the frequency domain diversity, (ii) the mitigation of jamming and provision of the interference avoidance capability, (iii) the transmitter antennae array precoding (or pre-filtering) to mitigate the MAI interference, and (iv) analytical performance evaluation of the proposed MC-TDCS. Therefore, the proposed MC-TDCS will be a viable option for the TDCS over multipath fading with AWGN and the CR technique.

We also analyze the performance of joint space-frequency precoding approaches in terms of the average BER performance. Several linear power allocation strategies incorporated together with single user equalization schemes are compared to a joint precoding with an equal power constraint at the base-station and maximal ratio combining (MRC) at the mobile terminals (MTs). By conducting these studies, we can predict the performance of various space-frequency precoding schemes [22, 24–27, 36, 37] without massive simulations.

1.3 Outline of the Dissertation

The remainder of this dissertation is organized as follows:

In Chapter 2, we study the BER performance of the wireless communication systems considered in this dissertation. We describe interference model and study stationarity of intentional interference in Section 2.2. In Section 2.3, we study single-carrier modulation systems. OFDM and MC-CDMA are introduced as multi-carrier modulation (MCM) methods in Section 2.4. We study effects of jamming on MIMO in Section 2.5. Theoretical analysis to quantify the effects of interference on multi-carrier MIMO systems is conducted in Section 2.6. Finally, Section 2.7 summarizes this chapter.

In Chapter 3, we turn our attention to cracking DS-SS systems [38, 39]. Related works are discussed in Section 3.2. Section 3.3 describes the signal model. Section 3.4 introduces our method of identifying the start position of a data symbol in the spread signal. Section 3.5 presents how to remove data symbols from the intercepted signal.

Then, estimation of a spread sequence is presented in Section 3.6. Section 3.7 discusses how to identify a PN code generator polynomial and how to correct polarity errors. Section 3.8 presents simulation results to show the effectiveness and to validate the analytical probability of error of our approaches. Section 3.9 summarizes this chapter.

In Chapter 4, we proposes the ETDCS which is a practical alternative for the TDCS with a non-parametric spectral estimation method. In Section 4.2, we elaborate on a mathematical model of TDCS. In Section 4.3, an overview of the TDCS architecture is given, and the limitations of the TDCS and the proposed estimation method are investigated. Effects of various forms of jamming on the performance of ETDCS and comparative bit error performance analysis of the proposed ETDCS follow in Section 4.4. Finally, Section 4.5 summarizes this chapter.

In Chapter 5, we extend our previous approach in Chapter 4 to a multi-input multi-output (MIMO) communication system [35]. Section 5.2 presents our previous work. Section 5.3 describes a V-BLAST system model and the interference model. Section 5.4 introduces our proposed methodology. Section 5.5 presents simulation results to show the performance of our proposed approaches. Section 5.6 summarizes this chapter.

In Chapter 6, we analyze the BER performance of (joint) space-frequency precoding approaches. Section 6.2 elaborates on a system model of a DL TDD MC-TDCS. Then, various single-user equalization methods are discussed in Section 6.3. Section 6.4 describes how to mitigate the MAI with help of the transmitter diversity and the precoding at the transmitter. The performance analysis and verification by simulation are presented in Section 6.4.3 and Section 6.5, respectively. Finally, Section 6.6 summarizes this chapter.

In Chapter 7, we propose a multi-carrier transform domain communication system (MC-TDCS). Section 7.2 elaborates on a system model of the proposed MC-TDCS and describes a mathematical model of the proposed system. Then, single user equalizer performance for the single user detection is investigated in Section 7.3. Section 7.4 describes how to mitigate the MAI with the help of transmitter diversity and precoding

at the transmitter. The performance under NBI is validated in Section 7.5. Finally, Section 7.6 summarizes this chapter.

In Chapter 8, we summarize the dissertation and point out future research directions.

CHAPTER 2
PERFORMANCE OF WIRELESS COMMUNICATION SYSTEMS UNDER INTERFERENCE

2.1 Introduction

Wireless communication is, by any measure, the fastest growing segment of the communication industry. As such, it is very common both for commercial and military parties. However, the transmitted information-bearing signal is subject to various impairments caused by the transmission medium and vulnerable wireless channel combined with the mobility of transceiver. Therefore, special care must be taken to achieve security requirements of the wireless communication systems [13, 17][1] .

The purpose of this chapter is to investigate the performance of various wireless communication systems at physical layer under interference, since interference can disrupt communications by decreasing the signal-to-noise ratio (SNR). Therefore, we need to investigate the performance of wireless communication systems under interference to predict that performance or to mitigate interference for reliable communication.

The physical layer under study includes single-carrier systems, multi-carrier modulation system, single-input single-output (SISO) systems, multi-input multi-output (MIMO) systems, and so on. The performance measure of interest is the bit error rate (BER) in this chapter.

The remainder of this chapter is organized as follows. We describe interference model and study stationarity of intentional interference in Section 2.2. In Section 2.3, we study single-carrier modulation systems. Orthogonal frequency division multiplexing (OFDM) and multi-carrier code division multiple access (MC-CDMA) are introduced as multi-carrier modulation (MCM) methods in Section 2.4. We study effects of jamming on multiple-input multiple-output (MIMO) in Section 2.5. Theoretical analysis to quantify

[1] Please refer to Chapter 1.

the effects of interference on multi-carrier MIMO systems is conducted in Section 2.6. Finally, Section 2.7 summarizes this chapter.

2.2 Interference Model

Interference is the intentional or unintentional emission of signals to interfere with the operation of the communication system with noise or false information. Therefore, interference can disrupt reliable communication, and can decrease SNR ratio. We will investigate intentional interference (or jamming)[2] and unintentional interference in this section.

2.2.1 Intentional Interference

Intentional electromagnetic interference (IEME) can be categorized into four categories, based on the frequency content of their spectral densities, as "narrow band", "moderate band", "ultra-moderate band", and "hyperband" [1]. The definitions for bandwidth classification proposed in [1] is shown in Table 2-1 for reference.

Table 2-1. IMEM classification based on bandwidth in [1]

Band type	**Percentage bandwidth** $pbw = 200\frac{br-1}{br+1}$	**Bandratio** br
Narrow or hypoband	$< 1\%$	< 1.01
Moderate or mesoband	$1\% < pbw \leq 100\%$	$1.01 < br \leq 3$
Ultra-moderate or sub-hyperband	$100\% < pbw < 163.4\%$	$3 < br \leq 10$
Hyperband	$163.4\% < pbw < 200\%$	$br \geq 10$

We consider only narrow band interference (NBI) in this dissertation. The NBI further can be categorized into stationary or non-stationary interference with respect to

[2] We will use intentional interference and jamming interchangeably in this dissertation.

its time-varying characteristic in the frequency domain. Partial band, single-tone, and multi-tone jamming are stationary interferences and swept-tone jamming is non-stationary interference in terms of wide-sense stationarity.

2.2.1.1 Barrage noise jamming

Barrage noise jamming (BNJ) belongs to a broadband noise jamming form. In this case, the jammer interferes with the whole bandwidth by injecting a band-limited noise to the system. Its effect is the same as that of the additive white Gaussian noise (AWGN), so the power spectral density (PSD) of total noise becomes:

$$\mathrm{PSD}_N = N_0 + N_J \tag{2–1}$$

where N_0 is the noise PSD of complex AWGN and N_J is the PSD of complex BNJ.

2.2.1.2 Partial band jamming

Partial band jamming (PBJ) or partial band overlap is modeled as additive Gaussian noise with its power focusing on a portion of the entire bandwidth of the system. Since white noise is stationary, the PBJ is also stationary jamming. This strategy is considered more effective than BNJ since the jammer can concentrate more power to interfere with certain specific bandwidths.

2.2.1.3 Multi-tone jamming

Multi-tone jamming (MTJ) divides its total power into q distinct, equal power, random phase tones. Every jamming tone can be modeled as:

$$J(t) = A_J e^{j(2\pi f_J t + \varphi_J)} \tag{2–2}$$

where φ_J is the random phase, which is uniformly distributed over $[0, 2\pi]$. A_J and f_J are the amplitude and frequency, respectively. Single-tone jamming (STJ) is a special case of multi-tone jamming with $q = 1$.

The MTJ is a wide-sense stationary jamming. For $q = 1$, the mean of $J(t)$ is

$$\mathbf{E}[J(t)] = \int_0^{2\pi} A_J e^{j(2\pi f_J t + \phi_J)} \frac{1}{2\pi} d\phi_J = 0 \tag{2–3}$$

where $\mathbf{E}[\cdot]$ denotes expectation and autocorrelation of $J(t)$ becomes

$$\begin{aligned} \mathbf{E}[J^*(t)J(t+\tau)] &= A_J^2 e^{j2\pi f_J \cdot \tau} \\ &= R(\tau) \end{aligned} \tag{2–4}$$

where $(\cdot)^*$ denotes complex conjugation.

2.2.1.4 Swept-tone jamming

Swept-tone jamming (SWTJ) or sweep jamming can be achieved by two methods: (i) a narrow frequency band of jamming energy is repeatedly swept over a relatively wide frequency band, and (ii) the sweep rate is such as to be on any given frequency only long enough to accomplish its jamming task, returning to that frequency again before the expiration of the jammed circuit recovery time.

Note that SWTJ combines the advantages of both spot jamming and BNJ by rapid electronic sweeping of a narrow band of jamming signals over a broad frequency spectrum; the disadvantage of SWTJ is its high susceptibility to electronic counter-countermeasures. While this has the advantage of being able to jam multiple frequencies in quick succession, it does not affect them all at the same time, and thus limits the effectiveness of this type of jamming. Although, depending on the error checking in the device(s), this can render a wide range of devices effectively useless. Every swept-tone can be modeled as

$$\begin{aligned} J(t) &= A_J e^{j(2\pi f_J \cdot t + \phi_J)} \\ &= A_J e^{j(2\pi (f_L + \Delta t) \cdot t + \phi_J)} \end{aligned} \tag{2–5}$$

with $f_J = f_L + \Delta t$ where ϕ_J is random phase which is uniformly distributed over $[0, 2\pi]$. A_J and f_J are amplitude and frequency, respectively. f_L is lows of sweeps and t is sweep time and Δ is sweep interval.

Now we need to investigate the stationarity of the SWTJ. The mean of $J(t)$ is:

$$\begin{aligned}\mathbf{E}[J(t)] &= \mathbf{E}[A_J e^{j(2\pi f_J \cdot t + \phi_J)}] \\ &= \mathbf{E}[A_J e^{j(2\pi (f_L + \Delta t)\cdot t + \phi_J)}] = 0\end{aligned} \tag{2–6}$$

The autocorrelation of $J(t)$ becomes

$$\begin{aligned}\mathbf{E}[J^*(t)J(t+\tau)] &= \mathbf{E}\left[A_J e^{-j[2\pi(f_L+\Delta t)t+\phi_J]} A_J e^{j[2\pi(f_L+\Delta t+\Delta\tau)(t+\tau)+\phi_J]}\right] \\ &= A_J^2 e^{j2\pi(f_L\tau+\Delta\tau\cdot\tau)} e^{j2\pi[\Delta t\cdot\tau+\Delta\tau\cdot t]} = R(t;\tau)\end{aligned} \tag{2–7}$$

Therefore, the SWTJ is not a wide-sense stationary (WSS) jamming. However, the SWTJ is a cyclostationary process. Since

$$\begin{aligned}R(t+T_0;\tau) &= A_J^2 e^{j2\pi(f_L\tau+\Delta\tau\cdot\tau)} e^{j2\pi(\Delta(t+T_0)\cdot\tau+\Delta\tau\cdot(t+T_0))} \\ &= R(t;\tau)\end{aligned} \tag{2–8}$$

2.2.2 Unintentional Interference

2.2.2.1 Multiple access interference

In code division multiple access (CDMA) or multi-carrier CDMA (MC-CDMA) systems, because users do not use completely orthogonal spreading codes or orthogonality of the spreading codes are destroyed by multipath fading, there is residual multiple access interference (MAI) present at the output of a matched filter. We discuss the performance under MAI of the DS-CDMA and the MC-CDMA in Section 2.3.2 and Section 2.4.2, respectively.

2.2.2.2 Co-channel interference

Co-channel interference or CCI[3] is crosstalk from two different radio transmitters reusing the same frequency channel. CCI is introduced when a frequency band is shared by multiple users at the same time. In cellular systems, CCI arises by the frequency

[3] We do not study both CCI and ACI in this dissertation.

reuse in neighboring cells. As frequency reuse factor decreases to increase the system capacity, CCI increases as the distance between the co-channel cells decreases. Therefore, the performance of a frequency reuse system is limited by CCI rather than by additive noise [40].

2.2.2.3 Adjacent-channel interference

Adjacent-channel interference or ACI is interference caused by extraneous power from a signal in an adjacent channel. Note that adjacent channel interference may be caused by inadequate filtering, such as incomplete filtering of unwanted modulation products in frequency modulation (FM) systems, improper tuning, or poor frequency control, in either the reference channel or the interfering channel, or both.

2.3 Single-Carrier Modulation Systems

In this section, we describe single-carrier modulation systems under study in this dissertation. Section 2.3.1 introduces direct-sequence spread-spectrum (DS-SS) and linear feedback shift register (LFSR), and discusses vulnerabilities of that DS-SS system in terms of non-cooperative communication. Section 2.3.2 deals with the MAI of code division multiple access (CDMA). In Section 2.3.3, a transform domain communication system (TDCS) is introduced as an interference avoidance system.

2.3.1 Direct-Sequence Spread-Spectrum Systems

Spread-spectrum systems have been developed since about the mid-1950s. The initial applications have been to military anti-jamming tactical communication, to guidance systems, to experimental anti-multipath systems and other applications [2].

In DS-SS systems, the information signal is modulated by a PN sequence prior to transmission resulting in a wide band signal resistant to narrow band jamming and multipath. The DS-SS transmitters use a periodical pseudo-random sequence to modulate the baseband signal before transmission. The PN spreading sequence is typically known to the receiver, which uses the matched filtering operation and recovers the transmitted data [15, 16]. The DS-SS signal has the characteristics of pseudo-randomness and correlation

processing, which leads to many advantages such as anti-noise, anti-interference, and anti-multipath fading [2, 16].

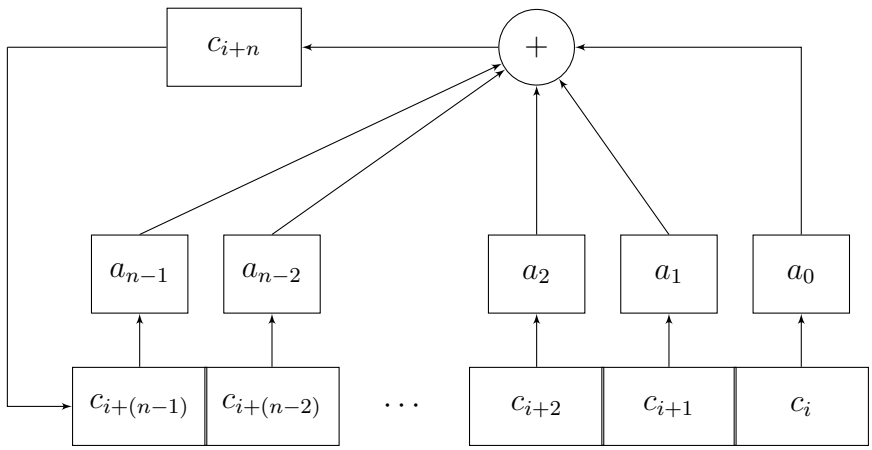


Figure 2-1. Linear feedback shift register [2–5]

Practical and efficient implementation techniques for PN sequences center on shift-register. Since crackability is such an important issue, it appears sensible to categorize PN code generator, according to increasing complexity, in the classes of (a) linear feedback shift register (LFSR); (b) one or more LFSRs with nonlinear feed forward logic (NFFL); and (c) general nonlinear feedback shift-register (NLFSR). Other ad hoc cases are possible.

Figure 2-1 shows a diagram of the LFSR. LFSRs can generate linear maximal sequences, m-sequences, or PN sequence, using selected stages of an n-stage shift register. The correct selection of the tap-weights (or feedback stages) will result in a maximal sequence length $N = 2^n - 1$. The classical properties of an m-sequence are [4, 5, 15]: (1) maximal-length for an n-stage generator; (2) maximum possible peak/side-lobe autocorrelation over the period N; and (3) a large number of maximum codes per n-stages.

However, non-cooperative communication systems, such as spectrums surveillance and electronic interception, are entirely different from cooperative communication systems. The receiver has minimal knowledge of the intercepted signal. In this case only blind

signal estimation procedures can be used. In the context of spectrum surveillance, the PN sequence used by the transmitter is unknown, so all related issues of synchronization, multipath equalization, data detection, and PN sequence detection become more challenging problems [41]. Capturing information from the intercepted signal is still an important and difficult problem to be solved in the non-cooperative communication system [38, 39, 42]. In Chapter 3, we discuss how to crack a DS-SS system. We consider the LFSR as the implementation technique for PN sequences in Chapter 3.

2.3.2 Code Division Multiple Access

As mentioned in Section 2.2, the downlink (DL) multiuser CDMA suffers from the MAI. Therefore, the performance of the CDMA is predetermined by the MAI. A transmitter precoding, as an alternative for combating the MAI in synchronous multiuser channel, was proposed in [43, 44]. The transmitter precoding reduces the multiuser detection problem into decoupled single user detection problem.

Asymptotic BER of a precoded random spreading system in [44] is

$$P_e = Q\left(\sqrt{2\frac{E_b}{N_0}(1-\beta)}\right) \tag{2–9}$$

where $Q(x) = 1/\sqrt{2\pi}\int_0^\infty e^{-x^2/2}dx$ and β is

$$\beta = \lim_{K,n\to\infty}\frac{K}{n} \tag{2–10}$$

where K is the number of users, and $K \leq n$ (n is the number of chips/bit). Moreover, the performance of the precoding and the receiver-based decorrelator with equal or unequal power distribution is asymptotically equivalent.

A reproduction of the asymptotic theoretical performance of the precoding and that of receiver-based decorrelator is shown in Figure 2-2 for β=0.2, 0.5, and 0.8 and n=100. The result shows that their performance are quite similar as expected. Interested readers should refer to [44] and references therein.

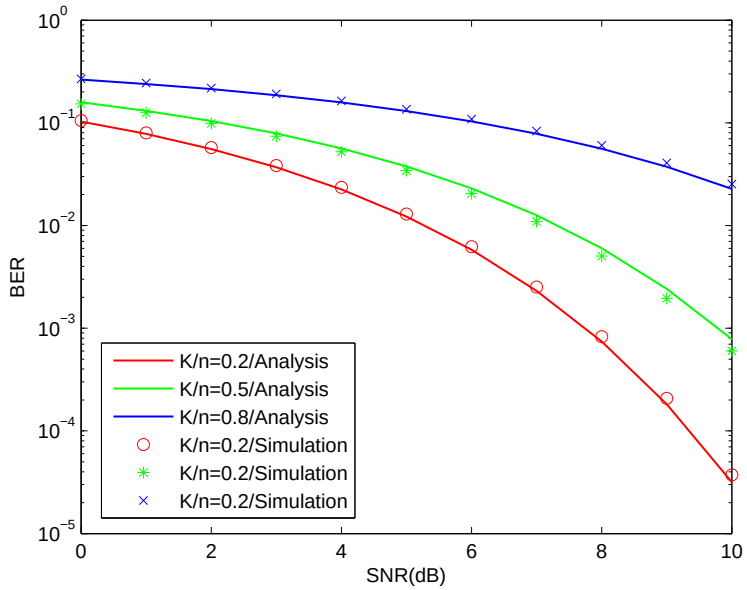


Figure 2-2. Performance of the precoding and the receiver-based decorrelator for β=0.2, 0.5, 0.8, and n=100

2.3.3 Transform Domain Communication Systems

TDCS in [9, 11] is a viable option for avoiding the interference considered in the previous Section 2.2.1. In TDCS, the transmitter generates an interference-free waveform to avoid the intentional interference, while the receiver needs to adapt its matched filter to match the transmitted waveform. Adaptive spectral notching avoids the spectrally crowded regions (or the jammed regions).

In Chapter 4, we propose an enhanced TDCS (ETDCS) which is a practical alternative for the TDCS in [9, 11] with a non-parametric spectral estimation method. In Chapter 5, we extend our approach in Chapter 4 to provide non-stationary as well as stationary interference avoidance capability to a vertical-Bell Laboratories layered space-time (V-BLAST) system. In Chapter 7, we propose a multi-carrier TDCS (MC-TDCS). The concept of transform domain processing (TDP) and multi-carrier modulation (MCM) are combined together in MC-TDCS to avoid intentional interference and to combat multipath fading. We will also study the performance under multiuser and

incorporate a precoding scheme at the transmitter antenna array to mitigate the MAI at the transmitter.

2.4 Multi-Carrier Modulation Systems

Multi-carrier modulation (MCM) is the principle of transmitting data by dividing the stream into several bit streams, each of which has a much lower bit rate, and by using these sub-streams to modulate several carriers. The OFDM in Section 2.4.1 is robust against inter-symbol interference (ISI) and fading caused by multipath fading, and is also robust against narrow band ICI. We study the MAI problem of MC-CDMA in Section 2.4.2.

2.4.1 Orthogonal Frequency Division Multiplexing

OFDM is a frequency-division multiplexing (FDM) scheme utilized as a digital multi-carrier modulation method. OFDM is a promising technology that enables transmission of a high data rate. The basic idea of OFDM is to use a large number of parallel narrow band sub-carriers instead of a single wide-band carrier to transport information. With its capability of adapting to severe channel conditions without complex equalization, OFDM can effectively provide broadband wireless communication in hostile multipath environments. Furthermore, OFDM is robust against ISI and fading caused by multipath propagation [23].

Since OFDM is a very important candidate for the core technique of next generation wireless communication systems, it is necessary to evaluate its performance under intentional interference over fading channels. In [45], a comprehensive study of the effect of different jamming techniques for an OFDM system was conducted. By comparing the bit error rate (BER) performance of different jamming techniques, the most effective jamming technique can be identified under various channel conditions. This is very critical for both jamming and anti-jamming applications for OFDM systems. BNJ, PBJ, and MTJ in a time-correlated Rayleigh fading channel with AWGN were evaluated in [45]. Interested

readers should refer to [45] to understand the effects of various types of jamming for OFDM systems.

2.4.2 Multi-Carrier Code Division Multiple Access

Aforementioned direct-sequence CDMA (DS-CDMA) in Section 2.3.2, where spreading is performed in the time domain, has high sampling rates. This high sampling rate makes DS-CDMA very susceptible to performance degradation caused by multipath propagation [23]. Therefore, MC-CDMA was developed to overcome this drawback of the DS-CDMA [21]. The main benefit of MC-CDMA in comparison to other OFDM-based multiple access methods in Section 2.4.1 is the inherent provision of frequency diversity. By contrast, a drawback of MC-CDMA, like DS-CDMA, is the MAI encountered. These factors predetermined the performance of MC-CDMA [23].

Because the loss of the orthogonality among users in multipath environments causes the MAI, we need to mitigate the MAI. While in DL transmissions (i.e., from the base station (BS) to the mobile terminals (MTs)), the single user detection (SUD) techniques are typically employed, guaranteeing reasonable trade-off between performance and system complexity, in uplink (i.e., from the MTs to the BS), multiuser detection (MUD) techniques seem to be mandatory [23].

The idea behind pre-equalization[4] [22, 25, 26, 46–48] is to vary the gain assigned to each sub-carrier so that the interference is reduced and a low complex detection scheme can be employed at the receiver. In order to work properly, the pre-equalization techniques require channel state information (CSI) at the transmitter. In Chapter 6, we analyze the bit error performance of various space-frequency precoding schemes of a DL MC-CDMA.

[4] We will use pre-equalization, pre-filtering, and precoding interchangeably in this dissertation.

2.5 Multi-Input Multi-Output Systems

MIMO systems that use multiple antennae at both the transmitter and receiver are a promising wireless communication technology for higher data rate, higher spectral efficiency, better quality of service, and high network capacity. Note that there are two types of MIMO systems: Bell Laboratories layered architecture space-time (BLAST) and space-time coding (STC). BLAST is intended to improve throughput while space-time coding is intended to improve reliability. We conduct theoretical analysis to qualify the effect of jamming on a STC in Section 2.5.1 and a vertical-BLAST (V-BLAST) in Section 2.5.2, respectively.

2.5.1 Space-Time Orthogonal Block Coding

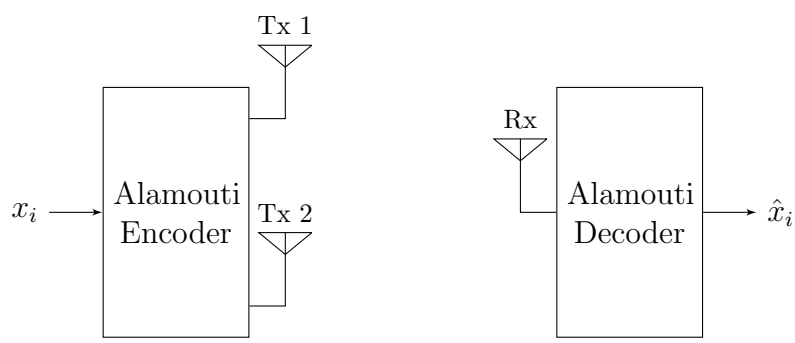


Figure 2-3. A schematic of Alamouti transmission strategy [6]

A very simple and effective scheme for two transmit antennae and a single receiver antenna achieving diversity order two was introduced by Alamouti in [49]. A transceiver architecture is shown in Figure 2-3.

It sends the sequence $\{x_1, -x_2^*\}$ on the first antenna and $\{x_2, x_1^*\}$ on the other.

$$\begin{aligned} y_1 &= h_1 x_1 + h_2 x_2 + n_1 = \begin{bmatrix} h_1 & h_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + n_1 \\ y_2 &= -h_1 x_2^* + h_2 x_1^* + n_2 = \begin{bmatrix} h_1 & h_2 \end{bmatrix} \begin{bmatrix} -x_2^* \\ x_1^* \end{bmatrix} + n_2 \end{aligned} \tag{2–11}$$

Assuming a flat-fading channel with coefficients h_1 and h_2, the received vector is formed by stacking two consecutive data samples y_1 and y_2^*. This can be formulated as follows:

$$\begin{bmatrix} y_1 \\ y_2^* \end{bmatrix} = \begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2^* \end{bmatrix} \tag{2–12}$$

or in short notation $\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}$. The resulting channel $\mathbf{H}$ is orthogonal, i.e., $\mathbf{H}^H\mathbf{H} = \mathbf{H}\mathbf{H}^H = h^2\mathbf{I}_2$ and the gain of the channel $h^2 = |h_1|^2 + |h_2|^2$, since the channel becomes:

$$\mathbf{H} = \begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix} \tag{2–13}$$

and

$$\begin{aligned} \mathbf{H}^H\mathbf{H} &= \begin{bmatrix} h_1^* & h_2 \\ h_2^* & -h_1 \end{bmatrix} \begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix} \\ &= \begin{bmatrix} |h_1|^2 + |h_2|^2 & 0 \\ 0 & |h_1|^2 + |h_2|^2 \end{bmatrix} = h^2\mathbf{I}_2 \end{aligned} \tag{2–14}$$

The transmitted symbols can be computed by the zero-forcing (ZF) approach:

$$\begin{aligned} \begin{bmatrix} \hat{x}_1 \\ \hat{x}_2^* \end{bmatrix} &= \frac{1}{h^2}\mathbf{H}^H \begin{bmatrix} y_1 \\ y_2^* \end{bmatrix} = \frac{1}{h^2} \begin{bmatrix} h_1^* & h_2 \\ h_2^* & -h_1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2^* \end{bmatrix} = \frac{1}{h^2} \begin{bmatrix} h_1^* y_1 + h_2 y_2^* \\ h_2^* y_1 - h_1 y_2^* \end{bmatrix} \\ &= \begin{bmatrix} x_1 \\ x_2^* \end{bmatrix} + (\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H \begin{bmatrix} n_1 \\ n_2^* \end{bmatrix} \end{aligned} \tag{2–15}$$

The relevant noise variance is given by $\sigma_n^2 \mathrm{tr}\left(\mathbf{H}^H\mathbf{H}\right)^{-1} = \sigma_n^2/h^2$. The denominator h^2 indicates diversity order two for the reception of both symbols. The BER performance of BPSK modulation is given by:

$$\bar{P}_b = \int_0^\infty Q\left(\sqrt{\frac{E_b}{N_0}}\right) \frac{\alpha}{\sigma^2} \exp\left(-\frac{\alpha^2}{2\sigma^2}\right) d\alpha \tag{2–16}$$

$$\bar{P}_{b,STBC} = \bar{P}_b^2 \left[1 + 2(1 - \bar{P}_b)\right] \tag{2–17}$$

if we use the equal power allocation for two transmit antennae.

2.5.2 Vertical-Bell Laboratories Layered Space-Time

MIMO wireless communication system has been shown to provide high capacity in a rich scattering environment. The V-BLAST architecture is one such MIMO system, which is attractive from the implementation standpoint. It has been shown that the theoretical capacity approximately increases linearly with the minimum number of transmit and receive antennae, when operated in a channel with AWGN. At each symbol it detects the strongest layer of the transmitted signal, cancels the effects of this strongest layer from each of the received signals, then continues to detect the strongest of the remaining layers, and so on [7, 20].

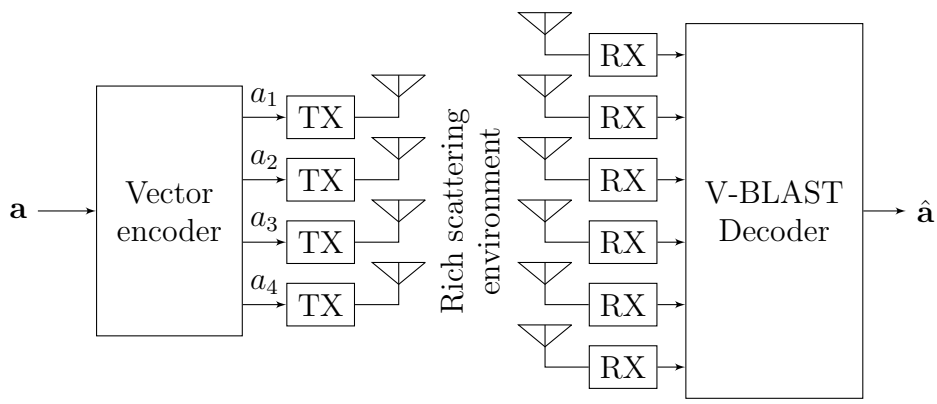


Figure 2-4. A high level system diagram of V-BLAST [7]

A high-level system diagram of a BLAST is shown in Figure 2-4 in [7]. The received signal vector becomes:

$$\mathbf{r} = \mathbf{H}\mathbf{a} + \mathbf{n} \tag{2–18}$$

where $\mathbf{r} = [r_1, \cdots, r_N]^T$ and $\mathbf{a} = [a_1, \cdots, a_M]^T$ are the received signal vector and transmitted signal vector, respectively. The channel matrix $\mathbf{H}$ is

$$\mathbf{H} = \begin{bmatrix} H_{1,1} & \cdots & H_{1,M} \\ \vdots & \ddots & \vdots \\ H_{N,1} & \vdots & H_{N,M} \end{bmatrix} \tag{2–19}$$

where $H_{n,m}$ is the channel link between transmit antenna m and receiver antenna n, N is the number of receive antennae, and M is the number of transmit antennae.

We assume that the receiver has the CSI. A full zero-forcing sequential interference cancelation (ZF-SIC) algorithm is described in Table 2-2 [20].

Table 2-2. A ZF-SIC V-BLAST detection algorithm

Initialization:			
	i	$\leftarrow$	1
	$\mathbf{G}_1$	$=$	$\mathbf{H}^+$
	k_1	$=$	$\underset{j}{\operatorname{argmin}} \left\|(\mathbf{G}_1)_j\right\|^2$
Recursion:			
	$\mathbf{w}_{k_i}$	$=$	$(\mathbf{G}_i)_{k_i}$
	y_{k_i}	$=$	$\mathbf{w}_{k_i}^T \mathbf{r}_i$
	$\hat{a}_{k_i}$	$=$	$Q(y_{k_i})$
	$\mathbf{r}_{i+1}$	$=$	$\mathbf{r}_i - \hat{a}_{k_i}(\mathbf{H})_{k_i}$
	$\mathbf{G}_{i+1}$	$=$	$\mathbf{H}^+_{\bar{k}_i}$
	k_{i+1}	$=$	$\underset{j \notin (k_1, \cdots, k_i)}{\operatorname{argmin}} \left\|(\mathbf{G}_{i+1})_j\right\|^2$
	i	$\leftarrow$	$i+1$

It is desirable to utilize the V-BLAST in the reliable wireless communication system under intentional interference, mentioned in Section 2.2.1. In Chapter 5, a TDP in Section 2.3.3 and minimum mean square error (MMSE) detector in [50] are combined with the V-BLAST to enhance performance in the NBI environment [35].

2.6 Multi-Carrier Multi-Input Multi-Output Systems

Combining MCM methods in Section 2.4 and MIMO in Section 2.5 will achieve unprecedented performance. Multi-carrier MIMO (MC-MIMO) systems are robust against frequency selective fading due to frequency diversity from OFDM, frequency flat fading owing to space diversity from MIMO, and high throughput due to MIMO. We conduct theoretical analysis to quantify the effects of interference on both a space-time OFDM (ST-OFDM) system and a multi-carrier V-BLAST (MC V-BLAST) system in Section 2.6.2 and Section 2.6.4, respectively.

2.6.1 Space-Time Orthogonal Frequency Division Multiplexing

Consider the successive data symbol vectors at the output of the serial to parallel converter one pair at a time. Denote the first vector in the pair as the odd vector, $\mathbf{X}_o$, and the second one the even vector, $\mathbf{X}_e$. For example, if $\mathbf{X}_o$ is the Mth block data vector and $\mathbf{X}_e$ is the $(M+1)^{th}$ block vector.

$$\begin{aligned} \mathbf{X}_o &= \begin{bmatrix} X(MN) & \cdots & X(MN+N-1) \end{bmatrix}^T \\ \mathbf{X}_e &= \begin{bmatrix} X(MN+N) & \cdots & X(MN+2N-1) \end{bmatrix}^T \end{aligned} \tag{2–20}$$

At the first transmitter, $\mathbf{X}_o$, is transmitted during the first time slot followed by $-\mathbf{X}_e^*$ in the second time slot. At the second transmitter, $\mathbf{X}_e$, is transmitted first followed by $\mathbf{X}_o^*$. The equivalent space-time block code transmission matrix is given by:

$$\mathcal{G} = \begin{bmatrix} \mathbf{X}_o & \mathbf{X}_e \\ -\mathbf{X}_e^* & \mathbf{X}_o^* \end{bmatrix} \tag{2–21}$$

i.e., entries of the transmission matrix are the OFDM symbol vectors $\mathbf{X}_o$, $\mathbf{X}_e$, and their conjugates.

Let $\mathbf{\Lambda}_1$ and $\mathbf{\Lambda_2}$ be two diagonal matrices whose diagonal elements are the DFTs of the respective channel impulse responses, $\mathbf{h}_1$ and $\mathbf{h}_2$. Assuming that the channel responses are constant during the two time slots, the demodulated vectors in the corresponding time slots are given by

$$\begin{aligned} \mathbf{Y}_1 &= \mathbf{\Lambda}_1\mathbf{X}_o + \mathbf{\Lambda}_2\mathbf{X}_e + \mathbf{Z}_1 \\ \mathbf{Y}_2 &= -\mathbf{\Lambda}_1\mathbf{X}_e^* + \mathbf{\Lambda}_2\mathbf{X}_o^* + \mathbf{Z}_2 \end{aligned} \tag{2–22}$$

Assuming the channel responses are known or can be estimated accurately at the receiver, the decision variables are constructed by combining $\mathbf{Y}_1$, $\mathbf{Y}_2$, and the channel response

matrices as

$$\hat{\mathbf{X}}_0 = \mathbf{\Lambda}_1^* \mathbf{Y}_1 + \mathbf{\Lambda}_2 \mathbf{Y}_2^*$$
$$\hat{\mathbf{X}}_e = \mathbf{\Lambda}_2^* \mathbf{Y}_1 - \mathbf{\Lambda}_1 \mathbf{Y}_2^* \tag{2–23}$$

Substituting (2–22) into (2–23) yields the following expressions:

$$\hat{\mathbf{X}}_0 = \left(|\mathbf{\Lambda}_1|^2 + |\mathbf{\Lambda}_2|^2\right) \mathbf{X}_0 + \mathbf{\Lambda}_1^* \mathbf{Z}_1 + \mathbf{\Lambda}_2 \mathbf{Z}_2^*$$
$$\hat{\mathbf{X}}_0 = \left(|\mathbf{\Lambda}_1|^2 + |\mathbf{\Lambda}_2|^2\right) \mathbf{X}_e + \mathbf{\Lambda}_2^* \mathbf{Z}_1 - \mathbf{\Lambda}_1 \mathbf{Z}_2^* \tag{2–24}$$

It is known that the MRC is the optimal linear combining technique for receiver diversity. The above decision equations for the transmitter diversity scheme are similar in form to that of a two-branch MRC receiver diversity system. The block diagram of space-time OFDM transmitter diversity system in [8] is shown in Figure 2-5. The BER performance of the space-time OFDM without jamming is given by (2–16) and (2–17).

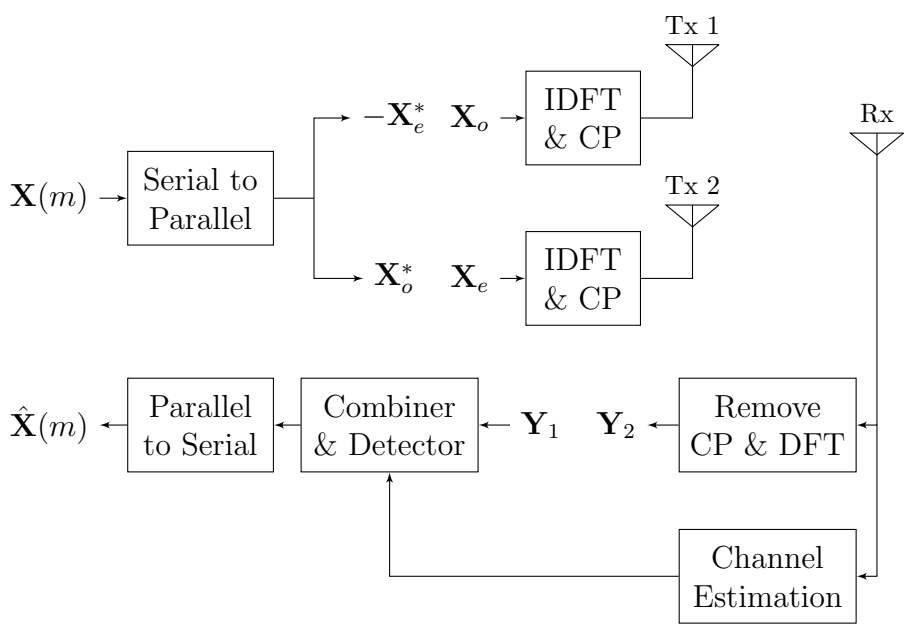


Figure 2-5. A block diagram of space-time OFDM systems [8]

2.6.2 Performance of ST-OFDM under Jamming

In the sequel, we study the BER performance of space-time OFDM [8] under jamming. The channel is modeled as a flat-fading Rayleigh channel. For every sub-carrier

in OFDM systems, its bandwidth is relatively small compared with the bandwidth of the channel, so it is reasonable to make this flat-fading assumption. Considering that the jamming and the signal are both independently attenuated by the channel, we use two independent random variables to describe the jamming channel power gain G_J and the signal channel power gain G_S, which are given as

$$G_S = \alpha^2 \tag{2–25}$$

$$G_J = \beta^2 \tag{2–26}$$

where α and β are independent Rayleigh random variables with variances σ_s^2 and σ_J^2 respectively. Because jamming and signal are under the same channel environment, σ_S and σ_J can be regarded as the same value σ. Therefore, we have the following signal model under jamming.

$$\begin{aligned} \mathbf{Y}_1 &= \mathbf{\Lambda}_1\mathbf{X}_o + \mathbf{\Lambda}_2\mathbf{X}_e + \mathbf{Z}_1 + \mathbf{\Delta}_1\mathbf{J}_1 \\ \mathbf{Y}_2 &= -\mathbf{\Lambda}_1\mathbf{X}_e^* + \mathbf{\Lambda}_2\mathbf{X}_o^* + \mathbf{Z}_2 + \mathbf{\Delta}_2\mathbf{J}_2 \end{aligned} \tag{2–27}$$

where $\mathbf{J}_1$ and $\mathbf{J}_2$ denote the DFTs of jamming and $\mathbf{\Delta}_1$ and $\mathbf{\Delta}_1$ are two diagonal matrices whose diagonal elements are the DFTs of the respective jammer channel impulse response.

In Rayleigh fading channel, the effective energy-per-bit becomes $G_S E_b$ and the effective PSD of the BNJ becomes $G_J N_J$. After simplifying, we get the BER

$$P_b(\alpha, \beta) = Q\left(\sqrt{\frac{\alpha^2 E_b}{N_0 + \beta^2 N_J}}\right) \tag{2–28}$$

Since there are two Rayleigh random variables, α and β, with the same variance, the average BER for BPSK can be expressed as:

$$\bar{P}_b = \int_0^\infty \int_0^\infty Q\left(\sqrt{\frac{\alpha^2 E_b}{N_0 + \beta^2 N_J}}\right) \frac{\alpha\beta}{\sigma^4} \exp\left(\frac{-\alpha^2 - \beta^2}{2\sigma^2}\right) d\alpha d\beta \tag{2–29}$$

Certainly, the infinite upper limit of integration should be replaced by finite approximated value in practice.

Figure 2-6 shows the performance of the space-time OFDM under BNJ with Rayleigh fading and AWGN. Note that the theoretical BER performance is drawn by (2–17) with (2–29). The OFDM system employed 256 sub-carriers. It was assumed that the perfect channel estimation was available at the receiver. The theoretical BER performance by (2–29) is a good approximation of the simulated BER performance.

