This is to certify that the
dissertation entitled

SECURE COMMUNICATION SYSTEM DESIGN
FOR WIRELESS NETWORKS

presented by

QI LING

has been accepted towards fulfillment
of the requirements for the

Doctoral degree in Electrical and Computer Engineering

Tongtong Li
Major Professor's Signature

12/07/2007
Date

SECURE COMMUNICATION SYSTEM DESIGN FOR WIRELESS NETWORKS

By

Qi Ling

A DISSERTATION

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

DOCTOR OF PHILOSOPHY

Department of Electrical and Computer Engineering

2007

ABSTRACT

SECURE COMMUNICATION SYSTEM DESIGN FOR WIRELESS NETWORKS

By

Qi Ling

Due to lack of a protective physical boundary, wireless communication is fragile to hostile jamming, detection and interception. Security becomes the key enabler for wireless networks now and in the future. Motivated by the observation that patching or add-on security is inadequate for addressing the needs on wireless security and can greatly complicate communication systems, in this dissertation, we focus on the fundamental study of developing spectrally efficient wireless system with built-in security.

First, we investigate the modeling and detection of hostile jamming in wireless communications. Hostile jamming, in which the jammer deliberately saturates the receiver with noise or false information, is one of the most commonly used techniques for limiting the effectiveness of an opponent's communications. Unlike existing jamming models that assume the jamming remains invariant during the signal transmission period, we propose a two-dimensional jamming generation model to characterize time-varying jamming phenomenons, and establish a novel jamming classification framework. Including all the existing jamming models as special cases, the new framework provides a broader horizon for systematic jamming modeling, jamming pattern recognition and adaptive transmitter design for optimum jamming resistance. New jamming detection methods are developed for both frequency hopping and DS-CDMA systems. Equalization and/or interference cancellation techniques are exploited to mitigate self-jamming and thus improve the accuracy of hostile jamming detection.

Next, we break new ground on spectrally-efficient anti-jamming system design. Mainly limited by multiuser interference, today's jamming resistant systems suffer from low spectral efficiency. In this research, first, we propose an innovative message-driven frequency hopping (MDFH) scheme, in which a large portion of information is embedded into the hopping frequency selection process and transmitted with no extra cost on bandwidth or power, leading to the significantly improved spectral efficiency. MDFH also reinforces information confidentiality since the hopping pattern is totally unpredictable. Secondly, we introduce the concept of collision-free frequency hopping (CFFH) from a cross-layer perspective. The CFFH scheme is developed based on the OFDM framework and the AES-controlled secure subcarrier assignment algorithm. While maintaining the inherent anti-jamming security feature, the proposed CFFH system can achieve high information capacity through collision-free multiple access.

Finally, we consider physical (PHY) layer built-in security enhancement for wireless systems. Generally, the PHY layer alone does not possess built-in security features except for spread spectrum systems. The inherent security provided by the existing spread spectrum systems is far from adequate and acceptable in wireless data communications. In this research, we propose to strengthen the PHY layer built-in information privacy by integrating cryptography techniques into the wireless transceiver design, and formulate a joint PHY layer and upper layer privacy protection mechanism. The proposed approaches are based on both cryptographic techniques and inherent ambiguity in signal detection over multiple access wireless channels. It turns out that PHY layer built-in security can introduce significant gains over the traditional isolated privacy protection. In fact, since complex signal detection/extraction processes must be performed first before decryption in every attack, the built-in security makes information recovery much more formidable to a malicious user.

Dedicated to my family

ACKNOWLEDGMENTS

I would like to take this opportunity to express my appreciation to my advisor, Dr. Tongtong Li, for her constant support, guidance and encouragement throughout the past four and half years. She makes her best endeavors to help me in every aspect, from providing advice on research to personal development and growth.

I want to thank Dr. Richard Enbody from Department of Computer Science and Engineering, and Dr. Jian Ren and Dr. Ning Xi from Department of Electrical and Computer Engineering for serving on my committee. I am deeply indebted to them for their kind support, either in the classroom or in all thoughtful correspondences. I would also like to thank Dr. Zhi Ding from Department of Electrical and Computer Engineering, University of California, Davis, for his recommendation of graduate study at Michigan State University and valuable help in research.

I am grateful to all my friends who have made my life at Michigan State University an enjoyable experience. I would like to extend my heartfelt thanks to Yong Ding, Yun Liu, Zhenwen Peng, Qionghua Qiang, Yingying Shi, Feng Wei, Channa Zhang and Miaomiao Zhang for being my great friends and for all the fun we have together. I would also like to send a special thank you to my lab mates Dr. Weiguo Liang, Mr. Leonard Lightfoot and Dr. Huahui Wang, for the valuable discussions on research and for the advice on the daily life in the United States.

Last, but not the least, I would like to thank my parents, my sister, my grandparents, my aunts and uncles for their love and continuous support. A special thanks goes to my friends, Kai Hu, Lei Zhu and Fanglei Zhuang, who always care for me as brothers and sisters and have given me good suggestions and ceaseless encouragement.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

"Images in this dissertation are presented in color"

CHAPTER 1

Introduction

1.1 Security in Wireless Communications

Wireless technology offers ease of accessibility, and enables freedom of mobility for users by releasing the constraint of physical connections to networks. Over the last few decades, wireless communication has exhibited explosive growth as an efficient transmission mechanism for voice, video and data services. In civilian communications, it is estimated that the number of wireless subscribers worldwide will reach 2.3 billion by 2009 [1]. In military communications, more than 98% of information transmission relies on wireless networks [2]. As people are relying more and more on wireless networks for critical information exchange in personal, industrial and military applications, the near ubiquitous wireless interconnectivity has given openings for malicious agents to exploit vulnerabilities on a widespread basis, such as wireless mobile Internet and e-commerce [3].

Due to *lack of a protective physical boundary*, wireless communications are much more vulnerable than their wireline counterparts. As data is being transmitted through the airlink, wireless transmissions are subjected to hostile jamming and interference. In addition, inherent broadcast nature of wireless communications results in potential interception and eavesdropping, since information intended to be received only by

authorized users can actually be intercepted by any suitable RF equipments within the radio range. Furthermore, the mobility and portability of wireless devices make them prone to losses and theft. All these factors cause serious and urgent security threats in wireless networks.

The future of wireless communications depends on our ability to strengthen security and provide a reliable information exchange platform. Patching or add-on security may be effective in the short run, but is far from adequate for addressing the needs on wireless security and can greatly complicate wireless communication systems. Driven by the ever-increasing demand on secure wireless networking, novel wireless systems with built-in security have become the next development impetus in communications.

1.2 Limitations with Existing Security Solutions

1.2.1 Lack of PHY Layer Security

Although security has emerged as an important issue in the design and development of wireless networks, most of research attention has been concentrated on the higher layers of the OSI model rather than the PHY layer.

Take privacy protection as an example. Privacy protection is the security service that ensures the confidentiality of the user data and control signals, for authorized users in a protected network. The most effective technique to achieve data privacy and information confidentiality is encryption. Encryption is a mechanism by which a message (i.e., plaintext) is combined with secret information (i.e., key) to generate a text (i.e., ciphertext) that cannot be recovered without the knowledge of the secret information. So far, source data encryption is the most widely used technique to ensure information confidentiality.

In today's wireless systems, privacy protection is primarily performed at upper layers, independent of the physical layer characteristics. This implies that data encryption and decryption are not assisted by, and considered in, physical layer transmitter-receiver designs. The major limitation with such an isolated privacy protection scheme is: Without the cooperation of a PHY layer enabled with built-in security, eavesdroppers can receive the encrypted message accurately. This potentially makes adversaries' job easier as the only barrier to obtaining the original information is the need for correct decryption, which is not too difficult when taking the weakness of some existing encryption algorithms into account. For example, several research groups [4–6] have reported some security holes and demonstrated to easily crack the 40-bit/128-bit WEP (Wired Equivalent Privacy) [7] because of the relatively weak encryption algorithm it uses.

The fact is, the PHY layer of a communication system, in general, does not possess security features. However, all the information transmission eventually takes place in the PHY layer. Without a inherently secure PHY layer, wireless signals are fragile to hostile jamming, information detection and interception.

1.2.2 Pure Signal Processing Based PHY Layer Security Techniques

With advances in array signal processing, some power-based and channel-based approaches have been proposed to strengthen PHY layer security by exploiting pure signal processing techniques.

Power-Based Approaches The adoption of smart or adaptive antenna arrays has been introduced as a promising technology to increase the capacity and improve the

performance [8–12]. Compared to the traditional omnidirectional antenna, the smart directional antenna can be used to physically keep intruder away from the legal user's propagation range to avoid the intentional interception. Some smart antennas can even provide a steerable beam to detect and distinguish the real signal and unwanted signal, and produce the sectored beam to the desired users and depress unwanted signals. The enhancement of information assurance in wireless networks can also be achieved through the use of adaptive antennas in conjunction with power control [13, 14].

Even with all the benefits of smart antennas, power-based security techniques have three problems. First, it is only an ideal case that the unauthorized user has null-receiving energy by simply deploying a directional antenna. There always exists some amount of energy leaking to the adversary, leading to a chance that the unauthorized user with powerful reception equipments can extract full/part of useful information. Second, smart antennas in general require heavy computation for eliminating interference, tracking source locations and synthesizing patterns. Many of these systems are thus limited by the speeds of analog-to-digital (A/D) converters or the complexity of the applied algorithms in the digital signal processing (DSP) domain. Third, the physical size of smart antennas is generally too large to fit into mobile devices and portable equipments.

Channel-Based Approaches Methods in this class aim to achieve information security by utilizing the wireless medium to either convey a confidential message or generate a secret key. Some transmission schemes have been designed by properly exploiting the channel between the transmitter and desired receiver, while the eavesdropper expects to experience considerable diversity loss based on the assumption any potential transmitter-eavesdropper channel will have totally different channel state in-

formation (CSI) [15–17]. As the channel condition matching to the true demodulator is required at the receiver side, the secure access on physical layer is realized [18–21]. It is also shown that a secret key can be generated from the natural environment of communication channels, i.e., the multi-path fading of a radio wave [22, 23]. The reciprocity in wave propagation is utilized to provide a secret key agreement scheme without intractable key management and key distribution processes.

However, the reciprocity of channels between the transmitter and the authorized user generally cannot be guaranteed in practical systems, since wireless medium itself is time-varying and unreliable. Moreover, the adversary can actively approach the authorized user, resulting in that the assumption that their transmissions are over different channels becomes invalid. Even if their channels are completely different, the unauthorized user may use blind estimation and equalization [24–32] to estimate channels and recover the original message subsequently, which makes many channel-based approaches lose secrecy.

1.2.3 PHY Layer Security in Spread Spectrum Systems

Generally, the PHY layer alone does not possess built-in security features except for spread spectrum systems. Historically developed for secure communication and military use, spread spectrum techniques, including direct-sequence code division multiple access (DS-CDMA) and frequency hopping (FH), are now major modulation and multiple access techniques in broadband cellular networks and WLAN communications.

Not only does spectral spreading force the interceptor to monitor an expanded frequency band, it also enables anti-jamming capability and location privacy [33, 34]. Although spread spectrum systems are resistant to narrow-band jamming, in reality, other jamming attacks can be used to compromise legal users' communication and the

jammer may very likely switch frequently from one pattern to another to improve its effectiveness. It is thus crucial to study the essential characteristics of commonly used hostile jamming attacks in spread spectrum systems and develop jamming classification methods, so that the appropriate anti-jamming procedures can be applied in an active, adaptive manner.

The inherent privacy potential of the DS-CDMA systems is based on the assumption that unintended receivers do not know the initial state used to generate the pseudo-random (PN) spreading sequence. Specifically, desired receivers use the initial seed to reconstruct, via a linear feedback shift register (LFSR), the spreading PN sequence. Unintended counterparts without the knowledge of the initial seed face a composite detection problem, whereby the unknown spreading sequence lies within an enormous set of valid choices. However, the seed of conventional binary-valued PN spreading sequences from known LFSRs can be consistently estimated based on noisy observations. Indeed, simple suboptimal estimators of the initial state of the LFSR can correctly identify the seed with very high probability based on just a fraction of the sequence period, even at very low chip power-to-noise ratios [35,36].

For FH systems, the inherent security relies on the difficulty to follow the desired user's transmitting frequency without the knowledge of the hopping pattern. Although frequency hopping is designed to minimize the probability of the unauthorized interception of telecommunications, the conventional FH systems suffer from *low spectral efficiency over large bandwidth.* Typically, FH systems require large bandwidth, which is proportional to the product of the hopping rate and the total number of all the available channels. In multiple access environment, collisions, caused by independent hops among different users, affect the system performance and reduce the spectral efficiency drastically. In the literature, considerable efforts have been devoted

to increasing the spectral efficiency of FH systems by applying high-dimensional modulation schemes [37–43]. However, existing work is far from adequate to address the enormously increased demand on inherently secure high speed wireless communication.

1.2.4 Summary of Major Limitations

- Without a secure PHY layer, wireless communication is fragile to lower layer attacks. An unprotected PHY layer enables the adversaries to perform traffic analysis/modification attacks and lowers the barrier to theft of user and network information.

- Strengthening the PHY layer security through pure signal processing techniques is an interesting research direction. However, some important issues go against their prevalence: High computational complexity and additional hardware cost severely restrict the practical application of power-based approaches; Channel-based approaches depend on some strong, unrealistic assumptions on channel state information, which can easily be violated in practical situations.

- The existing spread spectrum systems can provide a near-satisfactory PHY layer built-in security solution to voice-centric wireless communication, consisting generally of very short episodes. Nevertheless, the security provided by these systems is far from adequate and acceptable in wireless data communications. At the same time, driven by the ever increasing demand on high speed multimedia services, existing systems are also challenged to improve their spectral efficiency to support higher data rate without increasing the bandwidth.

1.3 Proposed Research Directions

This dissertation is focused on the fundamental study of developing spectrally efficient and inherently secure wireless air interface by integrating advanced signal processing techniques and cryptographic techniques into the PHY layer transceiver design. Multi-layer approaches are also investigated for secure information transmission in multiple access environment. More specifically, the proposed research directions are briefly summarized in the following subsections.

1.3.1 Resilient Time-Variant Jamming Modeling and Detection

In wireless networks, one of the most commonly used techniques for limiting the effectiveness of an opponent's communication is referred to as jamming, in which the authorized user's signal is deliberately interfered by the malicious user(s). Currently, jamming signals are classified into four groups: full-band jamming [44,45], partial-band jamming [46–48], tone jamming [49–51] and partial-time jamming [52–54]. Existing work on jamming detection and jamming prevention has generally been focused on a particular type of jamming, in which the jamming pattern is assumed to be known and invariant during the signal transmission period [51, 55–62]. However, in practical scenarios, hostile jamming can be dynamic and time variant. To the best of our knowledge, little attention has been paid to time-varying jamming modeling and jamming detection.

In this dissertation, we will study time-variant hostile jamming through the following thrusts: (i)Introduce a general, two-dimensional (2D) jamming generation model to characterize the time-varying jamming phenomenons; (ii) Establish a systematic

jamming classification framework based on the 2D model. The new framework will include all the existing jamming models as special cases. Statistics that characterize the average jamming lasting time and bandwidth will be introduced, to help achieve dynamic transmitter adjustment for optimum jamming resistance. (iii) Distinct hostile jamming from self-jamming (which is caused by multipath propagation and multiuser interference), and increase the accuracy of hostile jamming detection by exploiting self-jamming mitigation techniques.

1.3.2 Spectrally Efficient Anti-Jamming System Design

Existing jamming resistant systems, including DS-CDMA systems and FH systems, rely heavily on rich time-frequency diversity over large spread spectrum [63, 64]. Mainly limited by multiuser interference (caused by multipath propagation and asynchronization in DS-CDMA systems and by collision effects in FH systems), the spectral efficiency of existing jamming resistant systems are very low due to inefficient use of the large bandwidth. While these systems work reasonably well for voice centric communications which only requires relatively narrow bandwidth, their low spectral efficiency can no longer provide sufficient capacity for today's high speed multimedia wireless services. This turns out to be the most significant obstacle in planting anti-jamming features to high speed wireless communication systems, for which spectrum is one of the most precious resources. The major challenge here is: How to design wireless systems which are highly efficient but at the same time have excellent jamming resistance features?

In this dissertation, we aim to: (i) Incorporate advanced signal processing techniques and cryptographic algorithms into transmitter innovation; (ii) Integrate anti-jamming design into highly efficient communication systems (such as OFDM) through

a network-centric perspective. More specifically, we will introduce the concepts of message-driven frequency hopping and collision-free frequency hopping.

1.3.3 PHY-Driven Built-in Security Enhancement

As mentioned earlier, the PHY layer of most wireless systems (such as OFDM [65], GSM [66]) does not possess built-in security features. However, all the information exchange activities eventually have to take place in the PHY layer. Without the cooperation of a PHY layer enabled with built-in security, wireless signals are fragile to hostile jamming, detection and interception. This lowers the barrier to PHY layer attacks on user and network information, and also leads to inefficient transmission.

In this dissertation, by exploiting cryptographic encryption and inherent ambiguity in signal detection over multiple access channels, we plan to enhance the PHY layer built-in information confidentiality by integrating cryptography techniques into the transceiver design, and formulate a joint PHY layer and upper layer privacy protection mechanism. In essence, with the same computational complexity for the authorized parties, the built-in security makes information recovery much more formidable to a malicious user, since in every attack, complex (if at all possible) signal detection/extraction processes must be performed first before decryption. We will start with DS-CDMA, and then explore the establishment of PHY-layer built-in security in general wireless systems.

1.4 Overview of the Dissertation

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

- How to characterize time-varying jamming phenomenons and classify jamming

patterns efficiently?

- How to improve the spectral efficiency of the conventional FH systems, while maintaining the anti-jamming security feature?

- How to enhance the physical layer built-in security in wireless communications?

The dissertation is structured as follows.

Chapter II explores the time-varying jamming modeling and classification in wireless communications. First, a general, two-dimensional jamming generation model is introduced to characterize time-varying jamming phenomenons, including all the existing jamming models as special cases. The model is then studied closely and refined for spread spectrum systems, including both FH and DS-CDMA systems. According to our observation that self-jamming can be caused by multipath propagation and multiple access interference, we propose to study the difference between self-jamming and hostile-jamming. Taking DS-CDMA as the underlying communication system, self-jamming mitigation is discussed by exploiting interference cancellation methods. This is particularly important in improving the accuracy of hostile jamming detection in multiple access wireless environment. Novel jamming classification frameworks based on the time-varying jamming model are established, providing a broader horizon for systematic jamming modeling and jamming pattern recognition. By means of the statistical hypothesis test and the measurement/calculation of power spectral density (PSD) of the received signal, training-based and blind jamming detection approaches are developed. Finally, simulation examples are provided to demonstrate the effectiveness of the proposed approaches.

Chapter III presents two spectrally efficient secure communication interfaces: message-driven frequency hopping (MDFH) and collision-free frequency hopping

(CFFH). In MDFH, part of the message stream will be acting as the the PN sequence for hopping frequency selection, leading to the significantly improved spectral efficiency. Through blind detection of carrier frequencies, the MDFH scheme can resolve the synchronization limitation suffered by the conventional FH systems. From the security point of view, information confidentiality is also reinforced since the hopping pattern is message-driven, hence totally unpredictable. To make full use of the available spectrum in multiple access environment and further improve design flexibility, a highly bandwidth-efficient CFFH scheme is proposed. Based on the OFDM framework and the secure subcarrier assignment algorithm, the CFFH system can achieve high information capacity through collision-free multiple access, and can successfully relax the strict synchronization requirement. At the same time, as each user still transmits through a pseudo-random frequency hopping scheme, CFFH can maintain the inherent anti-jamming, anti-interception security features of the conventional FH system. The proposed schemes can be used for both civilian and military applications where secure high speed information transmission is needed.

Chapter IV exploits encryption based protection mechanism to strengthen the physical layer security in DS-CDMA systems and investigates possible extension to general wireless systems. First, security weakness of the operational and proposed CDMA airlink interfaces is analyzed. It is proved that the maximum complexity to recover the long code sequence is only $O(2^{42})$, which implies that the built-in information privacy provided by these systems is fairly unsatisfactory. Secondly, instead of using the conventional scrambling method, encrypted long code based on AES (advanced encryption standard) is proposed to enhance the security of DS-CDMA systems. Thirdly, motivated by the fact that chips spread from one symbol still cluster together after scrambling and are fragile to deep fading and/or strong burst errors,

chip-level secure interleaving is introduced as a substitution of securing scrambling to improve the system performance. Performance analysis demonstrates that information privacy can be significantly improved by integrating cryptographic techniques into the scrambling and/or interleaving process. Simulation examples are presented to illustrate the robustness of DS-CDMA systems with secure interleaving in adverse environments. Furthermore, both secure scrambling and secure interleaving can be extended to wireless systems other than DS-CDMA in multiple ways. As a start point, secure interleaving is integrated with the commonly deployed FEC (forward error control) process so that strong information confidentiality can be achieved through secure channel coding. The simplicity and effectiveness of the proposed schemes make them particularly attractive for 3G systems and beyond.

Chapter V summarizes the contributions and conclusions of the dissertation. An outline of related future work is also provided.

CHAPTER 2

Modeling and Detection of Hostile Jamming in Spread Spectrum Systems

In this chapter, a general, two-dimensional jamming generation model is presented to characterize jamming signals from both the time domain and the frequency domain. The model is studied closely and refined for spread spectrum systems, including both frequency hopping and direct-sequence CDMA systems. Self-jamming mitigation is investigated to increase the accuracy of hostile jamming detection by exploiting interference cancellation techniques. Novel jamming classification frameworks are established to provide a broader horizon for systematic jamming modeling and jamming pattern recognition. By means of the statistical hypothesis test and the measurement/calculation of power spectral density of the received signal, jamming detection approaches are developed. Simulation examples are provided to demonstrate the effectiveness of the proposed approaches.

2.1 Introduction

The fast computational speed improvement, rapid receiver technology advance and price declination facilitate the malicious attackers with an easy access to the wireless communication channels in the air. One of the most commonly used techniques for limiting the effectiveness of an opponent's communications is referred to as *jamming*. Generally, intentional jamming, also known as hostile jamming, intends to disable the legitimate transmission by saturating the receiver with noise or false information through deliberate radiation of radio signals, and thus significantly decreasing the signal-to-interference-plus-noise ratio (SINR).

Traditionally, hostile jamming has been characterized from either the frequency domain or the time domain: (i) Tone-jamming [49–51], where the jamming power is concentrated around carrier frequencies; (ii) Band-jamming [44–48], in which the jamming signal is modeled as a zero-mean wide sense stationary Gaussian random process. In general, band-jamming is further classified into full-band [44, 45], partial-band [46–48]. The power of full-band jamming is uniformly distributed over the bandwidth of interest with PSD N_J. Partial-band jamming is characterized by the additive Gaussian noise interference with PSD $\frac{N_J}{\rho}$ over a fraction ρ of the total bandwidth and negligible interference over the remaining fraction $(1-\rho)$ of the band; (iii) Partial-time jamming [52–54], where the jamming occurs at certain time periods during the signal transmission. It is basically a two-state Markov process. When the jammer is in state 0, it is off; when it is in state 1, the jammer emits the interfering signal. State 1 occurs with probability of ρ, along with the variance of jamming signals $\frac{N_J}{\rho}$. $(1-\rho)$ is the probability of occurrence of state 0, for which the variance of jamming signals is 0.

A considerable amount of work, see [51, 55–57, 59–62] for example, has been dedicated to the evaluation of the performance for a particular anti-jamming algorithm,

while little attention has been focused on the detection of hostile jamming. In fact, discovering jamming attacks is crucial because it is the first step towards building a secure and dependable wireless network. Efficient detection of hostile jamming makes it possible for the transmitter to implement a dynamic anti-jamming transmission scheme, and hence plays a key role in jamming prevention. However, the existing jamming detection methods are far from satisfactory. In virtue of powerful error-control coding (e.g., turbo codes), the maximum a posteriori (MAP) decoding algorithm was utilized to estimate the jammer's state by calculating the probability of a particular received symbol being jammed during its transmission [58, 67]. However, the computational complexity, mainly existing in two MAP algorithms running iteratively at the receiver, is prohibitively high. In [68], a hypothesis test was established with null hypothesis stating that the data channel was affected only by background thermal noise leading to a "small" channel error rate and the alternative hypothesis asserting that the data channel was being jammed with a "large" crossover probability. Basically, it is equivalent to measure the bit error rate (BER) of the normal traffic or jammed channel and then set a specific threshold for the BER, while completely ignoring the distinct characteristics of jamming signals with different underlying models.

Moreover, existing work on jamming suppression and jamming prevention is generally targeted at a particular jamming model at a time. That is, the jamming pattern is assumed to be known and invariant during the signal transmission period, see [51, 55–62] for example. In practice, however, in order to deliberately malfunction the anti-jamming algorithms, the jammer may very likely switch frequently from one pattern to another, with each jamming pattern only lasting a short period of time. In other words, hostile jamming can be dynamic and time-variant. Time-varying jamming modeling, classification and dynamic jamming detection, therefore, are highly

desirable in the sense that the transmitter can be adjusted adaptively to combat time-variant hostile jamming.

To this end, we investigate the modeling and detection of hostile jamming in wireless communications. First, a general 2D jamming generation model is presented to characterize the more realistic time-varying jamming phenomenons. Using such a model is advantageous to analyze the essential characteristics of commonly used jamming models, including the similarity and difference between different models. We extract discrimination features for the traditional jamming patterns and develop a binary decision tree for the purpose of identification. Next, a novel jamming classification framework is established based on the time-varying jamming model. Motivated by the results on time-varying channel modeling, we analyze the coherence time (the time period over which the jamming remains unchanged) and coherence bandwidth (the frequency range over which the jamming power spectrum is approximately flat) of the jamming generation system, and introduce the concepts of fast jamming, slow jamming, flat jamming and frequency-selective jamming. Including all the existing jamming models as special cases, this new framework provides a broader horizon for systematic jamming modeling and jamming pattern recognition. Finally, based on our observation that self-jamming can be caused by multipath propagation and multiple access interference, we propose to study the difference between self-jamming and hostile-jamming. Taking CDMA as the underlying communication system, self-jamming mitigation is investigated by exploiting interference cancellation methods. This is particularly important in improving the accuracy of hostile jamming detection in multiple access wireless environment.

The rest of the chapter is organized as follows: In Section 2.2, we introduce a general, two-dimensional jamming model. In Section 2.3, the model is studied closely

and refined for frequency hopping systems. In Section 2.4, the well-known "self-jamming" in both uplink and downlink CDMA is investiaged, and interference cancellation techniques are presented to enhance the discrimination of hostile jamming. In Section 2.5, two jamming classification frameworks are proposed based on the conventional and proposed jamming models, respectively. In Section 2.6, jamming detection methods are developed by means of the statistical hypothesis test and the measurement/calculation of power spectral density of the received signal. Simulation examples are provided in Section 2.7 and we conclude in Section 2.8.

2.2 A General Jamming Generation Model

Motivated by the fact that jamming signals may be time-variant, we propose to characterize hostile jamming in wireless systems through a more general and systematic model. We begin with a single-input-single-output AWGN channel. Let $s(t)$ be the transmitted signal, then the received signal can be written as:

$$r(t) = s(t) + n(t) + J(t), \tag{2.1}$$

where $n(t)$ is the white Gaussian noise, $J(t)$ represents the intentional jamming signal. We model the jamming signal $J(t)$ as the output of a time-varying jamming generating system represented by

$$J(t) = \int_{-\infty}^{\infty} g(t,\tau)x(t-\tau)d\tau, \tag{2.2}$$

where $x(t)$ is the input signal and $g(t,\tau)$ is the time-variant channel response of the jamming system at instant t to an impulse applied at time $t-\tau$.

Assume that $g(t,\tau)$ is wide-sense stationary (WSS) with respect to τ. Let

$R_g(t, \Delta\tau) = E[g(t, \tau + \Delta\tau)g(t, \tau)]$ be the time-varying correlation function of $g(t, \tau)$. Define $S_g(t, f)$ as the time-varying power spectral density of $g(t, \tau)$, given by

$$S_g(t, f) = \int_{-\infty}^{\infty} R_g(t, \Delta\tau) e^{-j2\pi\Delta\tau f} d(\Delta\tau). \tag{2.3}$$

Limited by the size and capability of the jamming generation device, the total jamming power is finite. Let P_J be the average jamming power, that is,

$$P_J = E\left[\int_{-\infty}^{\infty} S_g(t, f) df\right]. \tag{2.4}$$

Over short periods of time, $g(t, \tau)$ (as well as $S_g(t, f)$) may be approximately time-invariant. Taking this into consideration, it can be shown that this general model contains all the existing models as special cases. In fact, if $g(t, \tau) = g(\tau)$ is time-invariant, and $x(t) = \delta(t)$, then we have $J(t) = g(t)$, and $S_g(t, f)$ reduces to $S_g(f)(= S_J(f))$.

Let $[f_0, f_1]$ be the total available frequency band over which the message signal is transmitted, and $[t_0, t_1]$ be the time duration of the message signal. Let $x(t) = \delta(t)$.

- If $S_g(t, f) = \frac{P_J}{f_1 - f_0} \triangleq N_J, \forall f \in [f_0, f_1], \forall t \in [t_0, t_1]$, then $J(t)$ is traditional full-band jamming model as a white Gaussian process whose power spectral density is flat over the entire bandwidth.

- If $S_g(t, f) = P_J \delta(f - f_k), \forall t \in [t_0, t_1]$, where $f_k \in [f_0, f_1]$, then $J(t)$ is an ideal single-tone jamming with all the power accumulated on a particular frequency f_k. Similar definitions can be extended to multi-tone jamming. More specifically,

$$S_g(t, f) = \sum_{k=0}^{n} P_J(t, f_k)\delta(f - f_k), \text{with } \sum_{k=0}^{n} P_J(t, f_k) = P_J, \tag{2.5}$$

where $P_J(t, f_k)$ stands for the jamming power allocated for the kth frequency component at time instance t, and δ is the Dirac delta function.

- If $S_g(t, f)$ is a rectangular pulse along the f-axis and not varying along the t-axis from t_0 to t_1, i.e.,

$$S_g(t,f) = \begin{cases} 0, & \forall f \in [f_0, f_i) \bigcup (f_j, f_1], \forall t \in [t_0, t_1] \\ \frac{P_J}{f_j - f_i} = \frac{N_J}{\rho_f}, & \forall f \in [f_i, f_j],\ \forall t \in [t_0, t_1] \end{cases} \tag{2.6}$$

where f_i and f_j with $f_i \leq f_j$ are certain intermediate frequencies within $[f_0, f_1]$, $\rho_f \triangleq \frac{f_j - f_i}{f_1 - f_0}$ implies the fraction of the bandwidth being jammed, then $J(t)$ is a typical partial-band jamming during the time interval $[t_0, t_1]$.

- If $S_g(t, f)$ is a rectangular pulse along the t-axis during t_0 and t_1 and invariant along the f-axis within $[f_0, f_1]$,

$$S_g(t,f) = \begin{cases} 0, & \forall t \in [t_0, t_m) \bigcup (t_n, t_1], \forall f \in [f_0, f_1] \\ \frac{P_J}{f_1 - f_0} \frac{t_1 - t_0}{t_n - t_m} = \frac{N_J}{\rho_t}, & \forall t \in [t_m, t_n], \forall f \in [f_0, f_1] \end{cases} \tag{2.7}$$

where t_m and t_n with $t_m \leq t_n$ are certain intermediate time instances within $[t_0, t_1]$, $\rho_t \triangleq \frac{t_n - t_m}{t_1 - t_0}$ indicates the fraction of the time interval that the channel is jammed, then $J(t)$ is a typical partial-time jamming signal.

2.3 Jamming Model for Frequency Hopping Systems

Assume that the transmitter is able to hop among N_c available channels, each of which occupies a bandwidth of B_{ch}. In order to maintain the orthogonality among

carriers, B_{ch} needs to be an integer multiple of $\frac{1}{T}$, where T is the symbol interval in slow frequency hopping (SFH) systems or the hopping duration in fast frequency hopping (FFH) systems. In general, we simply set $B_{ch} = \frac{1}{T}$, in order to save the total bandwidth.

Define a binary vector $\underline{\alpha} \triangleq [\alpha_0, \alpha_1, \cdots, \alpha_{N_c-1}]$ for the transmitter. For $i = 0, 1, \cdots, N_c - 1$, $\alpha_i = 1$ indicates the ith channel is currently used by the transmitter to convey information. Otherwise, the ith channel is idle if $\alpha_i = 0$. Similarly, $\underline{\beta} \triangleq [\beta_0, \beta_1, \cdots, \beta_{N_c-1}]$ is defined as the jamming index vector, where the jth entry $\beta_j = 1$ implies that the jth channel is deliberately jammed, and $\beta_j = 0$ means that there is no intentional jamming on the jth channel, for $j = 0, 1, \cdots, N_c - 1$.

For either SFH or FFH systems, the transmitter changes its desired traffic channels from one hop to another. In other words, $\underline{\alpha}$ is actually a time-varying vector. On the other hand, the jammer can have its own jamming strategy, by choosing arbitrary $\underline{\beta}$. Specifically, based on the particular choice of $\underline{\beta}$, the jamming model can be generalized as follows:

- If $\underline{\beta} = \underline{c}$, where $\underline{c}$ is a constant binary vector, then the jamming is independent of time. It is referred to as *fixed-band jamming*. Two special cases are $\underline{c} = \underline{0}$ and $\underline{c} = \underline{1}$, where $\underline{0}$ is an all-zero vector and $\underline{1}$ is an all-one vector, corresponding to no jamming and full-band jamming, respectively.