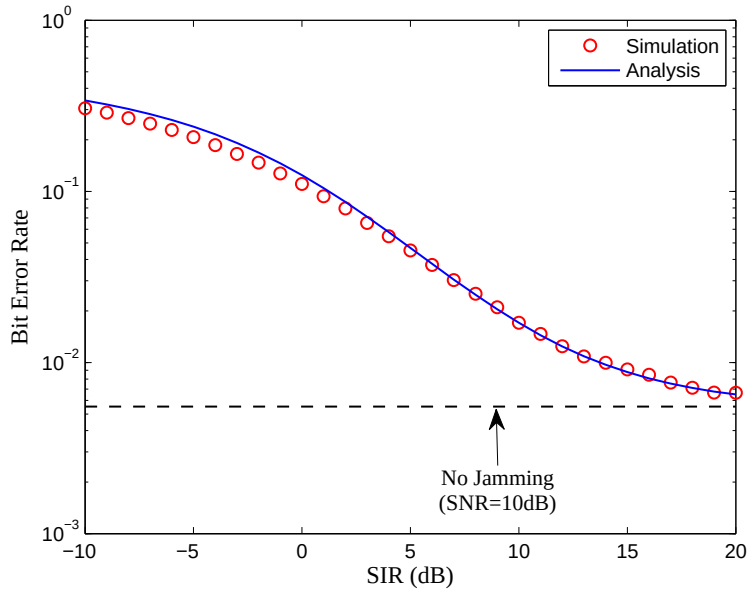


Figure 2-6. Performance of ST-OFDM system under BNJ with Rayleigh fading and AWGN

We consider the best jamming scenario for PBJ: The jamming signal bandwidth falls into that of the OFDM signal completely. The portion of jamming signal bandwidth can be described by:

$$\rho = \frac{W_J}{W_S} \tag{2–30}$$

where W_J is the bandwidth of the jamming signal and W_S is the bandwidth of the OFDM signal. We need to consider the jammed frequency bands and the un-jammed frequency bands. Given the average PSD of PBJ N_J, the effective PSD of PBJ in the first type of band becomes N_J/ρ, and there is no jamming at all in the second type of band. Then, we have the BER performance under the PBJ as follows:

$$P_b(\rho) = \rho Q\left(\sqrt{\frac{E_b}{N_0 + N_J/\rho}}\right) + (1-\rho)\, Q\left(\sqrt{\frac{E_b}{N_0}}\right) \tag{2–31}$$

For the time-correlated Rayleigh fading channel, following the same steps as before, the average BER for BPSK becomes:

$$\begin{aligned}\bar{P}_b = \rho \int_0^\infty \int_0^\infty Q\left(\sqrt{\frac{\alpha^2 E_b}{N_0 + \beta^2 N_J/\rho}}\right) \frac{\alpha\beta}{\sigma^4} \exp\left(\frac{-\alpha^2 - \beta^2}{2\sigma^2}\right) d\alpha d\beta \\ + (1-\rho) \int_0^\infty \int_0^\infty Q\left(\sqrt{\frac{\alpha^2 E_b}{N_0}}\right) \frac{\alpha\beta}{\sigma^4} \exp\left(\frac{-\alpha^2 - \beta^2}{2\sigma^2}\right) d\alpha d\beta\end{aligned} \tag{2–32}$$

Figure 2-7 shows the performance of the space-time OFDM under 50% PBJ with Rayleigh fading and AWGN.

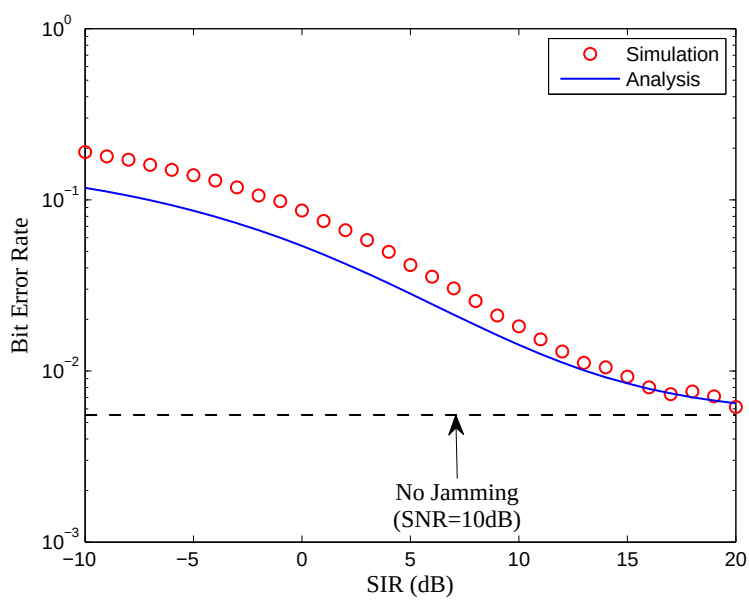


Figure 2-7. Performance of ST-OFDM system under $\rho = 0.5$ PBJ with Rayleigh fading and AWGN

For MTJ, we assume that those q jamming tones are perfectly aligned with q sub-carriers of the OFDM system. Then the portion of jamming signal bandwidth is defined as:

$$\rho = q/M \tag{2–33}$$

where M is the number of FFT points. We can analyze the performance of the space-time OFDM system under MTJ by (2–32). Figure 2-8 shows the performance of the space-time OFDM under 50% MTJ with Rayleigh fading and AWGN.

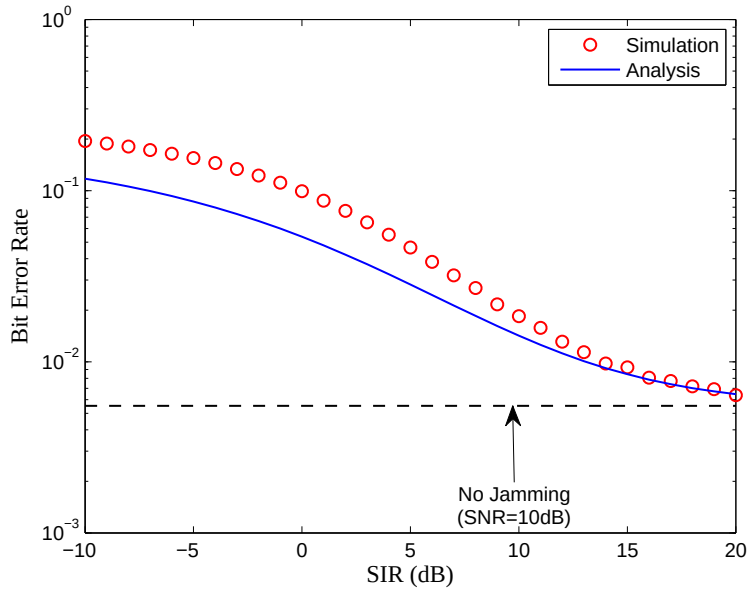


Figure 2-8. Performance of space-time OFDM system under $\rho = 0.5$ MTJ with Rayleigh fading and AWGN

2.6.3 Multi-Carrier Vertical-Bell Laboratories Layered Space-Time

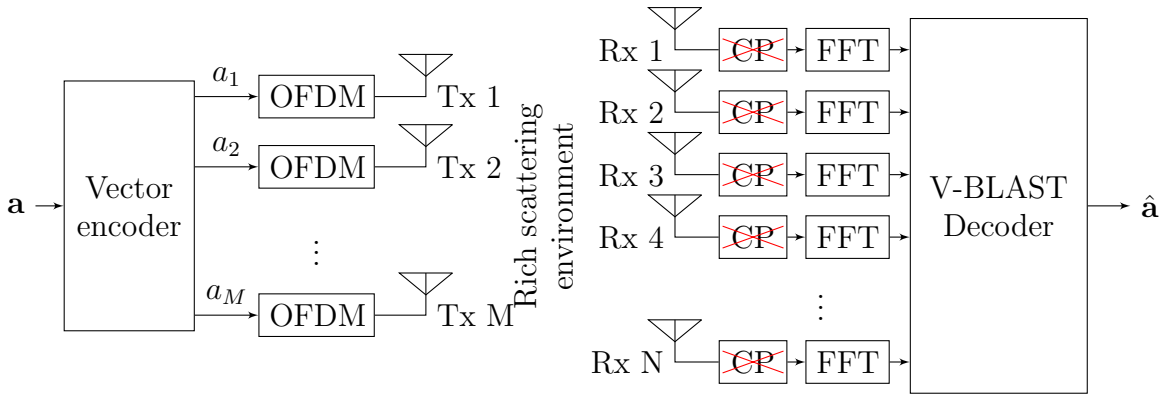


Figure 2-9. Multi-carrier V-BLAST high level system diagram where number of transmitters is M and number of receivers is N.

The V-BLAST is a MIMO system based on spatial multiplexing (SM) method, which provides trade-off between system performance and system implementation complexity [7,

20] . The V-BLAST is combined with OFDM modulation scheme to achieve high data rate transmission in frequency selective fading channel. Since the OFDM effectively divides the frequency selective fading channel into a number of flat fading sub-channels, a multi-carrier (MC) V-BLAST system comprises of narrow band V-BLAST systems on different sub-carriers. Therefore, the MC V-BLAST can provide both high data rate and high throughput transmission over rich scattering channel [23]. A V-BLAST transceiver model based on an OFDM modulation scheme is depicted in Figure 2-9.

A MC V-BLAST system with M transmit and N receiver antennae consists of one narrow band V-BLAST system on each subcarrier. Therefore, we can write the received signal vector on a specific sub-carrier as follows:

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} \tag{2–34}$$

where $\mathbf{y} = [y_1, \cdots, y_N]^T$ is the received signal, $\mathbf{x} = [x_1, \cdots, x_M]^T$ is the transmitted signal on each sub-carrier, and $\mathbf{n}$ is AWGN noise. The channel matrix $\mathbf{H}$ is a $N \times M$ matrix with each entry H_{mn} denoting the channel response between mth transmit antenna and nth receive antenna,

$$\mathbf{H} = \begin{bmatrix} H_{11} & \cdots & H_{1M} \\ \vdots & \ddots & \vdots \\ H_{N1} & \cdots & H_{MN} \end{bmatrix} \tag{2–35}$$

A V-BLAST algorithm will reconstruct the transmitted information signal with the information of the channel matrix by removing the effect of fading of the channel in frequency domain [7].

Figure 2-10 shows the BER performance for $M \times N = 2 \times 2$ transceiver MC V-BLAST for BPSK modulation in a flat fading independent Rayleigh channel for the different equalizers [20]. We use the same main simulation parameters used in [45]. We can see that the BER performance with a zero-forcing (ZF) equalizer is identical to that of $M \times N = 1 \times 1$ transceiver system, and equalizers with successive interference

cancelation (SIC) perform better than those equalizers without the SIC. We can see that the performance of the V-BLAST is lower bounded by that performance of $M \times N = 1 \times 2$ MRC receiver diversity system.

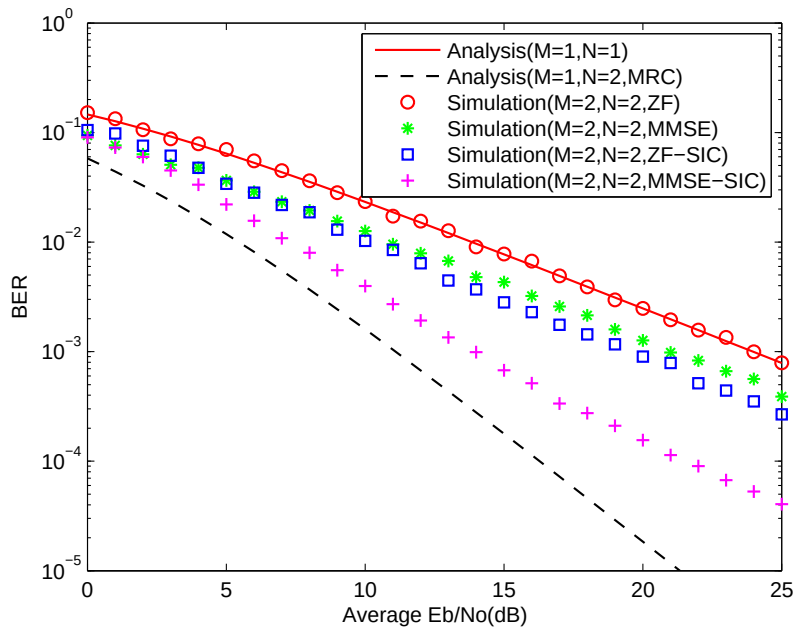


Figure 2-10. BER performance of MC V-BLAST for BPSK modulation with $M \times N = 2 \times 2$ MIMO Rayleigh Fading Channel

2.6.4 The Effects of Jamming on Multi-Carrier V-BLAST systems

In the sequel, we leverage on the BER performance of MC V-BLAST under jamming. We only consider $M \times N = 2 \times 2$ transceiver combination for simplicity.

Let both the jamming and the signal be independently attenuated by the channel and let two independent random variables be described by the jamming channel power gain $G_v = \beta^2$ and the signal channel power gain $G_x = \alpha^2$ where α and β are independent Rayleigh random variables with variance σ_x^2 and σ_v^2, respectively. Therefore, the MIMO signal model in (2–34) under jamming can be written as follows:

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{H}_v\mathbf{v} + \mathbf{n} \tag{2–36}$$

where $\mathbf{v}$ denotes the $M \times 1$ jamming signals on each sub-carrier and $\mathbf{H}_v$ is the $N \times M$ jammer channel matrix. Since the OFDM system performs no differently than conventional serial systems under the AWGN [23], the BER for BPSK is given by:

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_0 + N_J}}\right) \tag{2–37}$$

where E_b is the average energy-per-bit of OFDM signal. In Rayleigh fading channel, the effective energy-per-bit becomes $G_x E_b$ and the effective PSD of the BNJ becomes $G_v N_v$. After simplifying, we get the BER under Rayleigh fading channel as follows:

$$P_b(\alpha, \beta) = Q\left(\sqrt{\frac{\alpha^2 E_b}{N_0 + \beta^2 N_v}}\right) \tag{2–38}$$

Since there are two Rayleigh random variables, α and β, with the same variance, the average BER of zero-forcing MC V-BLAST with $M \times N = 2 \times 2$ under BNJ for BPSK can be expressed as:

$$\bar{P}_b^u = \int_0^\infty \int_0^\infty Q\left(\sqrt{\frac{\alpha^2 E_b}{N_0 + \beta^2 N_v}}\right) \frac{\alpha\beta}{\sigma^4} \exp\left(\frac{-\alpha^2 - \beta^2}{2\sigma^2}\right) d\alpha d\beta \tag{2–39}$$

The performance of the MC-VBLAST is lower bounded by:

$$\bar{P}_b^l = \left(\bar{P}_b^u\right)^2 \left(1 + 2\bar{P}_b^u\right) \tag{2–40}$$

where superscript l and u denote lower and upper bound of the BER. Certainly, the infinite upper limit of integration should be replaced by finite approximated value in practice. Figure 2-11 shows the performance of the 2×2 MC V-BLAST under BNJ with Rayleigh fading and AWGN. Note that the analytical BER performance is drawn by (2–39) and (2–40). In this simulation, we use the same simulation parameters used in Figure 2-10 with SNR = 10 dB.

Let $\rho = W_J/W_x$ denote the fraction of jammed bandwidth W_J with respect to total system bandwidth W_x for PBJ. Therefore, we have to consider the jammed bands and the un-jammed bands. The effective PSD of PBJ in the jammed bands becomes N_J/ρ given

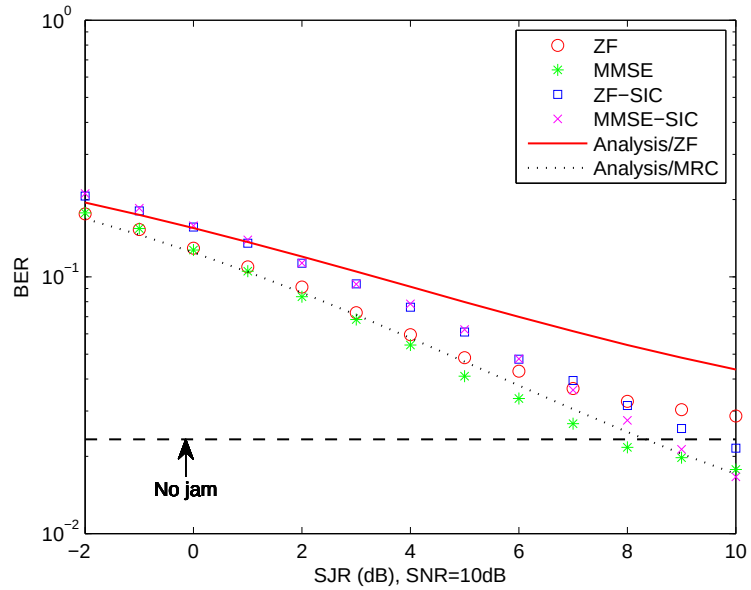


Figure 2-11. BER performance of MC V-BLAST under BNJ for BPSK modulation with 2×2 MIMO Rayleigh fading channel

the average PSD of PBJ N_J, while there is no jamming at all in the un-jammed bands. Therefore, the average BER under PBJ with AWGN becomes:

$$P_b(\rho) = \rho Q\left(\sqrt{\frac{2E_b}{N_0 + N_J/\rho}}\right) + (1-\rho)\, Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{2–41}$$

Note that the average BER under BNJ in (2–37) is a special case of (2–41) with $\rho = 1$ and (2–38) for PBJ becomes:

$$P_b(\rho, \alpha, \beta) = Q\left(\sqrt{\frac{2\alpha^2 E_b}{N_0 + \beta^2 N_J/\rho}}\right) \tag{2–42}$$

and the average BER for BPSK for the time-correlated Rayleigh fading channel becomes:

$$\begin{aligned} \bar{P}_b^u = \rho \int_0^\infty \int_0^\infty P_b(\rho, \alpha, \beta) \frac{\alpha\beta}{\sigma^4} \exp\left(\frac{-\alpha^2 - \beta^2}{2\sigma^2}\right) d\alpha d\beta \\ + (1-\rho) \int_0^\infty \int_0^\infty (\rho, \alpha, \beta = 0) \frac{\alpha\beta}{\sigma^4} \exp\left(\frac{-\alpha^2 - \beta^2}{2\sigma^2}\right) d\alpha d\beta \end{aligned} \tag{2–43}$$

Figure 2-12 shows the performance of the 2×2 MC V-BLAST under 50% ($\rho = 0.5$) PBJ with Rayleigh fading and AWGN. Note that the analytical BER performance is

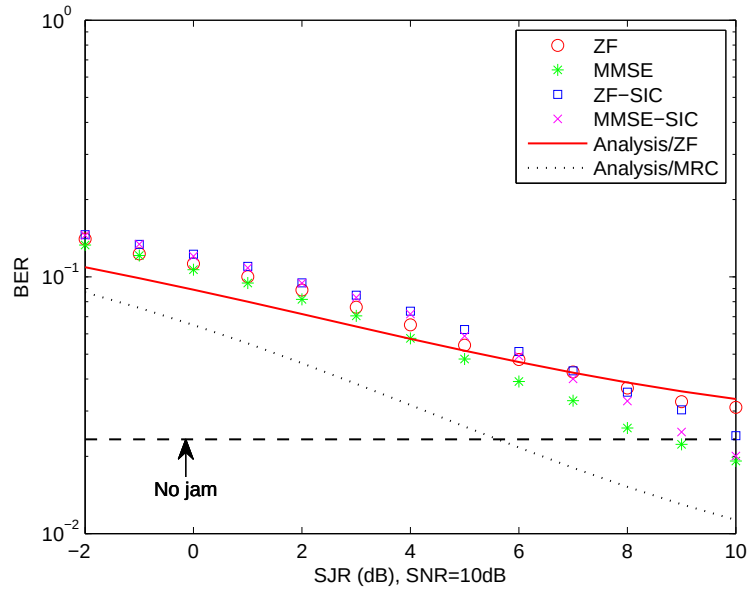


Figure 2-12. BER performance of MC V-BLAST under 50% PBJ for BPSK modulation with 2×2 MIMO Rayleigh fading channel

drawn by (2–43) and (2–40). In this simulation, we use the same simulation parameters used in Figure 2-11. In [45], a signal space model was proposed to analyze the BER performance of OFDM under AWGN. Thus BER performance of 2×2 zero-forcing MC V-BLAST for BPSK is given as:

$$P_b(E_b, N_0, \rho, SIR) = \rho \int_{-\infty}^{0} \int_{\sqrt{E_b}-A_J}^{\sqrt{E_b}+A_J} \frac{1}{\sqrt{\pi N_0}} \exp\left[-\frac{(w-y)^2}{N_0}\right] \frac{1}{\pi A_J \sqrt{1-\left(\frac{y-\sqrt{E_b}}{A_J}\right)^2}} dy dw + (1-\rho) Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{2–44}$$

where A_J can be obtained simply through the following equation

$$A_J = \sqrt{\frac{E_b}{\rho SIR}} \tag{2–45}$$

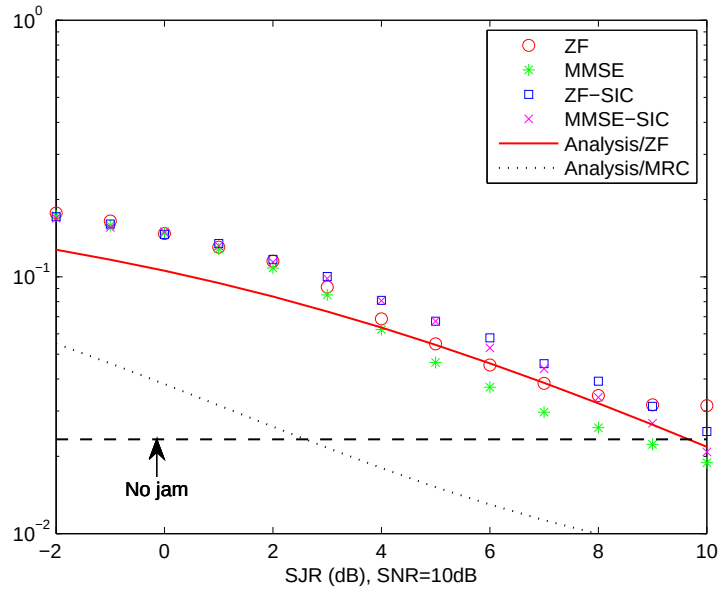


Figure 2-13. BER performance of MC V-BLAST under 50% MTJ for BPSK modulation with 2×2 MIMO Rayleigh fading channel

If the AWGN is negligible ($W = Y$) for simplicity, we have:

$$P_b(E_b, N_0, \rho, SIR) = \frac{\rho}{\pi}\left[\frac{\pi}{2} - \arcsin\left(\sqrt{\rho SIR}\right)\right] + (1-\rho)Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{2–46}$$

and the average BER performance of 2×2 ZF MC V-BLAST for BPSK under MTJ with Rayleigh fading channel and AWGN is

$$\bar{P}_b^u = \int_0^\infty \int_0^\infty P_b(\alpha^2 E_b, N_0, \rho, \alpha^2 SIR/\beta^2)\frac{\alpha\beta}{\sigma^4}\exp\left(-\frac{\alpha^2+\beta^2}{2\sigma^2}\right)d\alpha d\beta \tag{2–47}$$

Figure 2-13 shows the performance of the 2×2 MC V-BLAST under 50% ($\rho = 0.5$) MTJ with Rayleigh fading and AWGN. Note that the analytical BER performance is drawn by (2–47) and (2–40). In this simulation, we use the same simulation parameters which in Figure 2-11.

The MC V-BLAST combines the merits of multi-carrier modulation and MIMO system to achieve high data rate transmission under frequency selective fading channel. In this section, we investigate the effects of various jamming for MC V-BLAST under

Rayleigh fading with AWGN channel by means of simulation and analysis. Our study indicates that the performance of 2×2 transceiver MC V-BLAST using BPSK modulation is bounded between 1×1 system for BPSK modulation in Rayleigh channel and 1×2 system with MRC receiver.

2.7 Summary

Wireless communication is, by any measure, the fastest growing segment of the communication industry. We verify stationarity or non-stationarity of jamming. We evaluate the BER performance of various wireless communication systems under different jamming strategies. We also conduct theoretical analysis to quantify the effect of jamming and unintentional interference in terms of the BER. Throughout this study, we can predict the performance of wireless communication systems under interference, which leads us to mitigate interference for reliable communications.

CHAPTER 3
ON CRACKING DIRECT-SEQUENCE SPREAD-SPECTRUM SYSTEMS

3.1 Introduction

In this chapter, we consider the problem of eavesdropping on the adversary's communication, which uses direct-sequence spread-spectrum (DS-SS). The DS-SS is a covert communication technique; the information symbols are modulated by a pseudo-random noise (PN) sequence prior to transmission. This results in a wideband signal, which is resistant to interference, jamming, interception and multipath fading [2, 16, 18].

To eavesdrop on the adversary's communication, one needs to (a) identify the start position of data symbols in the intercepted spread signal for the purpose of symbol synchronization, (b) estimate data symbols, (c) estimate the PN sequence, and (d) estimate the code generator polynomial of the PN sequence.

To identify the start position of data symbols, we present a method based on the spectral norm which achieves smaller estimation error in Section 3.4. After the symbol synchronization, we remove a PN sequence from the intercepted signals by a correlation method to estimate data symbols without a priori knowledge about that PN sequence in Section 3.5. Identification of a PN sequence is processed by a matched filter between the intercepted signal and the estimated data symbols in Section 3.6.

One of the harder problems in eavesdropping on DS-SS signals is the polarity ambiguity of the estimated spread sequence and data symbols: Erroneous reversal of polarity of each chip in the estimated PN sequence compared to the true PN sequence is a major source of the performance degradation of an eavesdropper. Therefore, we need to estimate a code generator polynomial to mitigate this polarity problem. We propose a searching method to identify the code generator polynomial in order to correct polarity errors as well as to reduce memory requirement of an eavesdropper in Section 3.7.

Saving hundreds or thousands of sequence bits in the memory of an eavesdropper is very expensive.

The probability of error performance of an eavesdropper is a function of signal-to-noise ratio (SNR), the number of data symbols, and the length of the spread sequence of the intercepted signal. Therefore, we need to study the analytical probability of error performance of the eavesdropper with respect to these parameters. By doing so, we can efficiently predict the performance of the eavesdropper.

First, we use a Gaussian approximation method in [51] in order to find a marginal probability density function of the symbol estimator in Section 3.5 and the sequence estimator in Section 3.6, respectively. Second, we find the probability of error of the symbol detector without the proposed code generator estimator as a sum of products of error functions and frequencies of the number of errors in the estimated spread sequence. Finally, we compare the probability of error with and without the proposed generator polynomial estimator in Section 3.7.

The contributions of this chapter are: (i) a generator polynomial estimator which can identify a code generator polynomial and can correct polarity errors in the estimated PN sequence and estimated data symbols, (ii) a theoretical verification of the probability of error of a code generator estimator with respect to signal-to-noise ratio (SNR), the number of data symbols, and the length of the spread sequence of the intercepted signal, and (iii) the accuracy of performance prediction of an eavesdropper.

The remainder of this chapter is organized as follows: Related works are discussed in Section 3.2. Section 3.3 describes the signal model. Section 3.4 introduces our method of identifying the start position of a data symbol in the spread signal. Section 3.5 presents how to remove data symbols from the intercepted signal. Then, estimation of a spread sequence is presented in Section 3.6. Section 3.7 discusses how to identify a PN code generator polynomial and how to correct polarity errors. Section 3.8 presents simulation

results to show the effectiveness and to validate the analytical probability of error of our approaches. Section 3.9 summarizes this chapter.

3.2 Related Works

Wireless communications are very common both for military and commercial parties. The ability to use communication while mobile has great benefits for both parties. However, wireless communication has many security issues, since communication takes place over a wireless channel while the users are usually mobile. Such a wireless channel suffers from a number of vulnerabilities: (i) The channel is vulnerable to eavesdropping. (ii) The data can be altered. (iii) The absence of wired link makes it much easier to cheat on identities. (iv) The channel can be overused. (v) Finally, the channel can be jammed, notably in order to perpetrate a denial-of-service (DoS) attack [13, 14].

To eavesdrop on the adversary's communication which uses DS-SS, the estimation of the spread sequence from the intercepted signal is a key to crack on these DS-SS systems and is a challenging problem. The literature on this subject is not rich. We briefly discuss some related works which have studied this problem.

First, an eavesdropper needs to detect any transmission of DS-SS signals in order to crack a secure DS-SS signal. A method based on the fluctuation of an autocorrelation estimator, instead of on the autocorrelation itself, was proposed in [52]. The fluctuation of the autocorrelation estimator was used to estimate an accurate spread code period. Since the intercepted signal may experience delay, the interceptor must find the start position of a data symbol in the spread signal. To identify the start position of a data symbol in the spread signal, a correlation-based method was proposed in [42]. A method of maximizing the Frobenius norm of a covariance of the intercepted signal was proposed in [53]. However, the Frobenius norm may result in the increase of estimation error as the period of the PN sequence increases; hence, their method does not work well for the PN sequence of a long period. To address this limitation, a method based on the spectral

norm which achieves smaller estimation error than the Frobenius norm based method is proposed in Section 3.4.

Second, to identify the PN sequence, several methods were proposed in the literature [41, 42, 54, 55]. In [41], a method based on a multichannel identification technique was proposed to recover the convolution between the PN sequence and the channel response for blind channel estimation; the limitation of this method is high computational complexity. In [55], a method based on principal component analysis (PCA) was used to estimate the PN sequence from eigenvectors corresponding to the first and the second largest eigenvalues of the sample covariance matrix; however, the computational complexity required by PCA is high. To estimate the PN sequence and to use a parallel processing to combat the polarity ambiguity in successive demodulation and decoding, the use of chip-by-chip detection was suggested in [42]. However, their parallel processing approach has a limitation: It increases memory requirement and does not mitigate the polarity error. A multiple subsection cross-correlation averaging method was proposed to estimate the PN sequence in [54]; however, the method used only half of the captured symbols. It is known that the more data symbols used, the more accurate the estimation is. In Section 3.6, we propose a cross-correlation based method that uses all captured symbols and achieves higher estimation accuracy.

Third, to correct the polarity ambiguity in the estimated spread sequence and data symbols, an eavesdropper needs to estimate a code generator polynomial. The estimators used in [54, 55] did not consider the problem of polarity errors in the estimated PN sequence, i.e., erroneous reversal of polarity of each chip in the estimated PN sequence (compared to the true PN sequence). Therefore, the probability of correct estimation of the PN sequence, using their estimators, may be less than 50%. This leads to significant performance degradation in terms of bit error rate (BER) or symbol error rate (SER). We solve this problem by identifying the PN code generator polynomial in Section 3.7. Not only is it important to estimate the PN sequence, but we also need to identify the

PN code generator. Identifying the PN code generator polynomial improves the accuracy of estimating the PN sequence and data symbols by a factor of two, over the methods proposed in [54, 55].

In [42], the probability of error of their sequence estimator was analyzed for each chip of a spread sequence. They found a marginal probability density function of that sequence estimator by a numerical integration. However, they did not consider the polarity ambiguity in their correct estimation probability analysis. Therefore, their analysis had a limitation. In Section 3.7, we consider the polarity ambiguity in the analysis of the probability of error of a sequence estimator and a symbol detector. We also provide a complete expression for the probability of error of a symbol detector in Section 3.7.

Table 3-1. List of notations.

$\Pr(\cdot)$	Probability of $(\cdot)$
P_b	Probability of error
$(\cdot)^H$	Conjugate transpose of $(\cdot)$
$(\cdot)^T$	Transpose of $(\cdot)$
$\mathrm{Re}(\cdot)$	Real part of $(\cdot)$
$\mathrm{Im}(\cdot)$	Imaginary part of $(\cdot)$
GF	Galois field or finite field
F	Field
$\mathbf{E}(\cdot)$	Expectation of matrix $(\cdot)$
$\mathrm{sgn}(x)$	Sign of x
$\mathbf{a}$	A vector (or set) of sequence (symbol)
$\mathbf{a}^*$	$-\mathrm{sgn}(\mathbf{a})$
$\lfloor\cdot\rfloor$	The nearest integer less than equal $(\cdot)$
$\hat{a}$	Estimation of a
$< \mathbf{x}, \mathbf{y} >$	Inner product of $\mathbf{x}$ and $\mathbf{y}$
$\mathrm{erfc}(\cdot)$	Complementary error function of $(\cdot)$
$\lVert\cdot\rVert_2$	Spectral norm of $(\cdot)$
$\lVert\cdot\rVert_F$	Frobenius norm of $(\cdot)$
$\mathcal{N}$	Normal distribution
$\mathcal{B}$	Binomial distribution
λ	Eigenvalue
$a_{i,j}$	The $(i,j)^{th}$ Entry of a matrix $\mathbf{A}$
L	The number of synchronized data symbols
P	The length of the spread sequence

3.3 Signal Model

A baseband representation of a DS-SS signal is given by [41, 55]:

$$y(t) = \sum_{l=-\infty}^{+\infty} a_l h(t - kT_s) + n(t) \tag{3–1}$$

$$h(t) = \sum_{k=0}^{P-1} c_k p(t - kT_c) \tag{3–2}$$

where T_s is the symbol duration, and a_l is a QPSK or BPSK modulated symbol transmitted at time kT_s[1] . We assume the symbols a_l are centered and uncorrelated. Let $n(t)$ denote the noise at the output of the received filter and the noise is additive white Gaussian noise (AWGN) and uncorrelated with the information signal a_l. The effect of the transmitter filter, the reception filter, the channel response and the pseudo-random sequence c_k is represented by $h(t)$. Let $p(t)$ denote the convolution of all filters of the transmission chain. T_c is the chip duration and $\{c_k\}_{k=0,\cdots,P-1}$ is the pseudo-random sequence of length P where $P = T_s/T_c$. In this chapter, we assume the symbol duration T_s can be estimated by the method in [52] for simplicity. Note that we consider the AWGN channel only in this chapter. Our study can be extended to multipath environments if we use a blind channel estimation method proposed in [41]. However, in the current work, we limit ourselves to the AWGN channel for simplicity. Table 3-1 lists the notations used in this chapter.

3.4 Symbol Synchronization

The captured signal $y(t)$ in (3–1) is sampled and divided into non-overlapping windows with the eavesdropper's sampling duration T_{ev}. We assume the sampling duration of an eavesdropper is the chip duration for simplicity, however this is not a requirement of our method. Therefore, $P \cdot (L+1)$ samples are available by sampling $(L+1) \cdot T_s$ long signal

[1] For reasons of simplicity and clarity of presentation, we only focus on the QPSK/BPSK modulation. If we adopt a blind modulation detection method, our work can be applied to higher order modulation like 64-QAM with little modification.

with the sample duration T_c. Rewriting $P \cdot (L+1)$ samples as a matrix $\mathbf{y}^k$ with dimension $P \times (L+1)$, we have:

$$\mathbf{y}^k = \begin{bmatrix} \mathbf{y}^k_{-1} & \cdots & \mathbf{y}^k_{l-1} & \mathbf{y}^k_l & \cdots & \mathbf{y}^k_{L-1} \end{bmatrix} \tag{3–3}$$

where the superscript k represents the kT_c time-delayed desynchronized signal of (3–1) for $k = 0, \cdots, P-1$. Let $\mathbf{y}^k_l$ denote a column of the desynchronized $\mathbf{y}^k$. We may write $\mathbf{y}^k_l$ as follows:

$$\begin{aligned} \mathbf{y}^k_l &= \begin{bmatrix} y_{l,k} & \cdots & y_{l,P-1} & y_{l+1,0} & \cdots & y_{l+1,k-1} \end{bmatrix}^T \\ &= \begin{bmatrix} a_l h_{l,k} + n_k \\ \vdots \\ a_l h_{l,P-1} + n_{P-1} \\ a_{l+1} h_{l+1,0} + n_0 \\ \vdots \\ a_{l+1} h_{l+1,k-1} + n_{k-1} \end{bmatrix} \end{aligned} \tag{3–4}$$

where $[\cdot]^T$ denotes the transpose, $y_{l,k}$ is the kth entry of a column y^k_l and $h_{l,k}$ is the spreading sequence of $y_{l,k}$. Now, we can modify (3–4) as follows:

$$\begin{aligned} \mathbf{y}^k_l &= \begin{bmatrix} h_{l,k} & 0 \\ \vdots & \vdots \\ h_{l,P-1} & 0 \\ 0 & h_{l+1,0} \\ \vdots & \vdots \\ 0 & h_{l+1,k-1} \end{bmatrix} \begin{bmatrix} a_l \\ a_{l+1} \end{bmatrix} + \begin{bmatrix} n_k \\ \vdots \\ n_{P-1} \\ n_0 \\ \vdots \\ n_{k-1} \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{h}^e_l \; \mathbf{h}^b_{l+1} \end{bmatrix} \mathbf{a}^k_l + \mathbf{n}^k \\ &= \mathbf{h}^k_l \, \mathbf{a}^k_l + \mathbf{n}^k \end{aligned} \tag{3–5}$$

where $\mathbf{h}_l^e$ denotes a vector containing the end of the spreading waveform for a duration of $T_s - kT_c$ followed by zeroes for a duration kT_c; $\mathbf{h}_{l+1}^b$ is a vector containing zeroes for a duration $T_s - kT_c$ followed by the beginning of the spreading waveform for a duration kT_c; $\mathbf{a}_l^k$ denotes a vector containing two desynchronized symbols a_l and a_{l+1}; $\mathbf{n}^k$ stands for the noise. Therefore, it is necessary to make a column $\mathbf{y}_l^k$ have only one data symbol a_l. That is:

$$\begin{aligned} \mathbf{y}_l^0 &= \begin{bmatrix} y_{l,0} & \cdots & y_{l,k-1} & y_{l,k} & \cdots & y_{l,P-1} \end{bmatrix}^T \\ &= \mathbf{h}_l^0 a_l + \mathbf{n}^0 \end{aligned} \tag{3–6}$$

and (3–3) becomes:

$$\mathbf{y}^0 = \begin{bmatrix} \mathbf{y}_0^0 & \cdots & \mathbf{y}_{l-1}^0 & \mathbf{y}_l^0 & \cdots & \mathbf{y}_{L-1}^0 \end{bmatrix} \tag{3–7}$$

Note that samples which belong to a_{-1} and a_L in (3–3) are truncated in the synchronized intercepted signal (3–7). Let $\mathbf{R}$ denote the covariance matrix of (3–5).

$$\begin{aligned} \mathbf{R} &= \mathbf{E}[\mathbf{y}_l^k \mathbf{y}_l^{k^H}] \\ &= \mathbf{h}_l^k \mathbf{E}\left[\mathbf{a}_l^k \mathbf{a}_l^{k^H}\right] \mathbf{h}_l^{k^H} + \sigma_n^2 \mathbf{I}_P \end{aligned} \tag{3–8}$$

where $[\cdot]^H$ is the conjugate transpose, $\mathbf{I}_P$ represents a $P \times P$ identity matrix, $\mathbf{E}[\cdot]$ denotes expectation, and σ_n^2 is the noise variance.

To place the starting spread sequence $h_{l,0}$ in the proper position in (3–4), we search for a maximum of the spectral norm of the sample covariance matrix of (3–8). The spectral norm of a matrix is the square root of the largest eigenvalue of $\mathbf{R}$ in [56]. Let $\|\mathbf{y}\|_2$ denote the spectral norm of the square covariance matrix.

$$\|\mathbf{y}\|_2 = \sqrt{\lambda_{\max}(\mathbf{R})} \tag{3–9}$$

where $\lambda_{\max}(\mathbf{R})$ stands for the largest eigenvalue of the covariance matrix. Then, the spectral norm of (3–7) is:

$$\|\mathbf{y}_l^0\|_2 = \|\mathbf{h}_l^0\|^2 E\left[|a_l|^2\right] + \sigma_n^2 \tag{3–10}$$

However, the spectral norm of (3–5) is:

$$\|\mathbf{y}_l^k\|_2 = \begin{cases} \|\mathbf{h}_l^e\|^2 E\left[|a_l|^2\right] + \sigma_n^2 & \text{if } kT_c \leq \frac{T_s}{2} \\ \|\mathbf{h}_{l+1}^b\|^2 E\left[|a_{l+1}|^2\right] + \sigma_n^2 & \text{if } kT_c > \frac{T_s}{2} \end{cases} \tag{3–11}$$

if the singular values are expressed in decreasing order. Since $\|\mathbf{h}_l^0\|^2 \geq \|\mathbf{h}_l^e\|^2$ or $\|\mathbf{h}_l^0\|^2 \geq \|\mathbf{h}_{l+1}^b\|^2$, we can determine the synchronized version of (3–3) by maximizing the spectral norm in (3–9) with respect to $k = 0, \cdots, P-1$ as follows:

$$\begin{aligned} \hat{\mathbf{y}}^0 &= \underset{k\in[0,P-1]}{\operatorname{argmax}} \|\mathbf{y}^k\|_2 \\ &= \underset{k\in[0,P-1]}{\operatorname{argmax}} \sqrt{\lambda_{\max}(\mathbf{R})} \\ &= \underset{k\in[0,P-1]}{\operatorname{argmax}} \sqrt{\lambda_{\max}\left(\mathbf{E}\left[\mathbf{y}^k\mathbf{y}^{kH}\right]\right)} \end{aligned} \tag{3–12}$$

In [53], the Frobenius norm was used to search for the start position of a data symbol. Note that the square of the Frobenius norm $\|\mathbf{y}\|_F^2$ is the sum of squares of the singular values of $\mathbf{y}$. There are errors in the eigenvalue decomposition of the sample covariance $\hat{\mathbf{R}}$ due to the noise according to matrix perturbation theory [56]. The expected value of the perturbation error of the Frobenius norm is $P^2 \cdot \sigma_n^2$, while that of the spectral norm is σ_n^2 [56]. The Frobenius norm has a tendency to increase the mean square error (MSE) as the spread sequence length increases. Thus, their method does not perform well for long length sequences. To mitigate this limitation, we use the spectral norm in (3–12).

Figure 3-1 shows the theoretical and simulated squared spectral norm $\|\mathbf{y}^k\|_2$ in (3–12). For the calculation, 10,000 trials are carried out and averaged together. In the simulation, we use QPSK. The PN sequence is an m-sequence [4, 15, 16] with the length $P = 31$ and with a generator polynomial $f(x) = 1 + x^2 + x^5$. The SNR is -5dB. When $k = 0$, the spectral norm has a peak. Note that the more samples, the more accurate estimation of $\hat{\mathbf{y}}^0$ in (3–12) can be achieved.

We also compare the MSEs in the estimation of the time-delay kT_c, $\mathbf{E}[(\hat{k} - k)^2]$, between the spectral norm and the Frobenius norm. The same simulation parameters are

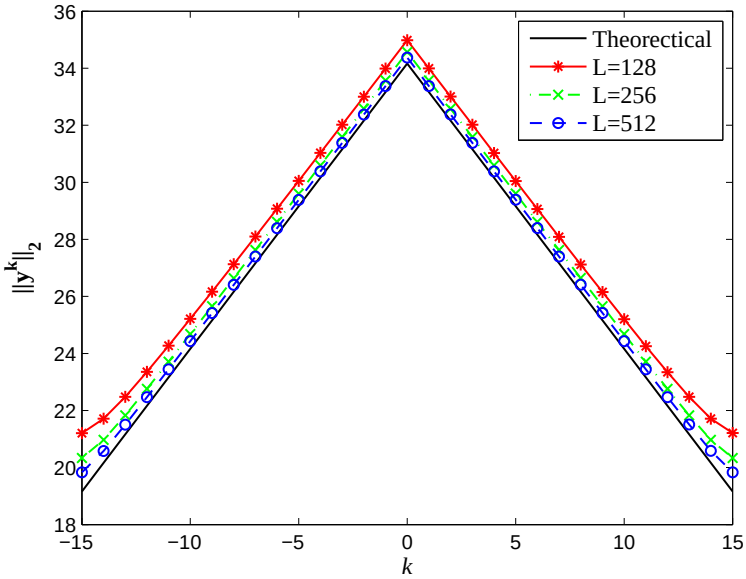
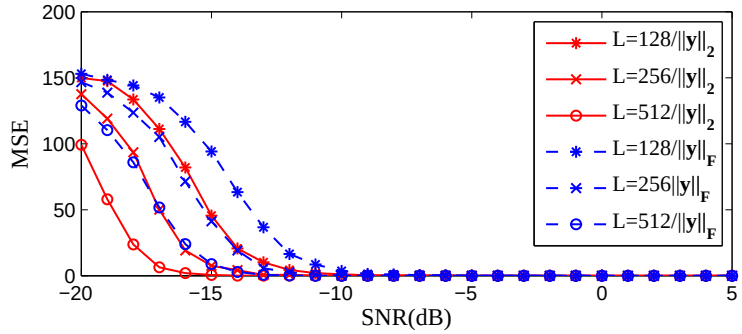
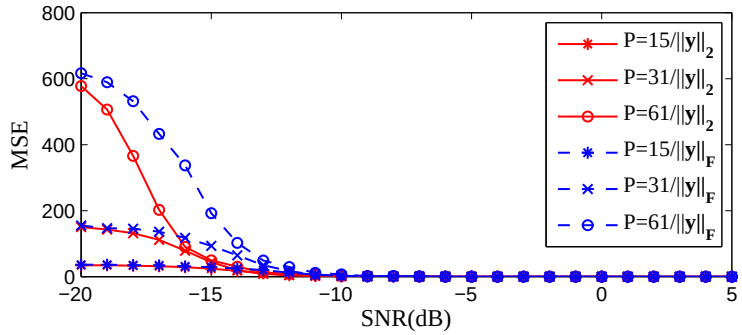


Figure 3-1. Theoretical and simulated spectral norm, $\|\mathbf{y}^k\|_2$, in (3–12) with $P = 31$ and SNR=-5dB



A $P = 31, L = 128, 256, 512$



B $L = 128, P = 15, 31, 63$

Figure 3-2. Comparison of MSE, $\mathbf{E}[(\hat{k} - k)^2]$, by the spectral norm vs. Frobenius norm

used in Figure 3-1, except that SNR is varied from -20dB to 5dB. Figure 3-2(a) shows that the spectral norm has smaller MSEs than the Frobenius norm, when the sequence length $P = 31$ is fixed and the number of symbols L is 128, 256 and 512. We can synchronize the captured signal with fewer symbols by the spectral norm. Figure 3-2(b) shows the case with the fixed number of symbols $L = 128$ and with the varied length of spread sequence P =15, 31, and 63. As the length P increases, the MSE is increased by a factor of P^2; that is, the MSE, normalized by the squares of the sequence length P^2, is almost the same.

3.5 Symbol Estimation

After symbol synchronization, we need to remove the spread sequence in (3–6) to estimate the information symbol a_l from the synchronized signal $\mathbf{y}_l^0$ in (3–7). With the property of strong self-correlation and weak cross-correlation of spread-spectrum, we use a method based on a cross-correlation between a test column, say $\mathbf{y}_t^0$, and a column of a data symbol a_l, say $\mathbf{y}_l^0$, of the synchronized signal in (3–7). Then, we have:

$$C_{\mathbf{y}_t^0\mathbf{y}_l^0}(\tau)=\mathbf{y}_t^0\mathbf{y}_l^{0H}(\tau) \tag{3–13}$$

If the spread sequence is an m-sequence [4, 15, 16], $C_{\mathbf{y}_t^0\mathbf{y}_l^0}(\tau = 0) \geq C_{\mathbf{y}_t^0\mathbf{y}_l^0}(\tau \neq 0)$. Then,

$$C_{\mathbf{y}_t^0\mathbf{y}_l^0}(0)=\sum_{k=0}^{P-1} y_{t,k}y_{l,k}^* \tag{3–14}$$

Now we can estimate the symbol a_l from (3–14) as follows:

$$\begin{aligned}\hat{a}_l = &\operatorname{sgn}\left[\operatorname{Re}\left(C_{\mathbf{y}_t^0\mathbf{y}_l^0}(0)\right)\right] \\ &+ j\cdot\operatorname{sgn}\left[\operatorname{Im}\left(C_{\mathbf{y}_t^0\mathbf{y}_l^0}(0)\right)\right]\end{aligned} \tag{3–15}$$

where $\operatorname{Re}(\cdot)$ takes the real part and $\operatorname{Im}(\cdot)$ takes the imaginary part of a complex. $\operatorname{sgn}(x)$ is the sign function with value 1, if $x > 0$, and -1 otherwise. Note that the estimated symbol $\hat{a}_l$ in (3–15) is estimated up to an unknown multiplicative factor. Therefore, the sign of the symbol in (3–15) can be reversed by this multiplicative factor. This problem

was not considered in [54, 55]. We will solve this problem by estimating a code generator polynomial in Section 3.7.

In order to analyze the performance of the symbol estimator in (3–14), we use a Gaussian approximation of the sum of products of two random variables in order to find a marginal probability density function of the symbol estimator in (3–14). Let $q_{l,k} = y_{t,k}y^*_{l,k}$, $a_t = a_0$, and $h_{0,k} = h_{l,k} = c_k$ in (3–14) for simplicity.

$$\begin{aligned} q_{l,k} &= (a_0 c_k + n_{0,k})(a_l c_k + n_{l,k})^* \\ &= c_k \left(a_0 + \frac{n_{0,k}}{c_k}\right) c_k^* \left(a_l^* + \frac{n^*_{l,k}}{c_k^*}\right) \\ &= |c_k|^2 \left(a_0 + \frac{n_{0,k}}{c_k}\right)\left(a_l^* + \frac{n^*_{l,k}}{c_k^*}\right) \end{aligned} \tag{3–16}$$

Assume $a_0 = 1$ and $a_l = 1$ for generality. Then,

$$q_{l,k} = \epsilon\,(1 + \sigma\bar{n}_{0,k})\left(1 + \sigma\bar{n}^*_{l,k}\right) \tag{3–17}$$

where $\epsilon = |c_k|^2$, $\sigma^2 = \sigma_n^2/\epsilon$, and $\bar{n}_{l,k}$ is a Gaussian random process with zero mean and a unit variance, i.e., $\bar{n}_{l,k} \sim \mathcal{N}(0,1)$. From the above definitions, we have the SNR $\rho = \epsilon/\sigma_n^2 = 1/\sigma^2$.

Let $\alpha^+ = 1 + \sigma\bar{n}_{0,k}$, $\beta^+ = 1 + \sigma\bar{n}_{l,k}$, and $\gamma^+ = \alpha^+\beta^+$. Since $\bar{n}_{l,k} \sim \mathcal{N}(0,1)$, $\alpha^+ \sim \mathcal{N}(1,\sigma^2)$ and $\beta^+ \sim \mathcal{N}(1,\sigma^2)$. We want to find the marginal probability density $f(\gamma^+)$ which is a product of two normal distributions. To find the marginal density $f(\gamma^+)$, we need to integrate the product of a conditional distribution $f(\gamma^+|\beta^+)$ and a marginal distribution $f(\beta^+)$ with respect to β^+.

$$\begin{aligned} f(\gamma^+) &= \int_{-\infty}^{\infty} f(\gamma^+|\beta^+) f(\beta^+) d\beta^+ \\ &= \frac{1}{2\pi\sigma^2}\int_{-\infty}^{\infty} \frac{1}{|\beta^+|} \exp\left[-\frac{1}{2\sigma^2}\left(\frac{\gamma^+ - \beta^+}{\beta^+}\right)^2\right] d\beta^+ \\ &+ \frac{1}{2\pi\sigma^2}\int_{-\infty}^{\infty} \frac{1}{|\beta^+|} \exp\left[-\frac{1}{2\sigma^2}\left(\beta^+ - 1\right)^2\right] d\beta^+ \end{aligned} \tag{3–18}$$

The integration in (3–18) can be obtained using a numerical integration, a Monte Carlo, or a Gaussian approximation with a given ρ [51]. Among these three methods, we use an approximation of products of two normal distributions. Let μ_{γ^+} denote the mean and $\sigma^2_{\gamma^+}$ denote the variance of γ^+. Since α^+ and β^+ are independent of each other, the mean and variance of γ^+ are:

$$\begin{aligned}\mu_{\gamma^+} &= \mathbf{E}[\alpha^+\beta^+] \\ &= \mathbf{E}[\alpha^+]\mathbf{E}[\beta^+] = \mu_{\alpha^+}\mu_{\beta^+} = 1\end{aligned} \tag{3–19}$$

$$\begin{aligned}\sigma^2_{\gamma^+} =& \mathbf{E}[(\alpha^+\beta^+)^2] - (\mathbf{E}[\alpha^+\beta^+])^2 \\ =& \mathbf{E}[(\alpha^+)^2]\mathbf{E}[(\beta^+)^2] - \mu^2_{\alpha^+}\mu^2_{\beta^+} \\ =& \mu^2_{\alpha^+}\sigma^2_{\beta^+} + \mu^2_{\beta^+}\sigma^2_{\alpha^+} + \sigma^2_{\alpha^+}\sigma^2_{\beta^+} \\ =& 2\sigma^2 + \sigma^4\end{aligned} \tag{3–20}$$

The mean and variance of $\epsilon\gamma^+$ are $\epsilon\mu_{\gamma^+}$ and $\epsilon^2\sigma^2_{\gamma^+}$. Since data symbols $\{q_{l,k}\}$ are independent of each other and have the same distribution, the distribution of $\hat{a}_l$ will be approximately normally distributed according to the central limit theorem [57]. Therefore, the distribution of $\hat{a}_l$ is a normal distribution $\mathcal{N}(\epsilon P\mu_{\gamma^+}, \epsilon^2 P\sigma^2_{\gamma^+})$ for $P \gg 1$.

Under the condition that $a_0 = 1$, the probability of the error estimation of $\hat{a}_l$ is

$$\begin{aligned}&p(\hat{a}_l < 0 | a_l = +1) \\ &= \int_{-\infty}^{0} \frac{1}{\sqrt{2\pi\epsilon^2 P\sigma^2_{\gamma^+}}} \exp\left[-\frac{(x-\epsilon P\mu_{\gamma^+})^2}{2\epsilon^2 P\sigma^2_{\gamma^+}}\right] dx \\ &= \frac{1}{2}\operatorname{erfc}\left(\mu_{\gamma^+}\sqrt{\frac{P}{2\sigma^2_{\gamma^+}}}\right)\end{aligned} \tag{3–21}$$

where

$$\operatorname{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^{\infty} \exp(-t^2)dt \tag{3–22}$$

For $a_l = -1$, with similar notations μ_{γ^-} and $\sigma^2_{\gamma^-}$ and using the same procedure, we have:

$$\begin{aligned} & p(\hat{a}_l > 0 | a_l = -1) \\ & = \int_0^\infty \frac{1}{\sqrt{2\pi\epsilon^2 P \sigma^2_{\gamma^-}}} \exp\left[-\frac{(x - \epsilon P \mu_{\gamma^-})^2}{2\epsilon^2 P \sigma^2_{\gamma^-}}\right] dx \\ & = 1 - \frac{1}{2}\operatorname{erfc}\left(\mu_{\gamma^-}\sqrt{\frac{P}{2\sigma^2_{\gamma^-}}}\right) \\ & = \frac{1}{2}\operatorname{erfc}\left(\mu_{\gamma^+}\sqrt{\frac{P}{2\sigma^2_{\gamma^+}}}\right) \end{aligned} \tag{3–23}$$

since $\mu_{\gamma^-} = -\mu_{\gamma^+}$ and $\sigma^2_{\gamma^-} = \sigma^2_{\gamma^+}$. The bit error rate of estimation of the symbol a_l is:

$$\begin{aligned} P_b^a &= p(\hat{a}_l > 0 | a_l = -1) p(a_l = -1) \\ &+ p(\hat{a}_l < 0 | a_l = +1) p(a_l = +1) \\ &= \frac{1}{2}\operatorname{erfc}\left(\mu_{\gamma^+}\sqrt{\frac{P}{2\sigma^2_{\gamma^+}}}\right) \end{aligned} \tag{3–24}$$

3.6 Spread Sequence Estimation

To recover the PN sequence in (3–6), we use a matched filter operation between the synchronized intercepted signal $\mathbf{y}^0$ in (3–7) and the estimated data symbols $\hat{\mathbf{a}}$ in (3–15). That is:

$$\hat{\mathbf{c}} = \operatorname{sgn}\left(< \mathbf{y}^0, \hat{\mathbf{a}} >\right) \tag{3–25}$$

where $\langle \cdot, \cdot \rangle$ denotes inner product, $\hat{\mathbf{a}} = [\hat{a}_0, \cdots, \hat{a}_{L-1}]^T$ is a vector of the estimated symbol, and $\hat{\mathbf{c}} = [\hat{c}_0, \cdots, \hat{c}_{P-1}]^T$ stands for a vector of the estimated spread sequence. The sign of the sequence in (3–25) can also be reversed by a multiplicative factor in (3–15).

To analyze the performance of the sequence estimator in (3–25), we use the same Gaussian approximation method in Section 3.5. The sequence estimator (3–25) can be

rewritten as follows:

$$\begin{aligned}\hat{c}_k &= \sum_{l=0}^{L-1} y_{l,k} \cdot \hat{a}_l \\ &= \sum_{l=0}^{L-1} (a_l h_{l,k} + n_{l,k}) \cdot \hat{a}_l\end{aligned} \tag{3–26}$$

Let $\omega_{l,k} = y_{l,k}\bar{a}_l$, and $h_{l,k} = c_k$ for simplicity. Assume $c_k = 1$ for generality. Then we have:

$$\begin{aligned}\omega_{l,k} &= (a_l c_k + n_{l,k})\,\hat{a}_l \\ &= a_l \left(c_k + \frac{n_{l,k}}{a_l}\right)\hat{a}_l \\ &= \sqrt{\epsilon}\,(1 + \sigma\bar{n}_{l,k})\,\hat{a}_l\end{aligned} \tag{3–27}$$

where $\sigma^2 = \sigma_n^2/\epsilon$, $\epsilon = |a_l|^2$. Let $u^+ = 1 + \sigma\bar{n}_{l,k}$, $\gamma^+ = \bar{a}_l$, and $w^+ = u^+\gamma^+$. Since $\bar{n}_{l,k} \sim \mathcal{N}(0,1)$, $u^+ \sim \mathcal{N}(1,\sigma^2)$. We need to find a marginal probability density $f(w^+)$ which is a product of two normal distributions as (3–18):

$$f(w^+) = \int_{-\infty}^{\infty} f(w^+|\gamma^+) f(\gamma^+) d\gamma^+ \tag{3–28}$$

Let μ_{w^+} denote the mean and $\sigma_{w^+}^2$ denote the variance of w^+. Since u^+ and γ^+ are independent, the mean and variance of w^+ are:

$$\begin{aligned}\mu_{w^+} &= \mathbf{E}[u^+\gamma^+] \\ &= \mathbf{E}[u^+]\mathbf{E}[\gamma^+] = \mu_{u^+}\mu_{\gamma^+} = 1\end{aligned} \tag{3–29}$$

$$\begin{aligned}\sigma_{w^+}^2 =& \mathbf{E}[(u^+\gamma^+)^2] - (\mathbf{E}[u^+\gamma^+])^2 \\ =& \mathbf{E}[(u^+)^2]\mathbf{E}[(\gamma^+)^2] - \mu_{u^+}^2\mu_{\gamma^+}^2 \\ =& \mu_{u^+}^2\sigma_{\gamma^+}^2 + \mu_{\gamma^+}^2\sigma_{u^+}^2 + \sigma_{u^+}^2\sigma_{\gamma^+}^2 \\ =& 3\sigma^2 + 3\sigma^4 + \sigma^6\end{aligned} \tag{3–30}$$

Therefore, the mean and variance of $\sqrt{\epsilon}w^+$ are $\sqrt{\epsilon}\mu_{w^+}$ and $\epsilon\sigma_{w^+}^2$. Since the sequence $\{\omega_{l,k}\}$ is independent of each other and has the same distribution, the distribution of $\hat{c}_k$ will be

approximately normally distributed according to the central limit theorem [57]. Therefore, the distribution of $\hat{c}_k$ is a normal distribution $\mathcal{N}(\sqrt{\epsilon}L\mu_{w^+}, \epsilon L\sigma^2_{w^+})$ for $L \gg 1$.

Under the condition that $c_k = 1$, the probability of the error estimation of $\hat{c}_k$ is:

$$\begin{aligned} &p(\hat{c}_k < 0 | c_k = +1) \\ &= \int_{-\infty}^{0} \frac{1}{\sqrt{2\pi\epsilon L\sigma^2_{w^+}}} \exp\left[-\frac{(x-\sqrt{\epsilon}L\mu_{w^+})^2}{2\epsilon L\sigma^2_{w^+}}\right] dx \\ &= \frac{1}{2}\,\mathrm{erfc}\left(\mu_{w^+}\sqrt{\frac{L}{2\sigma^2_{w^+}}}\right) \end{aligned} \tag{3–31}$$

For $c_k = -1$, with similar notations μ_{w^-} and $\sigma^2_{w^-}$ and using the same procedure, we have:

$$\begin{aligned} &p(\hat{c}_k > 0 | c_k = -1) \\ &= \int_{-\infty}^{0} \frac{1}{\sqrt{2\pi\epsilon L\sigma^2_{w^-}}} \exp\left[-\frac{(x-\sqrt{\epsilon}L\mu_{w^-})^2}{2\epsilon L\sigma^2_{w^-}}\right] dx \\ &= \frac{1}{2}\,\mathrm{erfc}\left(\mu_{w^+}\sqrt{\frac{L}{2\sigma^2_{w^+}}}\right) \end{aligned} \tag{3–32}$$

since $\mu_{w^-} = -\mu_{w^+}$ and $\sigma^2_{w^-} = \sigma^2_{w^+}$.

The probability of error P_b^c in estimation of the sequence c_k is:

$$\begin{aligned} P_b^c &= p(\hat{c}_k \neq c_k) \\ &= p(\hat{c}_k > 0 | c_k = -1)p(c_k = -1) \\ &+ p(\hat{c}_k < 0 | c_k = +1)p(c_k = +1) \\ &= \frac{1}{2}\,\mathrm{erfc}\left(\mu_{w^+}\sqrt{\frac{L}{2\sigma^2_{w^+}}}\right) \end{aligned} \tag{3–33}$$

Note that the probability of error in (3–24) and (3–33) does not account for the polarity error. We will address this problem in the succeeding section.

3.7 Identification of Generator Polynomial

It is expensive to save hundreds or thousands of sequence bits, say $\hat{\mathbf{c}} = [\hat{c}_0, \cdots, \hat{c}_{P-1}]^T$, in the memory of the eavesdropper. This motivates us to estimate a generator polynomial of the estimated spread sequence from (3–25).

Shift registers are the practical and efficient implementation for the spread sequence. We considered a linear feedback shift register (LFSR) as the implementation technique for PN sequence. The correct selection of the n-tuple tap-weights (or n feedback stages) will result in a maximal sequence of the length $N = 2^n - 1$ [4, 16].

Let $F = GF(q)$ where q is a prime or a power of a prime where GF[2] denotes a finite field and q is called the order of the field F [4]. If the feedback function $f(x_0, \cdots, x_{n-1})$ is a linear function; that is, if it can be expressed as

$$\begin{aligned} f(x_0, \cdots, x_{n-1}) = \\ w_0 x_0 + \cdots + w_{n-1} x_{n-1}, \quad w_i \in F \end{aligned} \tag{3–34}$$

where w_i denotes a tap weight of the LFSR for $i = 0, \cdots, n-1$ over F. Then, sequences have the linear recursion relation [4]:

$$c_{k+n} = \sum_{i=0}^{n-1} w_i c_{k+i}, \quad k = 0, 1, 2, \ldots \tag{3–35}$$

If we have $2n$ successive sequence bits, we can estimate the generator polynomial of sequence $\mathbf{c} = (c_0, \cdots, c_{P-1})$ over $F = GF(q)$. We may rewrite the recursion relation (3–35) into the following matrix representation [4]:

$$\begin{bmatrix} c_n \\ c_{n+1} \\ \vdots \\ c_{2n-1} \end{bmatrix} = \begin{bmatrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_1 & c_2 & \cdots & c_n \\ \vdots & \ddots & \ddots & \vdots \\ c_{n-1} & c_n & \cdots & c_{2n-2} \end{bmatrix} \begin{bmatrix} w_0 \\ w_1 \\ \vdots \\ w_{n-1} \end{bmatrix} \tag{3–36}$$

We can solve the recursion relation in (3–36) over $GF(q)$ to obtain tap weights $\mathbf{w} = (w_0, \cdots, w_{n-1})$. The next successive sequence bit can be generated and tested with the estimated tap weights $\hat{\mathbf{w}}$ and n successive sequences using transform matrix M of LFSR as

[2] Finite fields are called Galois fields. See [4].

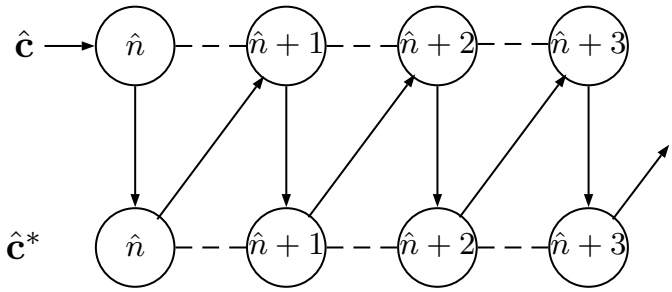


Figure 3-3. A graphical illustration of the zigzag estimator where $\hat{n} = \lfloor \log_2(P+1) \rfloor$ and $\hat{\mathbf{c}}^* = -\operatorname{sgn}(\hat{\mathbf{c}})$

follows [4]:

$$M = \begin{bmatrix} 0 & 0 & \cdots & 0 & \hat{w}_0 \\ 1 & 0 & \cdots & 0 & \hat{w}_1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \hat{w}_{n-1} \end{bmatrix} \tag{3–37}$$

and

$$\begin{aligned} &(\hat{c}_{k+1}, \hat{c}_{k+2}, \cdots, \hat{c}_{k+n}) \\ &\quad = (\hat{c}_0, \hat{c}_1, \cdots, \hat{c}_{n-1}) M^{k+1} \end{aligned} \tag{3–38}$$

Note that $det(M) = (-1)^n \hat{w}_0$ and thus M is invertible if and only if $\hat{w}_0 \neq 0$.

The method we propose is called a "*zigzag estimator*" which searches for a generator polynomial primarily based on (3–36) and (3–38) from the estimated sequence $\hat{\mathbf{c}}$ in (3–25), and also corrects the polarity error in the estimated sequence $\hat{\mathbf{c}}$ and data symbol $\hat{\mathbf{a}}$. A graphical representation of the zigzag estimator is given in Figure 3-3. A fundamental idea in correcting signs of the estimated sequence is that the zigzag estimator returns the non-sign reversed sequence if the zigzag estimator can find a code generator polynomial from the estimated sequence $\hat{\mathbf{c}}$. Let us introduce some mathematical notations. Let $\mathbf{c} = (c_0, c_1, \cdots)$ be the set of sequence or symbols. Let $\hat{\mathbf{c}}$ denote the estimated version of $\mathbf{c}$ and $\mathbf{c}^*$ be the sign-flipped version of $\mathbf{c}$, i.e., $\mathbf{c}^* = -\operatorname{sgn}(\mathbf{c})$. Let $\lfloor n \rfloor$ denote the nearest

integer less than or equal to n. Following is an algorithm for the zigzag estimator. Note that we do not claim the algorithm herein is optimal or sub-optimal.

Step 1 Estimate $\hat{\mathbf{c}}$ by (3–25). Store $\mathbf{s} \leftarrow \hat{\mathbf{c}}$ ($\mathbf{s}$ temporal memory of $\hat{\mathbf{c}}$). Initialize TestFlag $\leftarrow 0$, FlipCount $\leftarrow 0$, and $\hat{n} \leftarrow \lfloor \log_2(P+1) \rfloor$

Step 2 Estimate $\hat{f}_{\hat{n}}(x)$ by (3–36).

Step 3 Generate $2\hat{n}$ successive $\hat{\alpha}_i$ by (3–38). Increase FlipCount$\leftarrow$ FlipCount+1.

Step 4 Test $\hat{c}_i = \hat{\alpha}_{i,i=2\hat{n},\cdots,4\hat{n}-1}$.

(4a) If $\hat{c}_i = \hat{\alpha}_{i,i=2\hat{n},\cdots,4\hat{n}-1}$, set TestFlag $\leftarrow 1$ and go to (Step 6).

(4b) If $\hat{c}_i \neq \hat{\alpha}_{i,i=2\hat{n},\cdots,4\hat{n}-1}$, set TestFlag $\leftarrow 0$ and go to (Step 5).

Step 5 If TestFlag=0, flip the sequence $\hat{\mathbf{c}} \leftarrow \hat{\mathbf{c}}^*$

(5a) If FlipCount=1, increase FlipCount$\leftarrow$ FlipCount+1. Go to (Step 2).

(5b) If FlipCount=2, increase $\hat{n} \leftarrow \hat{n}+1$ and reset FlipCount $\leftarrow 0$. Go to (Step 2).

Step 6 Check polarity errors. If $\mathbf{s} \neq \hat{\mathbf{c}}$, $\hat{\mathbf{c}} \leftarrow \hat{\mathbf{c}}^*$. Store $\hat{\mathbf{c}}_{zigzag} \leftarrow \hat{\mathbf{c}}$.

Note that the method proposed in this section can also be applied to Gold codes. Some pairs of m-sequences with the same degree can be used to generate Gold Codes by linearly combining two m-sequences with different offsets in Galois field. If the estimated generator polynomial can be decomposed into two preferred pairs of m-sequence, we can decompose the estimated generator polynomial into two m-sequences. For example, a Gold code generator $f(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ can be factored into $f_1(x) = 1 + x + x^3$ and $f_2(x) = 1 + x^2 + x^3$[3] .

Finally, we use a matched filter operation between the intercepted signal $\mathbf{y}^s$ and the sign corrected estimated sequence $\hat{\mathbf{c}}_{zigzag}$ in (Step 6). That is:

$$\hat{\mathbf{a}}_{zigzag} = \text{sgn}\left(< \mathbf{y}^0, \hat{\mathbf{c}}_{zigzag} >\right) \tag{3–39}$$

[3] See 4.4 Decomposition of LFSR sequences in [4].

Table 3-2. Relationship among $\Pr(K=k)$ in (3–45), $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle$, and $\frac{1}{2}\operatorname{erfc}\left(\sqrt{\rho_{Ev}}\right)$ in (3–47) where k denotes the number of errors in the estimation of the spread sequence of the non-zigzag method.

k	0	1	$\cdots$	P
$\langle \mathbf{c}, \hat{\mathbf{c}} \rangle$	P	$P-2$	$\cdots$	$-P$
$\frac{1}{2}\operatorname{erfc}\left(\sqrt{\rho_{Ev}}\right)$	$\frac{1}{2}\operatorname{erfc}\left(P\sqrt{\frac{1}{2\sigma^2 P}}\right)$	$\frac{1}{2}\operatorname{erfc}\left((P-2)\sqrt{\frac{1}{2\sigma^2 P}}\right)$	$\cdots$	$\frac{1}{2}\operatorname{erfc}\left(-P\sqrt{\frac{1}{2\sigma^2 P}}\right)$
$\Pr(K=k)$	$f(0;P,P_b^c)$	$f(1;P,P_b^c)$	$\cdots$	$f(P;P,P_b^c)$

However,

$$\hat{\mathbf{a}}_{non-zigzag} = \operatorname{sgn}\left(< \mathbf{y}^0, \hat{\mathbf{c}} >\right) \tag{3–40}$$

Now we are ready to find the probability of error of the zigzag estimator in (3–39). First, we will find the probability of error of the symbol detector without the zigzag estimator of (3–40). After that, the probability of the symbol detector by the zigzag estimator (3–39) will be analyzed. A symbol detector of a cooperative receiver (Rx) can be written as follows:

$$\begin{aligned}\hat{\mathbf{a}} &= \operatorname{sgn}\left(\langle \mathbf{y}, \mathbf{c} \rangle\right) = \operatorname{sgn}\left(\langle \mathbf{c}\mathbf{a} + \sigma\bar{\mathbf{n}}, \mathbf{c} \rangle\right) \\ &= \operatorname{sgn}\left(\mathbf{a}\langle \mathbf{c}, \mathbf{c} \rangle + \sigma\langle \bar{\mathbf{n}}, \mathbf{c} \rangle\right)\end{aligned} \tag{3–41}$$

where $\bar{\mathbf{n}} \sim \mathcal{N}(0,1)$. Then, signal-to-noise ratio ρ_{Rx} of the cooperative receiver is:

$$\rho_{Rx} = \frac{\langle \mathbf{c}, \mathbf{c} \rangle^2}{\sigma^2 \|\mathbf{c}\|^2} = \frac{P}{\sigma^2} \tag{3–42}$$

Therefore, the probability of error of the cooperative receiver with the known spread sequence $\mathbf{c}$ is [58]:

$$P_{b,Rx}^a = \frac{1}{2}\operatorname{erfc}\left(\sqrt{\frac{P}{2\sigma^2}}\right) \tag{3–43}$$

However, signal-to-noise ratio ρ_{Ev} of the eavesdropper (Ev) is:

$$\rho_{Ev} = \frac{\langle \mathbf{c}, \hat{\mathbf{c}} \rangle^2}{\sigma^2 \|\hat{\mathbf{c}}\|^2} = \frac{\langle \mathbf{c}, \hat{\mathbf{c}} \rangle^2}{\sigma^2 P} \tag{3–44}$$

In Section 3.6, we find the probability of error P_b^c in the estimation of each chip in

(3–33). The number of incorrect estimations of each chip c_k in the spread sequence $\mathbf{c}$ is an independent yes/no experiment with a fail probability P_b^c. Let K denote the number of errors in the estimation of the spread sequence $\mathbf{c}$ of the length P. Then, we can write $K \sim \mathcal{B}(P, P_b^c)$. The probability of getting exactly k errors in the estimation of the spread sequence $\mathbf{c}$ with the length of P is given by:

$$\begin{aligned} \Pr(K = k) &= f(k; P, P_b^c) \\ &= \begin{pmatrix} P \\ k \end{pmatrix} (P_b^c)^k (1 - P_b^c)^{P-k} \end{aligned} \tag{3–45}$$

for $k = 0, 1, 2, \cdots, P$ with the binomial coefficient

$$\begin{pmatrix} P \\ k \end{pmatrix} = \frac{P!}{(P-k)!k!} \tag{3–46}$$

If there is no error in the estimation of the spread sequence $\mathbf{c}$, i.e., $\mathbf{c} = \hat{\mathbf{c}}$ or $k = 0$, $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P$ and $\rho_{Ev}(K = 0) = 1/\sigma^2$. If there is only one error in the estimation of the spread sequence $\mathbf{c}$, i.e., $k = 1$, $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P - 2$ and $\rho_{Ev}(K = 1) = (P-2)^2/(\sigma^2 P)$. Table 3-2 shows the relationship among $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle$, ρ_{Ev} and $\Pr(K = k)$ in (3–47) and (3–45). Therefore, the probability of error in the estimation of symbol without the zigzag estimator can be written as follows:

$$\begin{aligned} &P^a_{b,non-zigzag} = \\ &\sum_{k=0}^{P} \frac{1}{2} \operatorname{erfc}\left((P-2k)\sqrt{\frac{1}{2\sigma^2 P}} \right) \Pr(K = k) \end{aligned} \tag{3–47}$$

Since $f(k; P, P_b^c) = f(P-k; P, 1-P_b^c)$, the probability of k errors in the estimation of the spread sequence is the same as that of $P - k$ correct estimations of the spread sequence. Let Q denote the number of correct estimations of the spread sequence and $q = P - k$. If

the length of the spread sequence P is odd,

$$P^{a,odd}_{b,non-zigzag} = \sum_{k=0}^{\lfloor P/2 \rfloor} \frac{1}{2} \operatorname{erfc}\left((P-2k)\sqrt{\frac{1}{2\sigma^2 P}}\right) f(k; P, P_b^c) + \sum_{q=0}^{\lfloor P/2 \rfloor} \frac{1}{2} \operatorname{erfc}\left((2q-P)\sqrt{\frac{1}{2\sigma^2 P}}\right) f(q; P, 1-P_b^c) \tag{3–48}$$

If P is even,

$$P^{a,even}_{b,non-zigzag} = \sum_{k=0}^{P/2-1} \frac{1}{2} \operatorname{erfc}\left((P-2k)\sqrt{\frac{1}{2\sigma^2 P}}\right) f(k; P, P_b^c) + \binom{P}{P/2} (P_b^c)^{P/2}(1-P_b^c)^{P/2} + \sum_{q=0}^{P/2-1} \frac{1}{2} \operatorname{erfc}\left((2q-P)\sqrt{\frac{1}{2\sigma^2 P}}\right) f(q; P, 1-P_b^c) \tag{3–49}$$

The meanings of (3–48) and (3–49) are (i) the probability distribution of $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle$ is symmetric, (ii) the probability distribution of $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle > 0$ follows $f(k; P, P_b^c)$, and (iii) the probability distribution of $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle < 0$ follows $f(q; P, 1-P_b^c)$.

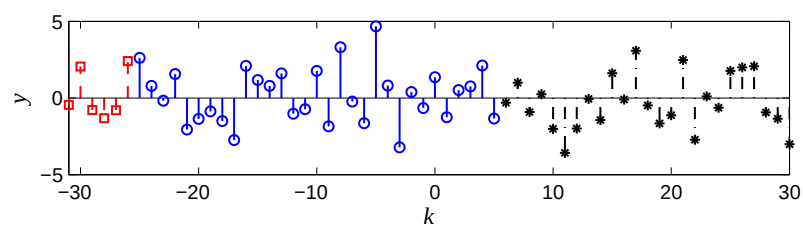
The zigzag estimator in (3–39) can identify the PN code generator polynomial to correct the polarity error in the estimation of the spread sequence if $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = -P$ or $k = P$ or $q = 0$. Then, the probability of error in the estimation of symbols with the zigzag estimator $P^a_{b,zigzag}$ is:

$$P^a_{b,zigzag} = \sum_{k=0}^{P-1} \frac{1}{2} \operatorname{erfc}\left((P-2i)\sqrt{\frac{1}{2\sigma^2 P}}\right) \Pr(K=k) + \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{P}{2\sigma^2}}\right) \Pr(K=P) \tag{3–50}$$

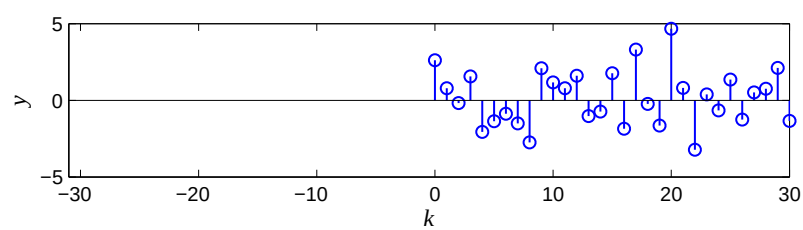
The probability of error of (3–50) by the zigzag estimator is enhanced by a factor of two, compared to (3–47) without the zigzag estimator, if the zigzag estimator can estimate a code generator polynomial. We will validate the probability of error of the symbol detector in (3–39) and (3–40) in the following Section 3.8.

3.8 Simulation and Validation

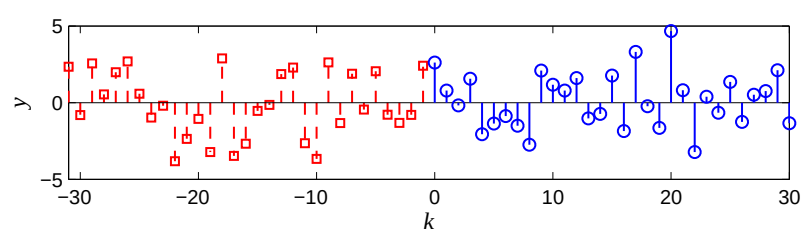
In this section, we present a complete simulation example to illustrate our approaches. We consider information symbols modulated by an m-sequence with the generator polynomial $f(x) = 1 + x^2 + x^5$ of length $N = P = 31$. Signal constellation is BPSK and the number of data symbols is $L = 128$. The received signal is corrupted by AWGN noise with SNR=-10dB. We assume the sampling rate of an eavesdropper is the chip rate T_c, however this is not required by our method.



A Desynchronized signal $\mathbf{y}_0^{k=26}$

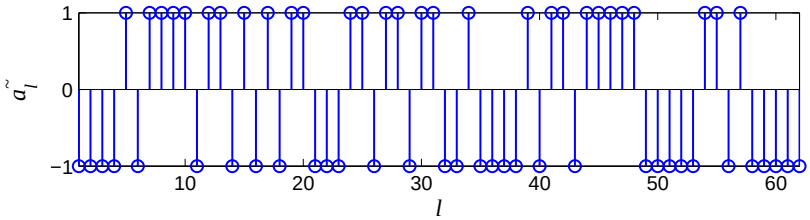


B Synchronized signal $\mathbf{y}_0^0$

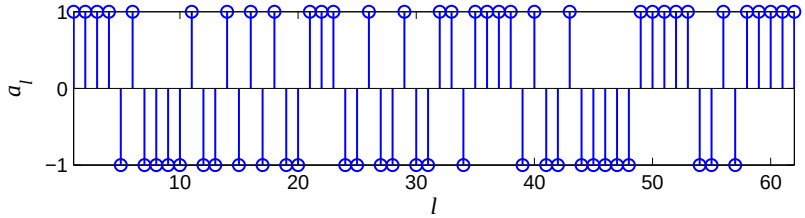


C True signal $\mathbf{y}$

Figure 3-4. Symbol synchronization by the spectral norm where the dashed □ denotes a_{-1}, the solid ∘ denotes a_0, the dashed-dotted ∗ denotes a_1, respectively

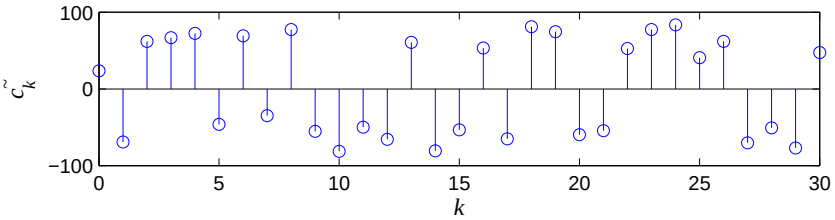


A Estimated data symbols $\hat{\mathbf{a}}$

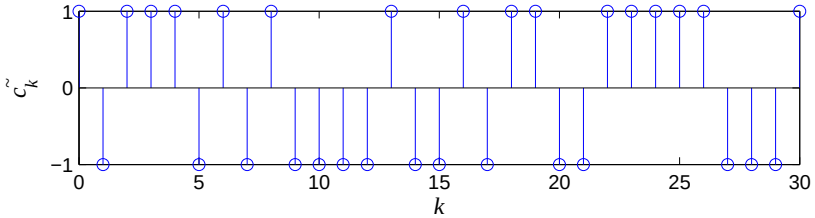


B True data symbols $\mathbf{a}$

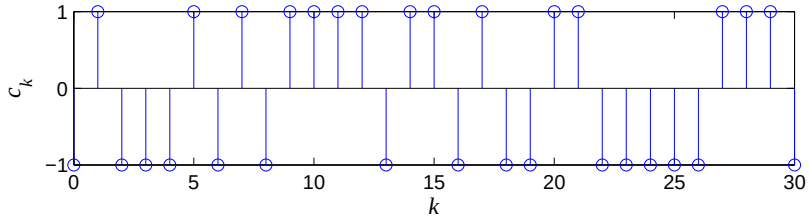
Figure 3-5. Data symbols estimation by (3–15)



A Noisy estimated sequence $\hat{\mathbf{c}}$

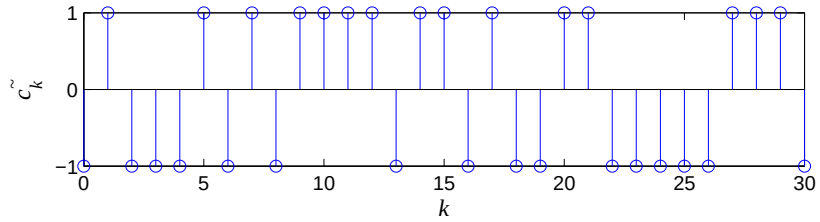


B Estimated sequence sgn $(\hat{\mathbf{c}})$

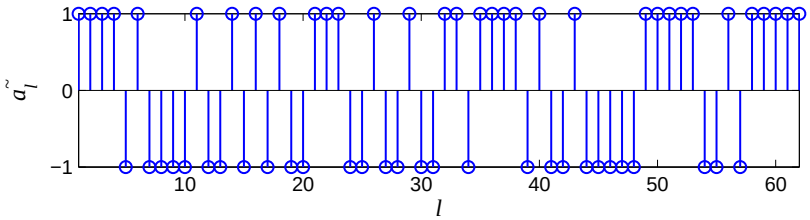


C True sequence $\mathbf{c}$

Figure 3-6. Spread sequence estimation by (3–25)



A Sign corrected sequence $\hat{\mathbf{c}}$



B Sign corrected data symbol $\hat{\mathbf{a}}$

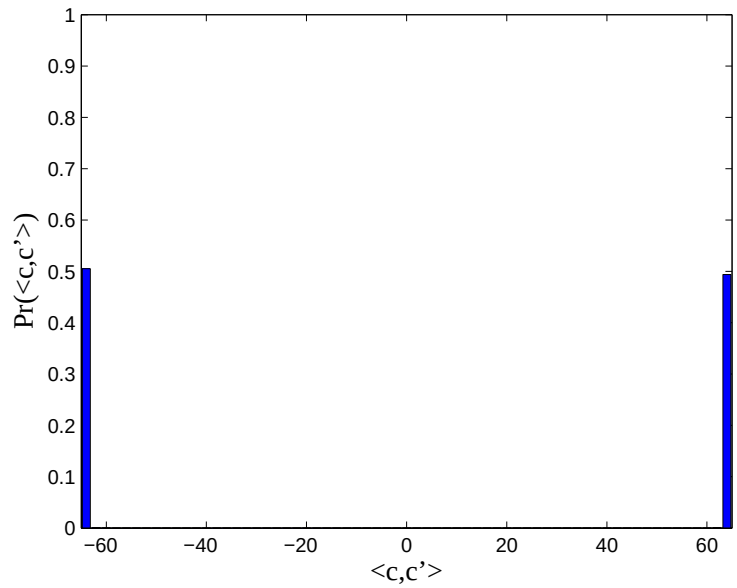
Figure 3-7. Sign correction by the zigzag estimator

First, we need to determine a synchronized version of the intercepted signal by (3–12). Figure 3-4(a) shows a desynchronized signal $\mathbf{y}^{k=26}$ delayed by $26T_c$. Therefore, a sample window $\mathbf{y}_{-1}^{k=26}$ contains the end of a symbol a_{-1} for a duration of $5T_c$ followed by the beginning of next symbol signal a_0 for a duration $26T_c$. A synchronized signal $\mathbf{y}_0^{k=0}$ by (3–12) is shown in Figure 3-4(b). Note that the desynchronized samples which belong to a_{-1} are truncated. Figure 3-4(c) shows two synchronized sample windows for the purpose of comparison.