- If $\underline{\beta}$ is a function of time, then *random jamming* happens when $\underline{\beta}$ is randomly chosen during each hopping duration. In the worst case, smart jammers can be implemented as long as the condition that $\underline{\beta} = \underline{\alpha}$ can always be satisfied. It essentially means the jammer can follow the frequency hop all the time.

- If $\underline{\beta}$ is neither an all-zero nor an all-one vector at any time instance, it is generally

partial-band jamming (either fixed-band or random jamming). If $\underline{\beta}$ is an all-zero vector within each hopping duration except for certain time intervals, it is referred to as partial-time jamming.

Suppose that the jammer changes its jamming index vector over time and spreads its available power equally over all the channels it intends to jam. We ameliorate the general white Gaussian model into a more sophisticated one with its time-varying power spectral density defined as follows:

$$S_g(t,f) = \overline{P_J} \sum_{j=0}^{N_c-1} \beta_j(t)\chi(f - f_0 - jB_{ch}), \tag{2.8}$$

where f_0 is the initial frequency shift, $\beta_j(t)$ indicates the jamming index β_j at the time instance t,

$$\overline{P_J} = \begin{cases} 0, & \text{if } \sum_{j=0}^{N_c-1} \beta_j(t) = 0, \\ \dfrac{P_J}{\sum_{j=0}^{N_c-1} \beta_j(t)B_{ch}}, & \text{if } \sum_{j=0}^{N_c-1} \beta_j(t) \neq 0, \end{cases} \tag{2.9}$$

$$\chi(f) = \begin{cases} 1, & \text{if } f \in [0, B_{ch}), \\ 0, & \text{else.} \end{cases} \tag{2.10}$$

2.4 Jamming Model for DS-CDMA Systems

2.4.1 Single-User Systems

We begin with the simple case where CDMA signals are sent over an AWGN channel. At the receiver end, it yields

$$r(t) = d(t)p(t) + n(t) + J(t), \quad 0 \leq t \leq T, \tag{2.11}$$

where $d(t)$ is the information signal, $p(t)$ is the signature wave, $n(t)$ is the additive white Gaussian noise, $J(t)$ is the jamming signal and T is the symbol period.

The power spectral density of $d(t)$ is approximately given by

$$S_d(f) = T\left(\frac{\sin \pi fT}{\pi fT}\right)^2. \tag{2.12}$$

Let $s(t) \triangleq d(t)p(t)$ be the spreading signal. Since $p(t)$ is the chip-level waveform at a rate of f_c chips/second, by substituting $\frac{1}{f_c}$ for T in (2.12), we can easily obtain the power spectral density of $s(t)$,

$$S_s(f) = \frac{1}{f_c}\left(\frac{\sin \pi f/f_c}{\pi f/f_c}\right)^2. \tag{2.13}$$

After despreading, we obtain

$$z(t) \triangleq r(t)p(t) \tag{2.14}$$

$$= d(t) + n(t)p(t) + J(t)p(t), \tag{2.15}$$

where $J(t)p(t)$ represents the code-modulated jamming signal.

Two scenarios are considered:

1. If the jamming signal expands the whole channel bandwidth, then the code-modulated jamming signal will further spread the spectrum, thus can be approximately modeled as white noise. On the other hand, the desired despread signal's power is concentrated within $[-\frac{1}{T}, \frac{1}{T}]$ Hz. To extract $d(t)$, we can pass $z(t)$ through a lowpass filter with a cutoff frequency $\frac{1}{T}$ Hz. At the output of the lowpass filter, the desired signal's power remains largely unchanged, while the jamming power is reduced by a fraction of $f_c T$. Therefore, the jamming-to-signal ratio (JSR) is decreased by $f_c T$.

2. If the jammer concentrates its available energy within the bandwidth associated with the original signal, for example, $J(t) = \sqrt{E_J/T}, \forall t \in [0, T]$, where E_J is the jamming energy and T is the symbol duration. In this case, the PSD of $J(t)$ has the same form as that of $S_d(f)$ in (2.12). Due to the frequency diversity in CDMA signals, a narrow-band interference elimination filter can be used to filter out the intentional jamming completely before despreading without seriously degrading the system performance.

Beyond the AWGN channel, if the channel impulse response is modeled as

$$h(t) = \sum_{l=0}^{L-1} h_l \delta(t - d_l), \tag{2.16}$$

where $\{h_l\}_{l=0}^{L-1}$ are complex attenuation coefficients and $\{d_l\}_{l=0}^{L-1}$ are delays for L

different paths, then the received signal can be written as

$$r(t) = \sum_{l=0}^{L-1} h_l s(t-d_l) + n(t) + J(t) \tag{2.17}$$

$$= h_0 s(t) + \sum_{l=1}^{L-1} h_l s(t-d_l) + n(t) + J(t), \tag{2.18}$$

where d_0 is assumed to be 0, without loss of generality.

As can be seen, in addition to the noise $n(t)$ and the jamming signal $J(t)$, multipath propagation results in *self-jamming*, i.e., $\sum_{l=1}^{L-1} h_l s(t-d_l)$.

Considering the well-known fact that the original data is spread by pseudo-random sequences leading to a wideband signal of $s(t)$, any delayed or scaled version of $s(t)$ does not change the signal's bandwidth, eventually resulting in the wideband characteristic of the self-jamming term. If $J(t)$ only occupies a narrow frequency band with strong power within that band, the hostile jamming can easily be detected, since the other terms except $J(t)$ on the right-hand side of (2.18) are all wideband signals with low power spectral density. That is, we are able to distinguish partial-band jamming from self-jamming, by simply taking samples over the entire bandwidth of the power spectral density of the received signal.

2.4.2 Multi-User Systems

For multiple access DS-CDMA systems, in addition to inter-symbol interference within each user's signal caused by frequency selective fading, self-jamming among authorized users occurs when the orthogonality of spreading codes among users is not maintained due to multipath propagation or asynchronous transmission.

Uplink

In DS-CDMA uplink, users are generally asynchronous. If the kth user's channel is modeled as

$$h_k(t) = \sum_{l=0}^{L-1} h_{k,l}\delta(t - d_{k,l}), \tag{2.19}$$

where $\{h_{k,l}\}_{l=0}^{L-1}$ are complex attenuation coefficients and $\{d_{k,l}\}_{l=0}^{L-1}$ are delays for L (the maximal channel order among all the multipath channels) different paths, then the received interference-free signal is given by

$$s(t) = \sum_{k=0}^{K-1}\sum_{l=0}^{L-1} h_{k,l} \sum_{m=-\infty}^{\infty} d_k(t - d_{k,l})p_k(t - d_{k,l}), \tag{2.20}$$

where $d_k(t)$ is the kth user's transmitted signal, $p_k(t)$ is the kth user's signature wave. Consequently, the received data in the presence of the additive noise and hostile jamming can be written as

$$r(t) = s(t) + n(t) + J(t). \tag{2.21}$$

It is reasonable to assume that the base station has the knowledge of all users' spreading codes. Once each uplink channel corresponding to one particular user is accurately estimated using high-power pilot symbols, the desired signal wave along with its delayed and scaled versions, i.e., $s(t)$, can be completely eliminated from the received signal $r(t)$, leaving only the additive white noise and possible hostile jamming signals behind. Then, if the jamming power is significant enough, simple detection methods at the receiver should be able to discover its occurrence.

Downlink

The situation is different, however, in DS-CDMA downlink. The signal received by the jth user is

$$r_j(t) = \sum_{k=0}^{K-1} \sum_{l=0}^{L-1} h_{j,l} \sum_{m=-\infty}^{\infty} d_k(t - d_{j,l}) p_k(t - d_{j,l}) + n(t) + J(t). \tag{2.22}$$

It is common sense that one user is unaware of any users' spreading codes except for his own code. Thus, multiuser interference cannot be directly removed from the unprocessed signal at the receiver end. Although there exist some approaches to mitigate or completely cancel the effect of self-jamming for downlink communications using judiciously designed linear transformation or spreading codes, see [69, 70] for example, the characteristics of the hostile jamming signal after performing such procedures are unpredictable, leading it difficult to be modeled and detected.

Here, we propose to detect hostile jamming by turns for each user. Accordingly, the jth user's received signal can be represented by

$$r_j(t) = \sum_{l=0}^{L-1} h_{j,l} \sum_{m=-\infty}^{\infty} d_j(t - d_{j,l}) p_j(t - d_{j,l}) + n(t) + J(t). \tag{2.23}$$

It is essentially equivalent to the case of single user's transmission, in which multipath propagation is the only cause of self-jamming. After obtaining the estimation of $\{h_{j,l}\}_{l=0}^{L-1}$ and $\{d_{j,l}\}_{l=0}^{L-1}$, the first term on the right-hand side of (2.23) can be removed by the jth user. Then the jth user can easily identify the jamming pattern on his own channel by following the procedures in Section 2.5.

2.5 Classification of Jamming Models

2.5.1 Jamming Classification Based on the Conventional Jamming Models

In order to identify the pattern of jamming signals, we first need to investigate distinguishable features among partial-time jamming ($0 < \rho_t < 1$), partial-band jamming ($0 < \rho_f < 1$), flat full-band jamming ($\rho_f = 1$) and no jamming ($\rho_f = 0$).

According to the definitions, only partial-time jamming has significant changes on power spectrum over a certain interval of time, while partial-band and full-band jamming hold a negligible variance on power spectrum with respect to time at individual frequencies. This critical characteristic of partial-time jamming can be used to distinct itself from other jamming patterns.

Similarly, the variance of power with respect to frequency can be exploited as a discriminant measurement between partial-band and flat full-band jamming. Next, it renders an intractable problem of separating flat full-band jamming from the background white noise. Unfortunately, flat full-band jamming cannot be easily differentiated from the background white noise, if the jamming power allocated for each frequency is unsubstantial. In that case, the hostile jamming signal can simply be regarded as the additional noise, since its negative effect on the system performance is negligible. In other words, it is meaningful to distinguish flat full-band jamming from the white noise only if the jamming power is significant enough to degrade the system performance drastically.

We propose to classify the jamming strategies by using a binary decision tree, where by convention the root node is put at the top, connected by successive links to other nodes, as shown in Figure 2.1.

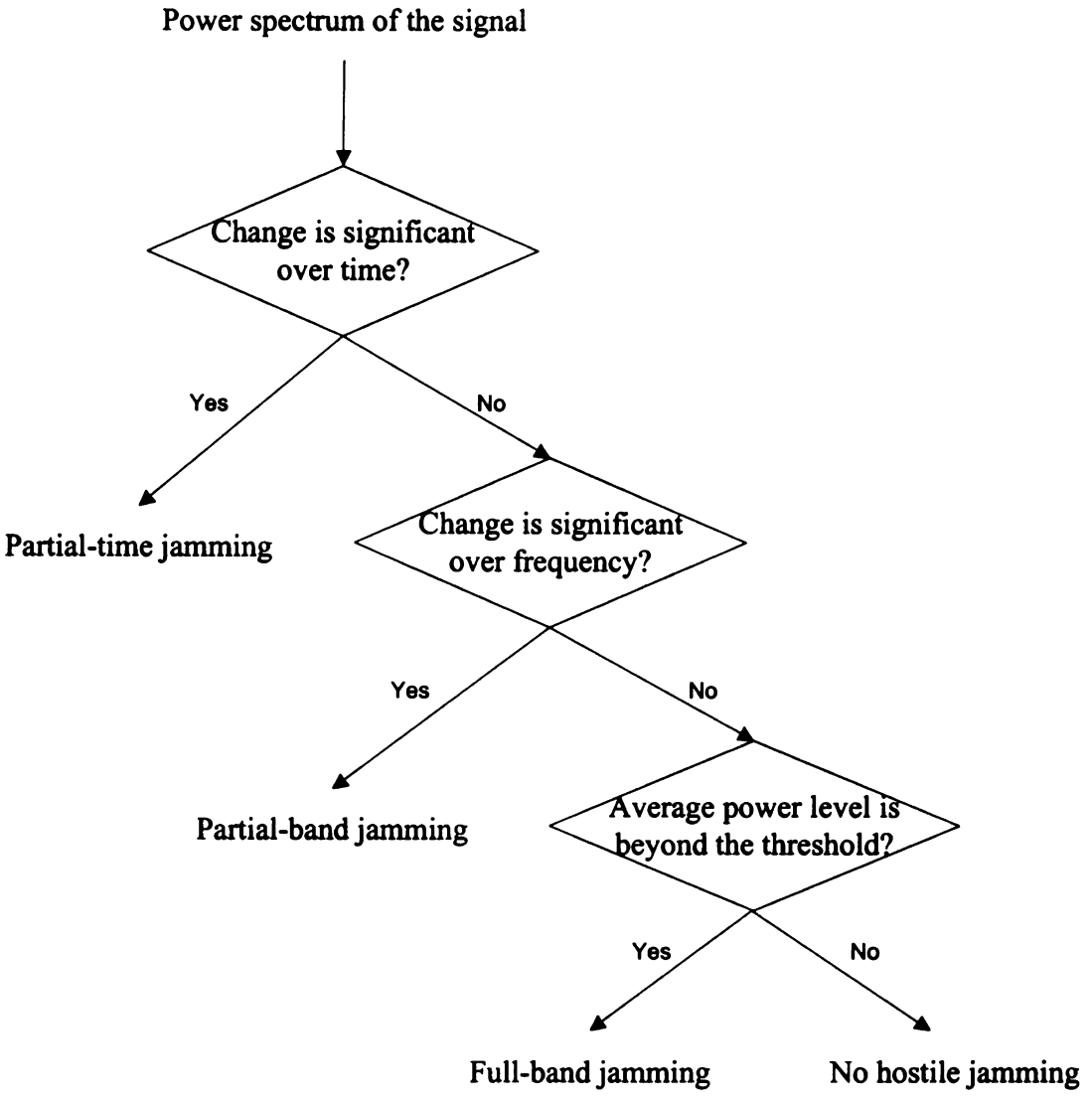


Figure 2.1. Flow diagram of classifying the traditional jamming models.

For real-time applications, the variance of signal power may not be accurately estimated due to lack of samples within a short period. Therefore, we resort to detecting step edges on the two-dimensional power spectrum in the sense that a rising/falling edge canonically represents an abrupt transition. For identification of partial-time jamming and estimation of the corresponding effective time, we utilize two thresholds (i.e., T_{r1} for the rising edge, T_{f1} for the falling edge). Two different thresholds T_{r2} and T_{f2} are similarly set for partial-band jamming. To distinguish flat full-band jamming from the background white noise, another threshold T_{r3} is used. Classification is carried out through the following procedures:

Step 1: Power spectrum is approximately estimated by the magnitude-squared FFT of the received signal using the sliding window approach.

Step 2: Average the power spectrum over frequency and measure the results successively along the time dimension. If none of signals' power exceeds T_{r1}, go to step 3. Otherwise, mark the first time instances with the power level over T_{r1} as $\hat{t}_l$, then below T_{f1} as $\hat{t}_h$. As a result, $\hat{\rho}_t$ is equal to the ratio of the estimated jamming duration $(\hat{t}_h - \hat{t}_l)$ to the total observation time. Go to step 5.

Step 3: Take the average of the power spectrum over time, then search the results in sequence along the frequency dimension. Once discovering one signal power exceeding T_{r2} at frequency $\hat{f}_l$, we assume that partial-band jamming is identified. As long as the power is not below T_{f2} until frequency $\hat{f}_h$, jamming remains effective. $\hat{\rho}_f$ is then calculated as the ratio of the estimated jamming bandwidth $(\hat{f}_h - \hat{f}_l)$ to the total available bandwidth. If partial-band jamming is not discovered, go to step 4, otherwise go to step 5.

Step 4: If the average power level goes beyond T_{r3}, then flat full-band jamming is rec-

ognized and $\hat{\rho}_f = 1$. Otherwise, no jamming occurs in the received signal and $\hat{\rho}_f = 0$.

Step 5: Go to step 1 to process the next received data block.

2.5.2 Jamming Classification Based on the Time-Variant Jamming Generation Model

In this subsection, we discuss time-varying jamming classification based on the two-dimensional jamming generation model.

We assume

1. $g(t, \tau)$ is zero-mean.
2. $g(t, \tau)$ is a WSS process.
3. For any $\tau_1 \neq \tau_2$, $g(t, \tau_1)$ and $g(t, \tau_2)$ are uncorrelated.

It then follows from these assumptions that

$$R_g(\Delta t, \tau_1, \tau_2) \triangleq \frac{1}{2} E[g(t + \Delta t, \tau_2) g^*(t, \tau_1)] \tag{2.24}$$

$$= R_g(\Delta t, \tau_1) \delta(\tau_1 - \tau_2). \tag{2.25}$$

Let $\Delta t = 0$, we have

$$R_g(\tau) = R_g(0, \tau) \tag{2.26}$$

$$= \frac{1}{2} E[g(t, \tau) g^*(t, \tau)] \tag{2.27}$$

$$= \frac{1}{2} E[|g(t, \tau)|^2]. \tag{2.28}$$

Let $G(t,f) = \int_{-\infty}^{\infty} g(t,\tau)e^{-j2\pi f\tau}d\tau$ be the Fourier transform of $g(t,\tau)$ with respect to variable τ. Assume $g(t,\tau)$ is WSS, so is $G(t,f)$.

Define $R_G(\Delta t, \Delta f) = \frac{1}{2}E\{G(t+\Delta t, f+\Delta f)G^*(t,f)\}$. Let $\Delta t = 0$, we obtain

$$\begin{aligned} R_G(\Delta f) &= \frac{1}{2}E[G(t,f+\Delta f)G^*(t,f)] && (2.29)\\ &= \frac{1}{2}E[[\int_{-\infty}^{\infty} g(t,\tau_1)e^{-j2\pi(f+\Delta f)\tau_1}d\tau_1][\int_{-\infty}^{\infty} g(t,\tau_2)e^{-j2\pi f\tau_2}d\tau_2]^*] && (2.30)\\ &= \frac{1}{2}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} E[g(t,\tau_1)g(t,\tau_2)^*]e^{-j2\pi f(\tau_1-\tau_2)}e^{-j2\pi\Delta f\tau_1}d\tau_1 d\tau_2. && (2.31) \end{aligned}$$

Since $g(t,\tau_1)$ and $g(t,\tau_2)$ are assumed to be uncorrelated,

$$R_G(\Delta f) = \int_{-\infty}^{\infty} R_g(\tau)e^{-j2\pi\Delta f\tau}d\tau. \qquad (2.32)$$

This is the frequency correlation function of the jamming generation function.

Let $(\Delta f)_c$ be the range of frequencies over which $R_G(\Delta f)$ is approximately flat ($R_G(\Delta f) \geq 0.9$ or 0.5), then $(\Delta f)_c$ is a coherence bandwidth of the jamming channel. As in the time-varying channel modeling, we introduce the concept of flat jamming and frequency-selective jamming based on the value of $(\Delta f)_c$ and the authorized user's signal bandwidth B.

If $(\Delta f)_c > B$, we say that the signal is experiencing *flat jamming*, otherwise, we say that the signal is undergoing *frequency-selective jamming*. We can say that full-band jamming belongs to flat jamming, and both partial-band jamming and tone-jamming belong to frequency-selective jamming.

If we set $\Delta f = 0$ in $R_G(\Delta t, \Delta f)$ and define

$$\overline{R}_G(\nu) = \int_{-\infty}^{\infty} R_G(\Delta t, 0) e^{-j2\pi\nu\Delta t} d\Delta t, \tag{2.33}$$

then $\overline{R}_G(\nu)$ is the Doppler power density of the jamming channel. Let B_d be the nominal bandwidth of $\overline{R}_G(\nu)$, then the coherence time of the jamming channel can be obtained as

$$(\Delta t)_c \approx \frac{1}{B_d}, \tag{2.34}$$

which is a statistical measure of the time duration over which the jamming channel is essentially invariant.

Let T_s be the symbol duration of the authorized user's signal. If $(\Delta t)_c < T_s$, then jamming variations are faster than signal variations, we call it *fast jamming*; If $(\Delta t)_c \geq T_s$, then jamming variations are slower than signal variations, and we call it *slow jamming*.

To estimate $(\Delta t)_c$, we perform time-frequency analysis on the observed one-dimensional signal wave $J(t)$ to generate a view of the signal represented over both time and frequency simultaneously. The most commonly used methods are Wavelet transforms, Wigner-Ville distribution and Short-Time Fourier Transform (STFT), which can provide some information about how the spectral content of the signal evolves with time.

Assume that the coherence time of jamming signals is invariant and prior knowledge of $(\Delta t)_c$ through rough estimation/previous estimate is known: $(\Delta t)_c \in [(\Delta t)_c^l, (\Delta t)_c^u]$. Once the two-dimensional power spectral density $S_J(t, f)$ is obtained, fine estimation of $(\Delta t)_c$ can be carried out as follows:

Step 1: Arbitrarily choose a start time t_s, then scan $S_J(t,f)$ along the t-axis to find K such that

$$\begin{cases} \text{diss}(S_J(t_s + k\Delta T, f), S_J(t_s, f)) \leq \Upsilon, & 0 \leq k < K \\ \text{diss}(S_J(t_s + K\Delta T, f), S_J(t_s, f)) > \Upsilon, \end{cases} \tag{2.35}$$

where ΔT is the time resolution of 2-D PSD, Υ is the specified threshold, and $\text{diss}(x,y)$ denotes a function that measures the dissimilarity between x and y. Specifically, $\text{diss}(x,y)$ returns a nonnegative scaler that indicates the pairwise difference between x and y. $\text{diss}(x,y) = 0$ if and only if $x = y$. For example, if the Euclidean distance is adopted as the difference measure, then (2.35) becomes

$$\begin{cases} \sqrt{\sum_k |S_J(t_s + k\Delta T, f_k) - S_J(t_s, f_k)|^2} \leq \Upsilon, & 0 \leq k < K \\ \sqrt{\sum_k |S_J(t_s + k\Delta T, f_k) - S_J(t_s, f_k)|^2} > \Upsilon. \end{cases} \tag{2.36}$$

An alternative measurement is correlation, which gives (2.35) another realization,

$$\begin{cases} |\sum_k S_J(t_s + k\Delta T, f_k) S_J^*(t_s, f_k)| \leq \Upsilon, & 0 \leq k < K \\ |\sum_k S_J(t_s + k\Delta T, f_k) S_J^*(t_s, f_k)| > \Upsilon, \end{cases} \tag{2.37}$$

where $'*'$ denotes the conjugate transpose.

Step 2: Let $t_s = t_s + K\Delta T$, then search for the end time, denoted by t_e, to get another K by following (2.35). As a result, $t_e = t_s + K\Delta T$.

Step 3: $(\hat{\Delta t})_c = t_e - t_s$. If $(\hat{\Delta t})_c$ does not fall within $[(\Delta t)_c^l, (\Delta t)_c^u]$, then the estimation of coherence time is unsuccessful, due to the insignificant change of jamming

signals during the time interval from t_s to t_e. To continue, let $t_s = t_e$ and then start over the above procedures.

2.6 Detection of Hostile Jamming

An important application of jamming detection is to avoid transmission over the intentionally jammed channels, because it is most likely that the detected and decoded information is erroneous due to the low SINR even if jamming suppression approaches are applied at the receiver.

The intuitive measurement for jamming is either the signal strength (if jammer emits a constant amplitude signal), or the energy level (if jammer emits a noise-like signal such as white Gaussian signals). Generally, clear, unjammed data record is needed at the receiver end to establish a statistical model describing the normal energy level prior to jamming.

2.6.1 Jamming Detection in Frequency Hopping Systems

We follow the idea of the hypothesis test and apply it to jamming detection,

$$\begin{aligned} H_0: &\quad \text{the channel is not jammed,} \\ H_1: &\quad \text{the channel is jammed.} \end{aligned}$$

Under the assumption that signals are transmitted over an AWGN channel, the two hypotheses can be represented by

$$\begin{aligned} H_0: &\quad r(t) = s(t) + n(t), \\ H_1: &\quad r(t) = s(t) + n(t) + J(t), \end{aligned}$$

where $n(t)$ is white Gaussian noise with single-sided PSD N_0 and $J(t)$ is simply modeled as a zero-mean white Gaussian process with single-sided PSD N_J.

Here, we consider two cases:

Training Available

First, update $r(t)$ by subtracting the training symbol $s(t)$ from it, then it yields

$$\begin{aligned} H_0: &\quad r(t) = n(t), \\ H_1: &\quad r(t) = n(t) + J(t). \end{aligned}$$

Under the null hypothesis H_0, $r(t)$ is a Gaussian random process with single-sided PSD N_0; Under the alternative hypothesis H_1, $r(t)$ is a Gaussian random process with single-sided PSD $N_0 + N_J$.

- If N_J is unknown (but definitely positive), during training phase, we measure the samples' energy, and build a threshold representing the normal energy level, e.g., $\lambda = E[|r(t)|^2]$. During test phase, we make the final decision whether or not there exists hostile jamming in $r(t)$, by comparing the average energy level obtained from samples $\{r_k\}_{k=1}^K$ with the threshold, that is,

$$\frac{1}{K}\sum_{k=1}^{K}|r_k|^2 \underset{H_0}{\overset{H_1}{\gtrless}} \lambda. \tag{2.38}$$

- If N_0 and N_J are fixed and known (or estimated from previous samples), then we can easily formulate two conditional probability density functions:

$$P(\underline{r}|H_0) = \frac{1}{(\sqrt{2\pi N_0})^K} e^{-\frac{1}{2N_0}\sum_{k=1}^{K}|r_k|^2}, \tag{2.39}$$

$$P(\underline{r}|H_1) = \frac{1}{(\sqrt{2\pi(N_0+N_J)})^K} e^{-\frac{1}{2(N_0+N_J)}\sum_{k=1}^{K}|r_k|^2}, \tag{2.40}$$

where $\underline{r} = [r_1, r_2, \cdots, r_K]^T$.

In this case, the likelihood ratio test (LRT) can be directly applied,

$$\Lambda \triangleq \frac{1}{N_0} \frac{N_J}{N_0 + N_J} \sum_{k=1}^{K} |r_k|^2 \underset{H_0}{\overset{H_1}{\gtrless}} \eta \tag{2.41}$$

Training Unavailable

Since no pilot symbols are available, we utilize second-order statistics (SOS) based blind detection at the receiver end.

First examine the mean of $r(t)$ under two hypotheses. Since both $n(t)$ and $J(t)$ are of zero mean, we have

$$\begin{aligned} H_0: \quad E[r(t)] &= E[s(t)] + E[n(t)] \\ &= E[s(t)], \\ H_1: \quad E[r(t)] &= E[s(t)] + E[n(t)] + E[J(t)] \\ &= E[s(t)]. \end{aligned} \tag{2.42}$$

As can be seen from (2.42), H_0 and H_1 share the same mean. The simplest solution under this circumstance is to calculate the covariance of $r(t)$ through time-averaging.

Considering the independence among the data symbol, the additive noise and the jamming signal, we get

$$
\begin{aligned}
H_0: \quad E[|r(t) - E[r(t)]|^2] &= E[|s(t) - E[s(t)]|^2] + E[|n(t)|^2] \\
&= \sigma_s^2 + N_0, \\
H_1: \quad E[|r(t) - E[r(t)]|^2] &= E[|s(t) - E[s(t)]|^2] + E[|n(t)|^2] + E[|J(t)|^2] \\
&= \sigma_s^2 + N_0 + N_J,
\end{aligned}
\tag{2.43}
$$

where σ_s^2 is the variance of message signals.

Based on (2.43), a simple decision rule can be obtained:

$$
\frac{1}{K}\sum_{k=1}^{K}|r_k - \frac{1}{K}\sum_{k=1}^{K} r_k|^2 \underset{H_0}{\overset{H_1}{\gtrless}} \lambda \tag{2.44}
$$

Taking channel fading effects (slow-varying) into consideration, we stack N samples of the received signal into a column vector $\underline{r}$,

$$
\begin{aligned}
H_0: \quad \underline{r} &= H\underline{s} + \underline{n}, \\
H_1: \quad \underline{r} &= H\underline{s} + \underline{n} + \underline{J},
\end{aligned}
\tag{2.45}
$$

where $\underline{s}$, $\underline{n}$ and $\underline{\mathrm{J}}$ are N-sample column vectors corresponding to data, noise and jamming, respectively, and H is channel convolution matrix. The covariance matrices of $\underline{r}$ under H_0 and H_1 are given as follows:

$$
\begin{aligned}
H_0: \quad E[(\underline{r} - E[\underline{r}])(\underline{r} - E[\underline{r}])^{\mathcal{H}}] &= \sigma_s^2 HH^{\mathcal{H}} + N_0 I, \\
H_1: \quad E[(\underline{r} - E[\underline{r}])(\underline{r} - E[\underline{r}])^{\mathcal{H}}] &= \sigma_s^2 HH^{\mathcal{H}} + N_0 I + N_J I,
\end{aligned}
\tag{2.46}
$$

where $\mathcal{H}$ denotes Hermitian transpose, and I represents an $(N \times N)$ identity matrix.

Note that the discriminant between H_0 and H_1 only exists on the main diagonal of $E[(\underline{r} - E[\underline{r}])(\underline{r} - E[\underline{r}])^{\mathcal{H}}]$. Consequently, we can calculate the covariance matrix of the received signal vectors, and then take the average of all the entries on the main diagonal. If the average value is greater than a threshold, then H_0 is rejected, and vice versa.

2.6.2 Jamming Detection in DS-CDMA Systems

Since signals in CDMA systems are characterized by low power spectrum density, jamming detection in frequency domain is more suitable for DS-CDMA systems.

Without Self-Jamming Cancellation

The amplitude of the normal power at all the frequency components of $r(t)$ under H_0 is first derived, where no significant difference in strength among all the frequency components should be detected. Then for the received signal r(t), the power spectrum can be estimated via the magnitude squared of the FFT of the windowed signal [71]. If there is one frequency component with an unusually high amplitude in the estimate of power spectral density, it is most likely that this frequency is jammed and should be excised or interpolated.

With Self-Jamming Cancellation

To further improve the accuracy of jamming detection, the self-jamming cancellation technique should be exploited.

Since the base station has the knowledge of all users' spreading codes and training symbols, the following procedures can be carried out to cancel the influence of self-jamming:

1. Estimate all the multipath channels using high-power pilot symbols.

2. Eliminate the self-jamming term from the received signal $r(t)$. The remaining signal is equivalent to the signal received from an AWGN channel.

3. Determine whether or not hostile jamming occurs in the remaining signal.

2.7 Simulation Results

In the simulation, a CDMA system with spreading factor 16 is considered. The binary spreading codes are randomly generated. BPSK modulation is adopted. JSR is defined as the ratio of the total jamming power to the average signal power, while SNR is defined as the ratio of the average signal power to the noise power.

2.7.1 Examples on Jamming Detection

Assume that BPSK signals are transmitted over an AWGN channel. Self-jamming is ignored, for the time being. The jammer uniformly distributes its available power over the randomly-chosen frequency band. At the receiver end, hostile jamming is informed if the unusually high amplitudes of frequency components are discovered beyond a certain threshold.

There are basically two types of detection errors: probability of miss and probability of false alarm. If no jamming is detected when the jammer is actually working, then miss detection happens. On the contrary, if the receiver determines that frequency band is being occupied by the hostile jamming signal when the jammer is actually off, the false alarm arises.

Figure 2.2 shows the performance of jamming detection with respect to different levels of JSR. According to the definition, probability of false alarm is not related

to JSR, but dependent upon SNR. Thresholds with regard to different SNRs are determined in a way that the probability of false alarm is approximately 0.04. As can be seen, it is more likely that jamming can be exhaustively detected as the total jamming power is increased. Moreover, the noise strength on the channel will affect the performance of jamming detection. Given a fixed amount of jamming power, if the noise power is large enough to make a significant contribution on the receiver's power spectral density, then the threshold must be high enough to achieve a small probability of false alarm, which consequently leads to a big chance that the receiver will fail to detect the existence of jamming, that is, a *miss* is most likely to occur.

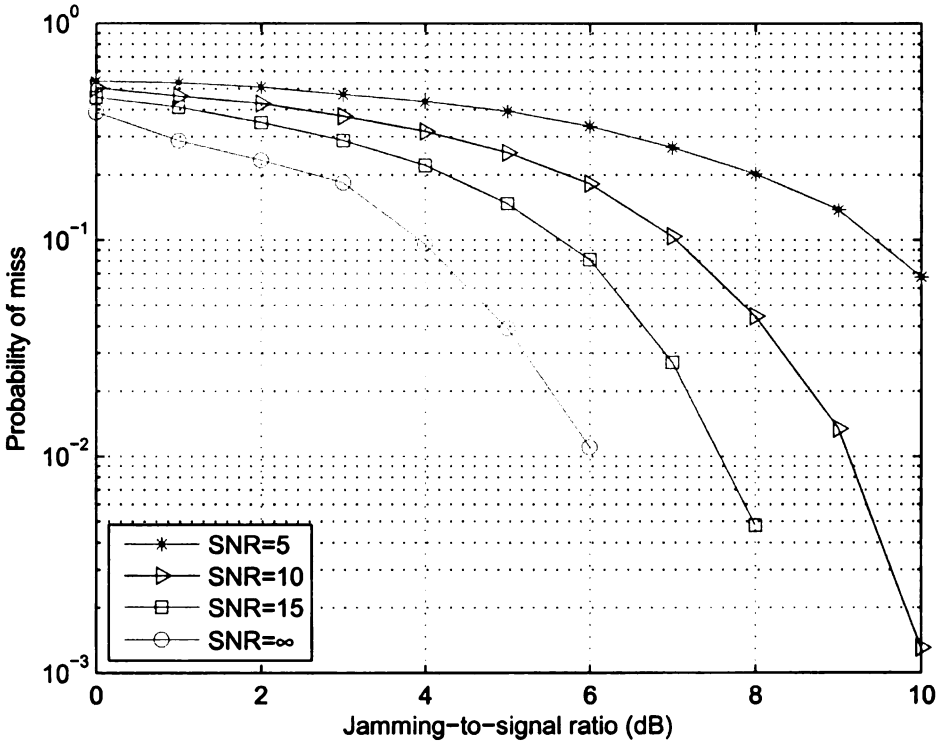


Figure 2.2. Probability of miss versus JSR (here the probability of false alarm ≈ 0.04).

2.7.2 Examples on Jamming Classification

In this example, a four-user CDMA system with random spreading codes of length 16 is considered, where message signals are sent over frequency-selective fading channels.

Denote full-band jamming strategy by S_1, partial-band jamming by S_2, partial-time jamming by S_3, and no jamming by S_4. Assume that the jammer randomly applies one of four strategies to interfere with normal data traffic of CDMA systems in each trial. If partial-time or partial-band jamming is adopted, ρ_t (or ρ_f) is randomly chosen within [0.2, 0.8]. In the simulation, the proposed binary decision tree is tested for different jamming power level by adjusting JSR from 0dB to 10dB while keeping the SNR level fixed. There are totally 10000 Monte Carlo runs for each JSR level.

A typical classification confusion matrix without consideration of self-jamming is provided in Table 2.1(a), while identification results after self-jamming elimination are given in Table 2.1(b), under the same JSR and SNR levels. The entry in the ith row and jth column of the matrix represents the number of classifications that S_j is identified when S_i is actually applied. Clearly, only the entries on the main diagonal of the confusion matrices are accurate classifications. Different thresholds are adopted in two scenarios. It can be observed that self-jamming in CDMA systems significantly affects the accuracy of classification. When the JSR is medium (e.g., 4dB), it is most likely that the power of jamming signals is not sufficiently high to ensure itself distinguishable from self-jamming, even if different thresholds are attempted. After the interference cancellation technique is applied to eliminate self-jamming, the accuracy of detection on hostile jamming is dramatically improved. Table 2.1(b) gives 100% accuracy of identification of jamming patterns by utilizing the proposed classification approach.

Figure 2.3 shows the significant improvement in the estimation accuracy of jam-

Table 2.1. Classification confusion matrices: JSR = 4dB, SNR = 3dB.

(a) Without self-jamming cancellation

Actual \ *Recognized*	S_1	S_2	S_3	S_4
S_1	1140	0	0	1342
S_2	923	515	0	1154
S_3	599	0	954	903
S_4	0	0	0	2470

(b) With self-jamming cancellation

Actual \ *Recognized*	S_1	S_2	S_3	S_4
S_1	2482	0	0	0
S_2	0	2592	0	0
S_3	0	0	2456	0
S_4	0	0	0	2470

ming bandwidth by exploiting self-jamming cancellation techniques. On the other hand, the error rate for estimation of ρ_f in the case without self-jamming elimination vanishes with a steep gradient as long as the JSR is greater than 7dB, which, from another point of view, illustrates the effectiveness of the decision tree classification.

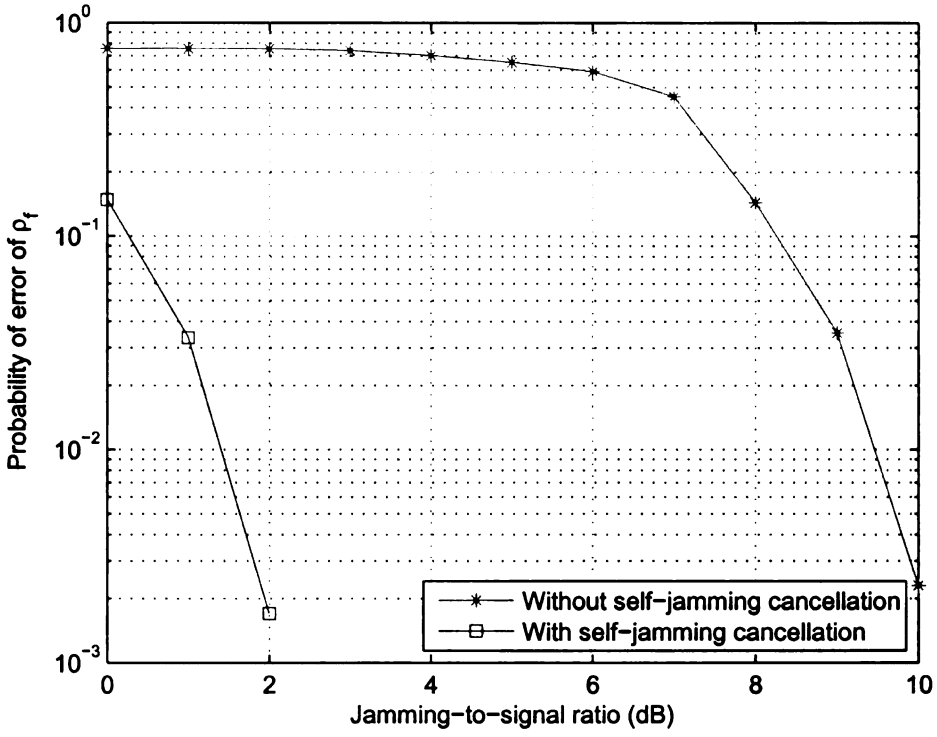


Figure 2.3. Probability of error in estimating ρ_f versus JSR.

2.8 Summary

In this chapter, we focused on modeling and detection of hostile jamming for wireless systems, particularly, for spread spectrum systems. A general two-dimensional jamming generation model was introduced, including all the existing models as special cases. The impact of hostile jamming in both frequency hopping and DS-CDMA systems was investigated. In addition, self-jamming effect was studied for uplink and downlink CDMA systems. It was shown that interference cancellation techniques could be exploited to eliminate self-jamming to further increase the accuracy of hostile jamming detection. Targeted at spread spectrum systems, jamming classification frameworks were presented, and both training-based and blind jamming detection methods were developed. The effectiveness of the proposed approaches was demonstrated by our simulation results.

CHAPTER 3

Spectrally Efficient Anti-Jamming System Design for Wireless Networks

In this chapter, we introduce two novel concepts on spectrally-efficient anti-jamming system design: message-driven frequency hopping (MDFH) and collision-free frequency hopping (CFFH). Unlike in traditional FH where the hopping pattern of each user is determined by a pre-selected pseudo-random (PN) sequence, in MDFH, part of the message stream will be acting as the PN sequence, and transmitted through hopping frequency control. As a result, system efficiency is increased significantly since additional information transmission is achieved at no extra cost on either bandwidth or power. From the security point of view, information confidentiality is reinforced since the hopping pattern is message-driven, hence totally unpredictable. In CFFH, based on the OFDM framework and the secure subcarrier assignment algorithm, the proposed CFFH system can achieve high information capacity through collision-free multiple access. At the same time, as each user still transmits through a pseudo-random frequency hopping scheme, CFFH can maintain the inherent anti-jamming, anti-interception security features of the conventional FH system. The pro-

posed schemes can be used for both civilian and military applications where secure high speed information transmission is needed.

3.1 Introduction

As one of the two basic modulation techniques used in spread spectrum communications [64], frequency hopping technique was originally designed to be inherently secure and reliable under adverse battle conditions for military purpose. In traditional FH systems, the transmitter "hops" in a pseudo-random manner among available frequencies according to a pre-specified algorithm, the receiver then operates in exact synchronization with the transmitter and remains tuned to the same center frequency.

Based on the hop duration period, FH systems can be further divided into two categories: fast hopping (FFH) scheme and slow hopping (SFH) scheme. In an FFH system, the carrier hops several times during one symbol period, while in an SFH system, each hop lasts at least one symbol period. Since different bands are unlikely to experience simultaneous fading, FH systems are robust against fast fading. At the same time, pseudo-random frequency hopping during radio transmission minimizes the possibility of hostile jamming and unauthorized interception.

In 1978, Cooper and Nettleton [72] first proposed a frequency hopping multiple access (FHMA) system with DPSK (Differential Phase-Shift Keying) for mobile communication applications. Later in the same year, Viterbi [73] initiated the use of MFSK (M-ary Frequency-Shift Keying) for low-rate multiple access mobile satellite systems. Since MFSK modulation enables non-coherent detection, it has been widely adopted in FHMA systems [74–77]. There are two major limitations with the conventional FH systems: (i) *Strong requirement on frequency acquisition.* In existing

FH systems, exact frequency synchronization has to be kept between transmitter and receiver. The strict requirement on synchronization directly influences the complexity and performance of the system [78], and turns out to be a significant challenge in fast hopping system design. (ii) *Low spectral efficiency over large bandwidth.* Typically, FH systems require large bandwidth, which is proportional to the product of the hopping rate and the number of all the available channels. In conventional FHMA, each user hops independently based on its own PN sequence, a collision occurs whenever there are two users transmit in the same frequency band. Mainly limited by the collision effect, the spectral efficiency of conventional FH systems is very low due to inefficient use of the large bandwidth. In the literature, considerable efforts have been devoted to increasing the spectral efficiency of FH systems by applying high-dimensional modulation schemes [37–43]. However, existing work is far from adequate to address the ever increasing demand on inherently secure high speed wireless communication.

In this chapter, we propose an innovative message-driven frequency hopping scheme. The basic idea is that part of the message will be acting as the PN sequence for carrier frequency selection at the transmitter. In other words, selection of carrier frequencies is directly controlled by the (encrypted) message stream rather than by a predetermined pseudo-random sequence as in the conventional FH systems. At the receiver, the transmitting frequency is captured using a filter bank as in the FSK receiver rather than using the frequency synthesizer. Therefore, the carrier frequency (hence the information embedded in frequency selection) can be blindly detected at each hop, and thus largely relaxes the burden of strict frequency synchronization at the receiver. More importantly, by embedding a large portion of information into the hopping selection process, additional information transmission is achieved with no extra cost on bandwidth or power. Therefore, the system spectral efficiency is signif-

icantly improved. In addition, MDFH makes it possible for faster frequency hopping in wideband systems. From the security point of view, it also reinforces the jamming resistance of the FH system since the message-driven hopping pattern is totally unpredictable.

To further increase spectral efficiency, an enhanced version of MDFH, named E-MDFH, is proposed by enabling simultaneous transmissions on multiple channels at each hop. This enhanced transmission scheme provides better design flexibility, and much higher spectral efficiency through a careful design of the hopping frequency selection process. It turns out that E-MDFH contains both MDFH and OFDM as special cases, and can readily be extended to a collision-free multiple access FH system through user multiplexing. Furthermore, quantitative performance analysis on both bit-error-rate and spectral efficiency is conducted based on theoretical derivation, as well as simulation examples. Our analysis demonstrates that: transmission of information through hopping frequency control essentially adds another dimension to the signal space, and the resulting coding gain can increase the spectral efficiency by *multiple* times.

Motivated by the advantages observed in E-MDFH which allows simultaneous transmissions over multiple frequency bands at each hop, a highly efficient secure communication interface – the collision-free frequency hopping system is developed. The major features of the CFFH scheme can be summarized as follows. First, CFFH is highly spectrally efficient because it is collision-free and makes full use of the available spectrum. Moreover, the spectral efficiency of CFFH is enhanced by the OFDM framework. OFDM allows frequency overlapping between subcarriers which are orthogonal to each other, and hence is much more efficient than the conventional FH system where guard band is needed between neighboring channels. Secondly, since OFDM is

implemented through FFT, CFFH can relax the complex frequency synchronization problem suffered by conventional FH systems. Thirdly, a dynamic subcarrier assignment algorithm is designed for the CFFH scheme. Ensured by AES, CFFH maintains the inherent anti-jamming security feature of conventional FH systems. Furthermore, in multiple access environment, anonymous multiparty communication can be achieved by sending dummy bits on certain subcarriers and hence can prevent traffic analysis by the hostile party.

The rest of the chapter is organized as follows. Section 3.2 describes major limitations of the conventional FH system. In Section 3.3, the concept of MDFH scheme is introduced, and then extended to efficiency enhanced MDFH. Quantitative performance analysis on BER and spectral efficiency is presented to demonstrate the superior bandwidth efficiency of MDFH. Section 3.4 is focused on the CFFH scheme. The signal transmission scheme and detection procedures are described, followed by an AES based secure subcarrier assignment algorithm. Performance analysis and simulation examples are provided to illustrate the advantages of CFFH. We conclude in Section 3.5.

3.2 Challenges in the Transceiver Design of Frequency Hopping Systems

The block diagram of a traditional FH system is shown in Figure 3.1. A main limitation with this design structure is the strong requirement on PN acquisition, as exact frequency synchronization has to be kept between transmitter and receiver. The strict requirement on synchronization directly influences the complexity and performance of the system. Slow hopping systems, therefore, have been popular because of their

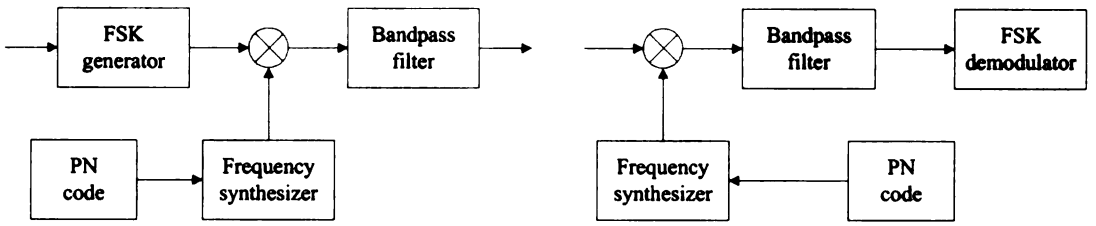


Figure 3.1. Block diagram of the conventional frequency hopping scheme.

relaxed synchronization requirement. On the other hand, due to their resistance to hostile jamming and interception, fast hopping systems are highly desired in classified information transmission. This raises a big challenge in transmitter-receiver design.

In addition, traditional frequency hopping systems are also being challenged to transport more information with little or no increase in allocated bandwidth. Along with rapid development of high-speed multimedia information transmission, spectrum has become the most precious resource in wireless communications, since the total available spectrum has to be shared by all wireless services. FSK generator in Figure 3.1 is generally realized by MFSK modulation. In order to maintain the orthogonality among carrier frequencies in SFH, the transmitted tones must be spaced at a separation equivalent to the baud rate (or the hop rate in FFH), or a multiple of the baud rate, otherwise it is difficult to separate one tone from another. Therefore, the constellation size M cannot be too large to support high speed communication, considering the stringent restriction of the total bandwidth.

Meeting these challenges, i.e., strict synchronization requirement and low spectral efficiency, calls for advanced signaling techniques.

3.3 Message-Driven Frequency Hopping

In this section, we introduce the concept of message-driven frequency hopping. The basic idea is that part of the message stream will be acting as the PN sequence for carrier frequency selection. Spectral efficiency of MDFH can be further enhanced by allowing simultaneous transmissions over multiple frequency bands at each hop. Including both MDFH and OFDM as special cases, the enhanced MDFH scheme, named E-MDFH, can achieve higher spectral efficiency while providing excellent design flexibility, and can readily be extended to a FH-based collision-free multiple access scheme. Our quantitative analysis on bit-error-rate and spectral efficiency indicates that: transmission of information through hopping frequency control essentially introduces another dimension to the signal space, and the corresponding coding gain increases system efficiency by multiple times.

3.3.1 Transmitter Design

Let N_c be the total number of available channels, with $\{f_1, f_2, \cdots, f_{N_c}\}$ being the set of all available carrier frequencies. Ideally all the available channels should be involved in the hop selection process, as is required by current frequency hopping specifications (e.g., Bluetooth). The number of bits required to specify each individual channel is $B_c = \lfloor \log_2 N_c \rfloor$, where $\lfloor x \rfloor$ denotes that largest integer less than or equal to x. If N_c is a power of 2, then there exists a 1-1 map between the B_c-bit strings and the available channels. Otherwise, when N_c is not a power of 2, we will allow some B_c-bit strings to be mapped to more than one channels. More specifically, for $i = 1, \cdots, N_c$, the ith channel will be associated with the binary representation of the modulated channel index, $[(i-1) \mod 2^{B_c}] + 1$. In the following, for simplicity of notation, we assume

that $N_c = 2^{B_c}$.

Let Ω be the selected constellation that contains M symbols, then each symbol in the constellation represents $B_s = \log_2 M$ bits. Let T_s and T_h denote the symbol period and the hop duration, respectively, then the number of hops per symbol period is given by $N_h \triangleq T_s/T_h$. We assume that N_h is an integer larger or equal to 1. In other words, we focus on fast hopping systems.

We start by dividing the data stream into blocks of length $L \triangleq N_h B_c + B_s$. Each block consists of $N_h B_c$ *carrier bits* and B_s *ordinary bits*. The carrier bits are used to determine the hopping frequencies, and the ordinary bits are mapped to a symbol which is transmitted through the selected N_h channels successively. Note that the number of the carrier bits is determined by B_c (the number of bits used to specify one hopping frequency) and N_h (the number of hops within one symbol period). The number of ordinary bits is exactly the number of bits represented by one individual symbol in constellation Ω. Denote the nth block by X_n, we intend to transmit X_n within one symbol period. The carrier bits in block X_n are further grouped into N_h vectors of length B_c, denoted by $[X_{n,1}, \cdots, X_{n,N_h}]$. The bit vector composed of B_s ordinary bits is denoted by Y_n, as shown in Figure 3.2.

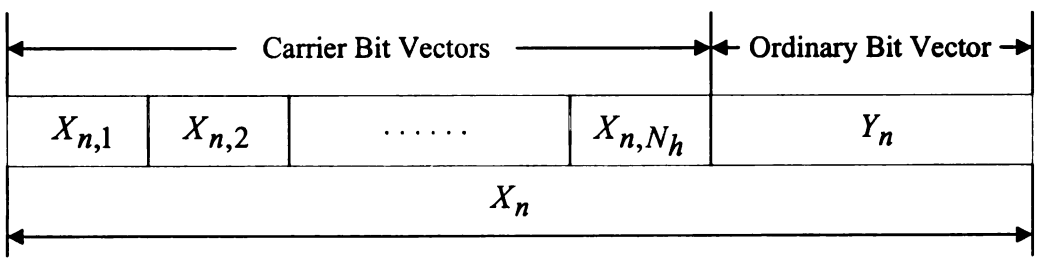


Figure 3.2. The nth block of the information data.

The transmitter block diagram of the proposed MDFH scheme is illustrated in Figure 3.3. Each input data block, X_n, is fed into a serial-to-parallel (S/P) con-

verter, where the carrier bits and the ordinary bits are split into two parallel data streams. The selected carrier frequencies corresponding to the nth block are denoted by $\{f_{n,1}, \cdots, f_{n,N_h}\}$, where each $f_{n,i} \in \{f_1, f_2, \cdots, f_{N_c}\}, \forall i \in [1, N_h]$. Assume Y_n is mapped to symbol A_n, and the corresponding baseband signal is denoted as $m(t)$.

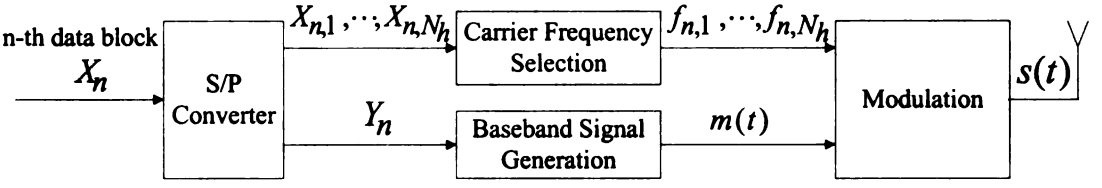


Figure 3.3. Transmitter structure of MDFH.

If pulse amplitude modulation (PAM) is adopted for baseband signal generation, then

$$m(t) = \sum_{n=-\infty}^{\infty} \sum_{i=1}^{N_h} A_n \, g(t - nT_s - (i-1)T_h), \tag{3.1}$$

where $g(t)$ is the pulse-shaping filter. Define $m_{n,i}(t) \triangleq A_n \, g(t - nT_s - (i-1)T_h)$, then $m(t) = \sum_{n=-\infty}^{\infty} \sum_{i=1}^{N_h} m_{n,i}(t)$. The corresponding passband waveform can be obtained as:

$$s(t) = \sqrt{\frac{2}{T_h}} Re\{ \sum_{n=-\infty}^{\infty} \sum_{i=1}^{N_h} m_{n,i}(t) e^{j2\pi f_{n,i} t} \chi_{n,i}(t)\}, \tag{3.2}$$

where

$$\chi_{n,i}(t) = \begin{cases} 1, & t \in [nT_s + (i-1)T_h, nT_s + iT_h], \\ 0, & \text{otherwise.} \end{cases} \tag{3.3}$$

If MFSK is utilized for baseband modulation, then

$$s(t) = \sqrt{\frac{2}{T_h}} \sum_{n=-\infty}^{\infty} \sum_{i=1}^{N_h} cos2\pi [f_{n,i} t + K_f \int_{-\infty}^{t} m_{n,i}(\tau) d\tau] \chi_{n,i}(t). \tag{3.4}$$

where K_f is a preselected constant.

Discussions on Bandwidth Requirement

As is well known, FM requires much larger bandwidth than PAM. Here, we will focus on PAM based FH systems. In equation (3.2), let $s_{n,i}(t) \triangleq [m_{n,i} \cos 2\pi f_{n,i} t]\chi_{n,i}(t)$. By definition, the bandwidth of $s_{n,i}(t)$ is determined by the spectrum of $g(t-nT_s-(i-1)T_h)\chi_{n,i}(t)$, which is given by the convolution $\mathcal{F}(g(t-nT_s-(i-1)T_h)) * \mathcal{F}(\chi_{n,i}(t))$, where $\mathcal{F}(x)$ denotes the Fourier transform of x. If the bandwidth of $g(t)$ is BW_g Hz, then the bandwidth of $g(t-nT_s-(i-1)T_h)\chi_{n,i}(t)$ is $BW_g + \frac{1}{T_h}$. Therefore, in general, the total channel bandwidth in order to avoid inter-carrier interference (ICI) in the FH case will be $2N_c(BW_g + \frac{1}{T_h})$.

In the particular case when $g(t)$ is a rectangular pulse, then $s_{n,i}(t) = m_{n,i}(t) \cos 2\pi f_{n,i} t$. Note that $|\mathcal{F}(\chi_{n,i}(t))| = T_h|sinc(\pi T_h f)|$, that is, when $f = \pm\frac{k}{T_h}$, $k \in Z^+$, $|\mathcal{F}(\chi_{n,i}(t))| = 0$. This implies that if carrier frequencies in the FH system are separated by integer times of $\frac{1}{T_h}$, there is no ICI between the carriers. Therefore, in this case, the minimum bandwidth requirement is $\frac{N_c+1}{T_h}$, and the $s(t)$ in (3.2) essentially reduces to an OFDM signal.

3.3.2 Receiver Design

The structure of the receiver is shown in Figure 3.4. Recall that $\{f_1, f_2, \cdots, f_{N_c}\}$ is the set of all available carrier frequencies. To detect the active frequency band, a bank of N_c bandpass filters (BPFs), each centered at f_i $(i = 1, 2, \cdots, N_c)$, and with the same channel bandwidth as the transmitter, are deployed at the front end. Since only one frequency band is occupied at any given moment, we simply measure the outputs of bandpass filters at each possible signaling frequency. The actual carrier frequency

at a certain hopping period can be detected by selecting the one that captures the strongest signal. As a result, blind detection of the carrier frequency is achieved at the receiver.

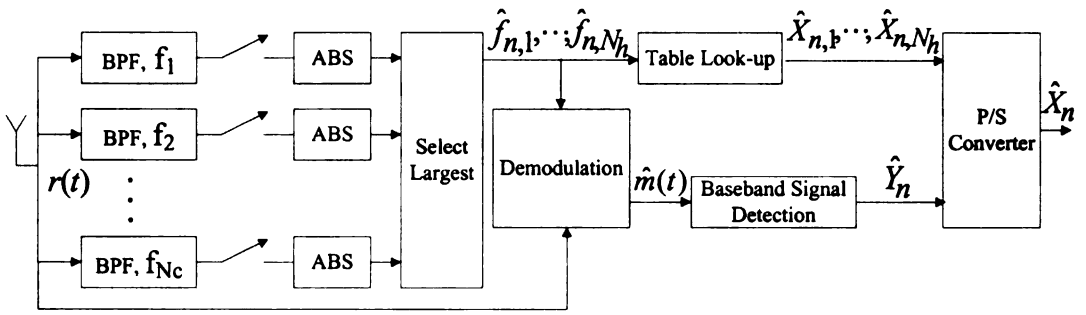


Figure 3.4. Receiver structure of MDFH, here ABS means taking the absolute value.

More specifically, the received signal can be written as

$$r(t) = h(t) * s(t) + w(t), \tag{3.5}$$

where $*$ stands for convolution, $h(t)$ is the channel impulse response, and $w(t)$ denotes the additive white Gaussian noise. Accordingly, the outputs of bandpass filters are given by

$$z_i(t) = q_i(t) * r(t), \quad \text{for } i = 1, \cdots, N_c, \tag{3.6}$$

where $q_i(t)$ is the ideal bandpass filter centered at frequency f_i, $i = 1, 2, \cdots, N_c$.

If the channel is ideal, i.e., $h(t) = \delta(t)$, then

$$z_i(t) = q_i(t) * s(t) + u_i(t), \quad \text{for } i = 1, \cdots, N_c, \tag{3.7}$$

where $u_i(t) = q_i(t) * w(t)$ is the filtered version of the noise. If the signal-to-noise ratio is sufficiently high, as in most useful communication systems, there is one and only

one significantly strong signal among the outputs of the filter bank. Suppose the lth filter captures this distinctive signal during the ith hop of the nth block, then we have $\hat{f}_{n,i} = l$. The same procedures can be carried out to determine the carrier frequency at each hop.

Next, the estimated hopping frequencies $\{\hat{f}_{n,1}, \cdots, \hat{f}_{n,N_h}\}$ are used to extract the input signal. On one hand, $\{\hat{f}_{n,1}, \cdots, \hat{f}_{n,N_h}\}$ are mapped back to B_c-bit strings to recover the carrier bits. We denote the estimated carrier bit-vectors as $\{\hat{X}_{n,1}, \cdots, \hat{X}_{n,N_h}\}$. On the other hand, the ordinary bit-vector, Y_n, is first estimated independently for each hop, then bit-wise majority voting is applied for all the N_h estimates to make the final decision on each ordinary bit in Y_n. We denote the estimated ordinary bit-vector as $\hat{Y}_n$. It then follows that the estimate of the nth block X_n can be obtained as: $\hat{X}_n = [\hat{X}_{n,1}, \cdots, \hat{X}_{n,N_h}, \hat{Y}_n]$.

Remark 3.1 *Unlike the conventional FH scheme for which the receiver can be designed through a single frequency tunable filter, the receiver that we use in MDFH is a filter bank consisting of bandpass filters, which is similar to the filter bank used for non-coherent detection of FSK signals. In fact, it can be implemented by paralleling several FSK receivers. Along with advances in large scale circuit integration and fabrication, this receiver design is both feasible and practical. It is interesting to note that in [79], the message is used to select the spreading code in CDMA and therefore increases the system capacity.* □

Remark 3.2 *Design of the MDFH receiver leads to a security observation: if such a filter bank is available to a malicious user, then both the conventional FH signals and the MDFH signals can largely be intercepted by an unauthorized party. This implies that to prevent unauthorized interception, information has to be encrypted before being transmitted over an FH system.* □

Remark 3.3 *One important feature of FH systems is jamming resistance. In MDFH, as the hopping frequency is determined by the encrypted message signal, the hopping pattern is more unpredictable than that in the conventional FH, which is determined by a pre-selected PN sequence. From this point of view, we can see that: while achieving higher spectral efficiency by embedding bits into the hopping frequency selection process, MDFH also has better or at least comparable jamming resistance with the conventional FH.* □

3.3.3 Efficiency Enhanced MDFH

To further improve spectral efficiency and design flexibility, we refine the transceiver design of the MDFH system by allowing simultaneous transmissions over multiple frequency bands. The modified scheme is referred to as enhanced MDFH (E-MDFH).

The Modified Hopping Frequency Selection Process

Recall that $N_c = 2^{B_c}$ is the number of all available carriers. We split the N_c carriers into N_g non-overlapping groups $\{C_l\}_{l=1}^{N_g}$, with $N_g = 2^{B_g}$, then each group has $N_f \triangleq N_c/N_g = 2^{B_c - B_g}$ carriers. Specifically, $C_1 = \{f_1, \cdots, f_{N_f}\}, C_2 = \{f_{N_f+1}, \cdots, f_{2N_f}\}, \cdots, C_{N_g} = \{f_{N_c-N_f+1}, \cdots, f_{N_c}\}$. Now we consider to modify the transmitter design in MDFH, such that simultaneous transmissions over multiple frequency bands can be achieved at each hop. An intuitive method is to employ an independent MDFH scheme within each C_l for $l = 1, \cdots, N_g$, referred to as FD-MDFH. In this case, the frequency hopping process is limited to N_f ($<< N_c$) successive carriers, leading to insufficient randomness and therefore inadequate jamming resistance.

To maximize the randomness, here we present an alternative approach. We divide the incoming data stream into blocks of length $[N_h(B_c - B_g) + B_s]N_g$. Denote the

nth block by X_n. X_n is further divided into N_g vectors: $X_n = [Z_{n,1}, \cdots, Z_{n,N_g}]$. For $m = 1, \cdots, N_g$, each $Z_{n,m}$ contains $N_h(B_c - B_g) + B_s$ bits. Write $Z_{n,m} = [D^1_{n,m}, \cdots, D^{N_h}_{n,m}, Y_{n,m}]$, where each $D^i_{n,m}$ is a bit-vector consisting of $(B_c - B_g)$ carrier bits, and bit-vector $Y_{n,m}$ consists of B_s ordinary bits. We adopt the notation "bin2dec" (used in Matlab) to denote the operation of converting a binary vector to a decimal number, and "dec2bin" the reverse operation. For $m = 1, \cdots, N_g, i = 1, \cdots, N_h$, we define $d^i_{n,m} \triangleq \text{bin2dec}(D^i_{n,m}) + 1$.

Recall that there are N_h hops in one symbol period, at each hop, the signal will be transmitted through N_g carriers simultaneously. For $i = 1, \cdots, N_h$, the frequency index for the mth carrier at the ith hop is defined as:

$$\begin{aligned} I^i_{n,1} &= d^i_{n,1}, && \text{when } m = 1 \\ I^i_{n,m} &= I^i_{n,m-1} + d^i_{n,m}, && \text{when } m = 2, \cdots, N_g. \end{aligned} \tag{3.8}$$

This carrier selection procedure is designed to ensure that: (i) All the available carriers are involved in the hopping selection process; (ii) The hopping frequencies have no collisions with each other at any given moment. In fact, at each hop,

$$I^i_{n,1} < I^i_{n,2} < \cdots < I^i_{n,N_g}, \tag{3.9}$$

since $I^i_{n,1} \in [1, N_f], I^i_{n,2} \in [I^i_{n,1} + 1, 2N_f], \cdots, I^i_{n,N_g} \in [I^i_{n,N_g-1} + 1, N_c]$. After the hopping frequencies are determined for all the N_g carriers, each $Y_{n,m}$ $(m = 1, \cdots, N_g)$ is mapped into a symbol in constellation Ω and then transmitted through the mth carrier, which hops through frequencies $f_{I^1_{n,m}}, \cdots, f_{I^{N_h}_{n,m}}$. As the result, X_n is now transmitted in one symbol period through simultaneous multicarrier transmission under the message-driven frequency hopping framework.

Signal Detection

As in MDFH, the receiver in E-MDFH also consists of a bank of N_c bandpass filters. However, the signal detection procedure needs to be modified. Take the extraction of X_n as an example. At the ith hop, instead of searching for the bandpass filter which captures the strongest output in MDFH, we now identify N_g filters which deliver the largest N_g outputs. According to equation (3.9), the indices of these N_g bandpass filters are sorted in ascending order, to obtain the estimated indices for $I^i_{n,m}$, that is, $\hat{I}^i_{n,1} < \hat{I}^i_{n,2} < \cdots < \hat{I}^i_{n,N_g}$. Now the carrier-bit vectors can be estimated as:

$$\begin{aligned} \hat{D}^i_{n,1} &= \text{dec2bin}(\hat{I}^i_{n,1} - 1), && \text{when } m = 1 \\ \hat{D}^i_{n,m} &= \text{dec2bin}(\hat{I}^i_{n,m} - \hat{I}^i_{n,m-1} - 1), && \text{when } m = 2, \cdots, N_g. \end{aligned} \tag{3.10}$$

At the same time, each ordinary bit-vector $Y_{n,m}$ is estimated from the received signal corresponding to the mth carrier based on bit-wise majority voting, similar to that in MDFH.