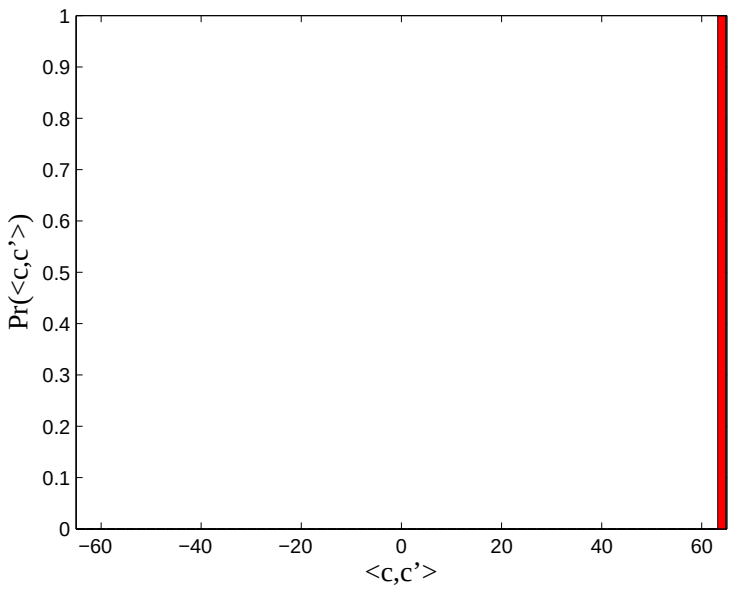
Second, estimations of data symbols and spread sequences are followed by the symbol synchronization. Figure 3-5 shows the first 62 estimated data symbols $\hat{\mathbf{a}}$ by (3–15). Figure 3-6 shows the noisy estimated sequence $\hat{\mathbf{c}}$ by (3–25). Note that the estimated data $\hat{\mathbf{a}}$ in Figure 3-5(a) and the estimated sequence in Figure 3-6(b) are sign reversed versions of the true symbol $\mathbf{a}$ and the true sequence $\mathbf{c}$, respectively. Therefore, $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = -P$. We can correct polarity errors in the estimated data symbol $\hat{\mathbf{a}}$ and the spread sequence $\hat{\mathbf{c}}$ by the proposed zigzag estimator.

Third, we can correct polarity errors in the estimated data symbol $\hat{\mathbf{a}}$ and the spread sequences $\hat{\mathbf{c}}$ by the zigzag estimator. The zigzag estimator in Section 3.7 searches and

tests a generator polynomial from the estimated sequence $\hat{\mathbf{c}}$ by the recursion relation in (3–36) and the transform matrix in (3–37). Figure 3-7 shows the sign corrected sequence $\hat{\mathbf{c}}_{zigzag}$ and data symbol $\hat{\mathbf{a}}_{zigzag}$ by the proposed zigzag estimator. We also conduct a



A Without the zigzag estimator



B With the zigzag estimator

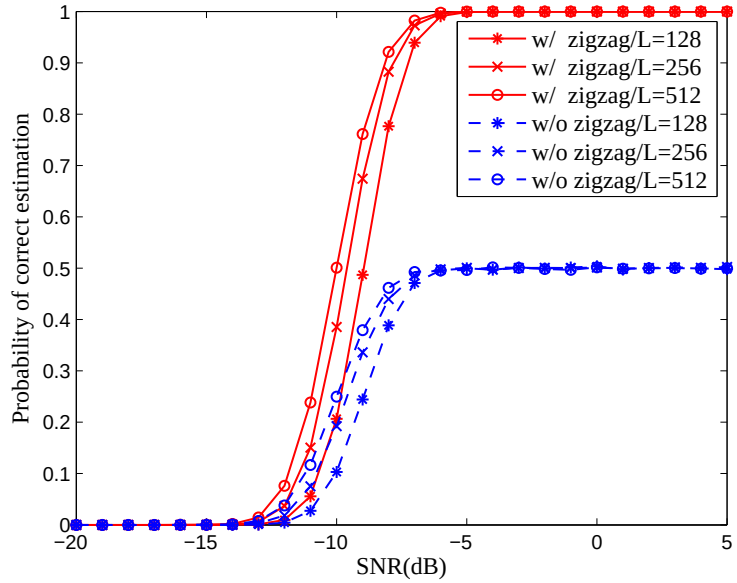
Figure 3-8. Histogram of $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle$ with $P = 64$, $L = 128$, and SNR=-5dB

simulation to evaluate the performance of the proposed zigzag estimator. The generator polynomial used in this simulation is an m-sequence with $f(x) = 1 + x + x^{11} + x^{12} + x^{14}$ and the sequence is truncated, $P < N = 2^n - 1$ for comparison. We randomly seed initial conditions and randomly generate data symbols corrupted by AWGN noise. The signal constellation is BPSK. 10,000 simulation trials are carried out and averaged.

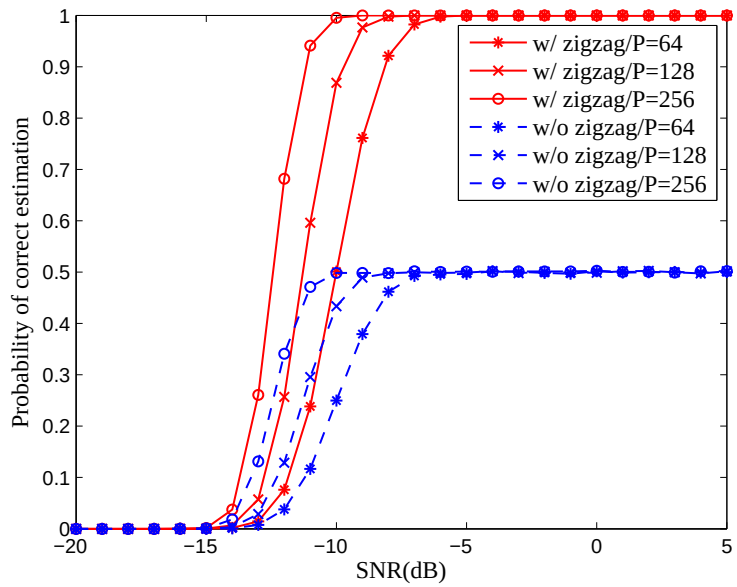
First, we compare the histogram of $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle$ between with the zigzag estimator and without the zigzag estimator to verify the relation between (3–47) and (3–50). In this simulation, we use the number of data symbol $L = 128$, the length of the spread sequence $P = 64$, and SNR=-5dB. Figure 3-8 shows the comparison of histograms $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle$ between with the zigzag estimator and without the zigzag estimator. The horizontal axis is the value $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle$ and the vertical axis represents the normalized occurrence frequency of $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle$. The occurrence frequency of $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P$ is 0.9991 and 0.4939 for with the zigzag estimator and without the zigzag estimator, respectively. However, the occurrence frequency of $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = -P$ with the zigzag estimator and without the zigzag estimator is 0.0000 and 0.5052. The zigzag estimator in Section 3.7 can identify the PN code generator polynomial to correct the polarity error in the estimation of the spread sequence when $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = -P$. Therefore, the occurrence frequency $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P$ with the zigzag estimator is the sum of that of $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P$ and $\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = -P$ without the zigzag estimator. This validates the relation between (3–47) and (3–50).

Second, we compare $\Pr(\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P)$ between with the zigzag estimator and without the zigzag estimator in (3–47) and (3–50), respectively. Figure 3-9 shows the $\Pr(\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P)$ with different combinations of the number of data symbols L and the length of the spread sequence P. Note that the $\Pr(\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P)$ corresponds to $\Pr(K = 0)$ without the zigzag estimator and $\Pr(K = 0) + \Pr(K = P)$ with the zigzag estimator. The $\Pr(\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P)$ increases as the number of the intercepted symbols L increased and also increases as the length of the spread sequence P increased. Therefore, the $\Pr(\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P)$ obtained by the zigzag estimator is almost two times greater than that without our

proposed zigzag estimator. Third, we compare the simulated probability of error of the



A P =64, L =128, 256, 512

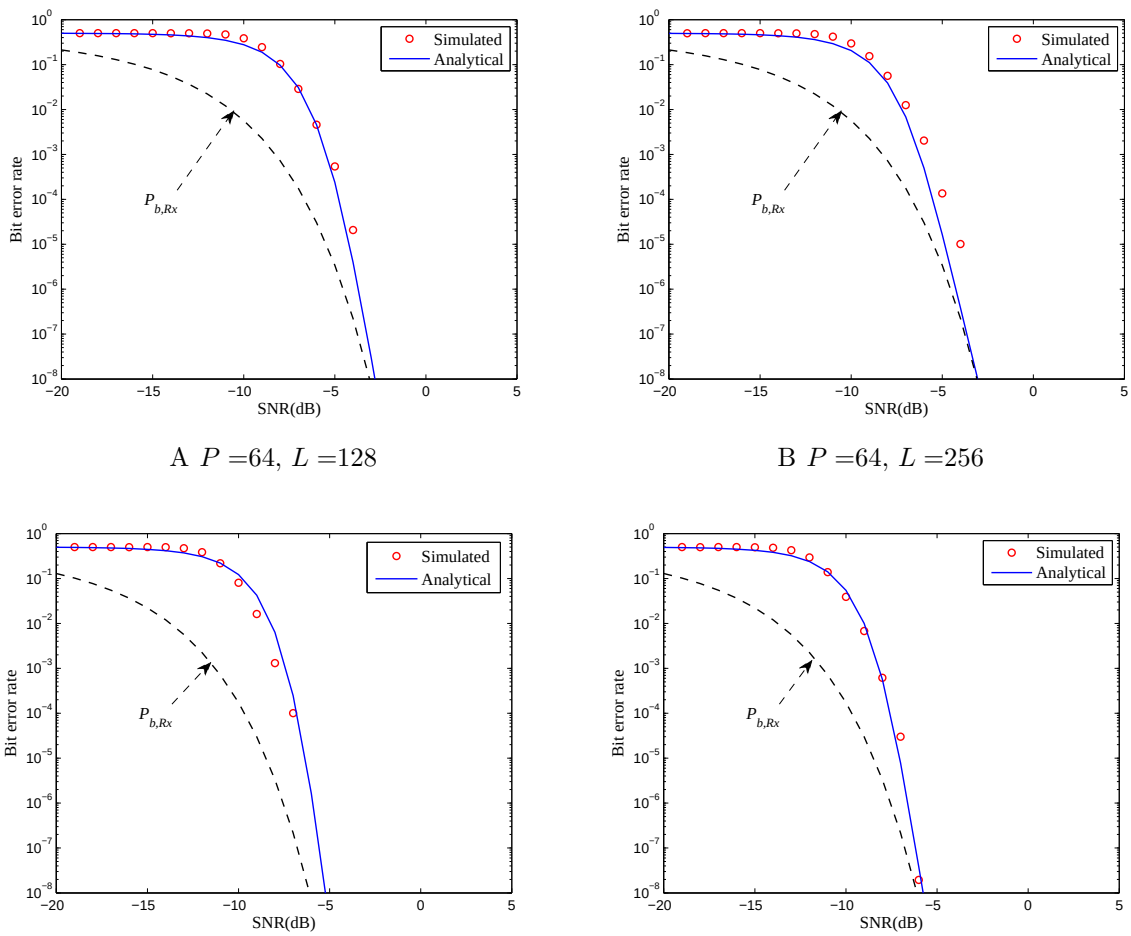


B L =512, P =64, 128, 256

Figure 3-9. Comparison of the probability of correct estimation of the spread sequence $\Pr(\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P)$

symbol detector in (3–39) and the analytical probability of error in (3–50). Figure 3-10 shows the $P^{a}_{b,zigzag}$ with different combinations of the number of data symbols L and the

length of the spread sequence P. Note that $P_{b,Rx}/P = 64$ denotes the probability of error of a cooperative receiver in (3–43) with $P = 64$ for comparison. The $P^a_{b,zigzag}$ is enhanced as the number of samples L increases and as the length of sequence P increases. Moreover, the analytical performance $P^a_{b,zigzag}$ of the symbol detector in (3–50) is almost the same as that of the simulated probability of error in (3–40). Since the simulated $\Pr(\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P) \simeq 1$ for $P = 64$, $L = 128$, SNR=-5dB in Figure 3-9 over 10,000 trials, $P^a_{b,zigzag} \simeq P_{b,Rx}$. Therefore, the analytical probability of error in (3–50) is a good approximation of the performance of an eavesdropper. This analytical performance can provide an efficient prediction of the performance of our proposed zigzag estimator. Finally, we conduct a



A P =64, L =128

B P =64, L =256

C P =128, L =256

D P =128, L =512

Figure 3-10. Comparison of the simulated and analytical probability of bit error $P^a_{b,zigzag}$ with the zigzag estimator in (3–50)

simulation with the n-tuple code generator polynomial to validate the performance of the proposed zigzag method with the long length sequence. The length of the spread sequence is $P = 2^n - 1$. We randomly seed initial conditions and randomly generate data symbols corrupted by AWGN noise with SNR $= -10$dB. The signal constellation is BPSK and 10,000 simulation trials are carried out and averaged. Figure 3-11 shows the probability of the correct estimation of the spread sequence $\Pr(\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P)$ with $n = 6, \cdots, 13$ with the number of data symbols $L = 256$. The $\Pr(\langle \mathbf{c}, \hat{\mathbf{c}} \rangle = P)$ increases as the length of the spread sequence $P = 2^n - 1$ increased.

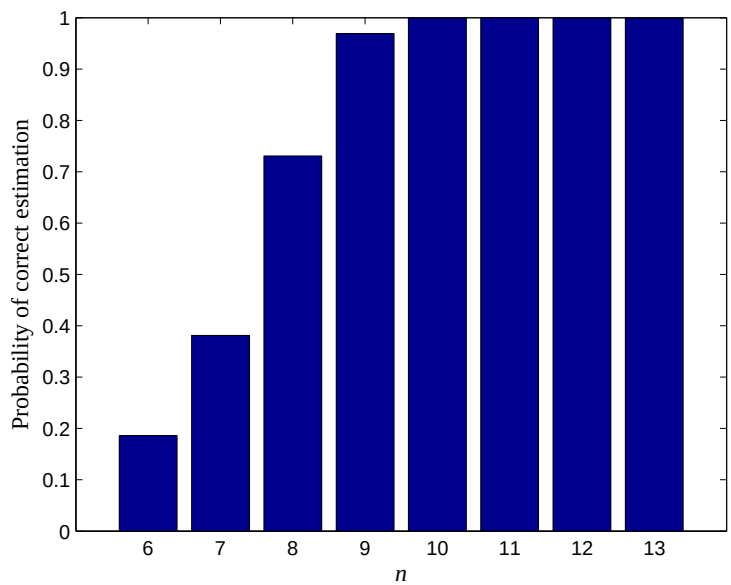


Figure 3-11. Probability of correct estimation of the spread sequence by the zigzag estimation with n-tuple generator polynomial, $P = 2^n - 1$, SNR=-10dB and L=256

3.9 Summary

In this chapter, we consider the problem of eavesdropping on the adversary's communication, which uses direct-sequence spread-spectrum (DS-SS). To intercept the adversary's communication, one needs to (a) identify the start position of a data symbol in the spread signal for symbol synchronization purpose, (b) remove the PN sequence, (c) estimate the PN sequence, and (d) estimate the generator polynomial. In

this chapter, we propose effective methods to address these four problems. To identify the start position of a data symbol, we developed a method that uses the spectral norm of the sample covariance matrix. After symbol synchronization, a method based on the cross-correlation was used to estimate data symbols up to an unknown multiplicative factor. These estimated symbols were used by a matched filtering operation for identifying the PN sequence from the intercepted signal. In addition to obtaining the PN sequence and the data symbols, we also proposed a zigzag estimator to identify the PN code generator polynomial and proposed a method to identify the polarity in the received signal. Our method improves the probability of correct estimation by a factor of two, compared to the previous method. We also analyze the probability of error of the zigzag estimator in terms of SNR, the number of intercepted data symbols, and the length of the spread sequence. Our validation by simulation and theoretical analysis show the effectiveness of our proposed method. Our proposed method can be used by an interceptor to eavesdrop on an adversary's communication. Other applications of our method include altering an adversary's information, isolating an adversary's communication link, and jamming by a denial-of-service (DoS) attack by our smart eavesdropper. Furthermore, our method can be used for the synchronization by estimating the received spread code by an intended receiver.

CHAPTER 4
ENHANCED TRANSFORM DOMAIN COMMUNICATION SYSTEM

4.1 Introduction

Both military and civilian parties desire reliable communication. Especially for the military communication system, it is very important to be able to operate in the presence of both intentional and unintentional interference. The primary objective of an interferer (jammer) is to degrade or disrupt communication system performance to the point where it is no longer considered reliable. Therefore, an important goal of communication research is to mitigate or avoid intentional interference (jamming).

Transform domain communication system (TDCS) [9, 11] provides a viable solution for interference avoidance. In the TDCS, an interference avoiding waveform is generated at the transmitter to avoid intentional interference, and the receiver needs to adapt its matched filter to match the transmitted waveform. Spectrally crowded regions are avoided altogether via adaptive spectral notching. Therefore, the foremost problem in the TDCS is accurate estimation of the spectral environment. The more accurate the estimation of the interference spectrum is, the better the performance the TDCS will achieve.

The TDCS [9, 11] utilized a parametric 10th-order autoregressive (AR) estimator to estimate the power spectral density (PSD) of the spectral environment. Since the AR-filter estimates the interference under the assumption that the interference process is stationary, the AR-estimator fails to provide accurate estimation under the non-stationary interference such as swept-tone jamming. For this reason, the TDCS based on the AR-estimator performed worse against the swept-tone interference, as compared to the case under the stationary interference.

To enhance the bit error rate (BER) performance of the TDCS under the non-stationary interference, the wavelet domain communication system (WDCS) [10] and the enhanced wavelet domain communication system (EWDCS) [19] were proposed in the literature. The WDCS and the EWDCS utilized a wavelet domain spectral estimator. The

WDCS used the concept of a wavelet periodogram for spectral estimation. However, the wavelet periodogram is not an accurate estimation of environment power spectral density and is not able to estimate a non-stationary interference. Thus, the WDCS [10] failed to mitigate a non-stationary interference like the swept-tone. However, the EWDCS used the evolutionary wavelet spectrum (EWS) which is related to the local auto-covariance through to auto-correlation of a wavelet. The BER performance of the EWDCS under a non-stationary interference was relatively sub-optimal compared to that under stationary interferences. Moreover, the BER performance of the EWDCS under stationary interferences was comparatively poorer than that of the TDCS under stationary interferences [19] under the same simulation environment.

To mitigate the problem of the TDCS [9, 11], WDCS [10], and EWDCS [19], we use a non-parametric spectral estimator, called Capon's method [59–61]. Capon's method (CM) for spectral estimation is based on a filter bank decomposition: the spectrum of a signal is estimated in each band by a simple filter design subject to some constraints and can provide fast speed of convergence. The CM has the ability to cope with a complicated interference environment in which the number of interfering sources is large. Combining the strength of the CM and aforementioned TDCS, we propose the enhanced transform domain communication system (ETDCS). The ETDCS will provide better bit error performance than the TDCS [9], WDCS [10], or EWDCS [19] for both the stationary interference and the non-stationary interference.

This chapter proposes the ETDCS which is a practical alternative for the TDCS with a non-parametric spectral estimation method. In Section 4.2, we elaborate on a mathematical model of TDCS. In Section 4.3, an overview of the TDCS architecture is given, and the limitation of the TDCS and the proposed estimation method are investigated. Effects of various jamming on the performance of ETDCS and comparative bit error performance analysis of the proposed ETDCS are followed in Section 4.4. Finally, Section 4.5 summarizes this chapter.

4.2 A Mathematical Model of TDCS

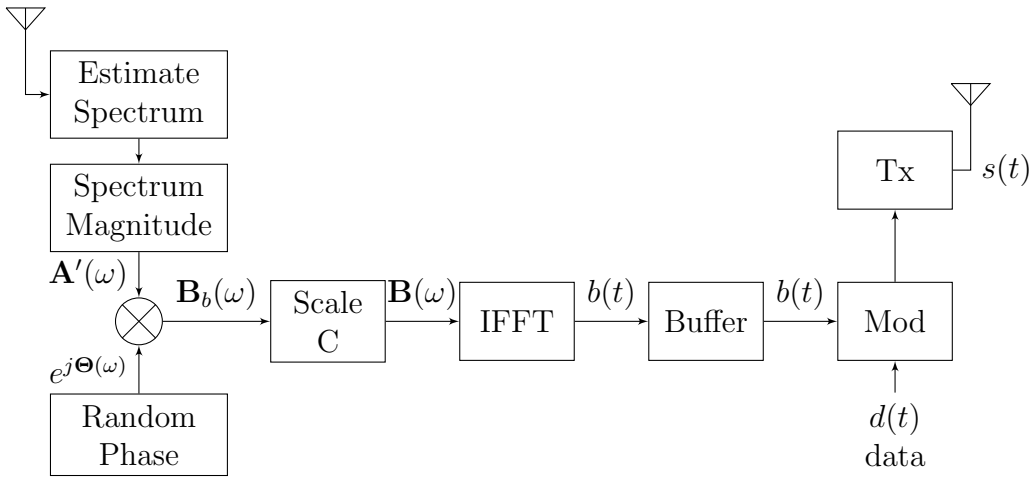


Figure 4-1. A block diagram of TDCS transmitter [9–11]

In this section, we elaborate on a mathematical model of the TDCS in [9–11], and analyze the bit error rate performance of the TDCS. The transmitter architecture of TDCS system is shown in Figure 4-1. The TDCS in [9–11] involves designing a waveform in the frequency domain rather than in the time domain (or wavelet domain) to avoid the interference. If the designed information-bearing waveform could avoid using bands occupied by interferences, the communication system would avoid the interference. Since the modulated information-bearing signal would have little or no spectrum at the interfered bands, it should not be affected by the interference and should not introduce new interference to other users. This interference avoiding concept serves as the basis for the TDCS design [9–11, 19].

We assume that the receiver and transmitter antennae experience the same spectral environment. Thus they can generate the same spectral estimation of the spectral environment. This assumption holds for short-range data communications. Scenarios in which the assumption is valid include vehicles or aircrafts grouped in tight formation under distant interference, or closely located secondary mobile users of an ad hoc network sharing the same spectrum with a primary user. For those scenarios where the assumption

might not be satisfied, we could assign a dedicated feedback channel to communicate the spectral estimation between the transmitter and receiver [19].

After estimation of the spectral environment, a band exceeds that of the noise level by a factor of a threshold level, interference is claimed to be present and the band is notched out, assigning value '0'. Otherwise, the bands are retained and set to the value '1'. That is:

$$A'(\omega) = \begin{cases} 0 \text{ if jammed} \\ 1 \text{ otherwise} \end{cases} \tag{4–1}$$

where $w = e^{j\frac{2\pi}{N}}$ is a primitive N^{th} root of unity. Consequently, an interference-free spectrum magnitude $A'(\omega)$ in Figure 4-1 is generated. After notching out the interferences, a multi-valued complex pseudo-random (PN) phase vector, $e^{j\Theta(\omega)}$, is generated from a linear feedback shift register (LFSR) identical in length to $A'(\omega)$ and multiplied element-by-element with $A'(\omega)$ in a process called *phase coding*, producing spectral vector, $B_b(\omega)$, with known amplitude and PN phase characteristics. The spectral vector $B_b(\omega)$ is then amplitude-scaled by constant C to ensure the communication symbol has the desired signal energy. Then we have:

$$B(\omega) = CA'(\omega)e^{j\Theta(\omega)} \tag{4–2}$$

The resultant spectral vector, $B(\omega)$, is inverse Fourier transformed to produce a time-domain *basis function*, $b(t)$, which is subsequently stored and modulated with data, $d(t)$. Let $B[k]$ denote a frequency domain representation of the basis function, $b(t)$ for $k = 0, \cdots, N-1$ where N is the number of FFT point. Then, we have:

$$b[n] = \sum_{k=0}^{N-1} B[k]e^{j\frac{2\pi k}{N}n} \tag{4–3}$$

This signature wave $b[n]$ stored into a buffer in Figure 4-1 and data modulated by $d(t)$.

An ith received signal at the receiver becomes:

$$\mathbf{r}^i = (-1)^{d_i}\mathbf{b} + \sigma_n\bar{\mathbf{n}} \tag{4–4}$$

where $d_i = 0$ or 1 for antipodal modulation and the noise $\bar{\mathbf{n}} \sim \mathcal{N}(0,1)$ is white and Gaussian. The noise power in a frequency band B_w is $2\sigma_n^2 B_w$.

Let $\mathbf{c}$ denotes the conjugate of the signature wave $\mathbf{b}$. An output of correlator at the receiver becomes:

$$< \mathbf{r}^i, \mathbf{c} > = < (-1)^{d_i}\mathbf{b}, \mathbf{c} > + \sigma_n < \bar{\mathbf{n}}, \mathbf{c} > \tag{4–5}$$

Then, the estimated data at the receiver becomes:

$$\hat{d}_i = \mathrm{sgn}(< \mathbf{r}^i, \mathbf{c} >) \tag{4–6}$$

If $A[k] = 1$ for $k = 0, \cdots, N-1$, the scale factor C becomes $1/\sqrt{N}$. Then, the signal-to-noise ratio becomes:

$$\gamma = \frac{\|\mathbf{b}\|^2}{\sigma_n^2} = \frac{1}{\sigma_n^2} = \frac{2E_b}{N_0} \tag{4–7}$$

Therefore, the bit error rate for the antipodal modulation becomes:

$$P_b = Q(\sqrt{\gamma}) = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{4–8}$$

where E_b is the average energy per bit and N_0 is the noise power density. The Q-function is the complementary error function.

4.3 Methodology

Spectral estimation is the first process and plays a major role in the TDCS. The transmitter first samples the electromagnetic environments over the system's operating bandwidth. Once sampled, the spectral content is estimated using any available techniques, e.g., periodogram, autoregressive (AR) linear predictive filtering, evolutionary wavelet spectrum, etc.

The TDCS [9, 11] used 10th-order AR-filter to estimate the spectral environment. The AR-filter used in the TDCS is a parametric estimation method. It fits an AR linear prediction filter model to the signal by minimizing the forward prediction error in the least square sense. Since the model in the AR-estimator did not fit the environments well

in the case of a non-stationary interference, the TDCS suffered significant performance degradation and failed to estimate the swept-tone interference. Therefore, the TDCS performance against swept-tone interference was shown to be sub-optimal by comparison with the other interference scenarios considered [9, 11].

The wavelet-based spectral estimations were found to be used in the WDCS [10] and the EWDCS [19]. The wavelet periodogram, comprised of the square of the wavelet coefficients, has been used in the WDCS to estimate the spectral environment. However, the wavelet periodogram is a noisy estimation of the environment's power distribution and hence can not estimate the non-stationary interference. The EWS used in the EWDCS addressed both the statistical and the non-stationary nature of the spectral estimation, however the EWDCS performance under swept-tone interference was shown to be relatively sub-optimal compared to other stationary interferences. Moreover, the bit error performance of the EWDCS under stationary interferences was comparatively poorer than that of the TDCS under stationary interferences [19]. Therefore, the spectral estimation techniques used in the TDCS, the WDCS, and the EWDCS, have their limitations.

There are basically two broad categories of the techniques for spectral estimation. One is the non-parametric approach based on the concept of bandpass filter. The other is the parametric method, which assumes a model for the data, and the spectral estimation becomes a problem of estimating the parameters in the assumed model. One of the most well-known non-parametric spectral estimation methods is Capon's approach, which is also known as minimum variance distortionless response (MVDR) [59–61]. At the stage of spectral estimation in the ETDCS, we used the Capon's method (CM) to estimate the interference environments. Capon's method for spectral estimation is primarily based on a filter bank decomposition: The spectrum of a signal is estimated in each band by a simple filter design subject with some constraints (Interested readers please refer to [59–61]).

In this chapter, we use the 16th-order CM method to estimate the spectral environment for both stationary and non-stationary interference. We make no claim that this value 16 is or is not optimal for our application. After estimation of the spectral environment, a threshold value equaling 15% of the peak's power is used. This threshold value has been empirically chosen based on the overall acceptable and comparable bit error performance versus stationary and non-stationary interference avoidance capabilities. Figure 4-2 shows an example of spectral estimation and spectral notching by the CM method. Figure 4-2(a) shows the spectral estimation by 16th-order CM where the X-axis is the normalized frequency over $[0, \pi]$ and the Y-axis is the power spectral density.

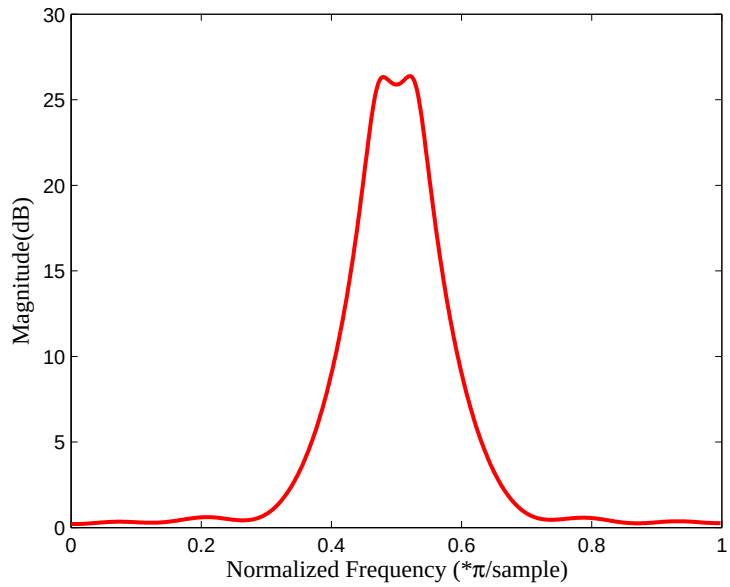
4.4 The Effects of Various Jamming on ETDCS

In this section, we investigate the bit error rate (BER) performance of the proposed ETDCS under several types of intentional interference (jamming) techniques with/without spectral notching by CM method. A similar simulation platform under different interference environments is implemented in order to compare with the TDCS, WDCS, and ETDCS. In each simulation, we sampled a duration of 100 data bits, and subsequent stages of the ETDCS are performed in Figure 4-1. After data modulation, the signal is transmitted over AWGN channel under various interferences. The symbols were finally demodulated at the receiver with the matched filter operation, and the number of bit errors was recorded. The simulations were terminated when the total number of bit errors exceeded 500 bits unless otherwise mentioned; this number was chosen empirically and was sufficient to produce relatively smooth bit error performance (BER) curves.

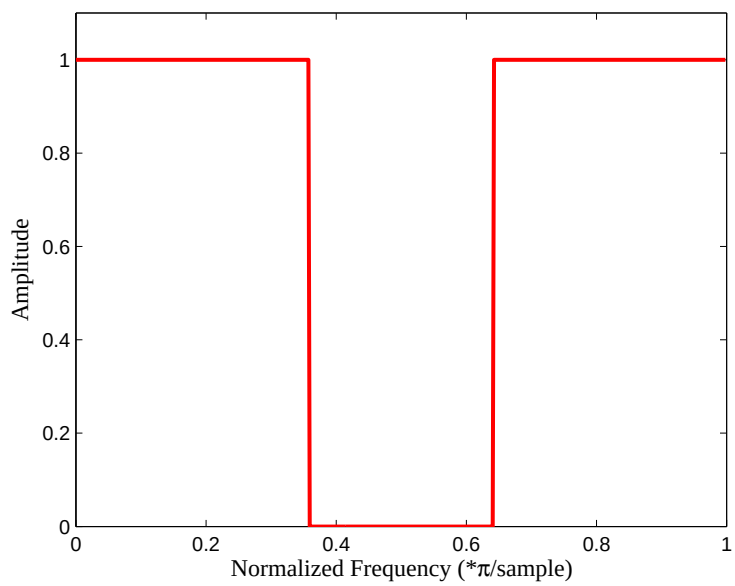
In this chapter, we use antipodal modulation as our signal mapping method. Antipodal modulation is a form of binary modulation that uses the basis function $b(t)$ as one symbol, $s_1(t)$, and the negative basis function $-b(t)$ as the second symbol, $s_2(t)$.

$$s_1(t) = b(t) \tag{4–9}$$

$$s_2(t) = -s_1(t)$$



A CM estimation of 10% partial band jamming



B Corresponding Spectrum Magnitude $A'(\omega)$

Figure 4-2. Spectral estimation and spectral notching

The theoretical BER P_b of antipodal modulation over an additive white Gaussian noise (AWGN) without jamming is given by (4–8). Figure 4-3 shows the antipodal BER performance under AWGN in the absence of the intentional interference to ensure proper

operation of the proposed method. The simulation results nearly match theoretical, antipodal signaling bit error performance - a mean absolute error of 8.8×10^{-4} and standard deviation of 1.3×10^{-6} over the range of the indicated E_b/N_0 value.

However, the theoretical performance without spectral shaping is estimated by assuming constant interference power spectral density N_J over the system bandwidth, effectively adding to the system noise floor and impacting bit error performance per (4–8) for the antipodal case. That is [14]:

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_0 + N_J}}\right) \tag{4–10}$$

where N_J is the interference noise power. Figure 4-4 shows the theoretical and simulated antipodal BER performance without spectral shaping adding constant interference power spectral density over the system bandwidth. The BER performance was simulated at the average signal-to-noise ratio (SNR) $E_b/N_0 = 4$ dB and an average interference-to-signal energy per bit (I/E) ranging from 0.0 dB to 16.0 dB. Note that the "No Jamming (SNR = 4dB)" performance in Figure 4-4 and others is the value of (4–8) for the $E_b/N_0 = 4$ dB (i.e., $P_b = 1.25 \times 10^{-2}$). These results are important and provide a baseline for comparing the performances without spectral shaping and with interference avoiding system. Note that the purpose of the interference mitigation is to enhance the BER performance from (4–10) to (4–8) under various jamming environments with the proposed ETDCS.

Next, various intentional interference scenarios are presented to the proposed ETDCS. Intentional electromagnetic interference (IEME) can be categorized into four categories, based on the frequency content of their spectral densities as "narrow band", "moderate band", "ultra-moderate band", and "hyperband" [1]. We consider only narrow band interference (NBI) in this chapter. The NBI further can be categorized into stationary or non-stationary interference with respect to its time-varying characteristic in the frequency domain. Partial band, single-tone, and multitone jamming are stationary interferences and swept-tone jamming is a non-stationary interference in terms of wide-sense stationarity.

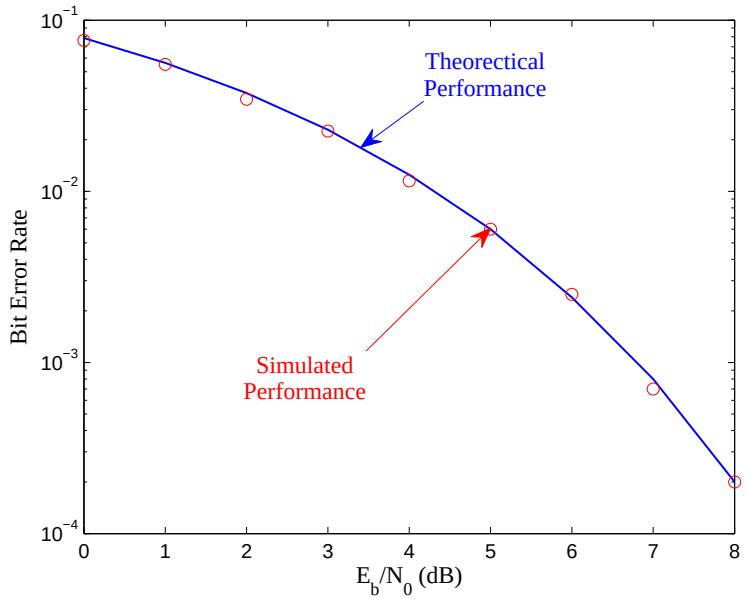


Figure 4-3. Antipodal signaling BER performance without interference in (4–8)

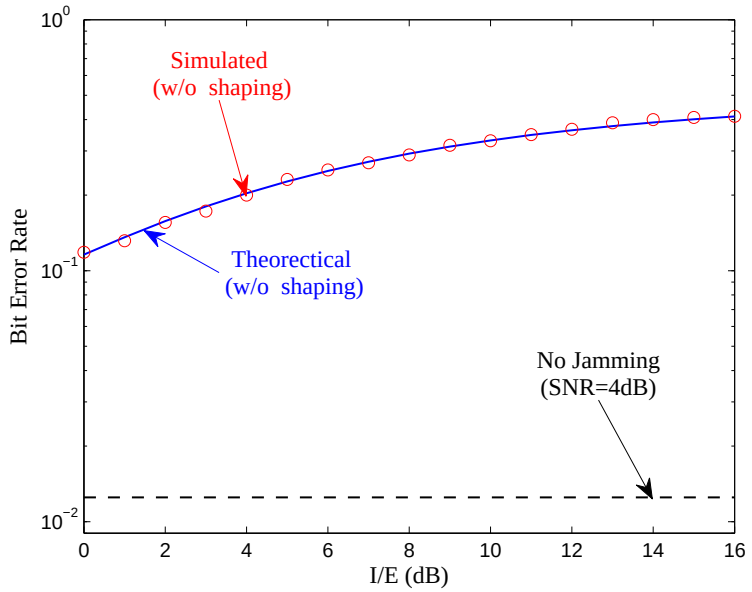


Figure 4-4. Theoretical and simulated performance without spectral shaping in (4–10)

As mentioned, we assume that the transmitter and the receiver are able to generate the same basis function. First, partial band interference (PBJ) occupies a continuous range of system bandwidth. The PBJ is modeled as additive Gaussian noise with its power focusing on a portion of the entire bandwidth of the system. Since white noise

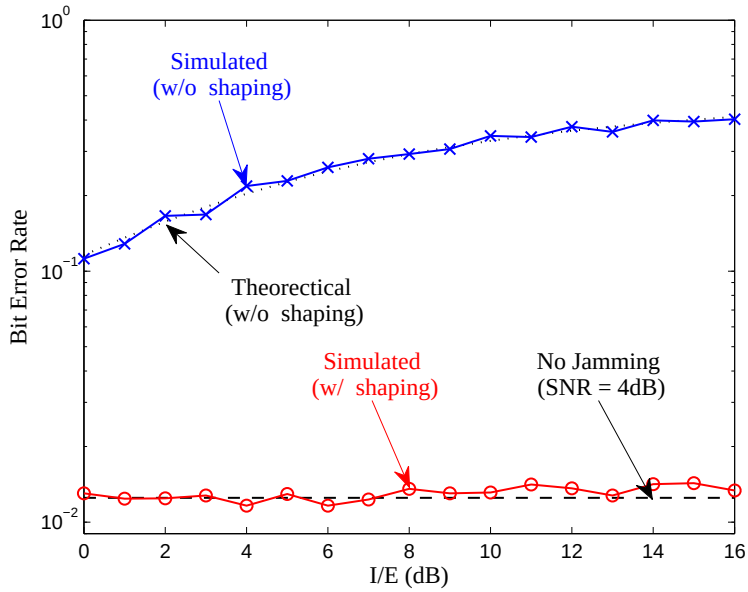


Figure 4-5. Antipodal signaling BER performance under 10% partial band jamming

is stationary, the PBJ is also a stationary jamming. Figure 4-5 and Figure 4-6 show the performance of the proposed ETDCS under 10% and 70% PBJ, respectively. The performance without spectral shaping under PBJ is closely approximated (4–10) for all I/E value considered. However, that with the proposed ETDCS under 10% and 70% is close to the "No Jamming (SNR=4dB)" in (4–8). Therefore, the proposed ETDCS successfully mitigates the PBJ.

Second, multi-tone jamming (MTJ) divides its total power into q distinct, equal power, random phase tones. Every jamming tone can be modeled as:

$$j(t) = A_J e^{j(2\pi f_J \cdot t + \phi_J)} \tag{4–11}$$

where ϕ_J is random phase, which is uniformly distributed over $[0, 2\pi]$. A_J and f_J are amplitude and frequency, respectively. Note that single-tone jamming (STJ) is a special case of multi-tone jamming with $q = 1$. The MTJ is a wide-sense stationary jamming, since the mean $\mathbf{E}[j(t)] = 0$ and the autocorrelation $\mathbf{E}[j^*(t)j(t+\tau)] = R(\tau)$ where $\mathbf{E}[\cdot]$ denotes the expectation. Figure 4-7 and Figure 4-8 show the performance of the proposed

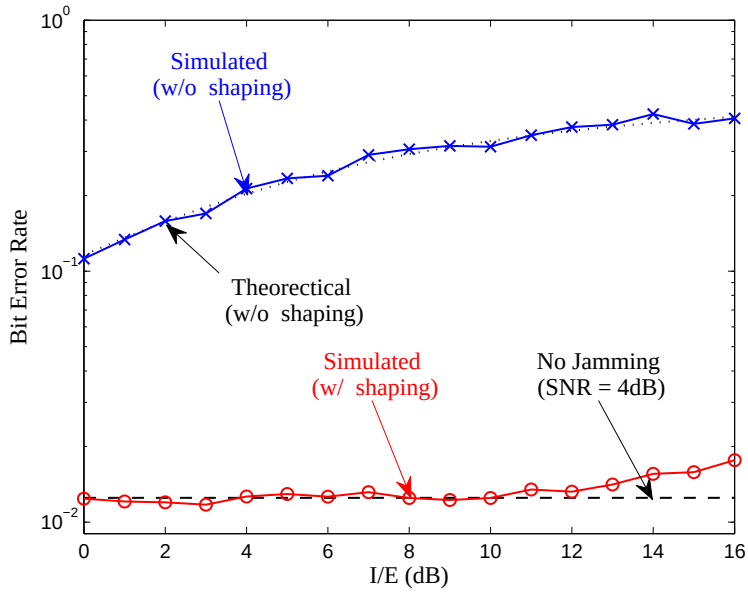


Figure 4-6. Antipodal signaling BER performance under 70% partial band jamming

ETDCS under STJ and MTJ, respectively. The performance without the spectral shaping under STJ is worse than (4–10). However, MTJ is a more effective jamming scenario than PBJ and STJ in the viewpoint of the jammer performance if the spectral shaping by CM method is not employed. Note that the proposed ETDCS successfully countermeasures the STJ and MTJ.