Remark 3.4 *Taking the carrier usage into consideration, the modified design structure includes both MDFH and OFDM as special cases. In fact, if $N_g = 1$, then E-MDFH is reduced to MDFH. Likewise, if $N_g = N_c$, then E-MDFH can readily be implemented through an OFDM system. The advantage of E-MDFH is two-fold. First, E-MDFH improves the design flexibility in the sense the transmission scheme can be easily adjusted by tuning the values of B_g or N_g. Second, E-MDFH can achieve much higher spectral efficiency than MDFH. Unlike MDFH which occupies only one carrier at a time, E-MDFH makes better use of the available spectrum by allowing simultaneous transmissions over multiple channels.* □

3.3.4 Collision-Free MDFH in Multiple Access Environment

Collisions in Conventional FHMA systems

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

If there are N_c available channels and N_u active users (i.e., $N_u - 1$ possible interfering users), assuming that all N_c channels are equally probable and all users are independent, then the probability that a collision occurs is given by

$$P_h = 1 - (1 - \frac{1}{N_c})^{N_u - 1} \tag{3.11}$$

$$\approx \frac{N_u - 1}{N_c} \quad \text{when } N_c \text{ is large.} \tag{3.12}$$

Taking $N_c = 64$ as an example, the relationship between the probability of collision and the number of active users is shown in Figure 3.5. The high collision probability severely limits the number of users that can be simultaneously supported by an FH system. Assuming BFSK modulation and $N_h = 1$, if two users are not transmitting simultaneously through the same frequency band, then the probability of bit error is $P_e = \frac{1}{2}e^{-\frac{E_b}{2N_o}}$ where $\frac{E_b}{N_o}$ is the bit-level signal-to-noise ratio (SNR). If two users transmit simultaneously in the same frequency band, then the probability of bit error is generally assumed to be $\frac{1}{2}$. The overall probability of bit error can thus be modeled as

$$P_e = \frac{1}{2}e^{-\frac{E_b}{2N_o}}(1 - p_h) + \frac{1}{2}p_h. \tag{3.13}$$

It follows from equation (3.13) that there exists an error floor (i.e., $\frac{1}{2}p_h$) for the conven-

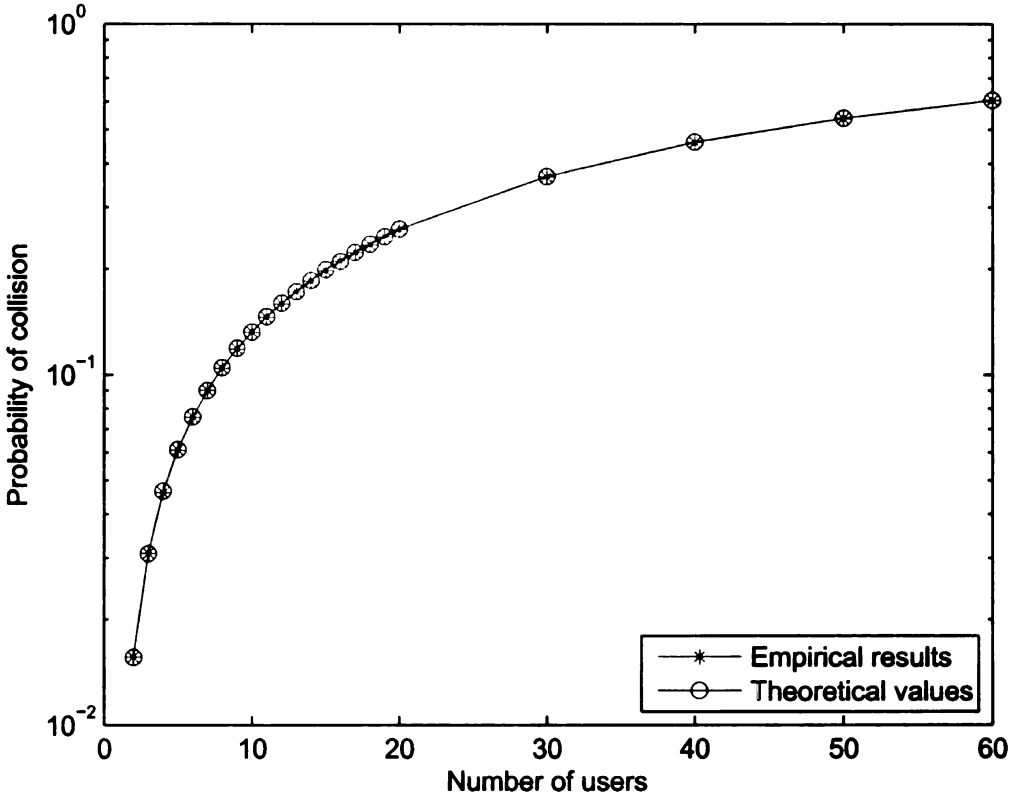


Figure 3.5. Probability of collision (P_h) versus the number of users (starting at the two-user case) for $N_c = 64$.

tional FHMA systems. Our discussions above indicate that an alternative approach is to develop collision-free FHMA techniques.

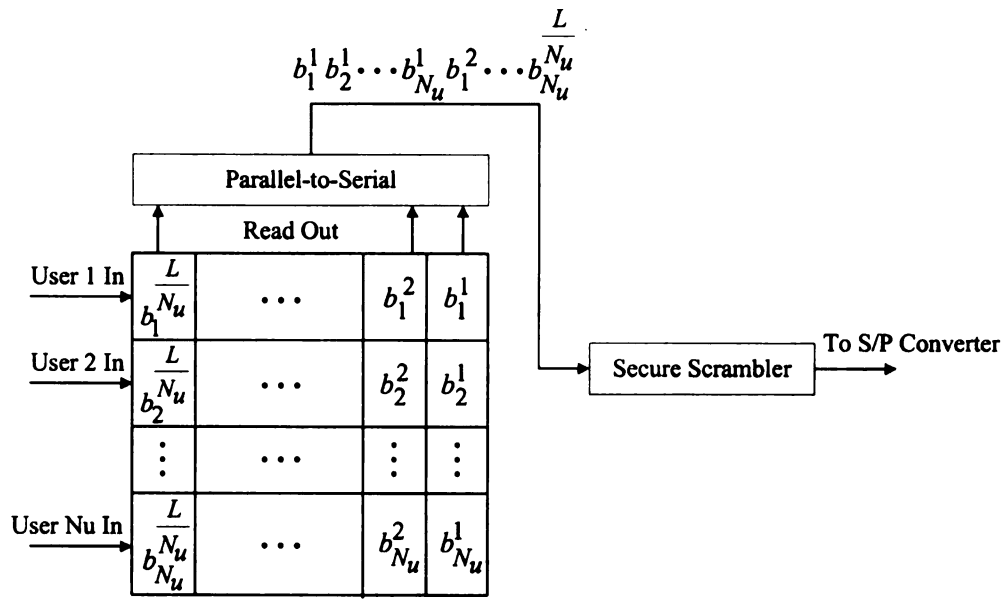
Proposed collision-free MDFH

The E-MDFH system can readily be extended to a **collision-free MDFH** scheme to accommodate more users in the multiple access environment, denoted as CF-MDFH.

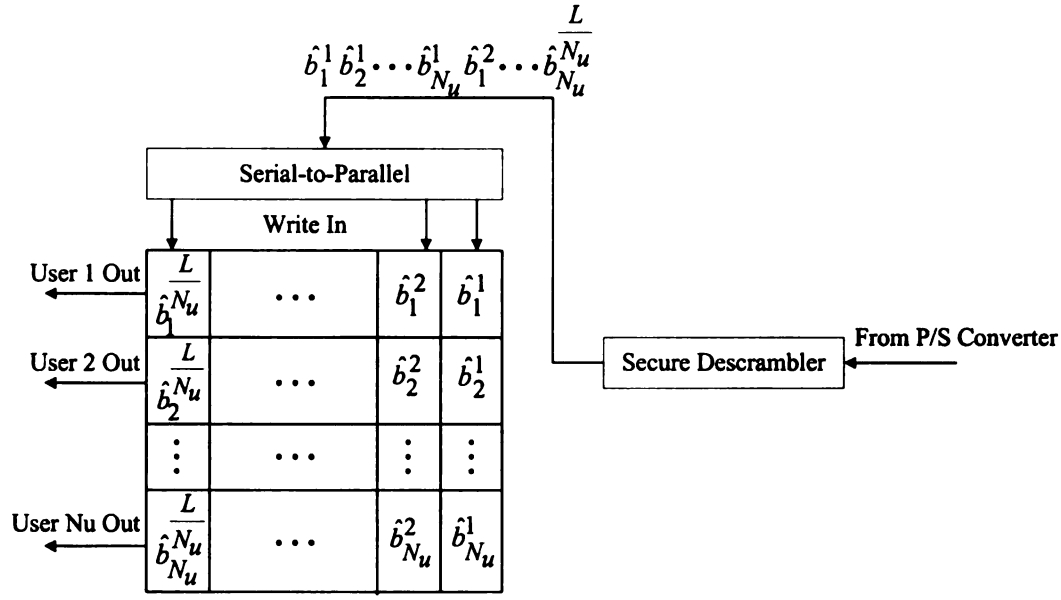
Assume there are N_u users in the system. Recall that the block length in the E-MDFH system is L. Without loss of generality, we assume that all the users have the same data rate, and the number of bits assigned to each user is an integer $N_b = \frac{L}{N_u}$. (Otherwise, users may have unequal number of bit assignments so that the total length of the block is L.)

Bit streams from different users are mixed through a simple user-multiplexer, as shown in Figure 3.6(a). The ith user's bit stream is written successively into the ith row of the block interleaver, for $i = 1, \cdots, N_u$. The content of the interleaver is column-wise read out. A secure scrambler is added after the user multiplexer to further randomize the carrier frequencies occupied by each user. A good example of secure scrambler design can be found in Section 4.4.1 or [80], where the secure scrambling sequence is obtained by encrypting a PN sequence with AES. Finally, the resulting sequence is fed into the input of serial-to-parallel converter in Figure 3.3. At the receiver, the corresponding de-multiplexer, as shown in Figure 3.6(b), is applied to recover the input bits. Separation of users' information is essentially the reverse operation of data multiplexing.

CF-MDFH is a joint time-division (TD) and frequency-division (FD) multiple accessing scheme, including both TD-MDFH [81] and FD-MDFH as special cases. The infrastructure of TD-MDFH is shown in Figure 3.7. For fairness, each user is periodi-



(a) Block-wsie user multiplexer



(b) Block-wsie user de-multiplexer

Figure 3.6. Block-wise user multiplexer and de-multiplexer, designed to process one data block of length L consisting of bits from N_u users. Here b_j^i denotes the ith bit of user j in the block.

cally assigned a time slot to transmit his/her information. Each active user transmits to the base station only in the assigned time slot or slots so that multiple-access interference (MAI) can be completely eliminated, assuming perfect timing synchronization is achieved at both sides. Because blind carrier frequency detection is still applicable in TD-MDFH, each data packet does not have to include a user-ID at each hop for each user, as long as the receiver knows the exact assignment of time slots for the corresponding transmitter. In this case, the reduced overhead results in the further increased spectral efficiency.

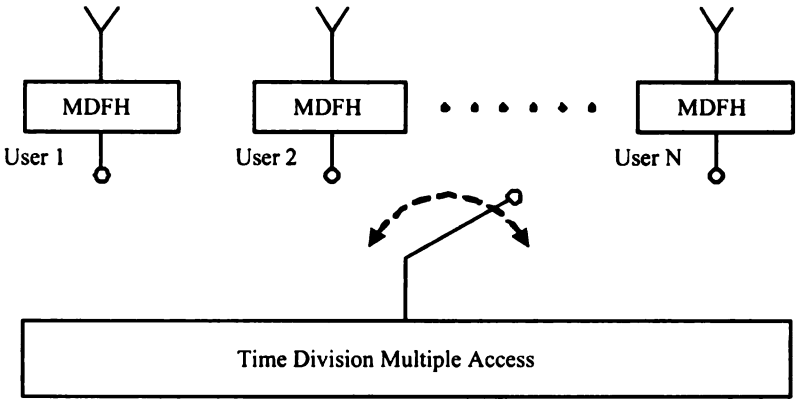


Figure 3.7. Infrastructure of the TD-MDFH scheme.

Remark 3.5 *CF-MDFH enjoys good* ***scalability*** *as the maximum user transmission rate is adaptive, and reversely proportional to the number of users in the system. Moreover, carrier frequencies at each hop are jointly determined by the information bits from all the users, and* ***source anonymity*** *is ensured by both the interleaver and the scrambler. Without the knowledge of the secure scrambler, even if the malicious user has a powerful set of equipments that can monitor the whole spectrum and can perfectly recover the carrier bits and the ordinary bits, extraction and composition of the desired user's information based on the securely scrambled sequence is a forbidden*

task. □

3.3.5 Bit-Error-Rate Analysis

Recall that in the MDFH and E-MDFH, the input bit stream is grouped into carrier bits and ordinary bits, where carrier bits are embedded in hopping frequency selection and ordinary bits are mapped to symbols in a certain constellation and then transmitted through selected carriers. It is interesting to note that *non-uniformity* exists between the carrier bits and the ordinary bits, in the sense that they have different BER performances. Since MDFH can be regarded as a special case of E-MDFH, we will focus on E-MDFH for bit error probability analysis.

BER of the carrier bits

Based on the receiver design in E-MDFH, BER analysis of the carrier bits is analogous to that of non-coherent FSK demodulation. For non-coherent detection of M_F-ary FSK signals, *the probability of symbol error* is given by [63, eqn. (5-4-46)]

$$P_{s,FSK}\left(\frac{E_b}{N_0}\right) = \sum_{m=1}^{M_F-1} \binom{M_F-1}{m} \frac{(-1)^{m+1}}{m+1} e^{-\frac{m\log_2 M_F}{(m+1)}\frac{E_b}{N_0}}, \tag{3.14}$$

where $\frac{E_b}{N_0}$ is the bit-level SNR. Let $k_F = \log_2 M_F$, then the probability of bit error, denoted by $P_{e,FSK}$, can be written as

$$P_{e,FSK}\left(\frac{E_b}{N_0}\right) = \frac{2^{(k_F-1)}}{2^{k_F}-1} P_{s,FSK}\left(\frac{E_b}{N_0}\right). \tag{3.15}$$

For an E-MDFH system with N_c channels, $M_F = N_c$, and $k_F = B_c$. Let $\frac{E_b^{(c)}}{N_0}$

and $\frac{E_b^{(o)}}{N_0}$ denote the effective bit-level SNR corresponding to the carrier bits and the ordinary bits, respectively, and $\frac{E_b}{N_0}$ the average bit-level SNR for the E-MDFH system. Recall that in the E-MDFH scheme, the length of each block is $L = [N_h(B_c - B_g) + B_s]2^{B_g}$, out of which there are $B_s 2^{B_g}$ ordinary bits and $N_h(B_c - B_g)2^{B_g}$ carrier bits. Note that in E-MDFH, the carrier bits are embedded in the carrier selection process and do not consume additional transmit power, the average bit-level SNR is

$$\frac{E_b}{N_0} = \frac{N_h N_g \bar{E}_s}{N_0[N_h(B_c - B_g) + B_s]2^{B_g}}, \tag{3.16}$$

where $\bar{E}_s$ is the average symbol power. In fact, let $E_1, \cdots, E_{N_t}$ be all the possible power levels in constellation Ω, and p_i the probability that an arbitrary information symbol has power E_i, then the average symbol power $\bar{E}_s$ is given by

$$\sum_{i=1}^{N_t} p_i E_i = \bar{E}_s, \text{where} \sum_{i=1}^{N_t} p_i = 1. \tag{3.17}$$

Without loss of generality, we assume $E_1 \leq E_2 \leq \cdots \leq E_{N_t}$. Taking 16-QAM as an example, $N_t = 3$, $E_1 = 2$, $E_2 = 10$, $E_3 = 18$, and $p_1 = 1/4$, $p_2 = 1/2$, $p_3 = 1/4$.

Since each frequency is uniquely identified by B_c bits, and each symbol represents B_s bits, the effective bit-level SNR corresponding to the carrier bits and the ordinary bits can be calculated as:

$$\frac{E_b^{(c)}}{N_0} = \frac{\bar{E}_s}{N_0 B_c}, \tag{3.18}$$

$$\frac{E_b^{(o)}}{N_0} = \frac{\bar{E}_s}{N_0 B_s}, \tag{3.19}$$

respectively. Substituting (3.16) into (3.18) & (3.19), it yields that

$$\frac{E_b^{(c)}}{N_0} = \frac{[N_h(B_c - B_g) + B_s]}{N_h B_c}\frac{E_b}{N_0}, \tag{3.20}$$

$$\frac{E_b^{(o)}}{N_0} = \frac{[N_h(B_c - B_g) + B_s]}{N_h B_s}\frac{E_b}{N_0}. \tag{3.21}$$

In the particular case when $N_g = 1$, E-MDFH is reduced to MDFH. Following (3.14), the BER for the carrier bits in MDFH can be obtained as:

$$P_{e,MDFH}^{(c)}\left(\frac{E_b}{N_0}\right) = \frac{2^{(B_c-1)}}{2^{B_c}-1}\sum_{i=1}^{N_t} p_i \sum_{m=1}^{N_c-1}\binom{N_c-1}{m}\frac{(-1)^{m+1}}{m+1}e^{-\frac{mB_c}{(m+1)}\frac{E_i}{E_s}\frac{E_b^{(c)}}{N_0}} \tag{3.22}$$

Let $P_{s,MDFH}^{(c)}$ denote the probability of carrier frequency detection error (corresponding to the symbol error in FSK) in MDFH, then we have

$$P_{s,MDFH}^{(c)}\left(\frac{E_b}{N_0}\right) = \frac{2^{B_c}-1}{2^{(B_c-1)}}P_{e,MDFH}^{(c)}\left(\frac{E_b}{N_0}\right). \tag{3.23}$$

In the more general case when $N_g \neq 1$, detection of the carrier bits in E-MDFH is similar to that of differential encoding (please refer to Section 3.3.3). Estimation error in one carrier index may cause detection errors in two neighboring carrier bit blocks. Denote the probability of carrier frequency detection error in E-MDFH as $P_{E-MDFH}^{(c)}$. It follows from (3.14) that

$$P_{E-MDFH}^{(c)}\left(\frac{E_b}{N_0}\right) = \sum_{i=1}^{N_t} p_i \sum_{m=1}^{N_c-1}\binom{N_c-1}{m}\frac{(-1)^{m+1}}{m+1}e^{-\frac{mB_c}{(m+1)}\frac{E_i}{E_s}\frac{E_b^{(c)}}{N_0}}. \tag{3.24}$$

Please note that $\frac{E_b}{N_0}$ in E-MDFH is different from that in MDFH due to their different

block structures.

Recall that for $i = 1, \cdots, N_h, m = 1, \cdots, N_g$, $I^i_{n,m}$ denotes the frequency index for the mth carrier at the ith hop of the nth symbol period. At each hop, $I^i_{n,m}$ should satisfy $I^i_{n,1} < I^i_{n,2} < \cdots < I^i_{n,N_g}$. For signal detection, after each individual carrier index is estimated, they are then sorted in ascending order to recover $I^i_{n,m}$. An error in the carrier index estimation may further introduce errors in the sorting process, and hence has negative impact on the index estimation for more than one $I^i_{n,m}$. Therefore, if $P^{(I)}_{E-MDFH}\left(\frac{E_b}{N_0}\right)$ denotes the average probability that an index $I^i_{n,m}$ is incorrectly estimated, then we have $P^{(I)}_{E-MDFH}\left(\frac{E_b}{N_0}\right) \geq P^{(c)}_{E-MDFH}\left(\frac{E_b}{N_0}\right)$.

Since $d^i_{n,1}$ is uniquely determined by $I^i_{n,1}$, it is clear that the probability of error in estimating $d^i_{n,1}$ is $P^{(I)}_{E-MDFH}\left(\frac{E_b}{N_0}\right)$. For the rest $\{d^i_{n,m}\}_{m=2}^{N_g}$, each $d^i_{n,m}$ relies on both $I^i_{n,m}$ and $I^i_{n,m-1}$. Therefore, the probability that $d^i_{n,m}$ is correctly detected, for $m = 2, \cdots, N_g$, is $\left[1 - P^{(I)}_{E-MDFH}\left(\frac{E_b}{N_0}\right)\right]^2$. Note that $P^{(I)}_{E-MDFH}\left(\frac{E_b}{N_0}\right) \geq P^{(c)}_{E-MDFH}\left(\frac{E_b}{N_0}\right)$. A lower bound of the BER for the carrier bits can thus be obtained as

$$P^{(c),L}_{e,E-MDFH}\left(\frac{E_b}{N_0}\right) = P_{s2e}\left\{\frac{1}{N_g}P^{(c)}_{E-MDFH}\left(\frac{E_b}{N_0}\right) + \frac{N_g-1}{N_g}\left\{1 - \left[1 - P^{(c)}_{E-MDFH}\left(\frac{E_b}{N_0}\right)\right]^2\right\}\right\} \quad (3.25)$$

where $P_{s2e} \triangleq \frac{2^{(B_c-B_g-1)}}{2^{(B_c-B_g)}-1}$.

Furthermore, the probability that all the indices $\{I^i_{n,m}\}_{m=1}^{N_g}$ are correctly estimated is $\left[1 - P^{(c)}_{E-MDFH}\left(\frac{E_b}{N_0}\right)\right]^{N_g}$. In this case, all the carrier bits can be perfectly recovered. If we assume that any estimation error in $\{I^i_{n,m}\}_{m=1}^{N_g}$ will incur detection errors in all the carrier bit blocks, then an upper bound of the BER for the carrier

bits can be derived:

$$P_{e,E-MDFH}^{(c),U}\left(\frac{E_b}{N_0}\right) = P_{s2e}\left\{1-\left[1-P_{E-MDFH}^{(c)}\left(\frac{E_b}{N_0}\right)\right]^{N_g}\right\}. \tag{3.26}$$

To summarize our discussions above, we have:

Proposition 3.1 *In E-MDFH, the BER of the carrier bits, $P_{e,E-MDFH}^{(c)}$, is bounded by*

$$P_{e,E-MDFH}^{(c),L}\left(\frac{E_b}{N_0}\right) \le P_{e,E-MDFH}^{(c)}\left(\frac{E_b}{N_0}\right) \le P_{e,E-MDFH}^{(c),U}\left(\frac{E_b}{N_0}\right). \tag{3.27}$$

Accordingly, the probability of error on the estimation of $d_{n,m}^{i}$, $P_{E-MDFH}^{(d)}$, for $i = 1,\cdots,N_h, m = 1,\cdots,N_g$ is bounded by

$$\underbrace{\frac{1}{P_{s2e}}P_{e,E-MDFH}^{(c),L}\left(\frac{E_b}{N_0}\right)}_{\triangleq P_{s,E-MDFH}^{(c),L}\left(\frac{E_b}{N_0}\right)} \le P_{E-MDFH}^{(d)}\left(\frac{E_b}{N_0}\right) \le \underbrace{\frac{1}{P_{s2e}}P_{e,E-MDFH}^{(c),U}\left(\frac{E_b}{N_0}\right)}_{\triangleq P_{s,E-MDFH}^{(c),U}\left(\frac{E_b}{N_0}\right)}.$$

BER of the ordinary bits

BER of the ordinary bits is determined by the modulation scheme used in the system. If FSK is utilized, then the BER of the ordinary bits can be calculated in a similar manner as that of the carrier bits. In the following, we consider the case of transmitting the ordinary bits through M-ary QAM. We start with MDFH, which is easier to analyze, then extend the results to E-MDFH.

Recall that if $M = 2^{B_s}$, where B_s is an even integer, the probability of symbol

error for M-ary QAM is [63, eqn. (5-2-78) & (5-2-79)]

$$P_{s,MQAM}\left(\frac{E_b}{N_0}\right) = 1 - \left[1 - 2(1 - \frac{1}{\sqrt{M}})Q\left(\sqrt{\frac{3\log_2 M}{(M-1)}\frac{E_b}{N_0}}\right)\right]^2, \tag{3.28}$$

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

Taking 16-QAM as an example, we have

$$P_{s,16-QAM}\left(\frac{E_b}{N_0}\right) = \frac{9}{4}\left(\frac{4}{3} - Q\left(\sqrt{\frac{4}{5}\frac{E_b}{N_0}}\right)\right)Q\left(\sqrt{\frac{4}{5}\frac{E_b}{N_0}}\right). \tag{3.29}$$

Accordingly, the probability of bit error is

$$P_{e,16-QAM}\left(\frac{E_b}{N_0}\right) = \frac{9}{16}\left(\frac{4}{3} - Q\left(\sqrt{\frac{4}{5}\frac{E_b}{N_0}}\right)\right)Q\left(\sqrt{\frac{4}{5}\frac{E_b}{N_0}}\right). \tag{3.30}$$

In MDFH, each QAM symbol undergoes N_h hops. Here we assume that N_h is odd. For signal detection, we first estimate the QAM symbol independently for each hop, and then apply bit-wise majority voting for the N_h estimates to make the final decision. Accordingly, the BER of the ordinary bits, $P_{e,MDFH}^{(o)}$, can be calculated as follows:

i) BER analysis at each individual hop: At each hop, the bit error can be classified into two types.

Type I error: bit is in error given that the carrier frequency is correctly detected. When the carrier frequency is detected correctly, for which the probability is $\left(1 - P_{s,MDFH}^{(c)}\left(\frac{E_b}{N_0}\right)\right)$, the probability of bit error can be calculated based on the BER of coherently detected M-ary QAM, given by $P_{e1} \triangleq P_{e,MQAM}\left(\frac{E_b^{(o)}}{N_0}\right)$. Here, $\frac{E_b}{N_0} = \frac{N_h B_s}{N_h B_c + B_s}\frac{E_b^{(o)}}{N_0}$.

Type II error: bit is in error when the carrier frequency is not correctly detected. When the carrier frequency is not correctly detected, for which the probability is $P^{(c)}_{s,MDFH}\left(\frac{E_b}{N_0}\right)$, it is reasonable to assume that probability of bit error is $P_{e2} \triangleq \frac{1}{2}$.

ii) Average BER calculation based on majority voting: In MDFH, each QAM symbol is transmitted through N_h hops. As a result, an error in a particular bit location is caused by at least $\lceil \frac{N_h}{2} \rceil$ unsuccessful recovery, where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. Let $P_{e,i}$, $i = 0, 1, \cdots, N_h$, be the conditional probability of bit error given that i out of N_h carrier frequencies are not correctly detected (i.e, $N_h - i$ carrier frequencies are correctly detected). Let j denote the number of unsuccessful bit recovery,

$$
\begin{aligned}
& P_{e,i}\left(\frac{E_b}{N_0}\right) \\
&= \sum_{j=\lceil \frac{N_h}{2} \rceil}^{N_h} \text{Prob}\{\text{errors in } j \text{ out of } N_h \text{ hops} \mid i \text{ carriers are wrong}\} \\
&= \sum_{j=\lceil \frac{N_h}{2} \rceil}^{N_h} \sum_{k=0}^{j} \text{Prob}\{k \text{ type I and } j-k \text{ type II errors} \mid i \text{ carriers are wrong}\} \\
&= \sum_{j=\lceil \frac{N_h}{2} \rceil}^{N_h} \sum_{k=0}^{j} P_B(k, P_{e1}, N_h - i) P_B(j-k, P_{e2}, i), \qquad (3.31)
\end{aligned}
$$

where $P_B(x, p, n) \triangleq \begin{pmatrix} n \\ x \end{pmatrix} (p)^x (1-p)^{n-x} = \frac{n!}{x!(n-x)!} (p)^x (1-p)^{n-x}$. Here we adopt the convention $\begin{pmatrix} n \\ x \end{pmatrix} = 0$ when $n < x$.

Taking the effect of the majority voting into consideration, the error probability for the ordinary bits, $P^{(o)}_{e,MDFH}$, is given by

$$\begin{aligned} & P^{(o)}_{e,MDFH}\left(\frac{E_b}{N_0}\right) \\ &= \sum_{i=0}^{N_h} \text{Prob}\{\text{bit is in error} \mid i \text{ carriers are wrong}\}\text{Prob}\{i \text{ carriers are wrong}\} \\ &= \sum_{i=0}^{N_h} P_{e,i}\left(\frac{E_b}{N_0}\right) P_B(i, P^{(c)}_{s,MDFH}, N_h). \end{aligned} \tag{3.32}$$

To determine the bit error probability for the ordinary bits in E-MDFH, we proceed in a similar manner as in MDFH, except for the use of different error probabilities in the detection of carrier frequency. More specifically, lower and upper bounds of the probability of bit error for the ordinary bits can be obtained by substituting $P^{(c),L}_{s,E-MDFH}\left(\frac{E_b}{N_0}\right)$ and $P^{(c),U}_{s,E-MDFH}\left(\frac{E_b}{N_0}\right)$ for $P^{(c)}_{s,MDFH}\left(\frac{E_b}{N_0}\right)$ in (3.32), respectively.

Overall BER for MDFH

The overall BER of the MDFH scheme is calculated as the linear combination of $P^{(c)}_{e,E-MDFH}$ and $P^{(o)}_{e,E-MDFH}$ based on the number of carrier bits and the number of ordinary bits in each block,

$$\begin{aligned} P_{e,E-MDFH}\left(\frac{E_b}{N_0}\right) &= \frac{N_h(B_c - B_g)}{N_h(B_c - B_g) + B_s} P^{(c)}_{e,E-MDFH}\left(\frac{E_b}{N_0}\right) \\ &+ \frac{B_s}{N_h(B_c - B_g) + B_s} P^{(o)}_{e,E-MDFH}\left(\frac{E_b}{N_0}\right). \end{aligned} \tag{3.33}$$

Example 3.1 - *BER Performance of E-MDFH* Assume the number of available carriers $N_c = 64$, and 16-QAM is adopted for baseband modulation in an E-MDFH system. Each 16-QAM symbol is transmitted via three hops. Four carriers are simultaneously used at each hop. In other words, $B_c = 6$, $B_s = 4$, $N_h = 3$, $B_g = 2$.

Figure 3.8 presents BER performance of the system. *Non-uniformity* can be observed in the carrier bits and the ordinary bits. In fact, the BER of carrier bits is worse than that of ordinary bits. The underlying argument is that the ordinary bits are transmitted through multiple hops, therefore, the BER can be substantially improved through majority voting. Comparison of the experimental results with the theoretical lower and upper bounds is also provided.

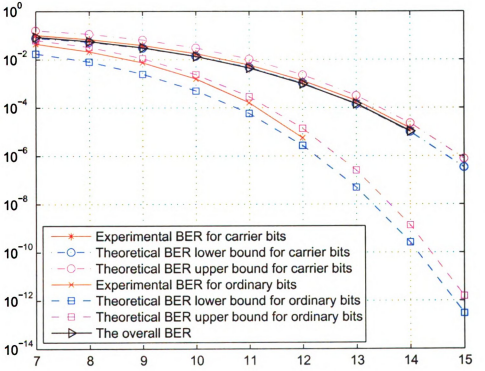


Figure 3.8. BER comparison of the carrier bits and the ordinary bits in E-MDFH: $N_h = 3$, $N_c = 64$ ($B_c = 6$), $B_s = 4$, $B_g = 2$.

3.3.6 Spectral Efficiency Analysis

We compare the spectral efficiency of the proposed E-MDFH scheme with that of the conventional FH scheme.

Single-user Case

There is only one user in both systems and no collisions need to be taken into consideration. Recall that T_s denotes the symbol period and T_h the hopping duration, $N_h = T_s/T_h$ ($N_h \geq 1$) is the number of hops per symbol period. For fair comparison, we assume that both systems have the same symbol period T_s, the same number of hops per symbol, N_h, and use constellation(s) of the same size M, i.e., the number of bits per symbol is $B_s = \log_2 M$. Let $R_s \triangleq 1/T_s$ be the symbol rate. Accordingly, the bit rate of the conventional FH can be expressed as:

$$R_{b,FH} = B_s R_s \text{ bits/second} \tag{3.34}$$

Recall that the data rate of E-MDFH $R_{b,E-MDFH}$ is $[N_h(B_c - B_g) + B_s]2^{B_g}$ bits every symbol period. That is,

$$R_{b,E-MDFH} = [N_h(B_c - B_g) + B_s]2^{B_g} R_s \text{ bits/second.} \tag{3.35}$$

Given N_h, B_c, B_s, an interesting question is to find the optimal B_g that maximizes $R_{b,E-MDFH}$. By solving $\frac{dR_{b,E-MDFH}}{dB_g} = 0$, we have $B_g = B_c + \frac{B_s}{N_h} - \frac{1}{\ln 2}$. Note that B_g must be an integer and $B_g \in [0, B_c]$. We have the following results:

Proposition 3.2 *Let* $B_g^{\perp} \triangleq \max\{0, \lfloor B_c + \frac{B_s}{N_h} - \frac{1}{\ln 2} \rfloor\}$ *and* $B_g^{\top} \triangleq \min\{B_c, \lceil B_c + \frac{B_s}{N_h} - \frac{1}{\ln 2} \rceil\}$, *where* $\lfloor x \rfloor$ *denotes the largest integer less than or equal to* x *and* $\lceil x \rceil$ *the*

smallest integer greater than or equal to x. The optimal value of B_g, denoted by B_g^*, that maximizes the throughput of the E-MDFH is given by

$$B_g^* = \begin{cases} B_g^{\perp}, & \text{if } \frac{[N_h(B_c - B_g^{\perp}) + B_s]2^{B_g^{\perp}}}{[N_h(B_c - B_g^{\top}) + B_s]2^{B_g^{\top}}} > 1, \\ B_g^{\top}, & \text{otherwise.} \end{cases} \tag{3.36}$$

□

Given that the total bandwidth $W_B = c_0 \frac{N_c}{T_h}$, where c_0 is a constant, the spectral efficiency (in bits/second/Hz) of the conventional fast FH and E-MDFH are given by

$$\eta_{FH} = \frac{R_{b,FH}}{W_B} = \frac{B_s}{c_0 N_c N_h}, \tag{3.37}$$

$$\eta_{E-MDFH} = \frac{R_{b,E-MDFH}}{W_B} = \frac{[N_h(B_c - B_g^*) + B_s]2^{B_g^*}}{c_0 N_c N_h}. \tag{3.38}$$

It is obvious that we always have $\eta_{E-MDFH} > \eta_{FH}$. That is, E-MDFH is always much more efficient than the conventional fast FH scheme.

Example 3.2 - *Single-user case* Assume the number of available channels is $N_c = 64$, and 16-QAM modulation is adopted for both MDFH and the conventional FH systems. That is, $B_c = 6$ and $B_s = 4$. The BER performance with respect to three different hop rates, i.e., $N_h = 3, 5, 7$, is independently measured for both systems, and the results are depicted in Figure 3.9. As can be seen, the MDFH system outperforms the FH system with big margins.

We further compare the BER performances of the carrier bits and the ordinary bits in MDFH, as shown in Figure 3.10. It can be seen that there is almost a perfect

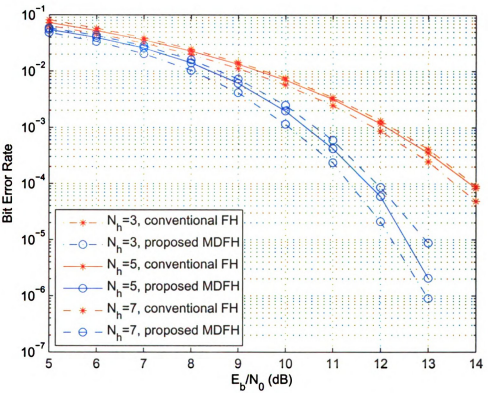


Figure 3.9. BER comparison of the conventional FH and the proposed E-MDFH in the single-user case: $N_c = 64$ ($B_c = 6$), $B_s = 4$, $B_g = 0$.

match between the simulation results and the theoretical results derived in (3.22) & (3.32). Moreover, it can be observed that the BER of ordinary bits is much better than that of carrier bits, since the same ordinary bits are transmitted via multiple hops, and the BER is therefore substantially improved through majority voting even if certain carrier frequencies are not correctly detected.

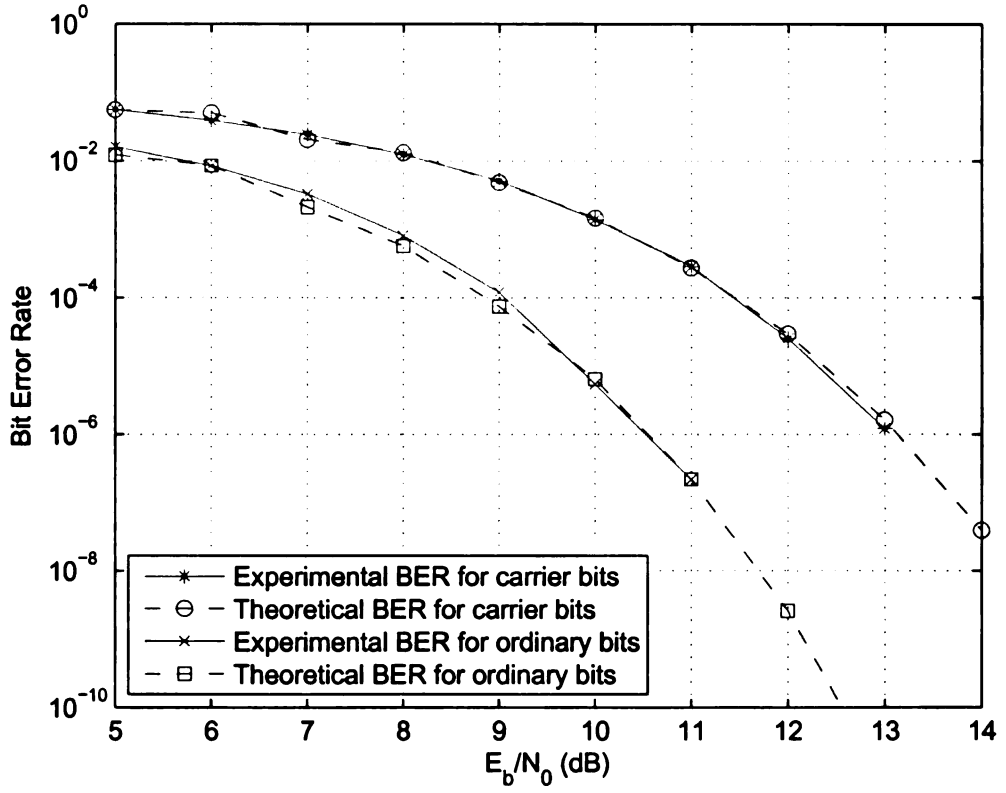


Figure 3.10. BER comparison of the carrier bits and the ordinary bits in E-MDFH: $N_h = 3$, $N_c = 64$ ($B_c = 6$), $B_s = 4$, $B_g = 0$.

Multiple-user Case

Next, we explore the more general case where there are multiple users in both systems. Consider a conventional fast FH system with $N_u(> 1)$ users, each transmitting 2^{B_c}-ary MFSK signals over N_c frequencies. At the receiver, after de-hopping, each user creates

a $2^{Bc} \times N_h$ decision table. For $i = 1, \cdots, 2^{Bc}$ and $j = 1, \cdots, N_h$, if the receiver decides a transmission is present on the ith carrier frequency during the jth hop duration, that is, if the output of the corresponding envelope detector exceeds some threshold, then the ith row and jth column of the decision table is filled, otherwise, it is left as blank. [73,82]

Note that in the conventional FHMA systems, different users hops in an independent manner, any one of the $2^{Bc} - 1$ carrier frequencies not occupied by the desired user may be filled incorrectly as a result of a tone transmitted by an interfering user. This event, known as *insertion*, occurs with probability $p = 1 - \left(1 - \frac{1}{2^{Bc}}\right)^{N_u - 1}$. Moreover, additive noise may also result in insertions to the decision table. As a result, the overall insertion probability P_I is given by [73]

$$P_I = p + (1 - p)e^{-\theta^2 \frac{B_c}{N_h} \frac{E_b}{N_0}}, \tag{3.39}$$

where θ is the normalized threshold.

On the other hand, because the interference may cause the decision statistic to fall below the threshold, a tone from the desire user may not appear among the receiver's positive decisions, resulting in a *deletion* in the decision matrix. The probability that a *deletion* occurs, denoted by P_D, is given by [73]

$$P_D = \frac{p}{3} + (1 - \frac{p}{3}) \left[1 - Q\left(\sqrt{\frac{2B_c}{N_h} \frac{E_b}{N_0}}, \theta \sqrt{\frac{2B_c}{N_h} \frac{E_b}{N_0}}\right)\right], \tag{3.40}$$

where $Q(x, y)$ is the Marcum Q-function [83].

In the ideal case, the row of the decision table, corresponding to the symbol transmitted by the desired user, will be fully filled. If it is the only full row, then the decoding is perfect. However, due to the presence of multiple-access interference and

additive white noise, insertion as well as deletion in the receive matrix may occur. When the filled entries in another row is more than that of the desired row, a symbol error occurs. When two or more rows in the receive matrix have the same number of entries, random decision (based on the toss of a coin) has to be used for MFSK symbol detection.

Let $P_d(i)$ denote the probability that i entries are filled on the desired row of the receive matrix, and $P_o(j)$ the probability that j entries are filled on any other row, then we have: $P_d(i) = \begin{pmatrix} N_c \\ i \end{pmatrix} (1-P_D)^i P_D^{N_h-i}$, and $P_o(j) = \begin{pmatrix} N_c \\ j \end{pmatrix} (1-P_I)^{N_h-j} P_I^j$.

Let $P_{e,FHMA}^{(u)}$ denote the bit-error-rate of the desired user in the conventional FHMA system. Let N_w be the total number of undesired rows, then $N_w = 2^{B_c} - 1$. Let j_n be the number of filled entries in an undesired row f_n, define $j_0 \triangleq \max\{j_n\}$, where the maximum operation is taken over all the undesired rows. As can be seen, a detection error occurs whenever $j_0 \geq i$. Since the probability that $j_n = j_0$ occurs in two or more undesired rows is very low, here we only consider the case where only one undesired row has j_0 entries. As a result, $P_{e,FHMA}^{(u)}$ can be approximated as

$$P_{e,FHMA}^{(u)} \approx \frac{2^{(B_c-1)}}{2^{B_c}-1} \begin{pmatrix} N_w \\ 1 \end{pmatrix} (\text{Prob\{j} > \text{i\}} + \frac{1}{2}\text{Prob\{j} = \text{i\}}), \tag{3.41}$$

$$= \frac{2^{(B_c-1)}}{2^{B_c}-1}(2^{B_c}-1)\left[\sum_{j=1}^{N_h} P_o(j) \sum_{i=0}^{j-1} P_d(i) + \frac{1}{2}\sum_{j=1}^{N_h} P_o(j)P_d(j)\right] \tag{3.42}$$

$$= 2^{(B_c-1)}\left[\sum_{j=1}^{N_h} P_o(j) \sum_{i=0}^{j-1} P_d(i) + \frac{1}{2}\sum_{j=1}^{N_h} P_o(j)P_d(j)\right], \tag{3.43}$$

where the factor of $\frac{1}{2}$ is the probability that the fair coin toss favors the wrong decision rather than the correct one.

For the proposed E-MDFH scheme, there is no multiple-access interference, therefore, the average BER in (3.33) is directly applicable to the multiuser case.

From the spectral efficiency perspective, we need to compare the total information bits allowed to be transmitted under the same BER and bandwidth requirements (i.e., the same hop rate). As it is not easy to derive an explicit expression of the maximum date rate in terms of BER for both conventional FHMA and E-MDFH systems, we illustrate the system performance through the following numerical example.

Example 3.3 - *Multiple-user case* Assume $N_c = 64$ (i.e., $B_c = 6$), $N_h = 5$, $B_s = 4$, $B_g = 2$, and the required BER is 10^{-4}. Consider the transmission over one symbol period.

From Figure 3.11(a), it can be seen that the proposed E-MDFH scheme can achieve the desired BER at $\frac{E_b}{N_0} = 13.6$dB. For clarity, this point is marked by a black '$*$' in two figures. During one symbol period, the total number of transmitted information bits in E-MDFH is $[N_h(B_c - B_g) + B_s]2^{B_g} = 4(5 \cdot 4 + 4) = 96$. Figure 3.11(b) depicts the BER as a function of $\frac{E_b}{N_0}$ for $N_u = 2, \cdots, 7$. In each case, the threshold θ is optimized to minimize the BER. It can be observed that the conventional FHMA system can only accommodate up to 5 users at $\frac{E_b}{N_0} = 13.6$dB, in order to achieve BER $= 10^{-4}$. Therefore, during one symbol period, the FH system can transmit at most $N_u B_c = 5 \cdot 6 = 30$ bits. In this case, E-MDFH achieves an increase of 220% in spectral efficiency.

Simulations are also carried out for $N_h = 3$ and $N_h = 7$, while keeping all the other parameters unchanged. The overall results are listed in Table 3.1. In E-MDFH, the required BER for the six cases can be obtained at $\frac{E_b}{N_0}$ equal to 11.9dB, 13.2dB, 13.6dB, 14.5dB, 13.8dB, 14.7dB, respectively. Subject to the same BER and bit-level

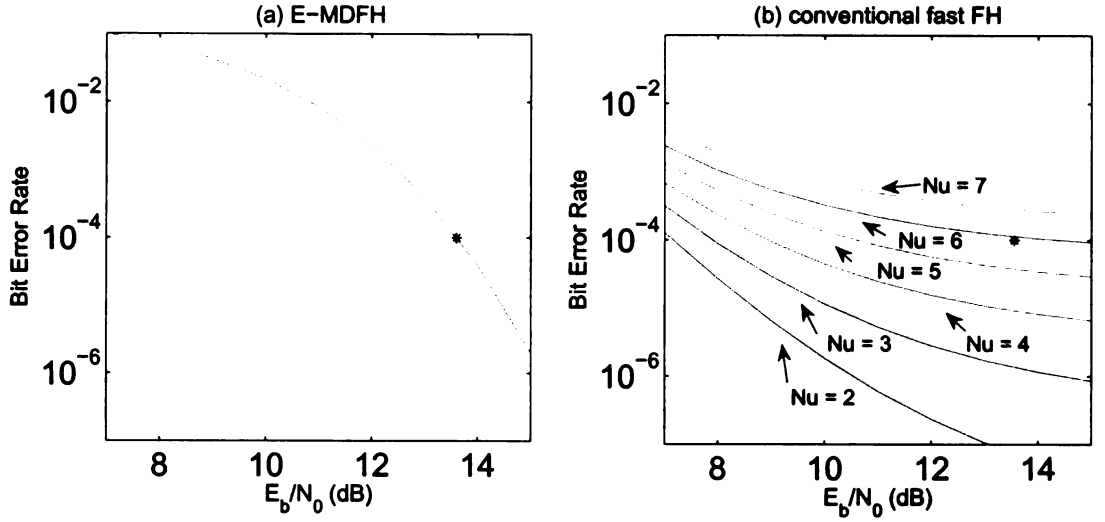


Figure 3.11. Performance comparison of E-MDFH and conventional FH in the multi-user case: $N_h = 5$, $N_c = 64$ ($B_c = 6$), $B_s = 4$, $B_g = 2$.

SNR, the conventional FHMA system can support at most 5, 3, 5, 4, 7, 5 users for the six cases, respectively. As can be seen, E-MDFH can achieve a spectral efficiency up to 4 times higher than that of the conventional FHMA system.

Table 3.1. Comparison of information bit rate between the conventional fast FH system and the proposed E-MDFH scheme for various hop rates: $N_c = 64$ ($B_c = 6$), $B_s = 4$, $B_g = 2$.

	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
N_h	3	3	5	5	7	7
Required BER	10^{-3}	10^{-4}	10^{-4}	10^{-5}	10^{-4}	10^{-5}
Conventional FH (bits/T_s)	30	18	30	24	42	30
E-MDFH (bits/T_s)	64	64	96	96	128	128

The above in-depth quantitative performance analysis and simulation examples demonstrate the superior performance of MDFH in terms of spectral efficiency.

3.4 Collision-Free Frequency Hopping

In this section, a highly efficient collision-free frequency hopping scheme is presented. The core components of the CFFH system is the OFDM framework and the dynamic subcarrier assignment algorithm. Although frequency hopping has been used to enrich the frequency diversity in OFDM systems [84, 85], we consider the contrary: how to increase the information capacity of FH systems by exploiting the OFDM structure.

First, we describe the signal transmission and detection scheme for each individual user. At each symbol period, each user transmits on specific subcarrier(s), based on the user's information rate requirement and total load of the system. Then, an AES based secure subcarrier assignment algorithm is proposed to ensure that: (i) Each user hops to a different set of subcarriers in a pseudo-random manner at the beginning of each hopping period; (ii) At each hopping period, different users always transmit on non-overlapping sets of subcarriers, and hence are collision-free.

We would like to emphasize that while it is possible to design collision-free frequency hopping system based on non-OFDM frameworks, the utilization of OFDM in the CFFH scheme has unique advantages which cannot be surpassed by other systems.

3.4.1 Signal Transmission and Detection

Consider a system with N_u users, utilizing an OFDM system with N_c subcarriers, $\{f_1, \cdots, f_{N_c}\}$. At each OFDM symbol period, each user is assigned a specific subset of the total available subcarriers. Assuming that at the nth symbol, user i has been assigned a set of subcarriers $C_{n,i} = \{f_{n,i_1}, \cdots, f_{n,i_{N_i}}\}$, that is, user i will transmit and only transmit on these subcarriers. Here, N_i is the total number of subcarriers

assigned to user i. Note that for any n,

$$C_{n,i} \bigcap C_{n,j} = \emptyset, \quad \forall \ i \neq j. \tag{3.44}$$

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

$$\bigcup_{i=1}^{N_u} C_{n,i} = \{f_1, \cdots, f_{N_C}\}. \tag{3.45}$$

For the ith user, if $N_i > 1$, then the ith user's information symbols are first fed into a serial-to-parallel converter. Suppose that at the nth symbol period, the ith user transmits the information symbols $\{u_{n,1}^{(i)}, \cdots, u_{n,N_i}^{(i)}\}$ (which are generally QAM symbols) through the subcarrier set $C_{n,i} = \{f_{n,i_1}, \cdots, f_{n,i_{N_i}}\}$. User i's transmitted signal at the nth OFDM symbol can then be written as:

$$s_n^{(i)}(t) = \sum_{l=1}^{N_i} u_{n,l}^{(i)} e^{j2\pi f_{n,i_l} t}. \tag{3.46}$$

Note that each user transmits zeros on subcarriers which are not assigned to him/her, and hence ensures collision-free transmission among different users.

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

$$r(t) = \sum_{i=1}^{N_u} r_n^{(i)}(t) + w(t), \tag{3.47}$$

where

$$r_n^{(i)}(t) = s_n^{(i)}(t) * h_i(t), \tag{3.48}$$

and $w(t)$ is the additive noise. In (3.48), $h_i(t)$ is the channel impulse response corre-

sponding to the ith user. Note that in OFDM systems, guard intervals are inserted between symbols to eliminate inter-symbol interference, so it is reasonable to study the signals in a symbol-by-symbol manner. Equations (3.46)~(3.48) represent an uplink system. The downlink system can be formulated in a similar manner.

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

$$\mathbf{u}_n^{(i)}(l) = \begin{cases} 0, & \text{if } l \notin \{i_1, \cdots, i_{N_i}\} \\ u_{n,l}^{(i)}, & \text{if } l \in \{i_1, \cdots, i_{N_i}\}. \end{cases} \tag{3.49}$$

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

$$\mathbf{s}_n^{(i)} = \mathbf{F}^{\mathcal{H}} \mathbf{u}_n^{(i)}, \tag{3.50}$$

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

$$\mathbf{F} = \frac{1}{\sqrt{N}} \begin{bmatrix} V_N^{00} & \cdots & V_N^{0(N-1)} \\ \vdots & \ddots & \vdots \\ V_N^{(N-1)0} & \cdots & V_N^{(N-1)(N-1)} \end{bmatrix},$$

with $V_N^{nk} = e^{-j2\pi nk/N}$, the superscript $\mathcal{H}$ denotes complex conjugate transpose. As we only consider one OFDM symbol at a time, for notation simplification, here we omit the insertion of the guard interval (i.e., the cyclic prefix which is used to ensure that there is no inter-symbol interference between two successive OFDM symbols).

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

let

$$\mathbf{H}_i = \mathbf{F}\mathbf{h}_i \tag{3.51}$$

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

$$\mathbf{z}_n^{(i)}(l) = \mathbf{u}_n^{(i)}(l)\mathbf{H}_i(l). \tag{3.52}$$

The overall received signal is then given by

$$\mathbf{z}_n(l) = \sum_{i=1}^{N_u} \mathbf{z}_n^{(i)}(l) + \mathbf{w}_n(l) \tag{3.53}$$

$$= \sum_{i=1}^{N_u} \mathbf{u}_n^{(i)}(l)\mathbf{H}_i(l) + \mathbf{w}_n(l). \tag{3.54}$$

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

Note that due to the collision-free subcarrier assignment, for each l, there is at most one non-zero item in the sum $\sum_{i=1}^{N_u} \mathbf{u}_n^{(i)}(l)\mathbf{H}_i(l)$. As a result, standard channel estimation algorithms and signal detection methods for OFDM systems can be implemented.

In the slow hopping case, where each user transmits a frame of OFDM symbols before it hops to a different set of subcarrier, each user can send pilot symbols on his subcarrier set to perform channel estimation. It should be pointed out that instead of estimating the whole frequency domain channel vector $\mathbf{H}_i$, for signal recovery, the ith user only needs to estimate the entries corresponding to his subcarrier set, that is the values of $\mathbf{H}_i(l)$ for $l \in \{i_1, \cdots, i_{N_i}\}$. After channel estimation, user i's information symbols can be estimated from

$$\hat{\mathbf{u}}_n^{(i)}(l) = \frac{\mathbf{z}_n(l)}{\mathbf{H}_i(l)}, \quad \forall\, l \in \{i_1, \cdots, i_{N_i}\}. \tag{3.55}$$

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

In the fast hopping case, where the hopping period is less than or equal to one OFDM symbol period, each user would then send one to two pilot (full OFDM) symbols, so that the channel information is available no matter which subcarrier set the user hops to. When there are multiple users in the system, different users should transmit their pilot symbols in non-overlapping time slots for accurate channel estimation.

3.4.2 Secure Subcarrier Assignment Algorithm

Design of secure subcarrier assignment algorithm is not unique. Here we present a secure carrier index assignment algorithm based on the advanced encryption standard (AES), also known as Rijndael.

Rijndael was identified as the new AES in October 2, 2000. Rijndael's combination of security, performance, efficiency, ease of implementation and flexibility makes it an appropriate selection for the AES. Rijndael is a good performer in both hardware and software across a wide range of computing environments. Its low memory requirements make it suitable for restricted-space environments such as mobile handset to achieve excellent performance. More details on AES can be found in [86].

The AES algorithm is used here to ensure the randomness and the security of the hopping system, so that there is no easy way for malicious users to find out the hopping pattern. Certainly, other advanced encryption algorithms can be implemented as well.

Without loss of generality, here we assume that the total number of carriers $N_c = 128$. The following algorithm can be straightforwardly extended to other values of N_c.

The proposed secure subcarrier assignment algorithm can be summarized as follows:

1. Generate a pseudo-random binary sequence using a 42-bit linear feedback shift register (LFSR) specified by the following characteristic polynomial:

$$\begin{aligned} & x^{42} + x^{35} + x^{33} + x^{31} + x^{27} + x^{26} + x^{25} \\ & + x^{22} + x^{21} + x^{19} + x^{18} + x^{17} + x^{16} \\ & + x^{10} + x^{7} + x^{6} + x^{5} + x^{3} + x^{2} + x + 1. \end{aligned} \tag{3.56}$$

   Group the sequence into blocks of length 128 bits, and denote the nth block as $\mathbf{X}_n$, which will be used to generate subcarrier indices for the nth hopping period.

2. Take the nth block $\mathbf{X}_n$ as the plaintext, and specify an arbitrary 128-bit key. Encrypt the plaintext with the key using the AES algorithm, and the resulting ciphertext is also 128 bits, denoted by $\{b_1,\ b_2,\ \cdots,\ b_{128}\}$.

3. Split $[b_1\ b_2\ \cdots\ b_{128}]$ into 127 binary vectors as follows:

$$[b_1\ b_2\ \cdots\ b_7],\ [b_2\ b_3\ \cdots\ b_8],\ \cdots,\ [b_{64}\ b_{65}\ \cdots\ b_{70}], \tag{3.57}$$

$$[b_{65}\ b_{66}\ \cdots\ b_{70}],\ [b_{66}\ b_{67}\ \cdots\ b_{71}],\ \cdots,\ [b_{96}\ b_{97}\ \cdots\ b_{101}], \tag{3.58}$$

$$[b_{97}\ b_{98}\ \cdots\ b_{101}],\ [b_{98}\ b_{99}\ \cdots\ b_{102}],\ \cdots,\ [b_{112}\ b_{113}\ \cdots\ b_{116}], \tag{3.59}$$

$$[b_{113}\ b_{114}\ b_{115}\ b_{116}],\ \cdots,\ [b_{120}\ b_{121}\ b_{122}\ b_{123}], \tag{3.60}$$

$$[b_{121}\ b_{122}\ b_{123}],\ [b_{122}\ b_{123}\ b_{124}],\ [b_{123}\ b_{124}\ b_{125}],\ [b_{124}\ b_{125}\ b_{126}], \tag{3.61}$$

$$[b_{125}\ b_{126}],\ [b_{126}\ b_{127}], \tag{3.62}$$

$$[b_{128}]. \tag{3.63}$$

   There are 64 7-bit groups in (3.57), 32 6-bit groups in (3.58), 16 5-bit groups in

(3.59), 8 4-bit groups in (3.60), 4 3-bit groups in (3.61), 2 2-bit groups in (3.62) and 1 1-bit group in (3.63). Each binary vector is then converted to a decimal integer with the first or last element of the vector considered to be the most significant alternately, denoted by ζ_i, for $i = 1, 2, \cdots, 127$.

4. Initialize two sets of integers as $\mathcal{N} = \{1, 2, \cdots, 128\}$ and $\mathcal{I} = \phi$. Randomly take one entry out of $\mathcal{N}$ at a time and put it successively into $\mathcal{I}$ as an index. Since one index is selected at random from $\mathcal{N}$ without replacement (meaning without repetition), after each update, the size of $\mathcal{N}$ is decreased by one, while that of $\mathcal{I}$ is increased by one.

   Because the first 64 indices are chosen from $\mathcal{N}$ with size of greater than 64, seven bits are required to uniquely represent the position of each selected index in $\mathcal{N}$, which is the reason why 64 7-bit vectors are formed as in (3.57). Justification for partition of $[b_1\ b_2\ \cdots\ b_{128}]$ corresponding to equations (3.58) $\sim$ (3.63) may be deduced by analogy.

   From a mathematical point of view, the random assignment algorithm can be achieved as follows:

$$\mathcal{I}(i) = \mathcal{N}(\zeta_i \% (129 - i) + 1), \quad \text{for } i = 1, 2, \cdots, 127, \tag{3.64}$$

   where the function $x\%y$ returns the remainder after x is divided by y. After the procedure in (3.64) is performed successively, the size of $\mathcal{I}$ becomes 127 and $\mathcal{N}$ only has one element left. Let $\mathcal{I}(128) = \mathcal{N}(1)$, then a sophisticatedly designed random index vector $\mathcal{I}$ of length 128 is obtained.

5. Recall that at each OFDM symbol, N_i subcarriers are assigned to user i. We

now assign the subcarriers with indices $\{\mathcal{I}(1), \mathcal{I}(2), \cdots, \mathcal{I}(N_1)\}$ to user 1, assign the subcarriers with indices $\{\mathcal{I}(N_1+1), \mathcal{I}(N_1+2), \cdots, \mathcal{I}(N_1+N_2)\}$ to user 2, and so on.

3.4.3 Performance Analysis in the Presence of Fixed-Band Jamming

Suppose that the total number of available subcarriers is N_c and the ith user is assigned N_i carriers. The jammer intentionally interferes N_j fixed subcarriers. Without loss of generality, we assume $N_i \geq N_j$. If subcarriers are allocated to each user randomly, then for the ith user, the probability that k out of N_i selected subcarriers are jammed is given by

$$P_c^{(k)} = \frac{\binom{N_j}{k}\binom{N-N_j}{N_i-k}}{\binom{N}{N_i}}, \quad \text{for } k = 0, \cdots, N_j. \tag{3.65}$$

In particular, the probability that none of N_i subcarriers are jammed is

$$P_c^{(0)} = \frac{\binom{N-N_j}{N_i}}{\binom{N}{N_i}} \tag{3.66}$$

$$= \frac{(N-N_i)!(N-N_j)!}{N!(N-N_i-N_j)!} \tag{3.67}$$

Consequently, we have the probability that at least one of N_i selected subcarriers are jammed: $1 - P_c^{(0)}$.

If no channel coding is employed, then the system performance can be measured independently for each subchannel and the probability of bit error is determined by the interference over the channel. If the BER is modeled as a function of the signal-to-interference-plus-noise ratio, then the overall system performance for the ith user can be obtained

$$\overline{P_e} = \frac{1}{N_i} \sum_{k=0}^{N_j} P_c^{(k)} [k P_e(\frac{N_j \cdot JSR \cdot SNR}{SNR + N_j \cdot JSR}) + (N_i - k) P_e(SNR)], \tag{3.68}$$

where SNR is defined as the ratio of the average signal power to the noise power, JSR represents the ratio of the total jamming power to the average signal power, and the jammer uniformly distributes its available power over N_j channels.

Taking channel coding into consideration, even if signals are transmitted over the jammed subchannels, it is still possible to recover the corrupted information due to the strong error-correcting capability of channel codes. All things considered, we have to utilize the average SINR for the decoding process. Hence, the BER performance is approximately given by

$$\overline{P_e} = \sum_{k=0}^{N_j} P_c^{(k)} P_e \left(\frac{N_i \cdot N_j \cdot JSR \cdot SNR}{k \cdot SNR + N_i \cdot N_j \cdot JSR} \right). \tag{3.69}$$

In both cases, there exists a lower bound for the overall BER, that is,

$$\overline{P_e} > P_e(SNR), \tag{3.70}$$

where $P_e(SNR)$ denotes the bit error rate of the system at a specific SNR level over an AWGN channel.

3.4.4 Simulation Examples

In the following, numerical examples are provided to illustrate the advantages of the CFFH scheme over the conventional FH systems.

Example 3.4 - *BER performance and spectral efficiency* Assume that the total number of available channels (subcarriers) is $N_c = 128$. Consider two systems: (i) A conventional FHMA system with $N_u = 8$ users, each using 4-FSK modulation; (ii) A CFFH system with 8 users, each transmitting QPSK symbols. The BER comparison of the two systems over AWGN channels is shown in Figure 3.12. As can be seen, the proposed CFFH system delivers excellent results. The conventional FHMA system, on the other hand, is severely limited by the collision effect, and does not really work. And it should be noted that in this example, the spectral efficiency of the CFFH system is 16 times that of the conventional FHMA system. Essentially, CFFH has the same spectral efficiency as the OFDM system, which is much higher than the conventional FHMA system.

Example 3.5 - *Jamming resistance* In the example, the total number of available subcarriers is $N_c = 256$ and the number of users is $N_u = 16$. Each user is assigned 16 subcarriers. Consider the performance of three systems under hostile jamming: (i) A conventional OFDMA system where each user transmits on 16 fixed subcarriers; (ii) A CFFH system with 16 subcarriers allocated to each user pseudo-randomly based

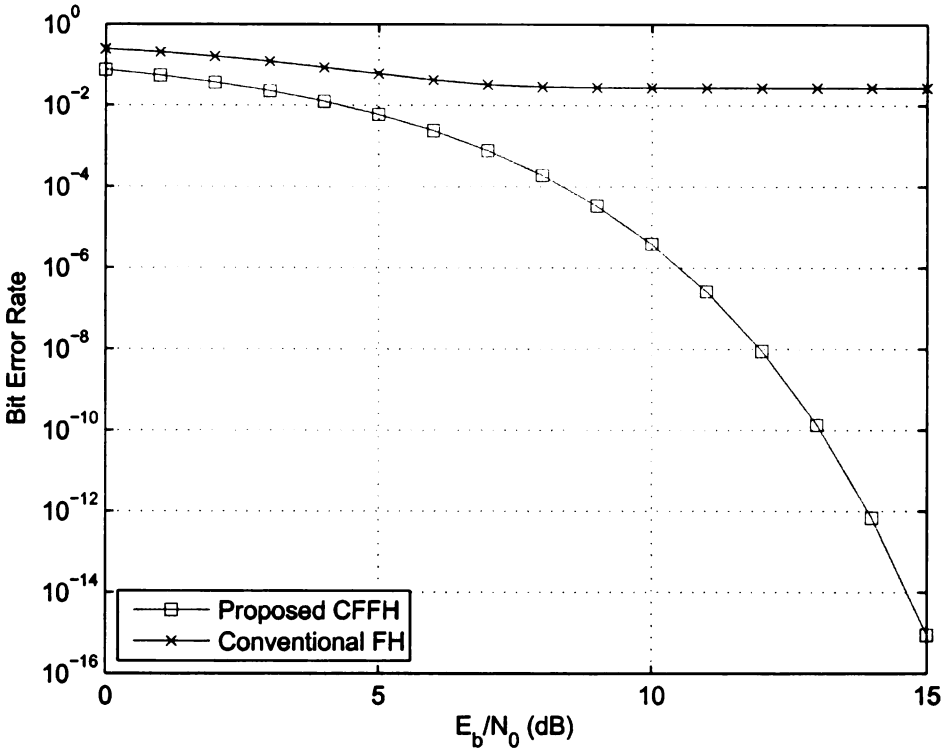


Figure 3.12. BER comparison of CFFH and conventional FHMA system over AWGN channels: $N_c = 128$, $N_u = 8$.

on the secure subcarrier assignment algorithm. (iii) A CFFH system with the knowledge of which subcarriers being jammed, where users are able to choose channels for information transmission to avoid the hostile jamming. The third case is essentially equivalent to a jamming-free CFFH or OFDMA system. We assume that the jammer intentionally interferes 8 subcarriers, which are coincidentally used by a user in system (i). E_b/P_J is defined as the ratio of the average bit-level energy to the total jamming power. SNR is defined as the ratio of the average signal power to the noise power, and is fixed at 7 dB in the simulation.

At the transmitter, a rate-$\frac{1}{2}$ turbo code is utilized for forward error control. The generation matrix of the constituent code is given by $[1, \frac{(7)_{octal}}{(5)_{octal}}]$, where $(7)_{octal}$ and $(5)_{octal}$ are the feedback and feedforward polynomials with memory length 2, respectively. The block length is 960. After encoding, 1920 bits are mapped into 16-QAM symbols and transmitted over the selected carriers. At the receiver, tentative soft decisions are made by 16-QAM demodulation, and then the resulting log-likelihood ratios (LLRs) of the code bits are fed into a turbo decoder. There is no iteration between the demodulator and the turbo decoder. The decoding algorithm is the canonical log-MAP [87]. The number of decoding iterations is 5, and no early termination scheme is applied.