Finally, the proposed ETDCS is exposed to a non-stationary interference, i,e., swept-tone jamming (SWTJ) (see Figure 4-9). The SWTJ is when a jammer's full power is shifted from one frequency to another. Every SWTJ can be modeled as:

$$j(t) = A_J e^{j(2\pi f_J(t)\cdot t + \phi_J)} \tag{4–12}$$

where ϕ_J is random phase which is uniformly distributed over $[0, 2\pi]$. A_J is amplitude and $f_J(t)$ is a sweeping frequency. Since the mean $\mathbf{E}[j(t)] = 0$ and the autocorrelation $\mathbf{E}[j^*(t)j(t+\tau)] = R(t;\tau)$, the SWTJ is a non-stationary interference. In the TDCS [9, 11], the swept-tone interference could not be accurately estimated due to the parametric spectral estimation method, i.e., AR-method. In the EWDCS [19], the performance under

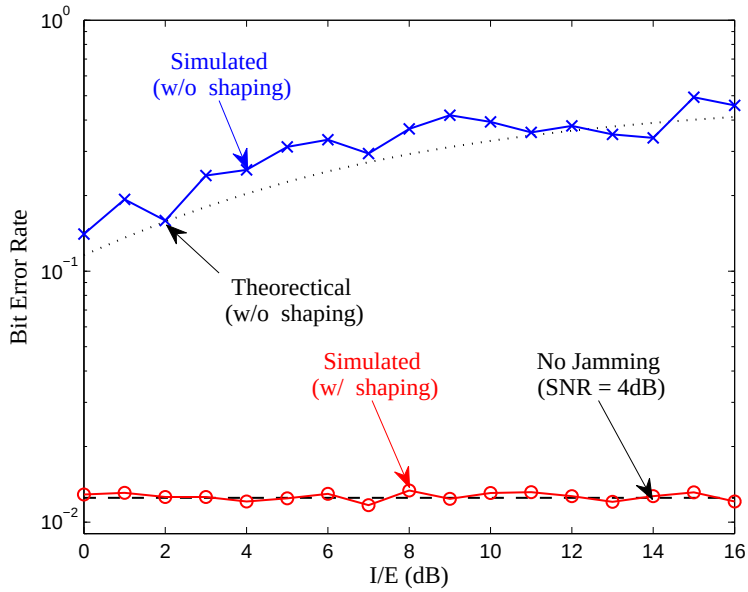


Figure 4-7. Antipodal signaling BER performance under single-tone Jamming

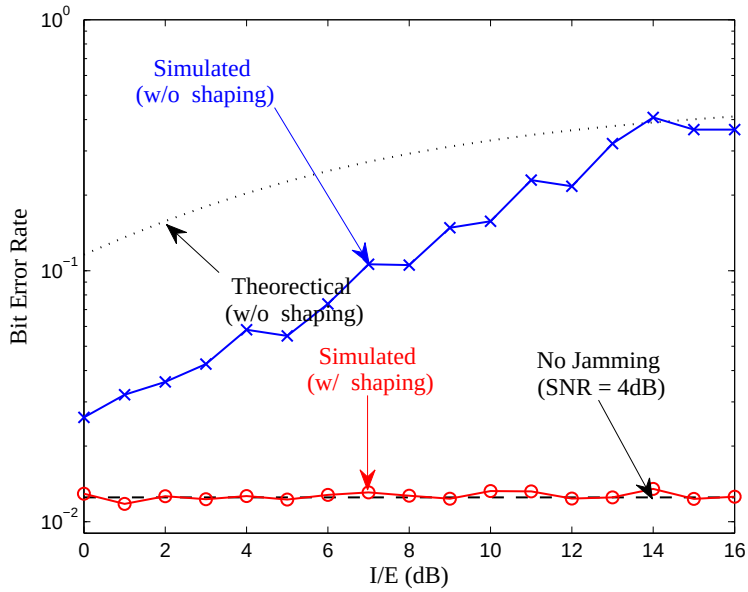


Figure 4-8. Antipodal signaling BER performance under multi-tone Jamming

swept-tone was sub-optimal compared to other interference scenarios. In Figure 4-9, we can see that the simulated BER performance under the SWTJ without spectral notching is closely approximated to (4–10) for the overall range of I/E considered. However, the

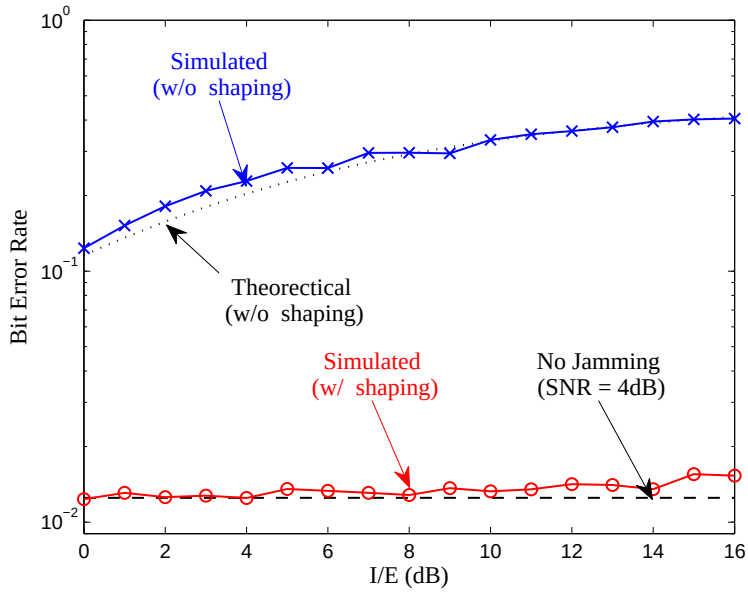


Figure 4-9. Antipodal signaling BER performance under swept-tone jamming

proposed ETDCS successfully mitigated a non-stationary interference with the spectral estimation by CM method.

In summary, Table 4-1 shows the comparative BER performance among the TDCS, the EWDCS, and the proposed ETDCS. The average ETDCS antipodal BER performance for all stationary interferences is 1.29×10^{-2}. The average ETDCS antipodal BER performance for the swept-tone interference is 1.35×10^{-2}. This kind of a non-stationary interference could not be handled by the TDCS [9, 11] and made sub-optimal performance for the EWDCS [19]. The proposed ETDCS demonstrates the ability to mitigate the different types of interferences. In particular, the proposed ETDCS extends this capability from the stationary interference to the non-stationary interference. Moreover, the proposed ETDCS has consistent performance for all types of interference considered in this section. This is the most notable strength of the proposed ETDCS.

4.5 Summary

The spectral estimation process plays an important role in the generation of the interference-free basis function for the transform domain communication system. The

Table 4-1. Comparison of the average BER performance of TDCS, EWDCS, and ETDCS with antipodal modulation (E_b/N_0 = 4dB, I/E = 0∼16 dB)

Avg. P_b	Stationary interference (PBJ,STJ,MTJ)	Non-stationary interference (SWTJ)	Overall
Native mode	2.62×10^{-1}	2.90×10^{-1}	2.67×10^{-1}
EWDCS [19]	1.50×10^{-2}	2.30×10^{-2}	1.66×10^{-2}
TDCS [9]	1.38×10^{-2}	N/A (Not Applicable)	N/A
Proposed ETDCS	1.29×10^{-2}	1.35×10^{-2}	1.30×10^{-2}

proposed ETDCS with CM method can properly estimates the interference environment considered in this chapter. Simulation results indicate that the proposed ETDCS offers a significant interference avoidance capability for both the stationary and non-stationary interference. bit error performance analysis for the stationary and non-stationary interference scenarios confirmed that the ETDCS system is highly capable of estimating and mitigating interference environments. Especially the proposed ETDCS extends interference avoidance capability from the stationary to the non-stationary interference for the TDCS and other similar systems. The ETDCS was simulated using an average signal-to-noise ratio of 4.0 dB and average interference-to-average signal energy I/E values ranging from 0.0 dB to 16.0 dB. For antipodal modulation, the overall average bit error probability was 1.30 $\times 10^{-2}$. The proposed ETDCS outperformed other similar methods such as the TDCS, WDCS, and EWDCS. Moreover, the ETDCS shows the consistent bit error performance under both the stationary interference and the non-stationary interference. Our research results indicate the proposed ETDCS is a viable alternative for the interference avoidance communication for highly reliable communication.

CHAPTER 5
AN ENHANCED V-BLAST WITH NON-STATIONARY INTERFERENCE AVOIDANCE CAPABILITY

5.1 Introduction

Multiple-input and multiple-output (MIMO) systems that use multiple antennae at both the transmitter and receiver are a promising wireless communication technology for higher data rate, higher spectral efficiency, better quality of service, and high network capacity. The vertical-Bell Laboratories layered space-time (V-BLAST) is one of such MIMO systems for realizing very high data rates over the rich-scattering wireless channel. The channel capacity approximately increases linearly with the number of transmitter and the number of receiver antennae, when operated in a channel with white Gaussian noise [7, 20]

Highly reliable communication has been desired by both military and civilian parties. It is very important, especially for the military communication systems, to be able to operate under both unintentional and intentional interferences. Therefore, it is desirable to use the V-BLAST system as a highly reliable communication system under these interferences.

One of the objectives of a communication interferer (or jammer) is to disrupt or degrade performance of the communication system up to the point where it is no longer reliable. Therefore, communication security research mainly centers on providing countermeasures to overcome such intentional communication interferences. However, the mitigation of the NBI has not been studied in the MIMO system, especially for the V-BLAST architecture.

The NBI has been investigated thoroughly for the single-input and single-output (SISO) system by transform domain processing (TDP). A fundamental idea of the TDP is the design of an interference-free adaptive waveform in frequency-domain rather than in time-domain. Spectrally crowded regions are avoided by adaptive spectral notching in the TDP [9, 33].

In the work of [12], they combined the fundamental concept of TDP with V-BLAST based on zero-forcing (ZF) detector to mitigate NBI. However, they failed to mitigate non-stationary interference, like swept-tone interference. The lack of stationarity of a non-stationary interference affected the performance of the spectral estimator, 10th-order autoregressive (AR) filter. Therefore, the system proposed in [12] did not work well for non-stationary interferences. Because the ZF detector generally suffers from noise enhancement at early stages, they used higher SNRs (15dB and 25dB) in their simulation studies.

In our previous work [33], we proposed a viable option of the reliable SISO communication system, called ETDCS. The enhanced transform domain communication system (ETDCS) offered a significant interference avoidance capability for both stationary and non-stationary interference with a non-parametric spectral estimator, Capon's method (CM) [33, 59, 61].

In this chapter, we extend our previous approach in Chapter 4 to provide non-stationary as well as stationary interference avoidance capability to the V-BLAST system. The TDP by CM and minimum mean square error (MMSE) detector are combined with the V-BLAST to enhance bit error performance in NBI environment; that is, the TDP by CM will provide better avoidance of the spectrally crowded regions and will enhance the bit error performance of the V-BLAST system under a reasonable SNR by MMSE detector.

The remainder of this chapter is organized as follows: Section 5.2 presents our previous work. Section 5.3 describes a V-BLAST system model and the interference model. Section 5.4 introduces our proposed methodology. Section 5.5 presents simulation results to show the performance of our proposed approaches. Section 5.6 summarizes this chapter.

5.2 Related Works

See Chapter 4.

5.3 System and Interference Model

Figure 5-1 shows a high-level system block diagram of a V-BLAST system model with M transmitters and N receivers. We assume perfect channel estimation at the receiver and we do not consider the power allocation problem such that the power launched by each transmitter is proportional to $1/M$. In each use of the MIMO channel, a vector $\mathbf{a} = (a_1, \cdots, a_M)^T$ of complex numbers is sent and a vector $\mathbf{r} = (r_1, \cdots, r_N)^T$ of complex numbers is received where $[\cdot]^T$ denotes transpose. We use the relation between $\mathbf{a}$ and $\mathbf{r}$ as follows:

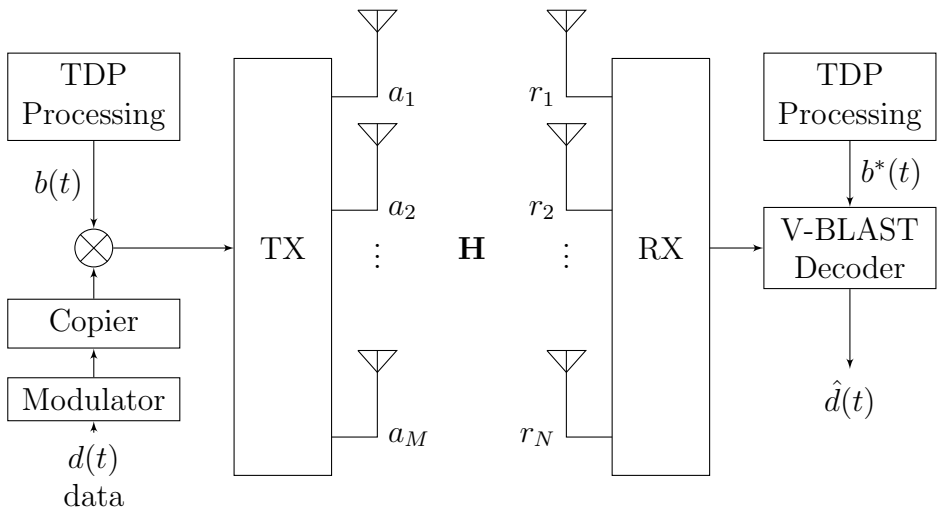


Figure 5-1. V-BLAST with the TDP [12]

$$\mathbf{r} = \mathbf{H}\mathbf{a} + \mathbf{n} \tag{5–1}$$

where $\mathbf{H}$ is $N \times M$ matrix representing the scattering effects of the channel and $\mathbf{n}$ is the noise vector. We assume that $\mathbf{H}$ is a random matrix with independent zero mean complex Gaussian. We also assume that $\mathbf{n}$ is a complex random vector with i.i.d. elements and its covariance matrix is the identity matrix scaled by the noise variance σ_n^2. Let $\mathbf{v} = (v_1, v_2, \cdots, v_N)^T$ denote one type of the NBI interference vector. Then, the NBI

interfered version of (5–1) can be modeled as follows:

$$\mathbf{r} = \mathbf{Ha} + \mathbf{n} + \mathbf{v} \tag{5–2}$$

We also assume the same electromagnetic environment for all transceivers. Therefore, all transceivers experienced the same interference $\mathbf{v}$ and can generate the same adaptive interference-free waveform at both the M transmitters and the N receivers in the TDP processing stage. If this is not true, a dedicated feedback loop may be employed. The NBI can be categorized into stationary or non-stationary interference with respect to its time-varying characteristic in the frequency domain. partial band, single-tone, and multi-tone interference are stationary interferences and swept-tone interference is a non-stationary interference.

partial band interference (PBJ) occupies a continuous range of system bandwidth. Multi-tone jamming (MTJ) divides its total power into several distinct, equal power and random phase tones. Single-tone interference (STJ) is a special case of MTJ. Swept-tone interference (SWTJ) is like a single-tone changing frequency over time. We assume that stationary interferences do not change the frequency they occupied and swept-tone interference sweeps the bands with a certain pattern in a specific time interval.

5.4 Proposed Methodology

To avoid interfered regions, the accurate estimation of the spectrally crowded electromagnetic environment is the most important in designing the adaptive interference-free waveform in TDP. Therefore, proper selection of a spectral estimator is the most important step of TDP processing.

There are basically two broad categories of techniques for spectral estimation. One is the non-parametric approach based on the concept of bandpass filter. The other is the parametric method: It assumes a model for the data so that the spectral estimation becomes a problem of estimating the parameters in the assumed model [61].

The AR-estimator used in [9] and its extension to a V-BLAST in [12] is a parametric estimation method. It fits an AR linear prediction filter model to the signal by minimizing the forward prediction error in the least square sense. Since the model in the AR-estimator did not fit the environments well in the case of a non-stationary interference, the TDP suffered significant performance degradation and failed to estimate a swept-tone interference. One of the most well-known non-parametric spectral estimation methods is Capon's approach which is also known as minimum variance distortionless response (MVDR) [59, 61–63]. Capon's method (CM) for spectral estimation is primarily based on a filter bank decomposition: The spectrum of signals is estimated in each band by a simple filter design subject to some constraints. We use CM method to estimate interfered environment at the TDP processing stage in our proposed V-BLAST.

After the spectral estimation, a band which exceeds the noise level is notched out with a certain threshold. Otherwise, that band is retained. Consequently, an interference-free spectrum magnitude $A'(\omega)$ is generated. After notching out the interferences, a multi-valued complex pseudo-random (PN) phase vector is generated from a linear feedback shift register (LFSR) identical in length to $A'(\omega)$ and multiplied element-by-element with $A'(\omega)$ in a process called *phase coding*, producing spectral vector, $B_b(\omega)$, with known amplitude and PN phase characteristics. The spectral vector $B_b(\omega)$ is then amplitude-scaled by constant C to ensure a communication symbol has the desired signal energy. The resultant spectral vector, $B(\omega)$, is inverse Fourier transformed to produce a time-domain *basis function*, $b(t)$.

After generation of the basis function $b(t)$, input data stream $d(t)$ is demultiplexed and modulated into M sub-streams, and finally fed into each transmitter. We used a cyclic code shift keying (CCSK) [64] which is a form of M-ary signalling over a communication channel. That is, in its simplest form, a basis function $b(t)$ is chosen, and a cyclically (circularly) shifted version of $b(t)$ is used to modulate a carrier. The receiver also generates $b(t)$ to demodulate the detected symbol with the correlation detector.

Table 5-1. V-BLAST/MMSE with ETDP Detection

Initialization:

$$\begin{aligned}
\mathbf{W}_1 &= \tfrac{\rho}{M}\mathbf{H}^\dagger\left(\tfrac{\rho}{M}\mathbf{H}\mathbf{H}^\dagger + \sigma_n^2\mathbf{I}_N\right)\\
i &= 1
\end{aligned}$$

Recursion:

$$\begin{aligned}
k_i &= \underset{j\notin\{k_1,\cdots,k_{i-1}\}}{\operatorname{argmin}} \|(W_i)_j\|^2\\
y_{k_i} &= (\mathbf{W}_i)_{k_i}\mathbf{r}_i\\
\hat{a}_{k_i} &= Q(y_{k_i})\\
&= \underset{p=1,2,\cdots,16}{\operatorname{argmax}} \left\langle y_{k_i}, d\left(t-\frac{pT_s}{16}\right)\right\rangle\\
\mathbf{r}_{i+1} &= \mathbf{r}_i - \hat{a}_{k_i}(\mathbf{H})_{k_i}\\
\mathbf{W}_{i+1} &= \tfrac{\rho}{M}\mathbf{H}^\dagger_{k_i^-}\left(\tfrac{\rho}{M}\mathbf{H}_{k_i^-}\mathbf{H}^\dagger_{k_i^-} + \sigma_n^2\mathbf{I}_N\right)\\
i &= i+1
\end{aligned}$$

The proposed V-BLAST uses a MMSE detector [50] at the receiver sides. Since the ZF detector suffers from the noise enhancement at the early stages, the detector with MMSE criterion is favorable under the interference. The detector algorithm of a V-BLAST decoder is shown in Table 5-1. This version of the V-BLAST is based on the MMSE and the correlation detection. Note that the major difference with the general V-BLAST/MMSE detection and Table 5-1 is in the 3rd step of Recursion where the detected signal correlates with the cyclic shift version of the basis function $b(t)$.

5.5 Simulation and Analysis

To verify the performance of the proposed system under the intentional interferences, the BER is studied as an important performance measure for the reliability of a communication system. We use the same simulation platform in [12] and add our proposed approach in that platform. We also use the same interference model in [12]. In each simulation, we first sampled the environment for a duration of 10 symbols and the fundamental waveform $b(t)$ was generated. After demultiplexing and 16-CCSK modulation, the signal $\mathbf{a}$ was transmitted by each transmitter over an MIMO channel $\mathbf{H}$ with the channel noise $\mathbf{n}$ and the various interference $\mathbf{v}$. By MMSE and correlation

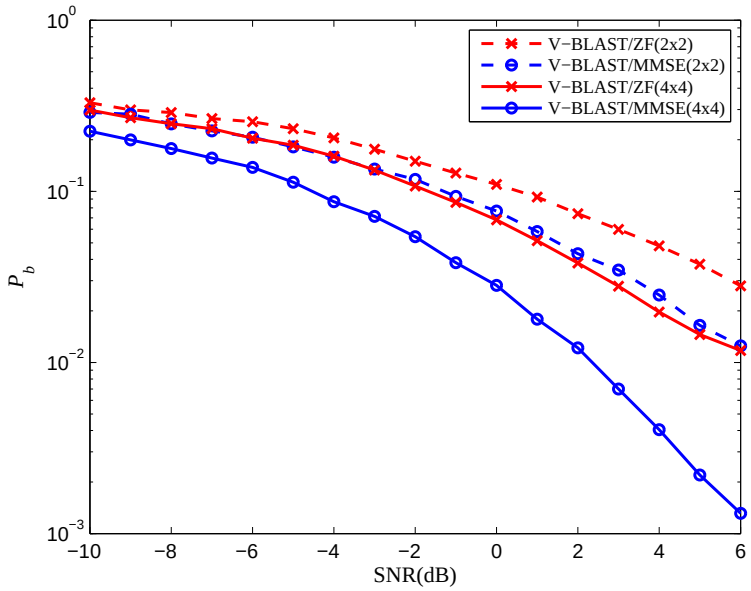


Figure 5-2. BER performance without interference

detection at the receiver given in Table 5-1, the symbols were finally demodulated and the BER was recorded.

First, a simulation is run in the absence of the intentional interference to ensure proper operation of the proposed method. Figure 5-2 shows the simulation results for $(M, N) = (2, 2)$ and $(M, N) = (4, 4)$. The E_b/N_0 is ranged between -10dB and 6dB in steps of 1dB. The BER, P_b, is calculated by terminating the simulation when the total number of bit errors exceeds 500 bits - this number is chosen empirically and is sufficient to produce relatively smooth bit error performance curves. We observe that the V-BLAST/MMSE performes better than the V-BLAST/ZF for overall ranges of E_b/N_0.

Finally, the proposed system is exposed to various interferences. The 30% partial band, single-tone and multi-tone interference are used for the stationary interferences, and the swept-tone is used for the non-stationary interference model. The BER performance is simulated at the signal-to-noise ratio $E_b/N_0 = 4dB$ and the average interference-to-signal energy per bit (I/E) is ranged from 1.0 dB to 10.0 dB.

We compare BER performance between our proposed method and the system proposed in [12] under the same simulation parameters. The threshold used for the 10th-order AR-estimator is 40% [12], while that used for our proposed 16th-order CM is 30%. Note that we make no claim that these parameters are or are not optimal for our application. These values are empirically chosen based on the overall acceptable and comparable BER performance versus stationary and non-stationary interference avoidance capability.

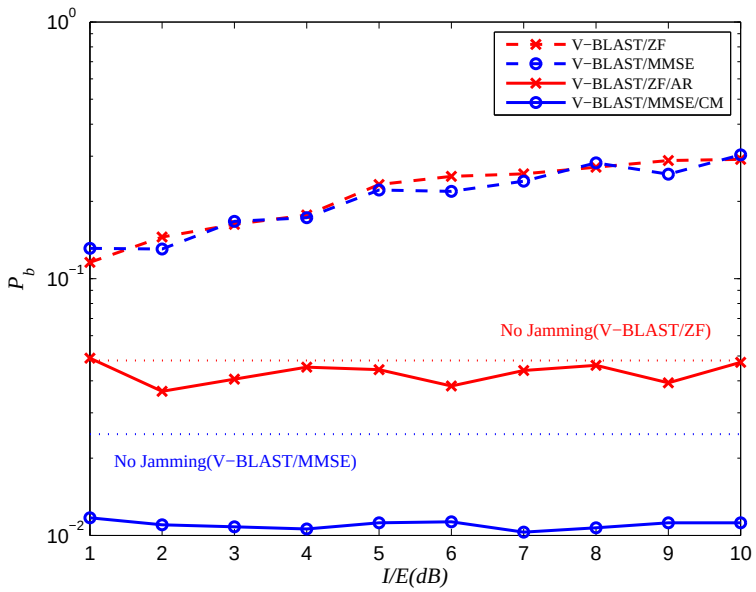


Figure 5-3. BER performance for $M \times N = 2 \times 2$ under 30% partial band Interference

Figure 5-3, 5-4, 5-5, and 5-6 show simulation results for $(M, N) = (2, 2)$, while Figure 5-7, 5-8, 5-9, and 5-10 shows the simulation results for $(M, N) = (4, 4)$, respectively. Note that V-BLAST/MMSE/CM (or V-BLAST/ZF/AR) denotes V-BLAST with the MMSE (or ZF) detector and the TDP based on CM (or AR), while V-BLAST/MMSE (or V-BLAST/ZF) denotes normal V-BLAST system without the TDP processing. We also present the BER performance without interference (no jamming) for both V-BLAST/ZF and V-BLAST/MMSE system from Figure 5-2 for comparison.

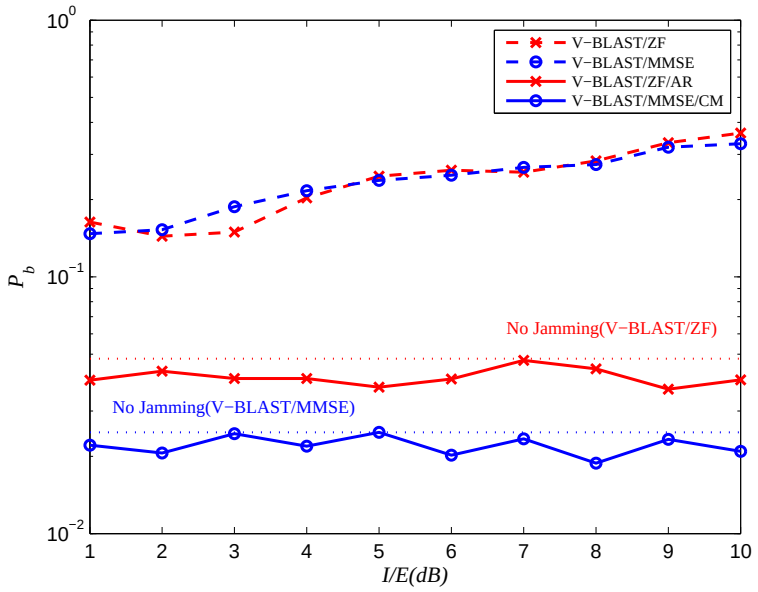


Figure 5-4. BER performance for $M \times N = 2 \times 2$ under single-tone interference

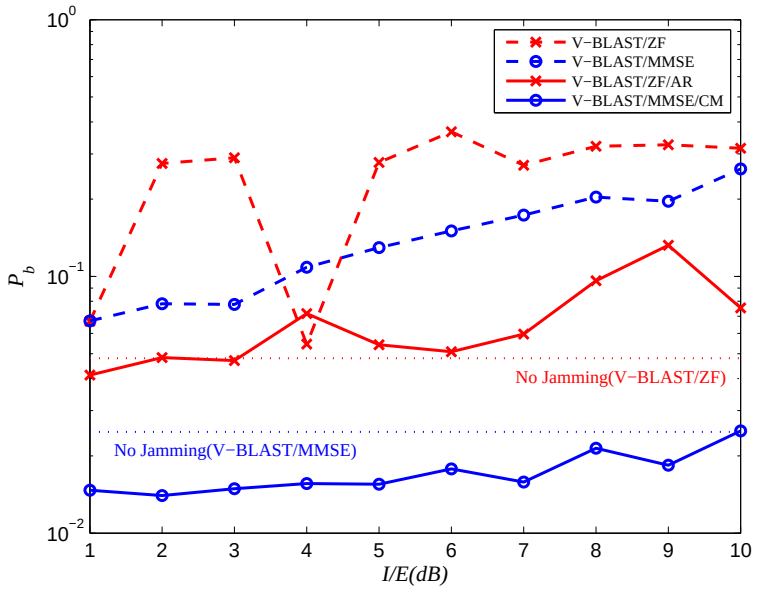


Figure 5-5. BER performance for $M \times N = 2 \times 2$ under swept-tone interference

Even without TDP processing, V-BLAST/MMSE performs better than V-BLAST/ZF. The performance of V-BLAST/ZF is unstable for cases of the swept-tone and multi-tone interference as shown in Figure 5-5 and Figure 5-6 for (M, N)=(2,2) and Figure 5-9 and 5-10 for (M, N)=(4,4). This is due to noise enhancement of the ZF detector. Therefore,

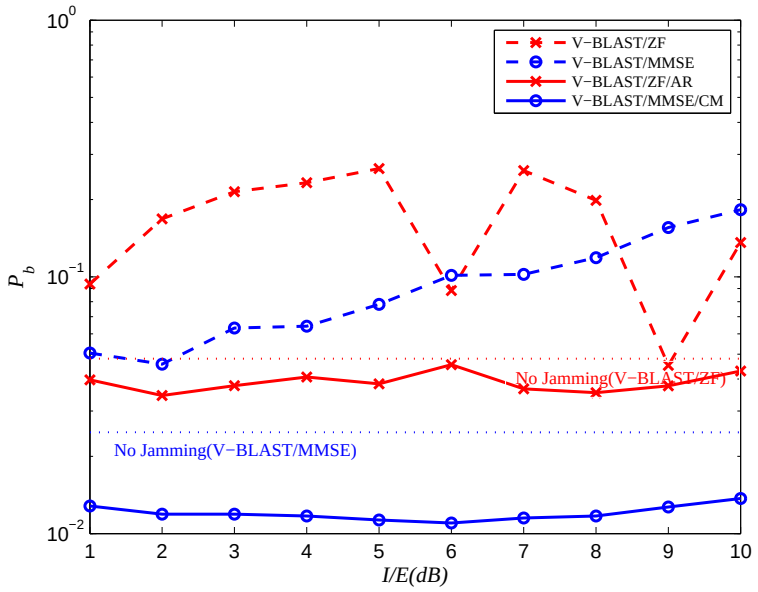


Figure 5-6. BER performance for $M \times N = 2 \times 2$ under multi-tone interference

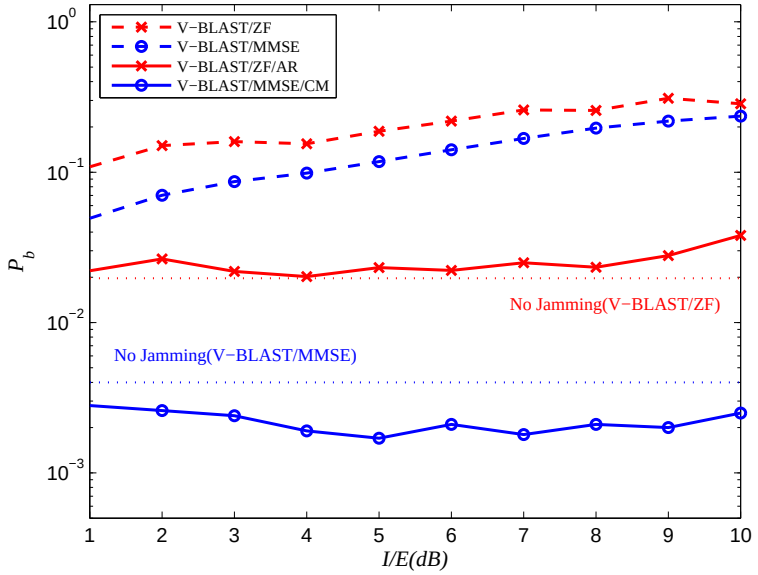


Figure 5-7. BER performance for $M \times N = 4 \times 4$ under 30% partial band interference

the method proposed in [12] used higher SNRs (15dB and 25dB) in their performance studies.

As shown in Figure 5-3 ∼ 5-10, V-BLAST/MMSE/CM approach significantly improves the BER performance under both the stationary and the non-stationary

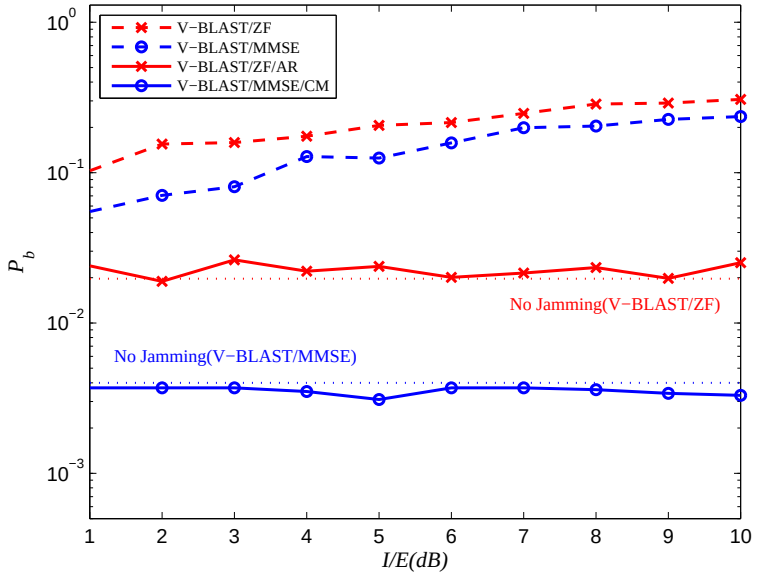


Figure 5-8. BER performance for $M \times N = 4 \times 4$ under single-tone interference

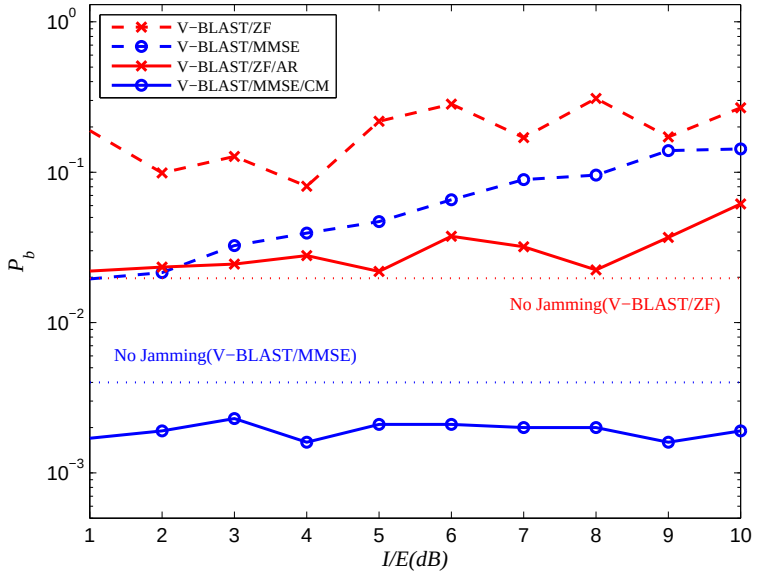


Figure 5-9. BER performance for $M \times N = 4 \times 4$ under swept-tone interference

interference with respect to V-BLAST/ZF/AR. The performance improvement is obtained by both the MMSE detector in V-BLAST detection and CM method in the TDP processing stage. V-BLAST/ZF/AR method improves the BER performance under the stationary interference, while it does not work well for the non-stationary

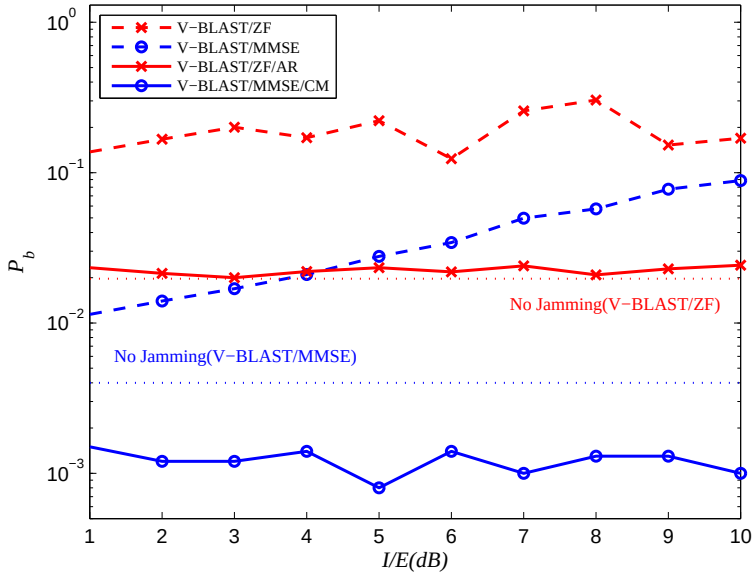


Figure 5-10. BER performance for $M \times N = 4 \times 4$ under multi-tone interference

interference due to the stationarity assumption on the AR estimator. Therefore, the proposed method extends its NBI interference avoidance capability from the stationary NBI to the non-stationary NBI, and has consistent performance for all type of interference considered in this chapter.

If we look at the performance in terms of a jammer (or interferer), the single-tone interference can disrupt or degrade the performance of the V-BLAST system more than other interference scenarios. Since the single-tone interference can concentrate more interference power than other interferences, an adaptive threshold selection for this type of NBI should be provided by TDP processing in future research.

5.6 Summary

It is very important to support countermeasures for a communication system under NBI interference. In this chapter, we consider the problem of mitigating the NBI interference for V-BLAST system. The proposed V-BLAST system combines the merits of both the TDP processing based on CM method and detection based on MMSE nulling under the intentional interference. To avoid interfered regions, accurate

estimation of the spectrally crowded electromagnetic environment is critical in designing the adaptive interference-free waveform in TDP processing. We use the 16th-order CM method to estimate interfered spectral environments. We also use the MMSE detector to prevent noise enhancement in V-BLAST detection. Combined effects of MMSE nulling in V-BLAST detection and CM method in the TDP processing stage mitigate both stationary and non-stationary interferences. Our simulation results validate the performance of our proposed V-BLAST as a viable countermeasure against NBI interference. Moreover, our approach extends its NBI interference mitigation capability from stationary NBI to non-stationary NBI.

CHAPTER 6
ON THE PERFORMANCE OF JOINT PRECODING AND EQUALIZATION FOR TRANSMITTER ANTENNA ARRAY DOWNLINK TDD MC-CDMA

6.1 Introduction

Wireless communication is, by any measure, the fastest growing segment of the communication industry. As such, it is very common both for commercial and military parties. However, the transmitted information-bearing signal is subject to various impairments caused by the transmission medium and vulnerable wireless channel combined with the mobility of the transceiver. Therefore, special care must be taken to satisfy security requirements of the wireless communication systems [13, 17].

Direct-sequence code division multiple access (DS-CDMA), where spreading is performed in the time domain, has high sampling rates. This high sampling rate makes DS-CDMA very susceptible to performance degradation caused by multipath propagation [23]. Therefore, multi-carrier CDMA (MC-CDMA) was developed to overcome this drawback of the DS-CDMA [21, 58]. The main benefit of MC-CDMA in comparison to other OFDM-based multiple access methods is the inherent provision of frequency diversity. By contrast, a drawback of MC-CDMA, like DS-CDMA, is the multiuser interference (MUI) encountered due to loss of orthogonality. This factor predetermines the performance of MC-CDMA [21, 23].

Several advanced multiuser detection techniques are available for interference mitigation [58]. Despite the effectiveness of their approaches, these methods are not suitable for downlink (DL) applications due to the limited computational power of mobile terminals (MTs) [26]. As an alternative to multiuser detection, precoding techniques can be employed to mitigate the MAI and channel distortions in the DL. A fundamental idea of the precoding is to vary the complex gain assigned to each subcarrier such that interference is reduced and the signal at the receiver appears undistorted. The use of the precoding has several advantages: (i) reducing the MAI at MTs by the precoding at the base station (BS) so that the received signal at the decision point is free from interference,

(ii) moving most signal processing tasks from MTs to BS, and (iii) keeping the MTs at a very low complexity level.

In recent years, several linear precoding techniques have been proposed for multi-input single-output (MISO) DL time division duplex (TDD) MC-CDMA in the literature [22, 24–27, 36, 37]. The algorithm discussed in [24] aims at maximizing the signal to interference plus noise ratio (SINR) at MTs. This leads to a complicated joint optimization problem for the transmit filters of all active users, and thus a suboptimal approach was proposed based on a modified SINR. In [25], a space-frequency precoding technique based on minimization of the transmitted power subject to MAI elimination was proposed, which eliminates the necessity of the noise variance to be estimated at the MT and known at the BS. In [26], a different power constraint was derived for the approach proposed in [25]. A constraint on the overall transmit power allocated to all active users was imposed, instead of normalizing the transmit power for each user. This was further extended in [27], where alternative strategies to constrain the transmit power at the BS have been discussed. All of these space-frequency precoding schemes were derived considering that no channel equalization is performed at the MTs, while a combination of the precoding techniques and channel equalization at the receiver was proposed in [22].

In this chapter, we study an analytical bit error rate (BER) performance of a DL TDD MC-CDMA with a precoding transmitter antenna array at the BS. In [44], asymptotic BER of a precoded random spreading CDMA system in additive white Gaussian noise (AWGN) channels was analyzed. In [27], the performance of different space-frequency precoding methods was compared by numerical simulations. In [22], two space-frequency schemes with multiuser pre-filtering techniques for DL MC-CDMA were proposed and the performance of the proposed schemes was compared to other transmitter precoding approaches by simulation. However, not many analytical performance studies have been done for the precoded DL MC-CDMA. By conducting analytical study, we can predict and compare the performance of various precoding techniques.

The remainder of this chapter is organized as follows: Section 6.2 elaborates on a system model of a DL TDD MC-TDCS. Then, various single-user equalization methods are discussed in Section 6.3. Section 6.4 describes how to mitigate the MAI with help of the space-frequency diversity and the precoding at the transmitter. The performance analysis and verification by simulation are presented in Section 6.4.3 and Section 6.5, respectively. Finally, Section 6.6 summarizes this chapter.

6.2 System Model

In this section, we elaborate on both the system architecture and mathematical model of a DL TDD MC-CDMA. The MC-CDMA is a multi-carrier transmission where its bandwidth can be divided into smaller sub-bands. Precoding techniques in [22, 24–27, 36, 37] require channel state information (CSI) at the transmitter in order to work properly. This can be achieved in TDD systems by exploiting the channel reciprocity between alternative uplink and downlink transmission. If channel variations are sufficiently slow, the channel estimation derived at the BS during an uplink time slot can be reused for precoding in the subsequent downlink time slot [26, 43].

We consider a DL of the MC-CDMA network where the total number of sub-carriers N_c is divided into M smaller groups of L elements of the sub-carriers where $M = N_c/L$. We assume that the BS has P transmitter antennae and uses the sub-carriers of a given group to communicate K active users ($K \leq L$). Therefore each user k ($1 \leq k \leq K$) transmits M data symbols per OFDM symbol. Hence, each OFDM symbol has a data rate proportional to M times the original input data symbols. Active users are separated by their specific spreading code $\mathbf{c}_k$ of the kth user, usually chosen from an orthogonal set. Let's assume the L sub-carriers of a given group are uniformly distributed over the signal bandwidth to better exploit frequency diversity. Let i_n^m denote a sub-carrier index of the mth symbol of a user with $i_n^m = m + (n-1)N/L$ and $1 \leq n \leq L$.

Figure 6-1 shows the block diagram of a DL TDD MC-CDMA system under investigation. The data symbol vector $\mathbf{a}_k$ of the user k is fed into the serial-to-parallel

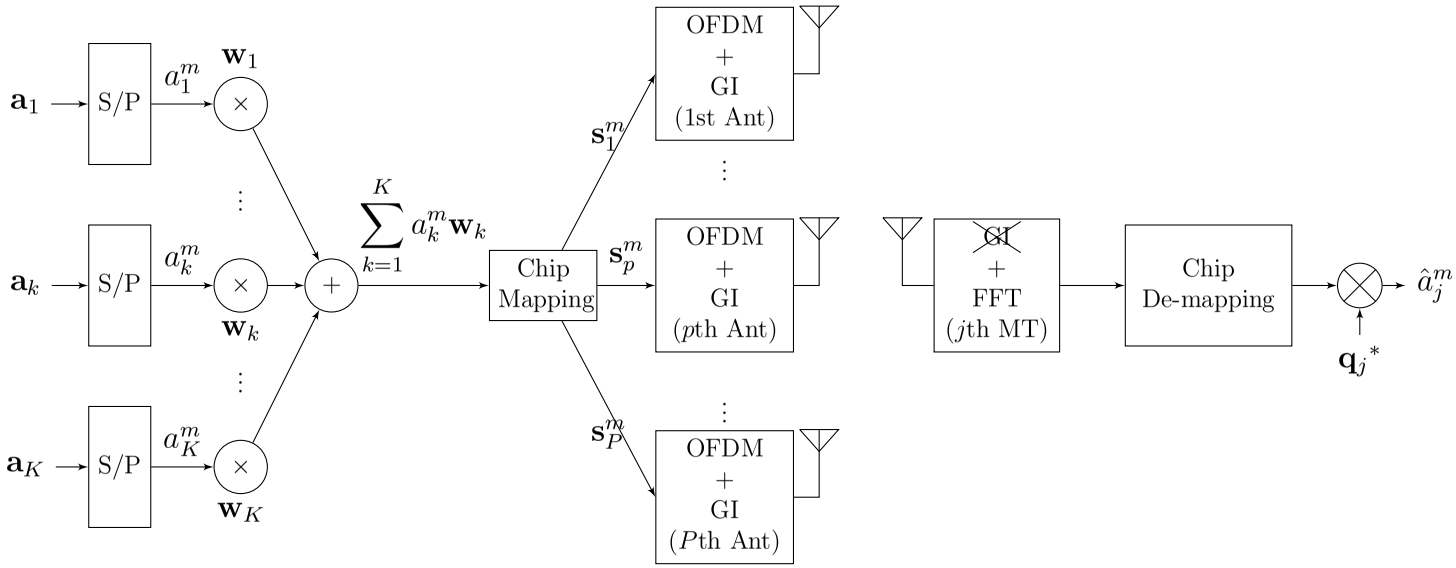


Figure 6-1. Architecture of MC-CDMA transceiver with multiple transmitter antennae, precoding and receiver-based equalization

block and the mth symbol of the kth user, a_k^m, is spread by L chips using the spread sequence $\mathbf{c}_k = [c_k(1), \cdots, c_k(L)]^H$ of the kth user where $c_k(n) \in \left\{\pm 1/\sqrt{L}\right\}$ and $(\cdot)^H$ denotes conjugate transpose. The resulting $a_k^m \mathbf{c}_k$ is weighted by the precoding coefficient $\mathbf{u}_{k,p}$ of the kth user at the pth antenna and is fed to each antenna. The weighted output $\mathbf{w}_{k,p} = [w_{k,p}(1), \cdots, w_{k,p}(L)]^H$ of the kth user of the pth antenna is a vector with entries $w_{k,p}(n) = c_k(n) u_{k,p}(n)$ for $n = 1, \cdots, L$.