The BER comparison of three systems over the same AWGN channel is shown in Figure 3.13. As can be seen, benefited from the jamming resistance property of the frequency hopping system, the proposed CFFH delivers much better performance under hostile jamming than the conventional OFDMA system with fixed carrier allocation. The performance of the conventional OFDMA system is severely limited by the jamming interference, even if a powerful error-correcting code (e.g., turbo coding) is employed. System (iii) is essentially jamming-free and its BER performance serves

as the lower bound in this example.

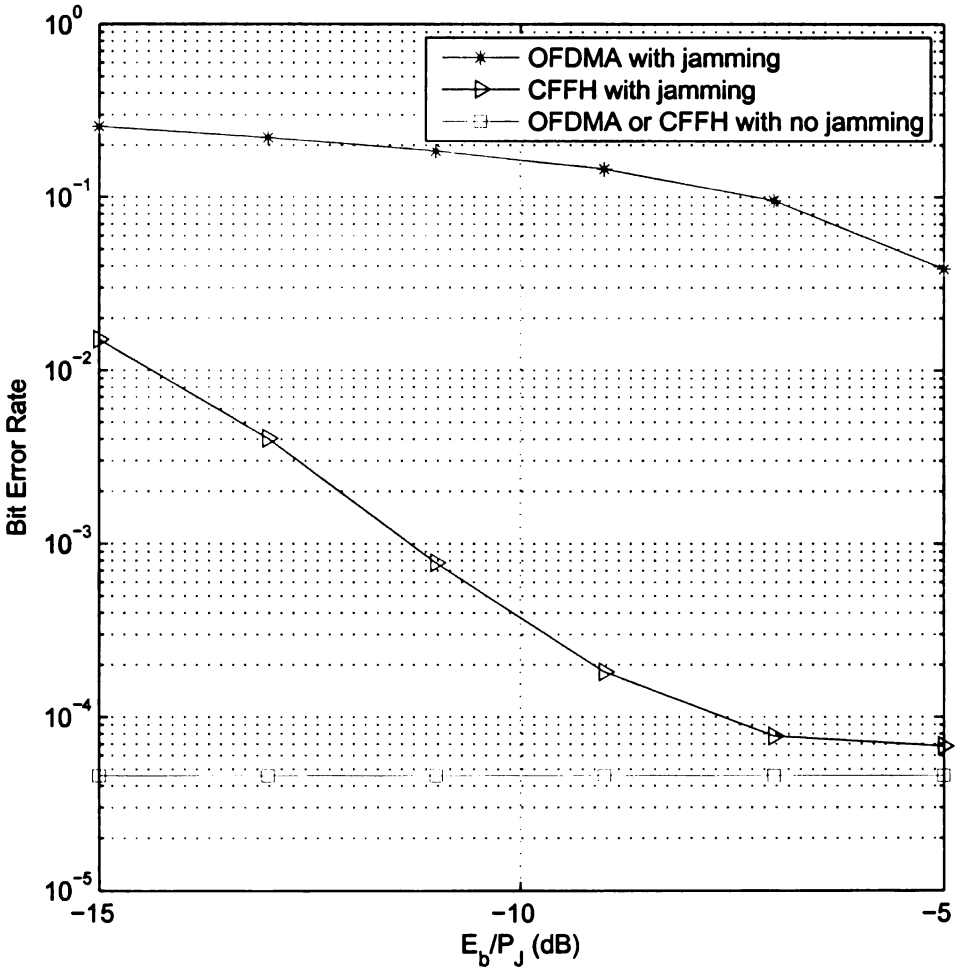


Figure 3.13. BER comparison for three systems under hostile jamming: $N_c = 256$, $N_u = 16$, SNR = 7dB.

3.5 Summary

In this chapter, we presented the design and in-depth analysis of two spectrally-efficient spread spectrum schemes. First, message-driven frequency hopping was proposed. By

transmitting a large portion of the information through message-driven hopping frequency control, spectral efficiency of the FH systems can be improved by multiple times. It turns out that the enhanced MDFH can further increase the spectral efficiency by allowing simultaneous transmission over multiple frequency bands, and can readily be extended to a collision-free multiple access scheme. In the meantime, information confidentiality was reinforced since the message-driven hopping pattern is totally unpredictable. Secondly, the collision-free frequency hopping scheme was developed based on the OFDM framework and the AES-controlled dynamic subcarrier index assignment algorithm. It is a highly efficient secure communication interface from a cross-layer perspective, since users always transmit on non-overlapping sets of subcarriers in multiple access environment. While keeping the inherent anti-jamming feature of the FH system, CFFH can relax the strict synchronization requirement suffered by the conventional FH systems. Our quantitative performance analysis and simulation examples demonstrated the superior performance of the proposed schemes.

CHAPTER 4

PHY Layer Built-in Security Analysis and Enhancement Algorithms

This chapter considers the enhancement of the PHY layer built-in information confidentiality of wireless systems by integrating cryptographic techniques into the transceiver design. First, security weakness of the operational and proposed CDMA airlink interfaces is analyzed. Secondly, based on AES, secure scrambling is designed to strengthen the physical layer built-in security of CDMA systems through the encrypted long code sequence. Thirdly, motivated by the fact that chips spread from one symbol still cluster together after scrambling and are fragile to deep fading and/or strong burst errors, a chip-level secure interleaving procedure is introduced as a substitution of securing scrambling to further protect wireless transmission from severe channel conditions. Security and performance analyses demonstrate that while providing significantly improved information confidentiality, CDMA systems with secure scrambling/secure interleaving have comparable computational complexity with that of conventionally scrambled systems. Simulation examples are provided to illustrate the robustness of CDMA systems with secure interleaving in adverse environments.

Moreover, possible extension of secure scrambling and secure interleaving to general wireless systems is investigated.

4.1 Introduction

Spread spectrum wireless system was historically developed for secure communication and military use. In spread spectrum systems, each user is assigned a specific spreading sequence to modulate its message signal. The spreading process increases the bandwidth of the message signal by a factor N, known as spreading factor or the processing gain, and meanwhile reduces the power spectrum density of the signal also by a factor N. With large bandwidth and low power spectrum density, spread spectrum signals are resistant to malicious narrow-band jamming and can easily be concealed within the noise floor, preventing from being detected by an unauthorized person. Moreover, the message signal cannot readily be recovered unless the spreading sequence is known, which makes it difficult for an unauthorized person to intercept the signal. It is also known as the physical layer built-in security feature of spread spectrum systems.

Due to relatively high spectral efficiency and simplicity in system planning [63, 64], spread spectrum is now finding widespread civilian and commercial applications such as cellular phones, personal communications and position location [88]. From multiple access system design point of view, since all users in a spread spectrum system are allowed to transmit through the same frequency band simultaneously, each user has a unique spreading code, which is used at the receiver end to perform multiuser signal separation and detection, spread spectrum system is also termed as *code-division multiple access* system. As is well known, CDMA is used in the US digital cellular

standard IS-95 [89] and has been identified as the major modulation technique for third generation (3G) wireless communications and beyond.

Relying on the long pseudo-random spreading sequence generator, the operational CDMA system (IS-95) and the proposed 3GPP UMTS system can provide a near-satisfactory physical layer built-in security solution to voice-centric wireless communications, which generally last only a short period of time. However, the security features provided by these systems are far from adequate and being acceptable when used for wireless data communications. In [90] and [91], the physical layer security weakness of the operational IS-95 CDMA airlink interface was analyzed. It was pointed out that as long as up to 42 contiguous long code sequence bits are intercepted, the whole long code sequence can be regenerated according to the Berlekamp-Massey algorithm [92]. Once the long code sequence is recovered, the desired user's signal can be recovered through various signal separation and extraction algorithms, see [93–95] for example.

Instead of using the conventional scrambling scheme as in IS-95 or 3GPP UMTS, encrypted long code based on AES is proposed to be used in the scrambling process. Next, motivated by concern that chips spread from one symbol still cluster together after spreading and scrambling and are thus fragile to severe fading effects or burst errors, in which the whole symbol may be lost, we consider using chip-level secure interleaving to replace secure scrambling. Ensured by AES, the proposed schemes can improve the physical layer built-in security of CDMA systems significantly. Performance analysis demonstrates that CDMA systems with secure scrambling have comparable computational complexity and system performance with that of the IS-95 systems, and CDMA systems with secure interleaving gain advantages of combating adverse transmission environments. Moreover, by scrambling the training sequence independently with a different scrambling sequence, both information privacy and

system performance can be further improved. Both secure scrambling and secure interleaving can be extended to wireless systems other than DS-CDMA in multiple ways. As a start point, secure interleaving is integrated with the commonly deployed FEC (forward error control) process so that strong information confidentiality can be achieved through secure channel coding. The simplicity and effectiveness of the proposed schemes make them particularly attractive for 3G systems and beyond.

The rest of the chapter is organized as follows. Section 4.2 gives a quick review of the conventional DS-CDMA system as well as the built-in security features. In Section 4.3, security weakness of the existing CDMA airlink interfaces is investigated. Section 4.4 introduces two security enhancement approaches based on the AES algorithm, and the relationship between scrambling and interleaving is discussed. Security of the proposed schemes is analyzed in Section 4.5. Comparison of computational complexity and system performance are provided in Section 4.6. Discussion on extension of the developed methods is presented in Section 4.7 and we conclude in Section 4.8.

4.2 System Description

In the operational and proposed DS-CDMA systems, as shown in Figure 4.1, each user's signal is first spread using a code sequence (known as *channelization code*) spanning over just one symbol or multiple symbols. The spread signal is then further scrambled using a pseudo-random sequence, to randomize the interference and meanwhile make it difficult to intercept and detect the transmitted signal.

Consider a DS-CDMA system with N_u users and K receive antennas. Assuming the processing gain is N, that is, there are N chips per symbol. Let $u_j(k)$ $(j = 1, \cdots, N_u)$

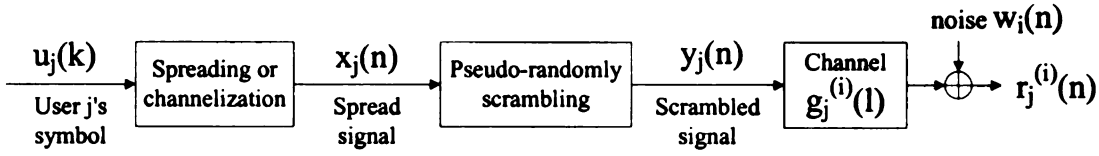


Figure 4.1. Block diagram of a long code DS-CDMA system.

denote the jth user's kth symbol. Without loss of generality, let

$$\mathbf{c}_j = [c_j(0), c_j(1), \cdots, c_j(N-1)] \tag{4.1}$$

denote the jth user's channelization code or spreading code. The spread chip-rate signal can be expressed as

$$x_j(n) = \sum_{k=-\infty}^{\infty} u_j(k) c_j(n - kN). \tag{4.2}$$

The successive scrambling process is achieved by

$$y_j(n) = x_j(n) d_j(n), \tag{4.3}$$

where $d_j(n)$ is the jth user's chip-rate scrambling sequence.

Let $\{g_j^{(i)}(l)\}_{l=0}^{L-1}$ denote the (chip-rate) channel impulse response from the jth user to the ith antenna, the received chip-rate signal at the ith antenna ($i = 1, 2, \cdots, K$) can be written as

$$r_i(n) = \sum_{j=1}^{N_u} \sum_{l=0}^{L-1} g_j^{(i)}(l) y_j(n-l) + w_i(n). \tag{4.4}$$

where $w_i(n)$ is the additive white noise.

From (4.4), we can see that it is nearly impossible to recover the desired user's signal without the knowledge of either the user's channelization code or scrambling

code. This is known as the *built-in security* feature of DS-CDMA systems.

4.3 Physical Layer Built-in Security Evaluation for IS-95 and 3GPP UMTS CDMA Systems

Since the channelization codes are chosen to be Walsh codes, which are easy to generate, the physical layer built-in information privacy of CDMA systems mainly relies on the long pseudo-random scrambling sequence, also known as *long code.* In the following, taking as typical examples of spread spectrum systems, we evaluate the physical player built-in security of the operational IS-95 system and the proposed 3GPP UMTS system.

4.3.1 Recovery of the Long Code Sequences in IS-95 Systems

In IS-95, the long code generator consists of a 42-bit binary string called *long code mask* and a 42-bit LFSR specified by the following characteristic polynomial:

$$\begin{aligned} & x^{42} + x^{35} + x^{33} + x^{31} + x^{27} + x^{26} + x^{25} \\ & + x^{22} + x^{21} + x^{19} + x^{18} + x^{17} + x^{16} \\ & + x^{10} + x^{7} + x^{6} + x^{5} + x^{3} + x^{2} + x + 1, \end{aligned} \tag{4.5}$$

where the 42-bit long code mask is shared between the mobile and the base station.

As shown in Figure 4.2, each chip of the long code is generated by the modulo-2 inner product of the 42-bit mask and the 42-bit state vector of the LFSR shared between the mobile handset and the base station.

Let $\mathbf{m} = [m_1, m_2, \cdots, m_{42}]$ denote the 42-bit mask and $\mathbf{s}(t) =$

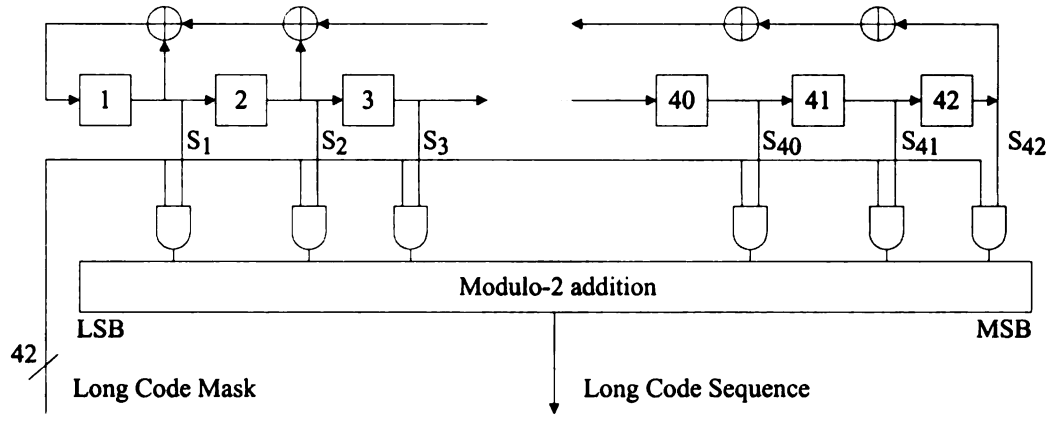


Figure 4.2. Long code generator in IS-95 systems.

$[s_1(t), s_2(t), \cdots, s_{42}(t)]$ denote the state of the LFSR at time instance t. The long code sequence $c(t)$ at time t can thus be represented as

$$c(t) = m_1 s_1(t) + m_2 s_2(t) + \cdots + m_{42} s_{42}(t), \tag{4.6}$$

where the additions are modulo-2 additions.

As is well known, for a sequence generated from an n-stage linear feedback shift register, if an eavesdropper can intercept a $2n$-bit sequence segment, then the characteristic polynomial and the entire sequence can be reconstructed according to the Berlekamp-Massey algorithm [92]. This leaves an impression that the maximum complexity to recover the long code sequence $c(t)$ is $O(2^{84})$. However, for IS-95, since the characteristic polynomial is known to the public, an eavesdropper only needs to obtain 42 bits of the long code sequence to determine the entire sequence. That is, the maximum complexity to recover the long code sequence $c(t)$ is only $O(2^{42})$.

In fact, since $s_1(t), s_2(t), \cdots, s_{42}(t)$ are the outputs of the same LFSR, they should

all be the same except for a phase difference, i.e.,

$$s_{42}(t) = s_{41}(t-1) = \cdots = s_1(t-41). \tag{4.7}$$

Let $\mathbf{a} = [a_1, a_2, \cdots, a_{42}]$ denote of the coefficient vector of the characteristic polynomial in (4.5), then it follows from (4.7) that

$$\begin{aligned} s_1(t) &= a_1 s_1(t-1) + a_2 s_2(t-1) + \cdots + a_{42} s_{42}(t-1) \\ &= a_1 s_1(t-1) + a_2 s_1(t-2) + \cdots + a_{42} s_1(t-42). \qquad (4.8) \\ s_i(t) &= s_1(t-i+1), \quad \forall i \in [2, 42]. \qquad (4.9) \end{aligned}$$

After some manipulations on (4.8) and (4.9), we have, for $i = 1, \cdots, 42$,

$$s_i(t) = a_1 s_i(t-1) + a_2 s_i(t-2) + \cdots + a_{42} s_i(t-42). \tag{4.10}$$

Substituting (4.10) into (4.6), we have

$$\begin{aligned} c(t) &= \sum_{i=1}^{42} m_i s_i(t) \\ &= \sum_{i=1}^{42} m_i \left(\sum_{j=1}^{42} a_j s_i(t-j) \right) \\ &= \sum_{j=1}^{42} a_j \left(\sum_{i=1}^{42} m_i s_i(t-j) \right) \\ &= \sum_{j=1}^{42} a_j c(t-j). \end{aligned}$$

Define

$$\mathbf{A} = \begin{bmatrix} a_1 & 1 & 0 & \cdots & 0 \\ a_2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{41} & 0 & 0 & \cdots & 1 \\ a_{42} & 0 & 0 & \cdots & 0 \end{bmatrix}, \tag{4.11}$$

then it follows that

$$[c(t), c(t-1), \cdots, c(t-41)] = [c(t-1), c(t-2), \cdots, c(t-42)]\mathbf{A}. \tag{4.12}$$

Let $\mathbf{c}(t) = [c(t), c(t-1), \cdots, c(t-41)]$, then for any $n \geq t$, from (4.12) we have

$$\mathbf{c}(n) = \mathbf{c}(t)\mathbf{A}^{n-t}. \tag{4.13}$$

Thus, as long as $\mathbf{c}(t)$ for a time instance t is known, the entire long code sequence can be recovered. In other words, as long as an eavesdropper can intercept/recover up to 42 contiguous long code sequence bits, the whole long code sequence can be regenerated. Therefore, the long code sequence of IS-95 is vulnerable under ciphertext-only attacks as the maximum complexity to recover it is only $O(2^{42})$ [91].

4.3.2 Recovery of the Long Code Sequences in 3GPP UMTS Systems

In the 3GPP UMTS standard, Gold codes (I sequence and Q sequence) generated from two generator polynomials of degree 18 are used as scrambling codes, as shown in Figure 4.3.

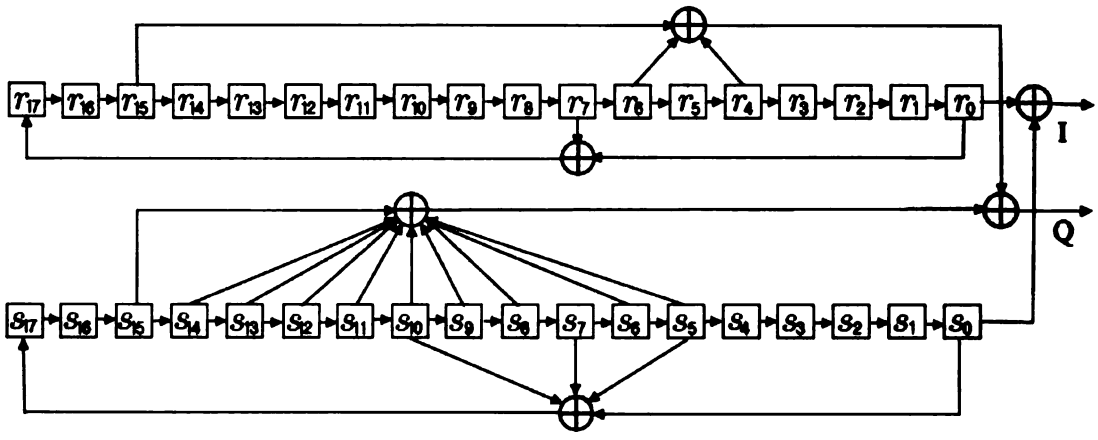


Figure 4.3. Scrambling sequence generator in 3GPP UMTS systems.

Denote the states for the two LFSRs at time instance t as $\mathbf{r}(t) = [r_{17}(t), r_{16}(t), \cdots, r_1(t), r_0(t)]$ and $\mathbf{s}(t) = [s_{17}(t), s_{16}(t), \cdots, s_1(t), s_0(t)]$, where

$$\begin{aligned} r_{17}(t) &= r_7(t-1) + r_0(t-1), \\ s_{17}(t) &= s_{10}(t-1) + s_7(t-1) + s_5(t-1) + s_0(t-1). \end{aligned}$$

Then at time instance t, sequence I can be written as

$$I(t) = r_0(t-1) + s_0(t-1), \tag{4.14}$$

while sequence Q can be expressed as [80]

$$Q(t) = \sum_{i=0}^{17} a_i r_i(t-1) + \sum_{i=0}^{17} b_i s_i(t-1),$$

where a_i and b_i are either 0 or 1 as shown in Figure 4.3.

Note that $r_0(t) = r_1(t-1) = \cdots = r_{17}(t-17)$ and $s_0(t) = s_1(t-1) = \cdots =$

$s_{17}(t-17)$, we have

$$Q(t) = \sum_{i=0}^{17} a_i r_0(t+i-1) + \sum_{i=0}^{17} b_i s_0(t+i-1). \tag{4.15}$$

From (4.14) and (4.15), it follows that the maximum complexity to recover the scrambling code of the 3GPP UMTS system based on ciphertext-only attack is $O(2^{36})$.

This implies that the physical layer built-in security of the 3GPP UMTS system is actually weaker than that of the IS-95 system.

4.3.3 Recovery of the Desired Information

Once the long code sequence is recovered, the desired user's signal can be recovered through signal separation and extraction techniques. If the training sequence is known, simple receivers, for example, the Rake receiver, can be used to extract the desired user's signal. For secure transmission, it is reasonable to assume that the training sequence of the desired user is unknown, however, it is still possible to recover the signal through blind multiuser detection and signal separation [93,94,96–98], which rely only on the statistics of the input signals and the received signals, but independent of the training sequence. When taking security into consideration, blind signal detection turns out to be a *double-edged sword* as it can also be used by malicious users to obtain the desired information.

Recently, blind multiuser detection methods targeting at long-code CDMA systems have been proposed. Based on the channel model, existing blind algorithms can roughly be divided into three categories: (i) Symbol-by-symbol approaches, see [99–102] for example, in which channel estimation and equalization are carried out for each individually received symbol by taking instantaneous estimates of signal

statistics based on the sample values of each symbol. (ii) Frame-by-frame approaches, see [95, 103] for example. Algorithms in this category stack the total received signal corresponding to a whole frame or slot into a long vector, and formulate a deterministic channel model. (iii) Chip-level equalization, see [104–108] and references therein. In this category, by taking chip-rate information as input, the time-varying effect of the pseudo-random sequence is absorbed into the input sequence, and chip-level equalization is performed as the receiver.

All the existing work on blind detection reveals the vulnerability of long-code CDMA systems: **recovery of the long code sequence largely implies immediate security compromise and the interception of the user's data transmission.**

4.4 Confidentiality Enhancement through Secure Scrambling and Secure Interleaving

Having demonstrated the weakness of the stand-alone CDMA built-in security mechanism, we plan to fundamentally strengthen the built-in security through design integration with cryptographic techniques, while minimizing the changes required to the existing standards. More specifically, to reinforce information confidentiality, we propose to enhance the physical layer built-in security by integrating the state-of-the-art cryptographic techniques into the physical layer transceiver design. We will focus our discussion on the IS-95 system as it has a stronger physical layer security and the results can be directly applied to 3GPP UMTS systems.

4.4.1 Security Scrambling Based on AES

In the first stage, advanced cryptographic algorithms are incorporated into the scrambling process of CDMA systems. Instead of using the pseudo-random sequences directly as scrambling sequences, we encrypt them first with advanced cryptographic algorithms (e.g., AES), and then use the encrypted sequences as the scrambling sequences.

As shown in Figure 4.4, the proposed secure scrambling is essentially a counter mode AES. In Figure 4.4, $s_0 s_1 s_2 \cdots$ represents the output of the LFSR characterized by (4.5) as in the IS-95 system, K is the 128-bit common secret encryption key shared between the base station and the mobile station (K can also be 192 bits or 256 bits, as specified by the AES algorithm), and $M_0, M_1, \cdots, M_i$ denote successive message blocks with size of 128 bits, d is the shift between the successive inputs to the AES engine. If the input to the i-th encryption block is $s_{t+id}, s_{t+1+id}, \cdots, s_{t+127+id}$ with initial delay t, then the input to the $(i+1)$-th block is $s_{t+(i+1)d}, s_{t+1+(i+1)d}, \cdots, s_{t+127+(i+1)d}$. The selection of d should maximize the diversity between different inputs to the AES engine, which can be achieved by requiring d and $2^{42} - 1$ be relatively prime. In other words, d should not be divided by 3, 7, 43 and 127.

The secure scrambling process can be summarized as follows:

1. The base station and the mobile station share a common initial state for the LFSR and an L-bit ($L = 128, 192$ or 256) common secret encryption key K;

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

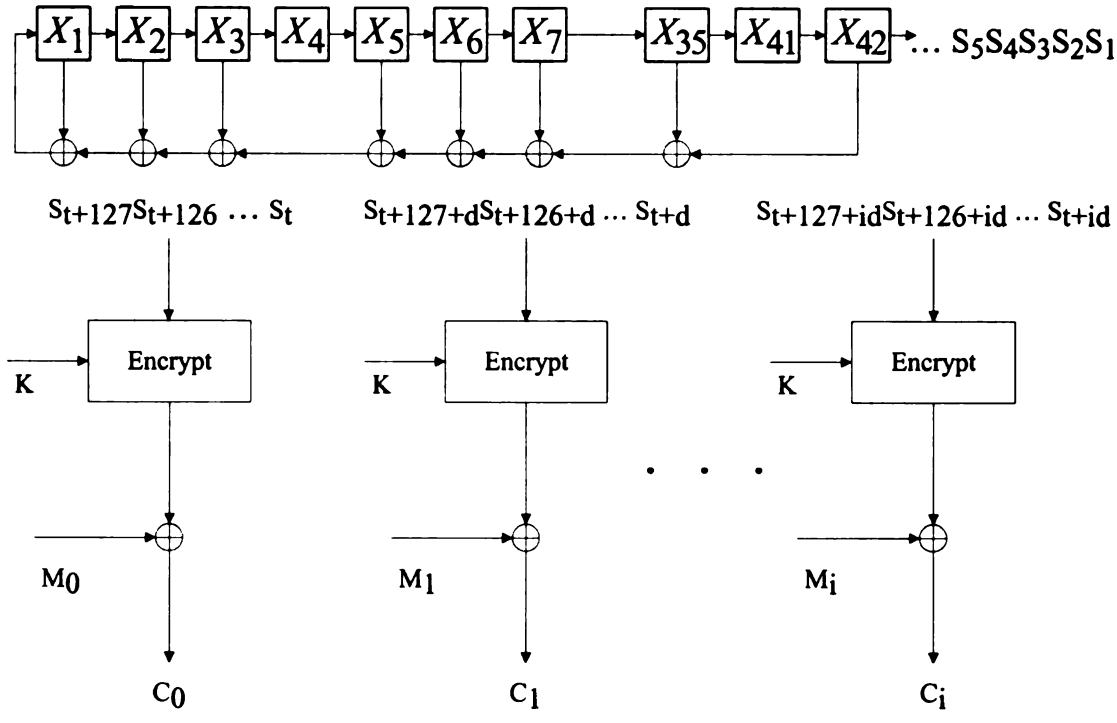


Figure 4.4. Design of physical layer secure scrambling in DS-CDMA systems.

3. The scrambling process is realized by implementing the exclusive OR (XOR) operation between the scrambling sequence and the chip-rate spread signal.

For the 3GPP system, secure scrambling can be performed in the same manner by applying AES to the I, Q scrambling sequences separately. As described in [109,110], the shared secret data between the mobile station and the base station can be updated from time to time. To prevent malicious key reload, the key update request can only be initiated from the base station.

Note that after spreading and scrambling, chips spread from one symbol still cluster together, and could be fragile to deep fading or burst errors, in which the whole symbol may be lost. Interleaving is a widely used technique to randomize burst errors. In this following subsections, we first investigate the relationship between interleaving and scrambling, and then consider using chip-level secure interleaving to replace

scrambling. The purpose is to further protect wireless transmission from strong burst errors and severe fading while enhancing the security measure at the same time.

4.4.2 Relationship between Scrambling and Interleaving

Interleaving is commonly used to obtain time diversity without adding any overhead. An interleaver π is a permutation $i \mapsto \pi(i)$ that changes the time order of an input data sequence. If the input data sequence is $\mathbf{d} = [d_1\ d_2\ \cdots\ d_N]$, then the interleaved data sequence is given by $\mathbf{d}^{\pi} = \mathbf{d} \cdot P$, where P is a permutation matrix with a single one in each row and column, all other entries being zero.

From a mathematical point of view, the process of chip-level interleaving in a DS-CDMA system with BPSK modulation can be represented by:

$$\mathbf{y}_j^{\pi} = \mathbf{y}_j \cdot \mathbf{c}_j,\ j = 1, \cdots, N_u, \tag{4.16}$$

where $\mathbf{y}_j$ is the jth user's chip sequence before interleaving, $\mathbf{y}_j^{\pi}$ denotes the jth user's interleaved chip sequence and "$\cdot$" represents element-wise production. $\mathbf{c}_j$ turns out to be a binary ($\pm$ 1) vector which can be viewed as a special scrambling sequence. That is, *interleaving is a special case of scrambling.* However, *scrambling is not necessarily a case of interleaving*, because scrambled chip sequence may not be permuted to the original chip sequence by simply arranging the time order of the scrambled sequence in all possible ways.

If the interleaver is deep enough, the resulting $\mathbf{c}_j$ will be a random sequence, which can scramble the spread data sequence so that the interference caused by multiple access can be effectively suppressed. That is, the major functionality of scrambling sequence can be retained by a random interleaver.

The advantage of an interleaver is to randomize the information sequence so that even if the successive data symbols undergo deep fading or strong burst noise, they will not possibly be corrupted at the same time. In fact, after interleaving, the corrupted chips will be uniformly distributed over several original bits so that each bit only suffers a small portion of loss and can still be correctly recovered. Therefore, chip-level interleaver can effectively combat deep fade with relatively long duration, such as more than half of the symbol period, in which case the scrambling process will most likely result in an error during signal detection.

4.4.3 System Model for DS-CDMA Systems with Chip-Level Interleaving

Since interleaving can randomize the spread data sequence so as to suppress the interference like scrambling, we propose to use chip-level interleaving as a substitution of scrambling.

Again consider a DS-CDMA system with N_u users, as shown in Figure 4.5. The chip-rate spread signal can be written as

$$x_j(n) = \sum_{k=-\infty}^{\infty} u_j(k)c_j(n - kN). \tag{4.17}$$

where $u_j(k)$ $(j = 1, \cdots, N_u)$ denotes the jth user's kth symbol, $c_j(n)$ is the jth user's spreading code with processing gain N. The successive interleaving process is achieved by

$$y_j(n) = \pi_j(x_j(n)), \tag{4.18}$$

where π_j represents a one-to-one mapping from $x_j(n)$ to $y_j(n)$.

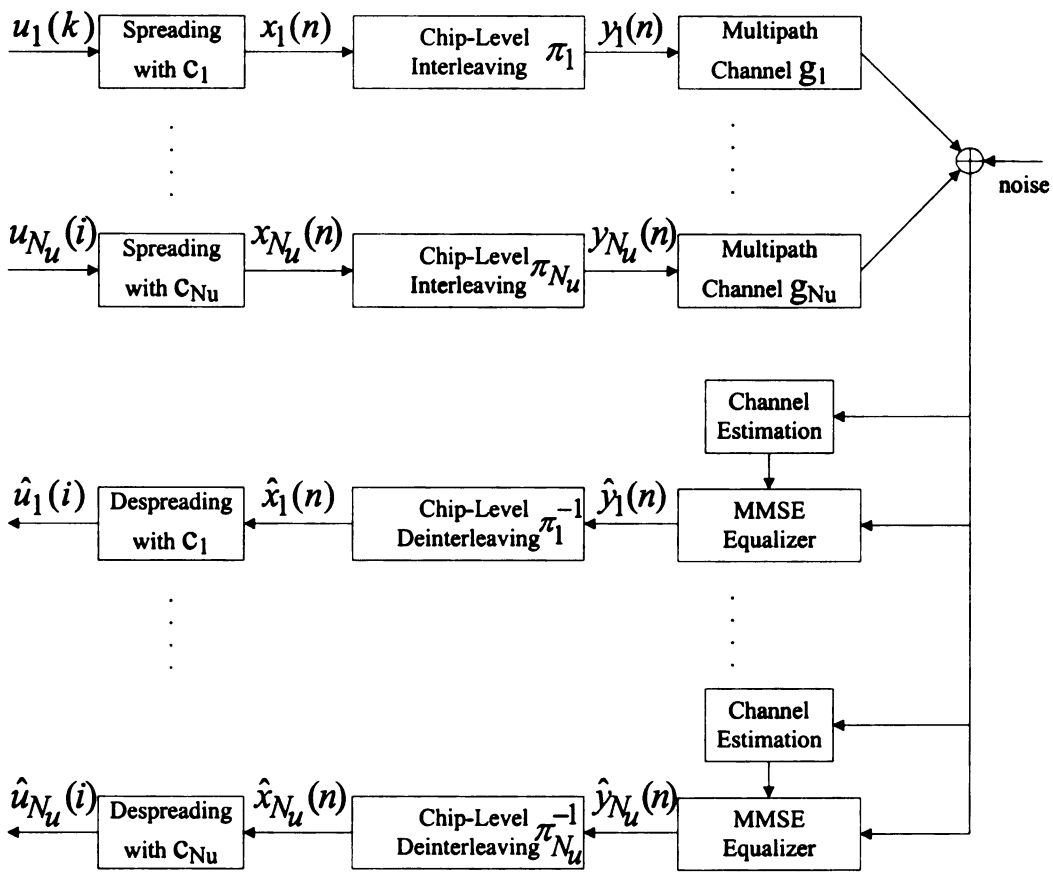


Figure 4.5. Block diagram of a DS-CDMA system with chip-level interleaving.

Let $\{g_j^{(i)}(l)\}_{l=0}^{L-1}$ denote the (chip-rate) channel impulse response from the jth user to the ith receiver, the received chip-rate signal can be expressed as

$$r_i(n) = \sum_{j=1}^{N_u} \sum_{l=0}^{L-1} g_j^{(i)}(l) y_j(n-l) + w_i(n), \tag{4.19}$$

where $w_i(n)$ are samples of zero-mean complex Gaussian random process independent of the information sequences.

At the receiver end, channel estimation is performed through correlation-based method and MMSE equalizer is applied to compensate the disturbance induced by multipath propagation. Then, chip-level deinterleaving and despreading are sequentially carried out to recover the symbol-level signals.

Without the knowledge of interleaver/deinterleaver, it is intractable to recover the desired user's signal. Consequently, the physical layer built-in security of the proposed scheme relies on the security of the interleaver/deinterleaver. In the next subsection, we aim to generate a secure interleaver in combination with the AES algorithm.

4.4.4 Secure Block Interleaving Based on AES

The secure block interleaving is easy to implement and can be summarized as the following three steps:

i. Stack the chip-level sequence column-wise into a conventional block interleaver of size $N_r \times N_c$, where N_r, N_c are powers of 2, and $N_r N_c \geq L_c$, where L_c is the length of the chip sequence. If $\frac{L_c}{N_r}$ is not an integer, fill in the rest of the block interleaver with 0's.

ii. Calculate the row index vector for the mth row using AES algorithm, denoted

by π_m^r, for $m = 1, 2, \cdots, N_r$. Similarly, calculate the column index vector for the nth column, denoted by π_n^c, for $n = 1, 2, \cdots, N_c$.

iii. Perform row permutation π_m^r for the mth row, for $m = 1, 2, \cdots, N_r$, followed by column permutation π_n^c for the nth column, for $n = 1, 2, \cdots, N_c$, then read out the contents of the interleaver in row-wise.

For clarity, we take a 128 × 128 block interleaver as an example, to illustrate the generation of a row index vector π_m^r. The column index vector π_n^c can be created in the same manner.

1. Specify an arbitrary 128-bit plaintext and a 128-bit key. Encrypt the plaintext with the key using the AES algorithm. The resulting ciphertext is also 128 bits, denoted by $\{b_1, b_2, \cdots, b_{128}\}$.

2. Because the subcarrier index is from 1 to 128, each position can be represented by $\log_2(128) = 7$ bits. Form a 1×134 vector by cyclic padding, $[b_1\ b_2\ \cdots\ b_{128}\ b_1\ b_2\ \cdots\ b_6]$. Then split it into 128 7-bit groups as follows:

$$[b_1\ b_2\ \cdots\ b_7],\ [b_2\ b_3\ \cdots\ b_8]\ \cdots,\ [b_{128}\ b_1\ \cdots\ b_6]. \tag{4.20}$$

3. For $i = 1, 2, \cdots, 128$, let $P(i)$ denote the decimal number corresponding to the ith 7-bit vector $\mathbf{b}(i)$ ($\triangleq [b_{(i-1 \bmod 128)+1}\ b_{(i \bmod 128)+1}\ \cdots\ b_{(i+5 \bmod 128)+1}]^T$) with the first element being the most significant, i.e.,

$$P(i) = [2^6\ 2^5\ 2^4\ 2^3\ 2^2\ 2^1\ 2^0]\mathbf{b}(i) + 1. \tag{4.21}$$

Define $\mathcal{P} = [P(1)\ P(2)\ \cdots\ P(128)]$. $\mathcal{P}$ does not necessarily contain all the numbers from 1 to 128 as there might exist some numbers occurring more than once. The following operations are performed to replace all the repeated numbers with the missing numbers:

(a) By comparing with the set of all the indices $[1, 2, 3, \cdots, 128]$, we can find all the missing numbers in $\mathcal{P}$ and stack them into a vector $\mathcal{A}$, $\mathcal{A} = [A(1)\ A(2)\ \cdots\ A(\mathcal{M})]$.

(b) Find the indices of each repeated number in $\mathcal{P}$ and stack them to formulate another vector $\mathcal{B}$, $\mathcal{B} = [B(1)\ B(2)\ \cdots\ B(\mathcal{M})]$. Clearly the length of $\mathcal{A}$ is equal to that of $\mathcal{B}$.

(c) Let $\mathcal{P}(B(i)) = A(i)$, i.e., substitute $A(i)$ for the $B(i)$'s entry in $\mathcal{P}$, for $i = 1, \cdots, \mathcal{M}$.

The resulting vector $\mathcal{P}$ contains all the indices from 1 to 128, and each number occurs only once. This index vector is exactly a row permutation, called "*row interleaver*".

Similarly, we can obtain the rest 127 row interleavers and all 128 column interleavers. The complete secure block interleaving process is illustrated in Figure 4.6.

At the receiver end, "*secure block deinterleaving*" is performed by reverse permutation. Both the transmitter and the receiver share the same key and initial vectors to generate synchronous row index vectors and column index vectors.

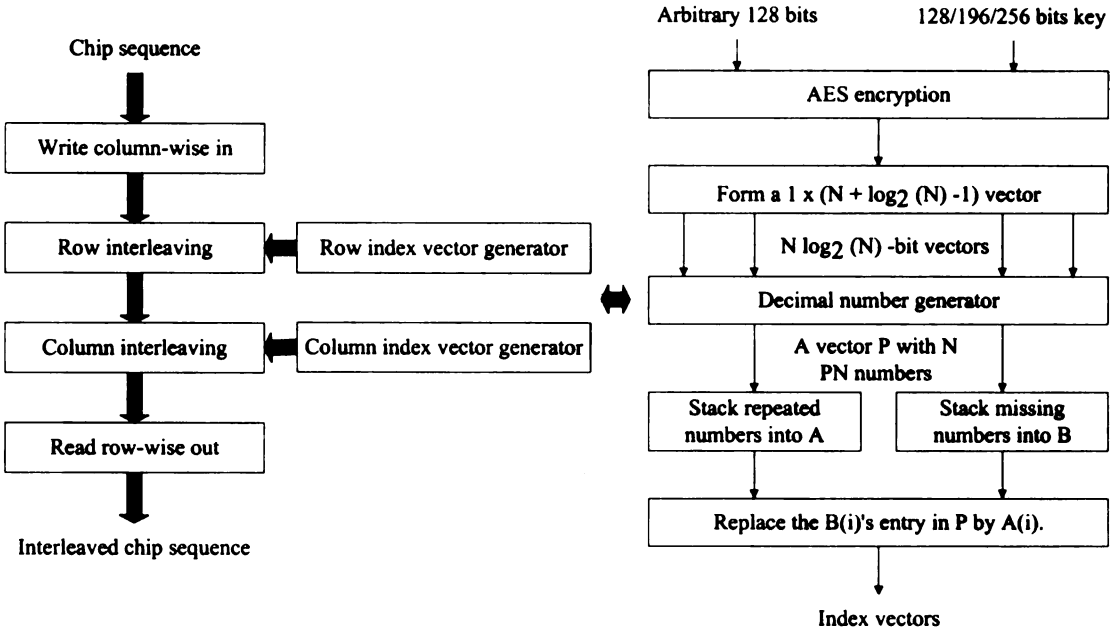


Figure 4.6. Design flowchart of secure block interleaving.

4.5 Security Analysis of the Proposed Scrambling and Interleaving Processes

4.5.1 Security Based on the Large Key Space

We use Data Encryption Standard (DES) [111] as a benchmark to evaluate the security of the proposed secure scrambling and secure block interleaving, which are essentially ensured by AES. We compare the number of possible keys of AES and that of IS-95 scrambling sequence. The number of keys determines the effort required to crack the cryptosystem by trying all possible keys.

The most important reason for DES to be replaced by AES is that it is becoming possible to crack DES by exhaustive key search. Single DES uses 56-bit encryption key, which means there are approximately 7.2×10^{16} possible DES keys. In the late

1990s, specialized "DES Cracker" machines were built and could recover a DES key within a few hours. In other words, by trying all possible key values, the hardware could determine which key was used to encrypt a message [112]. Compared with DES, IS-95 has only 42-bit shared secret, i.e., the initial states of LFSR. The approximate number of keys is about 4.40×10^{12}, which is less than 10^{-4} of the number of DES 56-bit keys. This makes it possible to break the IS-95 long code mask almost in real time through exhaustive key search.

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

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

Thus, if we choose $L = 128$, then there are on the order of 10^{21} times more AES 128-bit keys than DES 56-bit keys. Assuming that one could build a machine that could recover a DES key in a second (i.e., try 2^{55} keys per second), as we can see, this is a very ambitious assumption and far from what we can do today, then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key. To put that into perspective, the universe is believed to be less than 20 billion years old.

Security measurement through the number of all possible keys is based on the assumption that the attacker has no easy access to the secret encryption key, therefore, the attacker has to perform an exhaustive key search in order to break the system. As is well known, the security of AES is based on the infeasible complexity in recovering the encryption key. Currently, no weakness has been detected for AES, thus, exhaustive

key search is still being recognized as the most effective method in recovering the encryption key and breaking the cryptosystem. In the case of secure scrambling, in order for the attacker to obtain the scrambling sequence, the attacker needs to know the input sequence and encryption key. It is reasonable to require that the 42 bits initial state of the LFSR in Figure 4.4 be kept secret together with the 128-bit encryption key. And the attacker will only have access to the scrambled message sequence, for which the secure scrambling sequence is generated from encryption of a 128-bit segment of the LFSR sequence using 128-bit shared secret key between the mobile station and the base station.

As pointed out in Section 4.3.1, for the IS-95 system, the entire scrambling sequence can be regenerated as long as 42 contiguous bits of the scrambling sequence are recovered. In the proposed secure scrambling, even if one block of the scrambling sequence is intercepted, the attacker still needs to recover the secret key K and the input segments $[s_{t+id} \cdots s_{t+127+id}]$ in order to regenerate the entire scrambling sequence, that is, the attacker still needs to break AES. Similarly, for secure block interleaving, even when one row or column interleaver is accidentally exposed to the attacker, regenerating the entire secure block interleaver yet requires to crack the secret key K. Infeasible complexity in recovering the encryption key of AES ensures that the proposed schemes can significantly improve the physical layer built-in security of CDMA systems.

4.5.2 Security Based on the Inherent Ambiguity in Signal Detection

Next, we evaluate the cost of each attack in wireless systems with built-in security. Note that complex signal detection processes must be performed first before decryp-

tion, as part of attacker's key recovery process. The computational complexity of signal detection process is analyzed by enumerating the amount of relevant operations required to extract a block of information bits. In general, we define multiplication as a basic operation to estimate the computational complexity. The addition operation is ignored because it can be much faster than the multiplication in hardware implementation.

First, we consider the single user case. Since the receiver generally consists of channel estimator, equalizer, slicer and channel decoder that are connected in serial, the cost of the signal detection process can be estimated separately. Let L be the channel order, L_t the length of training sequence. The computational complexity of two training-based channel estimation methods is listed in Table 4.1.

Table 4.1. Complexity of training-based channel estimation methods.

	Correlation-based	Lease Square
Complex Multiplications	$O(L_t \cdot L)$	$O(L_t \cdot L^2)$

Let M be the constellation size, L_s the block length of symbol sequence. Table 4.2 gives the computational complexity of commonly used symbol detection methods.

Table 4.2. Complexity of commonly used symbol detection methods.

	Rake	ZF	ML
Complex Multiplications	$O(L_s \cdot (L+M))$	$O(L_s \cdot (L_s^2+M))$	$O(M^{L_s})$

If channel coding is employed, decoding has to be performed before decryption. Take the prevalent turbo coding as an example. Factors determining computational complexity of a turbo decoder include state complexity, iterations allowed, and number of constituent decoders. With the BCJR decoding algorithm, the amount of complex multiplications is approximately given by $(10 \cdot S + 2) \cdot I \cdot L_b \cdot P$, where S is the number

of states, I is the number of iterations, L_b is the block size of information bit, and P is the number of constituent decoders. The code rate R is defined as $R \triangleq \frac{L_b}{L_s \log_2 M}$.

Next, for the purpose of the numerical evaluation, we reduce all involved multiplications to a set of logical operations – *bitwise-AND* and *bitwise-OR*. For an n-bit multiplier, the required number of two-input AND and OR gates are $(6n^3 - 5n^2)$, $(3n^3 - 3n^2)$, respectively. Usually, $n = 16$, which indicates 23296 AND and 11520 OR operations involved in one 16-bit multiplication. Assume we use the relatively simple receiver structure: correlation-based channel estimation and Rake receiver, for a DS-CDMA system with $N = 16$, and let $L = 5$, $L_t = 16$, $L_b = 640$, $L_s = 320$, $M = 16$, $S = 8$, $I = 5$, $P = 2$, $R = 1/2$. Each source data block consists of 640 bits, which indicates 5 AES encryptions (with key length of 128 bits). The results with regard to complexity evaluation of signal detection and source data decryption are reported in Table 4.3.

Table 4.3. Complexity evaluation of signal detection and source data decryption in the single-user case.

	AND	OR	Total operations
Signal detection	4.934×10^{10}	2.440×10^{10}	7.374×10^{10}
AES decryption	2.070×10^{5}	2.053×10^{5}	4.123×10^{5}

It can be observed from Table 4.3 that the cost of each attack, measured in terms of the total number of required logical operations, is drastically increased from $O(10^5)$ to $O(10^{10})$. Computational complexity in signal detection process actually predominates over decryption efforts in each attempt to crack the secret key. Thus, the built-in security makes information recovery much more formidable to a malicious user.

For the multiuser case, signal detection for the desired user becomes more complicated, as the interference, in addition to channel distortion caused by fading effects and multipath propagation, arises in multiple access environment. Various multiuser

detection (MUD) techniques have been proposed to mitigate MAI based on the knowledge of spreading codes, see [113–115] for example. With secure scrambling or secure interleaving, the cost evaluation of signal detection should include the extra complexity involved in MUD process. In [116, 117], two low-complexity iterative multiuser receivers were proposed for turbo-coded DS-CDMA systems. The total number of operations required in multiuser detection process for one block of all users' information is listed in Table 4.4. Here, R is the code rate of the turbo code in use, I_b is the block size, N_u denotes the number of users and I_u stands for the number of iterations in multiuser detection.

Table 4.4. Computational complexity of two iterative multiuser receivers.

Method	Complexity for extraction one block of all user's information
MUD in [116]	$[N_u^2/R + I_u(3N_u^2 + 3N_u + 2)/(2R)]I_b$
MUD in [117]	$[2^{N_u}(7{N_u}^3 + 24{N_u}^2 + 36N_u + 24)/(6R) + I_u 2^{N_u}(N_u - 1)/R]I_b$

Consider a DS-CDMA system with processing gain $N = 16$. We determine the total number of logical operations required for recovering all users' information using the receivers proposed in [116, 117], both of which include matched filter, iterative signal detector and turbo decoder. Let $L = 5$, $L_t = 16$, $L_b = 640$, $L_s = 1280$, $M = 2$, $S = 8$, $I = 5$, $P = 2$, $R = 1/2$, $N_u = 4$, $I_u = 5$. Based on the results in Table 4.5, the cost of each attack is increased by one order of magnitude in the multi-user case.

Table 4.5. Complexity evaluation of signal detection in the multi-user case.

	AND	OR	Total operations
Receiver in [116]	2.53×10^{11}	1.25×10^{11}	3.78×10^{11}
Receiver in [117]	3.31×10^{11}	1.64×10^{11}	4.95×10^{11}

If malicious users decide to extract all users' information jointly, the key space grows exponential with the number of users, eventually leading to the exponentially increased complexity in signal detection. Now assume each user uses a 128-bit secret

key in a DS-CDMA system with secure scrambling. Note that the conventional IS-95 system only has 42-bit shared secret. For these two systems, the maximum complexity to recover all users' data information is calculated in Table 4.6.

Table 4.6. Maximum complexity of recovering all four users' information.

	AND	OR	Total operations
Conventional Scrambling	9.49×10^{61}	4.69×10^{61}	1.32×10^{62}
Secure Scrambling	3.38×10^{165}	1.67×10^{165}	5.05×10^{165}

As can be seen, joint multiuser information recovery for DS-CDMA systems with FEC requires prohibitively high computational complexity, which makes exhaustive key search attack more infeasible. Moreover, even if all users' information can be perfectly recovered, attackers still face a big challenge in distinguishing the desired user's signal from others', if no identity is explicitly incorporated in the information stream.

4.6 Performance Analysis of CDMA Systems with Security Enhancement Strategies

Pseudo-random scrambling in CDMA systems provides physical layer built-in user privacy for information transmission. However, from communications point of view, scrambling was originally designed to reduce interference of mobiles that use the same channelization code in different cells, and to ensure performance stability among user population by providing the desired wideband spectral characteristics, since the Walsh functions may not spread each symbol's power spectrum uniformly in the available frequency band [64, 118]. When applying secure scrambling/secure interleaving, two natural questions arise:

1. Will it introduce significant computational complexity?

2. What impact does it have on system performance?

In this section, it will be demonstrated that while providing strong physical layer built-in security, secure scrambling and secure block interleaving have comparable computational complexity and system performance with that of the conventional scrambling process. It is also observed that by scrambling the training sequence independently with a different scrambling sequence, both information privacy and system performance can be further improved.

4.6.1 Computational Complexity

In this subsection, we compare the computational complexity of the proposed secure scrambling, secure block interleaving and the conventional scrambling. For this purpose, we need to compare the complexity of the three generation methods. Note that both conventional and secure scrambling generation approaches use the same 42-bit LFSR as specified in (4.5). In IS-95, each bit of the long scrambling code is generated through

$$c(t) = m_1 s_1(t) + m_2 s_2(t) + \cdots + m_{42} s_{42}(t).$$

For the proposed secure scrambling, every 128-bit block of the scrambling sequence is generated through one AES encryption process. For the secure interleaving, each (1×128) index vector is created by postprocessing a 128-bit binary stream encrypted by AES. For fair comparison, we measure the number of instructions required by each method for every 128 bits, and also the time required for every 128 bits using a Dell computer with 1024M RAM and 2.8GHz CPU speed. The results are provided in Table 4.7. As can be seen, the computational complexity of secure scrambling and

secure block interleaving is both comparable with that of the scrambling process used in IS-95.

Table 4.7. Complexity comparison of two generation methods of long scrambling sequences and one generation method of secure block interleaver.

Method	Number of operations for every 128 bits				Time (seconds)
	AND	OR	BIT-SHIFT	TOTAL	
IS-95	5376	5248	5376	16000	0.0226
Secure Scrambling	19136	15392	8640	43168	0.0536
Secure Interleaving	27584	15520	4160	47264	0.0597

4.6.2 System Performance with Secure Scrambling and Further Improvement Using Separately Scrambled Training Sequence

Under the same spectral efficiency, in this subsection, we compare the input-output BER performance of CDMA systems with conventional scrambling and secure scrambling, respectively. In practical systems, after spreading and scrambling, passband PAM is performed. Mapping information bearing bits to symbols, passband PAM is equivalent to a complex-valued baseband PAM system [63] . When BPSK or QPSK is chosen, the modulo-2 addition between the message bits and the spreading sequence or the scrambling sequence is now equivalent to multiplying the message symbols by binary (± 1) sequences. Our discussion is based on the equivalent discrete-time baseband PAM model of CDMA systems, for which the spreading sequences and scrambling sequences are both binary antipodal sequences.

Based on (4.19), desired user's signal can be extracted through a two-stage procedure. First, training-based channel estimation is performed through correlation. Next, Rake receiver is applied to combine multipath components. It should be pointed out

that currently, it is a common practice in industry to choose the chip-rate training sequence be all 1's. The training sequence is put as a prefix to the chip-rate message sequence, and then scrambled using the long scrambling sequence. Channel estimation is therefore carried out based on the correlation property of the front part of the scrambling sequence.

This practice has two drawbacks. From the security point of view, the front part of the scrambling sequence is exposed to attackers, which makes it possible to recover the whole scrambling sequence right away if secure scrambling is not used. This, in the meantime, illustrates the importance of secure scrambling, which can prevent the whole scrambling sequence being recovered based on the knowledge of part of it. From the performance point of view, the correlation property of part of the scrambling sequence may not be ideal, and it can degrade the system performance due to non-accurate channel estimation.

To overcome these shortcomings, we propose to scramble the training sequence with an independent short scrambling sequence. The training sequence and its scrambling sequence are designed subject to the following constraints:

1. The short scrambling sequence is independent of the long scrambling sequence.
2. The short scrambling sequence has the same length as that of the training sequence.
3. The scrambled training sequence is a Gold sequence.

Or equivalently, we can choose the training sequence to be a Gold sequence and then no scrambling is necessary for it. In the meanwhile, the information sequence is scrambled using the long scrambling sequence. In other words, training sequence is separated from the information sequence in the scrambling procedure. As a result,

the long scrambling sequence will not be exposed to malicious attackers and channel estimation can be performed based on the low cross-correlation of Gold sequences. We term the proposed approach as "*separated training*", and denote the conventional practice by "*non-separated training*".

In the simulation, we only consider the single receiver case. All the other simulation parameters are listed in Table 4.8. The short scrambling sequence is chosen to be Gold sequences of length 63, and training sequence is chosen to be a sequence of all 1's of the same length. Note that the maximum multipath delay is allowed to be up to one symbol period, which is a reasonable assumption for wideband CDMA systems. Figure 4.7 shows the bit error rate versus different SNR levels, assuming four equal power users in the system. SNR is defined as the chip-level SNR with respect to user 1. Multipath channels and information sequences are generated randomly in each Monte Carlo run. And the result is averaged over 100 runs.

Table 4.8. Settings of the DS-CDMA system and the channel model in the simulation.

DS-CDMA system	Spreading codes	Walsh codes
	Processing gain	16
	Training sequence	Gold sequence of length 63
	Block size	1024
	Modulation	QPSK
	Desired user	User 1
Multipath channel	Number of paths	4
	Dominant path	The first path
	Delays of paths	Uniformly distributed over one symbol period

As can be seen, system with secure scrambling has comparable performance with that of IS-95, and "*separated training*" delivers much better results as compared to "*non-separated training*".

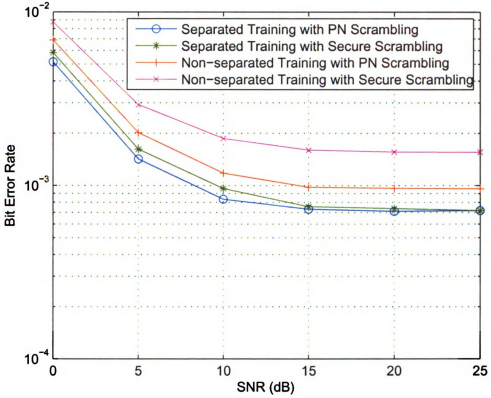


Figure 4.7. BER comparison of conventional scrambling and secure scrambling. Results from Rake receiver with no channel coding, four-ray multipath channel, processing gain $N = 16$, number of user $N_u = 4$.

4.6.3 Performance Improvement Using Secure Interleaving

A CDMA system with eight users is considered. Simulation set-up is listed in the Table 4.8. We follow the system design with separated training. Here, the training sequence is directly chosen to be a Gold sequence of length 63, and thus no scrambling or interleaving process is applied to the training part. The simulation results are averaged over 100 Monte Carlo runs, in which multipath channels and information sequences are generated randomly and independently. SNR is again defined as the chip-level SNR with respect to user 1.

Figure 4.8 and Figure 4.9 show the comparison of system performance over channels with severe fading for four scenarios: conventional scrambling, secure scrambling, pseudo-random interleaving and secure block interleaving. Assume that channel impulse response remains invariant over 1/4 block size and 1/4 block size of the chip sequence undergoes a deep fade through the channel. Pilot symbols are inserted for every 1/4 block to obtain accurate channel information. As can be seen, the proposed system using secure block interleaving has the significant improvement in terms of BER over channels with severe fades.

Figure 4.10 and Figure 4.11 show the comparison of four scenarios when the channel involves strong burst noise. 32 noise bursts, each of which lasts one symbol period and has the same power level as that of the desired user's signal, are randomly generated and added to the randomly selected symbols. The simulation results demonstrate the robustness of the proposed secure interleaving schemes over channels with strong burst errors.

In all, with comparable transmitter complexity, strong PHY layer built-in security can be achieved without any system performance degradation in terms of spectral and power efficiency.

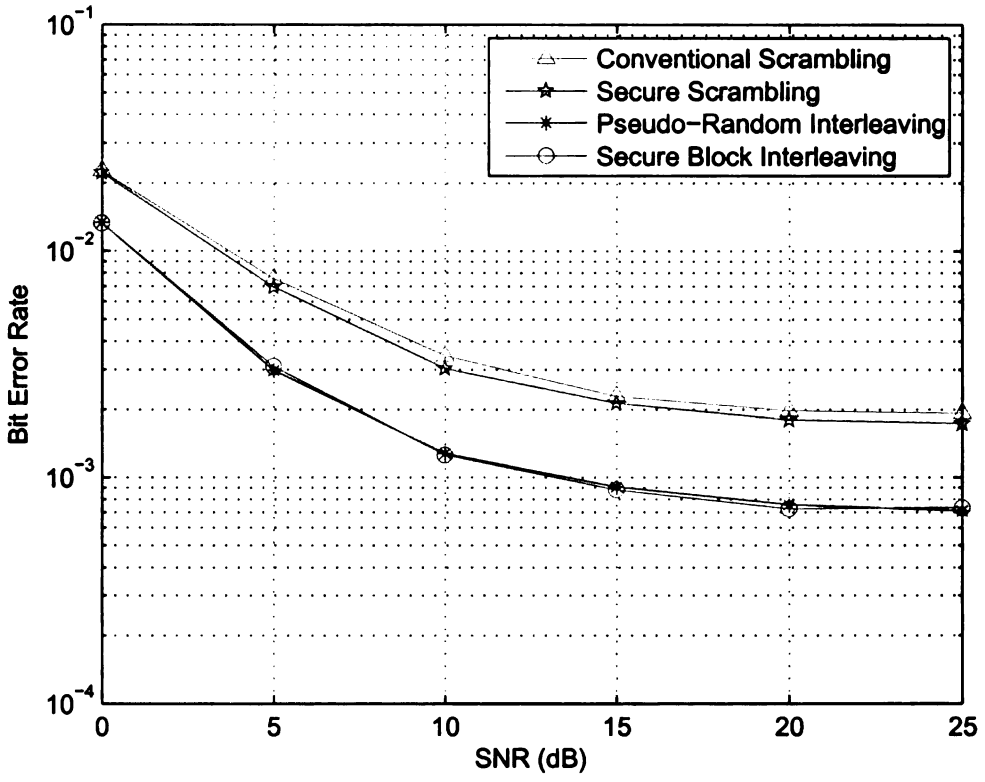


Figure 4.8. BER versus SNR, performance comparison over deep fading channel, processing gain $N = 16$, number of users $N_u = 8$.

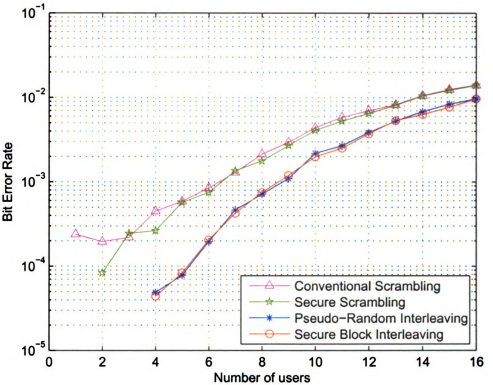


Figure 4.9. BER versus system load, performance comparison over deep fading channel, processing gain $N = 16$, SNR = 20dB.

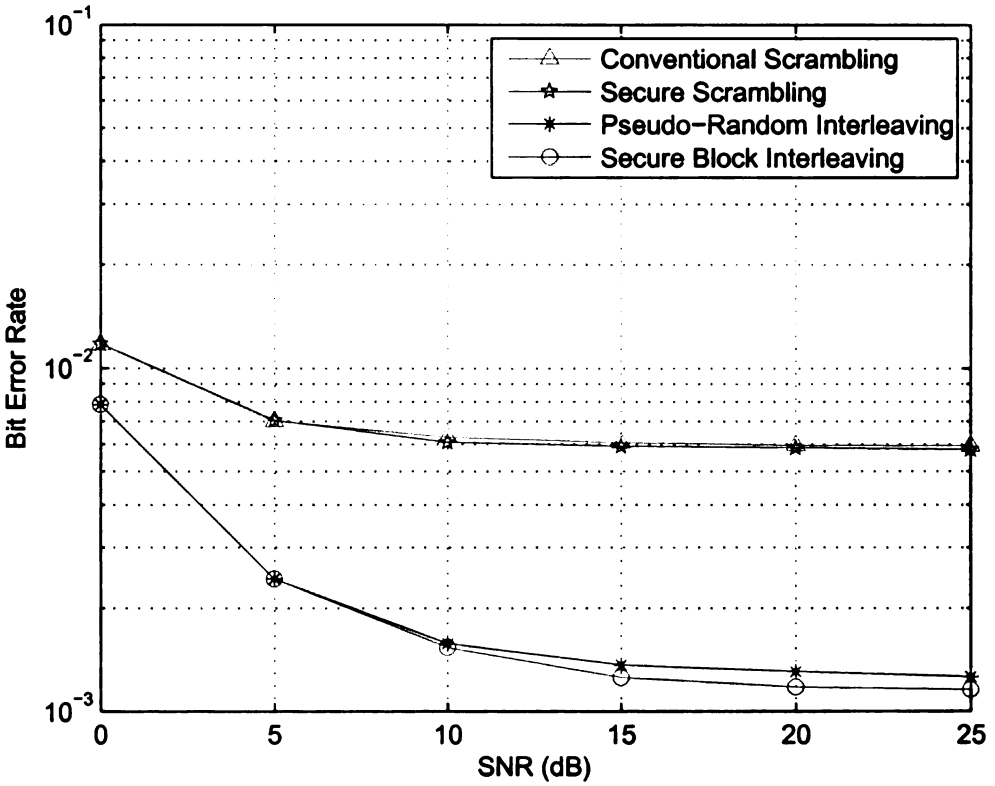


Figure 4.10. BER versus SNR, performance comparison over channel with strong burst noise, processing gain $N = 16$, number of users $N_u = 8$.

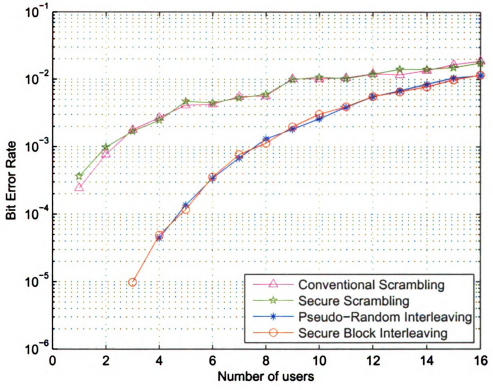


Figure 4.11. BER versus system load, performance comparison over channel with strong burst noise, processing gain $N = 16$, SNR $= 20$dB.

4.7 Discussions and Extension to Other Wireless Systems

From our previous discussion, although there exists a slight increase in complexity if secure scrambling or secure block interleaving is utilized, the physical layer built-in security of the CDMA systems can be improved significantly. Moreover, secure scrambling has the error-tolerant feature, i.e., an individual error in the received message will have a limited local effect, it will not prevent the decryption of other parts of the message. This feature is very helpful under circumstances where retransmission is difficult or even impossible. With secure blocking interleaving, higher layer data encryption is no longer necessary for the information bit stream, since a sophisticated design of pseudo-random permutation is equivalent to encryption of data blocks. Without the knowledge of the corresponding deinterleaver, the complexity of exhaustive search eventually makes malicious extraction of original information prohibitively infeasible.

It should be pointed out that both secure scrambling and secure interleaving can be extended to wireless systems other than CDMA in multiple ways, for example, by simply replacing the traditional block interleaving with the secure block interleaver. Here, we explore the possibility of enhancing the PHY layer built-in security of a wireless system by substituting the interleaver in turbo encoders with AES-controlled secure interleaver. As shown in Figure 4.12, in addition to incorporating AES into the interleaver design, secure turbo encoder prevents the systematic bits from direct connection from input to output as in the conventional turbo encoder, thus avoids the disclosure of the user's transmitted information.