The contribution of all K users are summed together in each sub-carrier index i_n^m $(1 \leq n \leq G)$ to form the following multiuser signal at the pth antenna

$$\mathbf{s}_p^m = \sum_{k=1}^{K} a_k^m \mathbf{w}_{k,p}, \quad p = 1, \cdots, P \tag{6–1}$$

Then, each $\mathbf{s}_p^m$ is uniformly mapped on L sub-carriers using the chip mapper. After an OFDM modulation for each antenna, N_G-point cyclic prefix (CP) (or guard interval (GI)) is added in the transmitted signals to avoid interference between adjacent OFDM blocks.

The transmitted signals by the BS antennae array propagate through multipath channels and experience frequency selective fading. The jth MT with a single antenna recombines signals from P antennae branches at the BS. The received signal after the OFDM demodulation and CP removal of the jth MT is given by

$$\mathbf{X}_j^m = \sum_{p=1}^{P} \sum_{k=1}^{K} a_k^m \mathbf{H}_{j,p} \mathbf{w}_{k,p} + \mathbf{n}_j \tag{6–2}$$

where $\mathbf{H}_{j,p} = \text{diag}\left\{H_{j,p}(i_1^m), \cdots, H_{j,p}(i_L^m)\right\}$ is a diagonal matrix of size $L \times L$, representing channel frequency response between pth transmitter antenna and jth MT over L sub-carriers, and $H_{j,p}(i_n^m)$ denotes complex flat fading channel of the nth sub-carrier on the pth antenna, $\mathbf{n}_j = [n_j(1), \cdots, n_j(G)]^T$ is thermal noise with zero mean and covariance matrix $\sigma_n^2 \mathbf{I}_L$.

The decision variable at the input of the demodulator for the desired jth user with a frequency domain equalization and despreading $\mathbf{q}_{k'}$ is given by:

$$\begin{aligned}\hat{a}_j^m &= \mathbf{q}_j^T \mathbf{X}_j^m \\ &= \underbrace{a_j^m \mathbf{q}_j^T \left(\sum_{p=1}^{P} \mathbf{H}_{j,p} \mathbf{w}_{j,p} \right)}_{\text{Desired signal}} + \underbrace{\left(\sum_{k=1, k\neq j}^{K} a_k^m \mathbf{q}_k^T \sum_{p=1}^{P} \mathbf{H}_{j,p} \mathbf{w}_{k,p} \right)}_{\text{MAI}} + \underbrace{\mathbf{q}_j^T \mathbf{n}_j}_{\text{Noise}}\end{aligned} \tag{6–3}$$

where $\mathbf{q}_k = [q_k(1), \cdots, q_k(L)]^T$ is a vector of size L that account for both despreading and channel equalization operations. As mentioned, the performance of the MC-CDMA is predetermined by the 2nd term in (6–3). Several receiver channel equalization methods for single user detection will be discussed in the sequel.

6.3 Single User Equalization at Receiver

For single user detection, the equalization coefficients are given by:

$$\mathbf{q}_j = \mathbf{G}_j \mathbf{c}_j^* \tag{6–4}$$

where $(\cdot)^*$ denotes the complex conjugate and $\mathbf{G}_j = \text{diag}\{g_j(1), \cdots, g_j(L)\}$ is a diagonal matrix of size $L \times L$, representing coefficients of the frequency domain channel equalization. If we use only the precoding at the transmitter antennae, we can use the pure despreading (PD) in order to keep the MTs at very low complexity. Then, the despreading and channel equalization vector $\mathbf{q}_k$ is the same as the user's despreading code as follows:

$$\mathbf{q}_j = \mathbf{c}_j^* \tag{6–5}$$

6.3.1 Maximal Ratio Combining

$$g_j(n) = \left(\sum_{p=1}^{P} H_{j,p}(i_n^m) \right)^* \quad n = 1, \cdots, L \tag{6–6}$$

In maximal ratio combining (MRC), a stronger signal is assigned a higher weight by the diversity combiners than a weaker signal, since its contribution is more reliable.

6.3.2 Equal Gain Combining

$$g_j(n) = \frac{\left(\sum_{p=1}^{P} H_{j,p}(i_n^m)\right)^*}{|\sum_{p=1}^{P} H_{j,p}(i_n^m)|} \quad n = 1, \cdots, L \tag{6–7}$$

The equal gain combining (EGC) attempts to correct the channel-induced phase rotations, leaving the faded magnitudes uncorrected.

6.3.3 Orthogonality Restoring Combining

$$g_j(n) = \frac{\left(\sum_{p=1}^{P} H_{j,p}(i_n^m)\right)^*}{|\sum_{p=1}^{P} H_{j,p}(i_n^m)|^2} \tag{6–8}$$

If we cancel the effect of the channel transfer function by estimating it and reversing its effects, the orthogonality of the different users can be maintained if orthogonal codes are used. This is the aim of the orthogonality restoring combining (ORC) or zero forcing (ZF) equalization.

6.3.4 Minimum Mean Square Error Equalization

$$g_j(n) = \frac{\left(\sum_{p=1}^{P} H_{j,p}(i_n^m)\right)^*}{|\sum_{p=1}^{P} H_{j,p}(i_n^m)|^2 + \sigma_n^2} \tag{6–9}$$

To mitigate the noise enhancement of ORC, particularly at lower SNR values, the minimum mean square error (MMSE) equalization can be used.

6.4 Space-Frequency Precoding

The purpose of precoding schemes is to remove the MAI and channel distortions at MTs. In this section, we discuss various space-frequency precoding approaches for the MC-CDMA system in Section 6.2. If we don't use the precoding at the transmitter antennae, we can use the pure spreading (PS). The weighted output $\mathbf{w}_{j,p}$ of the jth user of the pth antenna in (6–3) for the PS is the same as the jth user spreading code. That is:

$$\mathbf{w}_{j,p} = \mathbf{c}_j \tag{6–10}$$

6.4.1 Filter Design

The 2nd term in (6–3) is the interference of the jth MT on the kth MT. That is:

$$MAI(j \rightarrow k) = \mathbf{q}_k^T \sum_{p=1}^{P} \mathbf{H}_{k,p} \mathbf{w}_{j,p} \tag{6–11}$$

The joint precoding and spreading weight vector $\mathbf{w}_{j,p}$ of the jth MT at the pth transmit antenna is then obtained by constraining the desired signal part of its own decision variable to a given constant while canceling (or zero-forcing) the MAI contribution at all other MTs. This leads to the following set of conditions:

$$\begin{cases} \mathbf{q}_j^T \sum_{p=1}^{P} \mathbf{H}_{j,p} \mathbf{w}_{j,p} = \alpha_j \\ \mathbf{q}_k^T \sum_{p=1}^{P} \mathbf{H}_{k,p} \mathbf{w}_{j,p} = 0 \;\; \forall k \neq j \end{cases} \tag{6–12}$$

where α_j is a positive real value that is chosen to meet some constraints. Note that the multiuser channel in (6–3) is decoupled into K single user parallel AWGN channel in (6–12) with transmission gains given by a specific value α_j, computed to meet some design criterion. By doing so, the purpose of the precoding is to eliminate the MAI caused by the jth user to other $K-1$ MTs and to mitigate the channel distortions of the jth user data symbol a_j at the jth MT. To compute the weight vector $\mathbf{w}_{j,p}$, we have to solve K linear equations given by:

$$\mathbf{Q}\mathbf{w}_j = \alpha_j \mathbf{b}_j \tag{6–13}$$

where $\mathbf{Q}$ is a complex channel and user code matrix of size $K \times PG$ and $\mathbf{b}_j$ is a vector of size K given by:

$$\mathbf{Q} = \begin{bmatrix} \mathbf{q}_1^T \mathbf{H}_{1,1} & \cdots & \mathbf{q}_1^T \mathbf{H}_{1,p} & \cdots & \mathbf{q}_1^T \mathbf{H}_{1,P} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{q}_j^T \mathbf{H}_{j,1} & \cdots & \mathbf{q}_j^T \mathbf{H}_{j,p} & \cdots & \mathbf{q}_j^T \mathbf{H}_{j,P} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{q}_K^T \mathbf{H}_{K,1} & \cdots & \mathbf{q}_K^T \mathbf{H}_{K,p} & \cdots & \mathbf{q}_K^T \mathbf{H}_{K,P} \end{bmatrix} \quad \mathbf{b}_j = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow j\text{th entry} \tag{6–14}$$

If we use the PD in (6–5) at the MT in (6–14) instead of the joint precoding and equalization in Section 6.3, the complex channel and user code matrix in (6–14) become:

$$\mathbf{Q} = \begin{bmatrix} \mathbf{c}_1^H\mathbf{H}_{1,1} & \cdots & \mathbf{c}_1^H\mathbf{H}_{1,p} & \cdots & \mathbf{c}_1^H\mathbf{H}_{1,P} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{c}_j^H\mathbf{H}_{j,1} & \cdots & \mathbf{c}_j^H\mathbf{H}_{j,p} & \cdots & \mathbf{c}_j^H\mathbf{H}_{j,P} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{c}_K^H\mathbf{H}_{K,1} & \cdots & \mathbf{c}_K^H\mathbf{H}_{K,p} & \cdots & \mathbf{c}_K^H\mathbf{H}_{K,P} \end{bmatrix} \quad \mathbf{b}_j = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow j\text{th entry} \tag{6–15}$$

where $(\cdot)^H$ denotes complex conjugate transpose. We want to minimize the transmitter power subject to K constraint given by (6–13). Thus the precoding optimization problem can be written as:

$$\underbrace{\min}_{\mathbf{w}_j} \mathbf{w}_j^H\mathbf{w}_j \quad \text{subject to} \quad \mathbf{Q}\mathbf{w}_j = \alpha_j\mathbf{b}_j \tag{6–16}$$

This optimization can be solved by the Lagrange multipliers method. The minimum-norm solution becomes:

$$\mathbf{w}_j = \alpha_j\mathbf{Q}^H\left(\mathbf{Q}\mathbf{Q}^H\right)^{-1}\mathbf{b}_j = \alpha_j\bar{\mathbf{w}}_j \tag{6–17}$$

where $\mathbf{Q}\mathbf{Q}^H$ is a complex square and Hermitian matrix of size $K \times K$, and $\bar{\mathbf{w}}_j$ represents the weight vector without power scaling and the transmitted power becomes:

$$\begin{aligned} p_{t,j} &= \bar{\mathbf{w}}_j^H\bar{\mathbf{w}}_j \\ &= \mathbf{b}_j^H\left(\mathbf{Q}\mathbf{Q}^H\right)^{-1}\mathbf{b}_j \end{aligned} \tag{6–18}$$

6.4.2 Power Allocation Strategies

Several linear power allocation approaches that can be used to limit the transmit power at a given constant will be discussed in this section. If we apply the weight vectors in (6–17) to (6–3), the decision variable of the jth MT becomes:

$$a_j^m = \alpha_j a_j^m + \mathbf{q}_j^T\mathbf{n}_j \tag{6–19}$$

The decision variable takes the same value as it would in a unitary gain AWGN channel, if the constraint α_j in (6–17) is normalized to 1 for a particular case. This implies that the received power is constrained to one at each MT, but there is no constraint on the transmitted power at the BS. Once the MAI is completely eliminated by using weight vectors in (6–17), different strategies can be used to constrain the transmit power subject to a given constraint [22]. There are several power constraint strategies in the literature [22, 25, 26, 46] for MC-CDMA such as maximization of the sum capacity, minimization of the average error probability, and linear power allocation approaches. However, we only consider linear power allocation approaches for the sake of simplicity.

The aim of linear power allocation approaches is to find simple expressions for the constraints α_j that can be easily implemented in practical mobile terminals. Overall transmitted power of all K active users is

$$\sum_{j=1}^{K} \alpha_j^2 \|\bar{\mathbf{w}}_j\|^2 = K \tag{6–20}$$

The constraint α_j can be obtained simply from (6–20),

$$\alpha_j = \sqrt{\frac{K}{\sum_{j=1}^{K} \|\bar{\mathbf{w}}_j\|^2}} \quad \forall j = 1, \cdots, K \tag{6–21}$$

In this case, the total transmitted power is normalized to K and the same constraint is used for all K active users as proposed in [43]. Another approach, called total interference removal (TIR), is to constrain the transmitted power to a given constant in order to normalize the weight vector $\bar{\mathbf{w}}$ according to [22, 24, 25, 65],

$$p_{t,j} = 1 \quad \forall j = 1, \cdots, K \tag{6–22}$$

In this case, the transmitted power is constrained to one, i.e., $\alpha_j^2 \|\bar{\mathbf{w}}_j\|^2 = 1$, for all K active users, and α_j is given by:

$$\alpha_j = \sqrt{\frac{1}{\|\bar{\mathbf{w}}_j\|^2}} \tag{6–23}$$

where $\|\cdot\|$ represent the Euclidian norm. In [22, 26], a modification, called m-TIR (modified-TIR), of the power constraint given by (6–23) was proposed. The idea is to minimize the sum of the inverse of SNR, not SNR under the constraint given by (6–13) which the total transmitter power is constrained to K. Thus, the following cost function was introduced in [22, 26].

$$J_{\text{m-TIR}} = \sum_{j=1}^{K} \frac{\sigma_n^2}{\alpha_j^2} + \lambda \left(K - \sum_{j=1}^{K} \alpha_j^2 \|\mathbf{w}_j\|^2 \right) \tag{6–24}$$

The α_j for each user j by the m-TIR is given by:

$$\alpha_j = \sqrt{\frac{K}{\|\bar{\mathbf{w}}_j\| \sum_{j=1}^{K} \|\bar{\mathbf{w}}_j\|}} \tag{6–25}$$

Intuitively, the constraints given by (6–25) and (6–21) only give better performance than the one given by (6–23) for the case where we do not have enough degree of freedom to minimize the transmit power [22].

6.4.3 Performance Analysis

In this section, we study the BER performance of linear power allocation approaches in the previous section. The BER of the user j in (6–19) is given by:

$$P_e(\alpha_j) = \mathbf{E}_{\alpha_j} \left[Q\left(\sqrt{\frac{\alpha_j^2}{\sigma_n^2}} \right) \right] \tag{6–26}$$

from (6–19) with $Q(x) = 1/\sqrt{2\pi} \int_x^\infty e^{-t^2/2} dt$ where $\mathbf{E}[\cdot]$ denotes expectation. If we use the α_j in (6–23), the BER of the user j can be written as follows:

$$\begin{aligned} P_{e,TIR}(\alpha_j) &= \mathbf{E}_{\alpha_j} \left[Q\left(\sqrt{\frac{1}{\sigma_n^2 \|\bar{\mathbf{w}}_j\|^2}} \right) \right] \\ &= \mathbf{E}_{\alpha_j} \left[Q\left(\sqrt{\frac{1}{\sigma_n^2 \mathbf{R}_{j,j}^{-1}}} \right) \right] \end{aligned} \tag{6–27}$$

since

$$\begin{aligned}\|\bar{\mathbf{w}}_j\|^2 &= \bar{\mathbf{w}}_j^H \bar{\mathbf{w}}_j \\ &= \mathbf{b}_j^H \left(\mathbf{Q}\mathbf{Q}^H\right)^{-1} \mathbf{b}_j \\ &= \mathbf{b}_j^H \mathbf{R}^{-1} \mathbf{b}_j = \mathbf{R}_{j,j}^{-1}\end{aligned} \tag{6–28}$$

where $\mathbf{R}_{j,j}^{-1}$ denotes the (k,k) element of the inverse of the scatter matrix $\mathbf{R} = \mathbf{Q}\mathbf{Q}^H$. Let $\mathbf{Q} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^H$ denote the singular value decomposition of $K \times LM$-sized $\mathbf{Q}$ where $\mathbf{U}$ is the $K \times K$ unitary left singular vector matrix, $\mathbf{\Sigma}$ is $K \times LM$ diagonal singular value matrix with nonnegative real numbers on the diagonal, and $\mathbf{V}^H$ denotes the conjugate transpose of $\mathbf{V}$, an $LM \times LM$ unitary right singular vector. Then, the scatter matrix $\mathbf{R}$ can be factored into

$$\begin{aligned}\mathbf{R} &= \mathbf{Q}\mathbf{Q}^H \\ &= \mathbf{U}\mathbf{\Sigma}\mathbf{V}^H\mathbf{V}\mathbf{\Sigma}^H\mathbf{U}^H \\ &= \mathbf{U}\mathbf{\Lambda}\mathbf{U}^H\end{aligned} \tag{6–29}$$

where $\mathbf{\Lambda}$ is the diagonal matrix, the entries of which are eigenvalues λ_j for $j = 1, \cdots, K$. Since $\mathbf{R}^{-1} = \mathbf{U}\mathbf{\Lambda}^{-1}\mathbf{U}^H$ and $\mathbf{R}_{j,j}^{-1} = \mathbf{\Lambda}_{j,j}^{-1} = \lambda_j^{-1}$, $\alpha_j = \sqrt{\lambda_j}$. Therefore, the BER of the jth user with α_j in (6–23) becomes:

$$P_{e,TIR}\left(\alpha_j\right) = \mathbf{E}_{\lambda_j}\left[Q\left(\sqrt{\frac{\lambda_j}{\sigma_n^2}}\right)\right] \tag{6–30}$$

If we use the gain α_j in (6–25) and (6–21), the BER of the jth user becomes

$$\begin{aligned}P_{e,SINR}\left(\alpha_j\right) &= \mathbf{E}_{\alpha_j}\left[Q\left(\sqrt{\frac{K}{\sigma_n^2 \sum_{k=1}^{K} \|\bar{\mathbf{w}}_k\|^2}}\right)\right] \\ &= \mathbf{E}_{\lambda_j}\left[Q\left(\sqrt{\frac{K}{\sigma_n^2 \sum_{k=1}^{K} \lambda_k^{-1}}}\right)\right]\end{aligned} \tag{6–31}$$

and

$$
\begin{aligned}
P_{e,m-TIR}\left(\alpha_j\right) &= \mathbf{E}_{\alpha_j}\left[Q\left(\sqrt{\frac{K}{\sigma_n^2\|\bar{\mathbf{w}}_j\|\sum_{k=1}^{K}\|\bar{\mathbf{w}}_k\|}}\right)\right] \\
&= \mathbf{E}_{\lambda_j}\left[Q\left(\sqrt{\frac{K\lambda_j^{1/2}}{\sigma_n^2\sum_{k=1}^{K}\lambda_k^{-1/2}}}\right)\right]
\end{aligned}
\tag{6–32}
$$

Note that the BER performance of the jth user in (6–27), (6–31), and (6–32) depends on the eigenvalues of the scatter matrix $\mathbf{R} = \mathbf{Q}\mathbf{Q}^H$. The numerical average BER becomes:

$$
\begin{aligned}
P_{avg} &= \frac{1}{K}\sum_{j=1}^{K} P_e\left(\alpha_j\right) \\
&= \frac{1}{K}\sum_{j=1}^{K} Q\left(\frac{\alpha_j}{\sigma_n}\right)
\end{aligned}
\tag{6–33}
$$

6.5 Simulation and Verification

To evaluate the performance of various linear power allocation approaches discussed Section 6.4 with the SUD in Section 6.3 for the MC-CDMA system in Section 6.2, we use system parameters based on the 802.11a physical layer standard. We assume that the distance between transmit antennae is far apart to consider P independent channels for each user.

The main simulation parameters used in this simulation are the number of sub-carrier (N_c) set to 64; OFDM symbol duration is 3.2μs; system bandwidth is 20MHz; number of data symbol (M) per frame is 8; length of spread code (L) or spreading factor (SF) is 8; cyclic prefix contains 16 samples or 0.8μs; number of active users is 1, 4, or 8 ($K \leq L$); modulation is BPSK; and channel is modeled as Rayleigh fading with AWGN channel. We use Walsh-Hadamard spreading sequences for a DL synchronized transmission. The channel is flat at least between two sub-carriers and is kept fixed over an OFDM symbol duration, but it varies from OFDM symbol to symbol. As mentioned, we assume a perfect CSI knowledge for the unlink channel at the BS and for the DL at the MT (if the single

user detection schemes are employed). No channel coding scheme is employed for the sake of simplicity.

It is interesting to observe the effects of number of active users ($K \leq L$) and the number of transmitter antennae, P, on the BER performance when the PS in (6–10) and MRC in (6–6) are used at both the BS and MTs, respectively. We refer this approach as the PS/MRC and the same notation will be used in the sequel. The effect of MRC is equivalent to that of the matched filtering, where the filtering is matched to the channel transfer function. Matched filtering constitutes the optimal filtering, which maximizes the SNR at the output of the decision device. The achievable BER, P_e, of the single user performance of MRC over Rayleigh fading channel having D-independent propagation paths (or diversity order) is given by:

$$P_e = \left[\frac{1}{2}(1-\mu)\right]^D \sum_{k=0}^{D-1} \binom{D-1+k}{k} \left[\frac{1}{2}(1+\mu)\right]^k \tag{6–34}$$

where μ is defined as

$$\mu \simeq \sqrt{\frac{\bar{\gamma}_b}{D+\bar{\gamma}_b}} \tag{6–35}$$

and $\bar{\gamma}_b$ is the average energy per bit, $\bar{E}_b$, divided by the noise power spectral density, N_0 [23]. The signal-to-interference-noise ratio (SINR) in (6–3) of PS/MRC with $P = 1$ is

$$\bar{\gamma}_{b,SINR} = \frac{\bar{E}_b}{N_I + N_0} = \frac{\bar{E}_b}{\bar{E}_b(K-1)/L + N_0} \tag{6–36}$$

Simulation results for SF=8 with one transmit antenna ($P = 1$) is shown in Figure 6-2. The analysis curves are drawn by (6–34) with (6–35) and (6–36) for $K = 1$ and $K = 8$. As the number of active users was increased, the BER increased significantly due to the increased amount of the 2nd term in (6–3). Figure 6-3 shows effects of array gain on the BER performance of the PS/MRC with P =1, 2, and 4 transmit antennae for single user ($K = 1$). As the number of transmit antennae was increased, the BER decreased due to the array gain.

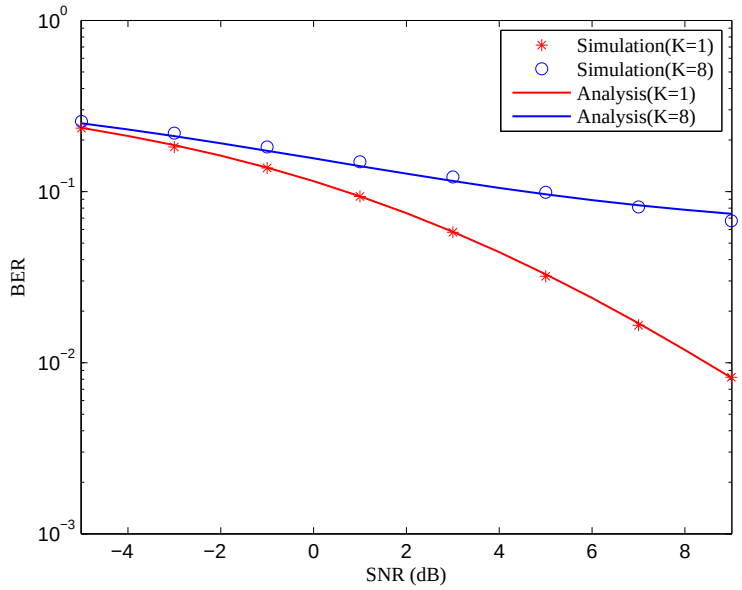


Figure 6-2. Average BER of synchronous MC-CDMA downlink using PS/MRC for single user ($K = 1$) and full load ($K = 8$) with $P = 1$ over Rayleigh fading channel

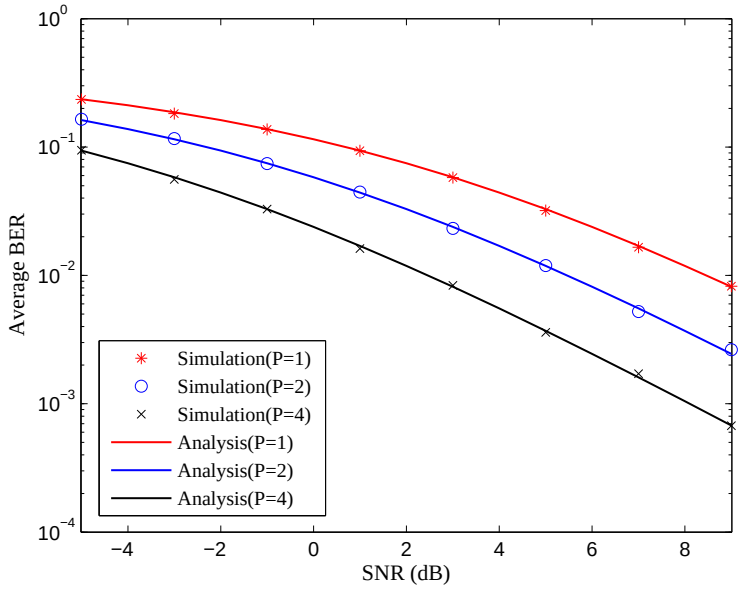


Figure 6-3. Effect of array gain on the average BER using PS/MRC for single user ($K = 1$) with $P = 1, 2, 4$ over Rayleigh fading channel

Next, we analyze the average BER performance of a joint space-frequency precoding with the TIR/MRC scheme. As mentioned in Section 6.4.1, the multiuser channel is decoupled into K single user parallel AWGN channels with transmission gain given by a specific constant α_j in (6–23), which is constrained to one for all K active users by (6–22). Since the MRC is employed, the gain α_j is to choose the weights to be faded to each sub-carrier. Therefore, we can use the single user performance in (6–34) with the diversity order D. Since we use both the space diversity and frequency diversity at the same time in the joint precoding, the diversity order is a function of these diversities. Figure 6-4 shows the average performance of the TIR/MRC approach. Analysis curves in Figure 6-4 are drawn by (6–34) with the diversity order, $D_{TIR/MRC} = D_{PS/MRC} + P - 1$, and average signal-to-noise ratio $\bar{\gamma}_{b,TIR/MRC} = P\bar{E}_b/N_0$. This analytical performance can provide an efficient prediction of various combinations of the joint precoding schemes in Section 6.4.

Figures 6-6 to 6-9 are simulation results of various combinations of joint precoding and single user equalization with respect to the TIR/MRC scheme. The performance results of different space-frequency precoding approaches are derived for the MC-CDMA in terms of the average BER as a function of SNR.

We can see that the BER performance is enhanced as the number of transmit antennae increased due to array gain. The performance with m-TIR in (6–25) and SINR in (6–21) is, in general, better than that of TIR in (6–23), since these schemes can redistribute the transmission power among active users according to the CSI. However, the performance with ORC in Figure 6-8 indicates that the ORC with unequal power constraints can degrade the performance with respect to equal power constraint.

From Figure 6-5 and Figure 6-7, the performance of the precoding with the PD and EGC is basically the same; only minor differences in terms of gains is observed. The use of an equalizer at the MTs brings some benefits, since the burden of mitigating channel impairments can be distributed among the BS and MTs when the BS is equipped with only one or two transmit antennae. This may incur increasing computational complexity

at the MTs. If we have enough space diversity, the MTs may not be required to use single user equalization schemes.

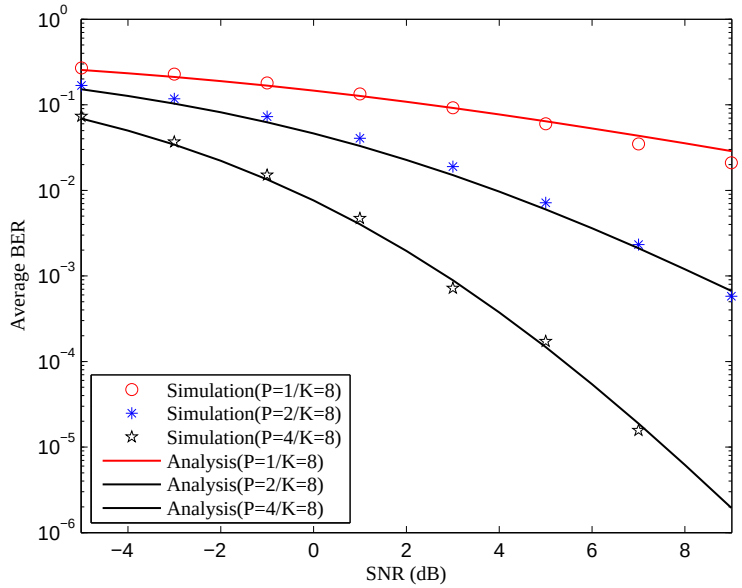


Figure 6-4. Average BER of synchronous MC-CDMA downlink using TIR/MRC for K=8 active users with $P = 1, 2, 4$ over Rayleigh fading channel

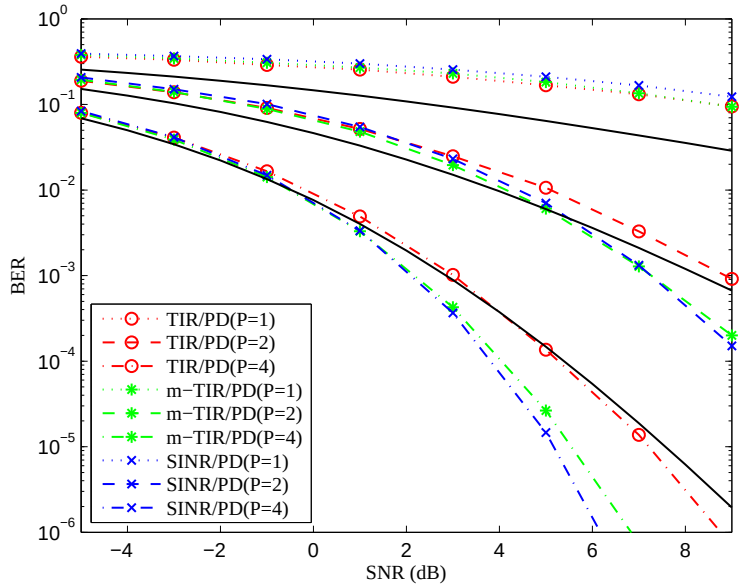


Figure 6-5. Performance comparison of synchronous MC-CDMA downlink using PD for K=8 active users with $P = 1, 2, 4$ over Rayleigh fading channel

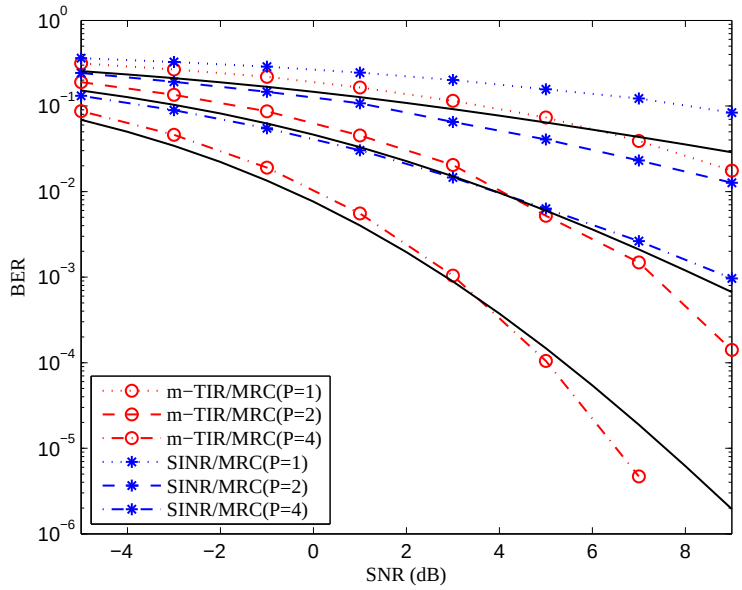


Figure 6-6. Performance comparison of synchronous MC-CDMA downlink using MRC for K=8 active users with $P = 1, 2, 4$ over Rayleigh fading channel

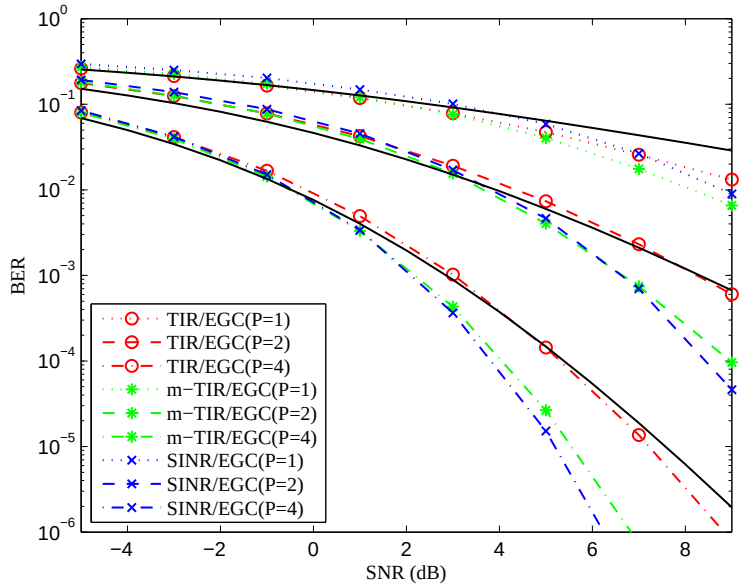


Figure 6-7. Performance comparison of synchronous MC-CDMA downlink using EGC for K=8 active users with $P = 1, 2, 4$ over Rayleigh fading channel

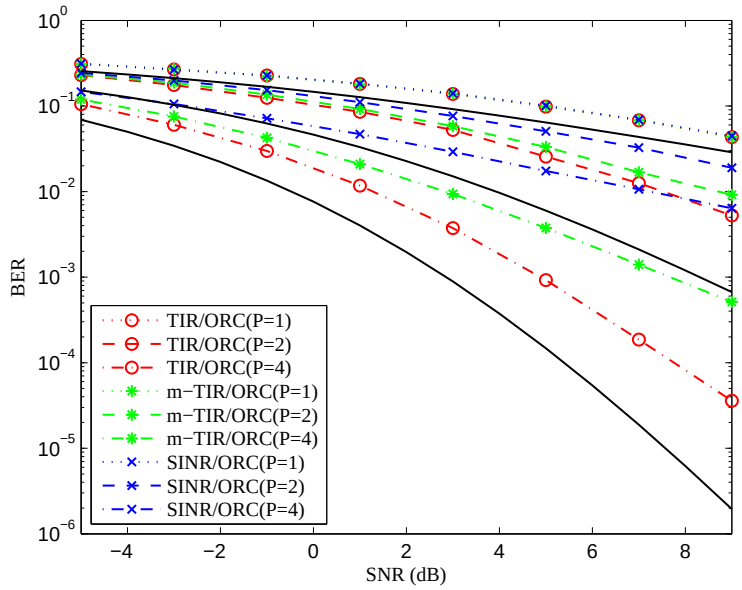


Figure 6-8. Performance comparison of synchronous MC-CDMA downlink using ORC for K=8 active users with $P = 1, 2, 4$ over Rayleigh fading channel

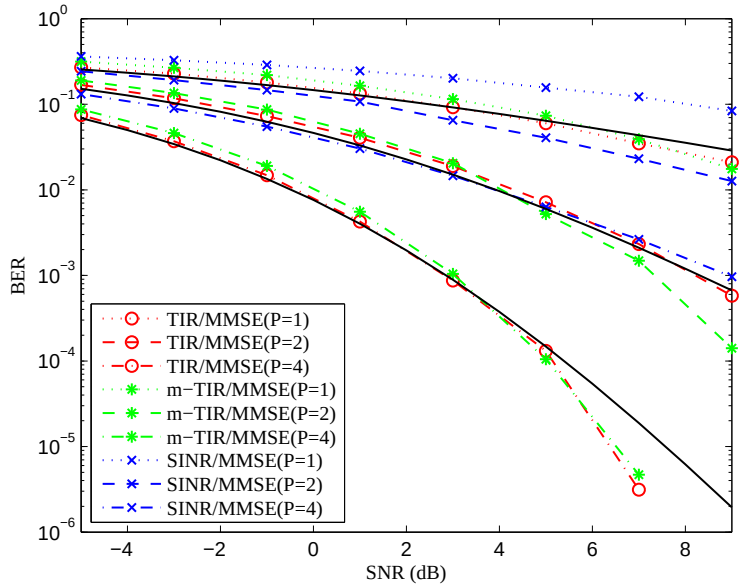


Figure 6-9. Performance comparison of synchronous MC-CDMA downlink using MMSE for K=8 active users with $P = 1, 2, 4$ over Rayleigh fading channel

6.6 Summary

We analyze the performance of joint space-frequency precoding approaches in terms of the average BER performance. Several linear transmitter power allocation strategies incorporated together with single user equalization schemes are compared to a joint precoding with an equal power constraint at the BS and MRC at the MTs. The performance of various linear space-frequency precoding schemes is a function of eigenvalues of the scatter matrix which can be computed by the channel state information and spreading codes of all active users. It is very clear from the presented results that the precoding schemes allow a significant performance improvement over one transmit antenna at the BS exploiting space-frequency diversity.

CHAPTER 7
MULTI-CARRIER TRANSFORM DOMAIN COMMUNICATION SYSTEM: AN INTERFERENCE AVOIDANCE MULTI-CARRIER SYSTEM

7.1 Introduction

Wireless communication security both for the civilian and military parties is a critical issue. Thought the same may be said of all communication systems, wireless communication systems have special requirements and vulnerabilities, therefore we have a special concern for securing those systems [13, 66].

A cost effective transmission technique that can use scarce spectral resource is in need for wireless services. Multi-carrier code division multiple access (MC-CDMA) has been developed as a candidate air-interface, especially for downlink (DL), to provide high bit rates. However, the performance of MC-CDMA is essentially limited by multiple access interference (MAI), and low computational complexity or resource usages are desired at mobile terminals (MTs) [21–23]. Especially for the military communication system, it is very important to be able to operate in the presence of both jamming and unintentional interference.

To mitigate the MAI, the use of pre-filtering with MC-CDMA systems has also been considered recently. Pre-filtering approaches designed in frequency and space for DL time division duplex (TDD) MC-CDMA systems have been proposed in [22, 24–27]. However, not much work has been done to mitigate jamming for the MC-CDMA. The MC-CDMA has anti-jamming capability due to usage of spread sequence, not interference avoidance capability.

Transform domain communication system (TDCS) can provide the interference avoidance capability for single-carrier (SC) communication system [9, 11]. In the TDCS, an interference avoiding waveform is adaptively generated both at the transmitter and receiver side in frequency domain via a spectral environment estimation and spectral notching process. Several approaches have been proposed to mitigate narrow band interference (NBI) and to enhance performance of the single-input single-output (SISO)

SC-TDCS under jamming and additive white Gaussian noise channel (AWGN) [9, 10, 19, 34].

For multiple-input multiple-output (MIMO), especially vertical-Bell Laboratories layered space-time (V-BLAST) system, the fundamental concept of transform domain processing (TDP) and zero-forcing (ZF) V-BLAST was combined to mitigate NBI in [12]. However, the approach used in [12] did not work well for non-stationary interferences because of the noise enhancement of the ZF detector. In [35], authors extend our previous approach in [34] to V-BLAST to provide non-stationary as well as stationary interference avoidance capabilities to the V-BLAST system.

A performance comparison of the SC-TDCS and (multi-carrier) OFDM based cognitive radio for MIMO system using V-BLAST receiver architecture to reconstruct the transmitted data in Rayleigh fading channel was presented in [32]. A modification of both the transmitter and the receiver block diagram according to [11] had been made in their system. CR with OFDM consistently outperforms the CR with TDCS architecture by more than $5 - 6$ dB signal-to-noise ratio (SNR) per bit gain either for a single transmit and receive antenna or MIMO system with a balanced design of transmit and receive antennae[1] with antipodal modulation scheme and frequency domain zero-forcing equalizer. Since the zero-forcing equalizer removed the frequency selectivity of the channel transfer function, there is no room for improvement with the aid of the frequency domain diversity. Therefore, we need to enhance the bit error rate (BER) performance of the TDCS under Rayleigh fading with the help of the frequency domain diversity combining techniques.

OFDM-based transform domain communication system in CR for control message transmission was proposed in [29]. However, only a SISO antenna configuration was considered and the performance under the intentional interference was not investigated.

[1] See Figure 7 in [32].

Research results aimed at characterizing TDCS performance in multiple access environment (MAE) under AWGN channel was presented in [28] and that performance under multipath fading was studied in [29].

The purpose of this chapter is to propose a multi-carrier TDCS (MC-TDCS). The concept of TDP processing and multi-carrier modulation (MCM) are combined together in MC-TDCS to avoid intentional interference and to combat multipath fading. We also study the performance under multiuser and incorporate a precoding at transmitter antenna array to mitigate the MAI at the transmitter, not at the receiver.

The contributions of this chapter are: (i) the performance improvement of TDCS under multipath fading with the help of frequency domain diversity, (ii) the mitigation of jamming and provision of the interference avoidance capability, (iii) the transmitter antenna array precoding (or pre-filtering) to mitigate the MAI interference, and (iv) analytical performance evaluation of the proposed MC-TDCS. Therefore, the proposed MC-TDCS will be a viable option for the TDCS over multipath fading with AWGN.

The remainder of this chapter is organized as follows: Section 7.2 elaborates on a system model of the proposed MC-TDCS and describes a mathematical model of the proposed system. Then, various single user equalizer performance for the single user detection is investigated in Section 7.3. Section 7.4 describes how to mitigate the MAI with helps of the transmitter diversity and the precoding at the transmitter. The performance under NBI is validated in Section 7.5. Finally, Section 7.6 summarizes this chapter.