The major design challenge lies in the necessary requirement that FEC performance should be preserved. To test the effectiveness of the design integration, we

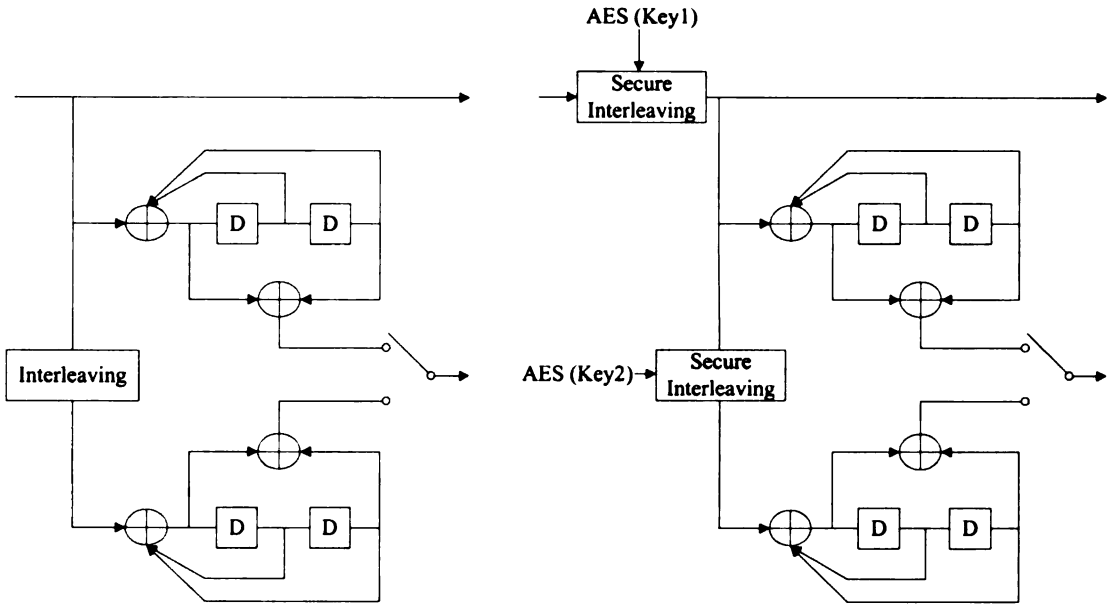


Figure 4.12. Conventional turbo encoder and secure turbo encoder.

carry out one simulation with regard to the performance comparison of the proposed secure turbo coding and the conventional turbo coding. The generation matrix of two component encoders is given by $[1, \frac{(7)_{octal}}{(5)_{octal}}]$, where $(7)_{octal}$ and $(5)_{octal}$ are the feedback and feedforward polynomials with memory length 2, respectively. Two terminating bits are used to force the state of the first component encoder back to zero in each block, and the state of the second component encoder is left open. The block length is 1024. After encoding, encoded bits are mapped into BPSK symbols and transmitted over an AWGN channel. The decoding algorithm is the classic Max-log-MAP. The number of decoding iterations is 4. BER for three different code rates are averaged over 500 Monte Carlo runs. As shown in Figure 4.13, error correcting capability of the proposed secure turbo coding remains the same as that of the conventional turbo coding.

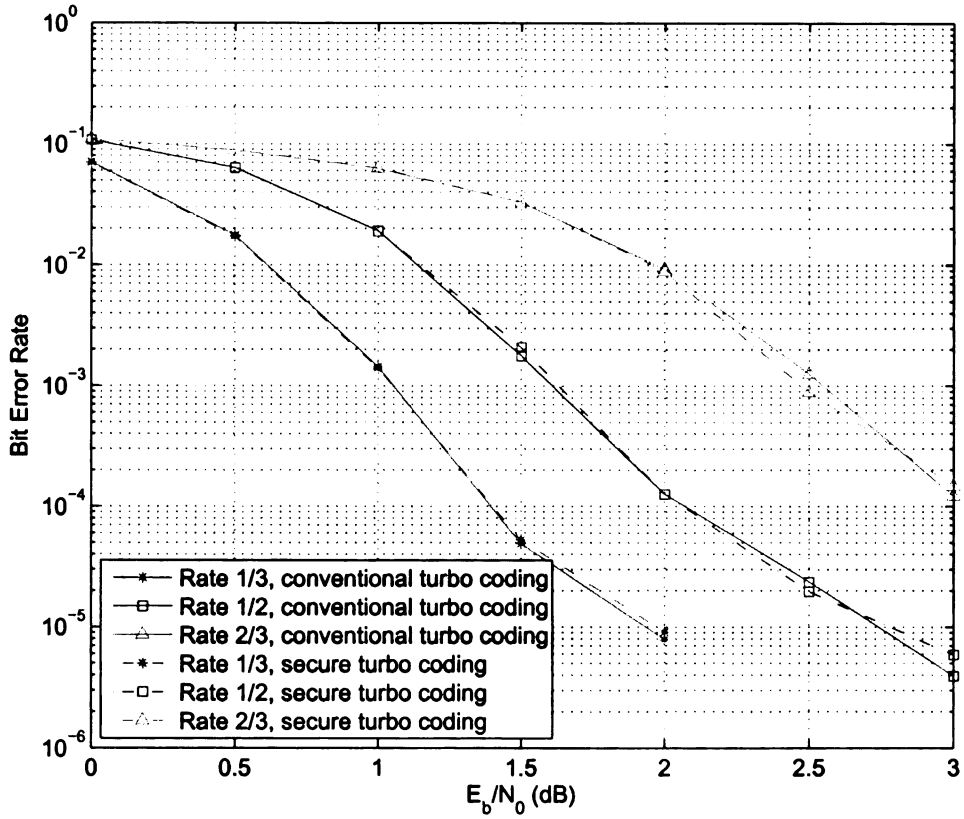


Figure 4.13. BER comparison of the proposed secure turbo coding and the conventional turbo coding.

From security point of view, as a result of the design integration, intruders will have to go through the channel decoding process and signal separation process every time a new key is tested, and thus increase the information confidentiality significantly.

4.8 Summary

In this chapter, security weakness of the operational and proposed CDMA systems was analyzed and two encryption-based security enhancement strategies were presented. First, instead of using the long code sequences generated by the LFSR directly, secure scrambling sequences were generated through AES operations. Secondly, in environment of deep fade or burst noise, secure block interleaving, also based on the AES encryption, was proposed as a substitution of the secure scrambling process. As a result, the physical layer built-in security of the CDMA system was significantly increased with very limited complexity load. Thirdly, by scrambling the training sequence independently with a different scrambling sequence, both information privacy and system performance were further improved. The proposed approaches through design integration with advanced cryptographic techniques is very feasible and can readily be implemented for security enhancement in wireless networks.

CHAPTER 5

Conclusions and Future Work

5.1 Conclusions

In this dissertation, we investigate the major limitations in existing work, and propose to strengthen the inherent security of wireless systems by integrating advanced signal processing techniques and cryptographic techniques into the transmitter-receiver design. In summary, our study on time-variant jamming classification and jamming detection makes it possible to achieve dynamic transmitter adjustment for optimum jamming resistance; Our spectrally efficient anti-jamming air interface design breaks through the bottleneck in developing high-capacity anti-jamming wireless communication systems; Our design of inherently secure wireless systems based on cryptographic techniques and inherent ambiguity in signal detection process greatly improves the information confidentiality and integrity over wireless networks. More specifically, based on our theoretical analyses and simulation results, we have the following conclusions:

On resilient time-variant jamming modeling and detection:

- An innovative two-dimensional jamming generation model is proposed to characterize jamming signals from both the time domain and the frequency domain. It includes all the existing jamming models as special cases, and makes it possible to characterize and track time-variant jamming attacks.

- With the concepts of fast jamming, slow jamming, flat jamming and frequency-selective jamming, a novel systematic jamming classification framework is established. Statistics that characterize the average jamming lasting time and bandwidth are derived from the framework to enable dynamic jamming pattern identification. It is of great significance for the transmitter to adjust itself adaptively to combat time-variant hostile jamming.

- It is important to distinct self-jamming from hostile jamming in multiple access wireless environment where multipath propagation and multiuser interference may occur. The simulation results demonstrate that with self-jamming mitigation techniques applied at the receiver end, the detection of hostile jamming activities becomes much easier and the estimation accuracy of jamming bandwidth/duration is substantially increased.

- By means of the statistical hypothesis test and the measurement of power spectral density of the received signal, both training-based and blind jamming detection approaches are developed. Simulation examples reveal that there is always a tradeoff between the two types of detection errors: probability of miss and probability of false alarm.

On spectrally efficient anti-jamming air interface design:

- The proposed message-driven frequency hopping system overcomes two major limitations of the conventional FH systems: low spectral efficiency over large bandwidth and strong requirement on frequency acquisition. The spectral efficiency is significantly improved by embedding a large portion of information into the hopping frequency selection process, since additional information transmission is achieved with no extra cost on bandwidth or power. Through blind

detection of carrier frequencies, MDFH can resolve the intractable synchronization issue suffered by the conventional FH systems.

- From a security perspective, MDFH has better or at least comparable jamming resistance with the conventional FH, as the hopping frequency in MDFH is determined by the encrypted message signal and the hopping pattern is unpredictable, while in the conventional FH, the hopping pattern is determined by a pre-selected PN sequence.

- The proposed collision-free frequency hopping scheme exploits advanced signal processing techniques and cryptographic techniques from a cross-layer perspective. High information capacity is achieved through the underlying OFDM framework where frequency overlapping is allowed between subcarriers and the collision-free subcarrier assignment in multiple access environment. Superiorities of CFFH in terms of both spectral efficiency and jamming resistance are demonstrated by performance analysis and simulation examples.

- Based on the dynamic subcarrier index assignment algorithm, CFFH is essentially a pseudo-random frequency hopping scheme and thus maintains the inherent anti-jamming, anti-interception security features of the conventional FH system. Furthermore, anonymous multiparty communication can be achieved in CFFH by sending dummy bits on certain subcarriers.

On PHY layer built-in security analysis and enhancement:

- The PHY layer built-in security of the operational and proposed CDMA airlink interfaces is far from adequate and acceptable for high-speed multimedia services, as the maximum complexity to recover the long code sequence generated by the

LFSR is only $O(2^{42})$, making information privacy vulnerable to the brute-force attack.

- By integrating cryptographic techniques into the PHY layer transceiver design, the proposed secure scrambling and secure interleaving can significantly enhance the PHY layer built-in security of the CDMA system with very limited complexity load. These two encryption-based security enhancement approaches can easily be extended to wireless systems other than DS-CDMA in multiple ways.

- The effects of secure scrambling and secure interleaving on computational complexity and system performance are investigated. The simulation results demonstrate that CDMA systems with secure scrambling have comparable computational complexity and system performance with that of the IS-95 systems, and CDMA systems with secure interleaving gain advantages of combating deep fade and burst errors.

- By scrambling the training sequence independently with a different scrambling sequence in DS-CDMA systems, both information privacy and system performance can be further improved.

Overall, we have been focused on the design, analysis and evaluation of inherently secure high capacity wireless communication systems. The proposed techniques can be applied to both civilian and military communication for highly efficient and reliable information transmission.

5.2 Related Future Work

In this section, we discuss the related research topics as a proposal for future work.

Further Directions in Modeling and Detection of Hostile Jamming

- In Chapter 2, a threshold-based approach has been developed to estimate the coherence time of the jamming signals. One further research direction is the estimation of the coherence time and coherence bandwidth of the jamming generation system based on the time-averaged statistics of the jamming signals.

- Detection of hostile jamming has only been considered for spread spectrum systems in Chapter 2. General methods for 3G systems and beyond are worth further investigation.

Further Research on Spectrally Efficient Anti-Jamming System Design

- In Chapter 3, E-MDFH has been proposed by allowing simultaneous transmission over multiple frequency bands to further increase the spectral efficiency. Systematic jamming resistance evaluation in addition to simulation examples needs to be conducted.

- For the CFFH system, we have derived a secure subcarrier assignment algorithm through AES operations. The impact of dynamic resource allocation on performance overhead in terms of throughput and complexity deserve thorough investigation.

Extension in Enhancement of Physical Layer Built-in Security

- Extension of the developed secure interleaving technique to the the commonly deployed FEC process has been introduced. A systematic analysis needs to be performed from both security point of view and system capacity aspects.

APPENDICES

APPENDIX A

List of Abbreviations and Acronyms

3G	Third Generation
3GPP	3rd Generation Partnership Project
A/D	Analog-to-Digital
AES	Advanced Encryption Standard
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPF	BandPass Filter
BPSK	Binary Phase-Shift Keying
CDMA	Code Division Multiple Access
CF-MDFH	Collision-Free Message-Driven Frequency Hopping
CFFH	Collision-Free Frequency Hopping
CSI	Channel State Information
DES	Data Encryption Standard
DPSK	Differential Phase-Shift Keying
DS-CDMA	Direct-Sequence Code Division Multiple Access
DSP	Digital Signal Processing

E-MDFH	Enhanced Message-Driven Frequency Hopping
FD-MDFH	Frequency-Division Message-Driven Frequency Hopping
FEC	Forward Error Control
FFT	Fast Fourier Transform
FFH	Fast Frequency Hopping
FH	Frequency Hopping
FHMA	Frequency Hopping Multiple Access
FSK	Frequency-Shift Keying
GSM	Global System for Mobile communication
IFFT	Inverse Fast Fourier Transform
ISI	Inter-Symbol Interference
JSR	Jamming-to-Signal Ratio
LDPC	Low Density Parity Check
LFSR	Linear Feedback Shift Register
LLR	Log-Likelihood Ratio
LRT	Likelihood Ratio Test
MAI	Multiple-Access Interference
MAP	Maximum A Posteriori
MDFH	Message-Driven Frequency Hopping
ML	Maximum Likelihood
MMSE	Minimum Mean Square Error
MUD	MultiUser Detection
PAM	Pulse Amplitude Modulation
PHY	Physical
PN	Pseudo-Random

PSD	Power Spectral Density
PSK	Phase-Shift Keying
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OSI	Open Systems Interconnection
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase-Shift Keying
SFH	Slow Frequency Hopping
SINR	Signal-to-Interference-Noise Ratio
SNR	Signal-to-Noise Ratio
SOS	Second-Order Statistics
STFT	Short-Time Fourier Transform
TD-MDFH	Time-Division Message-Driven Frequency Hopping
UMTS	Universal Mobile Telecommunications System
WLAN	Wireless Local Area Network
WEP	Wired Equivalent Privacy
WSS	Wide Sense Stationary
XOR	eXclusive OR
ZF	Zero-Forcing

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] In-Stat/MDR, "Worldwide Mobile Subscriber Forecasts - 3G Makes an Appearance," April 2005. [Online]. Available: http://www.instat.com/abstract.asp?id=29&SKU=IN0501705GW

[2] N. T. F. on Interoperability, "Why can't we talk?" 2003. [Online]. Available: http://www.agileprogram.org/ntfi/publications.html

[3] R. Nichols and P. C. Lekkas, *Wireless Security: Models, Threats, and Solutions.* McGraw-Hill Telecom, 2002.

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

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

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

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

[8] R. Haupt, "The development of smart antennas," in *IEEE Antennas and Propagation Society International Symposium*, Boston, MA, Jul. 2001, pp. 48–51.

[9] S. Bellofiore, C. Balanis, J. Foutz, and A. Spanias, "Smart-antenna systems for mobile communication networks. Part 1. Overview and antenna design," *IEEE Antennas and Propagation Magazine*, vol. 44, pp. 145–154, Jun. 2002.

[10] Z. Sun and J. Lu, "Improving the security performance in mobile wireless computing network using smart directional antenna," in *Proceedings of Asia-Pacific Conference on Environmental Electromagnetics*, Nov. 2003, pp. 47–50.

[11] A. Alexiou and M. Haardt, "Smart antenna technologies for future wireless systems: Trends and challenges," *IEEE Communications Magazine*, vol. 42, pp. 90–97, Sept. 2004.

[12] D. Goshi, K. Leong, and T. Itoh, "A secure high-speed retrodirective communication link," *IEEE Transactions on Microwave Theory and Techniques*, vol. 53, pp. 3548–3556, Nov. 2005.

[13] D. Qiao, S. Choi, A. Jain, and K. Shin, "Adaptive transmit power control in 802.11a wireless LANs," in *Proceedings of IEEE Vehicular Technology Conference*, Apr. 2003, pp. 433–437.

[14] J. Carey and D. Grunwald, "Enhancing WLAN security with smart antennas: A physical layer response for information assurance," in *Proceedings of IEEE Vehicular Technology Conference*, Sept. 2004, pp. 318–320.

[15] C. Sperandio and P. Flikkema, "Wireless physical-layer security via transmit precoding over dispersive channels: Optimum linear eavesdropping," in *Proceedings of IEEE Military Communications Conference*, Oct. 2002, pp. 1113–1117.

[16] P. Flikkema, "Exploiting mobility in Ad-Hoc wireless nets: Prospects for physical layer security in dispersive spatio-temporal channels," in *Proceedings of the Third Annual IEEE Information Assurance Workshop*, West Point, NY, Jun. 2002.

[17] X. Li, M. Chen, and P. Ratazzi, "A randomized space-time transmission scheme for secret-key agreement," in *Proceedings of Conference on Information Sciences and Systems*, Mar. 2005, pp. 433–437.

[18] G. Xu and H. Liu, "An effective transmission beamforming scheme for frequency-division-duplex digital wireless communication system," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, May 1995, pp. 1729–1732.

[19] M. Orihashi, Y. Nakagawa, Y. Murakami, and K. Kobayashi, "Channel synthesized modulation employing singular vector for secured access on physical layer," in *Proceedings of IEEE Global Telecommunications Conference*, San Francisco, CA, Dec. 2003, pp. 1226–1230.

[20] I. A.O. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, pp. 3235–3249, Dec. 2003.

[21] X. Li, M. Chen, and E. P. Ratazzi, "Array-transmission based physical-layer security techniques for wireless sensor networks," in *Proceedings of IEEE International Conference on Mechatronics and Automation*, Niagara Falls, Canada, Jul. 2005, pp. 1618–1623.

[22] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Transactions on Communications*, vol. 43, pp. 3–6, Jan. 1995.

[23] M. Horiike and H. Sasaoka, "A scheme of secret key agreement based on the random fluctuation of channel characteristics in land mobile radio," IEICE, Tech. Rep. RCS2002C173, 2002.

[24] H. Liu, G. Xu, and L. Tong, "A deterministic approach to blind identification of multichannel FIR systems," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 4, Apr. 1994, pp. 581–584.

[25] L. Tong, G. Xu, and T. Kailath, "Blind identification and equalization based on second-order statistics: A time domain approach," *IEEE Transactions on Information Theory*, vol. 40, pp. 340–349, Mar. 1994.

[26] L. Tong, G. Xu, B. Hassibi, and T. Kailath, "Blind channel identification based on second-order statistics: A frequency-domain approach," *IEEE Transactions on Information Theory*, vol. 41, pp. 329–334, Jan. 1995.

[27] E. Moulines, P. Duhamel, J.-F. Cardoso, and S. Mayrargue, "Subspace methods for the blind identification of multichannel FIR filters," *IEEE Transactions on Signal Processing*, vol. 43, pp. 516–525, Feb. 1995.

[28] G. Xu, H. Liu, L. Tong, and T. Kailath, "A least-squares approach to blind channel identification," *IEEE Transactions on Signal Processing*, vol. 43, pp. 2982–2993, Dec. 1995.

[29] Y. Hua, "Fast maximum likelihood for blind identification of multiple FIR channels," *IEEE Transactions on Signal Processing*, vol. 44, pp. 661–672, Mar. 1996.

[30] K. Abed-Meraim and Y. Hua, "Blind identification of multi-input multi-output system using minimum noise subspace," *IEEE Transactions on Signal Processing*, vol. 45, pp. 254–258, Jan. 1997.

[31] E. Serpedin and G. Giannakis, "Blind channel identification and equalization with modulation-induced cyclostationarity," *IEEE Transactions on Signal Processing*, vol. 46, pp. 1930–1944, Jul. 1998.

[32] T. Li, Q. Ling, and Z. Ding, "Transmit delay structure design for blind channel estimation over multipath channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, pp. Article ID 26 123, 12 pages, 2007.

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

[34] L. Milstein, D. Schilling, R. Pickholtz, V. Erceg, M. Kullback, E. Kanterakis, D. Fishman, W. Biederman, and D. Salerno, "On the feasibility of a CDMA overlay for personal communication networks," *IEEE Journal on Selected Areas in Communications*, vol. 10, pp. 655–668, May 1992.

[35] M. Mihaljević and J. Golić, "A comparison of cryptanalytic principles based on iterative error-correction," *Advances in Cryptology*, vol. 547, pp. 527–531, 1991.

[36] ——, "Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence," *Advances in Cryptology*, vol. 658, pp. 124–137, 1993.

[37] M. Simon, G. Huth, and A. Polydoros, "Differentially coherent detection of QASK for frequency-hopping systems-Part I: Performance in the presence of a Gaussian noise environment," *IEEE Transactions on Communications*, vol. 30, pp. 158–164, Jan. 1982.

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

[39] J. Cho, Y. Kim, and K. Cheun, "A novel FHSS multiple-access network using M-ary orthogonal Walsh modulation," in *Proceedings of IEEE Vehicular Technology Conference*, vol. 3, Sept. 2000, pp. 1134–1141.

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

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

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

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

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

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

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

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

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

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

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

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

[52] J.-W. Moon, J. Shea, and T. Wong, "Jamming estimation on block-fading channels," in *Proceedings of IEEE Military Communications Conference*, vol. 3, Oct. 31- Nov. 3 2004, pp. 1310–1316.

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

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

[55] S.-J. Lee, H.-Y. Um, S.-Y. Lim, and W.-G. Park, "Adaptive anti-jamming algorithm in DS-CDMA cellular system," in *Proceedings of IEEE Asia Pacific Conference on Circuits and Systems*, Nov. 1996, pp. 342–345.

[56] S.-J. Lee and W.-B. L. amd Hw-Young Um, "Anti-jamming algorithm for traffic load shedding in DS-CDMA cellular system," in *Proceedings of the Third IEEE*

International Conference on Electronics, Circuits, and Systems, vol. 2, Oct. 1996, pp. 1056–1059.

[57] Y. Zhang and J. Dill, "An anti-jamming algorithm using wavelet packet modulated spread spectrum," in *Proceedings of IEEE Military Communications Conference*, vol. 2, Oct. 31-Nov. 3 1999, pp. 846–850.

[58] M. Pursley and J. Skinner, "Turbo product coding in frequency-hop wireless communications with partial-band interference," in *Proceedings of IEEE Military Communications Conference*, vol. 2, Oct. 2002, pp. 774–779.

[59] F. Lau, M. Ye, C. Tse, and S. Hau, "Anti-jamming performance of chaotic digital communication systems," *IEEE Transactions on Circuits and Systems—Part I: Fundamental Theory and Applications*, vol. 49, pp. 1486–1494, Oct. 2002.

[60] G. Huang and L. Yang, "A radar anti-jamming technology based on blind source separation," in *Proceedings of the Seventh International Conference on Signal Processing*, vol. 3, Aug. 31-Sept. 4 2004, pp. 2021–2024.

[61] R. Liu and R. Ying, "Anti-jamming filtering in the autocorrelation domain," *IEEE Signal Processing Letters*, vol. 11, pp. 525–528, Jun. 2004.

[62] Y.-C. Chen and K.-C. Chen, "Anti-jamming and anti-multipath performances of generalized FH/BFSK," in *Proceedings of IEEE Vehicular Technology Conference*, Sept. 2006, pp. 1–5.

[63] J. Proakis, *Digital Communications*, 4th ed. McGraw-Hill, 2000.

[64] T. S. Rappaport, *Wireless Communications - Principles and Practices*, 2nd ed. Prentice Hall, 2002.

[65] R. van Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*. Norwood, MA: Artech House, 2000.

[66] Z. Zvonar, P. Jung, and K. Kammerlander, Eds., *GSM: Evolution Towards 3rd Generation Systems*. Norwell, MA: Kluwer Academic Publishers, 1998.

[67] J. Kang and W. Stark, "Turbo codes for noncoherent FH-SS with partial band interference," *IEEE Transactions on Communications*, vol. 46, pp. 1451–1458, Nov. 1998.

[68] S. Jayaraman and H. Viswanathan, "Optimal detection of a jammed channel," in *Proceedings of IEEE Global Telecommunications Conference*, Nov. 1996, pp. 87–91.

[69] S. Zazo, F. Bader, and J. Paez-Borrall, "A multiple access/self interference canceller receiver for DS-CDMA multiuser detection over fading channels," in *Proceedings of IEEE Vehicular Technology Conference*, vol. 4, Boston, MA, USA, Sept. 2000, pp. 1745–1750.

[70] A. Scaglione and G. Giannakis, "Design of user codes in QS-CDMA systems for MUI elimination inunknown multipath," *IEEE Communications Letters*, vol. 3, pp. 25–27, Feb. 1999.

[71] P. Welch, "The use of fast Fourier transforms for the estimation of power spectra: A method based on time averaging over short modified periodograms," *IEEE Transactions on Audio and Electroacoustics*, vol. 15, pp. 70–73, Jun. 1967.

[72] G. Cooper and R. Nettleton, "A spread spectrum technique for high capacity mobile communuzation," *IEEE Transactions on Vehicular Technology*, vol. 27, pp. 264–275, Nov. 1978.

[73] A. Viterbi, "A processing satellite transponder for multlple access by low-rate mobile users," in *Proceedings of the Fourth International Conference on Digital Satellite Communications*, Montreal, Canada, Oct. 1978, pp. 166–174.

[74] E. Geraniotis, "Multiple-access capability of frequency-hopped spread-spectrum revisited: An analysis of the effect of unequal power levels," *IEEE Transactions on Communications*, vol. 38, pp. 1066–1077, Jul. 1990.

[75] Y. Tsai and J. Chang, "Using frequency hopping spread spectrum technique to combat multipath interference in a multiaccessing environment," *IEEE Transactions on Vehicular Technology*, vol. 43, pp. 211–222, May 1994.

[76] M. Wickert and R. Turcotte, "Probability of error analysis for FHSS/CDMA communications in the presence of fading," *IEEE Journal on Selected Areas in Communications*, vol. 10, pp. 523–534, Apr. 1992.

[77] E. Geraniotis and M. Pursley, "Error probabilities for slow frequency-hopped spread-spectrum multiple-access communication over fading channels," *IEEE Transactions on Communications*, vol. 30, pp. 996–1009, May 1982.

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

[79] F. Fitzek, "The medium is the message," in *Proceedings of IEEE International Conference on Communications*, vol. 11, Jun. 2006, pp. 5016–5021.

[80] T. Li, Q. Ling, and J. Ren, "Physical layer built-in security analysis and enhancement algorithms for CDMA systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, pp. Article ID 83589, 7 pages, 2007.

[81] Q. Ling, T. Li, and Z. Ding, "A novel concept: Message driven frequency hopping (MDFH)," in *Proceedings of IEEE International Conference on Communications*, Glasgow, Scotland, Jun. 2007, pp. 5496–5501.

[82] D. Goodman, P. Henry, and V. Prabhu, "Frequency-hopped multilevel FSK for mobile radio," *Bell System Technical Journal*, vol. 59, pp. 1257–1275, Sept. 1980.

[83] J. Marcum, "Table of Q functions," *U.S. Air Force Project RAND Res. Memo. M-339*, Jan. 1950, ASTIA Document AD 1165451, Rand Corp.

[84] E. Lawrey and C. J. Kikkert, "Adaptive frequency hopping for multiuser OFDM," in *Proceedings of the Second International Conference on Information, Communications and Signal Processing*, vol. 1, Singapore, Dec. 1999, pp. 183–187.

[85] T. Scholand, T. Faber, Y. C. Juho Lee, Joonyoung Cho, and P. Jung, "Physical layer performance of a novel fast frequency hopping-OFDM concept," in *Proceedings of the 14th IST Mobile and Wireless Communications Summit*, Dresden, Germany, Jun. 2005.

[86] *Advanced Encryption Standard*, ser. FIPS-197, National Institute of Standards and Technology Std., Nov. 2001. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[87] J. Woodard and L. Hanzo, "Comparative study of turbo decoding techniques: an overview," *IEEE Transactions on Vehicular Technology*, vol. 49, pp. 2208–2233, Nov. 2000.

[88] P. Enge, "The global positioning system: Signals, measurements, and performance," *International Journal of Wireless Information Networks*, vol. 1, pp. 83–105, Apr. 1994.

[89] V. Garg, *IS-95 CDMA and cdma2000.* Prentice Hall, 2000.

[90] T. Li, J. Ren, Q. Ling, and W. Liang, "Physical layer built-in security analysis and enhancement of CDMA systems," in *Proceedings of Conference on Information Sciences and Systems*, Princeton, NJ, Mar. 2004.

[91] M. Zhang, C. Carroll, and A. Chan, "Analysis of IS-95 CDMA voice privacy," in *Proceedings of the Seventh Annual International Workshop on Selected Areas in Cryptography*, London, UK, 2000, pp. 1–13.

[92] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. 15, pp. 122–127, Jan. 1969.

[93] S. Bhashyam and B. Aazhang, "Multiuser channel estimation and tracking for long-code CDMA systems," *IEEE Transactions on Communications*, vol. 50, pp. 1081–1090, Jul. 2002.

[94] C. Escudero, U. Mitra, and D. Slock, "A Toeplitz displacement method for blind multipath estimation for long code DS/CDMA signals," *IEEE Transactions on Signal Processing*, vol. 49, pp. 654–665, Mar. 2001.

[95] L. Tong, A.-J. van der Veen, P. Dewilde, and Y. Sung, "Blind decorrelating RAKE receivers for long-code WCDMA," *IEEE Transactions on Signal Processing*, vol. 51, pp. 1642–1655, Jun. 2003.

[96] S. H. (Ed.), *Unsupervised Adaptive Filtering, Volume 1: Blind Source Separation.* Wiley, John & Sons, Inc., 2000.

[97] S. Haykin, *Unsupervised Adaptive Filtering, Volume 2: Blind Deconvolution.* Wiley, John & Sons, Inc., 2000.

[98] Z. Ding and Y. Li, *Blind Equalization and Identification.* Marcel Dekker, Jan. 2001.

[99] A. Weiss and B. Friedlander, "Channel estimation for DS-CDMS downlink with aperiodic spreading codes," *IEEE Transactions on Communications*, vol. 47, pp. 1561–1569, Oct. 1999.

[100] Z. Yang and X. Wang, "Blind multiuser detection for long-code multipath CDMA," in *Proceedings of Asilomar Conference on Signals, Systems and Computers*, vol. 2, Oct.29-Nov. 1 2000, pp. 1148–1152.

[101] Z. Xu and M. Tsatsanis, "Blind channel estimation for long code multiuser CDMA systems," *IEEE Transactions on Signal Processing*, vol. 48, pp. 988–1001, Apr. 2000.

[102] Z. Xu, "Low-complexity multiuser channel estimation with aperiodic spreading codes," *IEEE Transactions on Signal Processing*, vol. 49, pp. 2813–2822, Nov. 2001.

[103] Y. Sung and L. Tong, "Tracking of fast-fading channels in long-code CDMA," *IEEE Transactions on Signal Processing*, vol. 52, pp. 786–795, Mar. 2004.

[104] H. Liu and M. Zoltowski, "Blind equalization in antenna array CDMA systems," *IEEE Transactions on Signal Processing*, vol. 45, pp. 161–172, Jan. 1997.

[105] C. Frank, E. Visotsky, and U. Madhow, "Adaptive interference suppression for the downlink of a direct sequence CDMA system with long spreading sequences,"

The Journal of VLSI Signal Processing-Systems for Signal, Image, and Video Technology, vol. 30, pp. 273–291, 2002.

[106] T. Krauss, W. Hillery, and M. Zoltowski, "Downlink specific linear equalization for frequency selective CDMA cellular systems," *The Journal of VLSI Signal Processing-Systems for Signal, Image, and Video Technology*, vol. 30, pp. 143–161, 2002.

[107] T. Li, J. K. Tugnait, and Z. Ding, "Channel estimation for long-code CDMA systems utilizing transmission introduced cyclostationarity," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 4, Apr. 2003, pp. 105–108.

[108] T. Li, Z. Ding, J. K. Tugnait, and W. Liang, "Channel identification and signal separation for long-code CDMA systems using multistep linear prediction method," in *Proceedings of IEEE International Conference on Communications*, vol. 4, Paris, France, Jun. 2004, pp. 2437–2441.

[109] *Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System*, TIA/EIA/IS-95-B Std. TIA/EIA/IS-95-B, 1998.

[110] V. Garg, *IS-95 CDMA and cdma2000: Cellular/PCS Systems Implementation.* Pearson Education, 1999.

[111] *DES Modes of Operation*, Federal Information Processing Standard Publication 81, US National Bureau of Standards Std., Dec. 1980. [Online]. Available: http://www.itl.nist.gov/fipspubs/fip81.htm

[112] Electronic Frontier Foundation (EFF), "EFF DES Cracker Project," 2002. [Online]. Available: http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/

[113] R. Lupas and S. Verdu, "Linear multiuser detectors for synchronous code-division multiple-access channels," *IEEE Transactions on Information Theory*, vol. 35, pp. 123–136, Jan. 1989.

[114] S. Moshavi, "Multi-user detection for DS-CDMA communications," *IEEE Communications Magazine*, vol. 34, pp. 124–136, Oct. 1996.

[115] X. Wang and H. V. Poor, "Iterative (turbo) soft interference cancellation and decoding for coded CDMA," *IEEE Transactions on Communications*, vol. 47, pp. 1046–1061, Jul. 1999.

[116] J.-M. Hsu and C.-L. Wang, "A low-complexity iterative multiuser receiver for turbo-coded DS-CDMA systems," *IEEE Journal on Selected Areas in Communications*, vol. 19, pp. 1775–1783, Sept. 2001.

[117] M. Reed, C. Schlegel, P. Alexander, and J. Asenstorfer, "Iterative multiuser detection for CDMA with FEC: near-single-user performance," *IEEE Transactions on Communications*, vol. 46, pp. 1693–1699, Dec. 1998.

[118] S. Parkvall, "Variability of user performance in cellular DS-CDMA - long versus short spreading sequences," *IEEE Transactions on Communications*, vol. 48, pp. 1178–1187, Jul. 2000.