7.2 MC-TDCS System Model

In this section, we elaborate on both the system architecture and mathematical model of the proposed DL MC-TDCS. Figure 7-1 shows the proposed DL MC-TDCS transmitter of the base station (BS) and the receiver of the k'th user mobile terminal (MT). The BS and MTs jointly use a pre-filtering and frequency domain equalizer, respectively. MC-TDCS is a multi-carrier transmission where its bandwidth can be divided into smaller

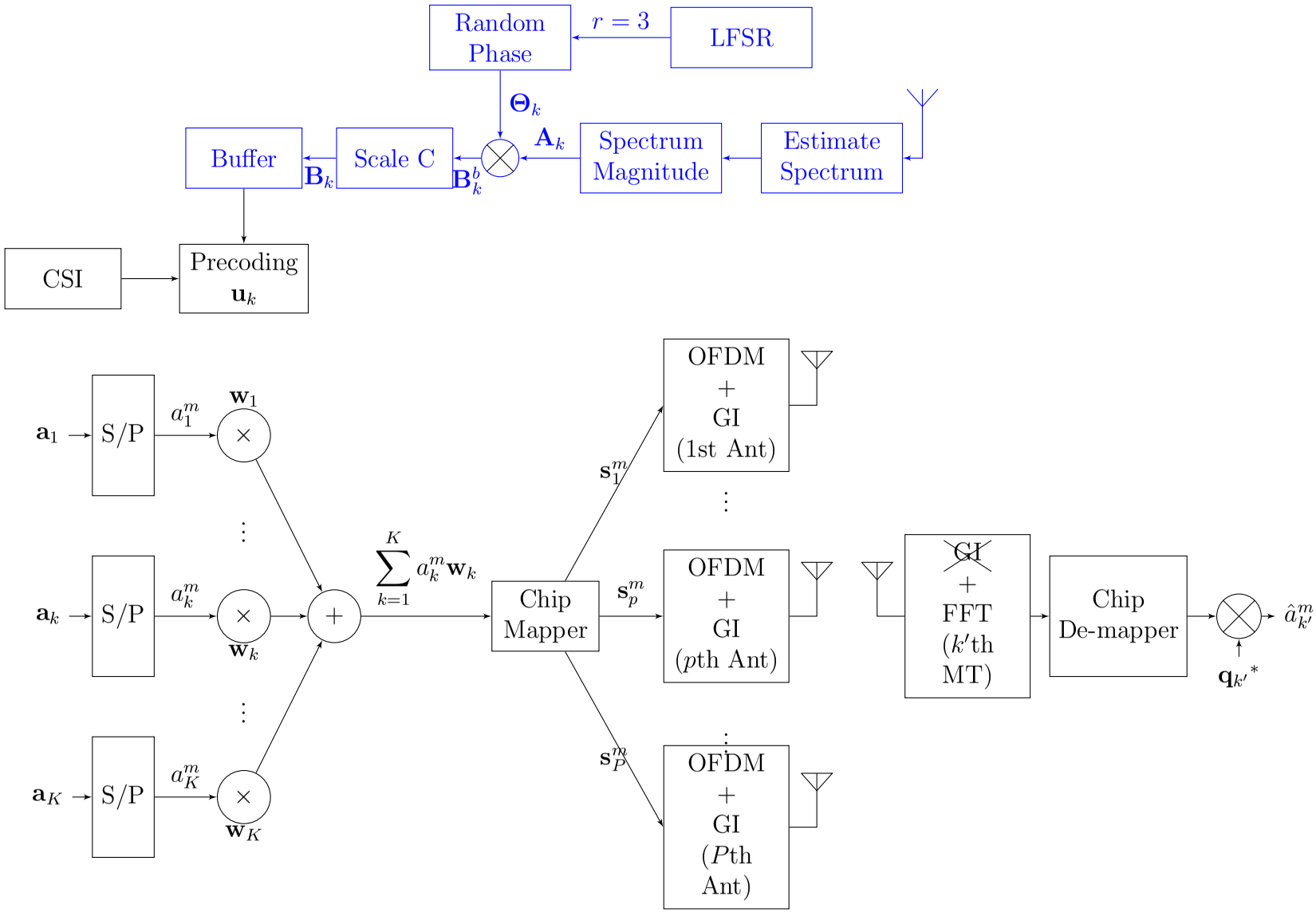


Figure 7-1. Transmitter and receiver architecture of MC-TDCS with multiple transmitter antennae, pre-filtering and receiver-based equalization

sub-bands. In MC-TDCS, instead of applying an interference-free signature wave in time domain [9, 11], we can apply them in frequency domain, mapping a different chip of a fundamental modulation signature waveform (FMW) to an individual OFDM sub-carrier adaptively.

The total number of sub-carriers N_c is divided into M smaller groups of L elements of the sub-carriers where $M = N_c/L$ in the DL MC-TDCS networks. Therefore each user k transmits M data symbols per OFDM symbol. Hence each OFDM symbol has a data rate proportional to M times the original input data symbols. We assume that the BS has P transmitter antennae and uses the sub-carriers of a given group to communicate K active users ($K \leq L$). Active users are separated by their specific FWM $\mathbf{B}_k$ of the kth user, adaptively generated by spectrum magnitude $\mathbf{A}_k$, and random phase vector $\mathbf{\Theta}_k$. Let's assume the M sub-carriers of a given group are uniformly distributed over the signal bandwidth to better exploit frequency diversity. Let i_n^m denote a sub-carrier index of the mth symbol of the kth user with $i_n^m = m + (n-1)N/L$ and $1 \leq n \leq L$. After estimation of the spectral environment, a sub-band exceeds that of the noise level by a factor of a threshold level, interference is claimed to be present and the sub-band is notched out, assigning magnitude value '0'. Otherwise, the sub-bands are retained and set to the value of '1'. That is:

$$A_k(n) = \begin{cases} 0 \text{ if jammed} \\ 1 \text{ otherwise} \end{cases} \tag{7–1}$$

The spectrum magnitude vector $\mathbf{A}_k = [A_k(1) \cdots A_k(L)]^T$ of the kth user is an element-by-element product of a random phase vector $\mathbf{\Theta}_k = [\theta_k(1) \cdots \theta_k(L)]^H$ of the user k where $\theta_{k,p}(n)$ is generated by r-bit outputs of a linear feedback shift register (LFSR) and $(\cdot)^{T(H)}$ denotes the (conjugate) transpose. If $r = 3$, for example, $\theta_k(n)$ has a value among

$\left[1, e^{j2\pi/8}, \cdots, e^{j2\pi(2^3-1)/8}\right]$ with an equal probability $1/2^r = 1/8$. Figure 7-2 shows the pseudo-random phase vector for r bit outputs of a LFSR. [2]

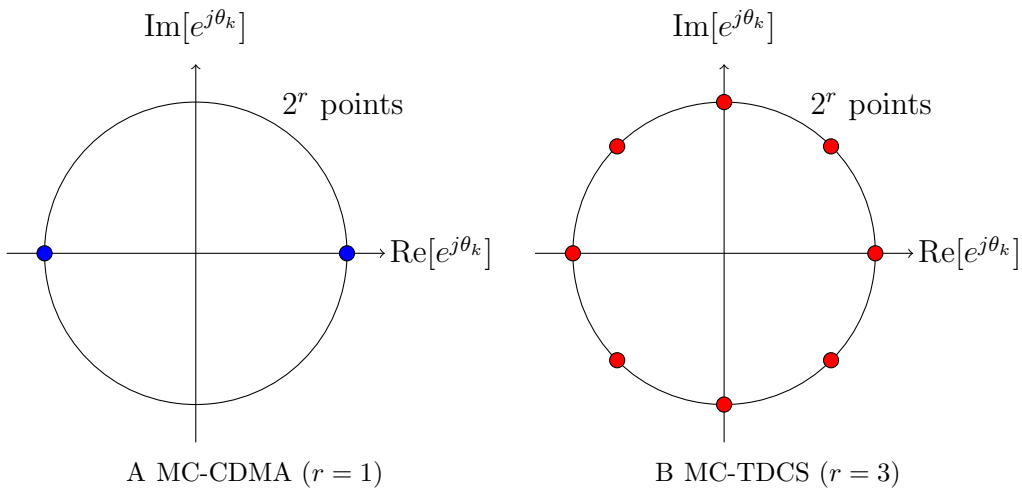


Figure 7-2. Pseudo-random phase vector for r, where r denotes the number of random sequence bits generated by LFSR

Then, the unscaled $\mathbf{B}_b$ becomes:

$$\begin{aligned} \mathbf{B}_k^b &= \mathbf{A}_k \odot \mathbf{\Theta}_k \\ &= [A_k(0)\theta_k(0), \cdots, A_k(L)\theta_k(L)]^H \end{aligned} \tag{7–2}$$

where $\odot$ denotes the Hadamard product (or entry-wise product). The energy-scaled FMW $\mathbf{B}_k$ of the kth user is:

$$\mathbf{B}_k = \mathbf{B}_k^b \frac{1}{\sqrt{\sum_{n=1}^{L} |A_k(n)\theta_k(n)|^2}} \tag{7–3}$$

The data symbol vector $\mathbf{a}_k$ of the user k is fed into the serial-to-parallel block and the mth symbol of the kth user, a_k^m, is spread by L chips using the FMW sequence $\mathbf{B}_k = [B_k(1), \cdots, B_k(L)]^H$ of the kth user. The resulting $a_k^m \mathbf{B}_k$ is weighted by a pre-filtering coefficient $\mathbf{u}_{k,p}$ of the kth user at the pth antenna and is fed to each antenna. The weighted output $\mathbf{w}_{k,p} = [w_{k,p}(1), \cdots, w_{k,p}(L)]^H$ of the kth user of the pth antenna is

[2] The proposed MC-TDCS can be regarded as a generalization of MC-CDMA.

a vector with entries $w_{k,p}(n) = c_k(n)u_{k,p}(n)$ for $n = 1, \cdots, L$. If the pre-filtering is not employed at the transmitter antennae, $\mathbf{w}_{k,p} = \mathbf{c}_k$ and $\mathbf{u}_{k,p} = \mathbf{1}_L$ where $\mathbf{1}_L$ denotes the $L \times 1$ matrix with one. The contribution of all K users are summed together in each sub-carrier index $i_n^m (1 \leq n \leq L)$ to form the following multiuser signal at the pth antenna

$$\mathbf{s}_p^m = \sum_{k=1}^{K} a_k^m \mathbf{w}_{k,p}, \quad p = 1, \cdots, P \tag{7–4}$$

Then, each $\mathbf{s}_p^m$ is uniformly mapped on L sub-carriers using the chip mapper[3] . After an OFDM modulator for each antenna, a N_G-point cyclic prefix (CP) (or guard interval (GI)) is added in the transmitted signals to avoid interference between adjacent OFDM blocks.

The transmitted signals by the BS array propagate through multipath channels and experience frequency-selective fading. We assume each MT has a single antenna and let $\mathbf{h}_{k,p} = [h_{k,p}(0), \cdots, h_{k,p}(L_{k,p} - 1)]^T$ be the discrete channel state information (CSI) between the pth transmission antenna and the kth MT. We assume the CSIs are practically constant over the DL time slot and perfect CSI is assumed at the BS for simplicity.

The transmitted signals from the P transmission antennae are recombined by the receiver antenna and are passed to an OFDM demodulator. The demodulator outputs $\mathbf{X}_{k'} = [X_{k'}(1), \cdots, X_{k'}(L)]^H$ correspond to the L sub-carriers of the considered group of the k'th user MT. If we assume ideal frequency and timing synchronization, we have

$$\mathbf{X}_{k'}^m = \sum_{p=1}^{P} \sum_{k=1}^{K} a_k^m \mathbf{H}_{k',p} \mathbf{w}_{k,p} + \mathbf{n}_{k'} \tag{7–5}$$

where $\mathbf{H}_{k',p}$ is a diagonal matrix

$$\mathbf{H}_{k',p} = \mathrm{diag}\left\{H_{k',p}(i_1^m), \cdots, H_{k',p}(i_L^m)\right\} \tag{7–6}$$

[3] The chip mapper and de-mapper can use another mapping and de-mapping policy, while we only consider the uniform mapping and de-mapping, for simplicity.

and $H_{k',p}(i_n^m)$ is the channel frequency response over the i_n^mth sub-carrier and is computed by taking the discrete fourier transform of $\mathbf{h}_{k,p}$

$$H_{k',p}(i_n^m) = \sum_{l=0}^{L_{k',p}-1} h_{k',p}(l) e^{-j\frac{2\pi l i_n^m}{N}}, \quad n = 1, \cdots, L \quad \& \quad m = 1, \cdots, M \tag{7–7}$$

and $\mathbf{n}_{k'} = [n_{k'}(1), \cdots, n_{k'}(L)]^T$ is thermal noise with zero mean and covariance matrix $\sigma_n^2 \mathbf{I}_L$.

The decision variable at the input of the demodulator for the desired k'th user is given by

$$\begin{aligned} \hat{a}_{k'}^m &= \mathbf{q}_{k'}^T \mathbf{X}_{k'}^m \\ &= \underbrace{a_{k'}^m \mathbf{q}_{k'}^T \left(\sum_{p=1}^{P} \mathbf{H}_{k',p} \mathbf{w}_{k',p} \right)}_{\text{Desired signal}} + \underbrace{\left(\sum_{k=1, k\neq k'}^{K} a_k^m \mathbf{q}_k^T \sum_{p=1}^{P} \mathbf{H}_{k',p} \mathbf{w}_{k,p} \right)}_{\text{MAI}} + \underbrace{\mathbf{q}_{k'}^T \mathbf{n}_{k'}}_{\text{Noise}} \\ &= \alpha + \zeta + \eta \end{aligned} \tag{7–8}$$

where $\mathbf{q}_k = [q_k(1), \cdots, q_k(L)]^T$ is a vector of size L that account for the both despreading and channel equalization operations. If we only use the pre-filtering at the transmitter antennae, we can use the pure despreading (PD) in order to keep the MTs at very low complexity. The despreading and channel equalization vector $\mathbf{q}_k$ is the same as the user's FMW $\mathbf{B}_k$ for the PD. Several channel equalization methods for single user detection will be discussed in the sequel.

7.3 Single User Detection

Three signal components in (7–8) predetermine the performance of the single user detection considered in this section. For single user detection, the equalizer coefficients are given by:

$$\mathbf{q}_k = \mathbf{G}_k \mathbf{B}_k^* \tag{7–9}$$

where $*$ denotes the complex conjugate and $\mathbf{G}_k = \text{diag}\{g_k(1), \cdots, g_k(L)\}$ is a diagonal matrix of size $L \times L$ representing coefficients of the channel equalizer, while the joint

pre-filtering and spreading coefficient becomes $\mathbf{w}_{k,p} = \mathbf{B}_k$. Therefore, the decision variable at the input of the demodulator in (7–8) becomes:

$$\begin{aligned}
\hat{a}_{k'}^m &= \mathbf{q}_{k'}^T \mathbf{X}_{k'}^m \\
&= \left(\mathbf{G}_{k'}\mathbf{B}_{k'}^*\right)^T \mathbf{X}_{k'}^m \\
&= \underbrace{a_{k'}^m \left(\mathbf{G}_{k'}\mathbf{B}_{k'}^*\right)^T \left(\sum_{p=1}^{P} \mathbf{H}_{k',p}\mathbf{B}_{k'}\right)}_{\text{Desired signal}} + \underbrace{\left(\sum_{k=1,k\neq k'}^{K} a_k^m \left(\mathbf{G}_k\mathbf{B}_k^*\right)^T \sum_{p=1}^{P} \mathbf{H}_{k,p}\mathbf{B}_k\right)}_{\text{MAI}} + \underbrace{\left(\mathbf{G}_{k'}\mathbf{B}_{k'}^*\right)^T \mathbf{n}_{k'}}_{\text{Noise}} \\
&= \underbrace{a_{k'}^m \left(\mathbf{B}_{k'}^H\mathbf{G}_{k'}\right) \left(\sum_{p=1}^{P} \mathbf{H}_{k',p}\mathbf{B}_{k'}\right)}_{\text{Desired signal}} + \underbrace{\left(\sum_{k=1,k\neq k'}^{K} a_k^m \left(\mathbf{B}_k^H\mathbf{G}_k\right) \sum_{p=1}^{P} \mathbf{H}_{k,p}\mathbf{B}_k\right)}_{\text{MAI}} + \underbrace{\left(\mathbf{B}_{k'}^H\mathbf{G}_{k'}\right) \mathbf{n}_{k'}}_{\text{Noise}} \\
&= \alpha_s + \zeta_s + \eta_s
\end{aligned} \tag{7–10}$$

where the subscript s denotes the SUD.

7.3.1 Maximal Ratio Combining

In maximal ratio combining (MRC) a stronger signal is assigned a higher weight by the diversity combiners than a weaker signal, since its contribution is more reliable. The corresponding equalization gain $\mathbf{G}_k$ is given as:

$$g_k(n) = \left(\sum_{p=1}^{P} H_{k,p}(i_n^m)\right)^* \quad n = 1, \cdots, L \tag{7–11}$$

The corresponding user's received signal component, α_s, is given by

$$\begin{aligned}
\alpha_s &= a_{k'}^m \mathbf{B}_{k'}^H \mathbf{G}_{k'} \sum_{p=1}^{P} \mathbf{H}_{k',p}\mathbf{B}_{k'} \\
&= a_{k'}^m \mathbf{B}_{k'}^H \left(\sum_{p=1}^{P} \mathbf{H}_{k',p}^* \sum_{p=1}^{P} \mathbf{H}_{k',p}\right) \mathbf{B}_{k'} \\
&= a_{k'}^m \sum_{p=1}^{P} \left|\mathbf{H}_{k',p}\right|^2
\end{aligned} \tag{7–12}$$

On the other hand, the MAI associated with MRC is given by

$$\begin{aligned}\zeta_s &= \sum_{k=1,k\neq k'}^{K} a_k^m \mathbf{B}_k^H \mathbf{G}_k \sum_{p=1}^{P} \mathbf{H}_{k,p}\mathbf{B}_k \\ &= \sum_{k=1,k\neq k'}^{K} a_k^m \mathbf{B}_k^H \sum_{p=1}^{P} \mathbf{H}_{k,p}^* \sum_{p=1}^{P} \mathbf{H}_{k,p}\mathbf{B}_k \\ &= \sum_{k=1,k\neq k'}^{K} a_k^m \mathbf{B}_k^H \left(\sum_{p=1}^{P} |\mathbf{H}_{k,p}|^2\right) \mathbf{B}_k\end{aligned} \tag{7–13}$$

Finally, the noise term, η_s, is obtained by

$$\eta_s = \mathbf{B}_{k'}^H \left(\sum_{p=1}^{P} \mathbf{H}_{k',p}\right) \mathbf{n}_{k'} \tag{7–14}$$

The effect of the matched filtering is equivalent to that of the MRC. Matched filtering constitutes the optimal filtering, which maximizes the SNR at the output of the decision device. The single user performance of MRC over Rayleigh fading channel having $L_{k,p}$ independent propagation paths for $P = 1$ is given by:

$$\bar{P}_e = \left[\frac{1}{2}(1-\mu)\right]^{L_{k,p}} \sum_{k=0}^{L_{k,p}-1} \binom{L_{k,p}-1+k}{k} \left[\frac{1}{2}(1+\mu)\right]^k \tag{7–15}$$

where μ is defined as

$$\mu \simeq \sqrt{\frac{\bar{\gamma}_b}{L_{k,p}+\bar{\gamma}_b}} \tag{7–16}$$

and $\bar{\gamma}_b$ is the average energy per bit, $\bar{E}_b$, divided by the noise power spectral density, N_0 [23]. A simulation result is shown in Figure 7-3 for $N_c = 1024$ sub-carriers, $L = 256$ code lengths, and $P = 1$ single antenna while varying the number of independent multipath $L_{k,p}$ paths over $E_b/N_0 = 0, \cdots, 14$dB. Note that the simulated BER performance of the MC-TDCS is the same as the analytical BER performance in (7–15).

It is interesting to observe the effects of the number of users and the number of transmitter antennae on the BER performance, when MRC is used. The BER performance of the proposed MC-TDCS is essentially limited by the MAI, ζ_s, in (7–10) due to

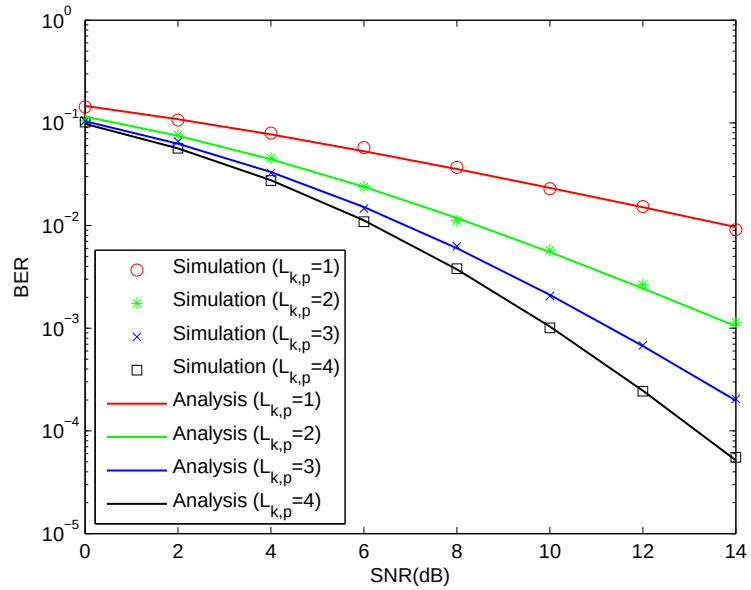


Figure 7-3. BER performance of the synchronous MC-TDCS downlink using MRC with single user and single transmit antenna over $L_{k,p}$-path Rayleigh fading

multipath fading. We study the performance of the DL (from BS to MT) MC-TDCS with pure spreading (PS) at BS, while the MTs use the MRC combiner.

The probability of bit error of the multiuser SC-TDCS in AWGN channel [28] is given by:

$$\begin{aligned} P_b(K, N_c) &= Q\left(\sqrt{\frac{2E_b}{N_0 + N_I}}\right) \\ &= Q\left(\sqrt{\frac{2}{\frac{N_0}{E_b} + \frac{K-1}{N_c}}}\right) \end{aligned} \tag{7–17}$$

where K denotes the number of users, while N_c denotes the code length of the FWM (or basis function) of the TDCS. Note that the MAI interference N_I increases as the number of users K increases (7–17). Now we need to consider the statistical properties of α_s and ζ_s in (7–12) and (7–13). Assuming statistically independent data symbols a_k^m with zero mean unit variance, from (7–10) we can see that the SINR at the k'th MT is given by:

$$\text{SINR}_{k'} = \frac{\mathbf{E}[\alpha_s^2]}{\mathbf{E}[\eta_s^2] + \mathbf{E}[\zeta_s^2]} \tag{7–18}$$

where $\mathbf{E}$ denotes the expected value. Since $\sum_{l=0}^{L_{k,p}-1} |h_{k,p}(l)|^2 = 1.0$ and $\sum_{n=1}^{N_c} |H_{k,p}(i_n^m)|^2 = N_c$ according to the discrete Parseval's theorem, we can assume that

$$\mathbf{E}\left[\sum_{n=1}^{L} |H_{k,p}(i_n^m)|^2\right] = L \tag{7–19}$$

Then the average signal power $E[{\alpha_s}^2]$ becomes

$$\begin{aligned}
\mathbf{E}[\alpha_s^2] &= \mathbf{E}\left[\left(a_{k'}^m \sum_{p=1}^{P} |\mathbf{H}_{k',p}|^2\right)^2\right] \\
&= \mathbf{E}\left[(a_k^m)^2\right] \mathbf{E}\left[\left(\sum_{p=1}^{P} |\mathbf{H}_{k',p}|^2\right)^2\right] \\
&= \mathbf{E}\left[(a_k^m)^2\right] \mathbf{E}\left[\left(\sum_{p=1}^{P}\sum_{n=1}^{L} |H_{k',p}(i_n^m)|^2\right)^2\right] \\
&= E_b\mathbf{E}\left[\left(\sum_{p=1}^{P}\sum_{n=1}^{L} |H_{k',p}(i_n^m)|^2\right)^2\right] \\
&= E_b(P\cdot L)\left(\mathbf{E}\left[|H_{k,p}(i_n^m)|^4\right] - \mathbf{E}\left[|H_{k,p}(i_n^m)|^2\right]^2\right) = E_b(P\cdot L)
\end{aligned} \tag{7–20}$$

where E_b is the signal energy per bit during the bit interval. If we assume that the absolute value of the sub-carrier channel transfer function, $H_{p,k}(i_n^m)$, obeys an independent identically distributed (iid) Rayleigh process with $\mathbf{E}\left[|H_{k,p}(i_n^m)|^2\right] = 2\sigma_{k,p}^2 = 1$ and $B_k^*(i_n^m)B_k(i_n^m)$ has an equal probability. Then,

$$\begin{aligned}
\mathbf{E}\left[\zeta_s^2\right] &= \mathbf{E}\left[\left(\sum_{k=1,k\neq k'}^{K} a_k^m \mathbf{B}_k^H \sum_{p=1}^{P} |\mathbf{H}_{k,p}|\mathbf{B}_k\right)^2\right) \\
&= \mathbf{E}[(a_k^m)^2](K-1)\mathbf{E}\left[\left(\sum_{P=1}^{P}\sum_{n=1}^{L} B_k^*(i_n^m)B_k(i_n^m)|H_{k',p}(i_n^m)|^2\right)^2\right] \\
&= E_b\frac{K-1}{L}\mathbf{E}\left[\left(\sum_{P=1}^{P}\sum_{n=1}^{L} |H_{k',p}(i_n^m)|^2\right)^2\right] \\
&= E_b\frac{K-1}{L}\cdot P\cdot L\cdot\left(\mathbf{E}\left[|H_{k,p}(i_n^m)|^4\right] - \mathbf{E}\left[|H_{k,p}(i_n^m)|^2\right]^2\right) \\
&= E_b(K-1)\cdot P
\end{aligned} \tag{7–21}$$

where $\mathbf{E}\left[|H_{k,p}(i_n^m)|^4\right] = 8\sigma_{k,p}^4 = 2$ is used and $\mathbf{E}[\eta_s^2] = L\sigma_n^2$.

Therefore, the SINR in (7–18) becomes:

$$\begin{aligned}\mathrm{SINR}_{k'} &= \frac{\mathbf{E}[\alpha^2]}{\mathbf{E}[\zeta^2] + \mathbf{E}[\eta^2]} \\ &= \frac{E_b P L}{E_b(K-1)P + L\sigma_n^2} \\ &= \frac{E_b P L}{E_b P(K-1) + L\sigma_n^2} \\ &= \frac{PL}{P(K-1) + L\frac{\sigma_n^2}{E_b}}\end{aligned} \tag{7–22}$$

This analysis in (7–22) is supported by the Figure 7-4. As the number of transmitter antennae increase, the BER performance is enhanced. Since $K = 1$, $\mathrm{SNR}_{k'} = PE_b/N_0$ according to (7–22). When $P = 2$, there is about 3dB enhancement in the BER. In so-called half ($K = L/2$) and fully ($K = L$) loaded conditions, the multiple access interference (MAI) dominates the system performance as opposed to the noise and the number of transmitter antennae. The corresponding simulation results are given in Figure 7-5 and 7-6 for $P = 2$ and $P = 4$, respectively.

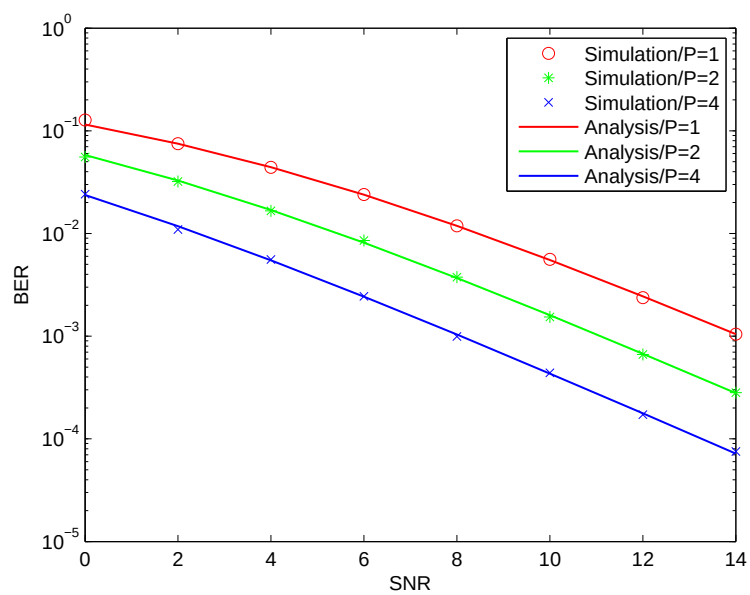


Figure 7-4. BER performance of the synchronous MC-TDCS downlink using MRC with single user ($K = 1$) and multiple antennae over $L_{k,p} = 2$-path Rayleigh fading

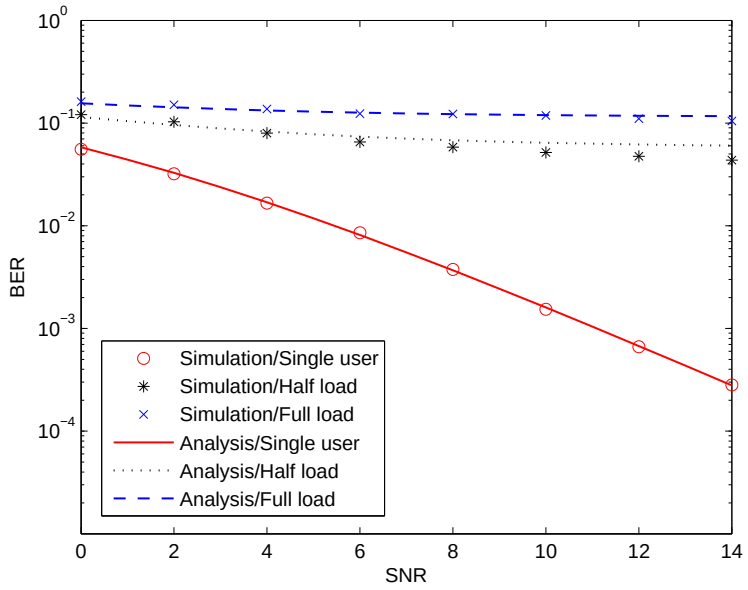


Figure 7-5. BER performance of the synchronous MC-TDCS downlink using MRC with two transmitter antennae ($P = 2$) over $L_{k,p} = 2$-path Rayleigh fading

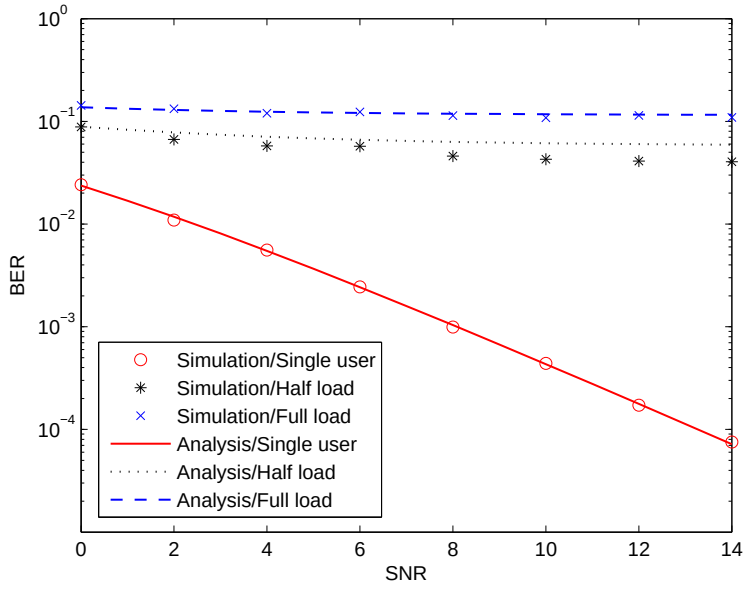


Figure 7-6. BER performance of the synchronous MC-TDCS downlink using MRC with four transmitter antennae ($P = 4$) over $L_{k,p} = 2$-path Rayleigh fading

7.3.2 Equal Gain Combining

The equal gain combining (EGC) attempts to correct the channel-induced phase rotations, leaving the faded magnitudes uncorrected. In this case, the equalization gain is given by:

$$g_k(n) = \frac{\left(\sum_{p=1}^{P} H_{k,p}(i_n^m)\right)^*}{|\sum_{p=1}^{P} H_{k,p}(i_n^m)|} \quad n = 1, \cdots, L \tag{7–23}$$

Then, the corresponding three components α_s, ζ_s, and η_s, are given as:

$$\alpha_s = a_{k'}^m \sum_{p=1}^{P} |\mathbf{H}_{k',p}| \tag{7–24}$$

$$\begin{aligned}
\zeta_s &= \sum_{k=1,k\neq k'}^{K} a_k^m \mathbf{B}_k^H \mathbf{G}_k \sum_{p=1}^{P} \mathbf{H}_{k,p}\mathbf{B}_k \\
&= \sum_{k=1,k\neq k'}^{K} a_k^m \mathbf{B}_k^H \frac{\left(\sum_{p=1}^{P} \mathbf{H}_{k,p}\right)^*}{|\sum_{p=1}^{P} \mathbf{H}_{k,p}|} \sum_{p=1}^{P} \mathbf{H}_{k,p}\mathbf{B}_k \\
&= \sum_{k=1,k\neq k'}^{K} a_k^m \mathbf{B}_k^H \left(\sum_{p=1}^{P} |\mathbf{H}_{k,p}|\right) \mathbf{B}_k
\end{aligned} \tag{7–25}$$

$$\eta_s = \mathbf{B}_{k'}^H \frac{\left(\sum_{p=1}^{P} \mathbf{H}_{k',p}\right)^*}{|\sum_{p=1}^{P} \mathbf{H}_{k',p}|} \mathbf{n}_{k'} \tag{7–26}$$

The simulation result is shown in Figure 7-7. Note that overall EGC BER performance of the MC-TDCS is worse than the MRC in Section 7.3.1.

7.3.3 Orthogonality Restoring Combining

If we cancel the effect of the channel transfer function by estimating it and reversing its effects, the orthogonality of the different users can be maintained. This is the aim of the orthogonality restoring combining (ORC) or zero forcing (ZF) equalization with the equalization gain, g_k

$$g_k(n) = \frac{\left(\sum_{p=1}^{P} H_{k,p}(i_n^m)\right)^*}{|\sum_{p=1}^{P} H_{k,p}(i_n^m)|^2} \tag{7–27}$$

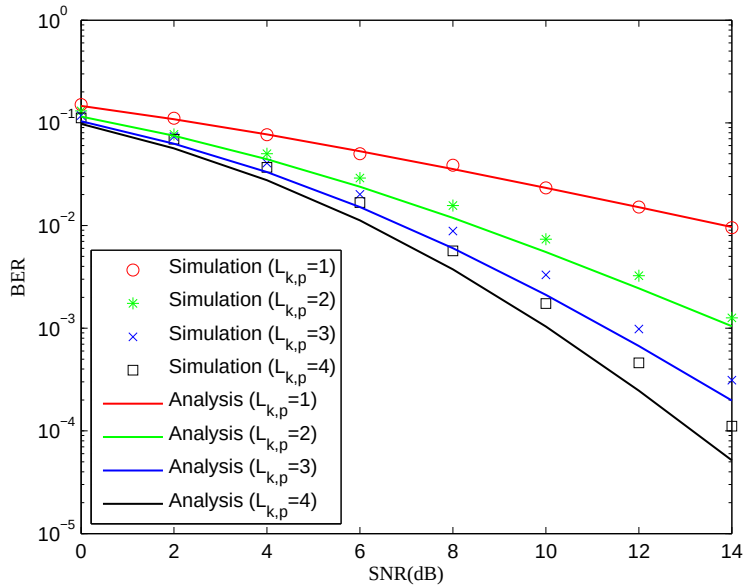


Figure 7-7. BER performance of the synchronous MC-TDCS downlink using MRC with single user (K=1) over $L_{k,p}$-path Rayleigh fading

The corresponding two components are:

$$\begin{aligned}\alpha_s &= a_{k'}^m \mathbf{B}_{k'}^H \mathbf{G}_{k'} \sum_{p=1}^{P} \mathbf{H}_{k',p} \mathbf{B}_{k'} \\ &= a_{k'}^m \mathbf{B}_{k'}^H \frac{\sum_{p=1}^{P} \mathbf{H}_{k',p}^*}{\left|\sum_{p=1}^{P} \mathbf{H}_{k',p}\right|^2} \cdot \sum_{p=1}^{P} \mathbf{H}_{k',p} \mathbf{B}_{k'} \\ &= a_{k'}^m \mathbf{B}_{k'}^H \mathbf{B}_{k'}\end{aligned} \tag{7–28}$$

On the other hand, the MUI associated with MRC is given by

$$\begin{aligned}\zeta_s &= \sum_{k=1,k\neq k'}^{K} a_k^m \mathbf{B}_k^H \mathbf{G}_k \sum_{p=1}^{P} \mathbf{H}_{k,p} \mathbf{B}_k \\ &= \sum_{k=1,k\neq k'}^{K} a_k^m \mathbf{B}_k^H \frac{\sum_{p=1}^{P} \mathbf{H}_{k,p}^*}{\left|\sum_{p=1}^{P} \mathbf{H}_{k,p}\right|^2} \cdot \sum_{p=1}^{P} \mathbf{H}_{k,p} \mathbf{B}_k \\ &= \sum_{k=1,k\neq k'}^{K} a_k^m \mathbf{B}_k^H \mathbf{B}_k\end{aligned} \tag{7–29}$$

Finally, the noise term, η_s, is obtained by

$$\eta_s = \mathbf{B}_{k'}^H \frac{\sum_{p=1}^{P} \mathbf{H}_{k',p}^*}{\left|\sum_{p=1}^{P} \mathbf{H}_{k',p}\right|^2} \mathbf{n}_{k'} \tag{7–30}$$

Simulation result is shown in Figure 7-8. Since the ORC scheme using perfect channel estimation had already removed the frequency selectivity of the channel transfer function, leaving no room for improvement with the aid of the frequency domain diversity. The source of the performance degradation is the noise enhancement, particularly at lower SNR values.

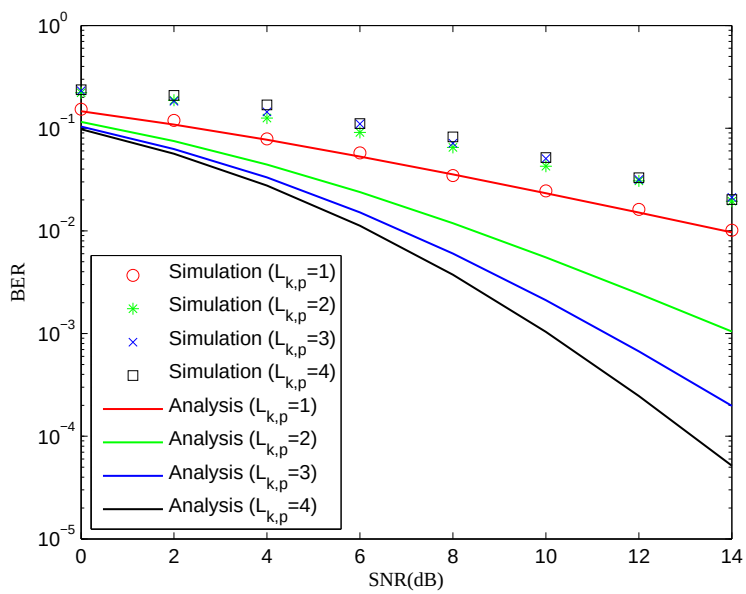


Figure 7-8. BER performance of the synchronous MC-TDCS downlink using ORC with single user over L-path Rayleigh fading where L is the diversity order

7.3.4 Minimum Mean Square Error Equalization

To mitigate the noise enhancement of ORC, particularly at lower SNR values, the minimum mean square error (MMSE) can be used with the equalization gain, g_k

$$g_k(n) = \frac{\left(\sum_{p=1}^{P} H_{k,p}(i_n^m)\right)^*}{\left|\sum_{p=1}^{P} H_{k,p}(i_n^m)\right|^2 + \sigma_n^2} \tag{7–31}$$

The corresponding three components

$$\alpha_s = a_{k'}^m \mathbf{B}_{k'}^H \frac{\left|\sum_{p=1}^{P} \mathbf{H}_{k',p}\right|^2}{\left|\sum_{p=1}^{P} \mathbf{H}_{k',p}\right|^2 + \sigma_n^2 \mathbf{I}_L} \mathbf{B}_{k'} \tag{7–32}$$

$$\zeta_s = \sum_{k=1,k\neq k'}^{K} a_k^m \mathbf{B}_k^H \frac{\left|\sum_{p=1}^{P} \mathbf{H}_{k,p}\right|^2}{\left|\sum_{p=1}^{P} \mathbf{H}_{k,p}\right|^2 + \sigma_n^2 \mathbf{I}_L} \mathbf{B}_k \tag{7–33}$$

$$\eta_s = \mathbf{B}_{k'}^H \frac{\sum_{p=1}^{P} \mathbf{H}_{k',p}^*}{\left|\sum_{p=1}^{P} \mathbf{H}_{k',p}\right|^2} \mathbf{n}_{k'} \tag{7–34}$$

Simulation result is shown in Figure 7-9. The overall BER performance of MMSE is almost better than that of EGC, but is worse than MRC.

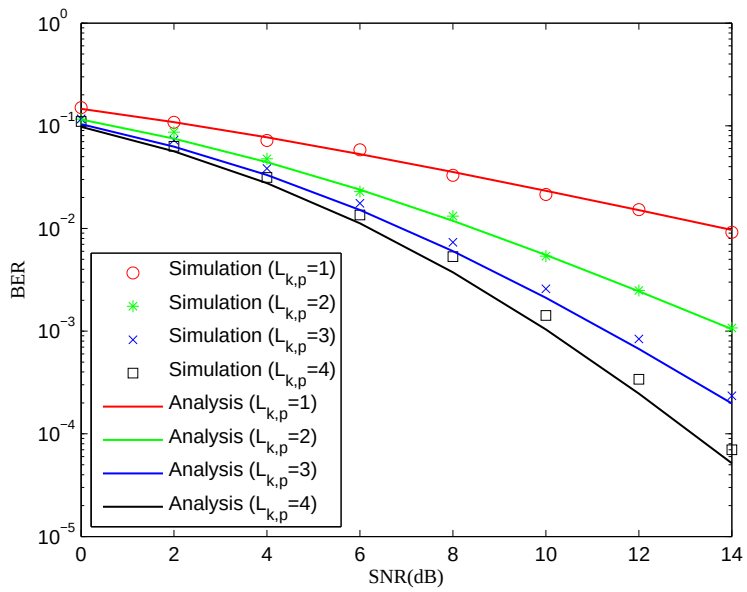


Figure 7-9. BER performance of the synchronous MC-TDCS downlink using MMSE with single user (K=1) over $L_{k,p}$-path Rayleigh fading where $L_{k,p}$ is the diversity order

7.4 Multiple Access Interference Mitigation

In this section, we will enhance the BER performance of the proposed MC-TDCS with a pre-filtering transmitter antenna arrays at the BS. As shown in Section 7.3, the performance of the proposed MC-TDCS is essentially limited by the MAI, caused by the loss of the orthogonality among users in multipath environments. In fact, while

in DL transmissions (i.e., from the BS to the MTs), the SUD techniques are typically employed, guaranteeing reasonable trade-off between performance and system complexity, in uplink (i.e., from the MTs to the BS), multiuser detection (MUD) techniques seems to be mandatory.

The idea behind pre-equalization (or pre-filtering) is to vary the gain assigned to each sub-carrier so that the the interference is reduced and a low complex detection scheme can be employed at the receiver. In order to work properly, the pre-equalization techniques require CSI at the transmitter. The use of the pre-filtering has several advantages: (i) reducing the MAI at MTs by the pre-filtering at the BS so that the received signal at the decision point is free from interference, (ii) moving most signal processing tasks from MTs to BS, and (iii) keeping the MTs at a very low complexity level. There are several pre-filtering methods proposed in the literature [22, 24–27] for MISO DL MC-CDMA. The pre-filtering methods are based on minimization of the transmitted power subject to MAI elimination. In the sequel, we will elaborate on the joint pre-filtering and spreading approach in [22] in the proposed MC-TDCS.

7.4.1 Filter Design

Recall that the 2nd term in (7–8) is the interference of the k'th MT on the kth MT. That is:

$$MAI(k' \rightarrow k) = \mathbf{q}_k^T \sum_{p=1}^{P} \mathbf{H}_{k,p} \mathbf{w}_{k',p} \tag{7–35}$$

The joint pre-filtering and spreading weight vector of the k'th MT is then obtained by constraint the desired signal part of its own decision variable to a given constant while canceling (or zero-forcing) the MAI contribution at all other MTs. This leads to the following set of conditions:

$$\begin{cases} \mathbf{q}_{k'}^T \sum_{p=1}^{P} \mathbf{H}_{k',p} \mathbf{w}_{k',p} = \alpha_{k'} \\ \mathbf{q}_k^T \sum_{p=1}^{P} \mathbf{H}_{k,p} \mathbf{w}_{k',p} = 0 \quad \forall k \neq k' \end{cases} \tag{7–36}$$

where $\alpha_{k'}$ is a positive real value that is chosen to meet some constraints. Note that the multiuser channel in (7–8) is decoupled into K single user parallel AWGN channel in (7–36) with transmission gains given by the specific value $\alpha_{k'}$. To compute the weight vector $\mathbf{w}_{k,p}$, we have to solve K linear equation given by:

$$\mathbf{Q}\mathbf{w}_k = \alpha_k \mathbf{b}_k \tag{7–37}$$

where $\mathbf{Q}$ is a complex channel and user code matrix of size $K \times PL$ and $\mathbf{b}_k$ is a vector of size K given by:

$$\mathbf{Q} = \begin{bmatrix} \mathbf{q}_1^T\mathbf{H}_{1,1} & \cdots & \mathbf{q}_1^T\mathbf{H}_{1,p} & \cdots & \mathbf{q}_1^T\mathbf{H}_{1,P} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{q}_k^T\mathbf{H}_{k,1} & \cdots & \mathbf{q}_k^T\mathbf{H}_{k,p} & \cdots & \mathbf{q}_k^T\mathbf{H}_{k,P} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{q}_K^T\mathbf{H}_{K,1} & \cdots & \mathbf{q}_K^T\mathbf{H}_{K,p} & \cdots & \mathbf{q}_K^T\mathbf{H}_{K,P} \end{bmatrix} \quad \mathbf{b}_k = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow k\text{th entry} \tag{7–38}$$

If we use the pure despreading (PD) at the MT in (7–38) instead of the joint pre-filtering and despreading, the complex channel and user code matrix becomes:

$$\mathbf{Q} = \begin{bmatrix} \mathbf{B}_1^T\mathbf{H}_{1,1} & \cdots & \mathbf{B}_1^T\mathbf{H}_{1,p} & \cdots & \mathbf{B}_1^T\mathbf{H}_{1,P} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{B}_k^T\mathbf{H}_{k,1} & \cdots & \mathbf{B}_k^T\mathbf{H}_{k,p} & \cdots & \mathbf{B}_k^T\mathbf{H}_{k,P} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{B}_K^T\mathbf{H}_{K,1} & \cdots & \mathbf{B}_K^T\mathbf{H}_{K,p} & \cdots & \mathbf{B}_K^T\mathbf{H}_{K,P} \end{bmatrix} \quad \mathbf{b}_k = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow k\text{th entry} \tag{7–39}$$

We want to minimize the transmitter power subject to K constraint. Thus the pre-filtering optimization problem can be written as:

$$\underbrace{\min}_{\mathbf{w}_k} \mathbf{w}_k^H \mathbf{w}_k \quad \text{subject to} \quad \mathbf{Q}\mathbf{w}_k = \alpha_k \mathbf{b}_k \tag{7–40}$$

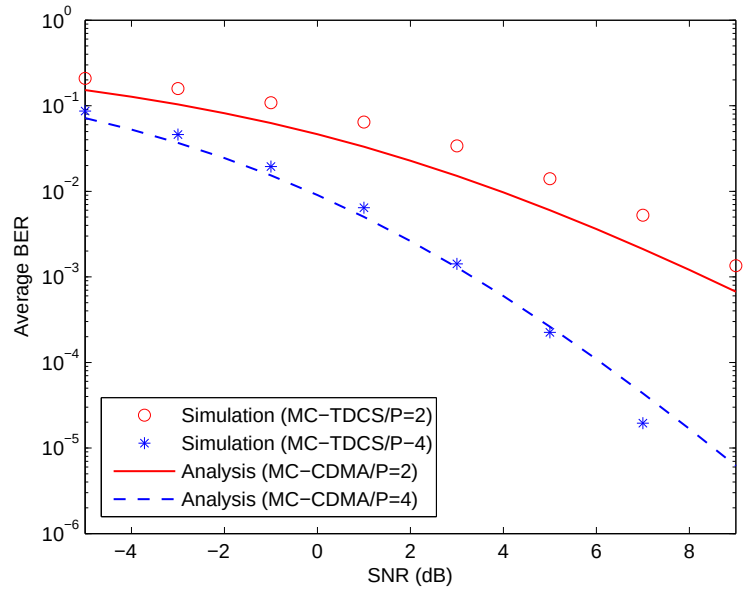


Figure 7-10. BER performance of a full-loaded MC-TDCS with TIR/PD scheme

This optimization can be solved by the Lagrange multipliers method. The minimum-norm solution becomes:

$$\mathbf{w}_k = \alpha_k \mathbf{Q}^H \left(\mathbf{Q}\mathbf{Q}^H\right)^{-1} \mathbf{b}_k = \alpha_k \bar{\mathbf{w}}_k \tag{7–41}$$

where $\left(\mathbf{Q}\mathbf{Q}^H\right)$ is a complex square and Hermitian matrix of size $K \times K$, and $\bar{\mathbf{w}}_k$ represents the weight vector without power scaling.

7.4.2 Power Allocation Schemes

See Section 6.4.2.

7.4.3 Performance Analysis

See Section 6.4.3.

7.4.4 Simulation and Comparison

To evaluate the performance of the pre-filtering schemes for DL MC-TDCS system, we study the average BER performance of a full-loaded MC-TDCS with TIR/MRC scheme. The main simulation parameters are the number of sub-carriers (N_c) set to 1,024; the number of users ($K \leq L$) is 256 for full-load; the frame contains M =4 OFDM symbols; modulation is BPSK. We consider perfect knowledge CSI at BS and the channel

is considered to be flat at least between two sub-carriers and is kept fixed over the OFDM symbol duration.

Analysis curves of MC-CDMA in Figure 7-10 are drawn by (6–34) with the diversity order, $D_{TIR/MRC} = D_{PS/MRC} + P - 1$, and average signal-to-noise ratio $\bar{\gamma}_{b,TIR/MRC} = P\bar{E}_b/N_0$. Comparing Figure 7-4, Figure 7-5, and Figure 7-10, we can see that the pre-filtering enhances the average BER performance as the number of transmitter antennae increased. Since the FMWs of MC-TDCS are not orthogonal each other, the performance of the MC-TDCS is poorer than that of MC-CDMA for $P = 2$. However, as the number of transmitter antennae increases, the performance of two systems is almost the same for $P = 4$. Therefore, the MC-TDCS can mitigate the MAI by the space-frequency precoding scheme.

7.5 Performance under Jamming

In this section, we will study the BER performance of the proposed MC-TDCS under various intentional interferences. We will use the MRC equalization gain in (7–11) and the single user performance in (7–15) in the sequel.

7.5.1 Performance under Barrage Noise Jamming

Barrage noise jamming (BNJ) belongs to a broadband noise jamming form. In this case, the jammer interferes with the whole bandwidth by injecting a band-limited noise to the system. Its effect is the same as that of the additive white Gaussian noise (AWGN), so the power spectral density (PSD) of total noise becomes:

$$\mathrm{PSD}_N = N_0 + N_J \tag{7–42}$$

where N_0 is the noise PSD of complex AWGN and N_J is the PSD of complex BNJ. Therefore, $\bar{\gamma}_b$ in (7–16) becomes the average energy per bit, $\bar{E}_b$, divided by the total noise power spectral density, $N_0 + N_J$. Simulation results are shown in Figure 7-11 and Figure 7-12 for MRC and EGC with SNR=10dB, respectively. Note that the simulated BER performance of the MC-TDCS is the same as the analytical BER performance in (7–15)

with (7–42), while the overall EGC BER performance of the MC-TDCS is worse than MRC under BNJ.

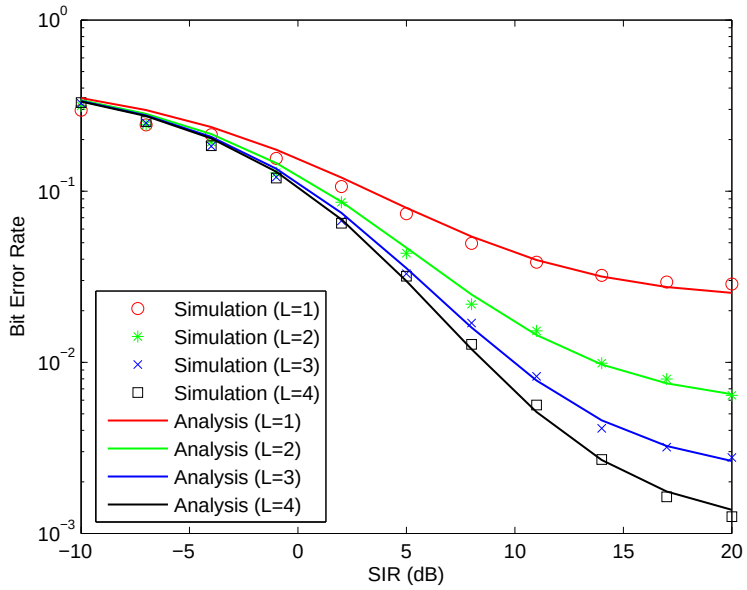


Figure 7-11. BER performance of the synchronous MC-TDCS downlink using MRC under BNJ over L-path Rayleigh fading where L is the diversity order

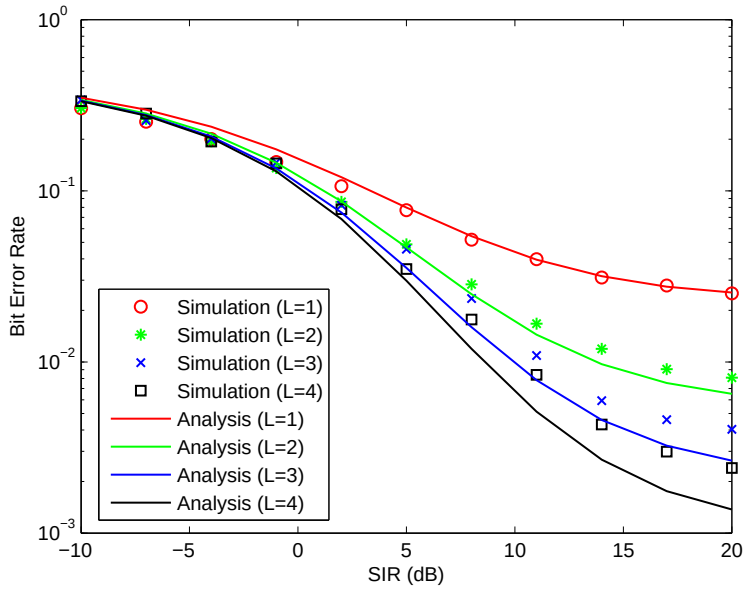
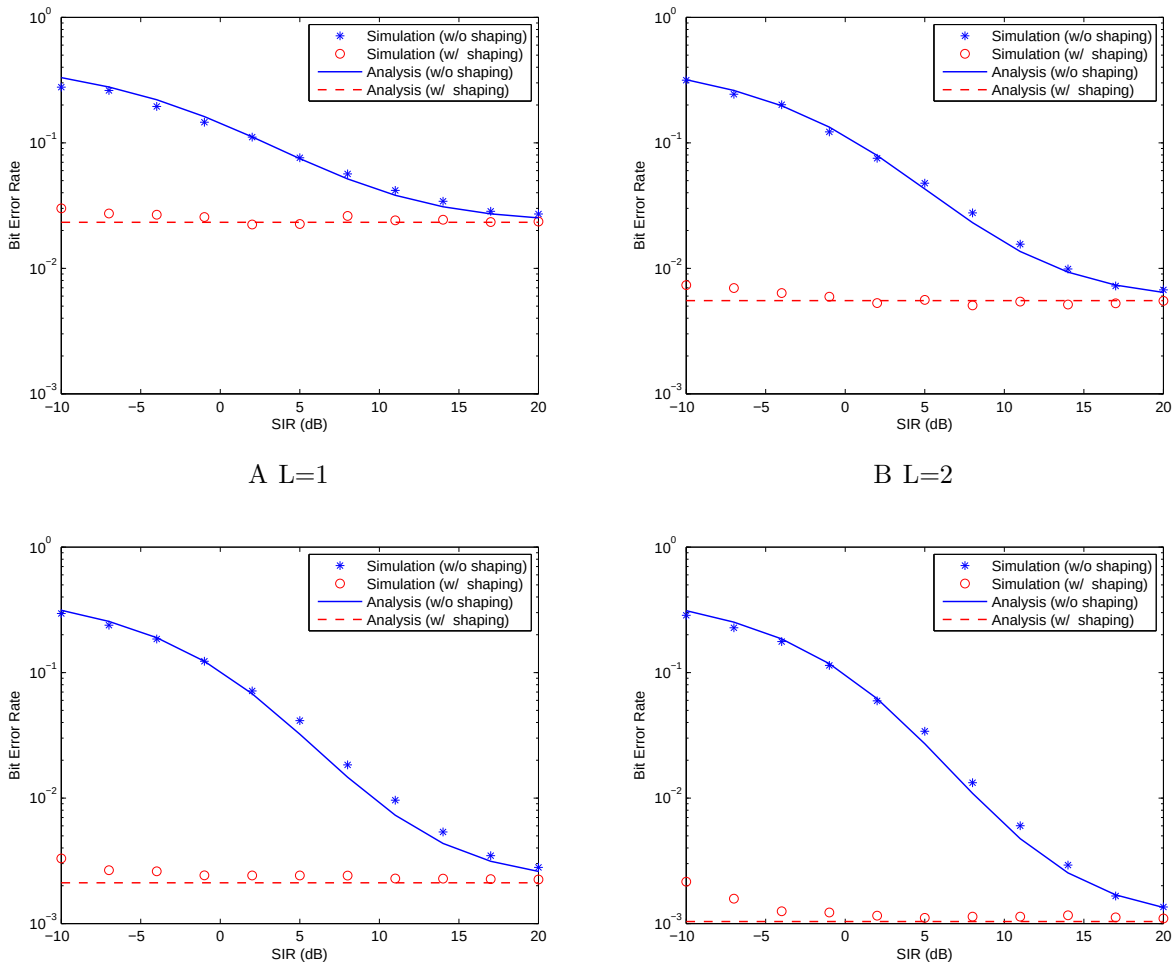


Figure 7-12. BER performance of the synchronous MC-TDCS downlink using EGC under BNJ over L-path Rayleigh fading where L is the diversity order

7.5.2 Performance under Partial Band Jamming

Partial band jamming (PBJ) occupies a continuous range of system bandwidth. As mentioned, the PBJ is stationary jamming. Simulation result for 10% PBJ is shown in Figure 7-13 for MRC. MC-TDCS avoids the interfered regions by the spectral shaping. Therefore, its performance with the spectral shaping is almost the same as that of the no-jamming case in Figure 7-3.



A L=1 B L=2

C L=3 D L=4

Figure 7-13. BER performance of the synchronous MC-TDCS downlink using MRC under 10 % PBJ over L-path Rayleigh fading where L is the diversity order

7.5.3 Performance under Multi-Tone Jamming

Multi-tone jamming (MTJ) divides its total power into q distinct, equal power, and random phase tones. Every jamming tone can be modeled as:

$$j(t) = A_J e^{j(2\pi f_J \cdot t + \phi_J)} \tag{7–43}$$

where ϕ_J is a random phase, which is uniformly distributed over $[0, 2\pi]$. A_J and f_J are amplitude and frequency, respectively. Note that single-tone jamming (STJ) is a special case of multi-tone jamming with $q = 1$. The MTJ is a wide-sense stationary jamming, since the mean $\mathbf{E}[j(t)] = 0$ and the autocorrelation $\mathbf{E}[j^*(t)j(t+\tau)] = R(\tau)$ where $\mathbf{E}[\cdot]$ denotes the expectation.

Simulation result for STJ and MTJ is shown in Figure 7-14 and Figure 7-15 with MRC, respectively. The proposed MC-TDCS mitigates STJ and MTJ with spectral shaping in frequency domain.

7.6 Summary

Secure transmission over a hostile wireless channel is desired by both civilian and military parties. In this chapter, we propose the MISO MC-TDCS in which the concept of TDP processing and multi-carrier modulation are combined together to avoid intentional interference and to combat multipath fading. We elaborate on both the system architecture and the mathematical model of the DL MC-TDCS. The proposed MC-TDCS also mitigates the MAI by the multiple antenna arrays (joint) precoding and mitigates jamming by TDP in frequency-domain. We also analyze the performance of the MC-TDCS under interference and verify the performance by simulations. The MC-TDCS is a generalized MC-CDMA while it has the interference avoidance capability in addition to properties of the MC-CDMA and exploits the frequency diversity and transmitter diversity.

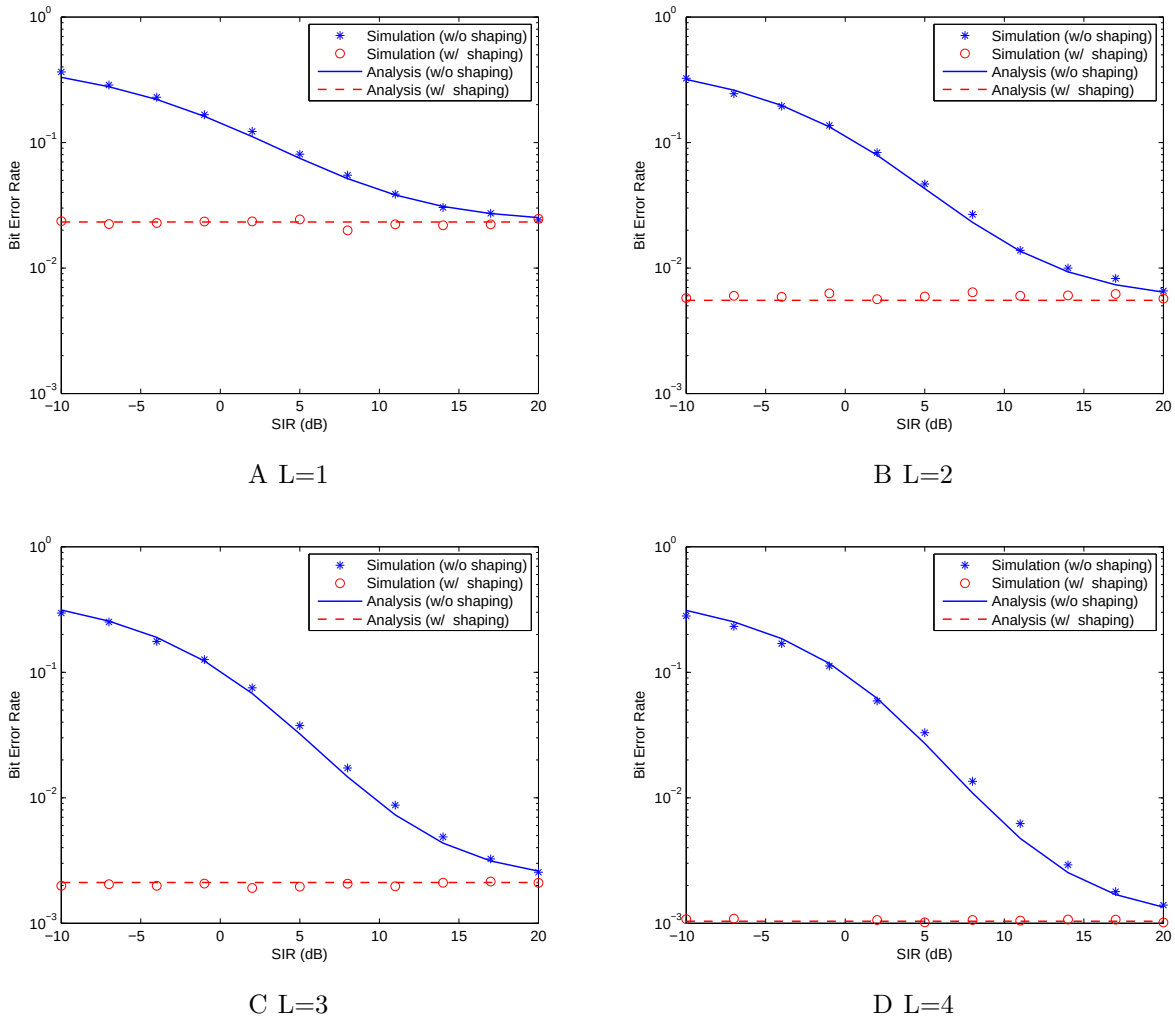


Figure 7-14. BER performance of the synchronous MC-TDCS downlink using MRC under STJ over L-path Rayleigh fading where L is the diversity order

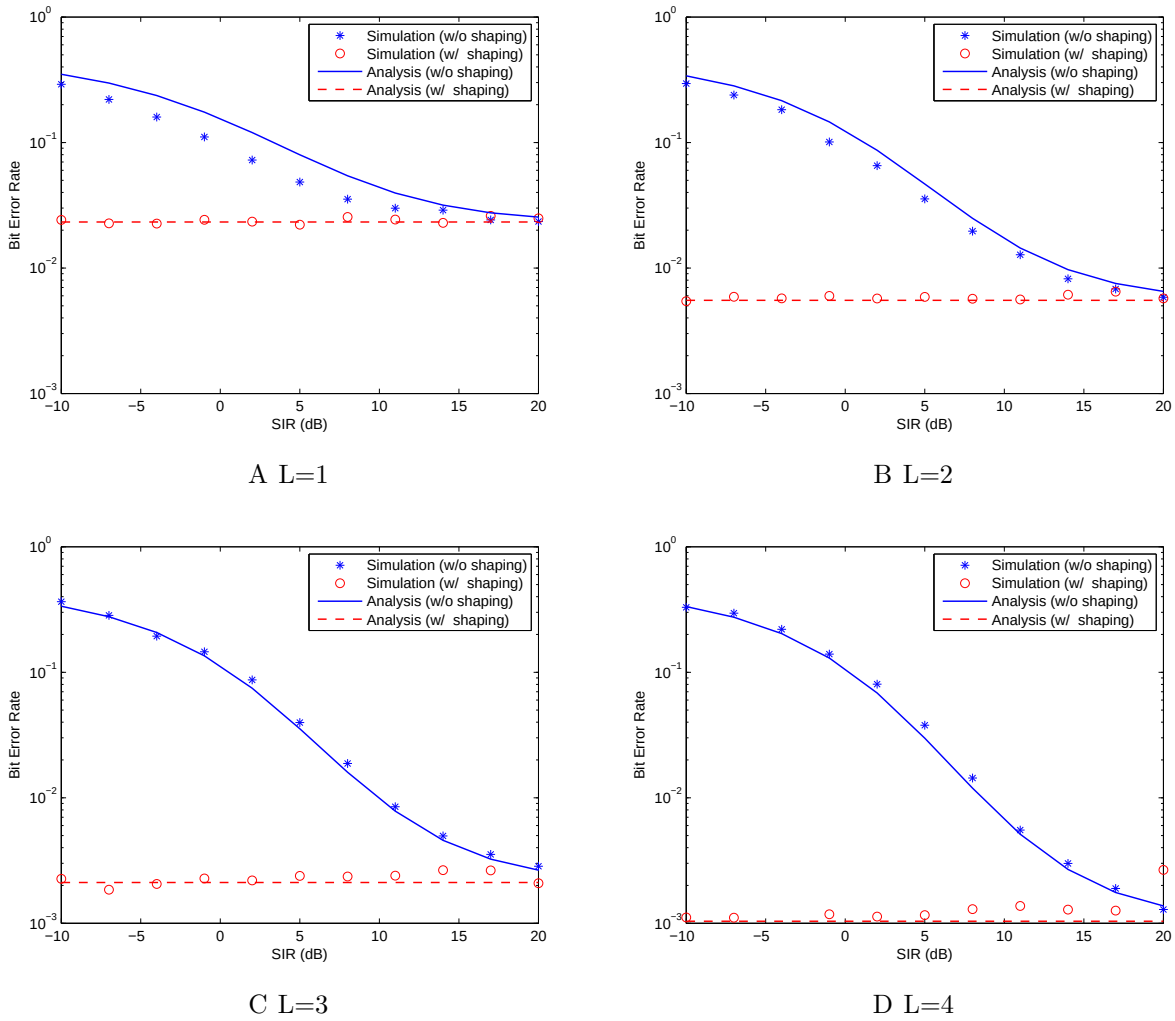


Figure 7-15. BER performance of the synchronous MC-TDCS downlink using MRC under MTJ over L-path Rayleigh fading where L is the diversity order

CHAPTER 8
CONCLUSION

8.1 Summary of the Dissertation

In this section, we summarize the research presented in this dissertation. We considered physical layer techniques in wireless communication security. We addressed how to crack the adversary's secure communication which uses direct-sequence spread-spectrum (DS-SS) and how to protect wireless communication systems against jamming and unintentional interference.

In Chapter 1, we introduced and motivated the problem. In Chapter 2, we leveraged on investigating the performance of various wireless communication systems at physical layer under interference, since interference can disrupt communications by decreasing the signal-to-noise (SNR) ratio. By doing so, we can predict the performance of wireless communication systems under interference as well as motivate us to mitigate interference for a reliable communication.

In Chapter 3, we considered how to crack an adversary's communication, which uses DS-SS. To eavesdrop on a secure adversary's communication, one needs to (a) identify the start position of a data symbol in the spread signal for symbol synchronization purpose, (b) remove the pseudo-random (PN) sequence, (c) estimate the PN sequence, and (d) estimate the generator polynomial. We addressed these four problems with effective methods in Chapter 3. To identify the start position of a data symbol, we developed a method that uses the spectral norm of the sample covariance matrix. After symbol synchronization, a method based on the cross-correlation was used to estimate data symbols up to an unknown multiplicative factor. In addition to obtaining the PN sequence and the data symbols, we also proposed a zigzag estimator to identify the code generator polynomial and proposed a method to identify the polarity in the intercepted signal. We also analyzed the probability of error of the zigzag estimator. Our validation by simulation and theoretical analysis show the effectiveness of our proposed method.

In Chapter 4, we proposed an enhanced transform domain communication system (ETDCS) which can secure a single-carrier single-input single-output (SC-SISO) system against stationary and non-stationary interference. The proposed ETDCS with Capon's Method (CM) can properly estimated intentional interference considered in Section 2.2.1. Analytical bit error rate (BER) study and simulation results verified that the ETDCS offers a significant interference avoidance capability for both the stationary and non-stationary interference.

In chapter 5, we considered the problem of mitigating the narrow band interference (NBI) for vertical-Bell Laboratories layered space-time (V-BLAST) system. The proposed V-BLAST system combined advantages of the transform domain processing (TDP) based on CM method in Chapter 4 and V-BLAST detection based on minimum mean square error (MMSE) under intentional interference. These combinations mitigated both stationary and non-stationary interference effectively. The performance of the proposed V-BLAST was verified by simulation results.

In Chapter 6, we studied an analytical BER performance of a downlink (DL) time division duplex (TDD) multi-carrier code division multiple access (MC-CDMA) with a precoding transmitter antenna array at the base station (BS). We analyzed the average BER performance of various linear space-frequency precoding approaches with linear power allocation strategies at the BS. The performance of precoding schemes is a function of eigenvalues of a channel scatter matrix based on the channel state information and spreading sequences of all active users. It was very clear that the precoding schemes allow a significant performance improvement over one transmit antenna at the BS exploiting space-frequency diversity. By conducting these studies, we can predict and compare the performance of various precoding techniques.

In Chapter 7, we proposed a multi-carrier TDCS (MC-TDCS) which can protect a MC multi-input single-output (MC-MISO) communication system against jamming and multiple access interference (MAI). The proposed MISO MC-TDCS combined the TDP

and multi-carrier modulation (MCM) in order to combat interference as well as multipath fading. We leveraged on both the system architecture and the mathematical model of the DL MC-TDCS. The MAI, which predetermines the performance of multiuser system, was mitigated by a pre-filtering transmitter antenna array at base-station in a downlink multiuser system.

In summary, this research studied physical layer measures in wireless communication security. Although there are still many issues to be resolved, we believe that our approaches in both protecting wireless communication systems under interference and cracking the foe's secure DS-SS communication system will provide physical layer means for security of wireless communication systems.

8.2 Future Work

The purpose of this dissertation is to study physical layer techniques in wireless communication security. In this section, we point out future research directions for two research areas.

8.2.1 Cracking Secure Wireless Communication Systems

In this dissertation, we eavesdropped on a secure DS-SS systems and presented an analytical probability of error of an eavesdropper without a priori knowledge about a spread sequence in Chapter 3. We will extend our research to study another type of spread-spectrum, namely, frequency-hopping spread-spectrum (FH-SS).

The FH-SS is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a PN sequence known to both transmitter and receiver. We will design and implement an eavesdropper which can intercept a secure FH-SS signal. We will also leverage on reverse engineering a PN sequence of the intercepted signals without a priori knowledge about transmitter and receiver.

8.2.2 Protecting Wireless Communication Systems Against Interference

In this dissertation, we studied the performance of wireless communication systems under interference in Chapter 2, and we leveraged on countermeasures for SC-SISO,

V-BLAST, and MISO multi-carrier system in Chapter 4, Chapter 5, Chapter 6, and Chapter 7, respectively.

We will use antenna array processing to mitigate interference, since it can provide interference avoidance capability due to its capability of nullifying interference signals coming from a certain direction. In this research, we will use detection and estimation theory to detect jamming/interference and estimate the angle of arrival of the interfering signal; we will design and implement antenna array processing techniques to counter the detected interference; we will evaluate the performance of the proposed countermeasure under different types of jamming and interference signals; we will also analyze the cost of the proposed countermeasure.

REFERENCES

[1] D. Giri and F. Tesche, "Classification of intentional electromagnetic environments (IEME)," *IEEE transactions on electromagnetic compatibility*, vol. 46, no. 3, pp. 322–328, 2004.

[2] R. Scholtz, "The origins of spread-spectrum communications," *IEEE Transactions on Communications*, vol. 30, pp. 822–854, 1982.

[3] S. Golomb, *Shift register sequences.* Aegean Park Press Laguna Hills, CA, USA, 1981.

[4] S. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar.* Cambridge University Press New York, NY, USA, 2004.

[5] M. Ristenbatt, "Performance criteria for spread spectrum communications," *IEEE Transactions on Communications*, vol. 25, 1977.

[6] A. Paulraj, R. Nabar, and D. Gore, *Introduction to space-time wireless communications.* Cambridge Univ Pr, 2003.

[7] G. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs Technical Journal*, vol. 1, no. 2, 1996.

[8] K. Lee and D. Williams, "A Space-Time Coded Transmitter Diversity Technique for Frequency Selective Fading Channels," in *Proceedings of the 2000 IEEE Sensor Array and Multichannel Signal Processing Workshop: SAM 2000: 16-17 March 2000, Cambridge, Massachusetts, USA.* IEEE, 2001, p. 149.

[9] M. Roberts, M. Temple, R. Raines, E. Magee, A. Center, and A. Kelly, "Initial acquisition performance of a transform domain communicationsystem: modeling and simulation results," in *MILCOM 2000. 21st Century Military Communications Conference Proceedings*, vol. 2, 2000.

[10] R. W. Klein, "Wavelet Domain Communication System (WDCS): Design, Model, Simulation and Analysis," MS Thesis, AFIT/GE/ENG/01M-06, AFIT, Wright-Peterson AFB OH, March 2000.

[11] V. Chakravarthy, A. Nunez, J. Stephens, A. Shaw, and M. Temple, "TDCS, OFDM, and MC-CDMA: a brief tutorial," *IEEE Communications Magazine*, vol. 43, no. 9, pp. S11–S16, 2005.

[12] K. Tan, Andrian, Z. Hao, and C. Zhou, "An Improved V-BLAST with Narrowband Interference Avoidance Capability," *The 9th Annual Symposium on Wireless Personal Multimedia Communication (WMPC 06)*, San Diego, CA, 2006.

[13] L. Buttyán and J. Hubaux, *Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing.* Cambridge Univ Pr, 2007.

[14] R. Poisel, *Modern communications jamming principles and techniques.* Artech House on Demand, 2003.

[15] D. Sarwate and M. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proceedings of the IEEE*, vol. 68, no. 5, pp. 593–619, 1980.

[16] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread spectrum communications handbook (revised ed.).* McGraw-Hill, Inc. New York, NY, USA, 1994.

[17] A. Goldsmith, *Wireless communications.* Cambridge Univ Pr, 2005.

[18] R. L. Peterson, D. E. Borth, and R. E. Ziemer, *An Introduction to Spread-Spectrum Communications.* Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1995.

[19] K. Tan, J. Andrian, F. Candocia, and C. Zhou, "An Enhanced Wavelet Domain Communication System (EWDCS) with Nonstationary Interference Avoidance Capability," in *2006 IEEE 64th Vehicular Technology Conference, 2006. VTC-2006 Fall*, 2006, pp. 1–6.

[20] P. Wolniansky, G. Foschini, G. Golden, and R. Valenzuela, "V-BLAST: an architecture for realizing very high data rates overthe rich-scattering wireless channel," in *Signals, Systems, and Electronics, 1998. ISSSE 98. 1998 URSI International Symposium on*, 1998, pp. 295–300.

[21] S. Hara and R. Prasad, "Overview of multicarrier CDMA," *IEEE communications magazine*, vol. 35, no. 12, pp. 126–133, 1997.

[22] A. Silva and A. Gameiro, "Transmission Strategies for MISO Downlink MC-CDMA Mobile Systems," *Wireless Personal Communications*, On-line.

[23] L. Hanzo, M. Münster, B. Choi, and T. Keller, *OFDM and MC-CDMA for broadband multi-user communications, WLANs, and broadcasting.* IEEE, 2003.

[24] T. Salzer, D. Mottier, D. Castelain, M. ITE, and F. Rennes, "Comparison of antenna array techniques for the downlink of multi-carrier CDMA systems," in *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*, vol. 1, 2003.

[25] A. Silva and A. Gameiro, "Pre-filtering antenna array for downlink TDD MC-CDMA systems," in *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*, vol. 1, 2003.

[26] M. Morelli and L. Sanguinetti, "A novel prefiltering technique for downlink transmissions in TDD MC-CDMA systems," *IEEE Transactions on Wireless Communications*, vol. 4, no. 5, pp. 2064–2069, 2005.

[27] A. Silva and A. Gameiro, "Performance and Analysis of Pre-Filtering Techniques for MISO Downlink TDD MC-CDMA Systems," in *IEEE 63rd Vehicular Technology Conference, 2006. VTC 2006-Spring*, vol. 1, 2006.

[28] P. Swackhammer, M. Temple, and R. Raines, "Performance simulation of a transform domain communication systemfor multiple access applications," in *IEEE Military Communications Conference Proceedings, 1999. MILCOM 1999*, vol. 2, 1999.

[29] C. Han, J. Wang, Y. Yang, and S. Li, "Addressing the control channel design problem: OFDM-based transform domain communication system in cognitive radio," *Computer Networks*, vol. 52, no. 4, pp. 795–815, 2008.

[30] J. Mitola III and G. Maguire Jr, "Cognitive radio: making software radios more personal," *IEEE personal communications*, vol. 6, no. 4, pp. 13–18, 1999.

[31] R. Brodersen, A. Wolisz, D. Cabric, S. Mishra, and D. Willkomm, "Corvus: A cognitive radio approach for usage of virtual unlicensed spectrum," *Berkeley Wireless Research Center (BWRC) White paper*, 2004.

[32] I. Budiarjo, H. Nikookar, and L. Ligthart, "Cognitive radio with single carrier TDCS and multicarrier OFDM approach with V-BLAST receiver in Rayleigh fading channel," *Mobile Networks and Applications*, vol. 13, no. 5, pp. 416–423, 2008.

[33] Y. Jo and D. Wu, "An Enhanced Transform Domain Communication System (ETDCS) with Narrow-Band Interference (NBI) Avoidance Capability," Department of Electrical and Computer Engineering, University of Florida, Tech. Rep., 2008.

[34] ——, "An enhanced transform domain communication system (ETDCS) with narrow-band interference (NBI) avoidance capability," in *Proceedings of SPIE*, vol. 7305, 2009, pp. 73 051C–73 051C–9.

[35] ——, "An enhanced V-BLAST with non-stationary interference avoidance capability," in *IEEE Military Communications Conference, 2008. MILCOM 2008*, 2008, pp. 1–7.

[36] L. Sanguinetti, M. Morelli, and I. Cosovic, "MMSE pre-filtering techniques for TDD MC-CDMA downlink transmissions," in *2005 IEEE 61st Vehicular Technology Conference, 2005. VTC 2005-Spring*, vol. 3.

[37] T. Sälzer and D. Mottier, "Downlink strategies using antenna arrays for interference mitigation in multi-carrier CDMA," in *Multi-carrier spread-spectrum: for future generation wireless systems, fourth international workshop, Germany, September 17-19, 2003*. Kluwer Academic Pub, 2003, p. 315.

[38] Y. Jo and D. Wu, "Blind synchronization, estimation of data symbol, spread sequence, and generator polynomial in direct sequence spread spectrum systems," in *IEEE Military Communications Conference, 2008. MILCOM 2008*, 2008, pp. 1–7.

[39] ——, "On Cracking Direct-Sequence Spread-Spectrum Systems," *Wireless Communication and Mobile Computing (Accepted)*, 2009.

[40] T. Rappaport, *Wireless communications.* Prentice Hall PTR New Jersey, 2002.

[41] M. Tsatsanis and G. Giannakis, "Blind estimation of direct sequence spread spectrum signals in multipath," *IEEE Transactions on Signal Processing*, vol. 45, no. 5, pp. 1241–1252, 1997.

[42] Y. Zhan, Z. Cao, and J. Lu, "Spread-spectrum sequence estimation for DSSS signal in non-cooperative communication systems," *IEE Proceedings-Communications*, vol. 152, no. 4, pp. 476–480, 2005.

[43] B. Vojcic and W. Jang, "Transmitter precoding in synchronous multiuser communications," *IEEE Transactions on Communications*, vol. 46, no. 10, pp. 1346–1355, 1998.

[44] W. Jang, L. Nguyen, and M. Hempel, "Precoded random spreading multiple access system in AWGN channels," *IEEE Transactions on Wireless Communications*, vol. 3, no. 5, pp. 1477–1480, 2004.

[45] J. Luo, J. Andrian, and C. Zhou, "Bit error rate analysis of jamming for ofdm systems," *Wireless Telecommunications Symposium 2007 (WTS 2007)*, pp. 1–8, April 2007.

[46] P. Bisaglia, L. Sanguinetti, M. Morelli, N. Benvenuto, and S. Pupolin, "Pre-equalization techniques for downlink and uplink TDD MC-CDMA systems," *Wireless Personal Communications*, vol. 35, no. 1, pp. 3–18, 2005.

[47] S. Nobilet and J. Helard, "A pre-equalization technique for uplink MC-CDMA systems using TDD and FDD modes," in *2002 IEEE 56th Vehicular Technology Conference, 2002. Proceedings. VTC 2002-Fall*, vol. 1, 2002.

[48] S. Yi, C. Tsimenidis, and B. Sharif, "Transmitter precoding in downlink MC-CDMA systems over frequency-selective Rayleigh fading channels," *IEE Proceedings-Communications*, vol. 152, no. 6, pp. 952–958, 2005.

[49] S. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on selected areas in communications*, vol. 16, no. 8, pp. 1451–1458, 1998.

[50] R. Cupo, G. Golden, C. Martin, K. Sherman, N. Sollenberger, J. Winters, and P. Wolniansky, "A four-element adaptive antenna array for IS-136 PCS base stations," in *1997 IEEE 47th Vehicular Technology Conference*, vol. 3, 1997.

[51] R. Ware and F. Lad, "Approximating the distribution for sums of products of normal variables," *University of Canterbury, England, Tech. Rep. UCDMS*, vol. 15, p. 2003, 2003.

[52] G. Burel, "Detection of Spread Spectrum Transmissions using fluctuations of correlation estimators, IEEE Int," in *Symp. on Intelligent Signal Processing and Communication Systems (ISPACS2000), Hawai*, 2000.

[53] C. Bouder, S. Azou, and G. Burel, "A robust synchronization procedure for blind estimation of the symbol period and the timing offset in spread spectrum transmissions," in *2002 IEEE Seventh International Symposium on Spread Spectrum Techniques and Applications*, vol. 1, 2002.

[54] L. Jiang, H. Ji, and L. Li, "A Blind Estimation Algorithm for PN Sequence in DS-SS Signals," in *8th International Conference on Signal Processing*, vol. 3, 16-20 2006, pp. –.

[55] G. Burel and C. Bouder, "Blind estimation of the pseudo-random sequence of a direct sequence spread spectrum signal," in *MILCOM 2000. 21st Century Military Communications Conference Proceedings*, vol. 2, 2000.

[56] G. Stewart, "Perturbation theory for the singular value decomposition," *Computer Science Technical Report Series; Vol. CS-TR-2539*, p. 13, 1990.

[57] P. Peebles, *Probability, random variables, and random signal principles.* McGraw-Hill College, 1993.

[58] S. Verdu, *Multiuser detection.* Cambridge Univ Pr, 1998.

[59] J. Capon, "High-resolution frequency-wavenumber spectrum analysis," *Proceedings of the IEEE*, vol. 57, no. 8, pp. 1408–1418, 1969.

[60] H. Simon, *Adaptive filter theory (4th Edition).* Prentice Hall, New Jersey, 2001.

[61] P. Stoica and R. Moses, *Spectral analysis of signals.* Pearson Prentice Hall, 2005.

[62] J. Benesty, J. Chen, and Y. Huang, "A generalized MVDR spectrum," *IEEE Signal Processing Letters*, vol. 12, no. 12, pp. 827–830, 2005.

[63] ——, "Estimation of the coherence function with the MVDR approach," in *2006 IEEE International Conference on Acoustics, Speech and Signal Processing, 2006. ICASSP 2006 Proceedings*, vol. 3, 2006.

[64] G. Dillard, M. Reuter, J. Zeiddler, B. Zeidler, S. Center, and C. San Diego, "Cyclic code shift keying: a low probability of intercept communication technique," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 39, no. 3, pp. 786–798, 2003.

[65] M. Brandt-Pearce, "Transmitter-based multiuser interference rejection for the down-link of a wireless CDMA system in a multipath environment," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 407–417, 2000.

[66] M. Rahman and H. Imai, "Security in wireless communication," *Wireless personal communications*, vol. 22, no. 2, pp. 213–228, 2002.

BIOGRAPHICAL SKETCH

Youngho Jo received a Bachelor of Science in physics from the Korea Military Academy, Seoul, Korea, in 1996, and a Master of Science in electrical and computer engineering from the University of Florida, Gainesville, Florida, in 2000. From 2000 to 2004, he was a faculty member of the Department of Electronics Engineering, Korea Military Academy. Since August 2006, he has been a doctoral student of the Department of Electrical and Computer Engineering at the University of Florida. His research interests are in the areas of wireless communication security, spread-spectrum communication, multi-carrier modulation, multi-input multi-output, and signal processing.